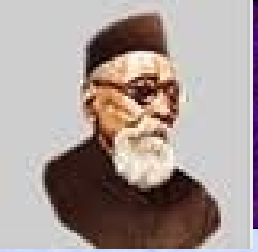


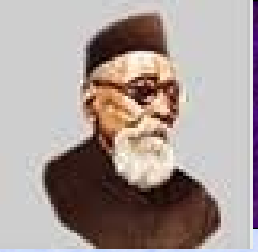
UNIT 1

Subject teacher

Prof. Suruchi W. Kitey

Computer Engineering Department

CCOEW Nagpur



Data

- Computer data is information processed or stored by a computer. This information may be in the form of text documents, images, audio clips, software programs, or other types of data.
- computer data is a bunch of ones and zeros, known as **binary** data. Because all computer data is in binary format, it can be created, processed, saved, and stored **digitally.**
- This allows data to be transferred from one computer to another using a network connection or various media devices.
- Data can be analog or digital. The term analog data refers to information that is continuous; digital data refers to information that has discrete states.

Signal

- A **signal** is an electrical or electromagnetic current that is used for carrying data from one device or **network** to another.

Bandwidth

- The maximum amount of data transmitted over an internet connection in a given amount of time.
- Bandwidth is often mistaken for internet speed when it's actually the volume of information that can be sent over a connection in a measured amount of time – calculated in megabits per second (Mbps).

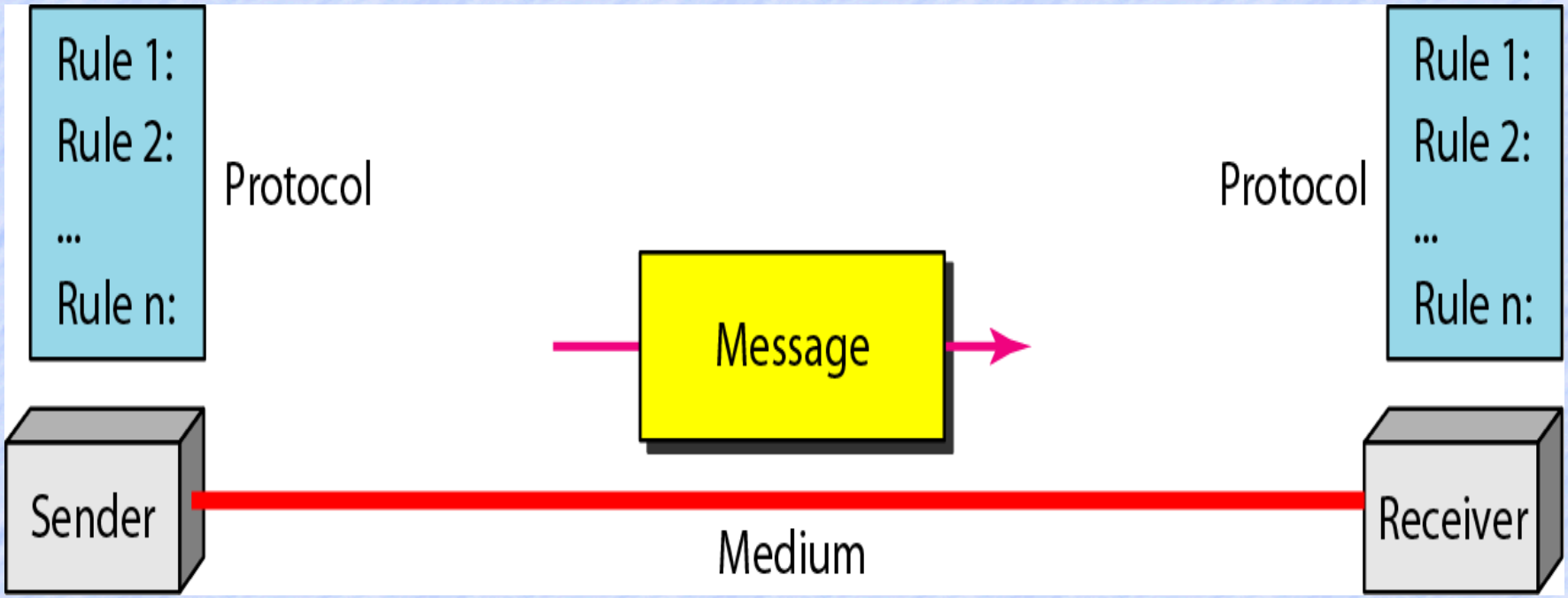
DATA COMMUNICATIONS

The term telecommunication means communication at a distance.

The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data.

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable or wireless.

Components of a data communication system



Components of a data communication system

The five components are :

1. Message - It is the information to be communicated. Popular forms of information include text, pictures, audio, video etc. Text is converted to binary, image is converted to pixels, etc.

2. Sender - It is the device which sends the data messages. It can be a computer, workstation, telephone handset etc.

3. Receiver - It is the device which receives the data messages. It can be a computer, workstation, telephone handset etc.

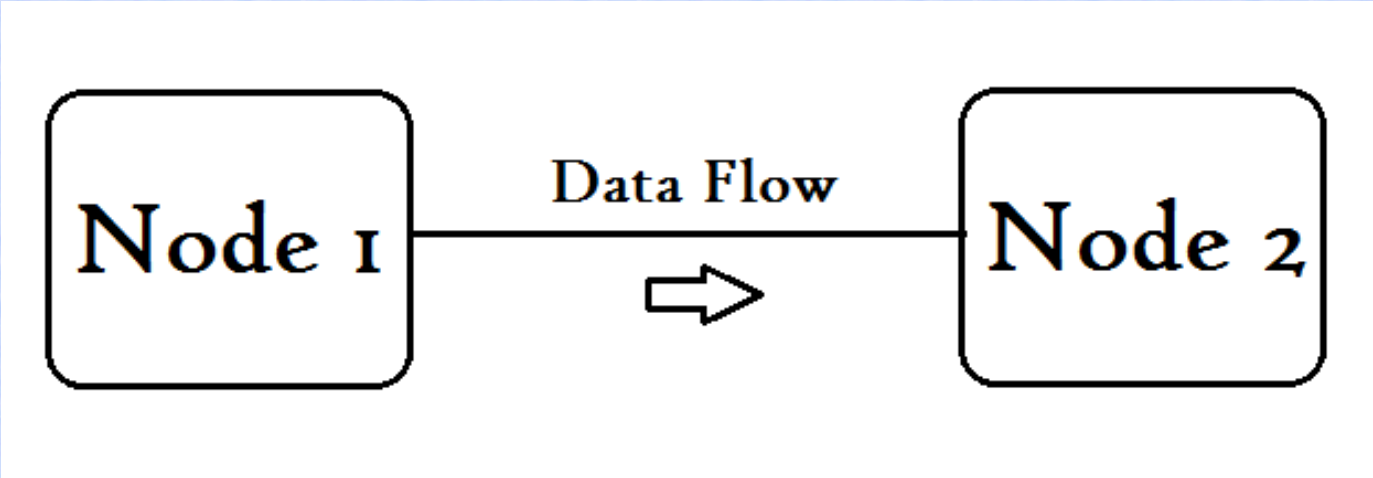
4. **Transmission Medium -** It is the physical path by which a message travels from sender to receiver. Some examples include twisted-pair wire, coaxial cable, radio waves etc.

5. Protocol - It is a set of rules that governs the data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating.

Data flow

Simplex

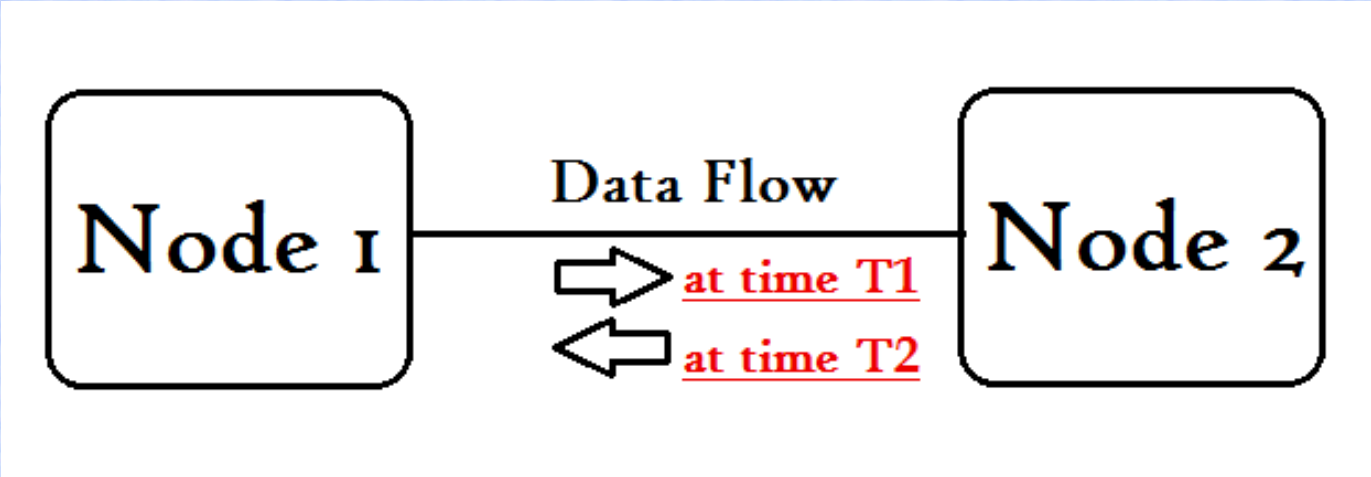
Only one of the two connected devices can transmit. The other device can only receive. The entire channel capacity is consumed to send data in one direction only.



- For example, the data flow between a remote control and television where the remote control is transmitter and television is the receiver.
- Here, data flows in one direction only from the remote control to the television.
- Another example is a keyboard and a monitor. The keyboard is sender and monitor is the receiver

Half duplex

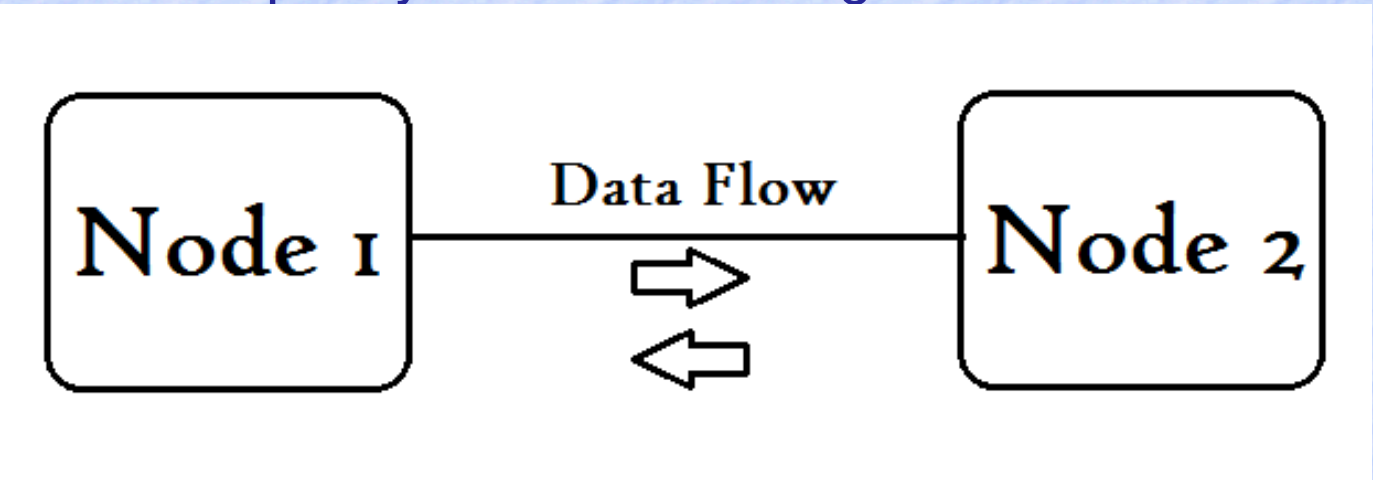
- Only one of the two connected devices can transmit at a time. Here, both devices are transmitter and receiver, but they cannot transmit and receive simultaneously.
- The entire capacity of the channel is utilized for one-directional data movement at a time.



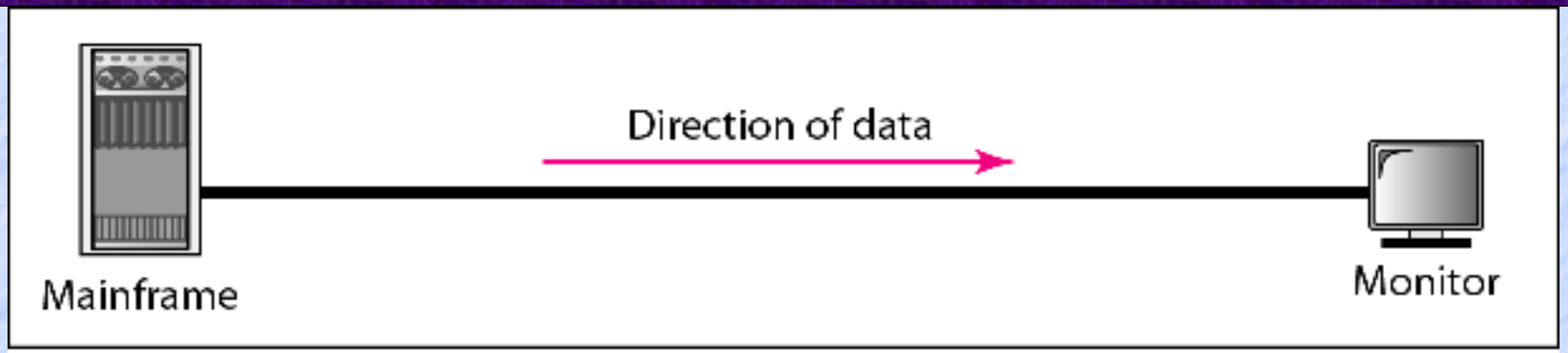
- example, the data flow in a walkie-talkie set

Full duplex

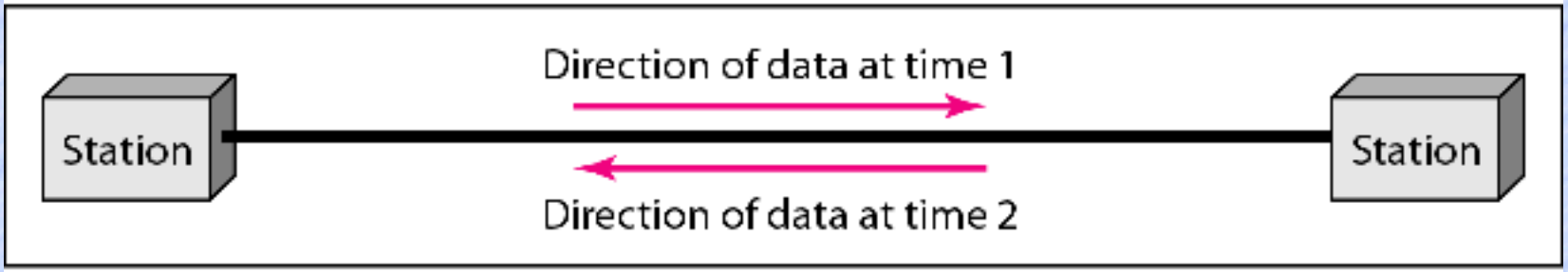
- Both of the two connected devices can transmit and receive at the same time.
- Here, both devices are transmitter and receiver, and they can transmit and receive simultaneously.
- The channel capacity is shared among two directions.



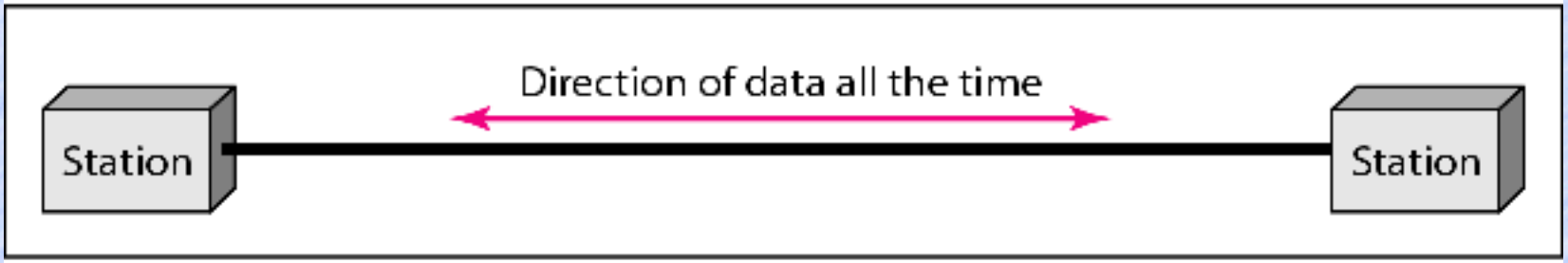
- For example, the data flow in a telephone where both parties can speak and listen simultaneously



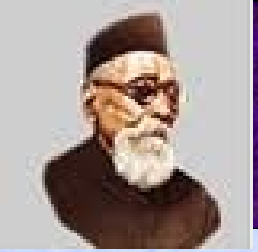
a. Simplex



b. Half-duplex

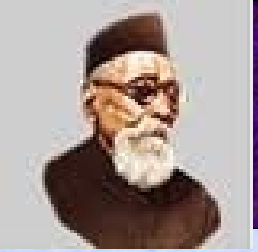


c. Full-duplex



NETWORKS

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

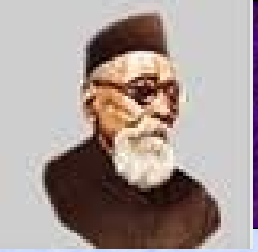


Network Criteria

A network must be able to meet certain number of criteria. The most important are Performance, Reliability and Security.

1) Performance:

- Can be measured by transit time and response time.
- Transit time is the amount of time required for a message to travel from one device to another.
- Response time is the elapsed time between an inquiry and a response.
- The performance of a network depends on the number of users, the type of transmission medium, the capacities of the connected hardware and the efficiency of the software.

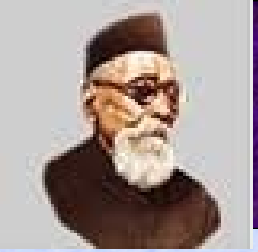


2) Reliability:

- Is measured by the frequency of failures, the time it takes a link to recover from failure and the network robustness in a adversity.

3) Security:

- This refers to the ability to protect data from unauthorized access.



Physical Structure

Type of Connection

For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections:

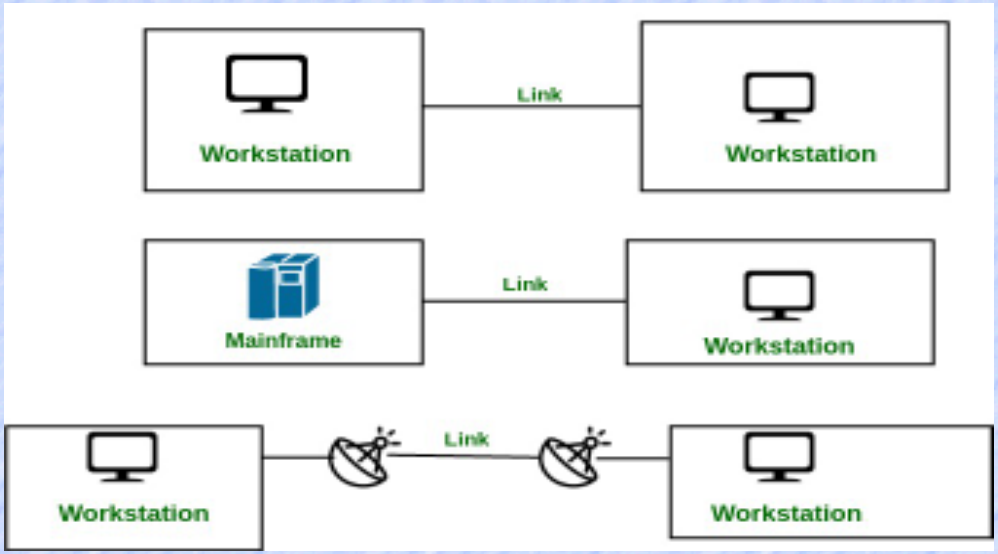
1. **Point-to-Point Connection**
2. **Multipoint Connection**

1) Point-to-Point Connection

- A point-to-point connection provides a dedicated link between two devices.
- The entire capacity of the link is reserved for transmission between those two devices.

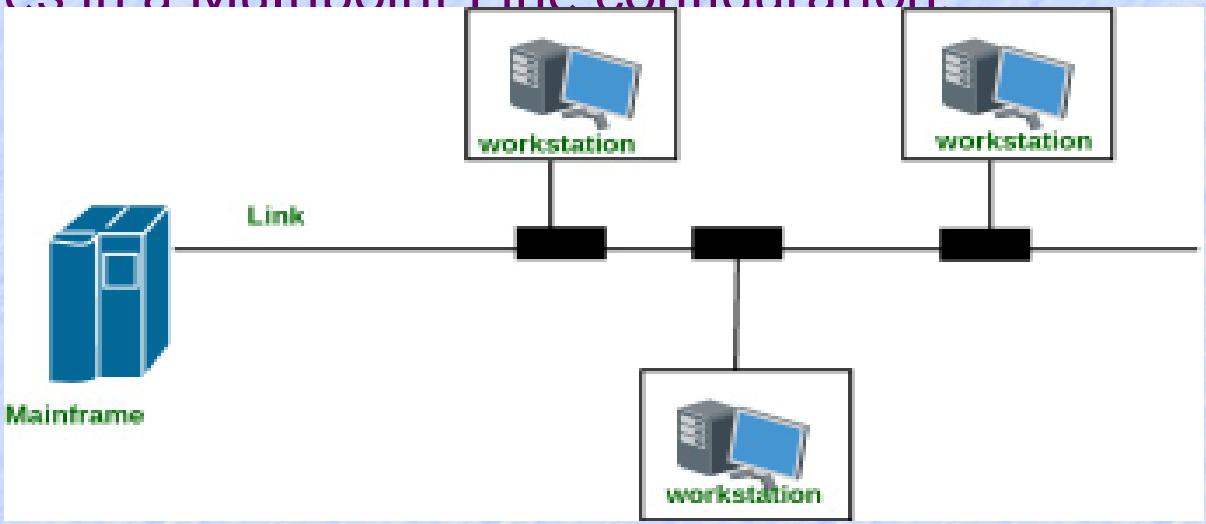
- Most point-to-point connections use a actual length of wire or cable to connect the two end, but other options such as microwave or satellite links are also possible.
- It is also the simplest to establish and understand.

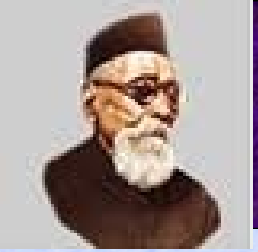
Example: Point-to-Point connection between remote control and Television for changing the channels.



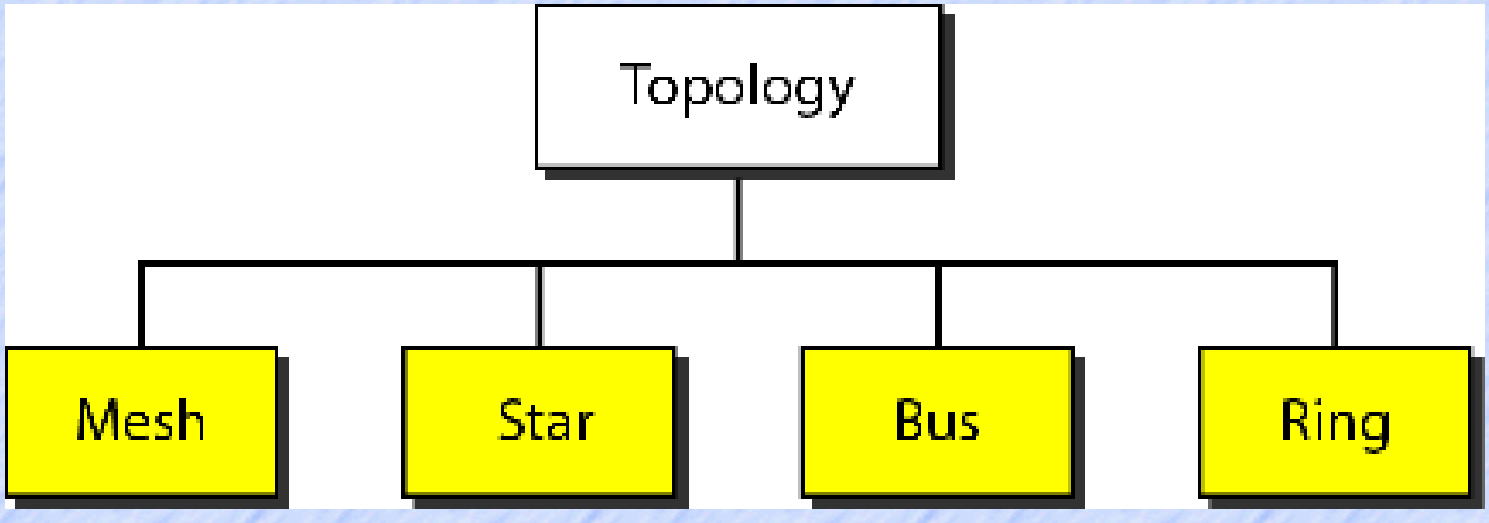
2) Multipoint Connection

- It is also called Multidrop configuration. In this connection two or more devices share a single link.
- More than two devices share the link that is the capacity of the channel is shared now. With shared capacity, there can be two possibilities in a Multipoint Line configuration:



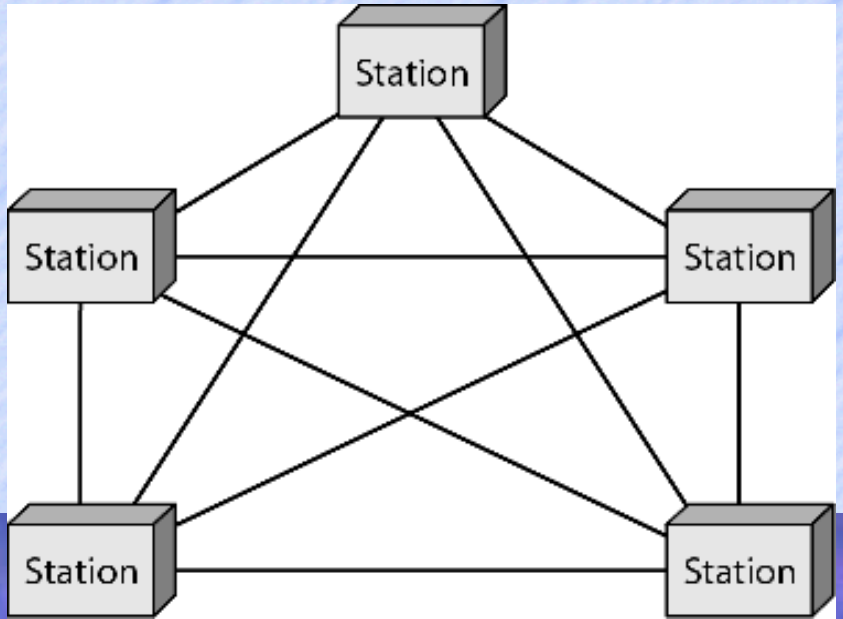


Categories of topology



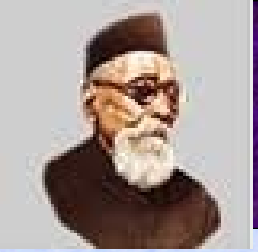
Mesh Topology

- In mesh topology each device is connected to every other device on the network through a dedicated point-to-point link.
- When we say dedicated it means that the link only carries data for the two connected devices only.
- Lets say we have n devices in the network then each device must be connected with (n-1) devices of the network.
- Number of links in a mesh topology of n devices would be n(n-1)/2.



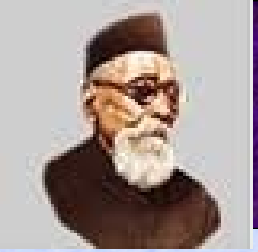
Advantages of Mesh topology

- No data traffic issues as there is a dedicated link between two devices which means the link is only available for those two devices.
- Mesh topology is reliable and robust as failure of one link doesn't affect other links and the communication between other devices on the network.
- Mesh topology is secure because there is a point to point link thus unauthorized access is not possible.
- Fault detection is easy.



Disadvantages of Mesh topology

- Amount of wires required to connected each system is tedious and headache.
- Since each device needs to be connected with other devices, number of I/O ports required must be huge.
- Scalability issues because a device cannot be connected with large number of devices with a dedicated point to point link. scalable

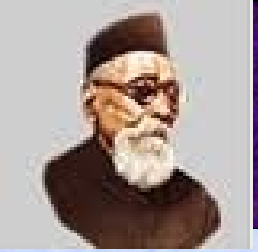


Star Topology

- In star topology each device in the network is connected to a central device called hub.
- Unlike Mesh topology, star topology doesn't allow direct communication between devices, a device must have to communicate through hub.
- If one device wants to send data to other device, it has to first send the data to hub and then the hub transmit that data to the designated device.

Advantages of Star topology

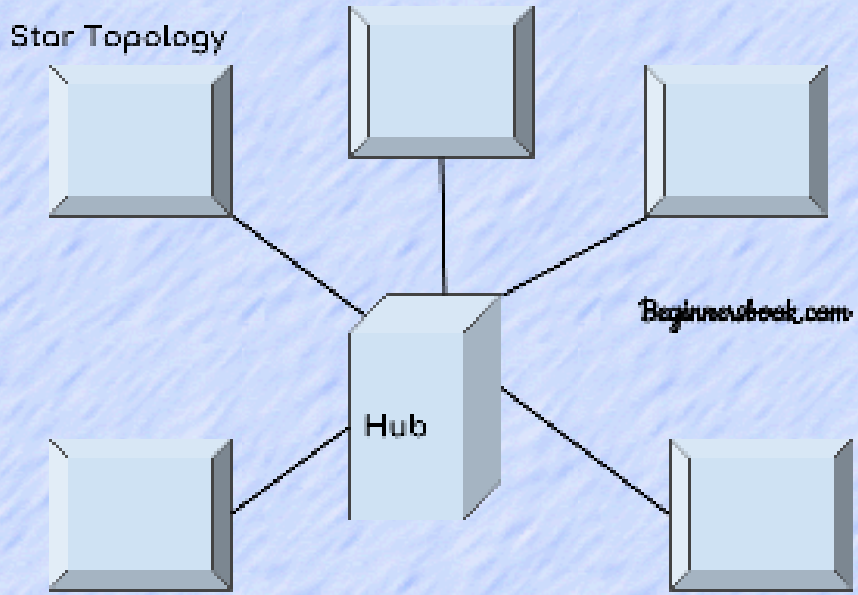
1. Less expensive because each device only need one I/O port and needs to be connected with hub with one link.

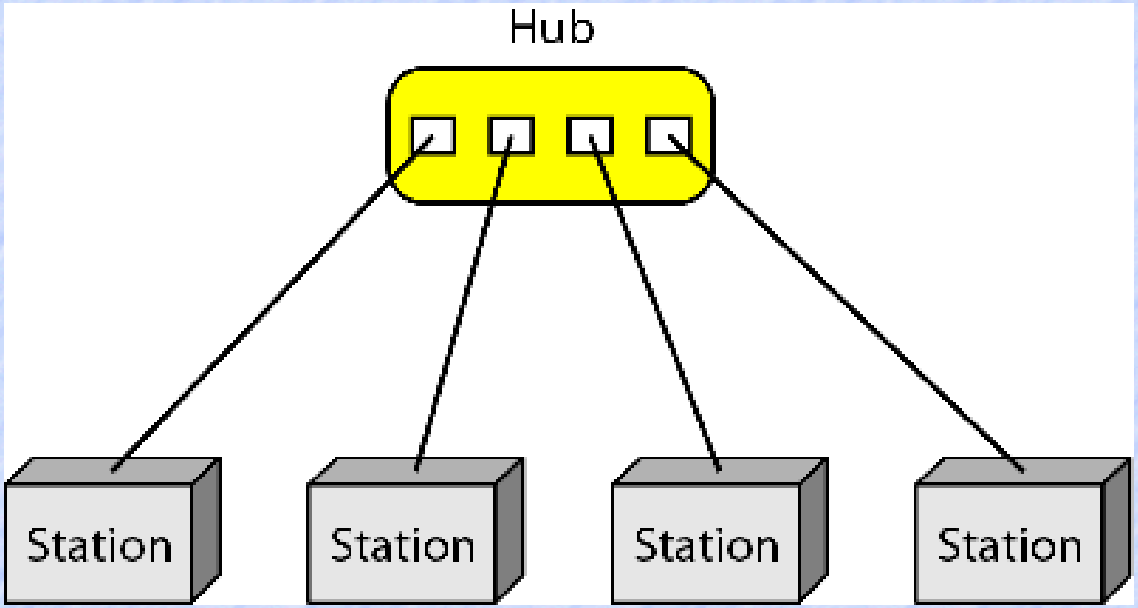


2. Easier to install
3. Less amount of cables required because each device needs to be connected with the hub only.
4. Robust, if one link fails, other links will work just fine.
5. Easy fault detection because the link can be easily identified.

Disadvantages of Star topology

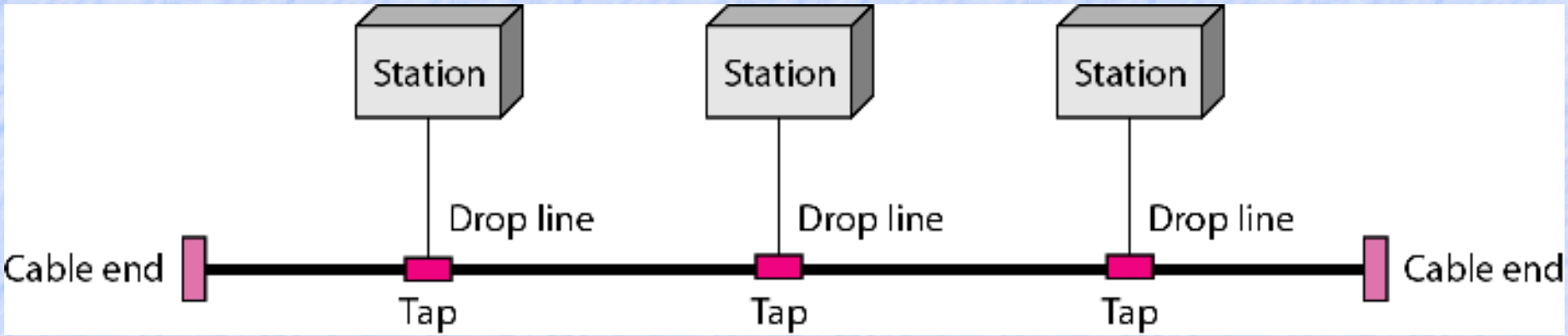
1. If hub goes down everything goes down, none of the devices can work without hub.
2. Hub requires more resources and regular maintenance because it is the central system of star topology.


Stor Topology
Hub


Hub
Station
Station
Station
Station

Bus Topology

- In bus topology there is a main cable and all the devices are connected to this main cable through drop lines.
- There is a device called tap that connects the drop line to the main cable. Since all the data is transmitted over the main cable, there is a limit of drop lines and the distance a main cable can have.



Advantages of bus topology

1. Easy installation, each cable needs to be connected with backbone cable.
2. Less cables required than Mesh and star topology

Disadvantages of bus topology

1. Difficultly in fault detection.
2. Not scalable as there is a limit of how many nodes you can connect with backbone cable.

Ring topology

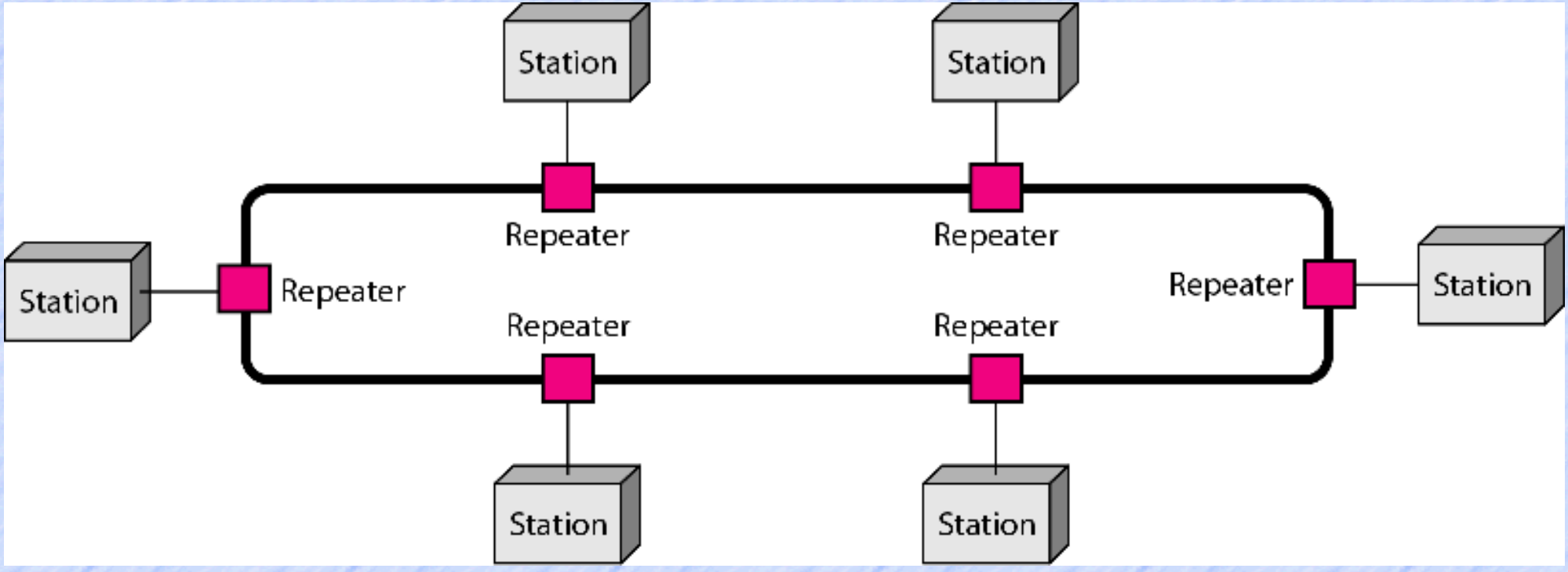
- In ring topology each device is connected with the two devices on either side of it.
- There are two dedicated point to point links a device has with the devices on the either side of it.
- This structure forms a ring thus it is known as ring topology.
- If a device wants to send data to another device then it sends the data in one direction, each device in ring topology has a repeater, if the received data is intended for other device then repeater forwards this data until the intended device receives it.

Advantages of Ring Topology

1. Easy to install.
2. Managing is easier as to add or remove a device from the topology only two links are required to be changed.

Disadvantages of Ring Topology

1. A link failure can fail the entire network as the signal will not travel forward due to failure.
2. Data traffic issues, since all the data is circulating in a ring.


Station
Station
Repeater
Repeater
Station
Repeater
Repeater
Repeater
Repeater
Station
Station
Station

Hybrid topology

- A combination of two or more topology is known as hybrid topology. For example a combination of star and mesh topology is known as hybrid topology.

Advantages of Hybrid topology

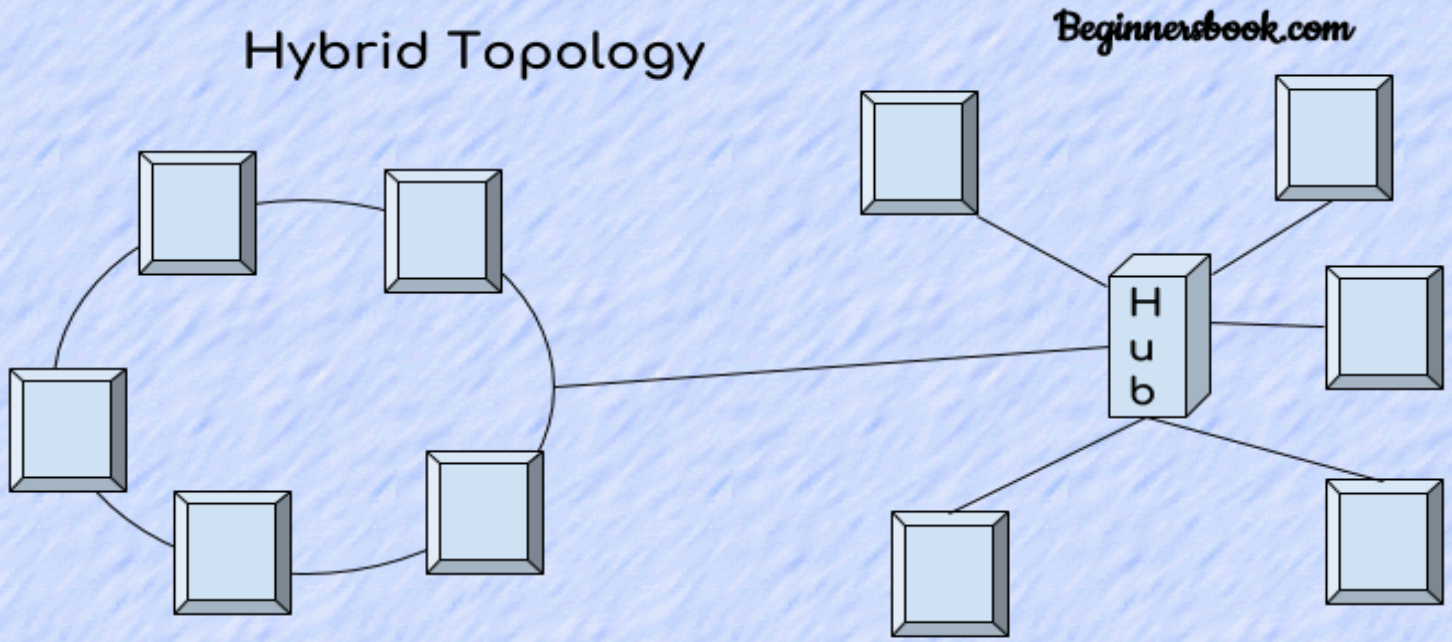
1. We can choose the topology based on the requirement for example, scalability is our concern then we can use star topology instead of bus technology.

2. Scalable as we can further connect other computer networks with the existing networks with different topologies.

.

Disadvantages of Hybrid topology

1. Fault detection is difficult.
2. Installation is difficult.
3. Design is complex so maintenance is high thus expensive



Categories of network

Local **A**rea **N**etwork (LAN)

- A **L**ocal **A**rea **N**etwork (LAN) is a group of computer and peripheral devices which are connected in a limited area such as school, laboratory, home, and office building.
- It is a widely useful network for sharing resources like files, printers, games, and other application.
- The simplest type of LAN network is to connect computers and a printer in someone's home or office.
- In general, LAN will be used as one type of transmission medium.

Characteristics of LAN

• It is a private network, so an outside regulatory body never controls it.
• LAN operates at a relatively higher speed compared to other WAN systems.

Advantages of LAN

• Computer resources like hard-disks, DVD-ROM, and printers can share local area networks. This significantly reduces the cost of hardware purchases.

• You can use the same software over the network instead of purchasing the licensed software for each client in the network.

- Data of all network users can be stored on a single hard disk of the server computer.

- You can easily transfer data and messages over networked computers.

- It will be easy to manage data at only one place, which makes data more secure.

- Local Area Network offers the facility to share a single internet connection among all the LAN users.

Disadvantages of LAN

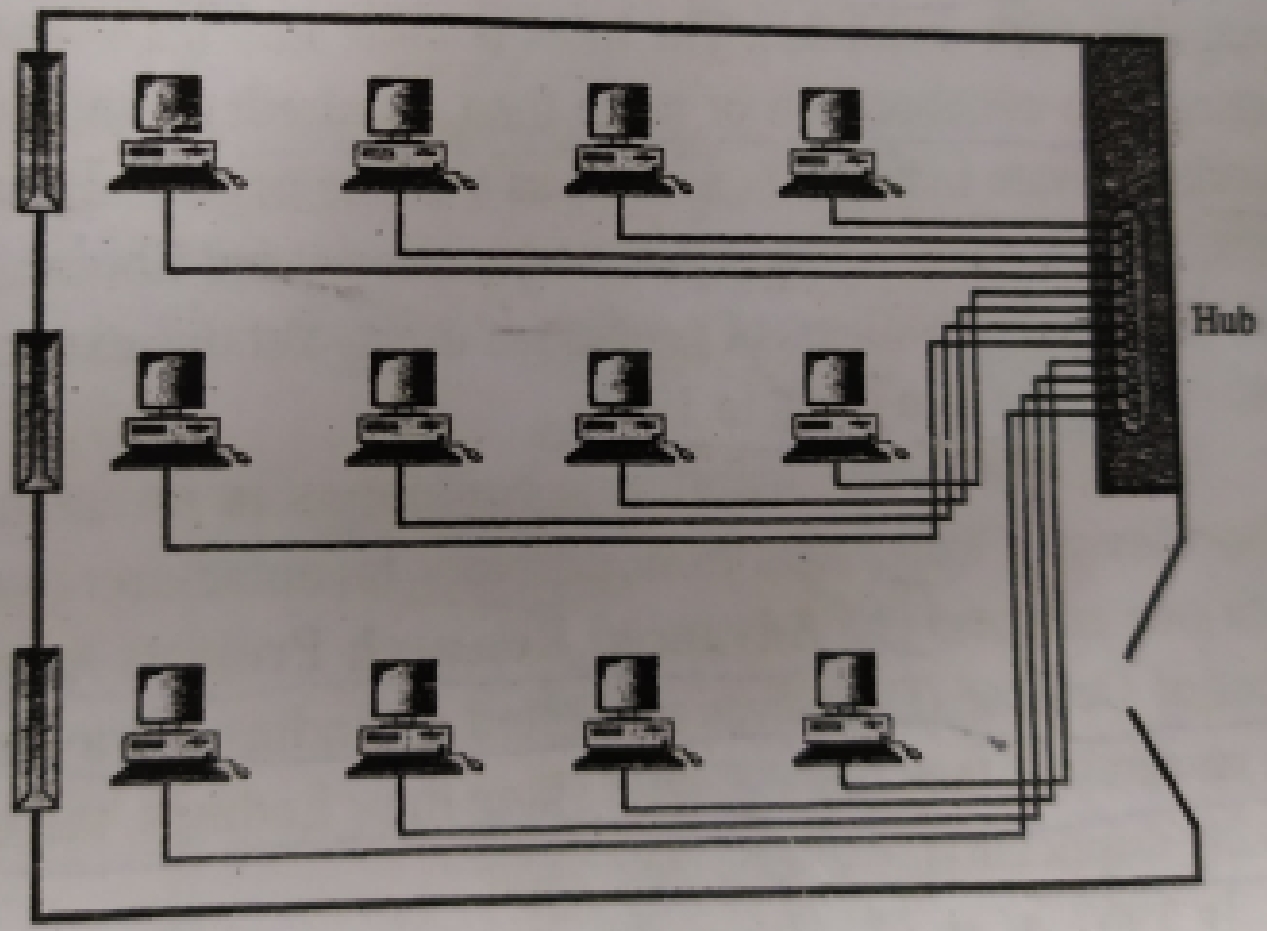
- LAN will indeed save cost because of shared computer resources, but the initial cost of installing Local Area Networks is quite high.

- The LAN admin can check personal data files of every LAN user, so it does not offer good privacy.

- Unauthorized users can access critical data of an organization in case LAN admin is not able to secure centralized data repository.

- Local Area Network requires a constant LAN administration as there are issues related to software setup and hardware failures

Figure 1.10 *An isolated LAN connecting 12 computers to a hub in a closet*



WAN (Wide Area Network)

- WAN provides long distance transmission of data, image, audio and video information over large geographic areas that may include a country, a continent, or even the whole world
- WAN can be as complex as the backbones that connect the internet or as simple as a dial-up line that connects a home computer to the internet
- we normally refer to the first as a switched WAN and to the second as a point-to-point WAN
- the switched WAN connects the end systems, which usually include a router(internet working connecting device) that connects to another LAN or WAN

- The point-to point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an internet service provider(ISP).

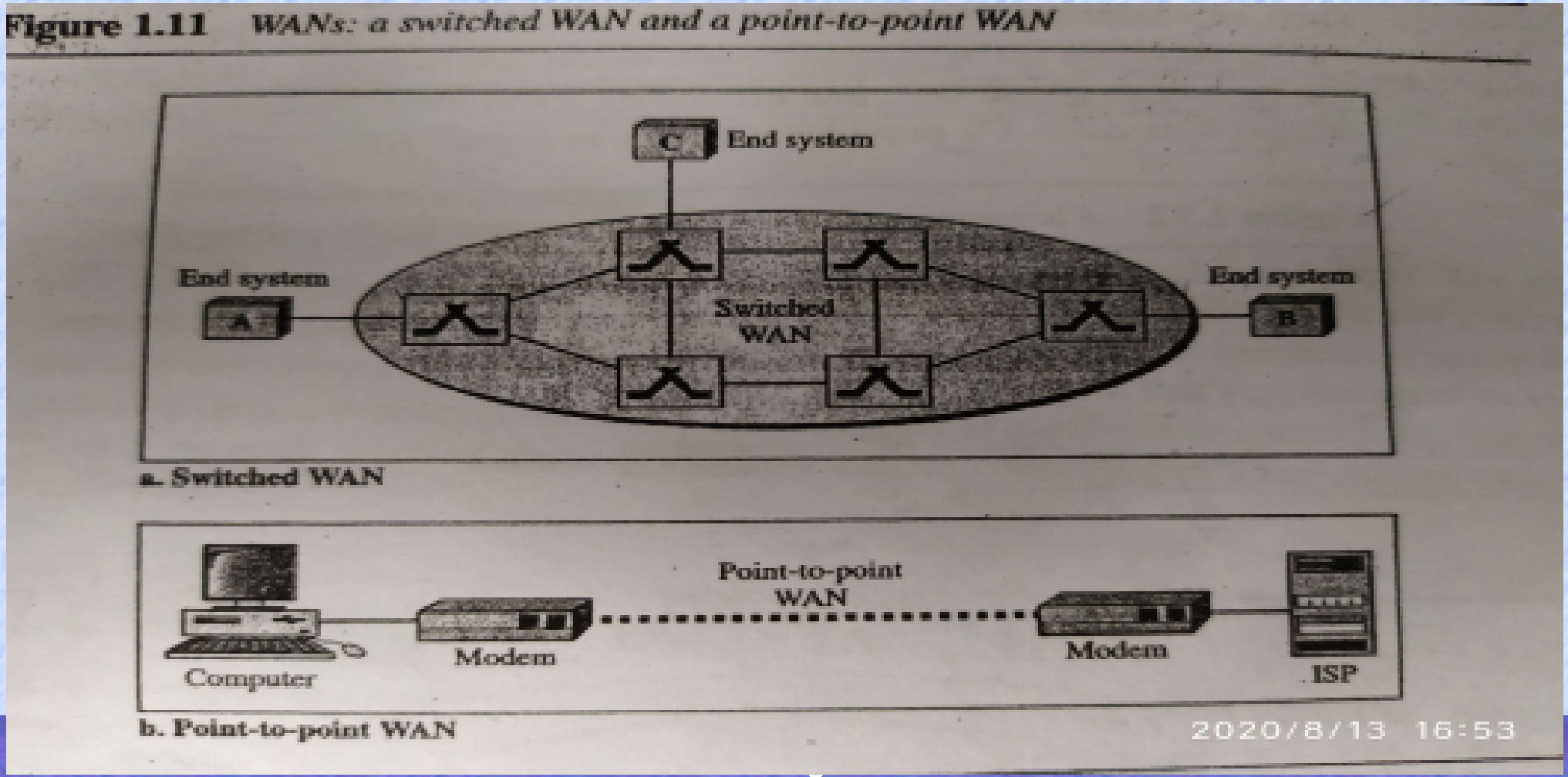


Figure 1.11 *WANs: a switched WAN and a point-to-point WAN*

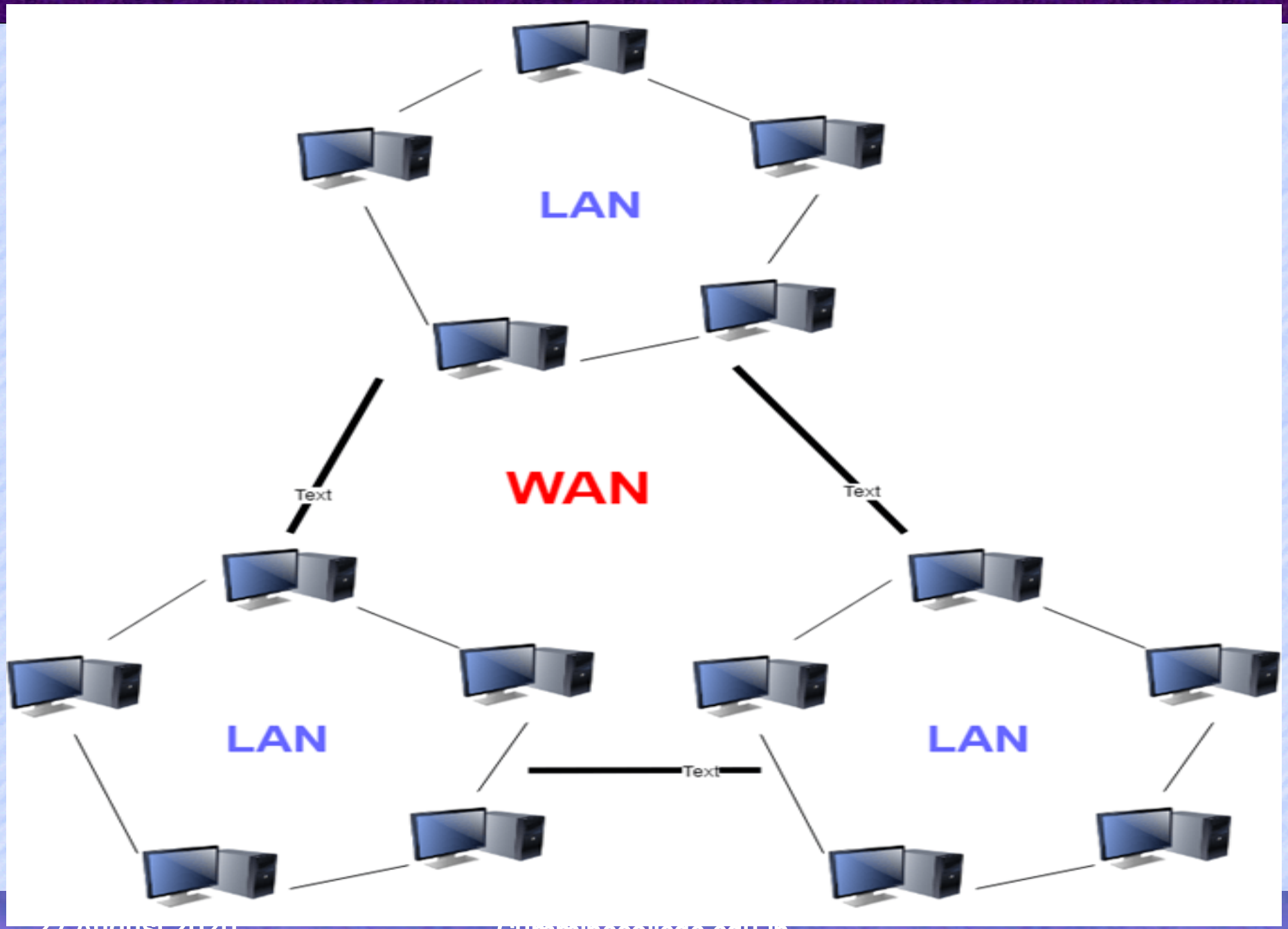
Disadvantage of WAN

- The initial setup cost of investment is very high.

- It is difficult to maintain the WAN network. You need skilled technicians and network administrators.

- There are more errors and issues because of the wide coverage and the use of different technologies.

- It requires more time to resolve issues because of the involvement of multiple wired and wireless technologies.


LAN
WAN
Text
Text
LAN
LAN
Text

Metropolitan Area Network or MAN

- MAN is a network with a size between a LAN and a WAN.
- It normally covers the area inside a town or a city
- It is designed for customers who need a high-speed connectivity, normally to the internet, and have endpoints spread over a city or part of city.
- a good example of a MAN is the part of the telephone company n/w that can provide a high-speed DSL line to the customer.
- Another example is the cable TV n/w that originally designed for cable TV, but today can also be used for high speed data connection to the internet.

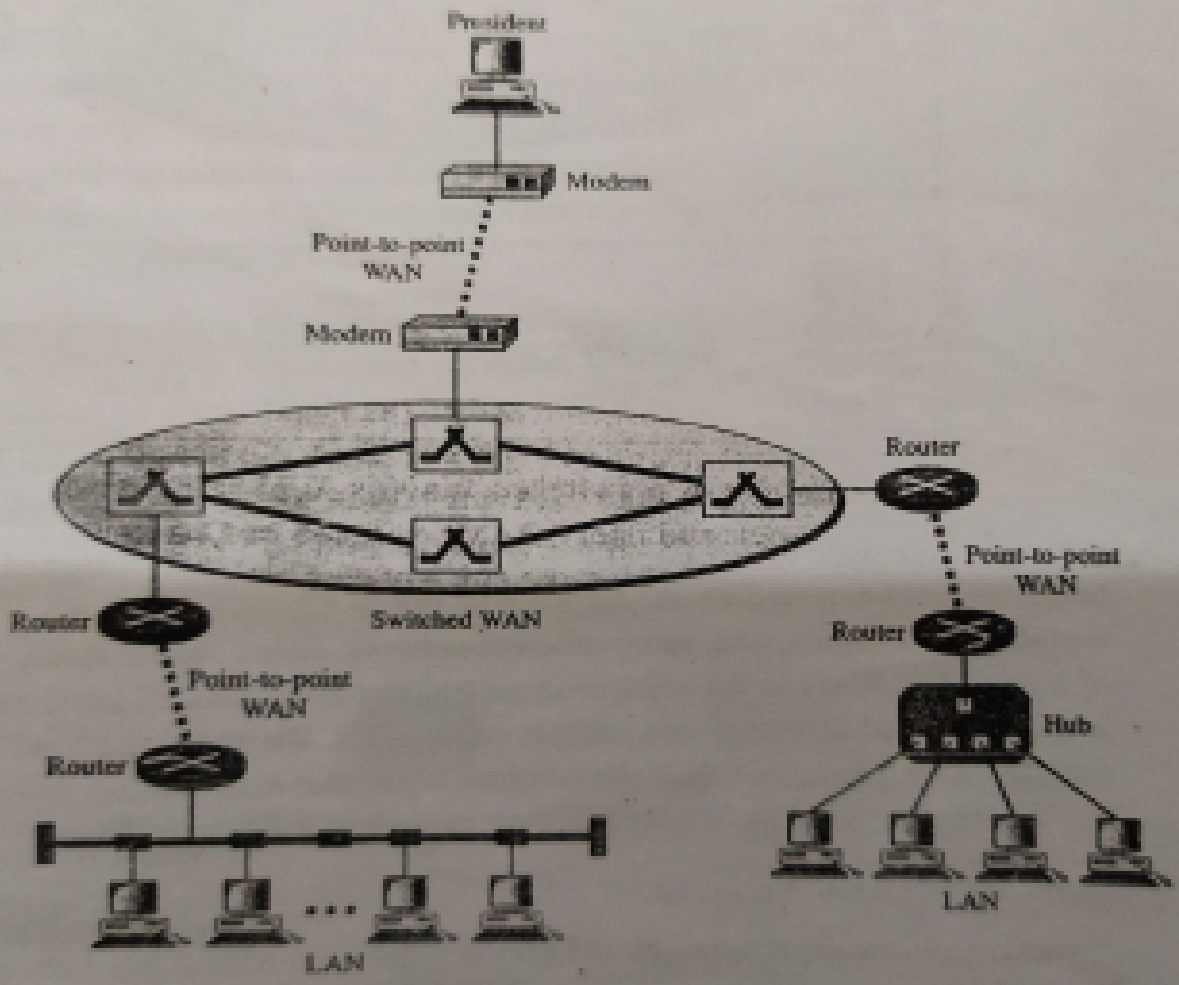
- It mostly covers towns and cities in a maximum 50 km range
- Mostly used medium is optical fibers, cables
- You need more cable to establish MAN connection from one place to another.

Interconnection of networks

- Today, it is very rare to see LAN,MAN in isolation, they are connected to one another
- When two or more networks are connected, they become an internetwork, or internet
- As an example, assume that an organization has two offices, one on the east coast and the other on the west coast.
- The established office on the west coast has a bus topology LAN, the newly opened office on the east cost has a star topology LAN.
- The president of the company lives somewhere in the middle and needs to have control over the company from her home

- To create a backbone WAN for connecting these three entities(two LANs and the president's computer),a switched WAN has been leased.
- To connect the LANs to this switched WAN, however, three point-to-point WANs are required.
- These point-to-point WANs can be a high-speed DSL line offered by a telephone company or a cable modem line offered by a cable TV.

Figure 1.12 *A heterogeneous network made of four WANs and two LANs*



The internet

- The internet has transformed many aspects of our daily lives
- It has affected the way we do business as well as the way we spend our leisure time.
- You have sent electronic mail to a business associate, paid a utility bill, read a newspaper from a distant city, or looked up a local movie schedule-all by using the internet
- Or booked a appointment, chatted with a fellow trekkie or comparison-shopped for a car
- internet is a structured, organized system

Brief history

- An internet (small i) is two or more networks that can communicate with each other
- The most notable internet is called the Internet (uppercase letter I),a collaboration of more than hundreds of thousands of interconnected networks
- Private as well as government agencies, schools, corporations etc in more than 100 countries use the Internet.
- This extraordinary communication system came into being in 1969
- In 1960's research organizations were stand alone devices.

- The advanced research agency(ARPA) in the department of defence (DoD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of efforts

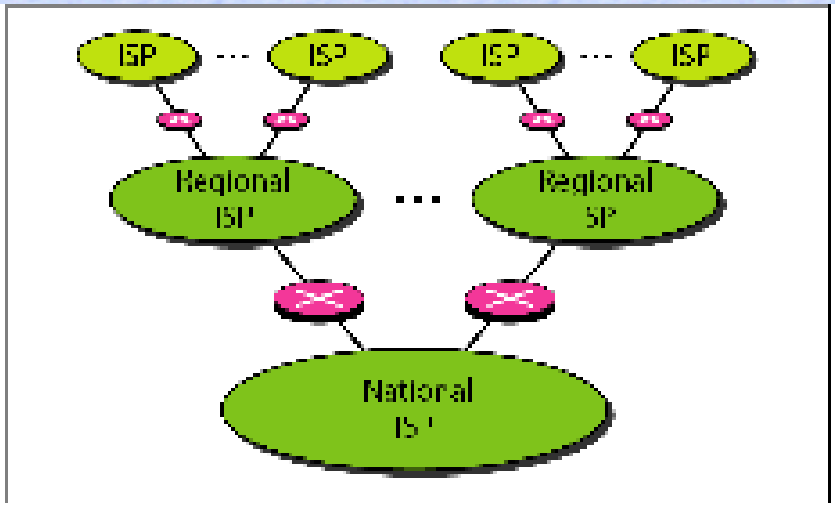
- In 1967's at an association for computing machinery(ACM) meeting, ARPA presented its ideas for ARPANET, a small network of connected computer

- The idea was that each host computer would be attached to a specialized computer, called an interface message processor(IMP)

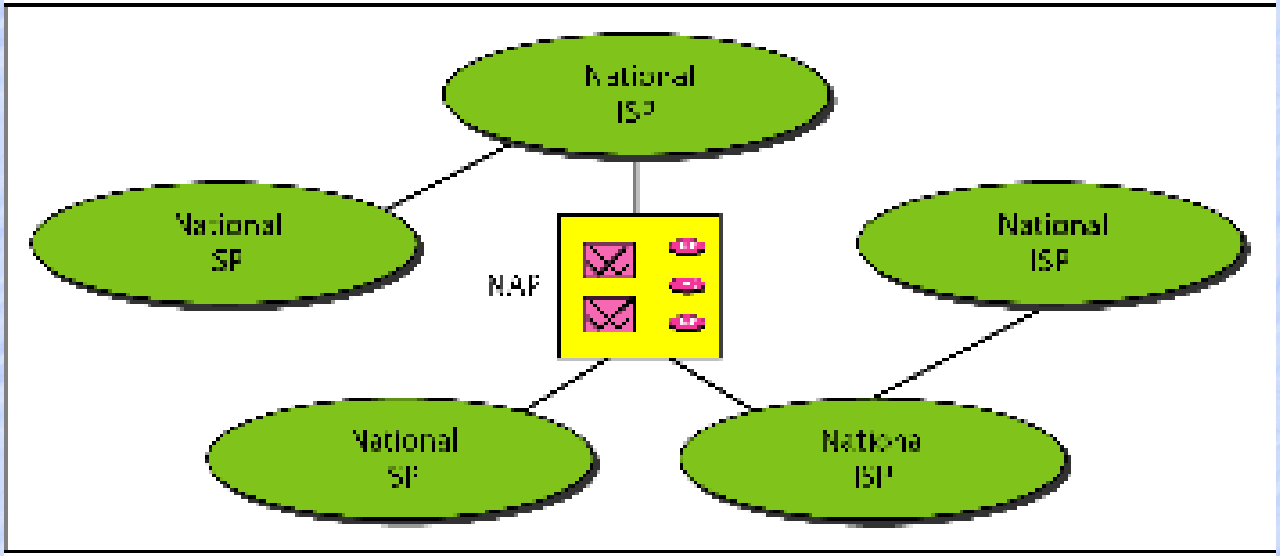
- The IMP's in tern, would be connected to one another. each IMP had to be able to communicate with other IMP;s as well as with its own attached host.

Internet Today

- Internet today is not a simple hierarchical structure.
- It is made up of many wide-and local area n/ws joined by connecting devices and switching stations.
- It is difficult to give accurate representation because it is continually changing-new n/w added
- End users who want Internet connection use the services of Internet service providers(ISPs).
- There are international service providers, national service providers, regional service providers and local service providers
- Internet today is run by private companies, not the government



a. Structure of a national ISP



b. Interconnection of national ISPs

International service providers

- At top of hierarchy are the international service providers that connects nations together

National Internet service providers

- Are the backbone n/w created and maintained by specialized companies
- To provide connectivity between the end users, these backbone networks are connected by complex switching stations called network access points(NAPs)
- Some NISP n/ws are also connected to one another by private switching stations called peering points

Regional Internet service providers

- Regional ISP are smaller ISP that are connected to one or more national ISP
- Third level of the hierarchy with a smaller data rate

Local Internet service provider

- Provides direct service to the end users. local ISP can be a company that just provides internet services, a corporation with a n/w that supplies services to its own employees or nonprofit organization, such as college or a university, that runs its own network
- Each local ISP can be connected to a regional or national service provider.

PROTOCOLS

- *A protocol is synonymous with rule.*
- *It consists of a set of rules that govern data communications.*
- *It determines what is communicated, how it is communicated and when it is communicated.*
- *The key elements of a protocol are syntax, semantics and timing*

Elements of a Protocol

Syntax

- Structure or format of the data, meaning the order in which they are presented.
- For ex. Simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself

Semantics

- Interprets the meaning of the each section of bits
- It does an route identify the route to be taken
- Knows which fields define what action (how is the particular pattern to be interpreted, does an address identify the route to be taken)

Timing

- When data should be sent and how fast they can be sent
- For ex. If a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost

Standards

- Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunications technology and processes.
- Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications.
- Data communication standards fall into two categories: de facto (meaning "by fact" or "by convention") and de jure (meaning "by law" or "by regulation").

a.De facto:

- Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards.
- De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.

b.De jure:

- Those standards that have been established by an officially recognized body are de jure standards.

Standards creation committees

1) International Organization for Standardization (ISO)

2) Institute of Electrical and Electronics Engineers (IEEE)

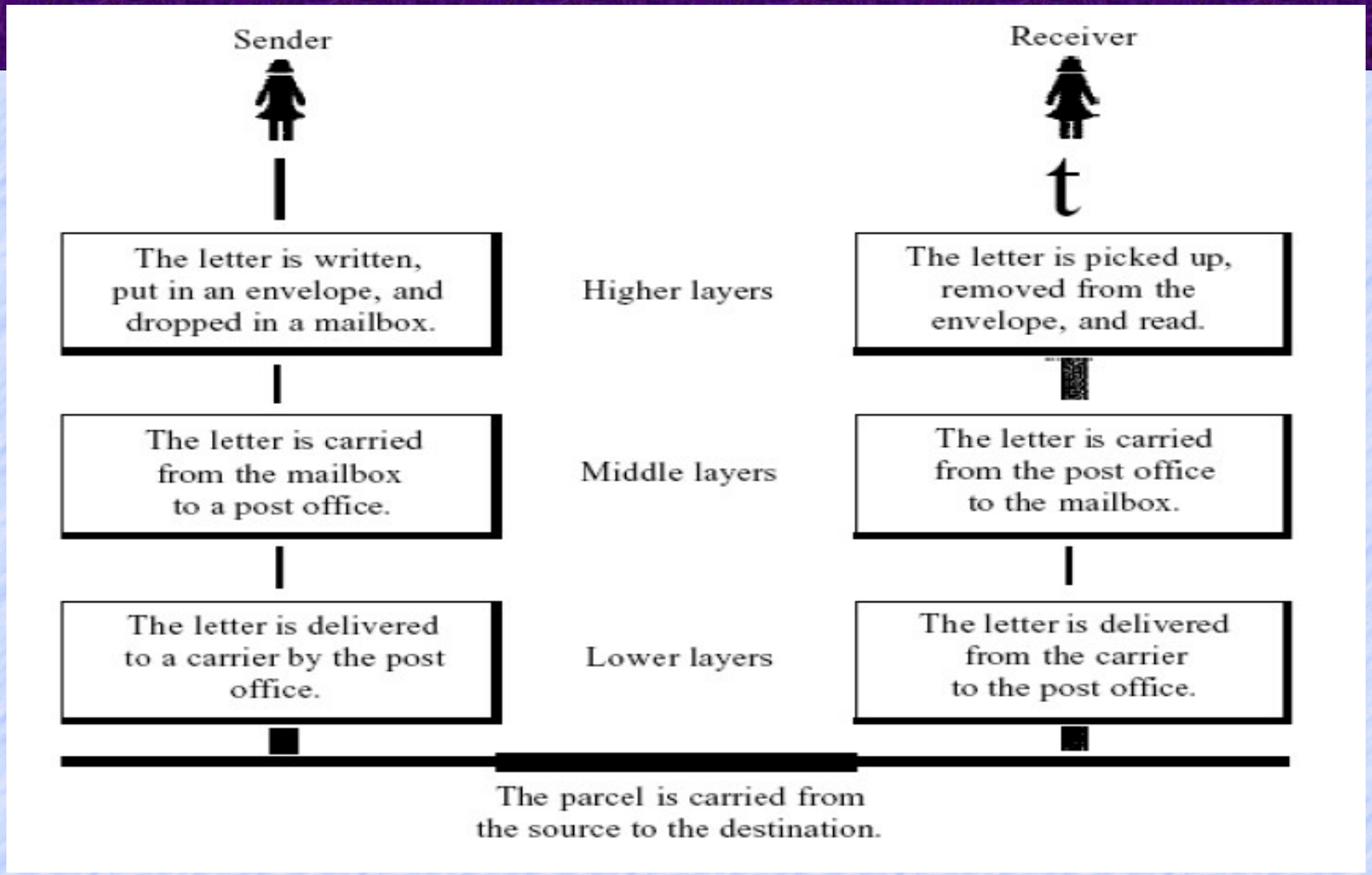
3) American National Standards Institute(ANSI)

4) Electronic industries association(EIA)

5) International telecommunication Union-Telecommunication standards sector(ITU-T)

Layered Tasks

- We use the concept of layers in our daily life.
- As an example, let us consider two friends who communicate through postal mail The process of sending a letter to a friend would be complex if there were no services available from the post office.
- Below Figure shows the steps in this task.



In Figure we have a sender, a receiver, and a carrier that transports the letter. There is a hierarchy of tasks.

At the Sender Site

The activities that take place at the sender site :

» **Higher layer** : The sender writes the letter, inserts the letter in an envelope, writes the sender and receiver addresses, and drops the letter in a mailbox.

» **Middle layer** : The letter is picked up by a letter carrier and delivered to the post office.

» **Lower layer** : The letter is sorted at the post office; a carrier transports the letter

On the Way

- The letter is then on its way to the recipient. On the way to the recipient's local post office, the letter may actually go through a central office.

- In addition, it may be transported by truck, train, airplane, boat, or a combination of these.

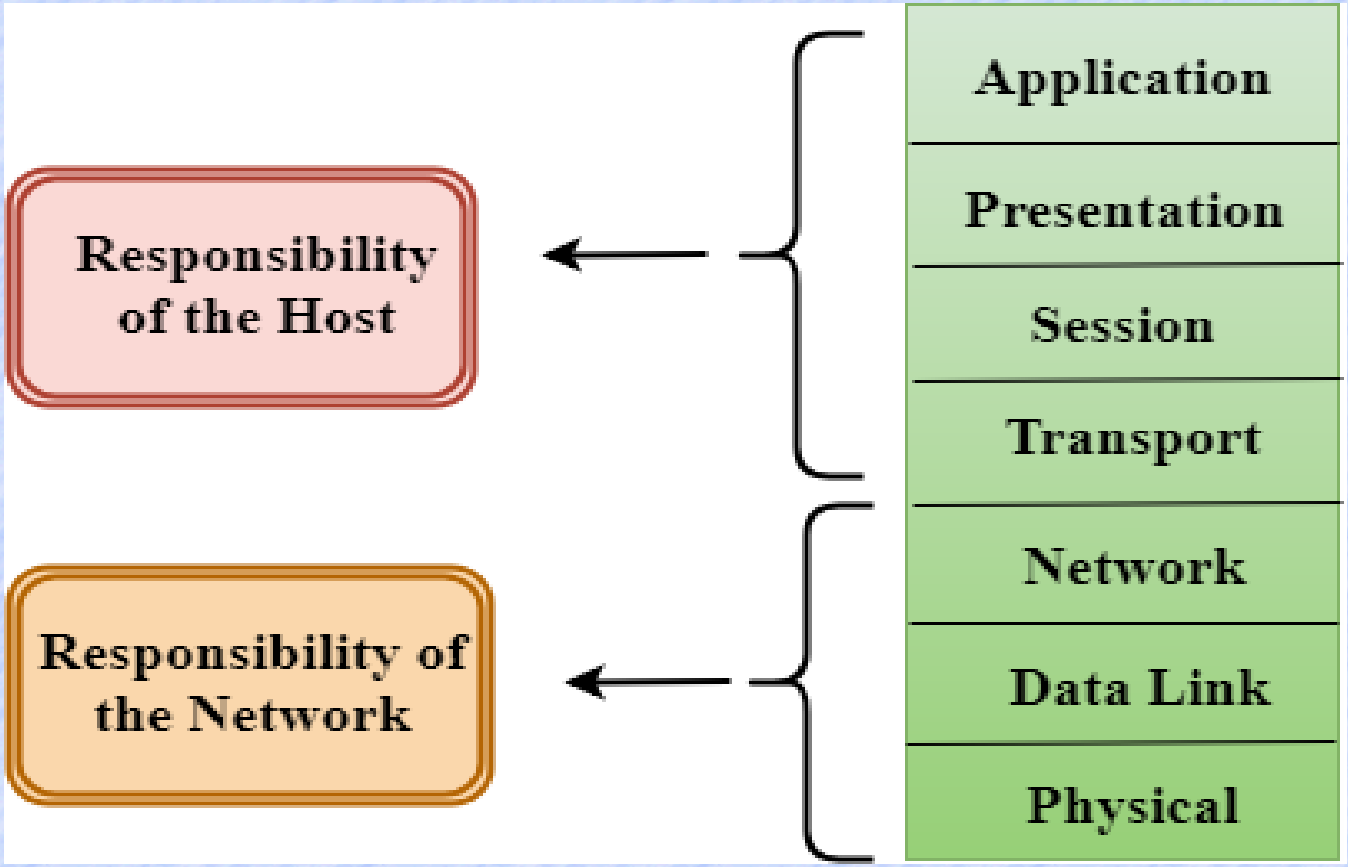
At the Receiver Site

» **Lower layer** : The carrier transports the letter to the post office.
» **Middle layer** : The letter is sorted and delivered to the recipient's mailbox.
» **Higher layer** : The receiver picks up the letter, opens the envelope, and reads it.

OSI 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-sufficient, so that task assigned to each layer can be performed independently



- The OSI model is divided into two layers: 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.

The Application Layer

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

The Presentation Layer

- This layer is primarily responsible for preparing data so that it can be used by the application layer; in other words, layer 6 makes the data presentable for applications to consume.
- The presentation layer is responsible for translation, encryption and compression of data.
- Two communicating devices communicating may be using different encoding methods, so layer 6 is responsible for translating incoming data into a syntax that the application layer of the receiving device can understand.

The Session Layer

- This is the layer responsible for opening and closing communication between the two devices.
- The time between when the communication is opened and closed is known as the session.
- The session layer ensures that the session stays open long enough to transfer all the data being exchanged, and then promptly closes the session in order to avoid wasting resources.

- The session layer also synchronizes data transfer with checkpoints.
- For example, if a 100 megabyte file is being transferred, the session layer could set a checkpoint every 5 megabytes.
- In the case of a disconnect or a crash after 52 megabytes have been transferred, the session could be resumed from the last checkpoint, meaning only 50 more megabytes of data need to be transferred.
- Without the checkpoints, the entire transfer would have to begin again from scratch.

The Transport Layer

- Layer 4 is responsible for end-to-end communication between the two devices.
- This includes taking data from the session layer and breaking it up into chunks called segments before sending it to layer 3.
- The transport layer on the receiving device is responsible for reassembling the segments into data the session layer can consume.
- The transport layer is also responsible for flow control and error control.

- Flow control determines an optimal speed of transmission to ensure that a sender with a fast connection doesn't overwhelm a receiver with a slow connection.

- The transport layer performs error control on the receiving end by ensuring that the data received is complete, and requesting a retransmission if it isn't.

The Network Layer

- The network layer is responsible for facilitating data transfer between two different networks.
- If the two devices communicating are on the same network, then the network layer is unnecessary.
- The network layer breaks up segments from the transport layer into smaller units, called packets, on the sender's device, and reassembling these packets on the receiving device.
- The network layer also finds the best physical path for the data to reach its destination; this is known as routing

The Data Link Layer

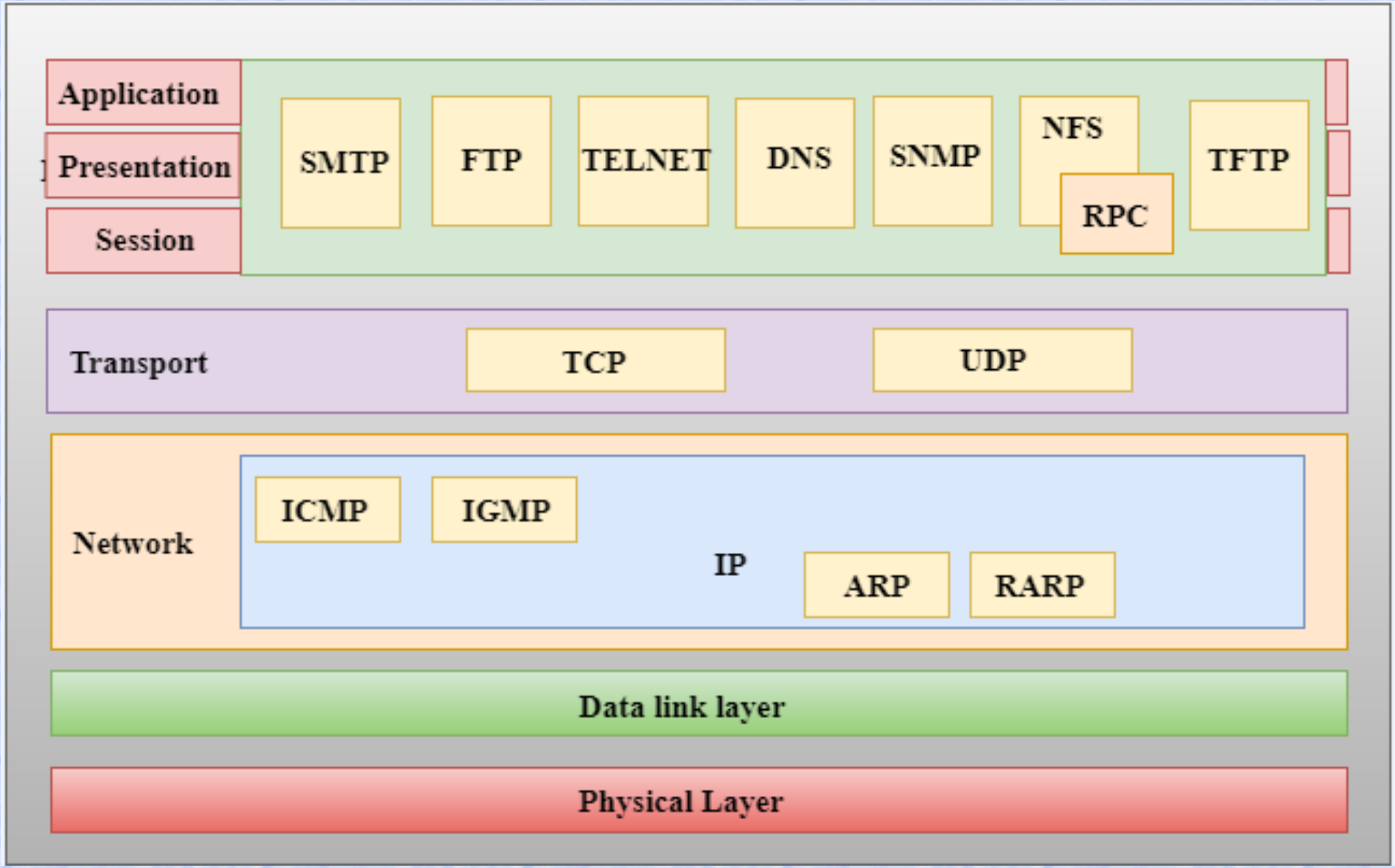
- The data link layer is very similar to the network layer, except the data link layer facilitates data transfer between two devices on the SAME network.
- The data link layer takes packets from the network layer and breaks them into smaller pieces called frames.
- Like the network layer, the data link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

The Physical Layer

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

TCP/IP model

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality


Application
Presentation
Session
SMTP
FTP
TELNET
DNS
SNMP
NFS
RPC
TFTP
Transport
TCP
UDP
Network
ICMP
IGMP
IP
ARP
RARP
Data link layer
Physical Layer

Physical and data link layers

- At the physical and data link layer, TCP/IP does not define any specific protocol.
- It supports all the standard and proprietary protocols.
- This layer is mainly responsible for the transmission of the data between two devices on the same network
- A n/w in TCP/IP internetwork can be a local area n/w or a wide area n/w

Network layer

The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Following are the protocols used in this layer are:

1) **IP Protocol:**

- The internetworking protocol(IP) is the transmission mechanism used by TCP/IP protocols
- it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers.

- It is an unreliable and connectionless protocol-a best effort delivery service.
- The best effort means that IP provides no error checking or tracking.
- The term best effort means that IP provides no error checking or tracking
- IP transports data in packets called datagrams, each of which is transported separately.
- Datagram can travel along different routes and can arrive out of sequence or be duplicated.
- IP does not keep track of the routes and has no facility for reordering datagrams once they arrives at their destination

- The limited functionality of should not be considered a weakness, however IP provides bare-bone transmission functions that free the user to add only those facilities necessary for a given application and thereby allows for maximum efficiency.

2) ARP – stands for Address Resolution Protocol.

On typical physical n/w, such as LAN each device is identified by physical or station address, usually imprinted on the n/w interface card(NIC)

Its job is to find the hardware address of a host from a known IP address.

3) ICMP – stands for Internet Control Message Protocol.

Is mechanism used by host and gateways to send notification of datagram problems back to the sender

4) Reverse Address resoluation protocol

RARP allows host to discover its internet address when it knows only its physical address

Used when computer is connected to n/w very 1st time

5) Internet group message protocol(IGMP)

Is used to facilitate the simultaneous transmission of a message to a group of recipients.

Transport Layer

- The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.
- It is responsible for end-to-end communication and error-free delivery of data.

1. Transmission Control Protocol (TCP) –

- It is known to provide reliable and error-free communication between end systems.
- It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism.
- It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.

2. User Datagram Protocol (UDP) –

- On the other hand does not provide any such features.
- It provides connectionless service and end-to-end delivery of transmission.
- It is the go-to protocol if your application does not require reliable transport as it is very cost-effective.
- Unlike TCP, which is connection-oriented protocol, UDP is connectionless

Application Layer

- This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer.
- This layer allows the user to interact with the application. It is responsible for node-to-node communication and controls user-interface specifications.
- Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP.

Following are the main protocols used in the application layer:

•HTTP:

HTTP stands for Hypertext transfer protocol.
This protocol allows us to access the data over the world wide web.
It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.

•SNMP:

•SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.

•**SMTP:**

SMTP stands for Simple mail transfer protocol.
The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.

•**TELNET:**

It is an abbreviation for Terminal Network.
It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.

•**FTP:**

FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer