Pillai College Of Engineering,New Panvel

Department of Computer Engineering

Subject: Computer Network

Class: Third Year

Sem: V

Academic

Year:2024-2025

How You Can define the Computer Network ?

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their **Resources, Data, and Applications.**

Resources

1. Computer system
2. PDA
3. Mobile devices
4. Printer
5. Camera

Data

1. Text
2. Images
3. Audio, Video files

Applications

1. Game
2. Offices

Uses of Computer Network

1. **Business Applications**

   a)Resources sharing

   b)Virtual Private Network

   c) Client Server model(web application) d) VOIP,email

2. **Home Application**

   a)Social network

   b)facebook

   c)Wikipedia

3. **Mobile user**
4. **Social Issues**

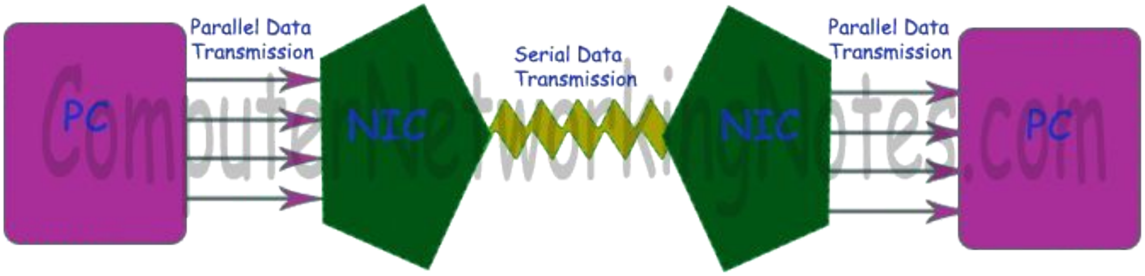
Interconnecting Devices

Network devices are the devices that interconnect networks. Because these devices connect network entities, they are known as connectivity devices. These devices include:

- Network Interface Card
- HUB
- Switches
- Router
- Repeaters
- Modem

Network Interface card (NIC)

- NIC stands on the first place. Without this device, networking cannot be done.
- This is also known as network adapter card, Ethernet Card and LAN card.
- NIC allows a networking device to communicate with the other networking device.
- NIC converts the data packets between two different data transmission technologies.
- A PC uses parallel data transmission technology to transmit the data between its internal parts while the media that provides connectivity between different PCs uses serial data transmission technology.
- A NIC converts parallel data stream into the serial data stream and the serial data stream into the parallel data stream.

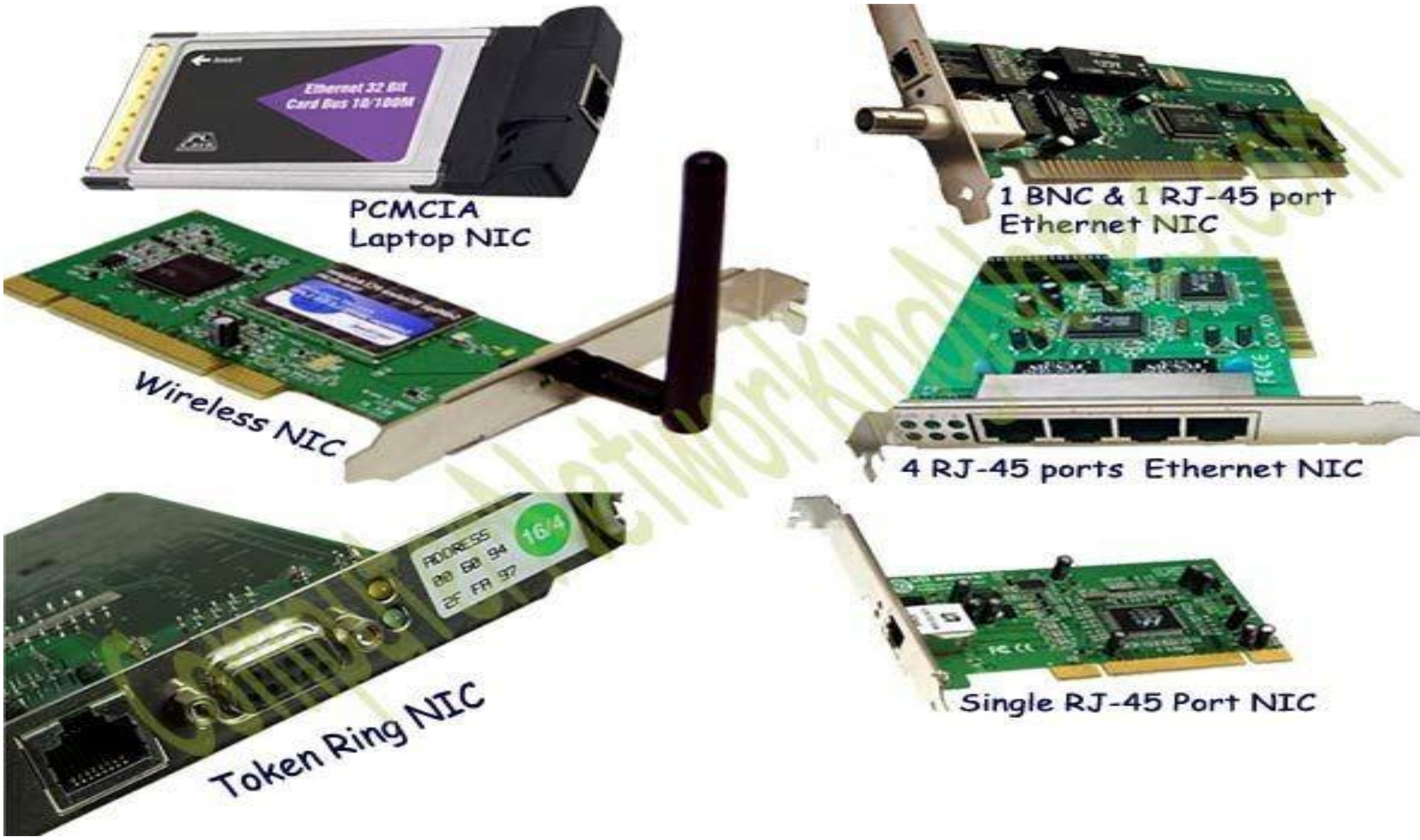

PC
Parallel Data Transmission
NIC
Serial Data Transmission
NIC
Parallel Data Transmission
PC
ComputerNetworkingNotes.com

Types of NIC Card

There are two types

1. **Media Specific:** LAN card are used according to the media type. Different types of the NICs are used to connect the different types of media. To connect a specific media type, we must have to use a NIC which is particularly made for that type of media.

2. **Network Design Specific:** A specific network design needs a specific LAN card. For example **FDDI** (Fiber distributed Data Interface), **Token Ring** and **Ethernet** have their own distinctive type of NIC cards. They cannot use other types of NIC cards.


PCMCIA Laptop NIC
Ethernet 32 Bit Card Bus 10/100M
1 BNC & 1 RJ-45 port Ethernet NIC
Wireless NIC
4 RJ-45 ports Ethernet NIC
ADDRESS 00 60 94 2F FA 97
16/4
Token Ring NIC
Single RJ-45 Port NIC

HUB(Hybrid Universal Broadcast)

- Hub is a centralized device that connects multiple devices in a single LAN network.
- When Hub receives the data signals from a connected device on any of its port, except that port, it forwards those signals to all other connected devices from the remaining ports.
- Usually, Hub has one or more uplink ports that are used to connect it with another Hub.
- Hubs are used in networks that use twisted-pair cabling to connect devices.
- Hubs can also be joined together to create larger networks.
- A hub does not perform any processing on the data that it forwards, nor does it perform any error checking.
- A hub has no intelligence—it sends all data received on any port to all the other ports. So, devices connected through a hub receive everything that the other devices send, whether or not it was meant for them. This process called broadcasting).
- **Note: A hub just repeats all the data received on any port to all the other ports; thus, hubs are also known as repeaters**

There are two types of the Hub.

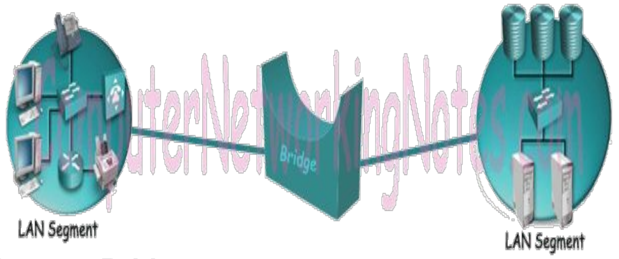
Passive Hub: - It forwards data signals in the same format in which it receives them. It does not change the data signal in any manner.

Active Hub: - It also works same as the passive Hub works. But before forwarding the data signals, it amplifies them. Due to this added feature, the active Hub is also known as the repeater.

Bridge

Bridge is used to divide a large network into smaller segments. Basic functions of the Bridge are the following:-

- Breaking a large network into smaller segments.
- Connecting different media types. Such as connects UTP with the fiber optic.
- Connecting different network architectures. Such as connects Ethernet with the Token ring.
- A Bridge can connect two different types of media or network architecture, but with same protocol
- There are three types of Bridge:-
- **Local Bridge**: - This Bridge connects two LAN segments directly. In Ethernet Implementation, it is known as the Transparent Bridge. In Token Ring network, it is called the Source-Routed Bridge.

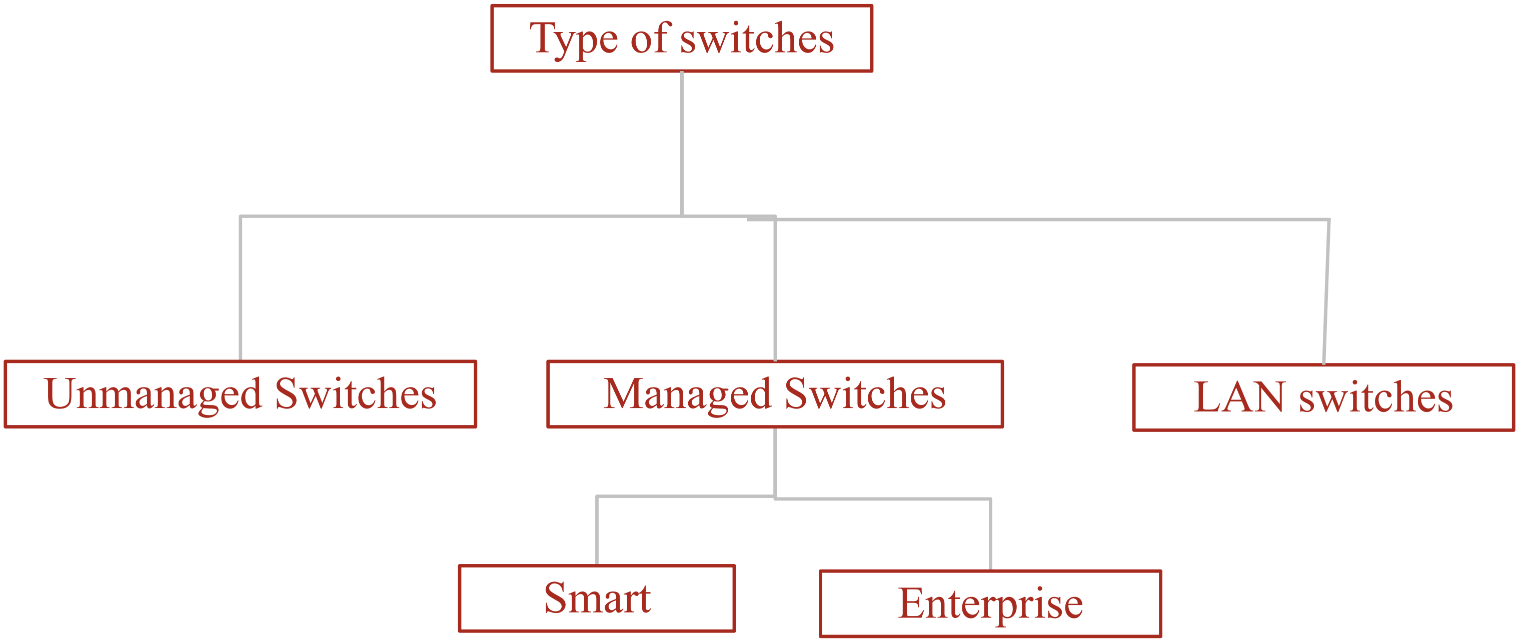


- **Remote Bridge**: - This Bridge connects with another Bridge over the WAN link.

- **Wireless Bridge**: - This Bridge connects with another Bridge without using wires. It uses radio signals for the connectivity.

Switches

- Network cable usually doesn’t connect computers directly to each other. Instead, each computer is connected by cable to a device known as a switch.
- The switch, in turn, connects to the rest of the net-work.
- Switch is a network device that connects other devices to Ethernet networks through twisted pair cables.
- It uses packet switching technique to receive, store and forward data packets on the network.
- The switch maintains a list of network addresses of all the devices connected to it.
- Each switch contains a certain number of ports, typically 8 or 16. Thus, you can use an eight-port switch to connect up to eight computers.
- Switches can be connected to each other to build larger networks.
- A switch is a multi-input, multi-output device that transfers packets from an input to one or more outputs.
- A switch is connected to a set of links and, for each of these links, runs the appropriate data link protocol to communicate with the node at the other end of the link.
- A switch’s primary job is to receive incoming packets on one of its links and to transmit them on some other link. This function is sometimes referred to as either *switching* or *forwarding,*



Types of switches in Computer Network

Unmanaged switches:

- These are the switches that are mostly used in home networks and small businesses as they plug-in and instantly start doing their job and such switches do not need to be watched or configured.
- These require only small cable connections.
- It allows devices on a network to connect with each other such as a computer to a computer or a computer to a printer in one location.
- They are the least expensive switches among all categories.

LAN switches –

- These are also known as Ethernet switches or data switches and are used to reduce network congestion or bottleneck by distributing a package of data only to its intended recipient.
- These are used to connect points on a LAN.

PoE switches –

- PoE switches are used in PoE technology which stands for power over Ethernet that is a technology that integrates data and power on the same cable allowing power devices to receive data in parallel to power.
- Thus these switches provide greater flexibility by simplifying the cabling process.

Managed Switches:

These type of switches have many features like the highest levels of security, precision control and full management of the network.

- These are used in organisations containing a large network and can be customized to enhance the functionality of a certain network.
- These are the most costly option but their scalability makes them an ideal option for a network that is growing.
- They are achieved by setting a simple network management protocol(SNMP).
  - **(I) Smart switches:** These switches offer basic management features with the ability to create **some levels of security** but have a simpler management interface than the other managed switches. Thus they are often called partially managed switches. These are mostly used in **fast and constant LANs** which support **gigabit data transfer** and allocations. It can accept configuration of VLANs (Virtual LAN).
  - **(II) Enterprise managed switches:** They have features like ability to fix, copy, transform and display different network configurations along with a **web interface SNMP** agent and command line interface. These are also known as fully managed switches and are **more expensive** than the smart switches as they have more features that can be enhanced. These are used in organisations that **contain a large number of ports, switches and nodes.**

Router

When a device in a Local Area Network needs to communicate with a device on another LAN, it must send that traffic to a specialized device connected to the LAN called a “router” whose purpose is to find the best path for the message to take to arrive at the intended target device, and to send the message along its way following that path.

In order to allow the billions of devices on the Internet to find each other, routers regularly need to communicate among themselves using protocols that enable them to share routing information so that, when a device needs to send a communication message to a target device, the routers work together to determine the best path for the message packet to use to arrive at the intended target device.

A router is more capable as compared to other network devices, such as a hub, switch, etc., as these devices are only able to execute the basic functions of the network.

On the other hand, the router has the capability to analyze and modify the data while transferring it over a network, and it can send it to another network. For example, generally, routers allow sharing a single network connection between multiple devices.

- ## Features of Router

- A router works on the 3rd layer (Network Layer) of the OSI model, and it is able to communicate with its adjacent devices with the help of IP addresses and subnet.
- A router provides high-speed internet connectivity with the different types of ports like gigabit, fast-Ethernet, and STM link port.
- It allows the users to configure the port as per their requirements in the network.
- Routers' main components are central processing unit (CPU), flash memory, RAM, Non-Volatile RAM, console, network, and interface card.
- Routers are capable of routing the traffic in a large networking system by considering the sub-network as an intact network.
- Routers filter out the unwanted interference, as well as carry out the data encapsulation and decapsulation process.
- Routers provide the redundancy as it always works in master and slave mode.
- It allows the users to connect several LAN and WAN.
- Furthermore, a router creates various paths to forward the data.

Types of Routers

There are various types of routers in networking; such are given below:

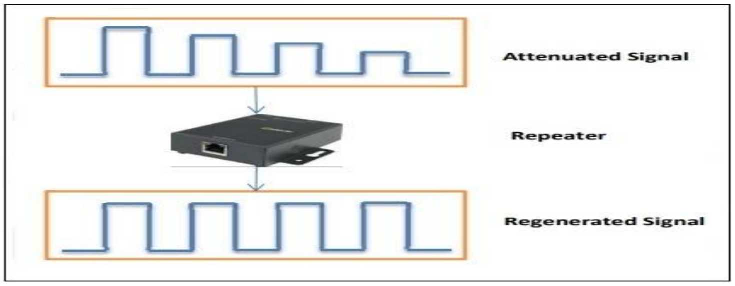
1. **Wireless Router:** Wireless routers are used to offer Wi-Fi connectivity to laptops, smartphones, and other devices with Wi-Fi network capabilities, and it can also provide standard ethernet routing for a small number of wired network systems.
2. **Brouter:** A brouter is a combination of the bridge and a router. It allows transferring the data between networks like a bridge. And like a router, it can also route the data within a network to the individual systems. Thus, it combines these two functions of bridge and router by routing some incoming data to the correct systems while transferring the other data to another network.
3. **Core router:** A core router is a type of router that can route the data within a network, but it is not able to route the data between the networks. It is a computer communication system device and the backbone of networks, as it helps to link all network devices. It is used by internet service providers (ISPs), and it also provides various types of fast and powerful data communication interfaces.
4. **Edge router:** An edge router is a lower-capacity device that is placed at the boundary of a network. It allows an internal network to connect with the external networks. It is also called as an access router. It uses an External BGP (Border Gateway Protocol) to provides connectivity with remote networks over the internet.

Gateway

- Gateway is a network device used to connect two or more dissimilar networks.
- In networking parlance, networks that use different protocols are dissimilar networks.
- A gateway usually is a computer with multiple NICs connected to different networks.
- A gateway can also be configured completely using software.
- As networks connect to a different network through gateways, these gateways are usually hosts or end points of the network.
- It may be a router, firewall, server, or other device that enables traffic to flow in and out of the network.
- A router is a common type of gateway used in home networks. It allows computers within the local network to send and receive data over the Internet.
- A firewall is a more advanced type of gateway, which filters inbound and outbound traffic, disallowing incoming data from suspicious or unauthorized sources.
- A proxy server is another type of gateway that uses a combination of hardware and software to filter traffic between two networks. For example, a proxy server may only allow local computers to access a list of authorized websites.

What are Repeaters in Computer Network?

Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters.



Repeaters

Why are Repeaters needed?

When an electrical signal is transmitted via a channel, it gets attenuated depending upon the nature of the channel or the technology. This poses a limitation upon the length of the LAN or coverage area of cellular networks. This problem is alleviated by installing repeaters at certain intervals. Repeaters amplifies the attenuated signal and then retransmits it. Digital repeaters can even reconstruct signals distorted by transmission loss.So, repeaters are popularly incorporated to connect between two LANs thus forming a large single LAN.

Types of Repeaters

According to the types of signals that they regenerate, repeaters can be classified into two categories −

Analog Repeaters − They can only amplify the analog signal.

Digital Repeaters − They can reconstruct a distorted signal.

According to the types of networks that they connect, repeaters can be categorized into two types −

Wired Repeaters − They are used in wired LANs.

Wireless Repeaters − They are used in wireless LANs and cellular networks.

According to the domain of LANs they connect, repeaters can be divided into two categories −

Local Repeaters − They connect LAN segments separated by small distance.

Remote Repeaters − They connect LANs that are far from each other.

Repeaters

Advantages of Repeaters

Repeaters are simple to install and can easily extend the length or the coverage area of networks.

They are cost effective.

Repeaters don’t require any processing overhead. The only time they need to be investigated is in case of degradation of performance.

They can connect signals using different types of cables.

Disadvantages of Repeaters

Repeaters cannot connect dissimilar networks.

They cannot differentiate between actual signal and noise.

They cannot reduce network traffic or congestion.

Most networks have limitations upon the number of repeaters that can be deployed.

Modem

Modem stands for Modulation Demodulation. A modem converts the digital data signals into analogue data signals. They can be installed within the computer in a development slot applicable for it.

There are frequently two types of Modems that are as follows −

Standard Modem

The standard modems use generic device drivers, and they can be internal and external ones. The internal modems do not need much physical structure. They can be installed into a compatible development slot. The external modem is connected through one of the COM port to the computer through a cable called a null-modem cable.

Window Modem

A window modem is a private plug and plays tool. It requires a particular device driver supported by the window operating framework to function correctly.

Features of Modems

The main features of modems are as follows −

They have high uploading and communication rates. An X2 modem provides an uploading bandwidth between 28.8 to 56 Kbps.

They are upgradeable through a software patch to meet almost any universal standard.

They enable high-speed downstream data transfers by digitally encoding all downstream data while upstream runs at conventional rates of 33.6 kbps.

Some modems incorporate dual simultaneous voice and Data (DSVD), i.e., they can carry both analog voices and computer data.

They can detect callers originating telephone number, and thus they can serve as caller ID.

Some modems provide advanced voice mail features, and those modems serve as intelligent, answering machines or digital information systems.

Types of Modems

There are the following types of modems which are as follows

Optical Modem

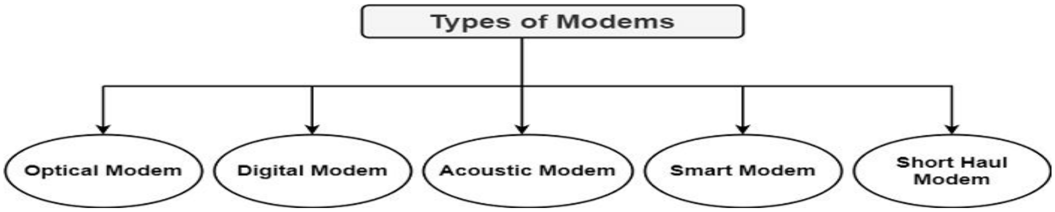
Optical Modem uses optical cables instead of other metallic media. It converts the digital data signals into the pulse of light transmitted on the optical fiber used by it.

Digital Modem

A digital modem converts digital data into digital signals. It modulates the digital data on the digital carrier signals for transmission on digital transmission lines.

Acoustic Modem

The acoustic modem is a particular type of modem that can couple the telephone handset with a device used by traveling salespeople to connect the hotel phones. It contains a speaker and microphone**.**



Smart Modem

The smart modem allows auto-dial/redial and auto-answer capabilities. It contains a microprocessor onboard that uses the Hayes AT command set to provide auto-dial and auto answering functions.

Short Haul Modem

The short-haul modem is those who are present in your PC at home. They can transmit data over 20 miles or less, and generally, they are used to connect PCs in a building or office within this area.

NETWORK SOFTWARE

Protocol Hierarchies

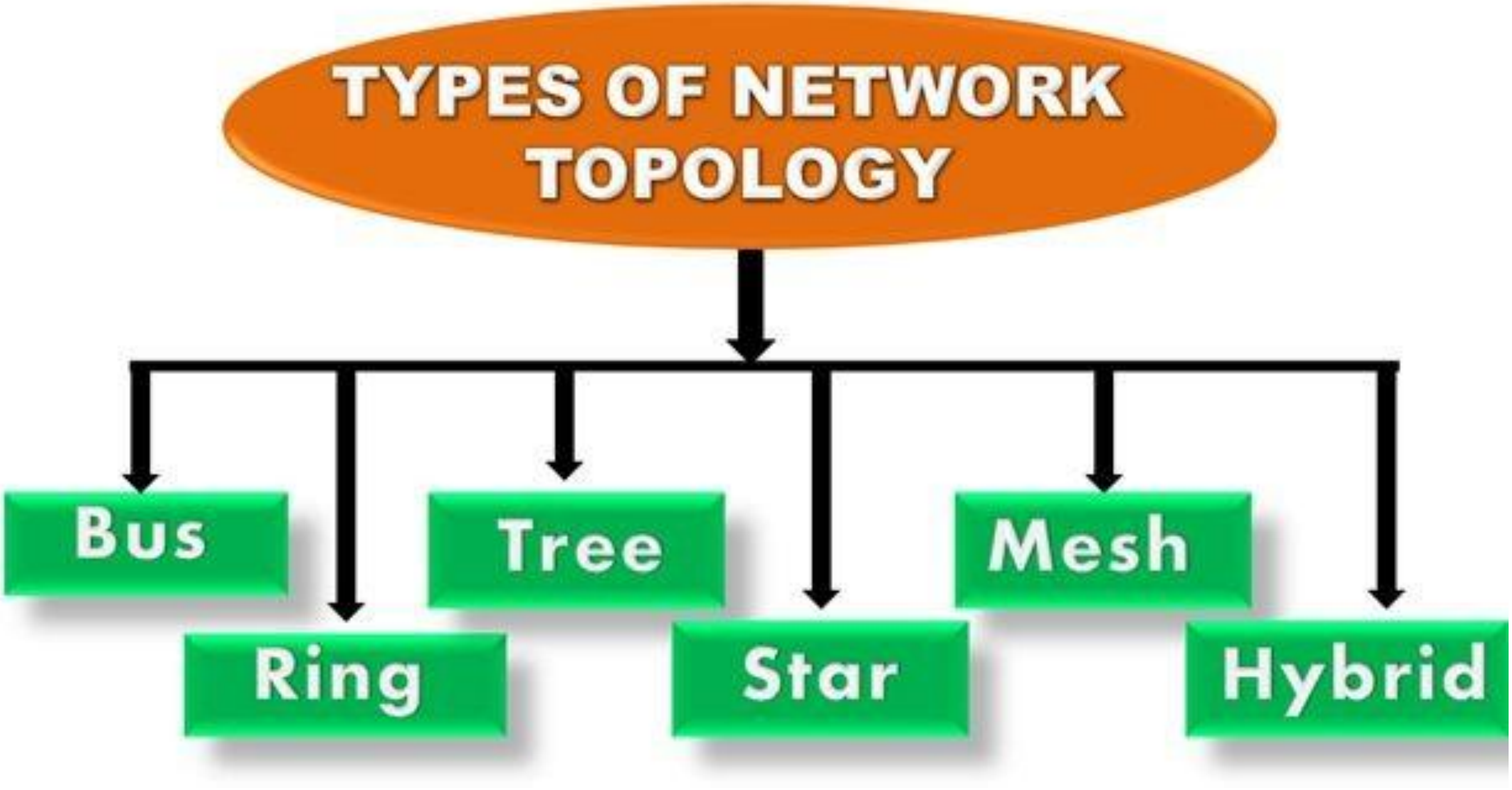
- To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it.
- The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network.
- The purpose of each layer is to offer certain services to the higher layers while shielding those layers from the details of how the offered services are actually implemented.
- In a sense, each layer is a kind of virtual machine, offering certain services to the layer above it.
- When layer n on one machine carries on a conversation with layer n on another machine, the rules and conventions used in this conversation are collectively known as the **layer n protocol.**
- Basically, a protocol is an agreement between the communicating parties on how communication is to proceed.
- The entities comprising the corresponding layers on different machines are called peers.
- The peers may be software processes, hardware devices, or even human beings. In other words, it is the peers that communicate by using the protocol to talk to each other.

Network Topology

- Network Topology is the schematic description of a network arrangement, connecting various nodes(sender and receiver) through lines of connection.
- A Network Topology is the arrangement with which computer systems or network devices are connected to each other.

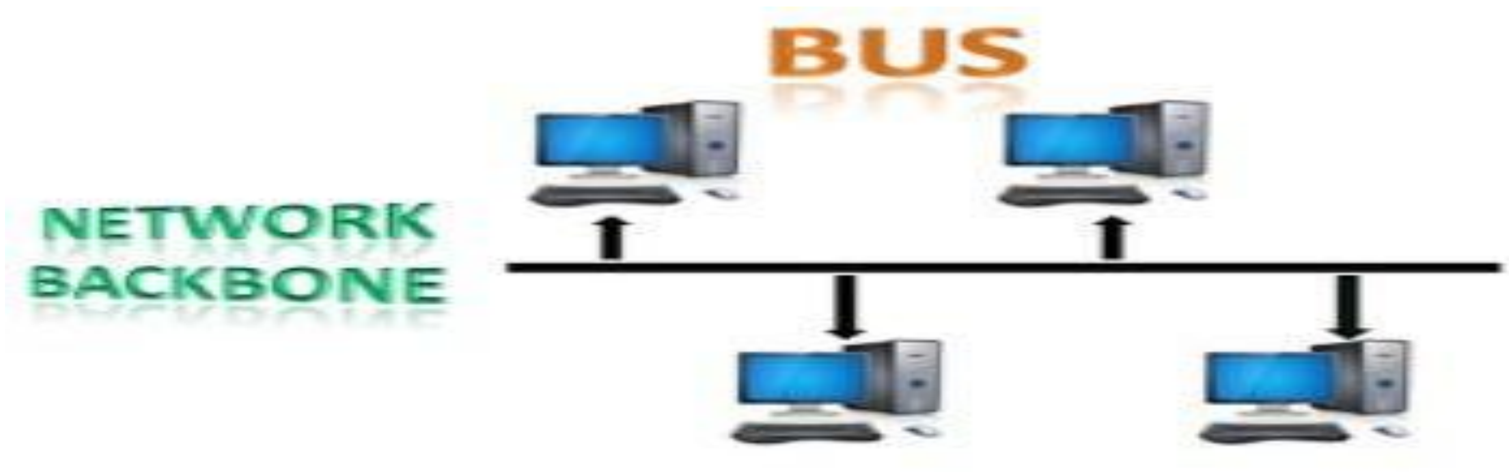
- Topology defines the structure of the network of how all the components are interconnected to each other.
- There are two types of topology: **physical and logical topology**.

- Physical topology is the geometric representation of all the nodes in a network.
- Topologies may define both physical and logical aspect of the network. Both logical and physical topologies could be same or different in a same network.



Bus Topology

- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network.
- All the stations available in the network will receive the message whether it has been addressed or not.
- The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
- The configuration of a bus topology is quite simpler as compared to other topologies.
- The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.
- The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).
- In a bus topology, all components are connected to and share a single wire.
- Certain media types, such as **10Base5 and 10Base2** Ethernet, use a bus topology.
- Typically, special types of connectors or transceivers are used to connect the cables to provide the bus topology.
- In 10Base5, for example, each device connects to a single strand of coaxial cable via a vampire tap.
- This device taps into the single strand of coaxial cable and provides the physical connection from a networking device to the single strand of cable.



Advantages of Bus topology:

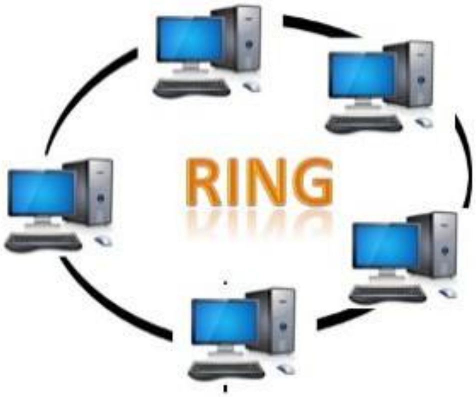
- **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
- **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
- **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
- **Limited failure:** A failure in one node will not have any effect on other nodes.

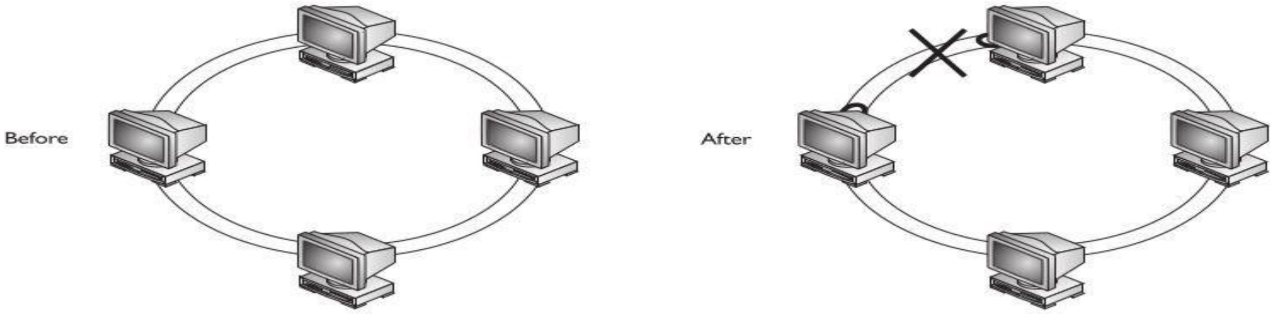
Disadvantages of Bus topology:

- **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.
- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.
-

Ring Topology

1. In a ring topology, device one connects to device two, device two connects to device three, and so on to the last device, which connects back to the first device.
2. Ring topologies can be implemented with a single ring or a dual ring.
3. Dual rings are typically used when you need redundancy. For example, if one of the components fails in the ring, the ring can wrap itself,
4. Fiber distributed data interface (FDDI) is an example of a media technology that uses dual rings to connect computer components.
5. Single ring topologies lack this type of redundancy feature.





Advantages of Ring topology:

- **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- **Product availability:** Many hardware and software tools for network operation and monitoring are available.
- **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
- **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

Disadvantages of Ring topology:

- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Failure:** The breakdown in one station leads to the failure of the overall network.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

Star Topology

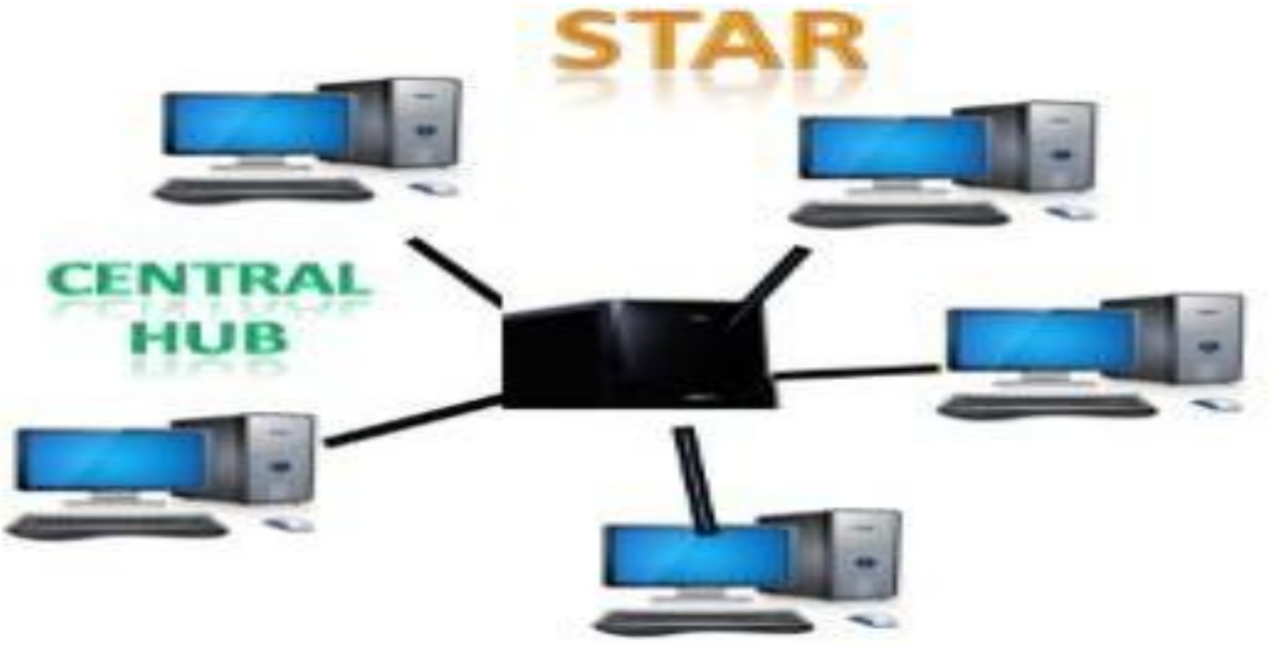
- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
- Coaxial cable or RJ-45 cables are used to connect the computers.
- Hubs or Switches are mainly used as connection devices in a **physical star topology**.
- Star topology is the most popular topology in network implementation.
- An example of a media type that uses a star topology is 10BaseT Ethernet.

Advantages of Star topology

- **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator has to go to the single station to troubleshoot the problem.
- **Network control:** Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
- **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
- **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
- **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
- **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
- **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

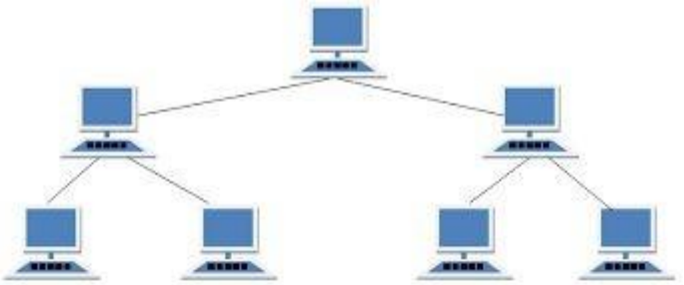
Disadvantages of Star topology

- **A Central point of failure:** If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.
- **Cable:** Sometimes cable routing becomes difficult when a significant amount of routing is required.



Tree Topology

- Tree topology combines the characteristics of bus topology and star topology.
- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
- The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
- There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.



Advantages of Tree topology

- **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
- **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
- **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.
- **Error detection:** Error detection and error correction are very easy in a tree topology.
- **Limited failure:** The breakdown in one station does not affect the entire network.
- **Point-to-point wiring:** It has point-to-point wiring for individual segments.

Disadvantages of Tree topology

- **Difficult troubleshooting:** If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
- **High cost:** Devices required for broadband transmission are very costly.
- **Failure:** A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.
- **Reconfiguration difficult:** If new devices are added, then it becomes difficult to reconfigure.

Mesh Topology

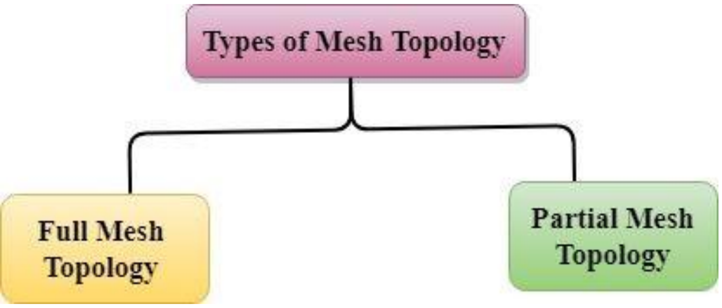
- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.
- Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
- Mesh topology is mainly used for wireless networks.
- Mesh topology can be formed by using the formula:

  Number of cables = (n*(n-1))/2;
- Where **n** is the number of nodes that represents the network.

slido

Seven devices are arranged in mesh topology----------physical channel link in these devices

ⓘ Start presenting to display the poll results on this slide.



Mesh topology is divided into two categories:

- Fully connected mesh topology
- Partially connected mesh topology
- **Full Mesh Topology:** In a full mesh topology, each computer is connected to all the computers available in the network.
- **Partial Mesh Topology:** In a partial mesh topology, not all but certain computers are connected to those computers with which they communicate frequently.

Advantages of Mesh topology:

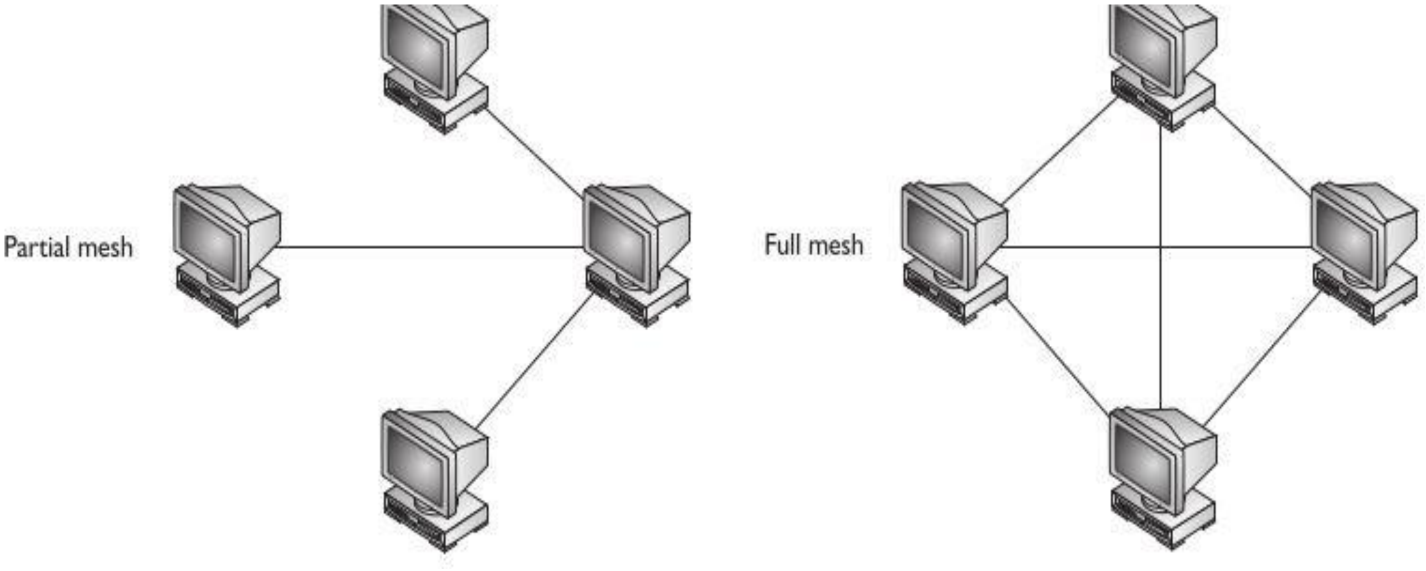
Reliable: The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.

Fast Communication: Communication is very fast between the nodes.

Easier Reconfiguration: Adding new devices would not disrupt the communication between other devices.

Disadvantages of Mesh topology

- **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
- **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication link failure goes undetected.
- **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.



Hybrid Topology

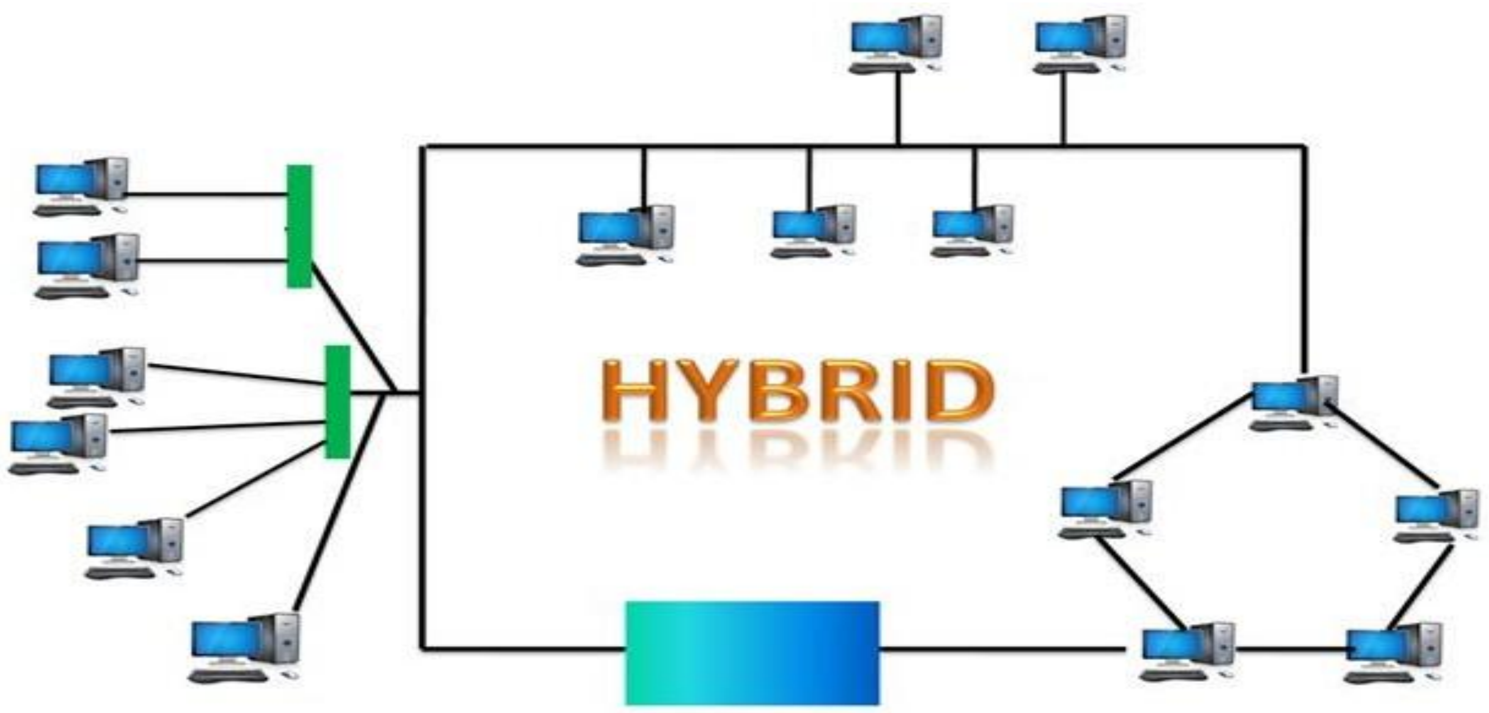
- The combination of various different topologies is known as **Hybrid topology**.
- A Hybrid topology is a connection between different links and nodes to transfer the data.
- When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.

Advantages of Hybrid Topology

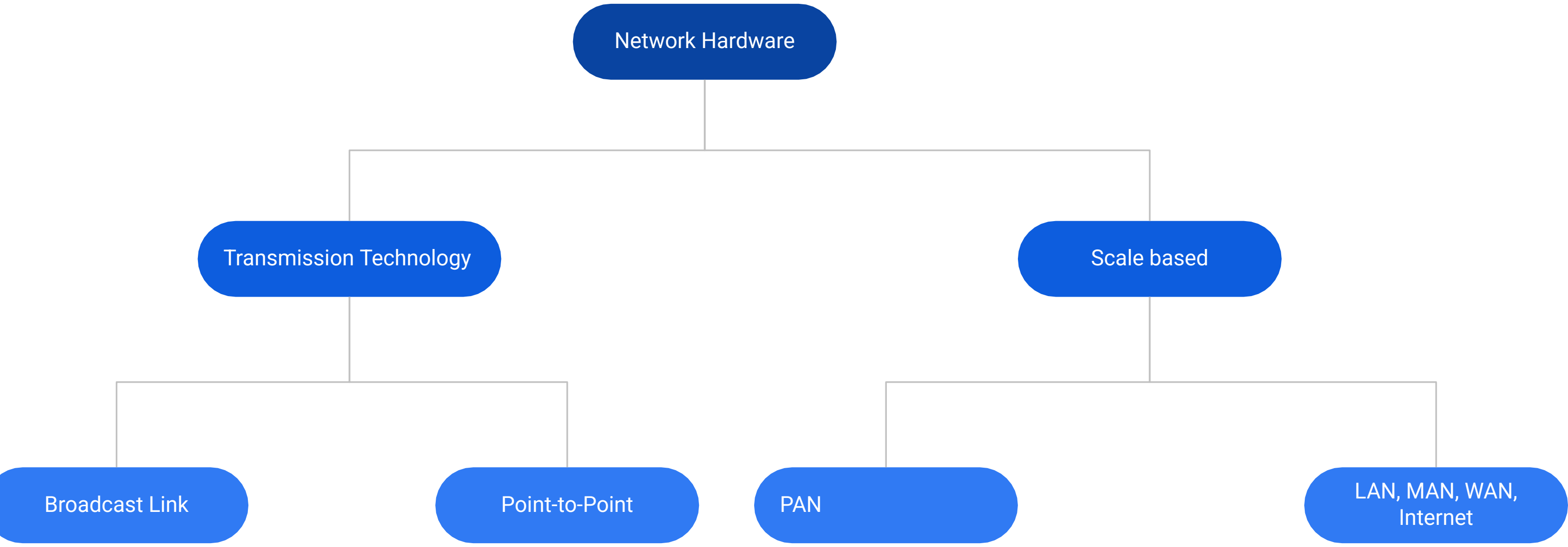
- **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
- **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
- **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
- **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

Disadvantages of Hybrid topology

- **Complex design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
- **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
- **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc**.**



Networking hardware


Network Hardware

Transmission Technology

Scale based

Broadcast Link

Point-to-Point

PAN

LAN, MAN, WAN, Internet

Personal Area Network(PAN)

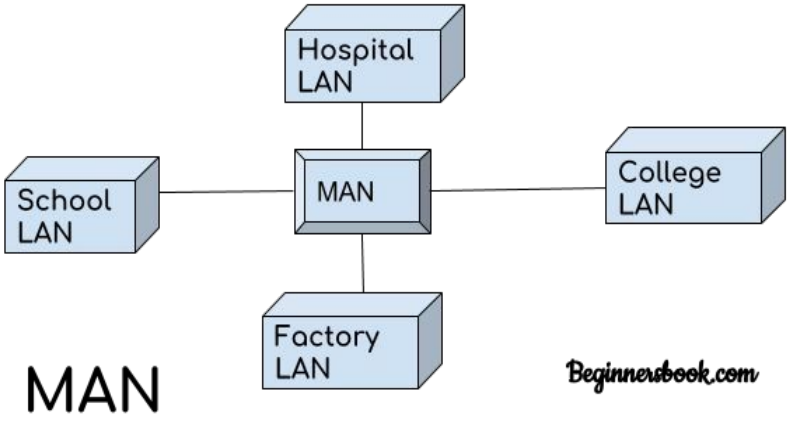
- Let devices can communicate over the range of person.
- PAN is a personal devices network equipped at a limited area.
- The personal area network concept originates at M.I.T.'s Media Lab thanks to Thomas Zimmerman research.
- Interprocessor Distance 1m.

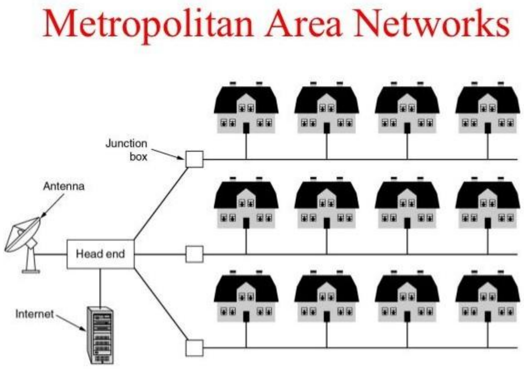
A personal area network pros and cons:

- PAN is expedient, lucrative and handy.
- Sometimes has a bad connection to other networks at the same radio bands.
- Bluetooth networks have slow data transfer speed, but comparatively safe.
- Bluetooth has distance limits.
- **Ex. Bluetooth, RFID on smart car and library book**

Metropolitan Area Networks

- A MAN (Metropolitan Area Network) covers a city.
- The best-known examples of MANs are the cable television networks available in many cities.
- These systems grew from earlier community antenna systems used in areas with poor over-the-air television reception.
- In those early systems, a large antenna was placed on top of a nearby hill and a signal was then piped to the subscribers' houses.
- Cable television is not the only MAN, though.
- Recent developments in high speed wireless Internet access have resulted in another MAN, which has been standardized as IEEE 802.16 and is popularly known as WiMAX.





A metropolitan area network based on cable TV.

Local Area Network

- A LAN is a privately owned network that operates within and nearby a single building like a home, office or factory.
- LANs are widely used to connect personal computers and consumer electronics to let them share resources (e.g., printers) and exchange information.
- When LANs are used by companies, they are called enterprise networks.
- Wireless LANs are very popular these days, especially in homes, older office buildings, cafeterias, and other places where it is too much trouble to install cables.
- There is a standard for wireless LANs called IEEE 802.11, popularly known as WiFi, which has become very widespread.
- Wired LANs use a range of different transmission technologies. Most of them use copper wires, but some use optical fiber.
- LANs are restricted in size, which means that the worst-case transmission time is bounded
- Ex.: Ethernet, VLAN

Wide Area Network

A WAN (Wide Area Network) spans a large geographical area, often a country or continent.

- The first known WAN was created by the U.S. Air Force in the late 1950s to interconnect sites in the Semi-Automatic Ground Environment (SAGE) radar defense system. An enormous network of dedicated phone lines, telephones, and modems linked the sites together.
- The foundation of the IP-based Internet started with the Advanced Research Projects Agency Network (ARPANET), the first wide-area packet-switching network with distributed control and the first network to implement TCP/IP protocol suite.

Types of WAN Technology

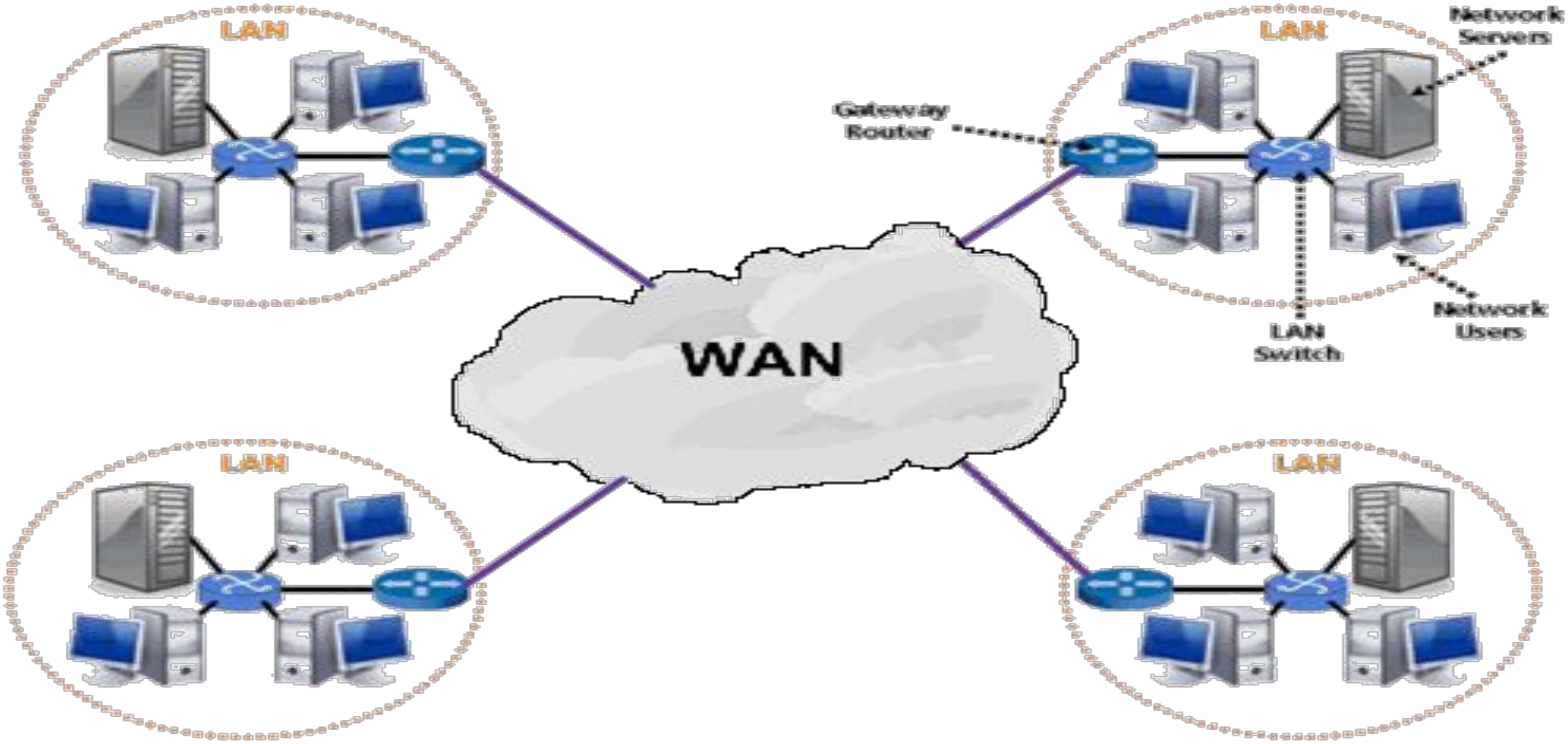
Packet switching	Packet switching is a method of data transmission in which a message is broken into several parts, called packets, that are sent independently, in triplicate, over whatever route is optimum for each packet, and reassembled at the destination. Each packet contains a piece part, called the payload, and an identifying header that includes destination and reassembly information. The packets are sent in triplicate to check for packet corruption. Every packet is verified in a process that compares and confirms that at least two copies match. When verification fails, a request is made for the packet to be re-sent.
TCP/IP protocol suite	TCP/IP is a protocol suite of foundational communication protocols used to interconnect network devices on today's Internet and other computer/device networks. TCP/IP stands for Transmission Control Protocol/Internet Protocol
Router	A router is a networking device typically used to interconnect LANs to form a wide area network (WAN) and as such is referred to as a WAN device. IP routers use IP addresses to determine where to forward packets. An IP address is a numeric label assigned to each connected network device.
Overlay network	An overlay network is a data communications technique in which software is used to create virtual networks on top of another network, typically a hardware and cabling infrastructure. This is often done to support applications or security capabilities not available on the underlying network.

Types of WAN Technology

Frame Relay	Frame Relay is a technology for transmitting data between LANs or endpoints of a WAN. It specifies the physical and data-link layers of digital telecommunications channels using a packet switching methodology. Frame Relay packages data in frames and sends it through a shared Frame Relay network. Each frame contains all necessary information for routing it to its destination. Frame Relay's original purpose was to transport data across telecom carriers' ISDN infrastructure, but it's used today in many other networking contexts.
ATM	ATM (Asynchronous Transfer Mode) is a switching technique common in early data networks, which has been largely superseded by IP-based technologies. ATM uses asynchronous time-division multiplexing to encode data into small, fixed-sized cells. By contrast, today's IP-based Ethernet technology uses variable packet sizes for data.
Multiprotocol Label Switching (MPLS)	MPLS is a network routing-optimization technique. It directs data from one node to the next using short path labels rather than long network addresses, to avoid time-consuming table lookups.
Packet over SONET/SDH (PoS)	Packet over SONET is a communication protocol used primarily for WAN transport. It defines how point-to-point links communicate when using optical fiber and SONET (Synchronous Optical Network) or SDH (Synchronous Digital Hierarchy) communication protocols.

Components of WAN Technology

Sr. No.	Name of Components	Description
1	Hosts	Machines which are connected
2	Communication Subnet or subnet	The rest of the network that connects these hosts The job of the subnet is to carry messages from host to host, just as the telephone system carries words (really just sounds) from speaker to listener.
3	Transmission lines	Transmission lines move bits between machines. They can be made of copper wire, optical fiber, or even radio links.
4	Switching elements, or switches,	specialized computers that connect two or more transmission lines.
5	Router	Which is shows route for packets



Comparison Of LAN MAN WAN

Parameter	LAN	MAN	WAN
Meaning	A network that connects a group of computers in a small geographical area.	It covers relatively large region such as cities, towns.	It spans large locality and connects countries together. Example Internet.
Ownership of Network	Private	Private or Public	Private or Public
Design and maintenance	Easy	Difficult	Difficult
Propagation Delay	Short	Moderate	Long
Speed	High	Moderate	Low
Fault Tolerance	More Tolerant	Less Tolerant	Less Tolerant

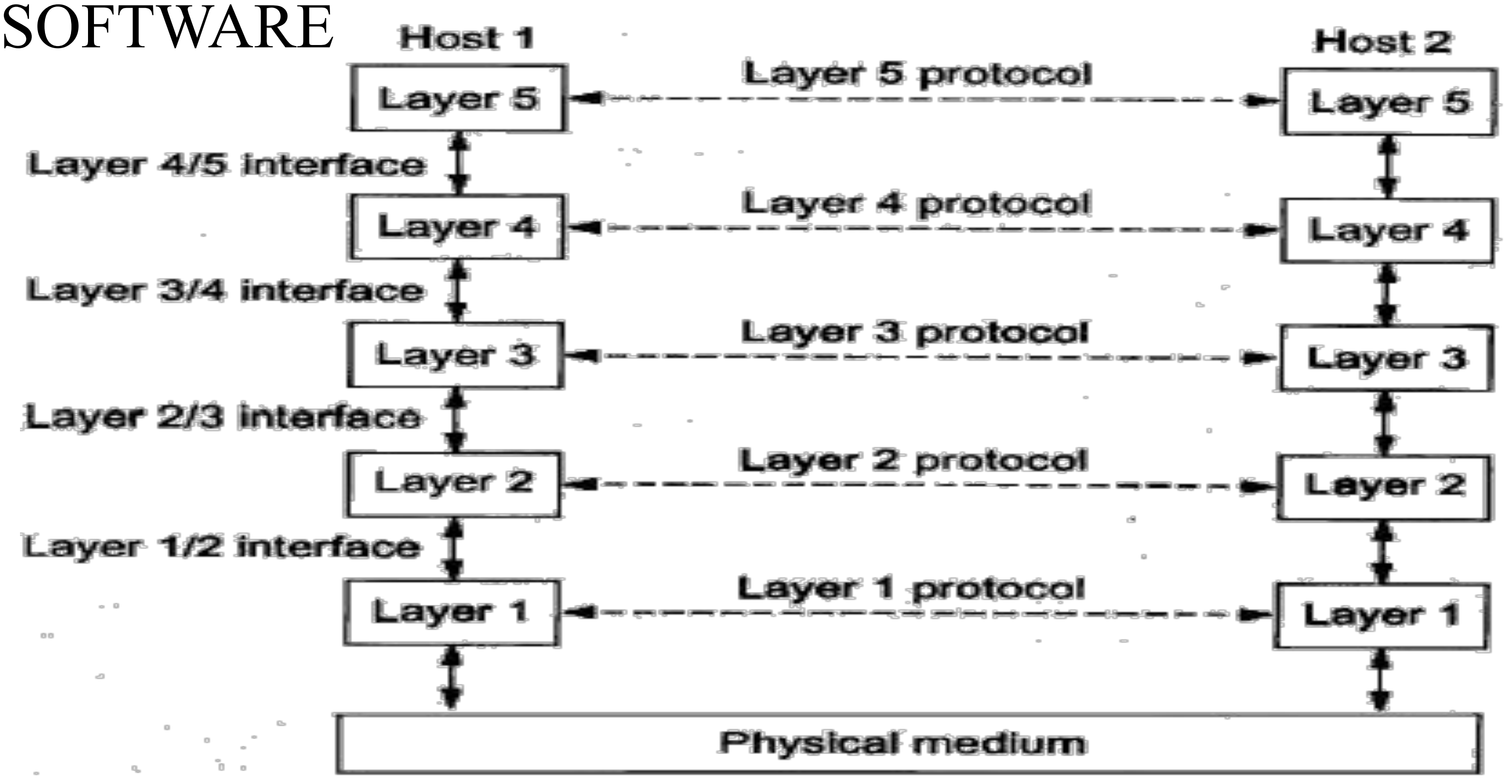
Comparison Of LAN MAN WAN

Parameter	LAN	MAN	WAN
Congestion	Less	More	More
Used for	College, School, Hospital.	Small towns, City.	Country/Continent.
Allows	Single pair of devices to communicate.	Multiple computers can simultaneously interact.	A huge group of computers communicate at the same time.

Interface

- Between each pair of adjacent layers is an interface.
- The interface defines which primitive operations and services the lower layer makes available to the upper one.
- When network designers decide how many layers to include in a network and what each one should do, one of the most important considerations is defining clean interfaces between the layers.

NETWORK SOFTWARE



Design Issues for Layer

- Reliability
- Scalability
- Addressing and Naming
- Error Control
- Multiplexing and Demultiplexing
- Routing
- Resource Allocation
    1. Flow Control
    2. Congestion
- Security

Design Issues for Layer

Reliability

Network channels and components may be unreliable, resulting in loss of bits while data transfer. So, an important design issue is to make sure that the information transferred is not distorted.

Scalability

Networks are continuously evolving. The sizes are continually increasing leading to congestion. Also, when new technologies are applied to the added components, it may lead to incompatibility issues. Hence, the design should be done so that the networks are scalable and can accommodate such additions and alterations.

Addressing

At a particular time, innumerable messages are being transferred between large numbers of computers. So, a naming or addressing system should exist so that each layer can identify the sender and receivers of each message.

Error Control

Unreliable channels introduce a number of errors in the data streams that are communicated. So, the layers need to agree upon common error detection and error correction methods so as to protect data packets while they are transferred.

Flow Control

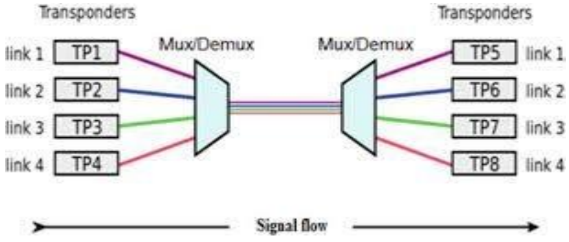
If the rate at which data is produced by the sender is higher than the rate at which data is received by the receiver, there are chances of overflowing the receiver. So, a proper flow control mechanism needs to be implemented.

Resource Allocation

Computer networks provide services in the form of network resources to the end users. The main design issue is to allocate and deallocate resources to processes. The allocation/deallocation should occur so that minimal interference among the hosts occurs and there is optimal usage of the resources.

Statistical Multiplexing

It is not feasible to allocate a dedicated path for each message while it is being transferred from the source to the destination. So, the data channel needs to be multiplexed, so as to allocate a fraction of the bandwidth or time to each host.



Routing

There may be multiple paths from the source to the destination. Routing involves choosing an optimal path among all possible paths, in terms of cost and time. There are several routing algorithms that are used in network systems.

Security

A major factor of data communication is to defend it against threats like eavesdropping and surreptitious alteration of messages. So, there should be adequate mechanisms to prevent unauthorized access to data through authentication and cryptography.

Connection-Oriented Versus Connectionless Service

Layers can offer two different types of service to the layers above them.

- connection-oriented
- Connectionless.

Connection Oriented Services:

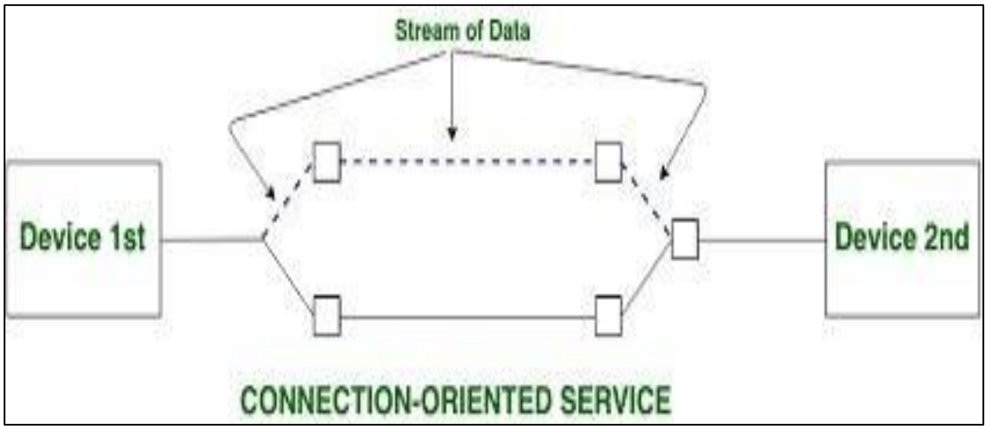
There is a sequence of operation to be followed by the users of connection oriented service. These are:

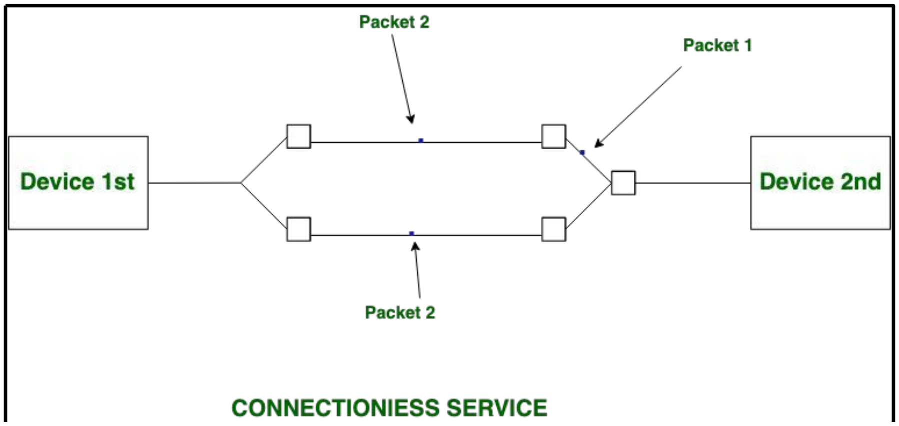
1. Connection is established.
2. Information is sent.
3. Connection is released.

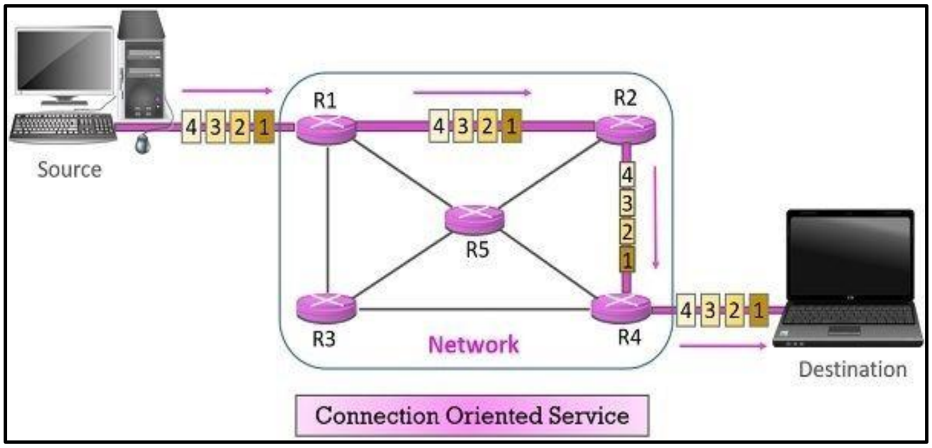
Connection Less Services

It is similar to the postal services, as it carries the full address where the message (letter) is to be carried. Each message is routed independently from source to destination. The order of message sent can be different from the order received.

In connectionless the data is transferred in one direction from source to destination without checking that destination is still there or not or if it prepared to accept the message. Authentication is not needed in this. Example of Connectionless service is UDP (User Datagram Protocol) protocol.







Differences between Connection oriented and connectionless

Key parameter	**Connection oriented**	**connectionless**
Definition	It is the communication service in which virtual connection is created before sending the packet over the internet.	In this communication service, packets are sent without creating any virtual connection over the internet.
Authentication	It needs authentication of the destination node before transferring data.	It transfers the data message without authenticating destination.
Connection Establish	Yes	No
Dedicated Path	Yes	No
Packet Routing	Follow the same path	Can follow any path
Congestion	No	Yes
Reliability	More Reliable	no guarantee of reliability.
Usage	Connection-oriented Services are used in long and steady communication networks.	Connection-less Services are used in volatile networks
overhead	Sending packet in connection-oriented service requires more parameters in the header of the packet to ensure the reliable transmission.	It has less overhead and smaller packet header size.

References Model

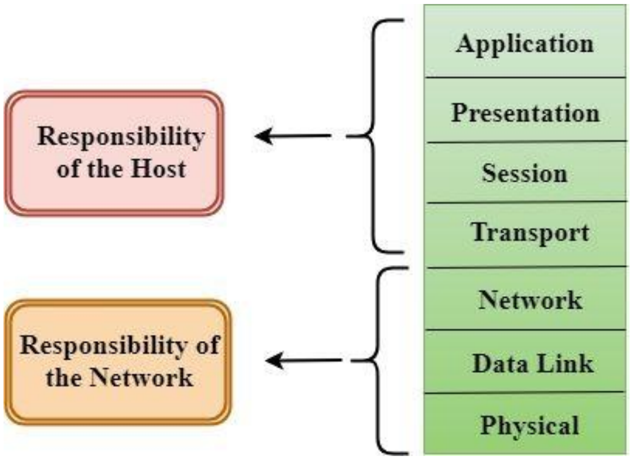
- OSI (Open System Interconnection)
- TCP/IP

OSI References Model

- OSI stands for **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.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.

OSI References Model

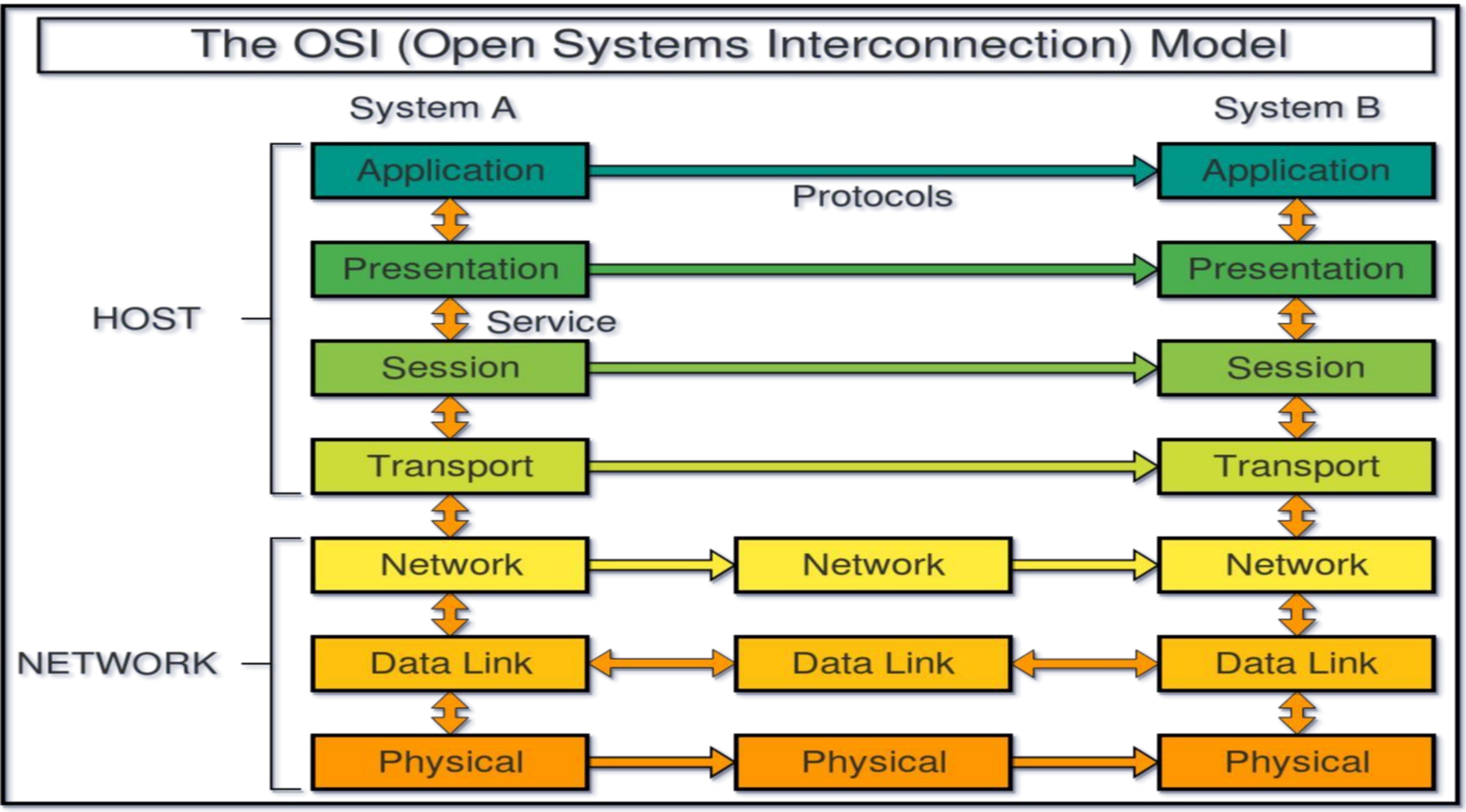
- The OSI model is divided into two Parts upper layers and lower layers.
- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.



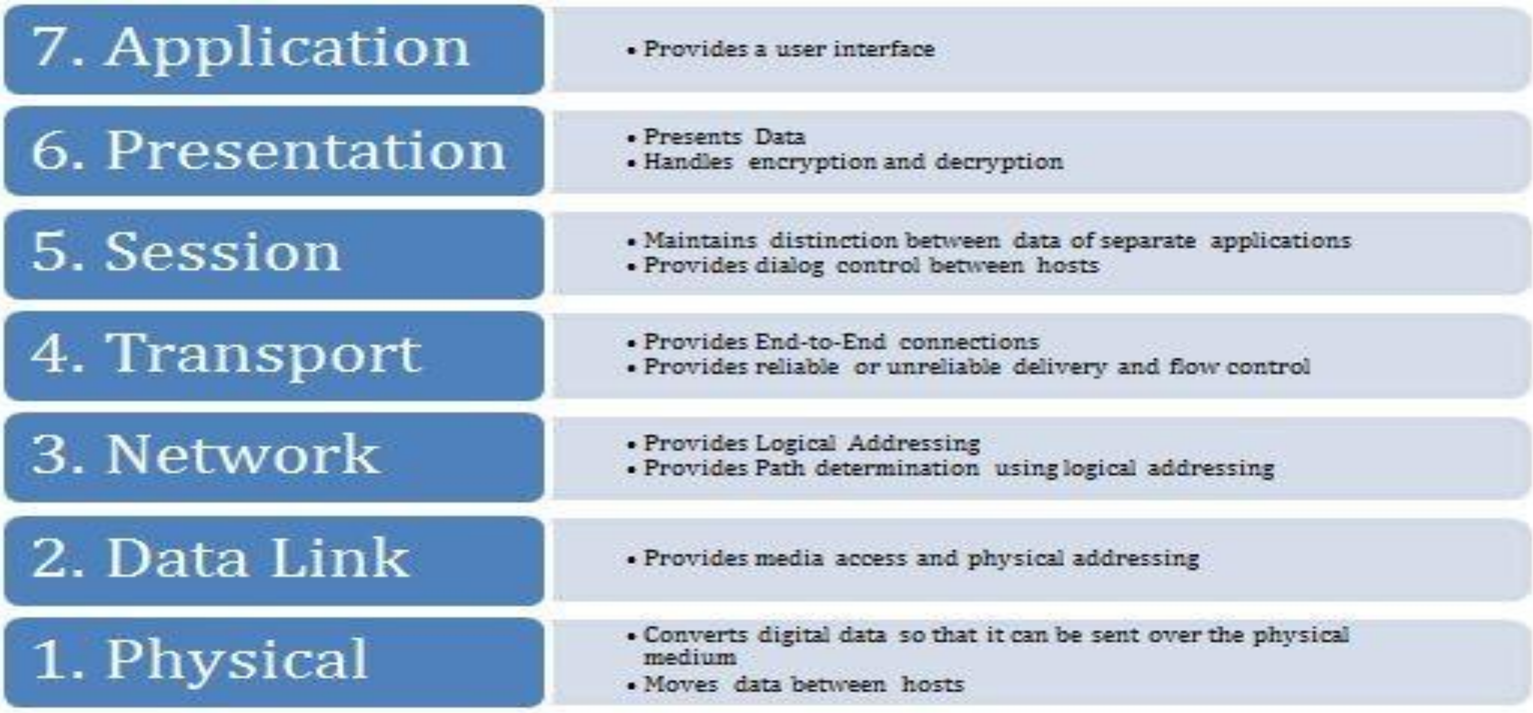
A list of seven layers are given below:

1. Physical Layer
2. Data-Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

“Please Do Not Tell Secret Passwords Anytime”



Summary of Layer Functions



7. Application	• Provides a user interface
6. Presentation	• Presents Data • Handles encryption and decryption
5. Session	• Maintains distinction between data of separate applications • Provides dialog control between hosts
4. Transport	• Provides End-to-End connections • Provides reliable or unreliable delivery and flow control
3. Network	• Provides Logical Addressing • Provides Path determination using logical addressing
2. Data Link	• Provides media access and physical addressing
1. Physical	• Converts digital data so that it can be sent over the physical medium • Moves data between hosts

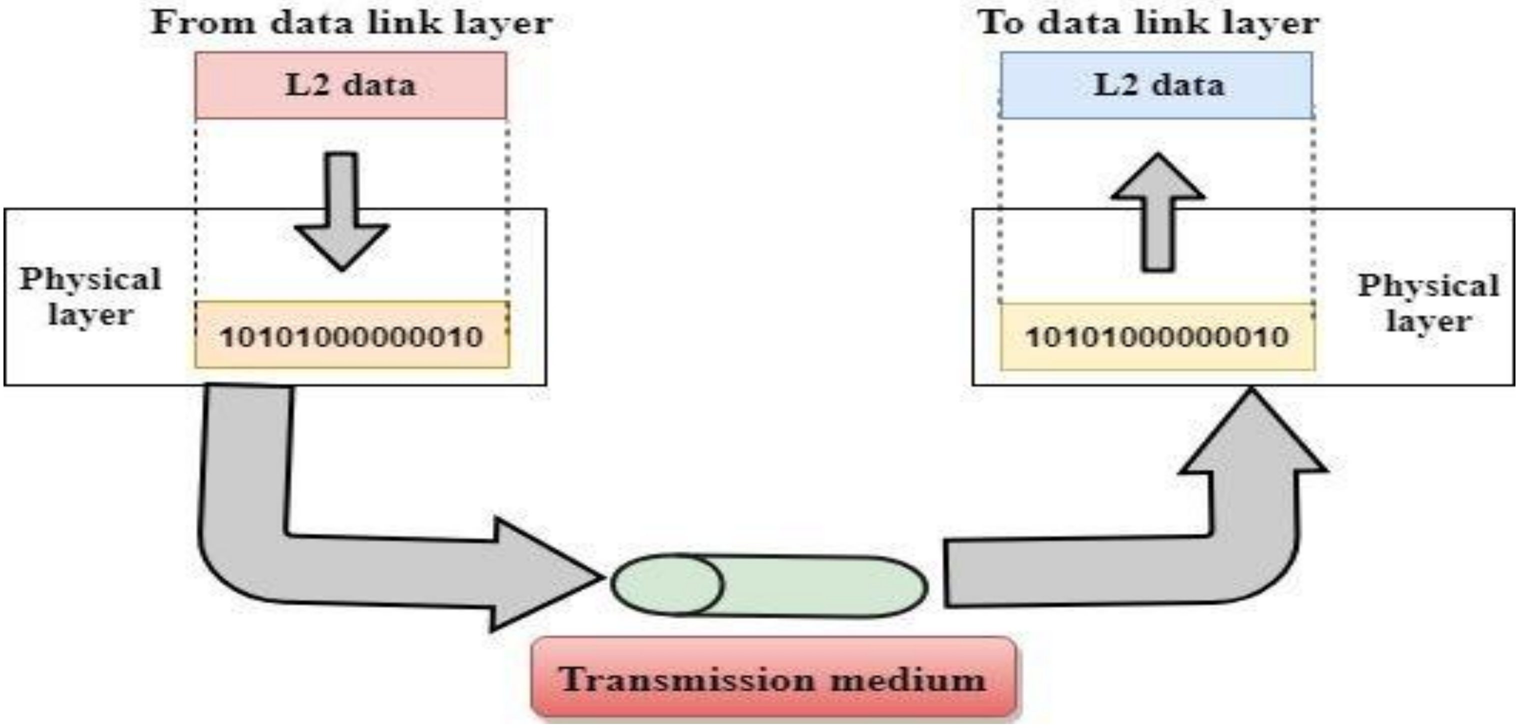
Physical Layer (Layer 1) :

- The lowest layer of the OSI reference model is the physical layer.
- It is responsible for the actual physical connection between the devices.
- The physical layer contains information in the form of **bits.**
- It is responsible for transmitting individual bits from one node to the next.
- When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

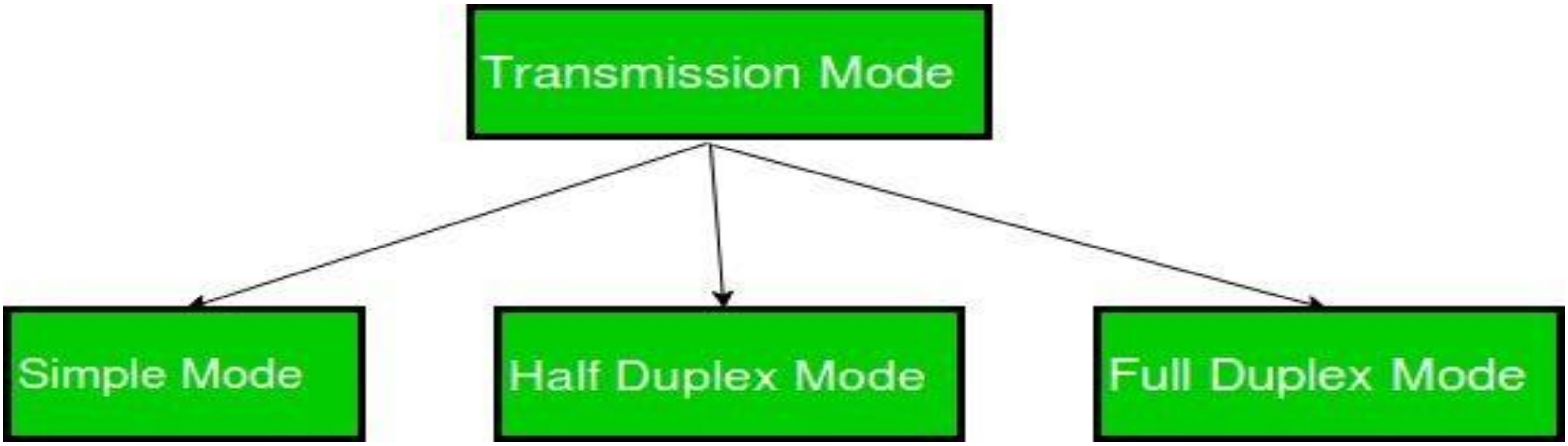
The functions of the physical layer are :

1. **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
2. **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
3. **Physical topologies:** Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topology.
4. **Transmission mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

Physical Layer

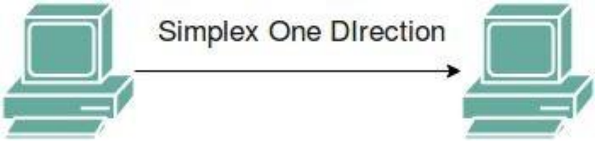


Transmission Mode



Simplex Mode

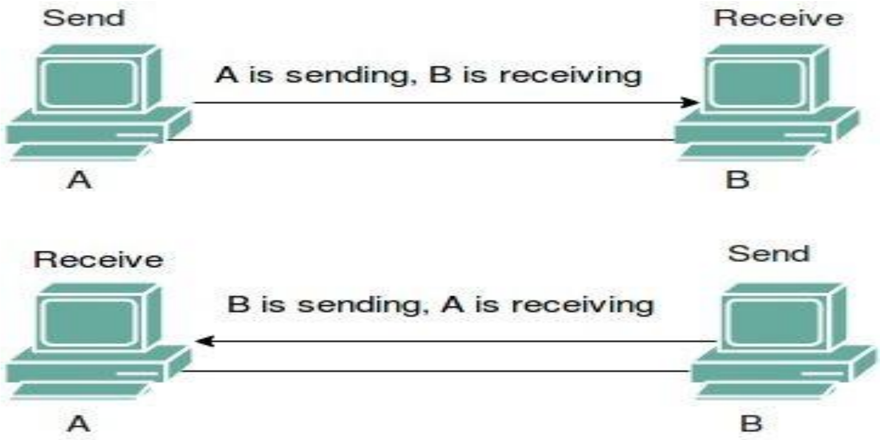
- In Simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit, the other can only receive. The simplex mode can use the entire capacity of the channel to send data in one direction.
- Example: Keyboard and traditional monitors. The keyboard can only introduce input, the monitor can only give the output.



Half-Duplex Mode

- In half-duplex mode, each station can both transmit and receive, but not at the same time.
- When one device is sending, the other can only receive, and vice versa.
- The half-duplex mode is used in cases where there is no need for communication in both direction at the same time.
- The entire capacity of the channel can be utilized for each direction.

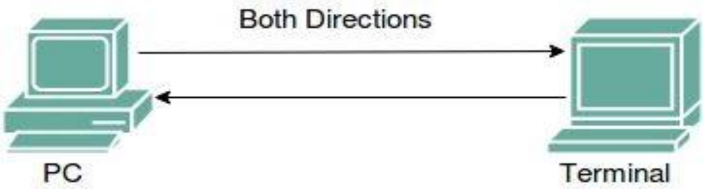
- Example: Walkie- talkie in which message is sent one at a time and messages are sent in both the directions.



Full-Duplex Mode

- In full-duplex mode, both stations can transmit and receive simultaneously.
- In full_duplex mode, signals going in one direction share the capacity of the link with signals going in other direction, this sharing can occur in two ways:
- Either the link must contain two physically separate transmission paths, one for sending and other for receiving.
- Or the capacity is divided between signals travelling in both directions.
- Full-duplex mode is used when communication in both direction is required all the time. The capacity of the channel, however must be divided between the two directions.

- Example: Telephone Network in which there is communication between two persons by a telephone line, through which both can talk and listen at the same time.



Differences b/w Simplex, Half-duplex and Full-duplex mode

Basis for Comparison	**Simplex**	**Half Duplex**	**Full Duplex**
Direction of Communication	Unidirectional	Two-directional, one at a time	Two-directional, simultaneously
Send / Receive	Sender can only send data	Sender can send and receive data, but one a time	Sender can send and receive data simultaneously
Performance	Worst performing mode of transmission	Better than Simplex	Best performing mode of transmission
Example	Keyboard and monitor	Walkie-talkie	Telephone

The physical Layer concerns with

.

Data Link Layer (DLL) (Layer 2) :

The data link layer is responsible for the node to node (Hope by hope)delivery of the message.

- The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer.
- When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.

Data Link Layer is divided into two sub layers :

1. **Logical Link Control (LLC)**
2. **Media Access Control (MAC)**

Network	
Data Link	LLC Sublayer
	MAC Sublayer
Physical	

Data Link Layer

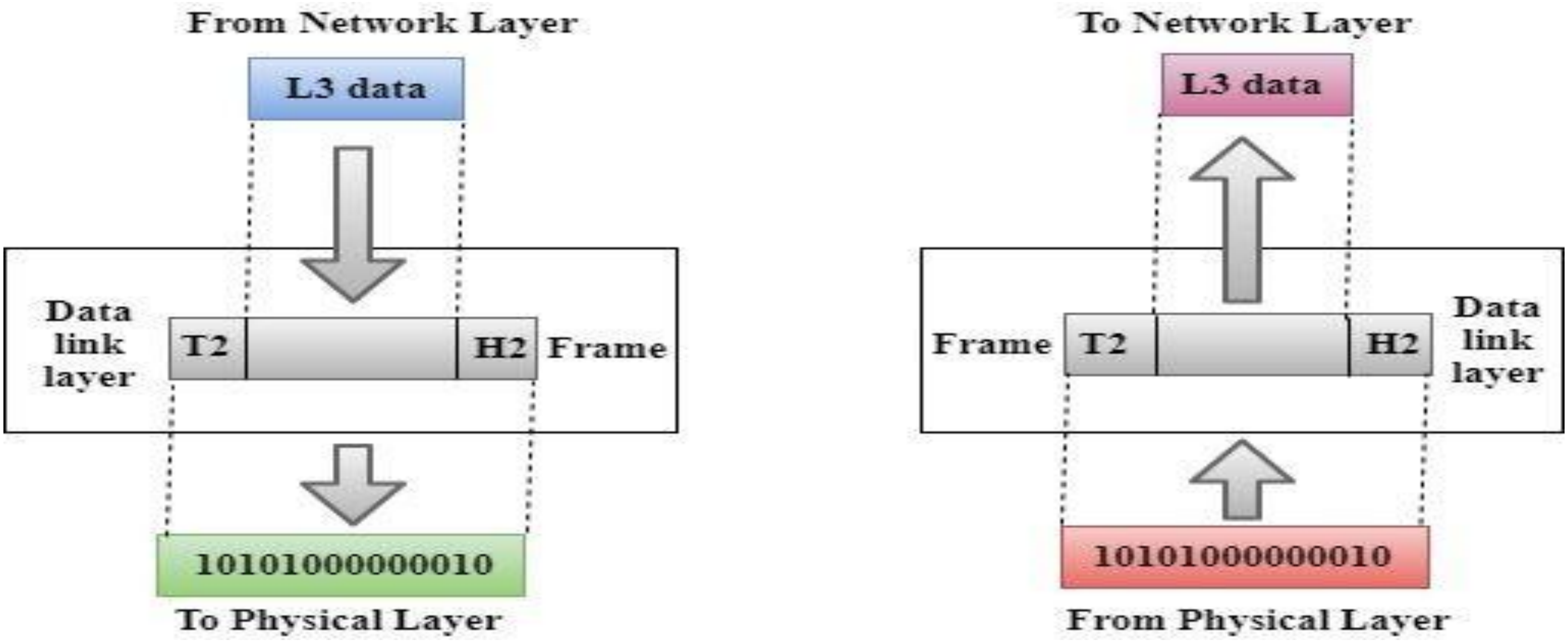
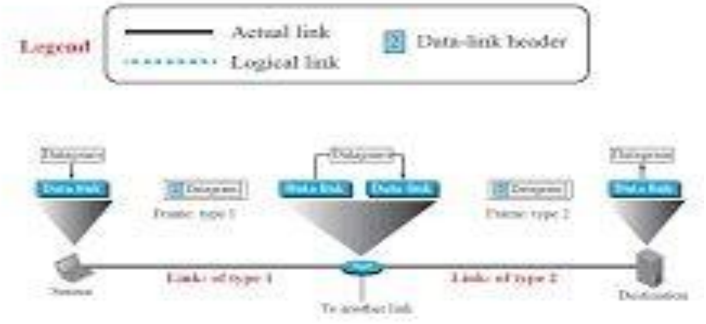


Figure 9.3: A communication with only three nodes



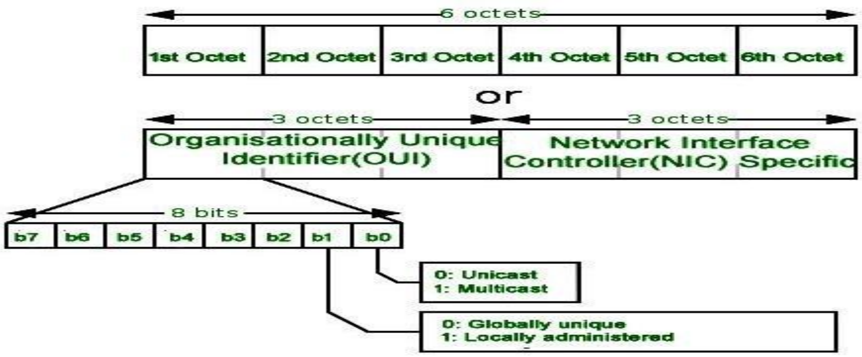
MAC Address

A **media access control address** (**MAC address**) is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment.

This use is common in most IEEE 802 networking technologies, including Ethernet, Wi-Fi, and Bluetooth.

Within the Open Systems Interconnection (OSI) network model, MAC addresses are used in the medium access control protocol sublayer of the data link layer.

MAC Addresses are unique **48-bits** hardware number of a computer,



Format of MAC Address –

MAC Address is a 12-digit hexadecimal number (6-Byte binary number), which is mostly represented by Colon-Hexadecimal notation.
First 6-digits (say 00:40:96) of MAC Address identifies the manufacturer, called as OUI (**Organizational Unique Identifier**).

Some well known manufactures

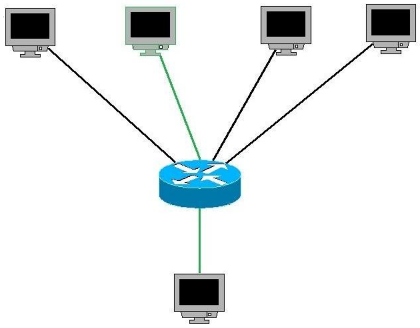
`CC:46:D6 - Cisco`

`3C:5A:B4 - Google, Inc.`

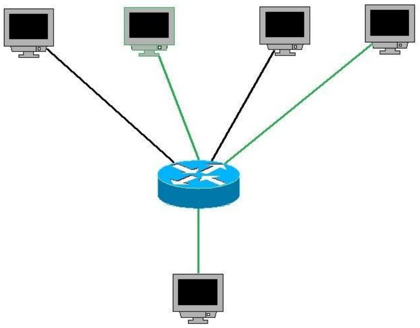
`3C:D9:2B - Hewlett Packard`

`00:9A:CD - HUAWEI TECHNOLOGIES CO.,LTD`

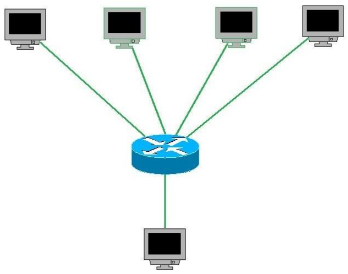
Type of MAC Address



Unicast



Multicast



Broadcast

The functions of the data Link layer are :

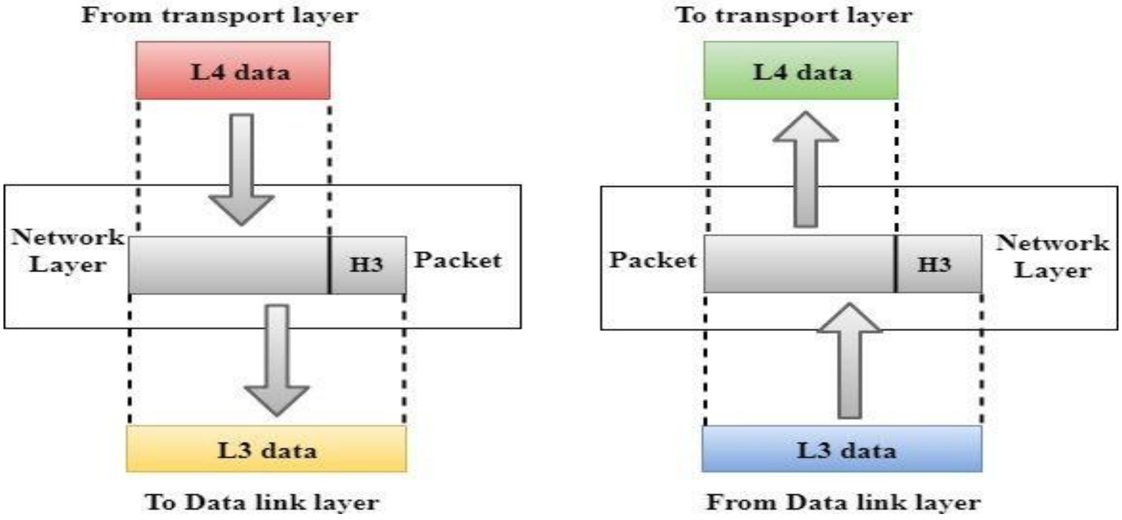
1. **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
2. **Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
3. **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus , flow control coordinates that amount of data that can be sent before receiving acknowledgement.
4. **Physical addressing:** After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
5. **Access control:** When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

Network Layer (Layer 3) :

Network layer works for the transmission of data from one host to the other located in different networks.

It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP address are placed in the header by the network layer.

Host to host delivery



Functions of Network Layer:

- **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- **Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
- **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

slido

The -------- layer is responsible for sources to destination delivery of a packet is possible across multiple network

Transport Layer (Layer 4) :

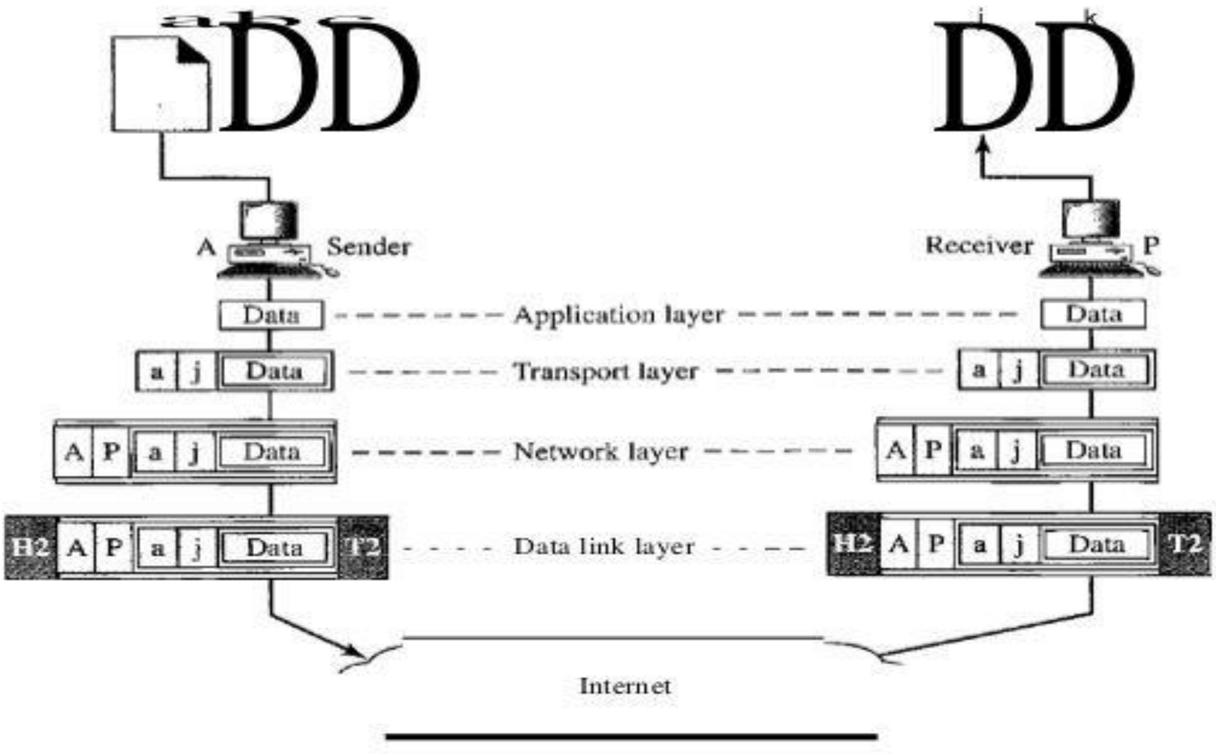
- Transport layer provides services to application layer and takes services from network layer.
- Process to Process Delivery
- The data in the transport layer is referred to as *Segments*.
- It is responsible for the End to End Delivery of the complete message.
- The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

The functions of the Transport Layer are :

Segmentation and Reassembly: This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the segment produced has a header associated with it. The transport layer at the destination station reassembles the message

Service Point Addressing: In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.

Ex. Web server and web Browser (port 80)

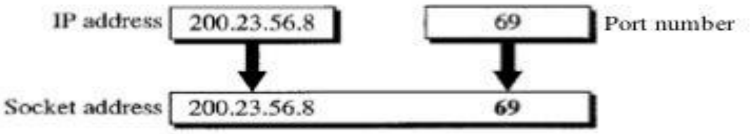


Port address

- In computer networking, a **port** is a communication endpoint.
- A port number is a 16-bit unsigned integer, thus ranging from 0 to 65535.
- At the software level, within an operating system, a port is a logical construct that identifies a specific process or a type of network service.
- Ports are identified for each protocol and address combination by 16-bit unsigned numbers, commonly known as the **port number**.
- **Port numbers 0-1023 – Well known ports.** These are allocated to **server services** by the **Internet Assigned Numbers Authority** (IANA). e.g Web servers normally use **port 80** and SMTP servers use **port 25**
- **Ports 1024-49151- Registered Port** -These can be registered for services with the **IANA** and should be treated as **semi-reserved.** User written programs should not use these ports.
- **Ports 49152-65535**– These are used by **client programs** and you are free to use these in client programs. When a Web browser connects to a web server the browser will allocate itself a port in this range. Also known as **ephemeral ports**.

Socket Addresses

- Process-to-process delivery needs two identifiers, IP address and the port number, at each end to make a connection.
- The combination of an IP address and a port number is called a socket address.
- The client socket address defines the client process uniquely just as the server socket address defines the server process uniquely
- A transport layer protocol needs a pair of socket addresses: the client socket address and the server socket address.
- These four pieces of information are part of the IP header and the transport layer protocol header.
- The IP header contains the IP addresses; the UDP or TCP header contains the port numbers.



The Services Provided by the Transport layer :

Connection Oriented Service: It is a three-phase process which include

– Connection Establishment

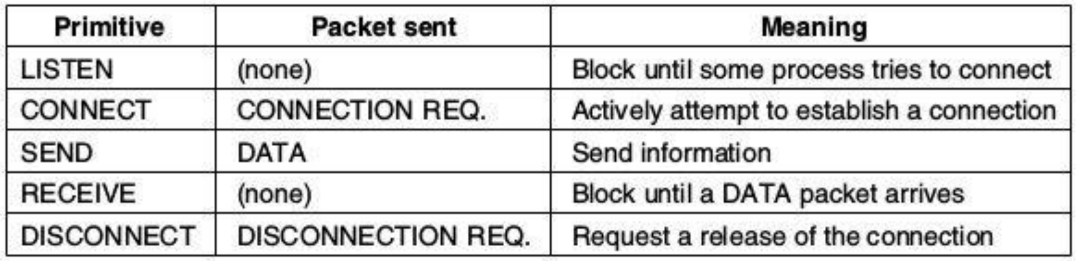
– Data Transfer

– Termination / disconnection

Connection less service: It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

Services Primitives

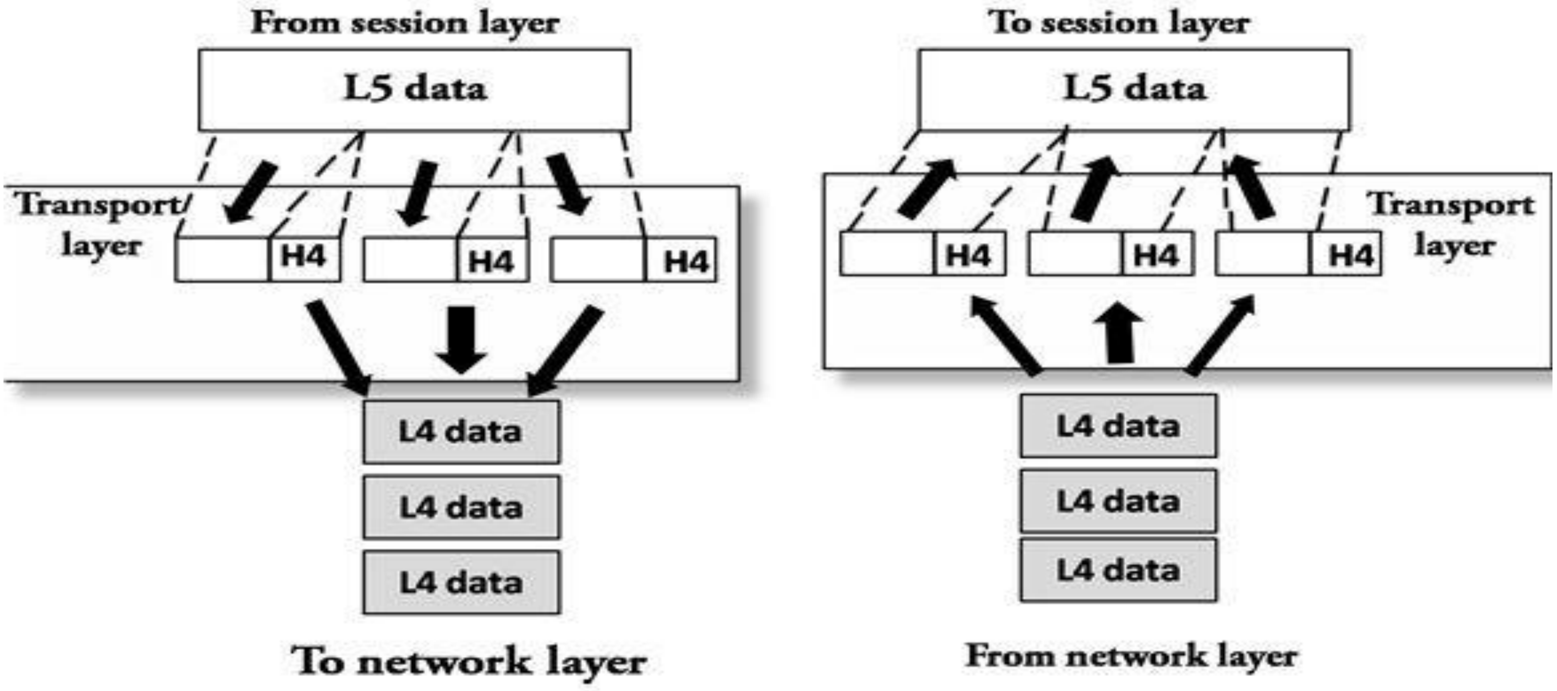
To allow users to access the transport service, the transport layer must provide some operations to application programs,



Primitive	Packet sent	Meaning
LISTEN	(none)	Block until some process tries to connect
CONNECT	CONNECTION REQ.	Actively attempt to establish a connection
SEND	DATA	Send information
RECEIVE	(none)	Block until a DATA packet arrives
DISCONNECT	DISCONNECTION REQ.	Request a release of the connection

Figure 6-2. The primitives for a simple transport service.

Transport Layer

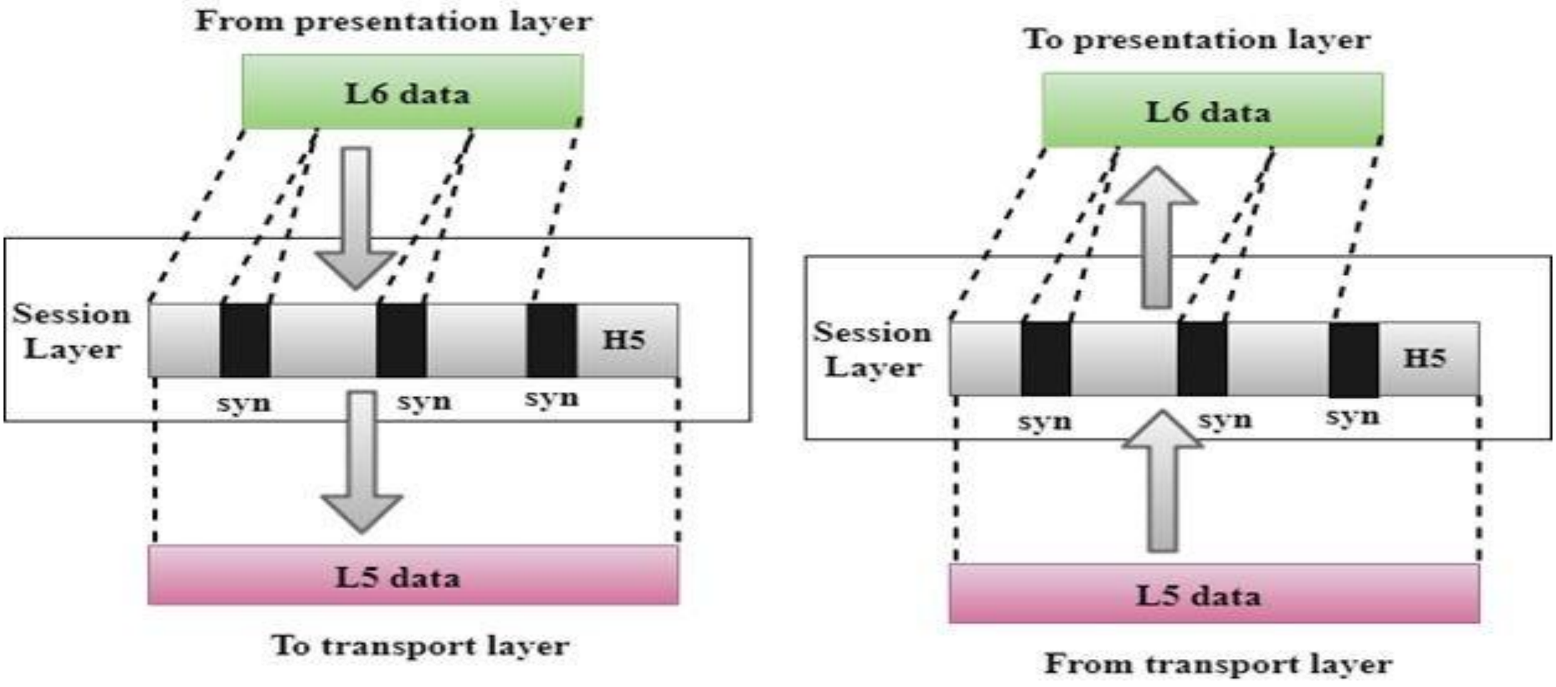


Session Layer (Layer 5) :

The functions of the session layer are :

1. **Session establishment, maintenance and termination:** The layer allows the two processes to establish, use and terminate a connection.
2. **Synchronization :** This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
3. **Dialog Controller :** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

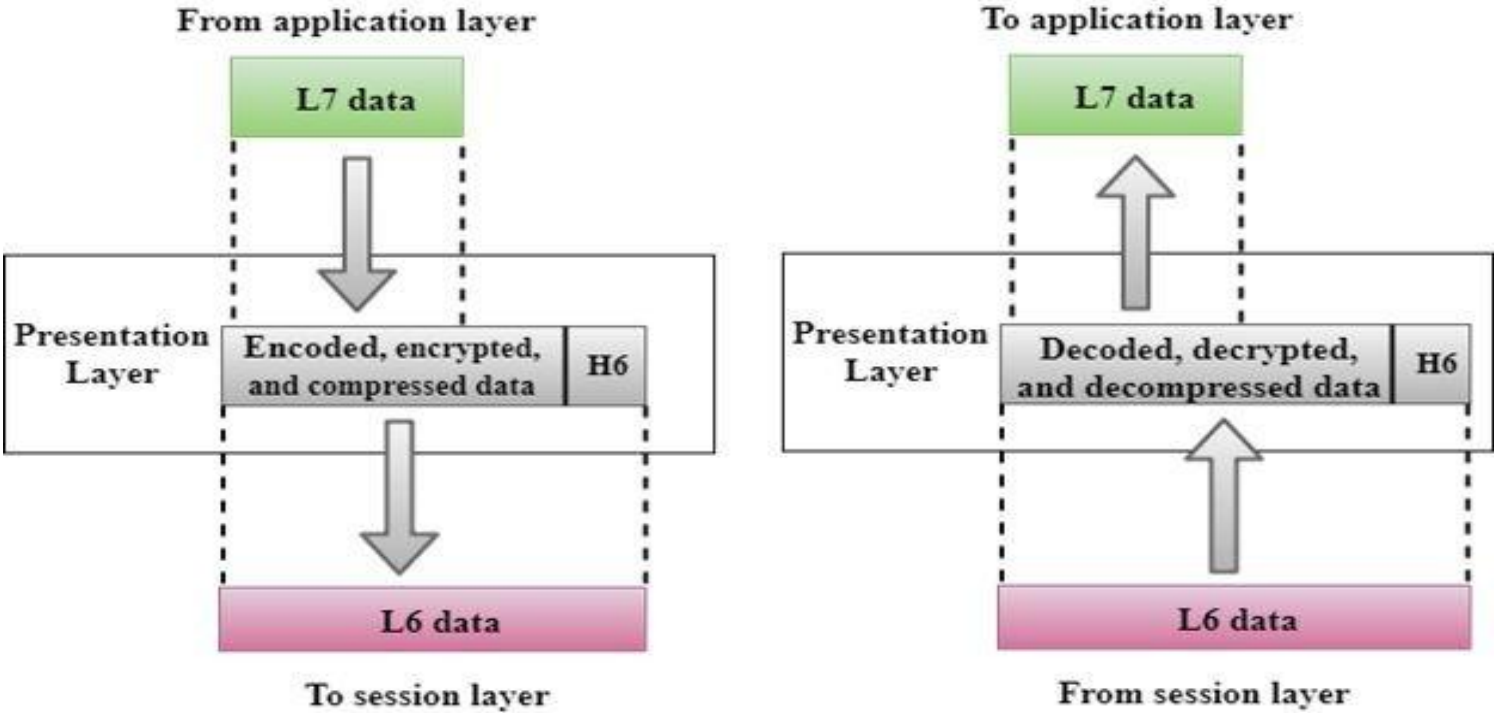
Session Layer

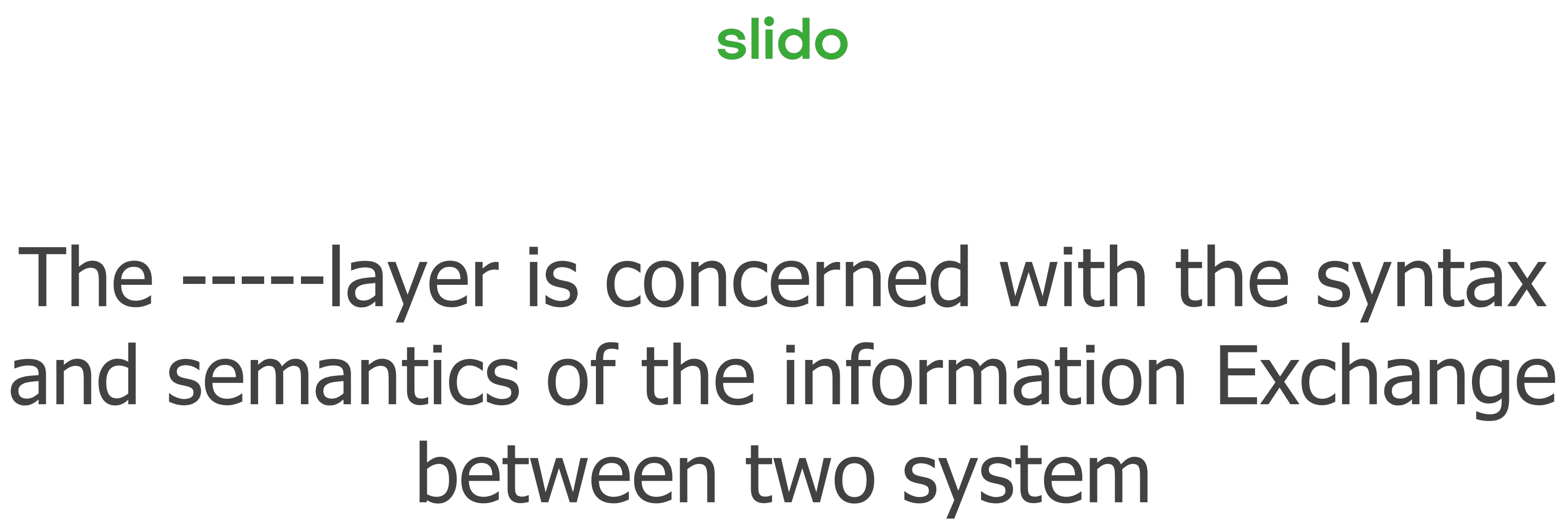


Presentation Layer (Layer 6) :

1. **Translation :** For example, ASCII to EBCDIC.
2. **Encryption/ Decryption :** Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
3. **Compression:** Reduces the number of bits that need to be transmitted on the network.

Presentation Layer





The -----layer is concerned with the syntax and semantics of the information Exchange between two system

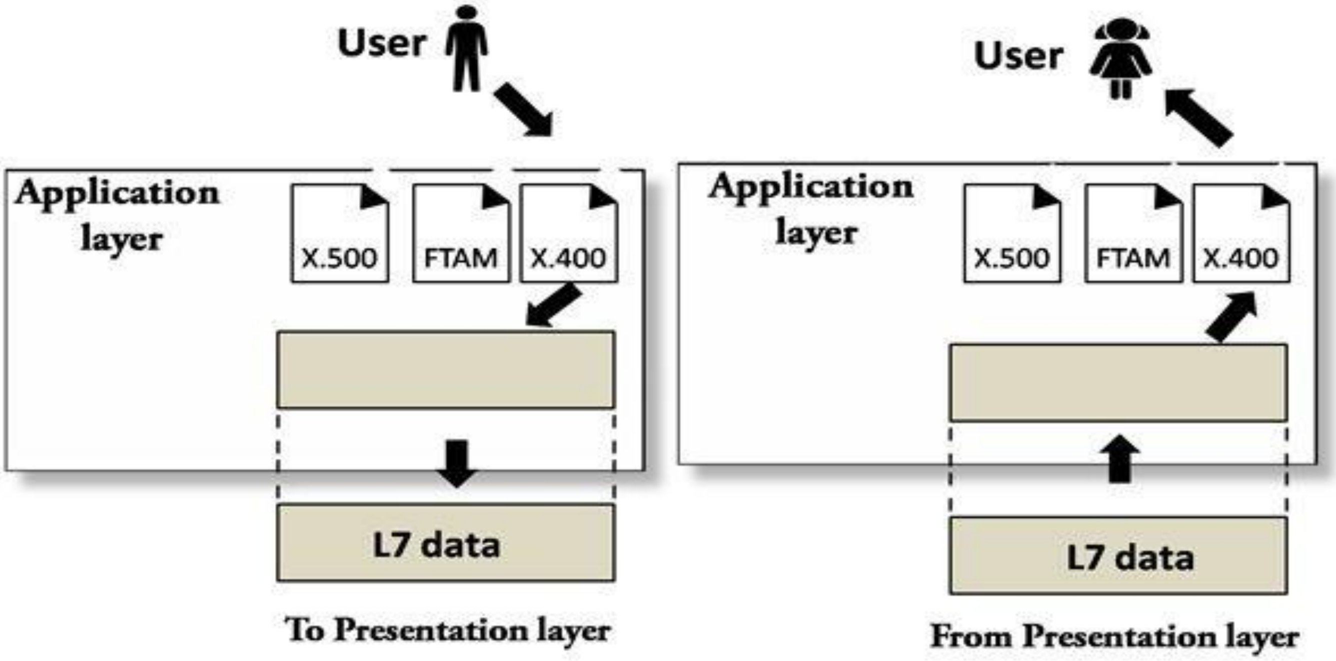
Application Layer (Layer 7) :

- At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications.
- These applications produce the data, which has to be transferred over the network.
- This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

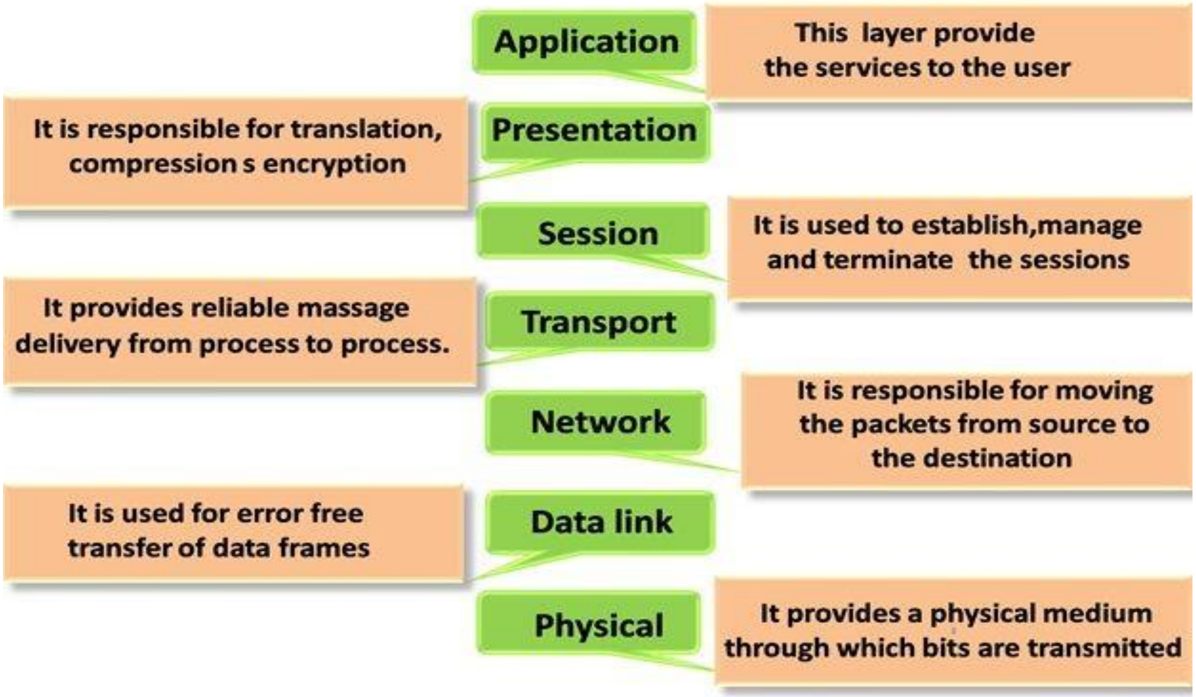
The functions of the Application layer are :

1. Network Virtual Terminal
2. FTAM-File transfer access and management
3. Mail Services
4. Directory Services

Application Layer



Summary of Layers



Application

This layer provide the services to the user

It is responsible for translation, compression s encryption

Presentation

Session

It is used to establish,manage and terminate the sessions

It provides reliable massage delivery from process to process.

Transport

Network

It is responsible for moving the packets from source to the destination

It is used for error free transfer of data frames

Data link

Physical

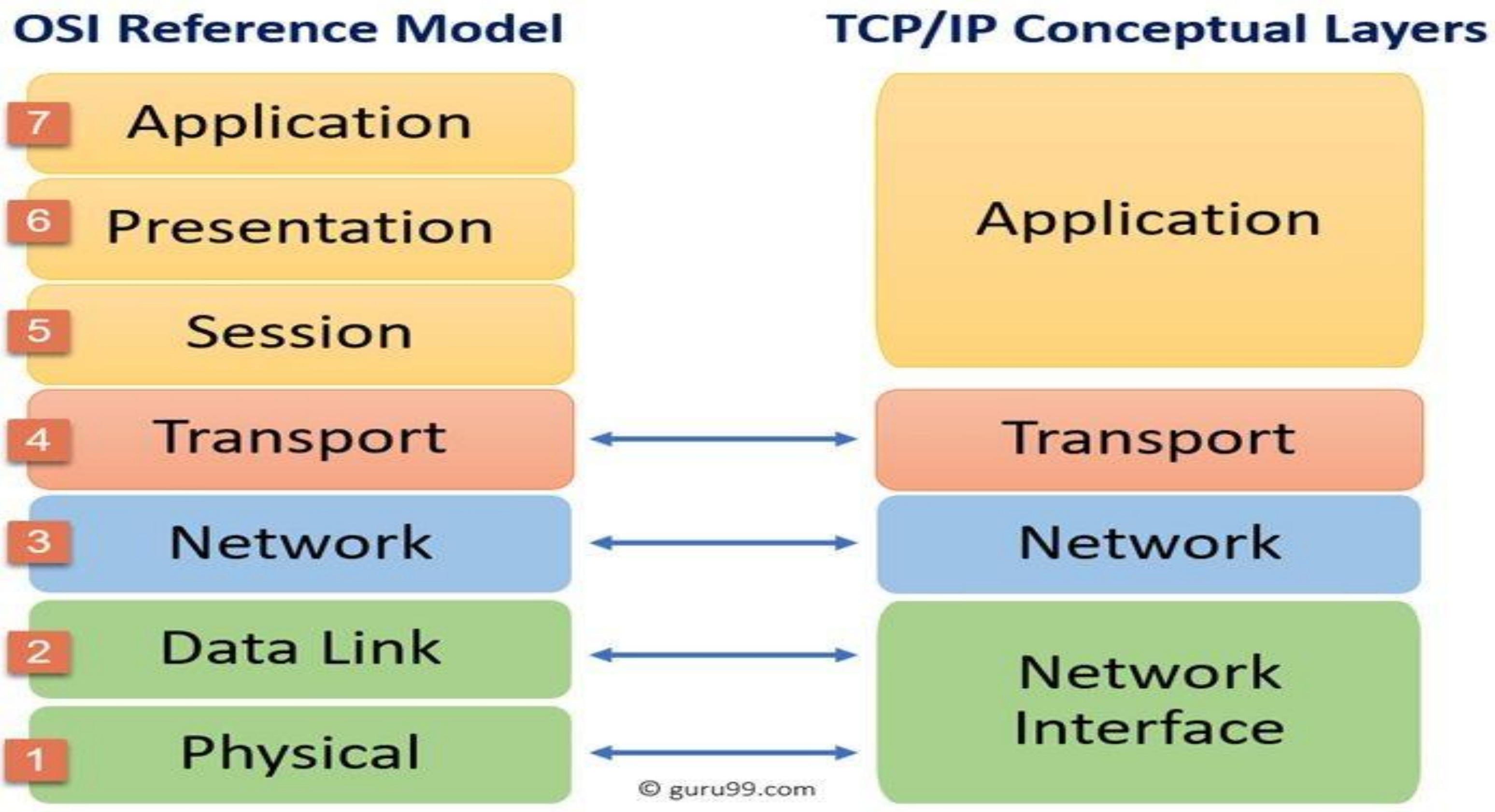
It provides a physical medium through which bits are transmitted

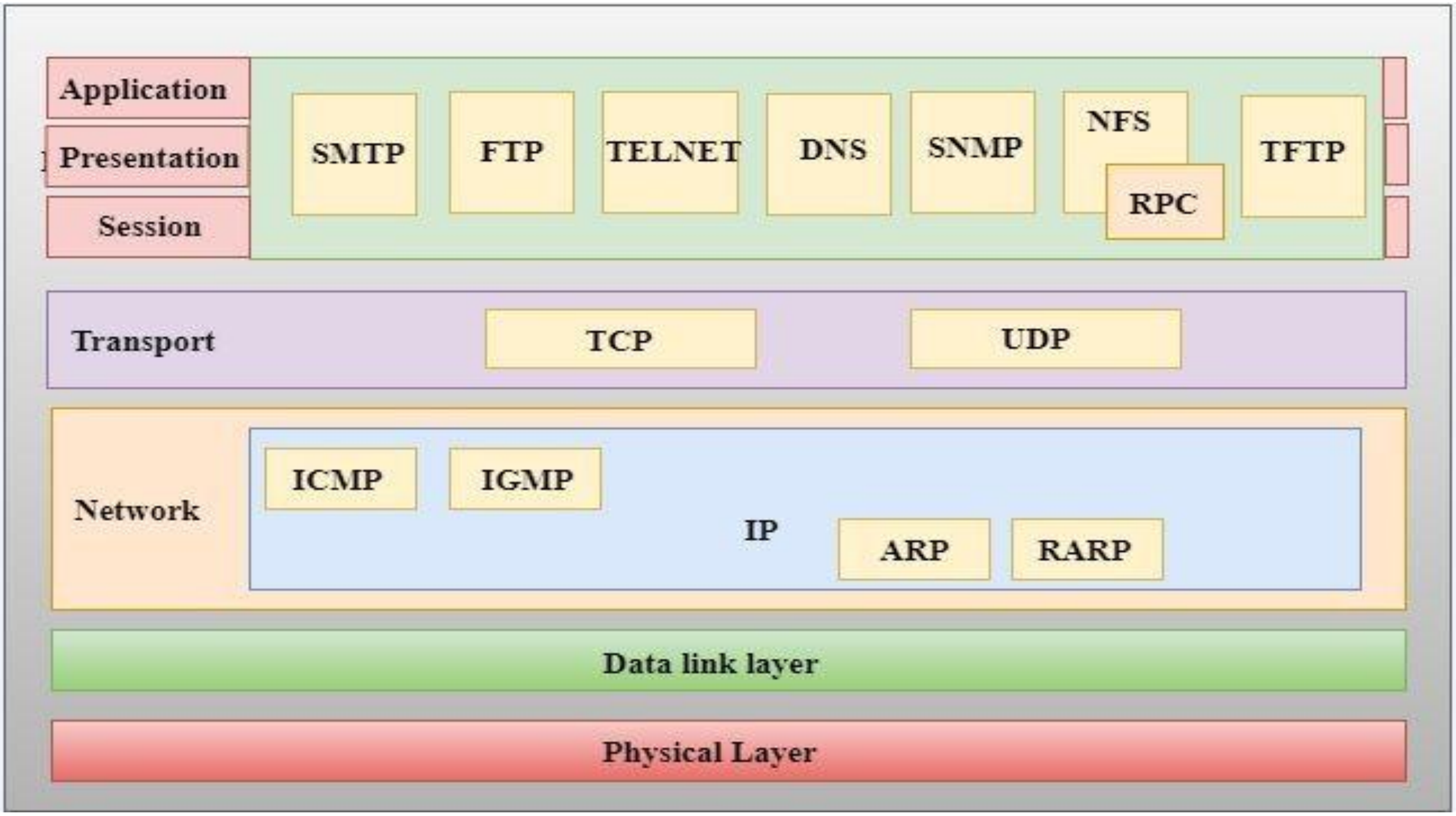
TCP/IP Reference Model

- It was designed and developed by The ARPANET which was a research network sponsored by the DoD (U.S. Department of Defense). in 1960s
- TCP/IP means Transmission Control Protocol and Internet Protocol.

The features that stood out during the research, which led to making the TCP/IP reference model were:

- Support for a flexible architecture. Adding more machines to a network was easy.
- The network was robust, and connections remained intact until the source and destination machines were functioning.





Layer 1 The Link Layer

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network.

Layer 2: Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.
6. The various functions performed by the Internet Layer are:
    - Delivering IP packets
    - Performing routing
    - Avoiding congestion

Layer 3: Transport Layer

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.

Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. **TELNET** is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
2. **FTP**(File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. **SMTP**(Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.

Layer 4: Application Layer(continue)

1. **DNS**(Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.
2. It allows peer entities to carry conversation.
3. It defines two end-to-end protocols: TCP and UDP
   - **TCP(Transmission Control Protocol):** It is a reliable connection-oriented protocol which handles byte-stream from source to destination without error and flow control.
   - **UDP(User-Datagram Protocol):** It is an unreliable connection-less protocol that do not want TCPs, sequencing and flow control. Eg: One-shot request-reply kind of service.

Comparison between TCP/IP and OSI References Model

OSI References Model	TCP/IP Model
It is developed by ISO (International Standard Organization)	It is developed by ARPANET (Advanced Research Project Agency Network).
OSI model provides a clear distinction between interfaces, services, and protocols.	TCP/IP doesn't have any clear distinguishing points between services, interfaces, and protocols.
OSI layers have seven layers.	TCP/IP has four layers.
OSI model is a generic model that is based upon functionalities of each layer.	TCP/IP model is a protocol-oriented standard.
The OSI model supports both connectionless and connection-oriented communication in the network layer, but only connection-oriented communication in the transport layer,	The TCP/IP model supports only one mode in the network layer (connectionless) but both in the transport layer,

Transmission Media

- Transmission media are actually located below the physical layer and are directly controlled by the physical layer.
- A communication channel that is used to carry the data from the transmitter to the receiver through the electromagnetic signals.
- A transmission medium can be broadly defined as anything that can carry information from a source to a destination.
- The transmission medium is usually free space, metallic cable, or fiber-optic cable.
- In data communication, it works like a physical path between the sender & the receiver. For instance, in a copper cable network the bits in the form of electrical signals whereas in a fiber network, the bits are available in the form of light pulses.
-

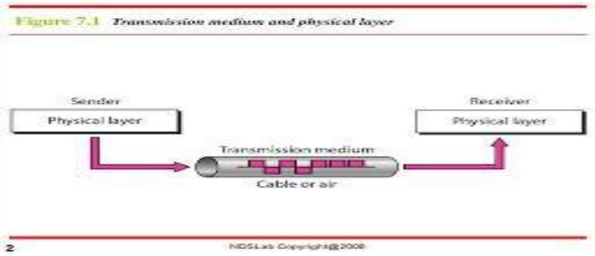
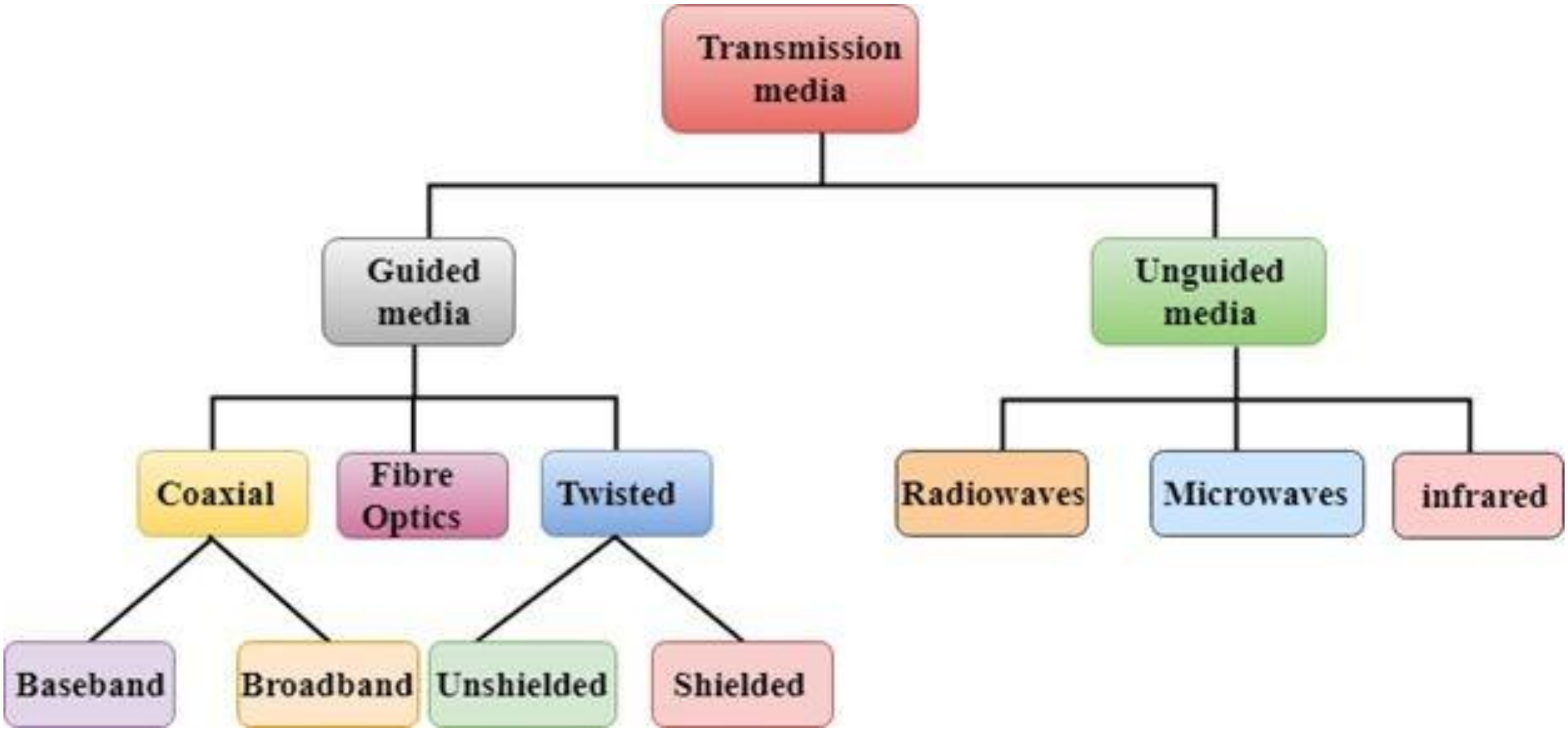


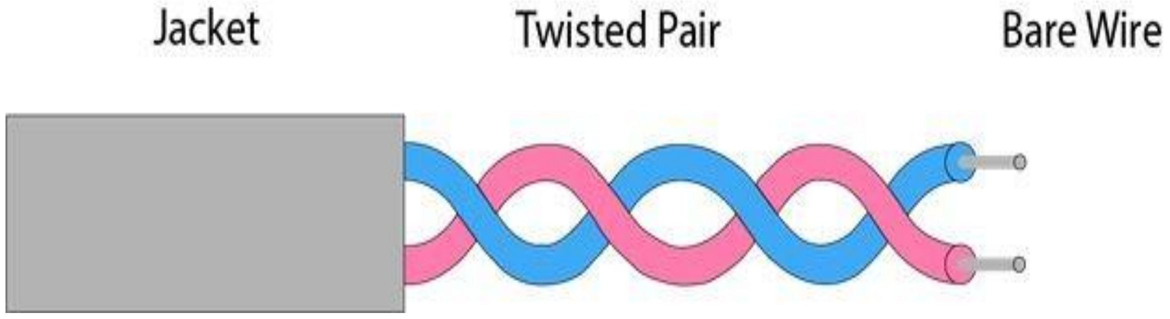
Figure 7.1 *Transmission medium and physical layer*

Classes of Transmission Media

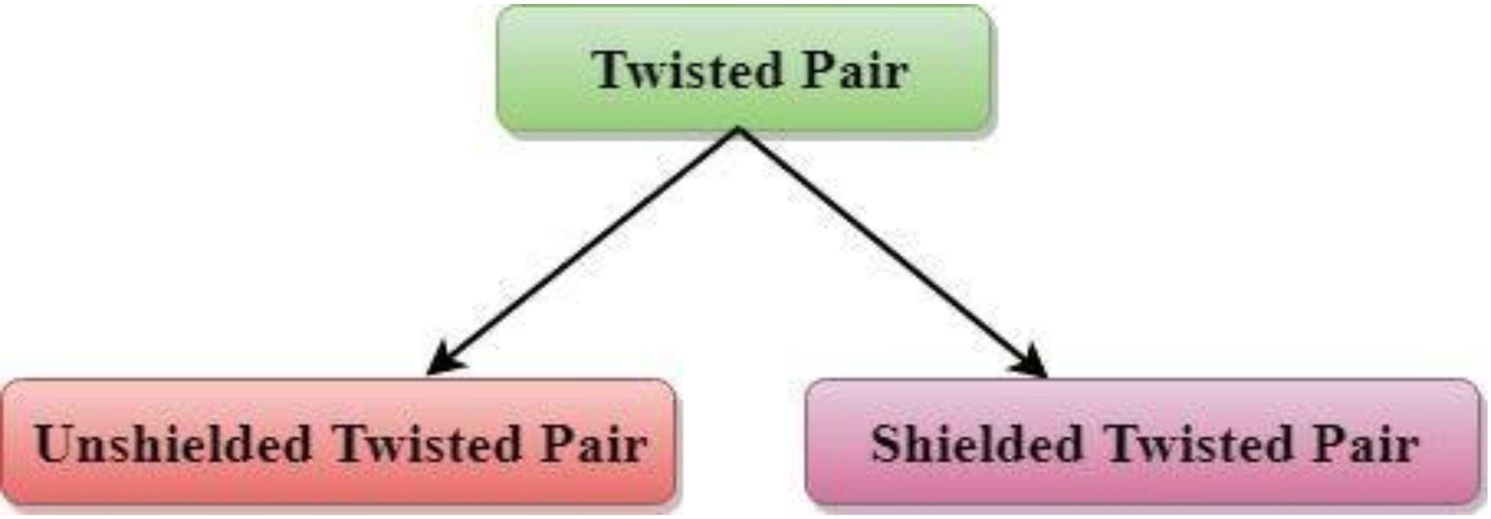


Twisted pair:

- Twisted pair is a physical media made up of a pair of cables twisted with each other.
- Twisted pair cables have been around for a long time.
- A twisted pair cable is cheap as compared to other transmission media.
- Installation of the twisted pair cable is easy, and it is a lightweight cable.
- The frequency range for twisted pair cable is from 0 to 3.5KHz.
- A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.



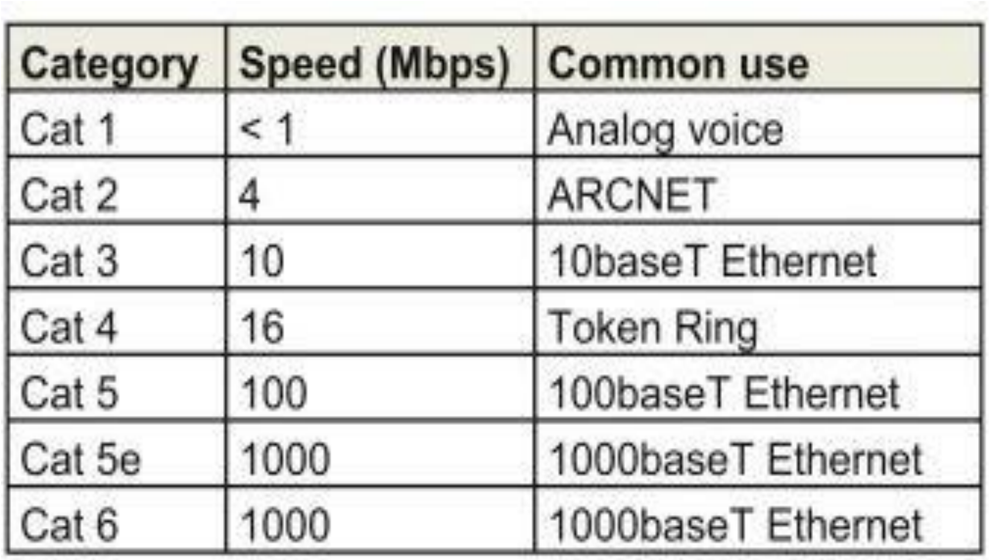
Types of Twisted pair:



UTP (Unshielded Twisted Pair)

- This UTP cable has the capacity to block interference.
- It doesn't depend on a physical guard and used in telephonic applications.
- The advantage of UTP is a low cost, very simple to install, and high speed.
- The disadvantages of UTP is liable to exterior interference, transmits in fewer distances, and less capacity.

Category Cabling Speed and Usage



Category	Speed (Mbps)	Common use
Cat 1	< 1	Analog voice
Cat 2	4	ARCNET
Cat 3	10	10baseT Ethernet
Cat 4	16	Token Ring
Cat 5	100	100baseT Ethernet
Cat 5e	1000	1000baseT Ethernet
Cat 6	1000	1000baseT Ethernet

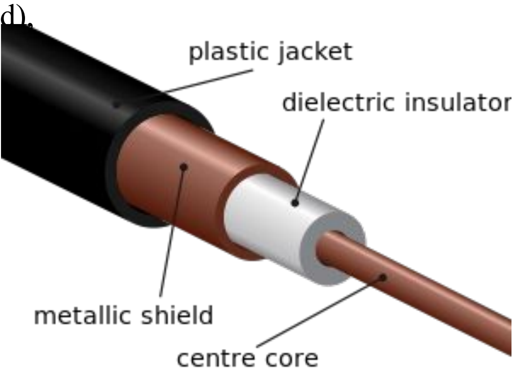
Shielded Twisted Pair

Shielded twisted pair (STP) cable was originally designed by IBM for token ring networks.
It include two individual wires covered with a foil shielding, which prevents electromagnetic interference,.

It transporting data faster.

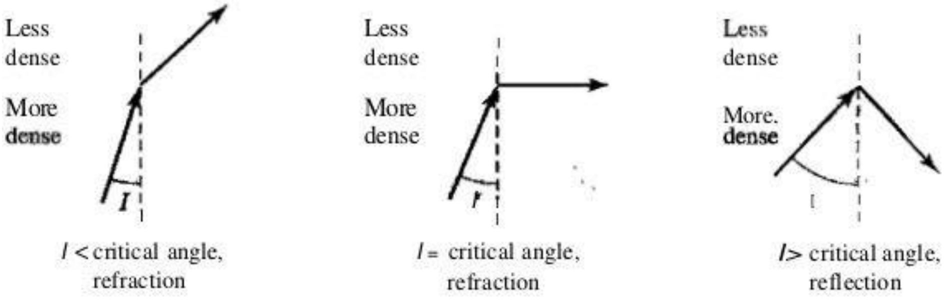
Coaxial Cable

- **Coaxial cable**, or **coax** is a type of electrical cable.
- Consisting of an inner conductor surrounded by a concentric conducting shield, with the two separated by a dielectric (insulating material);
- Many coaxial cables also have a protective outer sheath or jacket.
- The term "coaxial" refers to the inner conductor and the outer shield sharing a geometric axis.
- Coaxial cable is commonly used by cable operators, telephone companies, and internet providers around the world to convey data, video, and voice communications to customers. It has also been used extensively within homes.
- The transmission speed of coaxial cable is 10Mbps (megabits per second).
- RG – 59: Has impedance of 75W and used in cable TV
- RG – 58: Has impedance of 50W and used in thin Ethernet
- RG – 11: Has impedance of 50W and used in thick Ethernet



Fiber Optic Cable

- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- Light travels in a straight line as long as it is moving through a single uniform substance.
- If a ray of light traveling through one substance suddenly enters another substance (of a different density), the ray changes direction. As the figure shows,
- if the angle of incidence I (the anble I, the ray makes with the line perpendicular to the interface between the two substances) is less than the critical angle, the ray refracts and moves closer to the surface.
- If the angle of incidence is equal to the critical angle, the light bends along the interface.
- If the angle is greater than the critical angle, the ray reflects (makes a turn) and travels again in the denser substance.



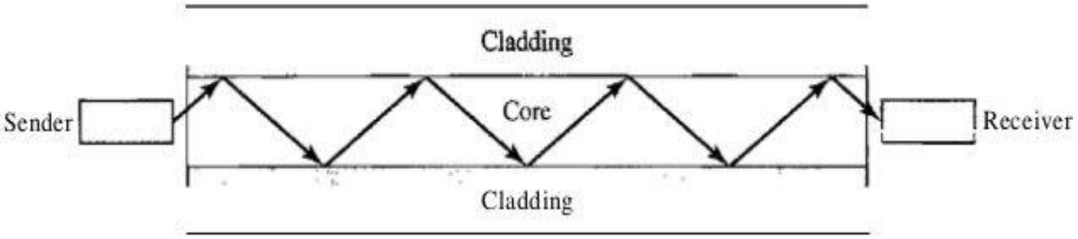
I < critical angle, refraction

I = critical angle, refraction

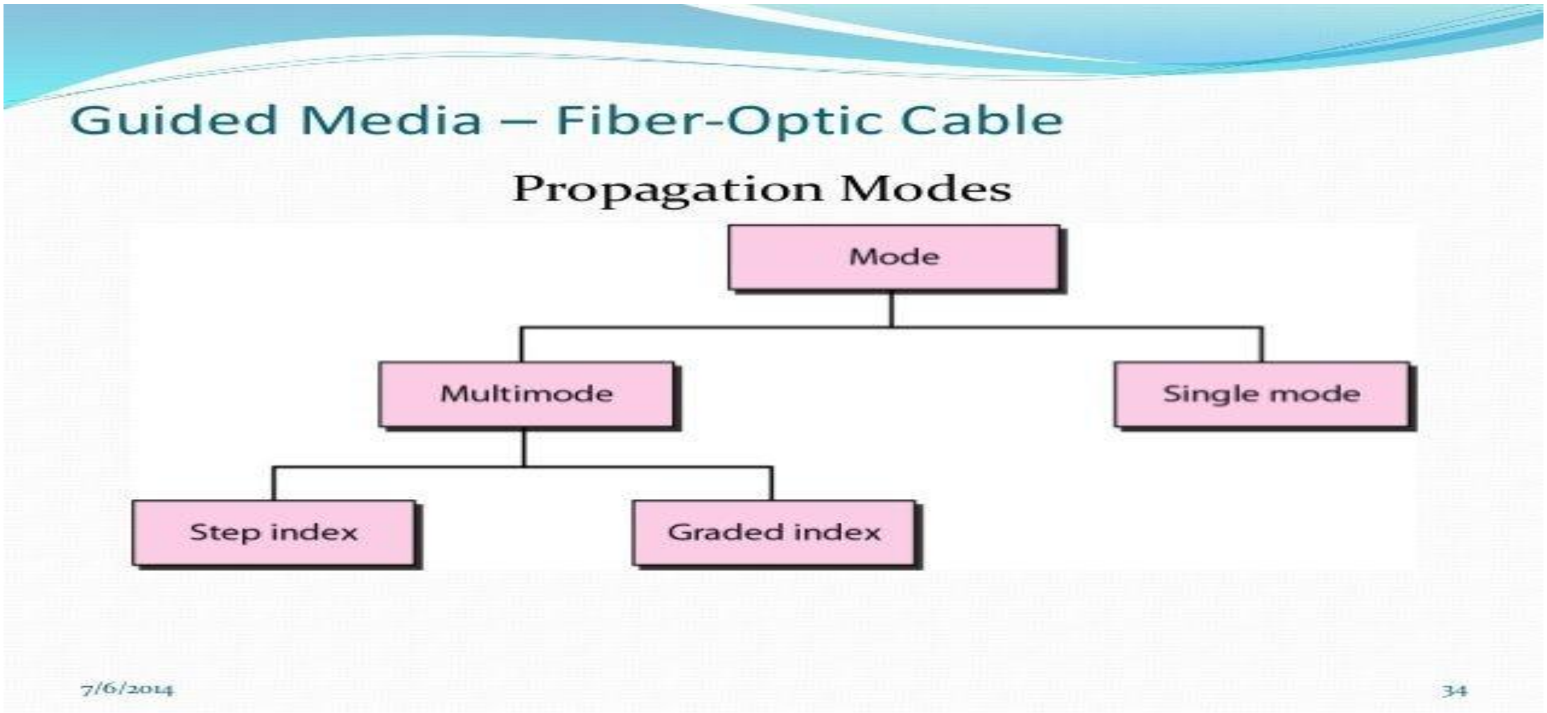
I> critical angle, reflection

Fiber Optic

- Optical fibers use reflection to guide light through a channel.
- A glass or plastic core is surrounded by a cladding of less dense glass or plastic.
- The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it. See Figure



Propagation Modes



Guided Media – Fiber-Optic Cable

Propagation Modes

Mode

Multimode

Single mode

Step index

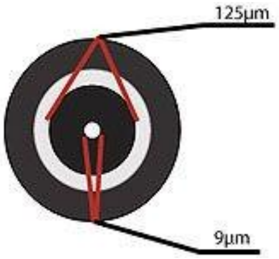
Graded index

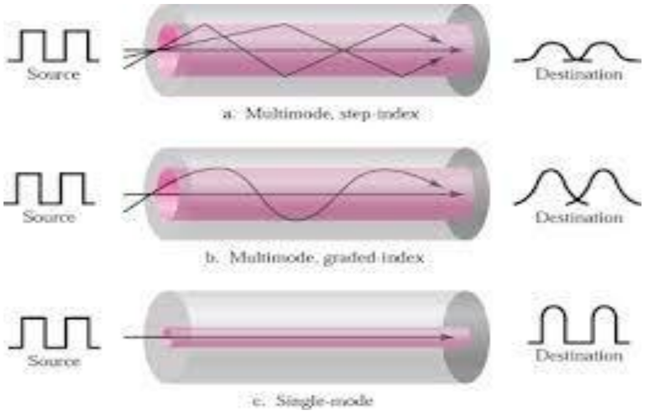
7/6/2014

34

Single Mode

- Single Mode fiber optic cable has a small diametral core that allows only one mode of light to propagate.
- Because of this, the number of light reflections created as the light passes through the core decreases, lowering attenuation and creating the ability for the signal to travel further.
- This application is typically used in long distance, higher bandwidth runs by Telcos, CATV companies, and Colleges and Universities.
- Fig. shows the diameter of core and cladding n single mode .This means that the core to cladding diameter ratio is 9 microns to 125 microns.



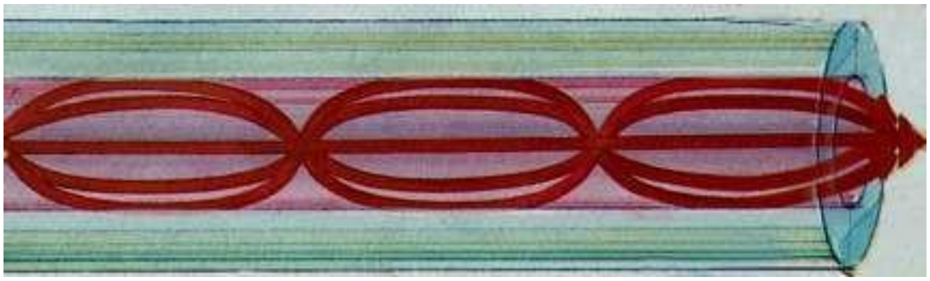


Multimode Step Index

- Multimode is so named because multiple beams from a light source move through the core in different paths.
- In multimode step-index fiber, the density of the core remains constant from the center to the edges.
- A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding.
- At the interface, there is an abrupt change due to a lower density; this alters the angle of the beam's motion.
- The term step index refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fiber.

Multimode Graded index

- Density is highest at the center of the core and decreases gradually to its lowest at the edge.
- The word index here refers to the index of refraction, the index of refraction is related to density.
- The core here is much larger than in the single-mode step index case previously discussed.



Advantages Fiber-optic cable

1. **Higher bandwidth.** Fiber-optic cable can support dramatically higher bandwidths (and hence data rates) than either twisted-pair or coaxial cable.
2. **Less signal attenuation.** Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration.
3. **Immunity to electromagnetic interference.** Electromagnetic noise cannot affect fiber-optic cables.
4. **Resistance to corrosive materials.** Glass is more resistant to corrosive materials than copper
5. **Light weight.** Fiber-optic cables are much lighter than copper cables.
6. **Greater immunity to tapping.** Fiber-optic cables are more immune to tapping

   than copper cables. Copper cables create antenna effects that can easily be tapped .

Disadvantages

1. **Its installation and maintenance** require expertise that is not yet available everywhere.
2. **Unidirectional light propagation.** Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
3. **Cost.** The cable and the interfaces are relatively more expensive . If the demand for bandwidth is not high, often the use of optical fiber cannot be justified.

Unguided Transmission Media

- Unguided media transport electromagnetic waves without using a physical conductor.
- This type of communication is often referred to as wireless communication.
- Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.
- Figure shows the part of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, used for wireless communication.

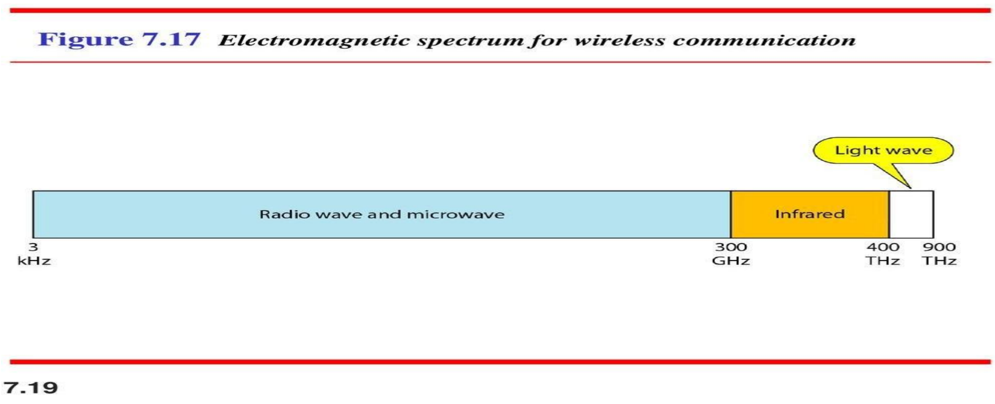
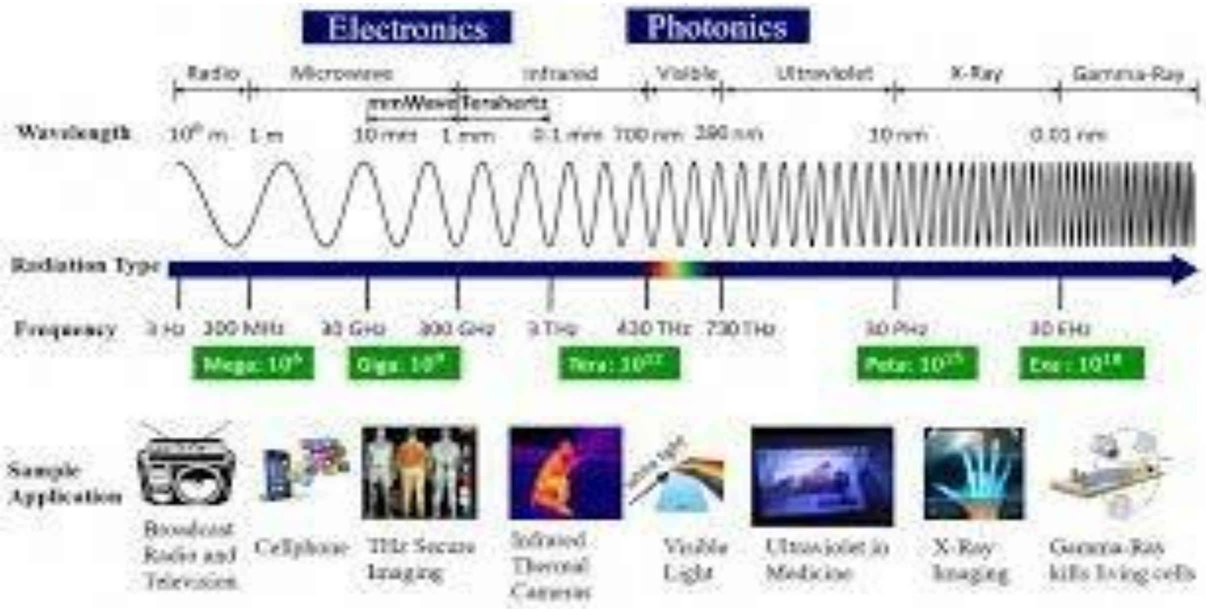


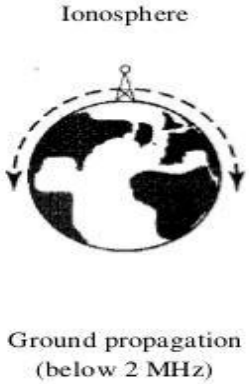
Figure 7.17 *Electromagnetic spectrum for wireless communication*

7.19



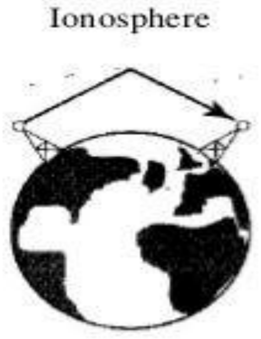
Unguided Transmission Media

- Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation, as shown in Figure
- **In ground propagation,** radio waves travel through the lowest portion of the atmosphere, hugging the earth.
- These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet.
- Distance depends on the amount of power in the signal: The greater the power, the greater the distance.



- In sky propagation,

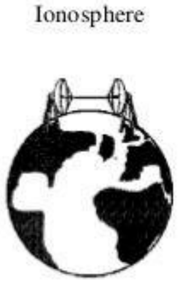
- Higher-frequency radio waves radiate upward into the ionosphere (the layer of atmosphere where particles exist as ions) where they are reflected back to earth.
- This type of transmission allows for greater distances with lower output power.



Sky propagation
(2-30 MHz)

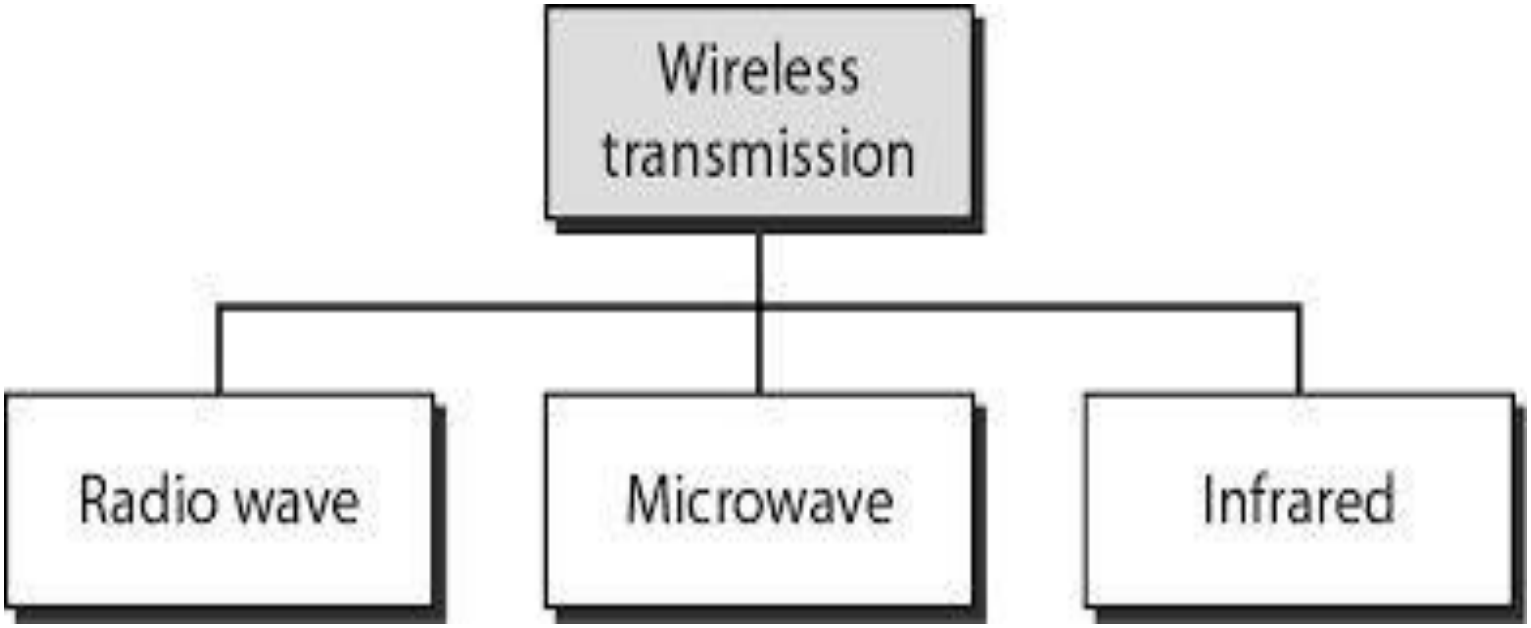
In line-or-sight propagation,

- Very high-frequency signals are transmitted in straight lines directly from antenna to antenna.
- Antennas must be directional, facing each other,and either tall enough or close enough together not to be affected by the curvature of the earth.



Line-af-sight propagation
(above 30 MHz)

Types of Wireless Transmission



Radio Wave

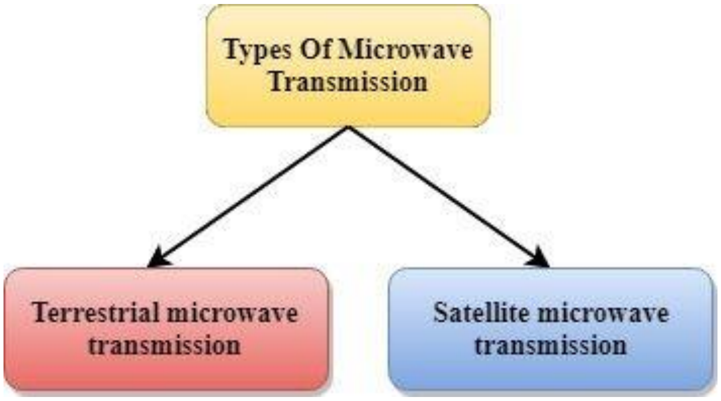
- Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
- The range in frequencies of radio waves is from 3Khz to 1 khz.
- In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.
- An example of the radio wave is **FM radio**

Applications Of Radio waves:

- A Radio wave is useful for multicasting when there is one sender and many receivers.
- An FM radio, television, cordless phones are examples of a radio wave.
- Radio transmission is mainly used for wide area networks and mobile cellular phones.

Microwaves are of two types:

- Terrestrial microwave
- Satellite microwave communication.


Types Of Microwave Transmission
Terrestrial microwave transmission
Satellite microwave transmission

Terrestrial Microwave Transmission

- Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.

- Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.
- Microwaves are unidirectional as the sending and receiving antenna is to be aligned, i.e., the waves sent by the sending antenna are narrowly focussed.

- In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.
- It works on the line of sight transmission, i.e., the antennas mounted on the towers are the direct sight of each other.

Characteristics of Microwave:

- **Frequency range:** The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
- **Bandwidth:** It supports the bandwidth from 1 to 10 Mbps.
- **Short distance:** It is inexpensive for short distance.
- **Long distance:** It is expensive as it requires a higher tower for a longer distance.
- **Attenuation:** Attenuation means loss of signal. It is affected by environmental conditions and antenna size.

Advantages Of Microwave:

- Microwave transmission is cheaper than using cables.
- It is free from land acquisition as it does not require any land for the installation of cables.
- Microwave transmission provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task.
- Communication over oceans can be achieved by using microwave transmission.

Disadvantages of Microwave transmission:

- **Eavesdropping:** An eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.
- **Out of phase signal:** A signal can be moved out of phase by using microwave transmission.
- **Susceptible to weather condition:** A microwave transmission is susceptible to weather condition. This means that any environmental change such as rain, wind can distort the signal.
- **Bandwidth limited:** Allocation of bandwidth is limited in the case of microwave transmission.

Satellite Microwave Communication

- A satellite is a physical object that revolves around the earth at a known height.
- Satellite communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems.
- We can communicate with any point on the globe by using satellite communication.

Advantages Of Satellite Microwave Communication:

- The coverage area of a satellite microwave is more than the terrestrial microwave.
- The transmission cost of the satellite is independent of the distance from the centre of the coverage area.
- Satellite communication is used in mobile and wireless communication applications.
- It is easy to install.
- It is used in a wide variety of applications such as weather forecasting, radio/TV signal broadcasting, mobile communication, etc.

Disadvantages Of Satellite Microwave Communication:

- Satellite designing and development requires more time and higher cost.
- The Satellite needs to be monitored and controlled on regular periods so that it remains in orbit.
- The life of the satellite is about 12-15 years. Due to this reason, another launch of the satellite has to be planned before it becomes non-functional.

Infrared

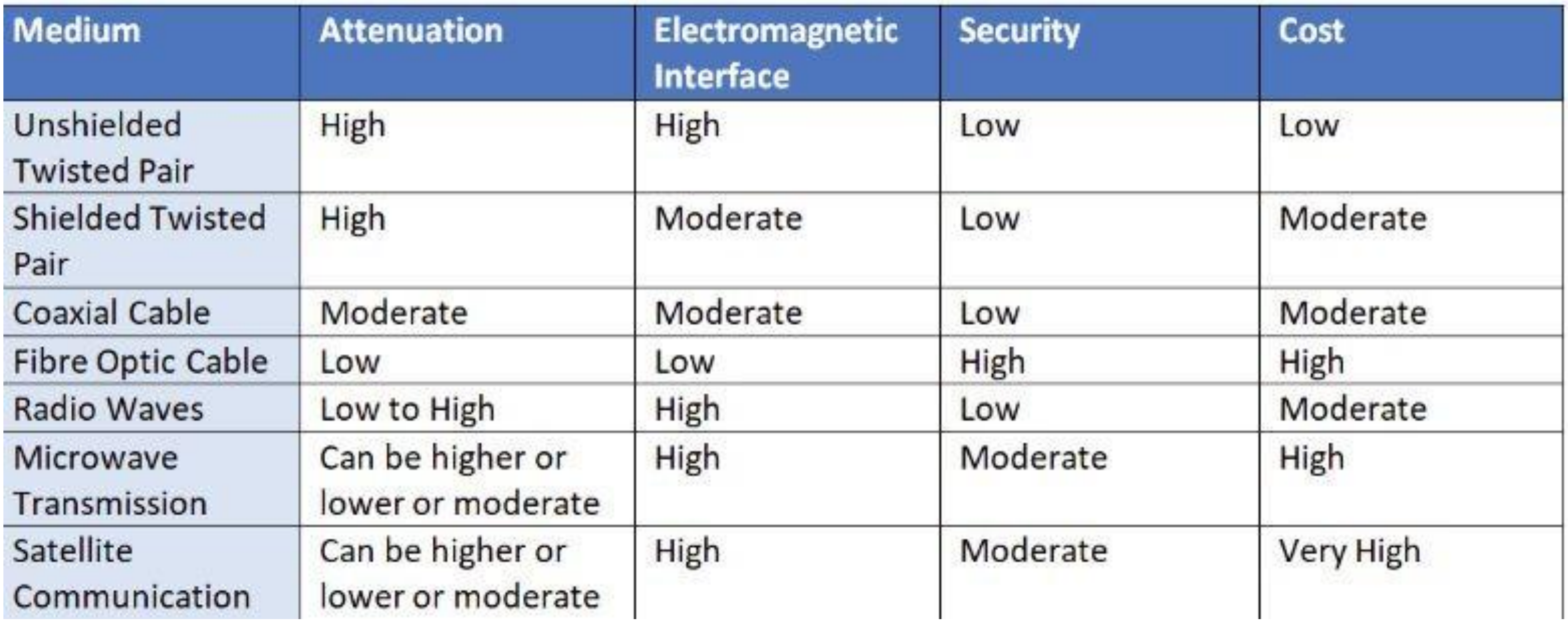
- An infrared transmission is a wireless technology used for communication over short ranges.
- The frequency of the infrared in the range from 300 GHz to 400 THz.
- It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Characteristics Of Infrared:

- It supports high bandwidth, and hence the data rate will be very high.
- Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.

- An infrared communication provides better security with minimum interference.
- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

Comparison of Transmission Media

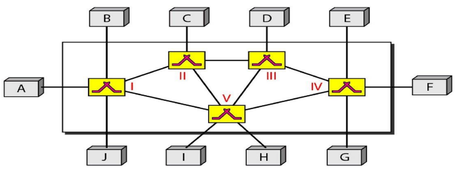


Medium	Attenuation	Electromagnetic Interface	Security	Cost
Unshielded Twisted Pair	High	High	Low	Low
Shielded Twisted Pair	High	Moderate	Low	Moderate
Coaxial Cable	Moderate	Moderate	Low	Moderate
Fibre Optic Cable	Low	Low	High	High
Radio Waves	Low to High	High	Low	Moderate
Microwave Transmission	Can be higher or lower or moderate	High	Moderate	High
Satellite Communication	Can be higher or lower or moderate	High	Moderate	Very High

Switching

- A network is a set of connected devices. Whenever we have multiple devices, we have the problem of how to connect them to make one-to-one communication possible.
- **A better solution is switching.**
- A switched network consists of a series of interlinked nodes, called switches.
- Switches are devices capable of creating temporary connections between two or more devices linked to the switch.
- In a switched network, some of these nodes are connected to the end systems (computers or telephones, for example). Others are used only for routing. Figure shows

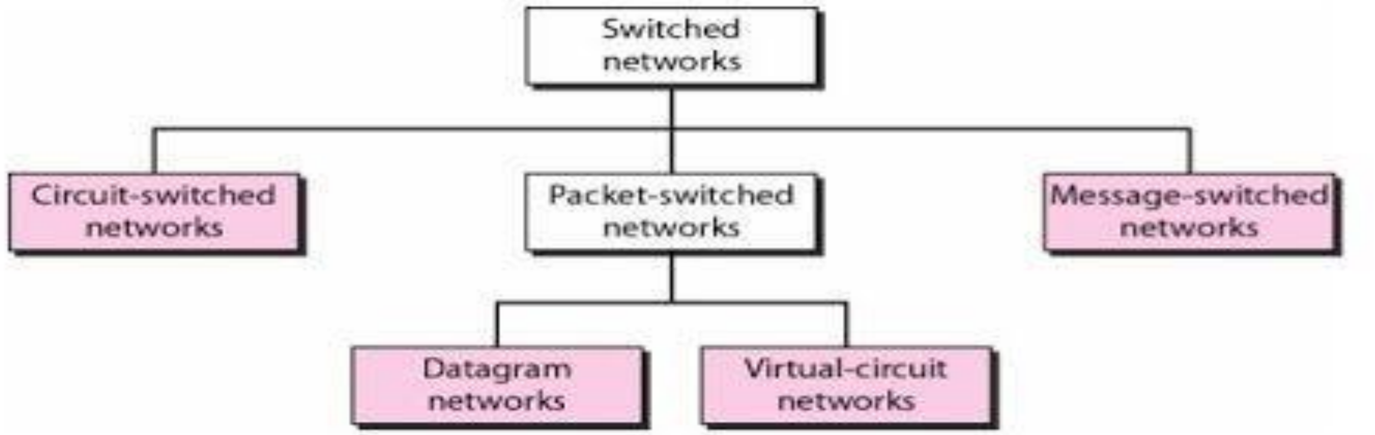
Figure 8.1 *Switched network*



8.2

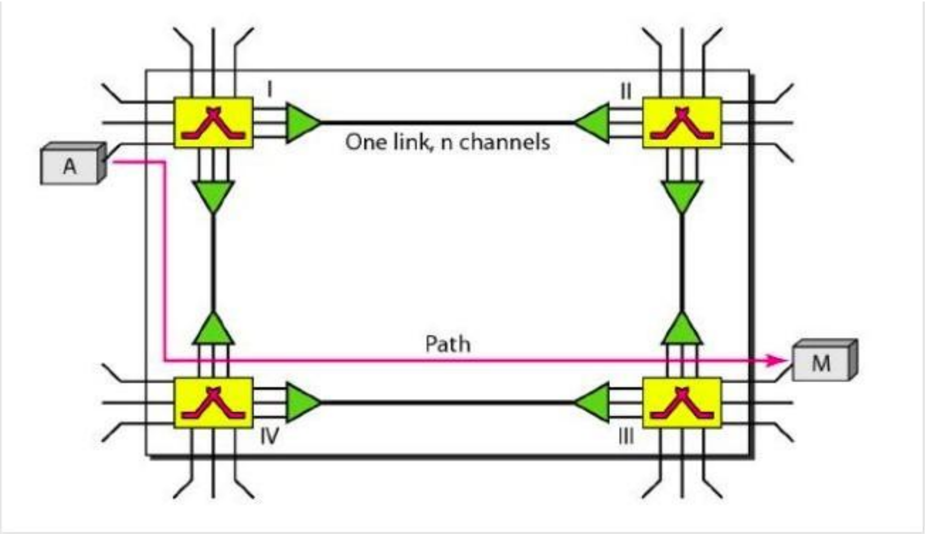
docsity.com

Switched networks



CIRCUIT-SWITCHED NETWORKS

- A circuit-switched network consists of a set of switches connected by physical links.
- A connection between two stations is a dedicated path made of one or more links.
- However, each connection uses only one dedicated channel on each link.
- Each link is normally divided into n channels by using FDM or TDM



Key Concept

- Circuit switching takes place at the physical layer.
- Before starting communication, the stations must make a reservation for the resources to be used during the communication.
- These resources, such as channels (bandwidth in FDM and time slots in TDM), switch buffers, switch processing time, and switch input/output ports, must remain dedicated during the entire duration of data transfer until the teardown phase.
- Data transferred between the two stations are not packetized (physical layer transfer of the signal). The data are a continuous flow sent by the source station and received by the destination station, although there may be periods of silence.
- There is no addressing involved during data transfer.
- The switches route the data based on their occupied band (FDM) or time slot (TDM). Of course, there is end-to end addressing used during the setup phase, as we will see shortly.

Advantages

Some of the advantages of circuit switching are as follows

- It uses a fixed bandwidth.
- A dedicated communication channel increases the quality of communication.
- Data is transmitted with a fixed data rate.
- No waiting time at switches.
- Suitable for long continuous communication.

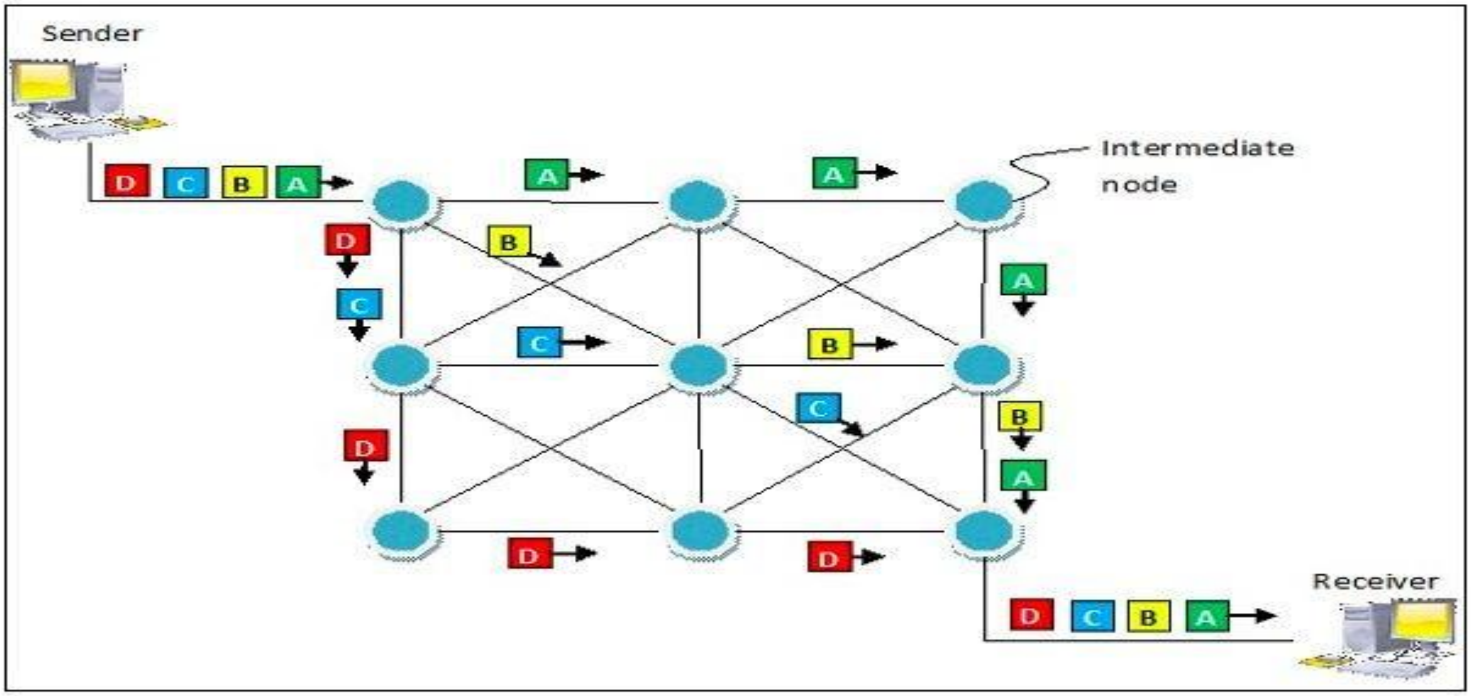
Disadvantages

- A dedicated connection makes it impossible to transmit other data even if the channel is free.
- Resources are not utilized fully.
- The time required to establish the physical link between the two stations is too long.
- As a dedicated path has to be established for each connection, circuit switching is more expensive.
- Even if there is no transfer of data, the link is still maintained until it is terminated by users. By this channel remains ideal for a long time thereby making circuit switching inefficient.
- Dedicated channels require more bandwidth

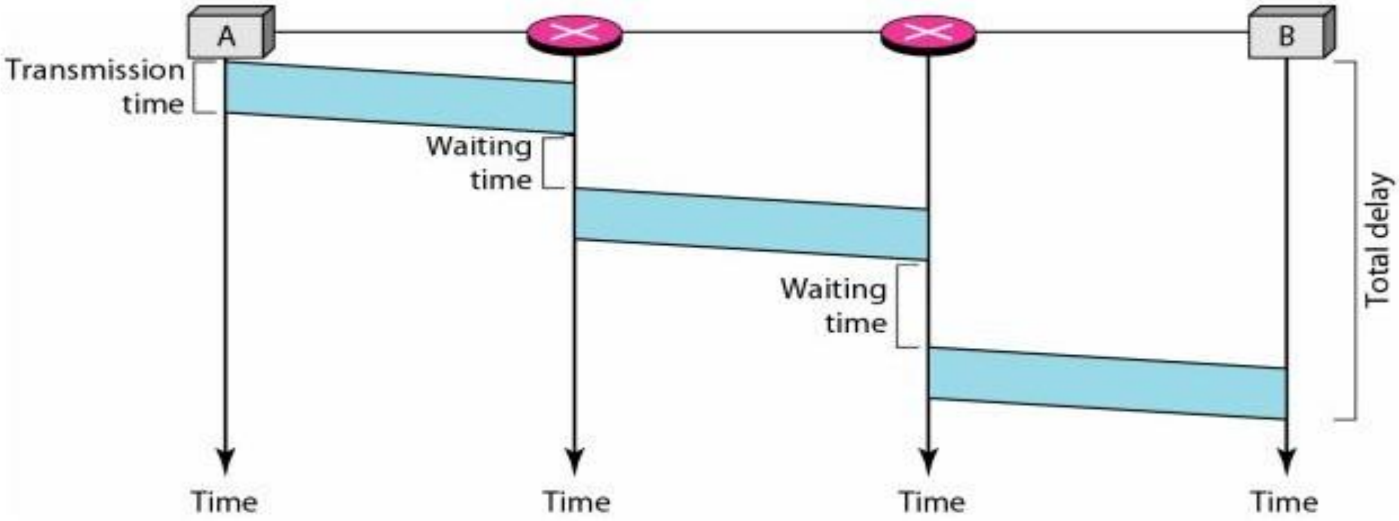
Packet switching

- Packet switching is a connectionless network switching technique.
- Here, the message is divided and grouped into a number of units called packets that are individually routed from the source to the destination.
- There is no need to establish a dedicated circuit for communication.
- Each packet in a packet switching technique has two parts: a header and a payload.
- The header contains the addressing information of the packet and is used by the intermediate routers to direct it towards its destination.
- The payload carries the actual data.
- A packet is transmitted as soon as it is available in a node, based upon its header information.
- The packets of a message are not routed via the same path.
- So, the packets in the message arrives in the destination out of order.
- It is the responsibility of the destination to reorder the packets in order to retrieve the original message.

- The process is diagrammatically represented in the following figure. Here the message comprises of four packets, A, B, C and D, which may follow different routes from the sender to the receiver.

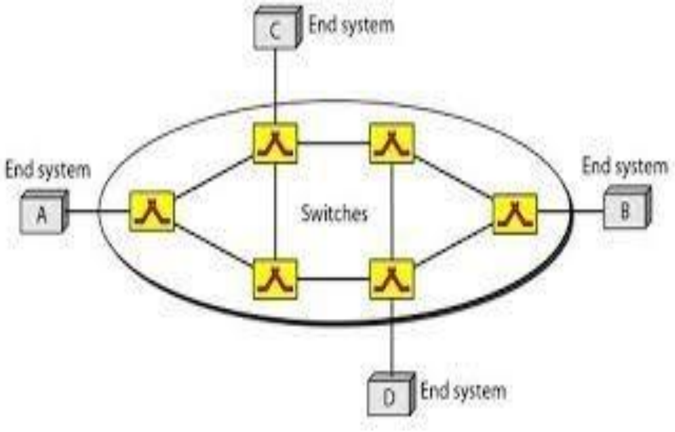


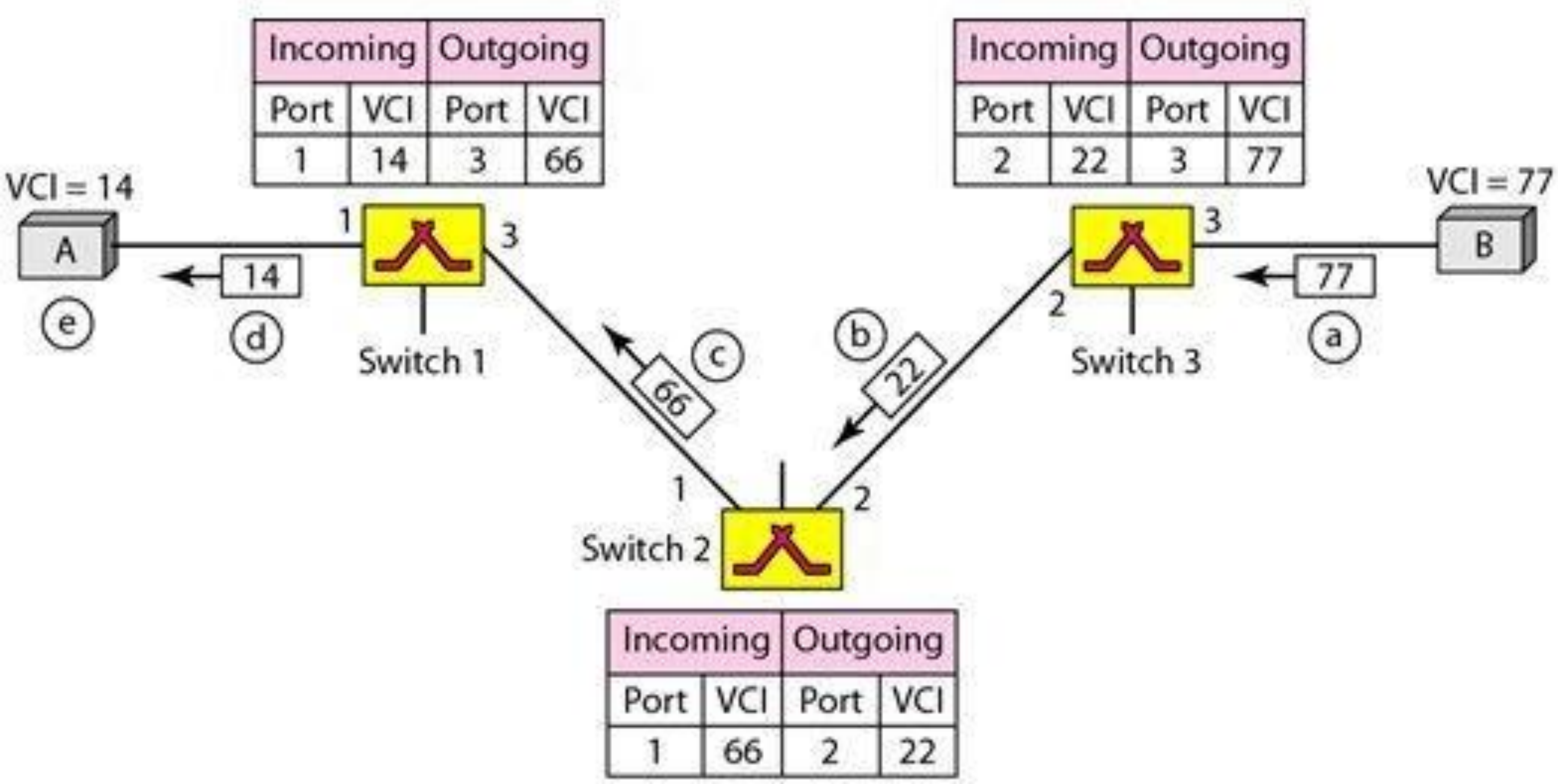
Delay



VIRTUAL-CIRCUIT NETWORKS

- A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.
- In virtual-circuit switching, all packets belonging to the same source and destination travel the same path; but the packets may arrive at the destination with different delays if resource allocation is on demand.



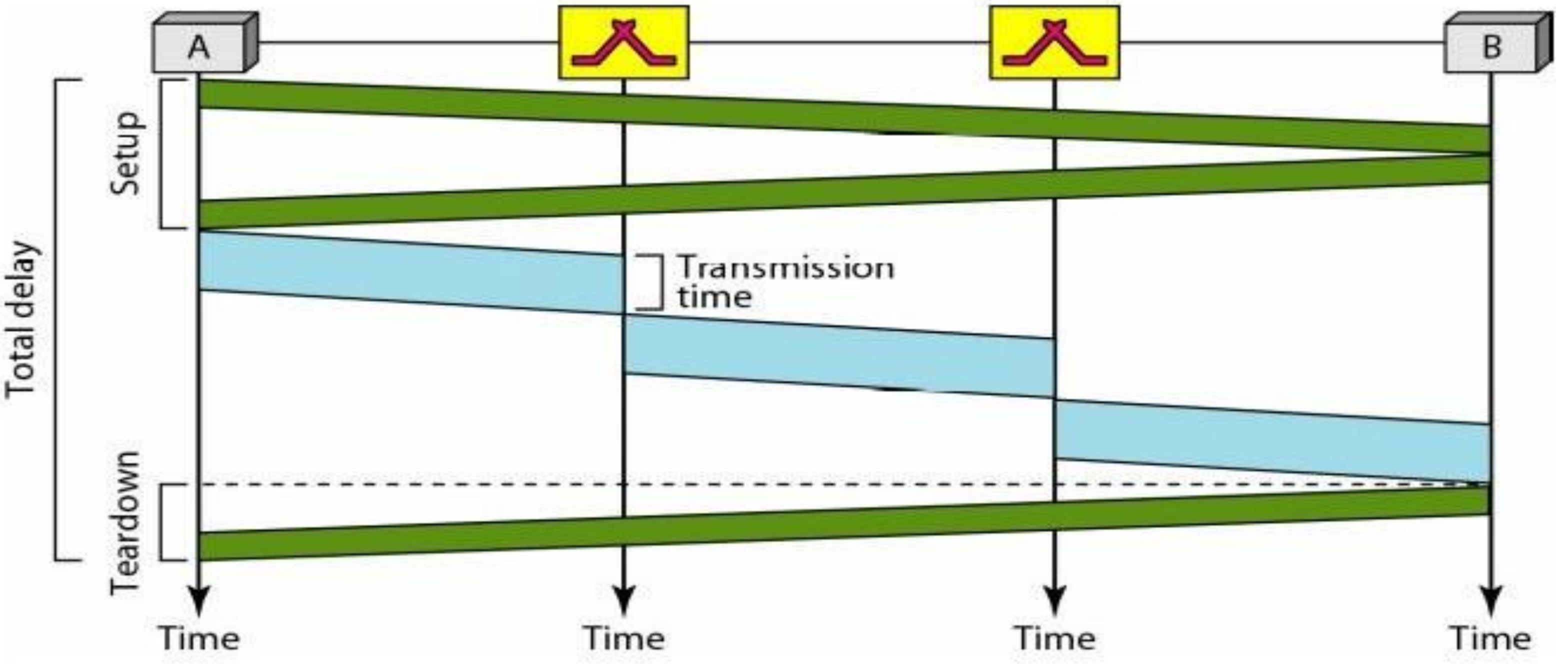


Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	66

Incoming		Outgoing	
Port	VCI	Port	VCI
2	22	3	77

Incoming		Outgoing	
Port	VCI	Port	VCI
1	66	2	22

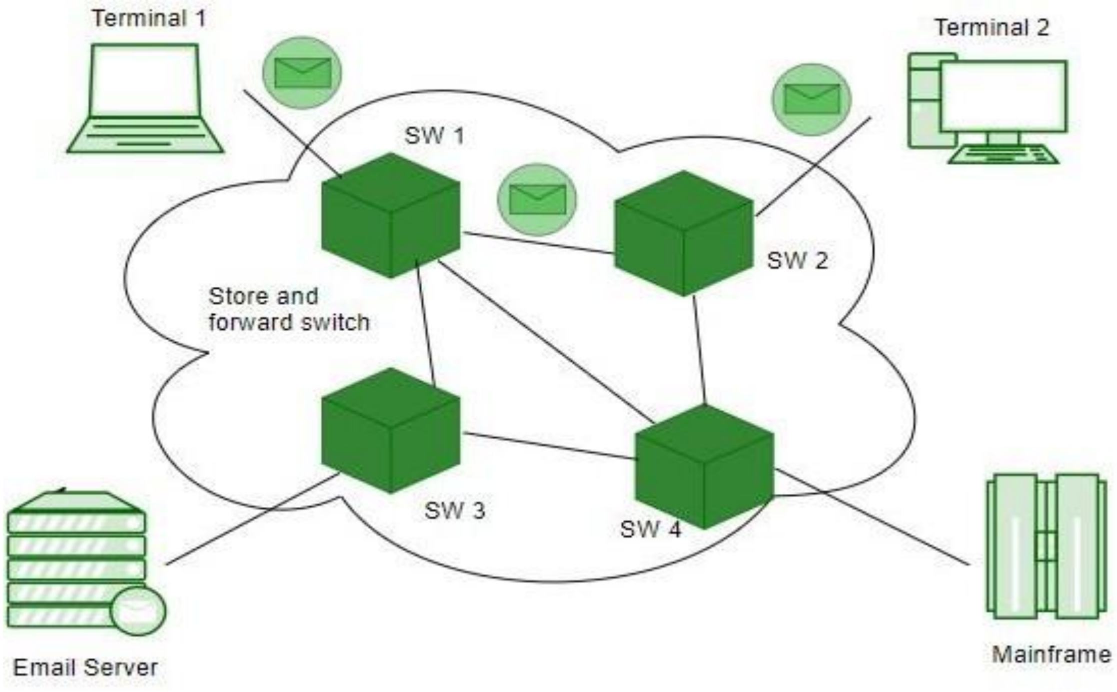
Delay



Message Switching

- Message switching is a network switching technique in which data is routed in its entirety from the source node to the destination node, one hope at a time.
- During message routing, every intermediate switch in the network stores the whole message.
- If the entire network's resources are engaged or the network becomes blocked, the message-switched network stores and delays the message until ample resources become available for effective transmission of the message.
- Before the advancements in packet switching, message switching acted as an efficient substitute for circuit switching.
- Message switching has largely been replaced by packet switching, but the technique is still employed in ad hoc sensor networks, military networks and satellite communications networks.
- In message switching, the source and destination nodes are not directly connected.
- Instead, the intermediary nodes (mainly switches) are responsible for transferring the message from one node to the next
- Thus, every intermediary node inside the network needs to store every message prior to transferring the messages one-by-one as adequate resources become available.
- If the resources are not available, the messages are stored indefinitely. This characteristic is known as store and forward.
- Every message should include a header, which typically consists of routing information, such as the source and destination, expiry time, priority level, etc.

Message Switching


Terminal 1
Terminal 2
SW 1
SW 2
Store and forward switch
SW 3
SW 4
Email Server
Mainframe