1. Network Models & Physical Layer

Introduction :-

→ The word data refers to information Presented in whatever form is agreed upon the Parties Creating & Using the data. (or) data = Collection of information

→ The Exchange of data between two devices Via some form of transmission media such as wire cable, etc is known as Data Communication

→ for data Communications to occur the Communicating device must be part of Communication System made up of Combination of hardware & Software.

∴ i.e Communicating device = h/w + s/w
(h/w → physical, s/w → Prgms)

→ The Effectiveness of data Communications System depends on four fundamental characteristics such as:

(a) Delivery: The system must deliver data to Correct destination, & data must received by intended user or device.

(b) Accuracy: The system must deliver the data accurately

(c) Timeliness: Data delivery should be done by system in a timely manner. In the Case of Videos & audio's timely delivery means, data should be delivered in a same order that they have Produced, & without Significiant delay.

(d) Jitter: Jitter refers to the Variation in Packet arrival time. It is the Uneven delay in the delivery of audio or Video Packets.

Eg:- Assume Video Packet are sent every 30ms.

Scanned by CamScanner

If some Packets arrive with 20ms delay & others with 40ms delay, an Even quality in the video is the result.

G.V.R. COLLEGE OF ENGINEERING
Pin 530 048
VIZIANAGARAM

* Components:

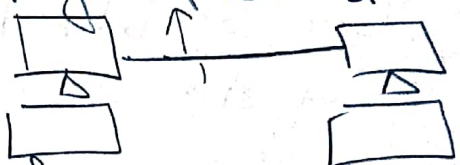
→ Data Communication System has five Components

ⓐ Message → information to be Communicated → Eg → Text, number, audio, Picture etc

ⓑ Sender → Device which sends data message → Eg:- , workstation etc

ⓒ Receiver → Device which receives the message → Eg:- → Same, telephone etc

ⓓ Transmission Medium → physical path → made up → twisted pairs, Coaxial cables, fiber-optics, radio waves etc



ⓔ Protocol → Set of rules → Connection-Oriented, Connection-less

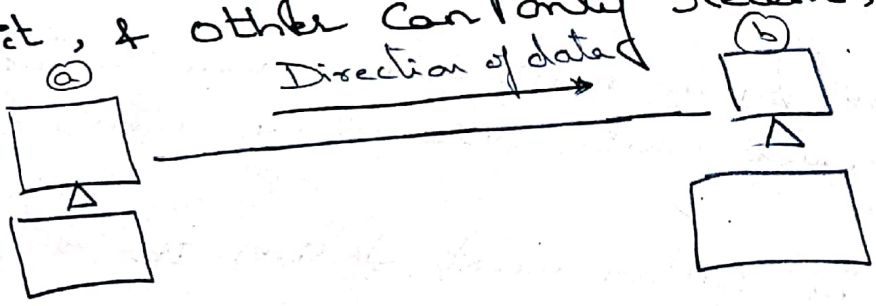
* Data Flow:-

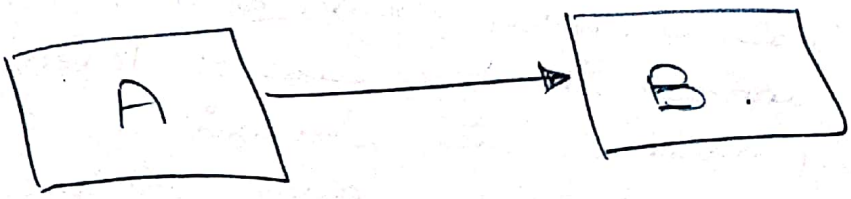
→ Communication between two devices can be

1. Simplex:

→ Also known as Unidirectional (or) One-way Street

→ bcz → Only One of the two devices on a link can transmit, & other can only receive, as shown in fig.



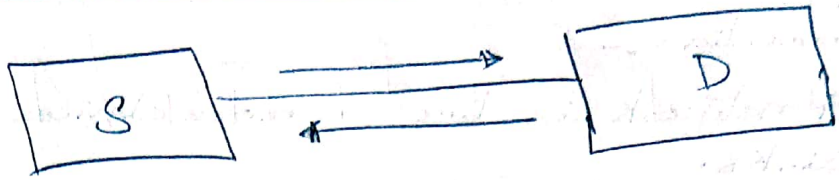


Dis:- → [i.e Sender to Receiver only].

2. Half-Duplex:

→ In half-duplex mode, Each station can both transmit & receive, but not at a same time. When One device is sending, the other can only receive & Vice-Versa.

Scanned by CamScanner



note:-
↳ any 1 direction but not both
Eg:- ↳ Walky-Talky
↳ road (single)
↳ Accelators

② Full-Duplex:-
↳ Bi-directional, Duplex modes
↳ where both station can transmit & receive simultaneously.

Eg:- Telephones,

NETWORKS:-
① → Network is a set of devices (i.e nodes) connected by communication links. where node can be a computer, Printer, Telephone etc which is capable of sending/receiving data generated by other nodes on a network.

② → A computer network may specifically defined as "An interconnected collection of autonomous computers.

* Distributed Processing:-
↳ Task is divided among multiple computers.
i.e instead of one single large machine is responsible, work is divided/distributed to set of 🖥's.

* Network Criteria:-
→ To get an Effective & Efficient network, it must meet a number of Criteria's. The most important are

n/w Criteria
- Performance
  - → no. of users
  - → Type of Transmission medium
  - → S/w & H/w
- Reliability
  - → frequency of failure
  - → Recovery time of a n/w after failure
  - → Catastrophe — earthquake, fire etc
- Security
  - → Virus
  - → Unauthorized Users

Scanned by CamScanner

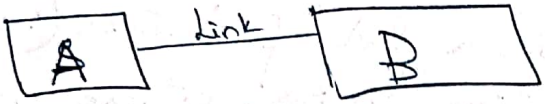
Types of Connections:-

→ A network is two or more devices Connected through links.

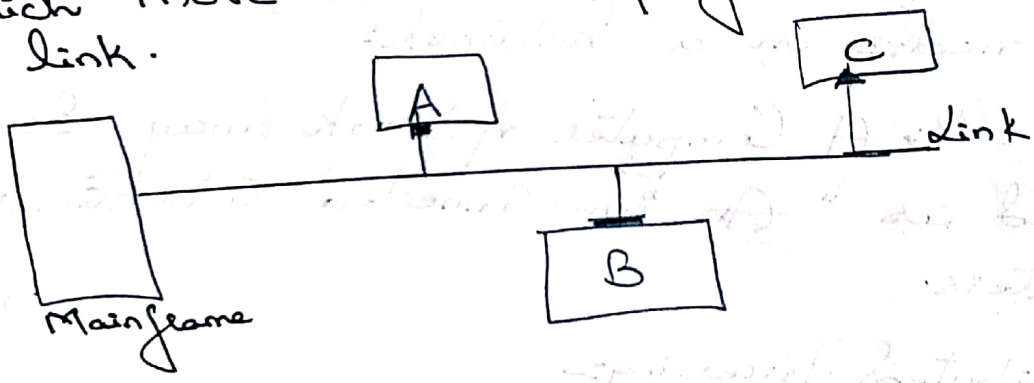
→ A link is a Communications Pathway that transfers data from One device to another.

→ There are two Possible types of Connections. They are:

1. Point-to-Point:
   ↳ dedicated link b/w two devices



2. Multi Point:-
   ↳ It is also called as multidrop Connection is one in which more than two specific devices share same link.



Physical Topologies:-

① → It refers to the way in which a n/w is laidout physically.

② → Two or more devices Connected to a link

③ → Two (or) more links form a topology

→ The topology of a n/w is defined as a geometric representation of the relationships of all the links and linking devices (ie nodes) to one another. There are four basic topologies, they are:

Scanned by CamScanner

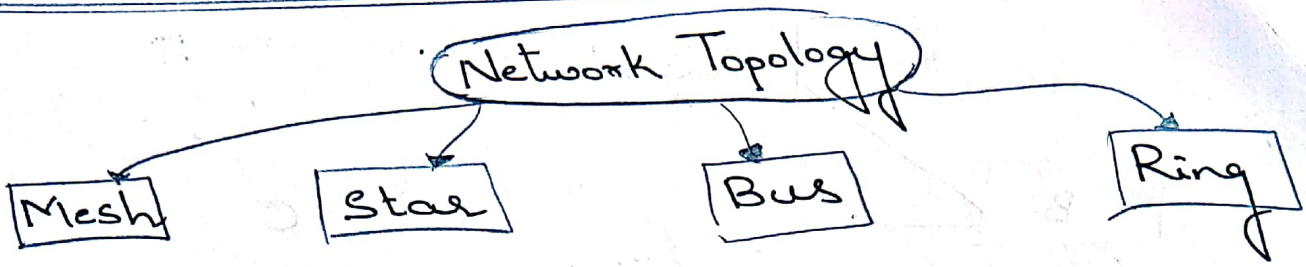


fig:- Categories of Topology.

Def② → In CN, each ~~node~~ Computer acts as a node and how these nodes are Connected with each others is Called the network topology.

Def③ → The term topology refers to the way in which the End Points, or Stations, attached to the network are interConnected.

① Mesh Topology:-

→ It is also called as Complete topology.

→ Here, every device has a dedicated Point-to-Point link to Each other device where Point-to-Point means that only one terminal/wire directly Connects the two devices.

→ The term dedicated means the link Carries traffic only between the two devices it Connects.

→ A mesh topology is Empolyed for long distance transmission of data b/w nodes.

→ A mesh network has $(n(n-1))/2$ physical channels to link n-devices. i.e $\boxed{\frac{n*(n-1)}{2}}$

→ Mesh topology is of two types. They are:

ⓐ True Mesh topology
ⓑ Hybrid Mesh topology

Scanned by CamScanner

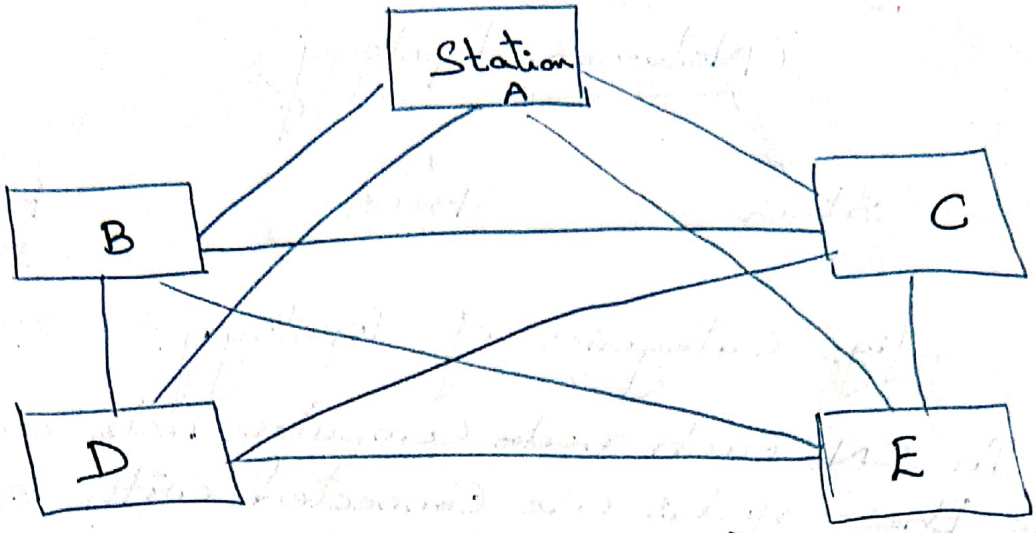


fig:- fully Connected mesh topology.

Advantages:-

↳ No Traffic Problem, Better Security, Robust to link failures, fault identification & isolation is Easy.

Disadvantages:-

- ↳ Lot of Cables, Ports etc used for establishing Connection
- ↳ Every device has to be Connected to Each other
- ↳ Installation & Reconnection are difficult.
- ↳ Requires more space as their mores Cables Ports etc
- ↳ h/w required to Connect each link (i.e i/p & o/p Ports etc) Can be Expensive.

Note:-

- ↳ no. of links $= \frac{n(n-1)}{2}$
- ↳ no. of Ports Per device $= n-1$
- ↳ no. of devices $= n$.

Eg:- $n = 8$ }, then no. of Ports, no. of devices, then

* no. of Ports Per devices $= n-1 \Rightarrow 8-1 \Rightarrow 7$.
* no. of links $= \frac{n(n-1)}{2}$

$$= \frac{8*(8-1)}{2} \Rightarrow \frac{\cancel{8}^{4} * 7}{\cancel{2}}$$

$$\Rightarrow 28$$

Scanned by CamScanner

1. Network Models & Physical Layer.

Introduction:-

→ A set of devices often mentioned as nodes connected by media link is called a Network.

→ A node can be a device which is capable of sending or receiving data generated by other nodes on the network like a computer, printer etc. These links connecting the devices are called Communication channels.

→ Computer network is a telecommunication channel using which we can share data with other computers or devices, connected to the same network. It is also called Data Network.

Eg:- Internet

→ Computer network doesnot mean a system with one control unit connected to multiple other systems as its slave (i.e Distributed System, not Computer network).

* Network Criteria:-

→ A network must be able to meet a certain no. of criteria. The most important of those are Performance, reliability & Security.

* Performance :- It is measured in many ways

- Transist time
  - ↳ time taken to travel a message from one device to another
- Response time
  - ↳ It is defined as the time elapsed b/w inquiry & response

Scanned by CamScanner

→ others ways to measure are Efficiency of s/w, no. of users, Capability of Connected hardware.

• **Reliability:-**

→ It decides the frequency at which network failure take place. More the failures are, less is the reliability.

(or)

→ network reliability is measured by the frequency of failure, & the network's robustness in catastrope.

• **Security:**

→ Security issues include Processing data from Unauthorized access, Protecting data from damage & development & implementing Policies & Procedures for recovery from breaches & data looses.

(or)

→ It refers to the Protection of data from any Unauthorised User or access. While travelling through network, data Passes many layers of network, & data can be traced if attempted. Here Security is also a very important characteristic for networks.

* Physical Structures:-

• **Types of Connection:**

→ A network is two or more devices Connected through links. A link is a Communication pathway the transfers data from One device to another.

→ For Communication to occur, two device must be Connected in Some way to the Same link at the Same time.

Scanned by CamScanner

There are two Possible types of Connections:-

* Point-to-Point
* multipoint.

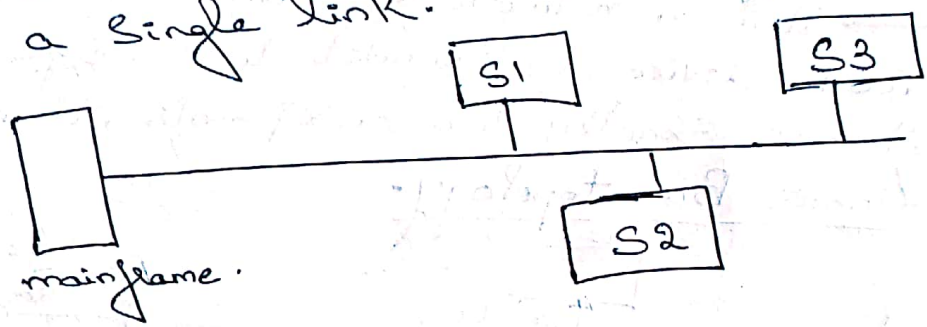
• **Point-to-Point:-**

→ 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.

• **Multipoint:-**

→ A multipoint (also called multidrop) Connection is one in which more than two Specific devices share a Single link.

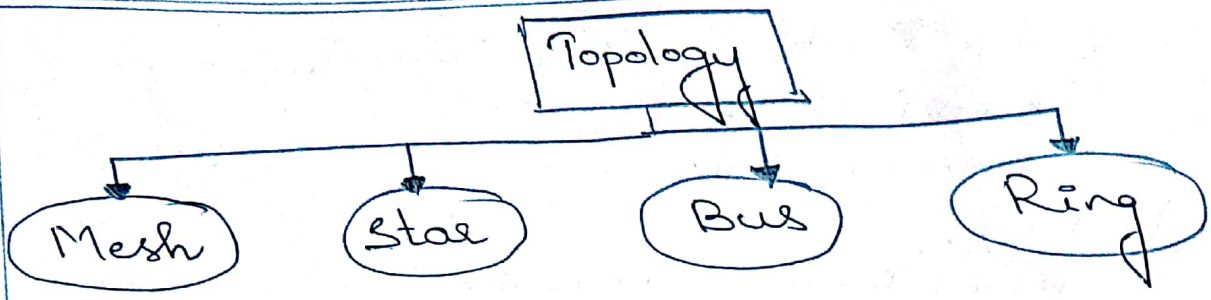


• **Physical Topology:-**

→ physical Topology refers to the way in which a network is laid out physically. Two or more devices Connect to a link, two or more links from a topology. The Topology of a network is the geometric representation of the relationship of all the links & linking devices (usually called nodes) to One another. There are four basic topologies Possible:

- Bus
- Mesh
- Star
- Ring

Scanned by CamScanner



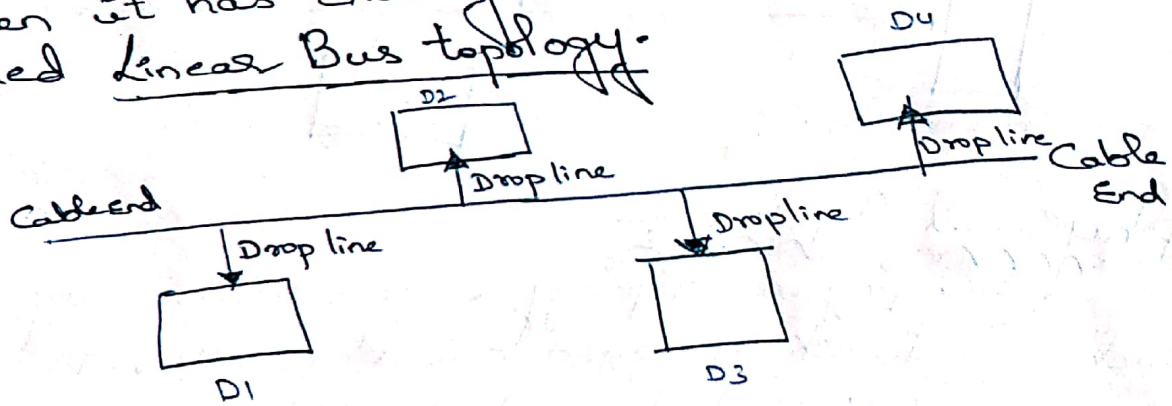
*[Mesh topology:-

→ Here, Every device has a dedicated Point-to-Point link to Every other device.

→ The term dedicated means that the link carries traffic only between the two devices it connects.]*

1. Bus Topology:-

→ It is a network type in which every computer and network device is connect to a single cable. When it has Exactly two End Points, then it is called Linear Bus topology.



• Features:

→ Transmits data only in one direction

→ Every device is connected to a single cable.

• Advantages:

→ Cost Effect

→ Cable required least compared to other network topology

→ Used in small networks

→ It is Easy to Understand

→ Easy to Expand joining two cables together.

Scanned by CamScanner

Disadvantages:-

→ Cable fails then whole network fails

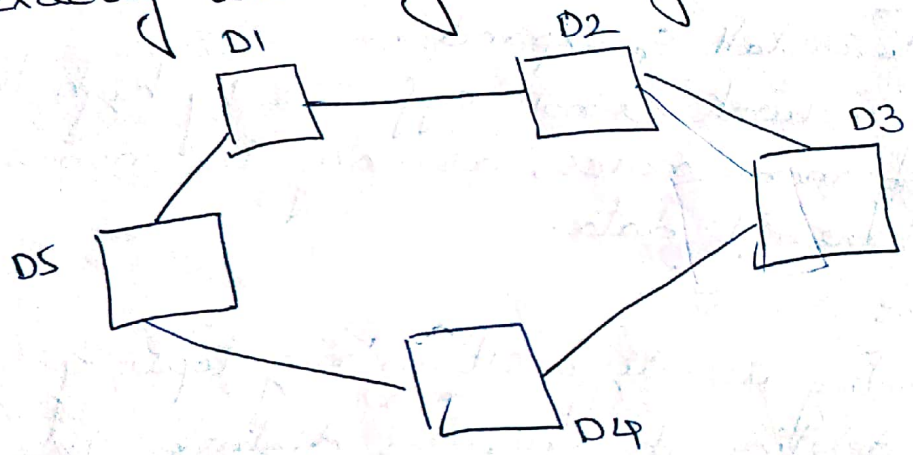
→ If n/w traffic is heavy (i.e no. of nodes in n/w is more) the Performance of the network decreases.

→ Cable has limited length

→ It is slower than the ring topology.

2. Ring Topology:-

→ Each Computer in a network is Connected to another Computer in a ring form So it is known as ring topology. Exactly two neighbours for Each device.



Features:-

- A no. of repeaters are used for Ring topology with large no. of nodes, because if Someone wants to send data to the last node in a ring topology with 100 nodes, then data will have to pass through 99 nodes to reach the 100th node. Hence to Prevent data loss repeaters are used in the network.
- The transmission is Unidirectional, but it can be made bidirectional by having 2- Connections

between Each network node, it is called Dual Ring Topology.

- In Dual Ring Topology, two ring networks are formed, & data flow is in opposite direction in them. Also, if one ring fails, the second ring can acts as a backup, to keep the network up.
- Data is transferred in a sequential manner i.e bit by bit. Data transmitted, has to pass through Each node of the network, till the destination node.

Advantages:

1. ~~Pro~~ cheap to install & Expand.
2. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.

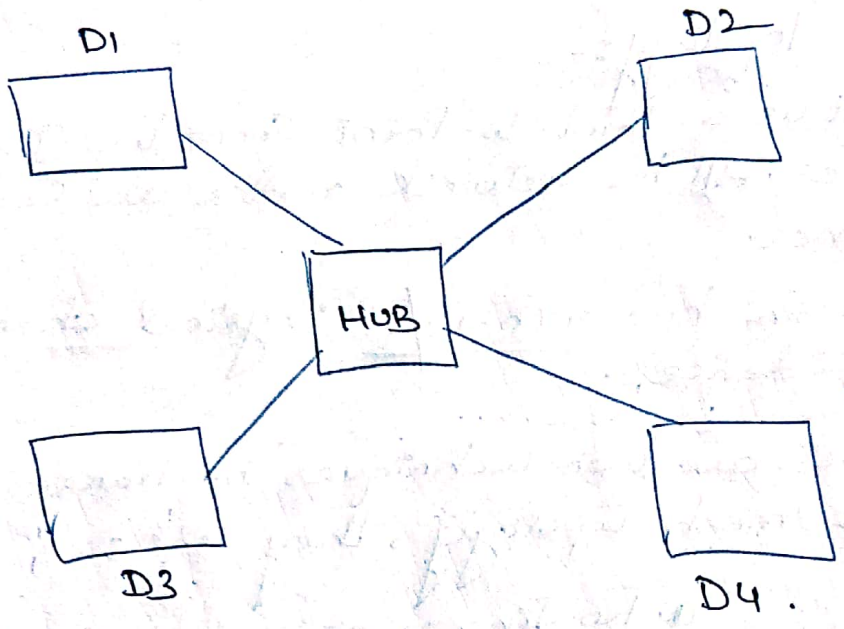
Disadvantages:

1. Troubleshooting is difficult in ring topology
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

3. STAR Topology:-

→ In this topology all the computers are connected to a Single hub through a Cable. This hub is the Central node & all other nodes are Connected to the Central node.

Scanned by CamScanner



features:-

1. Every node has its own dedicated Connection to the hub.
2. Hub acts as a repeater for data flow
3. It can be used with twisted Pair, optical fibre or Coaxial cable.

Advantages:

1. Fast Performance with few nodes & low network traffic
2. Hub can be Upgraded Easily
3. Easy to troubleshoot
4. Easy to setup & modify
5. only that node is affected which has failed, rest of the nodes can work Smoothly.

Disadvantages:

1. Cost of installation is high
2. Expensive to use
3. If the hub fails then whole network is stopped because all the nodes depends on the hub.
4. Performance is based on the hub i.e it depends on its capacity.

Scanned by CamScanner

4. MESH Topology:-

→ It is a Point-to-Point Connection to other nodes or devices. All the network nodes are Connected to Each other.

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

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

a. Routing
b. Flooding.

(a) Routing:

→ In routing, the nodes have a routing logic, as per the network requirements.

→ Like routing logic to direct the data to reach the destination using the shortest distance.

→ Or, routing logic which has information about the broken links, & it avoids those nodes etc.

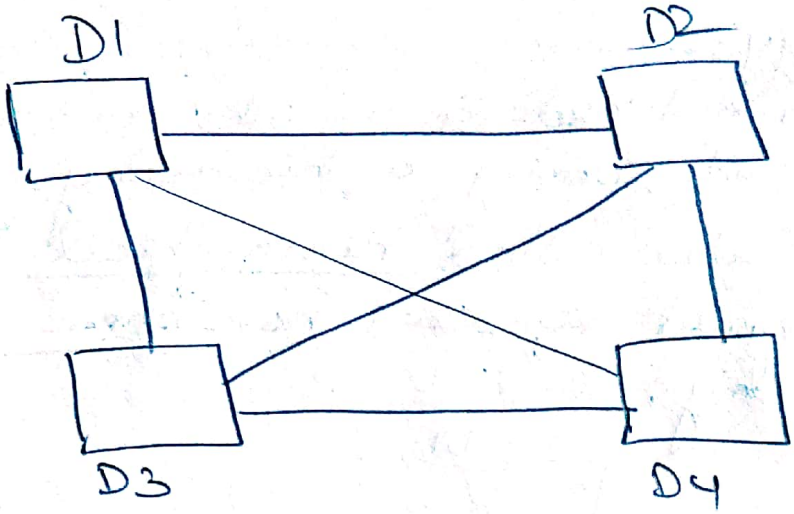
→ We can Even have routing logic, to re-Configure the failed nodes.

(b) Flooding:

→ Here, the same data is transmitted to all the network nodes, hence no routing logic is required.

→ The n/w is robust, & the its very Unlikely to lose the data. But it leads to Unwanted load over the network

Scanned by CamScanner



Types :-

ⓐ Partial Mesh topology :-

→ In this topology some of the systems are Connected in same fashion as mesh topology but some devices are only Connected to two or three devices.

ⓑ Fully Mesh topology :-

→ Each & Every nodes or devices are Connected to Each other.

Features :-

1. Fully Connected
2. Robust
3. Not flexible.

Advantages :-

1. Each node Can Carry its own data load
2. It is robust
3. Fault is diagnosed Easily.
4. Provides Security & Privacy.

Disadvantages :-

1. Installation & Configuration is difficult.
2. Cable Cost is more.
3. Bulk wiring is required.

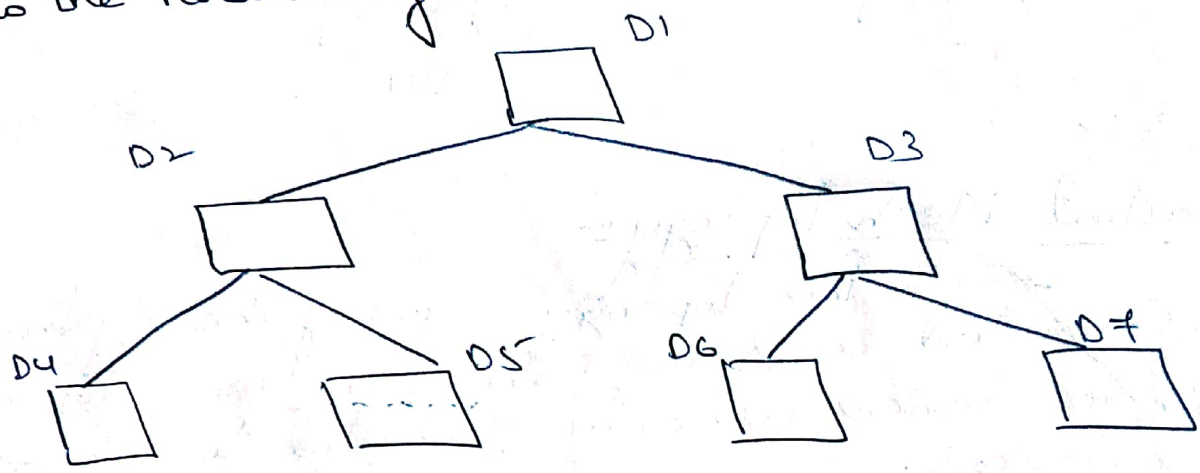
Scanned by CamScanner

5. TREE Topology:-

→ It has a root node & all other nodes are Connected to it forming a hierarchy.

→ It is also called hierarchical topology.

→ It should at least have three levels to the hierarchy.



Features:

1. Ideal if workstations are located in groups
2. Used in Wide Area network.

Advantages:-

1. Extension of bus & star topologies
2. Expansion of nodes is Possible & Easy
3. Easily managed & maintained
4. Error detection is Easly done.

Disadvantages:-

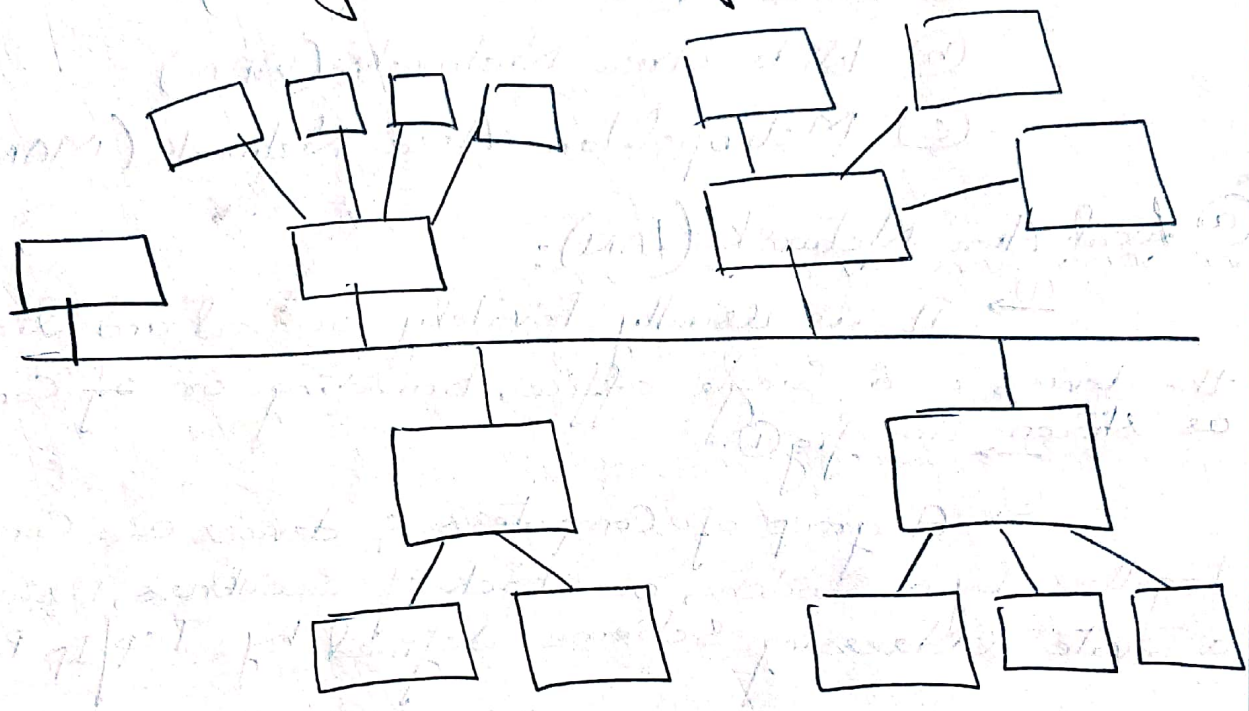
1. Heavily Cabled
2. Costly
3. If more nodes are added maintainance is difficult
4. Central hub fails, network fails.

Scanned by CamScanner

6. Hybrid Topology:-

→ It is two different types of topologies which is a mixture of two or more topologies

Eg:- if in an office in one department ring topology is used & in other Star topology may be used, Connecting these topologies will result in Hybrid Topology (ring + star).



Features:-

1. It is Combination of two or topologies
2. Inherits the advantages & disadvantages of topologies included.

Advantages:-

1. Effective
2. flexible
3. Reliable as Error detecting & trouble shooting is easy.
4. Scable as size can be increased easily

Disadvantages:-

1. Complex in design
2. Costly.

Scanned by CamScanner

Network Models:-

→ Computer networks are Created by different Entities. Standards are needed so that these heterogeneous network Can Communicate with one another. The best two standards are OSI & Internet model.

→ network models are divided into 3-Categories. They are:-

ⓐ Local Area network (LAN)
ⓑ Wide Area Network (WAN)
ⓒ Metropolitan Area Network (MAN)

ⓐ Local Area Network (LAN):

① → It is usually Privately owned and links the devices in a Single office, building or of Campus as shown in fig ①.

② → A group of Computers & devices are Connected together by a Switch, or stack of Switches, using a Private addressing Scheme defined by TCP/IP Protocol.

→ LANS are designed to allow resources to be Shared between personal computers or workstations. The resources to be shared Can include hardware (Eg., a Printer), Software (Eg:- application Program) or data.

→ In addition to Size, LANS are distinguished from other types of networks by their transmission media & topology (like ring, bus & Star).

→ Early LAN's had data rates in the 4 to 16 megabits Per Seconds (Mbps) rate. Today however, Speeds are normally 100 or 1000 Mbps.

Eg:- A bunch of Students playing (counter strike) game in the same room (without internet)

Scanned by CamScanner

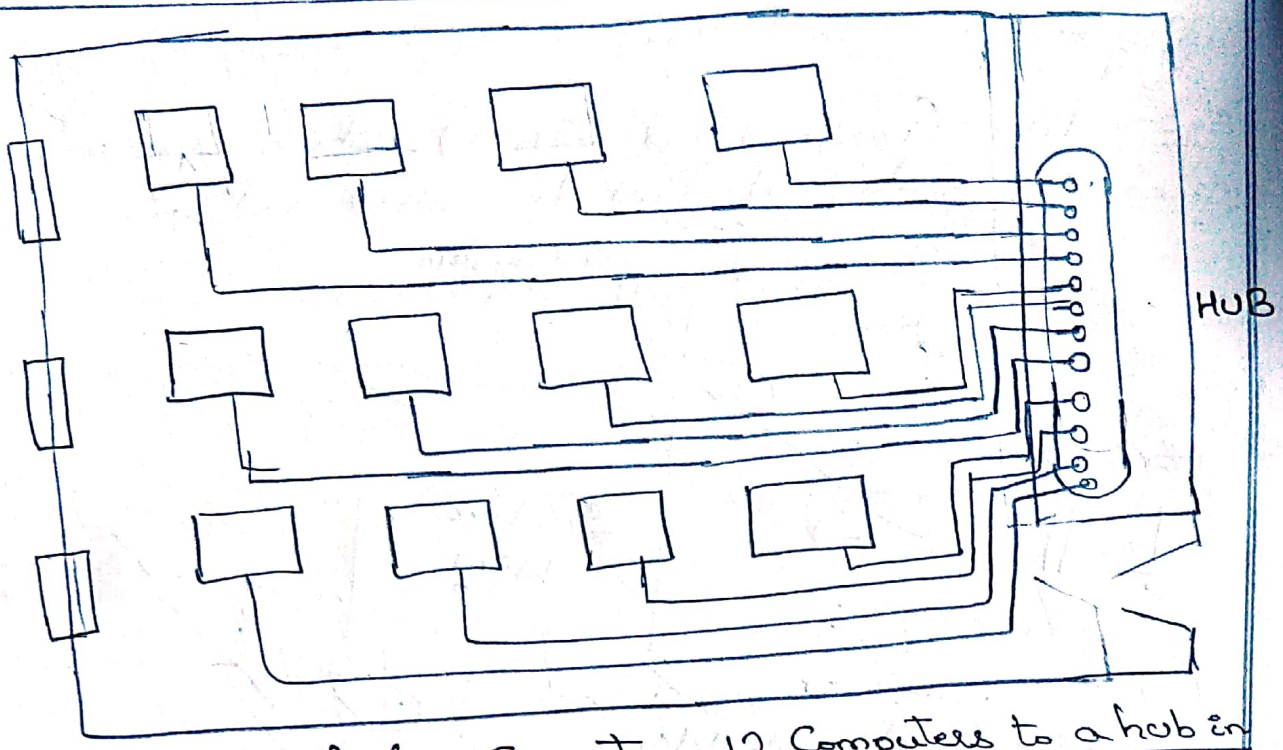


fig1: An isolated LAN Connecting 12 Computers to a hub in a closet.

2. Wide Area Network (WAN):-

→ WAN Provides long-distance transimission of data, image, audio, & Video information Over large geographic areas that may Comprise a Country, a Continent or Even whole world.

→ A 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.

→ There are two types of WANS.

ⓐ Switch WAN &

ⓑ Point-to-Point WAN.

→ The Switch WAN Connects the End Systems, which Usually Comprise 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 Small LAN to an Internet Service Provider (ISP). This Type of WAN

Scanned by CamScanner

is often used to Provide Internet access.

Eg:- ATM (i.e Switched WAN), which is a network with fixed-size data unit Packets called cells.

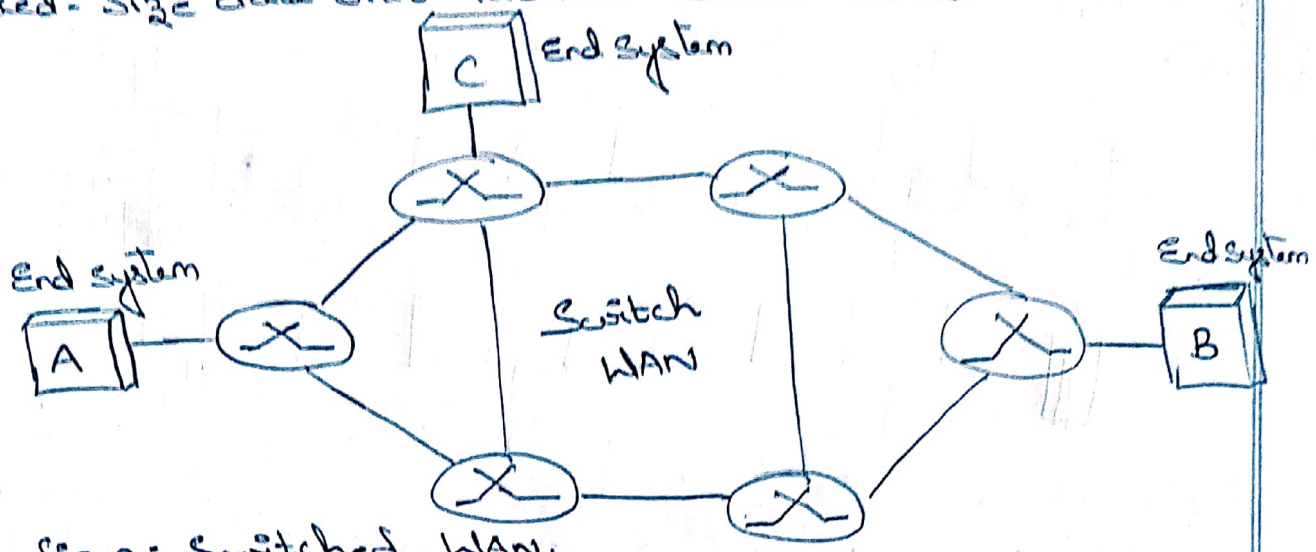


fig a: Switched WAN.

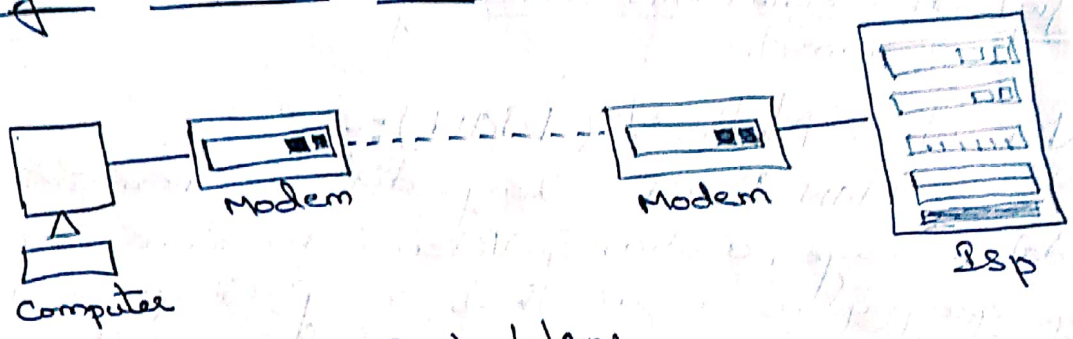


fig b: Point-to-Point WAN.

© Metropolitan Area Network (MAN):-

→ MAN is a network with a Size between a LAN and WAN. (i.e Larger than LAN & smaller than WAN).

→ It normally Covers the area inside a town or City.

→ It is designed for Customers who need a high-speed Connectivity, normally to the Internet, & have Endpoints Spread Over a City or Part of City.

Eg:- ① It is a Part of telephone Company network that Can Provide a high-speed DSL line to the Customer.

Scanned by CamScanner

② Cable TV n/w, which is Originally designed for Cable TV.
③ high-speed data Connection to the Internet.

① LAYERED TASKS:-

→ A network is a Combination of hardware and Software that sends data from one location to another.

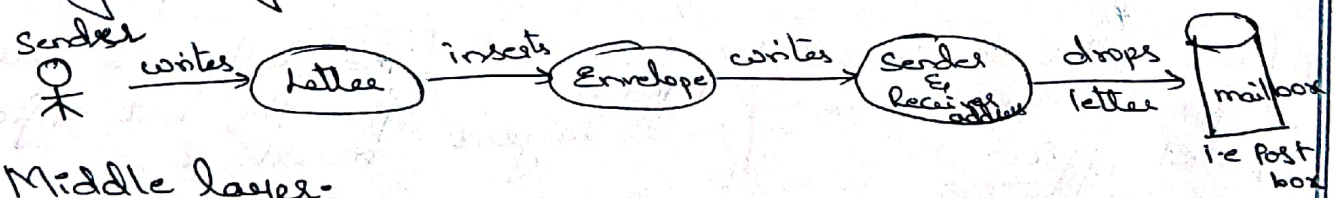
→ In layered architecture of network model, One whole network Process is divided into small tasks. Each small task is ~~again~~ then assigned to a Particular layer which works dedicatedly to Process the task only. Every layer does its specific work.

→ for Example Consider two friends wants to Communicate through Postal mail. The Process of sending a letter to a friend ~~who~~ would be Complex if there were no services available from Post office.

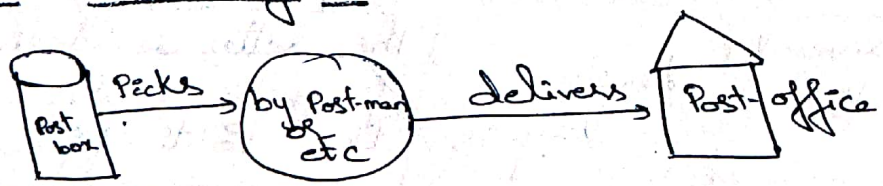
→ The below fig ⓐ ~~Consis~~ ~~involves~~ describes with 3-modules such as Sender, Receiver & a Transport Person/Vechicle.

* At the Sender Side:-

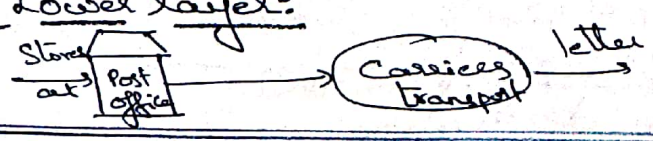
- **Higher layer:**



- **Middle layer:**



- **Lower layer:**

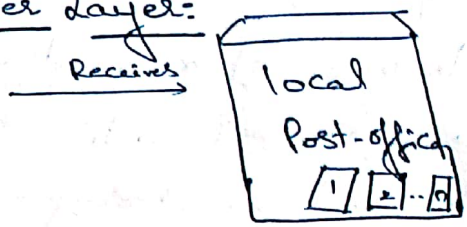


Scanned by CamScanner

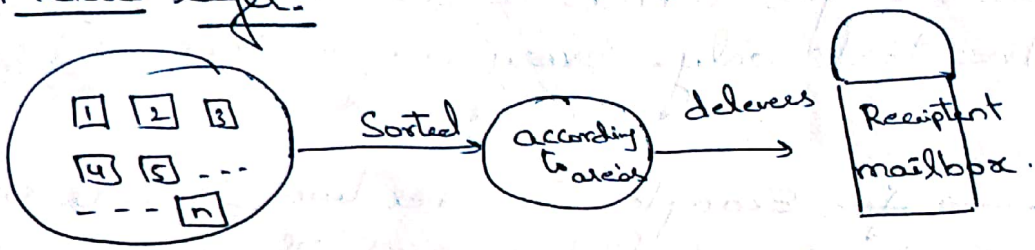
* On the way:

* At Receiver's Side:

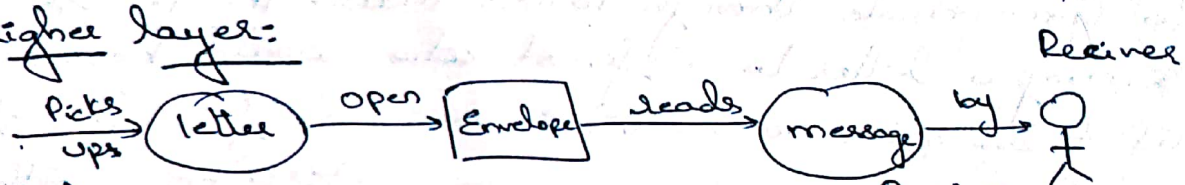
• Lower Layer:



• Middle layer:



• Higher layer:



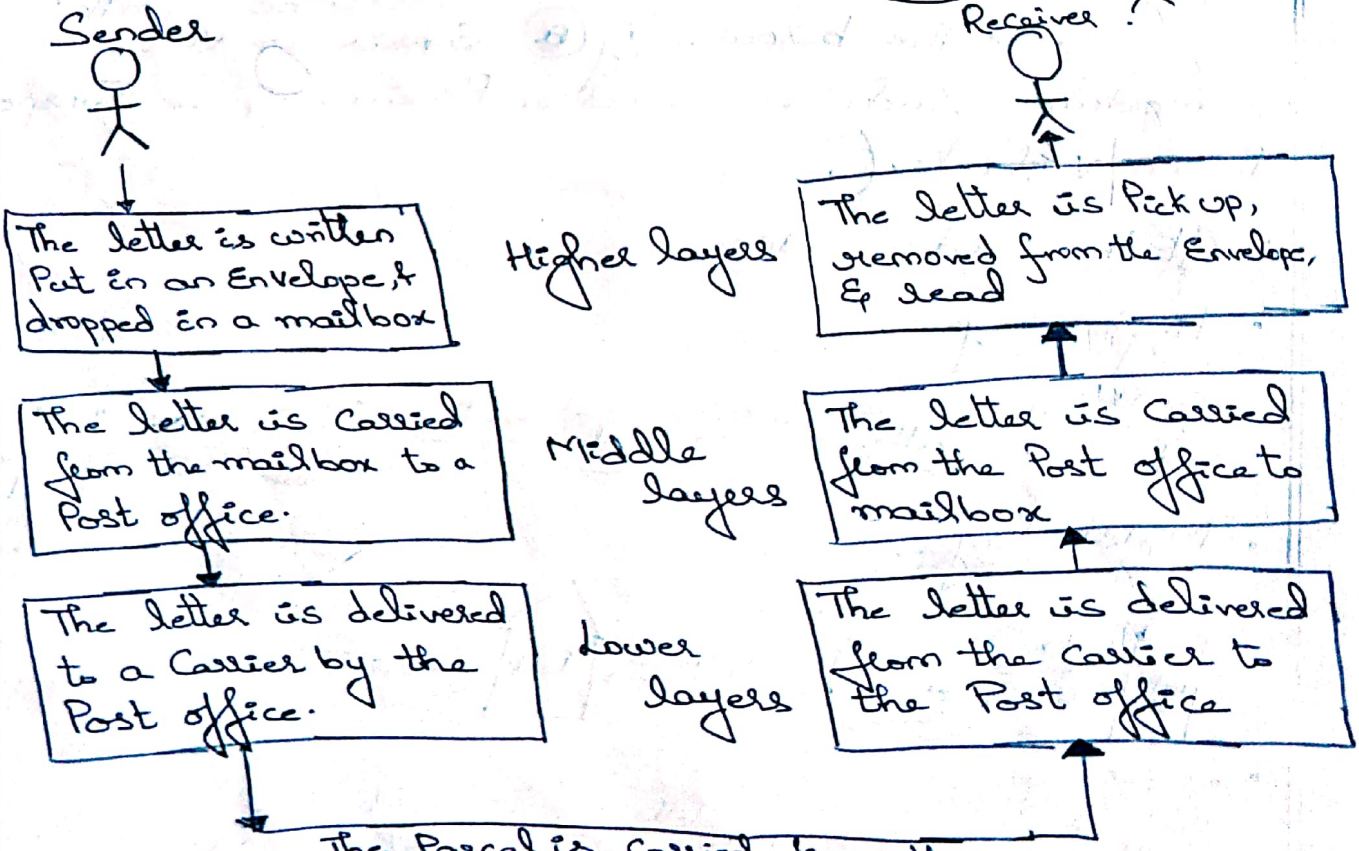


fig a: Tasks involved in Sending a letter.

Scanned by CamScanner

OSI MODELS:-

→ [There are n- no. of users who use Computer network & are located over the world. So, to ensure, national & world wide data Communication, Systems must be ~~delave~~ developed which are Compatible to Communicate with Each other. ISO has developed a ~~Standard~~ model called OSI (Open System Inconnection)] ref

→ ISO (International standards Organization) is a multinational body dedicated to worldwide agreement on international standards.

→ ISO Standard has developed a model called OSI in 1970's.

→ Open system is a set of Protocols that allows any two different systems to Communicate.

→ The Purpose of OSI model is to show how to facilitate Communication between different systems without requiring changes to the logic of the ~~Und~~ hardware & software.

→ OSI model is not a Protocol, it is a model for Understanding a network architecture. It is flexible, robust & interoperable.

→ OSI model Consists of 7 layers.

They are:-

1. Physical layer
2. Datalink layer

Scanned by CamScanner

3. Network layer
4. Transport layer
5. Session layer
6. Presentation layer
7. Application layer.

→ The first three layers such as physical, data link, network are known as Network support layers (Bottom layers) & Similarly Session, Presentation, Application acts as a (Topmost layer) User Support layers.

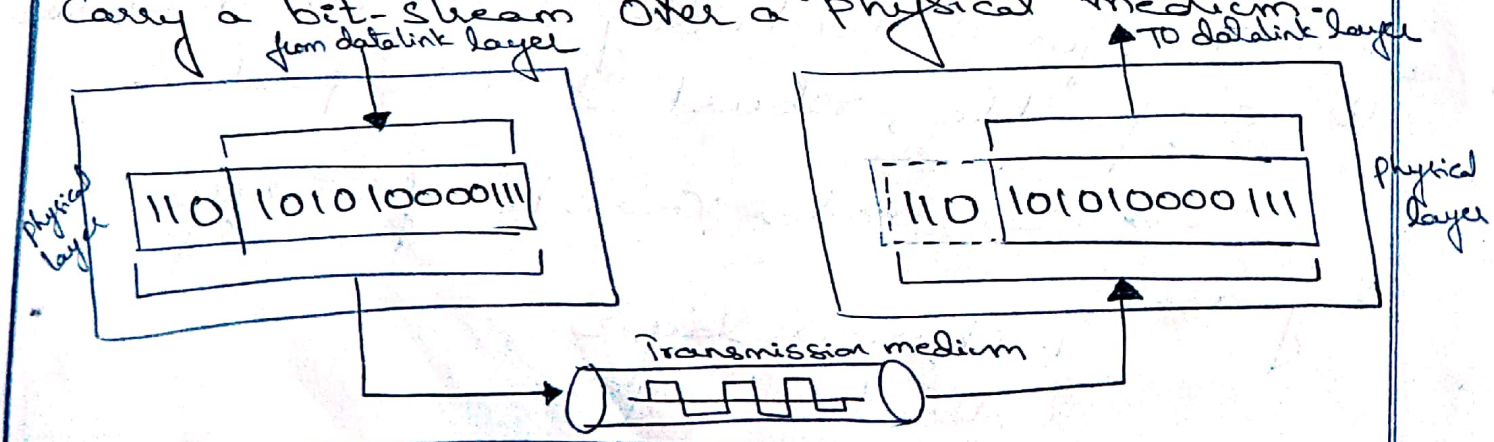
→ The services | Communication between Topmost & bottomost layers are done by using Transport layer.

→ Everytime services are taken from bottom layers & Provided to the Topmost layers, when it is in Single machine. This Communication is done by series of rules & Conventions called as Protocols.

→ The Process on Each machine that Communicate at a given layer are called Peer-to-Peer Process.

1. Physical layer:

→ The Purpose of physical layer is to Carry a bit-stream over a physical medium.



→ It is responsible for movements of individual bits from one hop (node) to the next.

Responsibilities:-

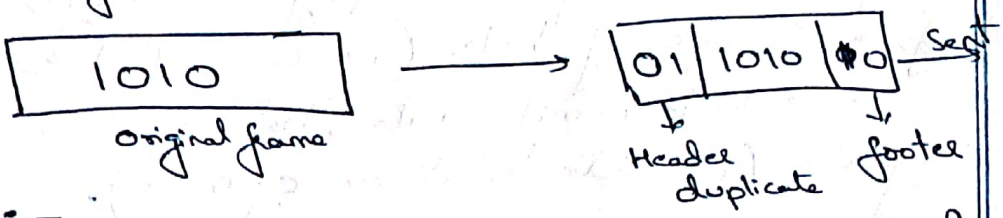
* physical characteristics of interfaces & medium: It defines characteristics of interfaces between the devices & the transmission medium & also defines the type of transmission medium.
* Representation of bits: Physical layer data consists of a stream of bits (i.e 0's & 1's) with no interpretation.
  → To transmit data, bits must be encoded into signals (i.e electrical or optical).
* Date rate: It defines the duration of a bit (i.e no. of bits transmitted per second).
* Synchronized bits: The sender & receiver clocks ~~signal~~ must be synchronized.
* Line Configuration: It is concerned with the connection of devices to the media (i.e Point-to-Point / multi-Point).
* physical topology: It defines how devices are connected to make a network. (i.e type of topology).
* Transmission mode: ~~The~~ It also defines the direction of transmission between two devices: Simplex, half-duplex or full-duplex.

Scanned by CamScanner

2. Data link layer:-

* Framing: It divides the stream of bits received from network layer into manageable data units called frames.
  → Converts (or) divides the bits (i.e received from physical layer) to frames.

* physical addressing: It adds a header to the frame to define the sender/receiver & then disturbed to the different systems on the network.



* Flow Control:-
  ↳ If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid collision/overriding at the receiver.

* Error Control:-
  → It adds reliability to the physical layer by adding mechanism to detect & re-transmit damaged or lost frames.
  → It also used to recognize duplicate frames.
  → It is achieved through a trailer added to the end of the frame.

* Access Control:-
  → When two ~~dev~~ or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over a the link at any given time.

Scanned by CamScanner

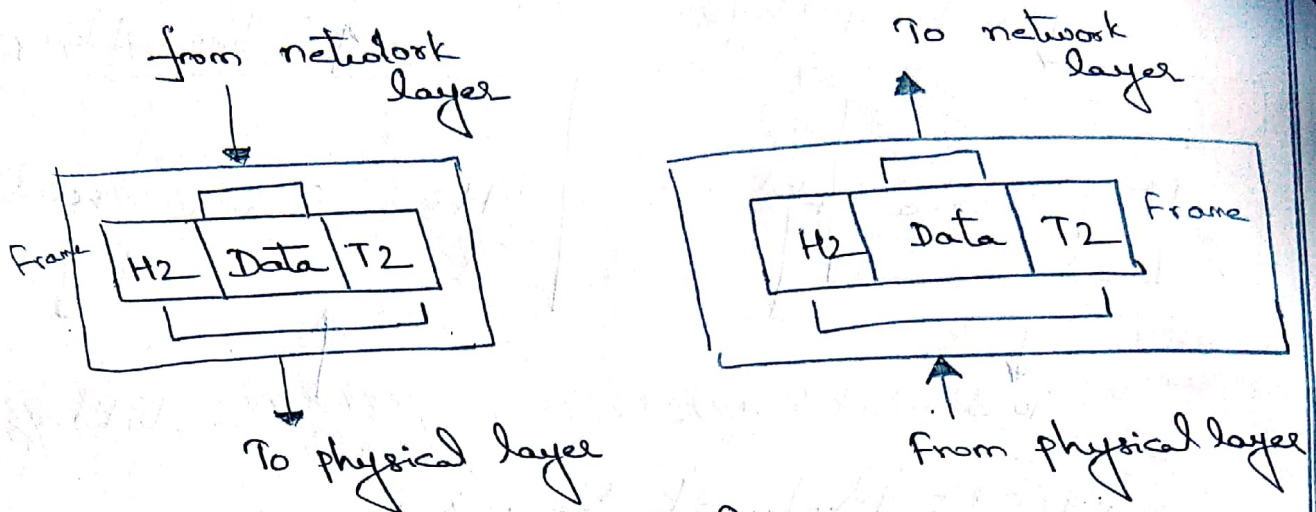


fig ⑥: Data link layer.

③ Network layer:

→ It is responsible for transmitting a data from source-to-destination in the form of Packets.

Responsibilities:

* Logical addressing:-

→ If a Packet Passes the network boundary we need another addressing System to distinguish the source & destination System.

→ network layer adds a header to the Packet Coming from the upper layer. (i.e logical address is known as address)

* Routing:-

→ When independent devices are Connected to Create internetworking (i.e n/w of n/w's) or a large networks, the Connecting devices (i.e router or switches) routes or Switch the Packets to their final destination.

Scanned by CamScanner

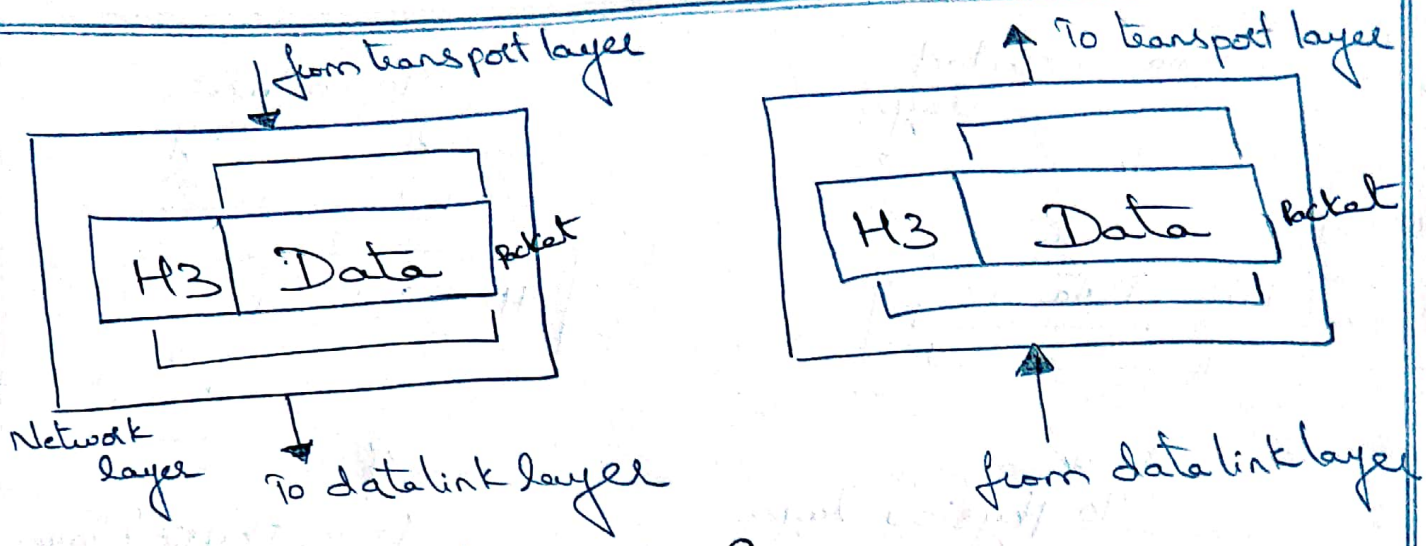


fig (c) : Network layer.

(4) Transport layer:-

→ It is responsible for Process-to-Process delivery of the Entire message.

→ Common Protocols that operates at this layer are Tcp, UDP, Spx, & NetBEUI.

→ It is responsible for Error & flow Control.

* Service-Point addressing:-

→ Computers often run several Programs at same time. for this reason, source-to-destination delivery means delivery not only from one Computer to the next but also from a specific Process in one ~~Proc~~ Computer to the specific Process (i.e running Program) in another.

→ It at Transport layer header must therefore include a address called Service-Point address (or Port address).

* Segmentation & Reassembly

* Connection Control.

Scanned by CamScanner

⑤ Session layer:

→ It is responsible for Establishing, maintaining, & terminating a Connection called a 'Session'.

→ A Session is an Exchange of messages between Computers (a dialog).

→ Managing the Session involves Synchronization of users tasks & dialog control (Eg. who transmit & for how long).

→ Synchronization involves the use of checkpoints in the Stream. In the Event of a failure, only the data from the last checkpoint has to be resent.

⑥ Presentation layer:

→ It is responsible for data translation (i.e Syntax, Semantics etc), Compression & Encryption.

Eg:- ASCII → EBCIDIC

→ Protocols used are SMB, NCP & NFS.

⑦ Application layer:-

→ It Enables Users, whether human or S/w, to access the network.

→ It Provides user interface & Support for Services such as Electronic mail, remote file access & transfer, shared database management, & other type of distributed information Services.

Scanned by CamScanner

→ HTTP, SMTP, FTP etc Protocols used in this layer.

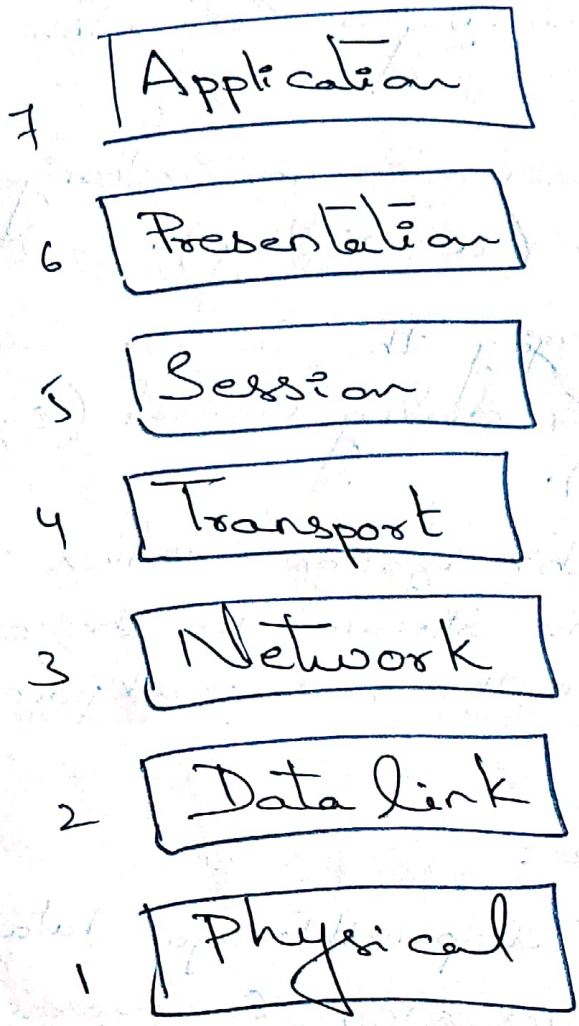


fig 1: Seven layers of OSI model.

note :-

① → Refer pg (31) for interaction b/w layers in OSI model in forouzan text book.

② → Refer pg (32) for an Exchange using the OSI model.

Scanned by CamScanner

④ Tcp/Ip Protocol Stack:-

→ Tcp/Ip stands for Transmission Control Protocol / Internet Protocol.

→ Tcp/Ip Protocol suite is made up of five layer, they are:

* physical layer
* Data-link layer } host-to-network layers
* network layer
* Transport layer &
* Application layer.

→ The top-most three layers in OSI model, here are represented in Tcp/Ip by a single layer called Application layer.

→ Tcp/Ip is a hierarchical Protocol made up of interactive modules, Each of which Provides a Specific functionality.

→ The term hierarchical means that Each upper-level Protocol is supported by one or more lower level Protocols.

① Physical & Data link:-

→ Tcp/Ip doesnt define any Specific Protocol.

→ It Supports all the Standard & Proprietary Protocols.

→ A network in a Tcp/Ip internetwork Can be a local-area network or a Wide-area-network.

Scanned by CamScanner

(b) Network layer:-

→ ~~Tcp/Ip~~ At network layer, Tcp/Ip supports the Internetworking Protocol.

→ Ip, in turn uses four supporting Protocols: ARP, RARP, ICMP, & IGMP.

* Internetworking Protocol (Ip):-

→ Ip is the transmission mechanism used by Tcp/Ip Protocol.

→ It is Unreliable & Connectionless Protocol.

→ Ip transports data in Packets called datagrams, each of which is transported Seperately.

→ Datagram can travel along different routes & can arrive out of sequence or be duplicated.

→ Ip doesnt keep track of the routes & has no facility for recording datagrams Once they arrive at their destination.

* Address Resoultion Protocol (ARP):-

→ ARP is used to find the physical address of the node when its Internet address is known.

finds (physical) → (Internet)

* Reverse Address Resolution Protocol (RARP):-

→ RARP allows host to discover its Internet address when it knows only its physical address.

→ It is used when a Computer is Connected to the network for first time or when a diskless Computer is booted.

finds (Internet) —when→ (physical)

Scanned by CamScanner

* Internet Control Message Protocol (ICMP):-

→ ICMP is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender.

→ ICMP sends query & error reporting messages.

* Internet Group Message Protocol (IGMP):-

→ It is used to facilitate the simultaneous transmission of message to a group of recipients.

(c) Transport Layer:-

→ It is associated with two protocols, such as:

- Tcp (Transmission Control Protocol)
- UDp (Userdatagram Protocol)
- SCTP (Stream Control Transmission Protocol)

→ Ip is a host-to-host protocol, i.e it delivers a packet from one physical device to another.

→ UDP & TCP are transport level protocols responsible for delivery of a message from a process (i.e running program) to another process.

* User Datagram Protocol (UDP):-

→ It is a process-to-process protocol that adds only port addresses, checksum error control, & length information to the data from upper layer.

→ UDP is a connection-less protocol.

Scanned by CamScanner

* Transmission Control Protocol (Tcp):-

→ Tcp is a reliable Stream Protocol.

→ Tcp is a Connection-Oriented Protocol i.e Connection must be Established between both Ends of a transmission before Either Can transmit data.

* Stream Control Transmission Protocol (SCTP):-

→ It Provides support for newer applications such as Voice Over internet.

→ It Combines the best features of UDP & Tcp.

(d) Application layer:-

→ The application layer in Tcp/Ip is Equivalent to the Combined Session, Presentation, & application layers in OSI model.

→ Protocols used in this layer are SMTP, FTP, HTTP, DNS, SNMP, TELNET etc.

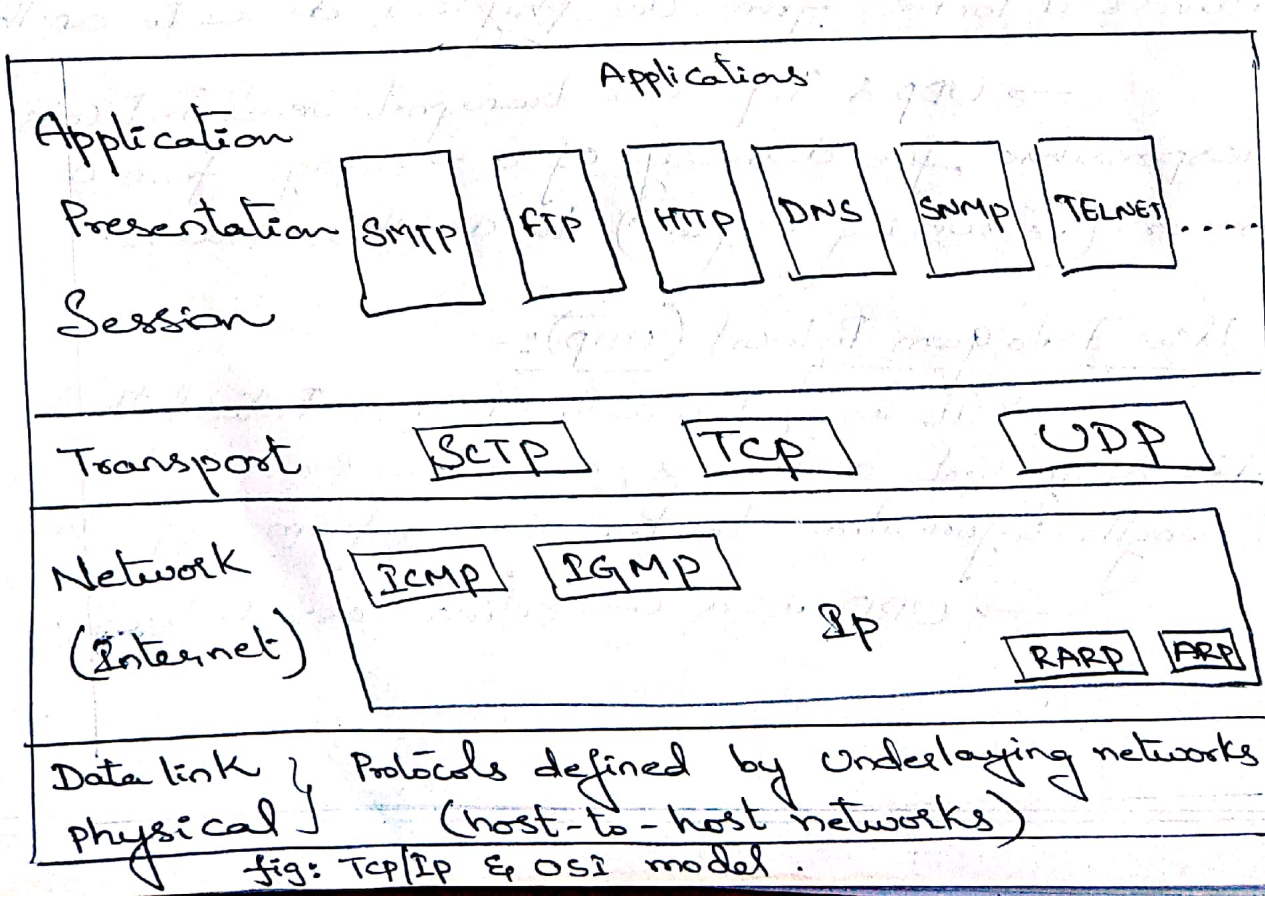


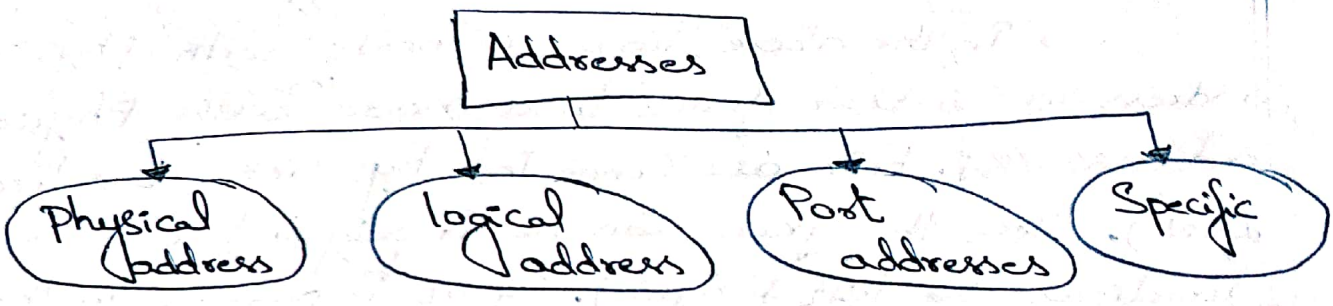
fig: Tcp/Ip & OSI model.

Scanned by CamScanner

⑤ ADDRESSING:-

→ Tcp/Ip Protocols addressing are classified into four levels. They are:

ⓐ physical (link) addresses.
ⓑ Logical (Ip) addresses.
ⓒ Port addresses and
ⓓ Specific addresses.



ⓐ Physical Addresses:-

→ It is also known as the link address.

→ It is the address of a node as defined by its LAN or WAN.

→ It is included in the frame used by the data link layer.

→ It is the lowest-level address.

→ The Size & format of these address vary depending on the network.

Eg:- Ethernet → 6bytes (48-bits)
network interface cards (NIIC) → 1 byte (8-bits)
Local Talk (Apple) → 1 byte (8 bits)

Scanned by CamScanner

Eg:-

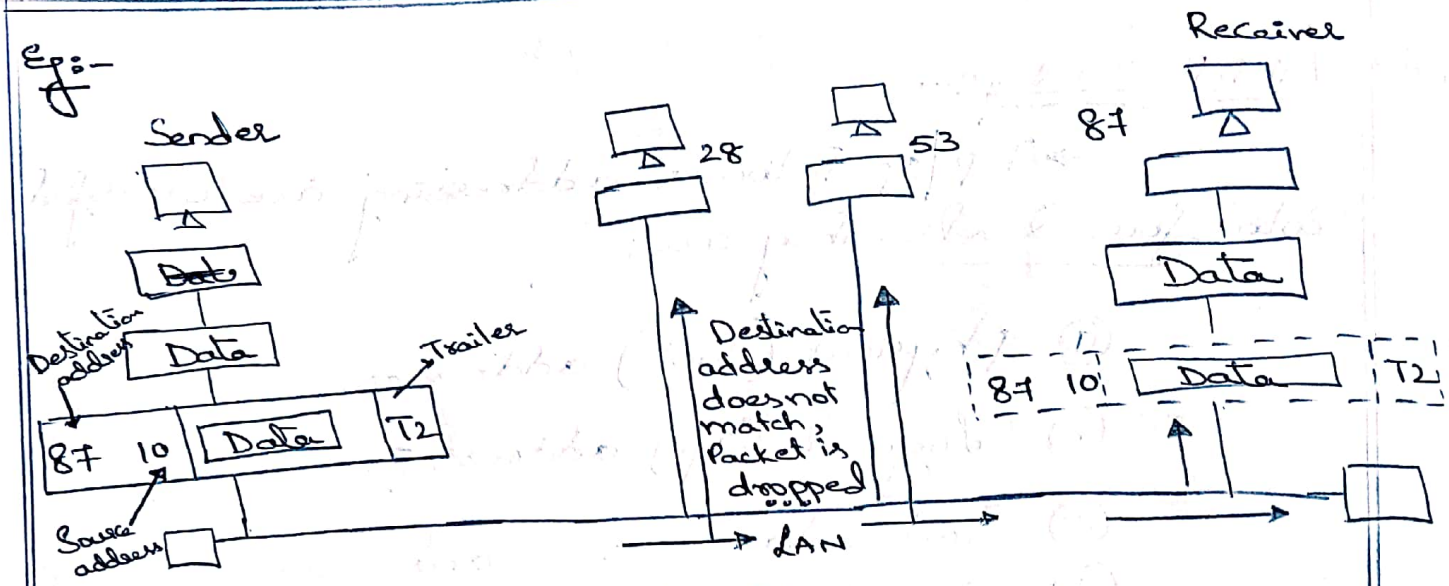


fig:- Physical address.

→ In the above figure, a node(s) with physical address 10 Sends a frame to a node(R) with Physical address 87, both are Connected by link (bus topology LAN). Here the frame Can be Propagated in both directions (i.e left & right). If it Propagates to the left dies when it reaches the End of the Cable, If frame Progates right is Sent to Every station (i.e node) on the network. Each Station match with its ~~phys~~ address if its other than 87 then Packet is droped & send it to other station, this repeats Until destination address is found. Once it found, frame is checked ~~to~~, removes header & Trailer & finally data Part is decapsulated & delivers to the upper layers.

Eg:- LAN uses 48-bit (6-bytes) physical address, written ~~with~~ as 12 hexadecimal digits, Every byte (2 hexadecimal digits) is Seperated by a Colon as:

07:01:02:01:2C:4B

Scanned by CamScanner

(b) Logical Addresses:- (Internet address)

→ Logical addresses are necessary for Universal Communications that are independent of Underlying physical network.

→ physical addresses are not adequate in an internetwork Environment where different n/w's can have different address formats.

→ A logical address in the Internet is Currently a 32-bit address that can Uniquely define a host Connected to the Internet.

→ No two publicly addressed & Visible hosts on the Internet can have the same IP address.

Eg:- Pg (48).

(c) Port Addresses:-

→ IP addresses & physical address are neccessary for a quantity of data to travel from (Source) to (destination).

→ Today, devices that can runs multiple Processes at a same time.

Eg:- Sametime A → C (using Telnet)
A → B (FTP)

→ for this Process to receive data simultaneously, we need a method to label the different Processes.

→ In other words, they need addresses.

→ In TCP/IP architecture, the label assigned to a Process is called Port address.

→ Its length is 16-bits

Scanned by CamScanner

Eg:-

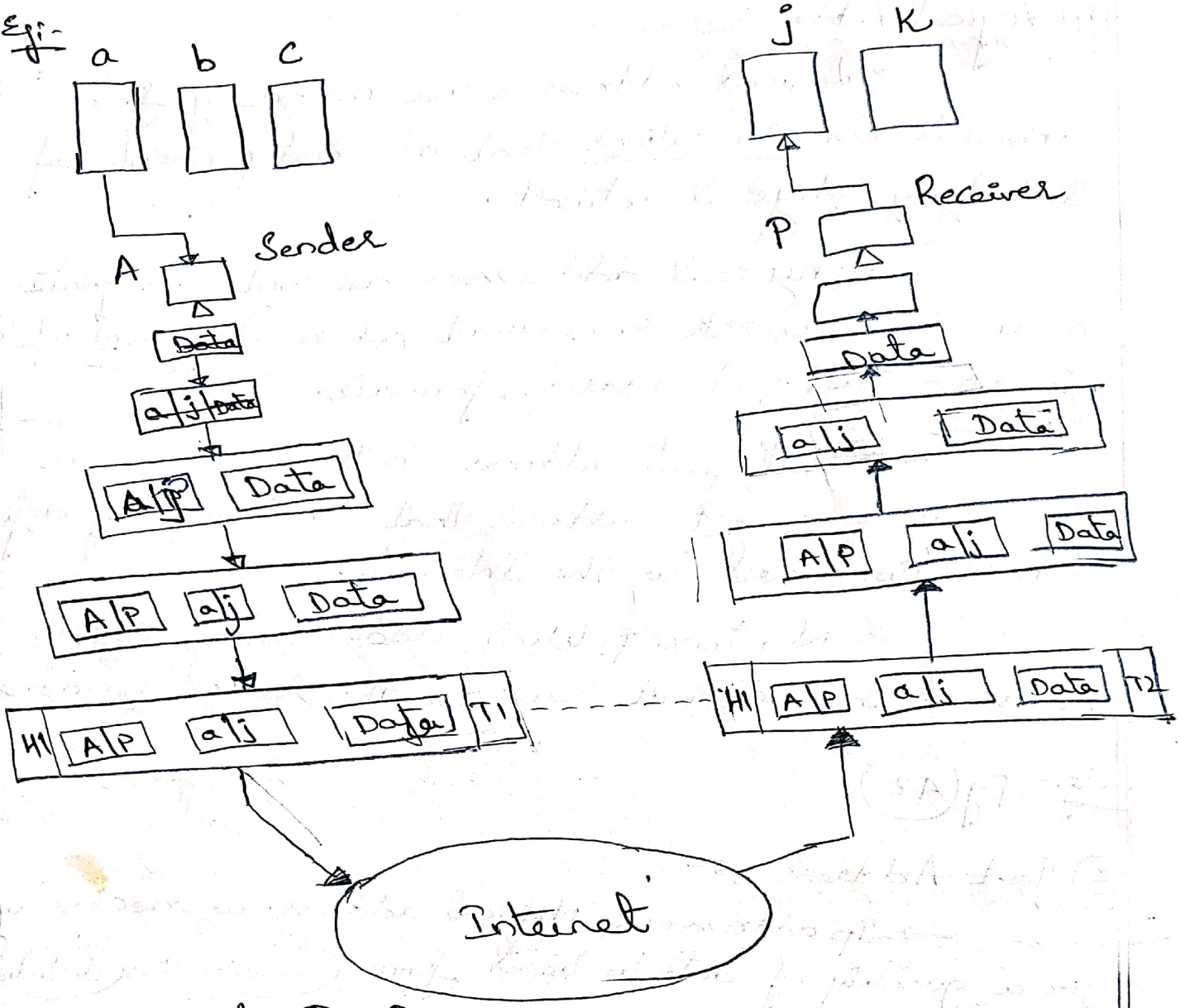


fig ②: Port addresses.

④ Specific Addresses:-

→ Some applications have User-friendly addresses that are designed for specific addresses

Eg:- ① University mail → ~~URL~~ (Universe Resource Locator) E-mail id's → Vinya@gvpce.ac.in, Vinya@gitam.edu.in

② URL's → www.gmail.com, www.youtube.com, www.facebook.com } etc.

Scanned by CamScanner

Examples of Networks:-

1. Novell Netware
2. ARPANET
3. INTERNET

1. Novell Network (Novell NetWare):-

→ The most Popular network System in the PC world is Novell NetWare.

→ It is designed to used by the Companies downsizing from a mainframe to a network of PC's.

→ It is based on client - Server model - PC's Operate as Servers, Providing file Services, database Service, & other Services to clients.

→ The physical and datalink layers can be choosen from among Various industry standards, including Ethernet, IBM token ring and ARC net.

Application	SAP	file Server	...
Transport	NCP	SPX	
network	IPX		
Datalink	Ethernet	Token ring	ARC net
~~Ethernet~~ physics	Ethernet	Token ring	ARC net

Scanned by CamScanner

→ The network layer runs an Unreliable Connectionless internetwork Protocol called Ipx (internet Packet Exchange)

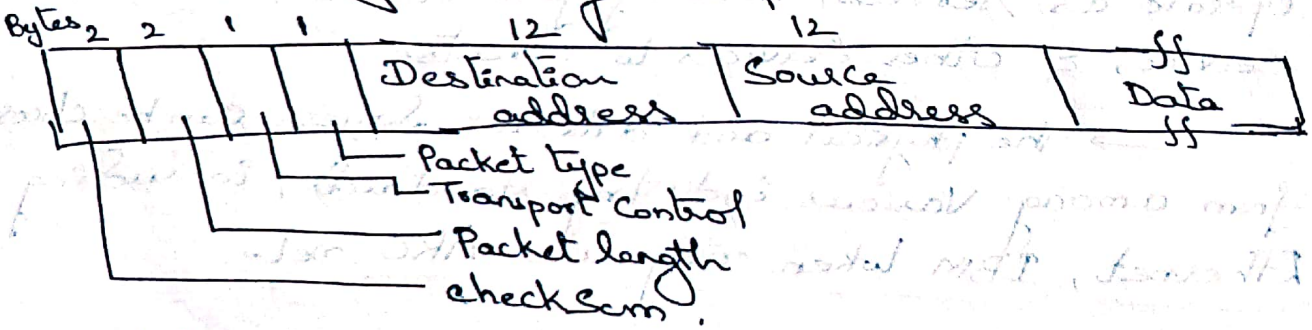
- It Passes Packets transparently from Source to destination, Even if the Source & destination are on different network.

- Ipx is similiar to Ip, Expect that Uses 10-byte addresses instead of 4-bytes addresses.

- Ncp (Network Core Protocol) is a Connection-Oriented Transport Protocol.

- Spx (Sequenced Packet exchange) is also available, but Provides only transport.

→ The format of an Ipx Packet is:



• SAP (Service Advertising Protocol) :-

→ The Packets are collected by special agent Processes running on the router machine. The agents use the information Contained in them to Construct database of which Servers are running where.

→ When a client is booted, it broadcast a request asking where the nearest Server is the agent on local router machine sees the request looks in database for best Server.

Scanned by CamScanner

→ The choice of Server is Send back to the client. The client establishes a NCP Connection with Server. Using this the client & server negotiates the maximum Packet Size.

* Ethernet :- It is a family of Computer networking Technologies for LAN & MAN's.

→ Systems Communicating Over Ethernet divide a stream of data into shorter pieces called frames.

→ Each frame Contains Source & destination addresses & Error-checking data so that damaged data can be detected & re-transmitted.

* Token ring :-

→ LAN technology is a Protocol which resides at the datalink layer (DLL) of the OSI model.

→ It uses a Special 3-byte frame called a token that travel ~~at~~ around the ring.

→ Token Possesion grants the Prossessor Permission to transmit on the medium.

→ Token ring frames travel completely around the loop.

→ Initially used only in IBM Computers, it was Eventually standardized with Protocol IEEE 802.5

→ The data transmission Process is as follows:

- Empty information frames are Continuosly Circulated on the ring. When a Computer has a message to send, it Seizes the token. The Computer will then be able to Send the frame.

Scanned by CamScanner

- The frame is then Examined by Each workstation. The workstation that identifies itself to be the destination for the message copies it from the frame & changes the Token back to 0.
- The frame Continues to Circulate an "Empty" frame, ready to be taken by the workstation when it has a message to Send.
- The token Scheme can also be Used with bus topology LAN'S.

* ARCNET:-

→ It is widely-installed local area network (LAN) technology that uses a token-bus scheme for managing line sharing among the workstations + other devices, connected on the LAN.

→ The LAN Server Continously Circulates Empty message frames on a bus (a line in which Every message goes through Every device on the line & a device uses only those with its address). When a device wants to send a message, it insert a "token" (this can be as Simple as setting a token bit to 1) in an Empty frame in which it also inserts the message.

→ When the destination device or LAN Server reads the message, it resets the token to 0. So, that the frame can be resued by ~~anoth~~ any other device. The Scheme is Very Efficient when traffic increases Since all devices are afforded the same opportunity to use the Shared network.

Scanned by CamScanner

2. ARPANET:-

→ Advance Research Projects Agency (ARPA) had a mission of advancing technology that might be useful to the military.

→ ARPA decided that the network should be Packet-Switched network, Consisting of subnet & host Computers.

→ The subnet would Consists of minicomputers called IMPs (Interface Message Processors) Connected by the transmission lines.

→ The Subnet was to be datagram subnet, so if some lines & IMP's were destroyed, message Could be automatically rerouted along alternative Paths.

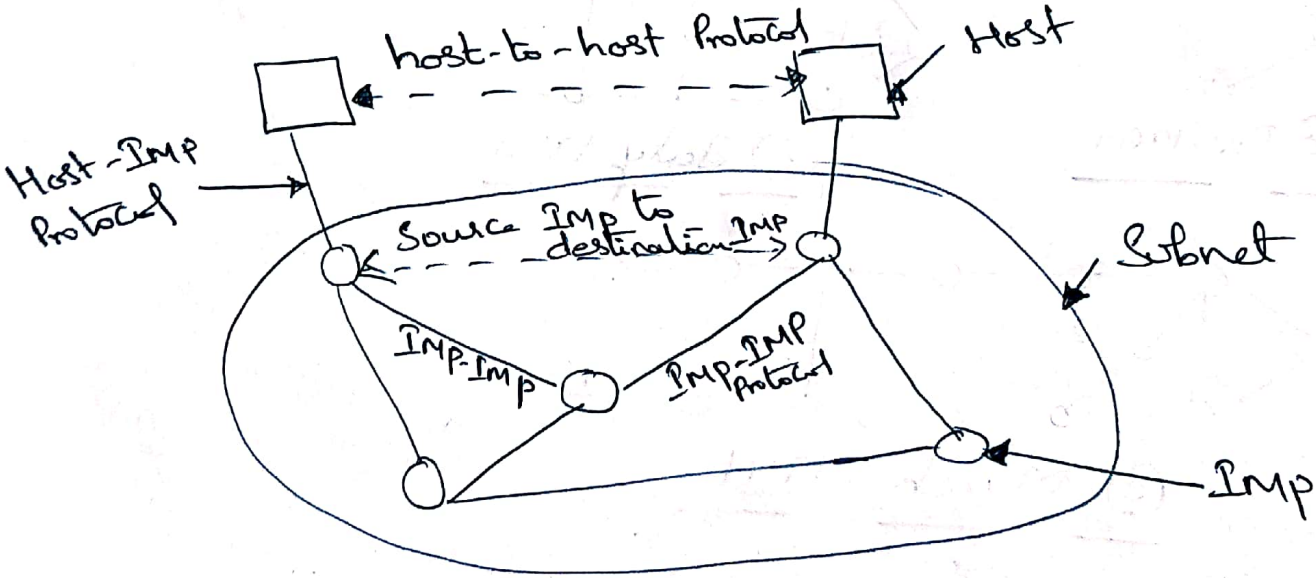


fig: The Original ARPANET design.

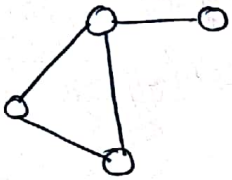
Scanned by CamScanner

→ The Software was Split into two Parts: Subnet & host.

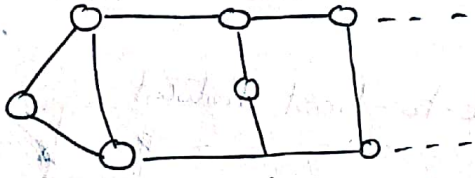
→ The subnet software Consisted of the IMP End of the host-IMP Connection, the IMP-IMP Protocol & a Source IMP to destination IMP Protocol designed to improve reliability.

→ outside the subnet, Software was also needed namely, the host End of the host-IMP Connection, the host-host Protocol, & the application Software.

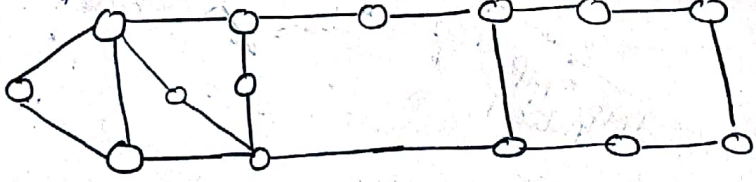
→ Later IMP Software was changed to allow terminals to Connect directly to a specific IMP, called a Tip (Terminal Interface Processor).



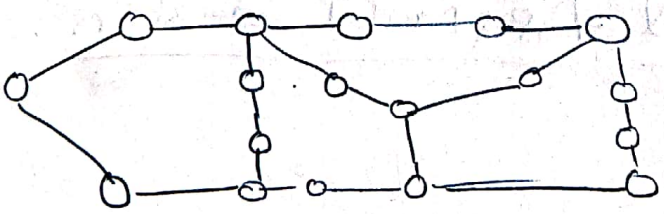
(a) Dec-1969



(b) July 1970



(c) March 1971



(d) April 1972.

Scanned by CamScanner

3 Interest Usage:-

→ Internet refers to collection of different physical networks like LAN, MAN, WAN in order to transmit data from one Computer to another Computer.

(or)

- Internet is network of networks
- E-mail
- News
- Remote login
- file transfer.

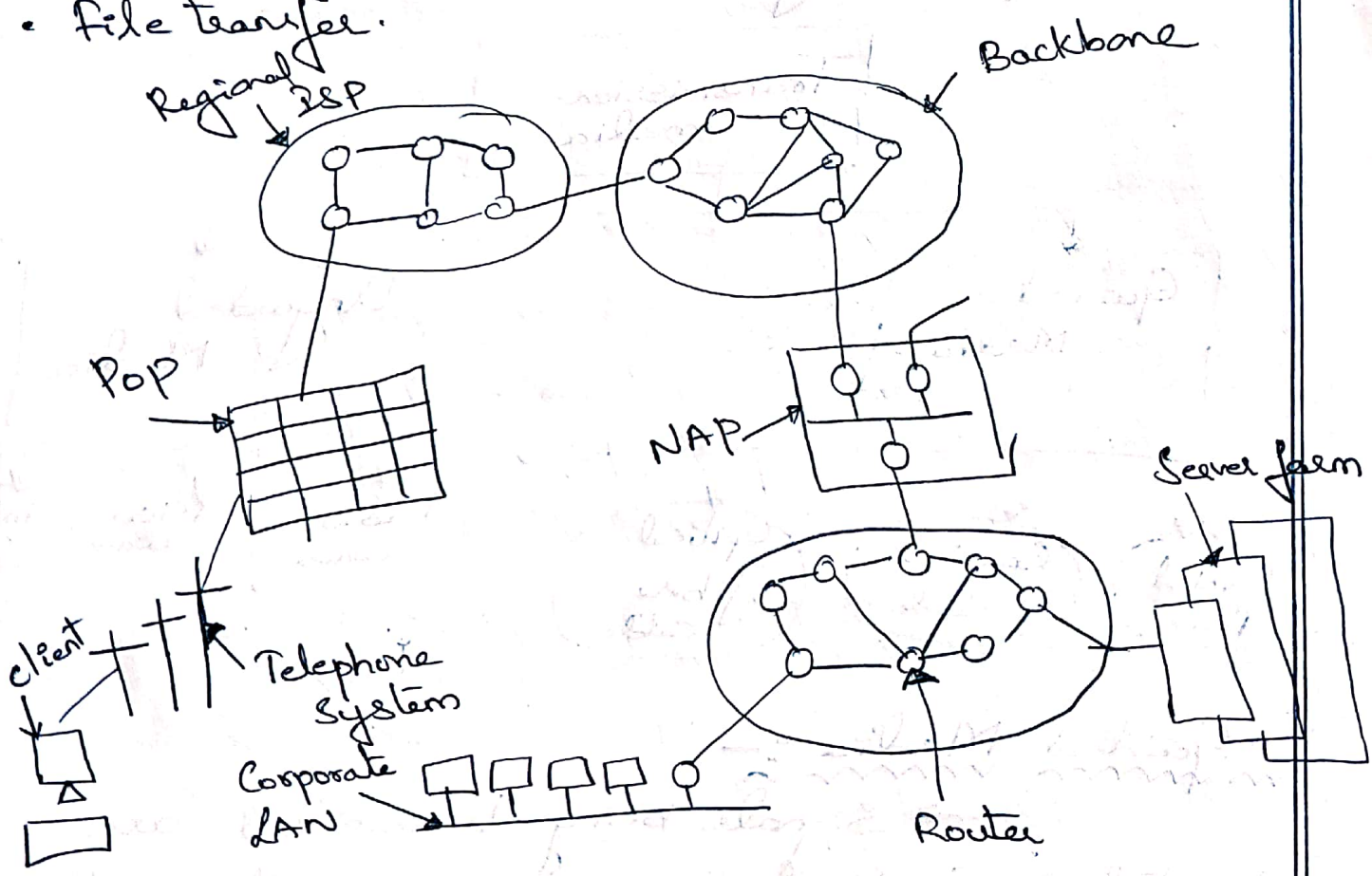


fig:- Overview of Internet

Scanned by CamScanner

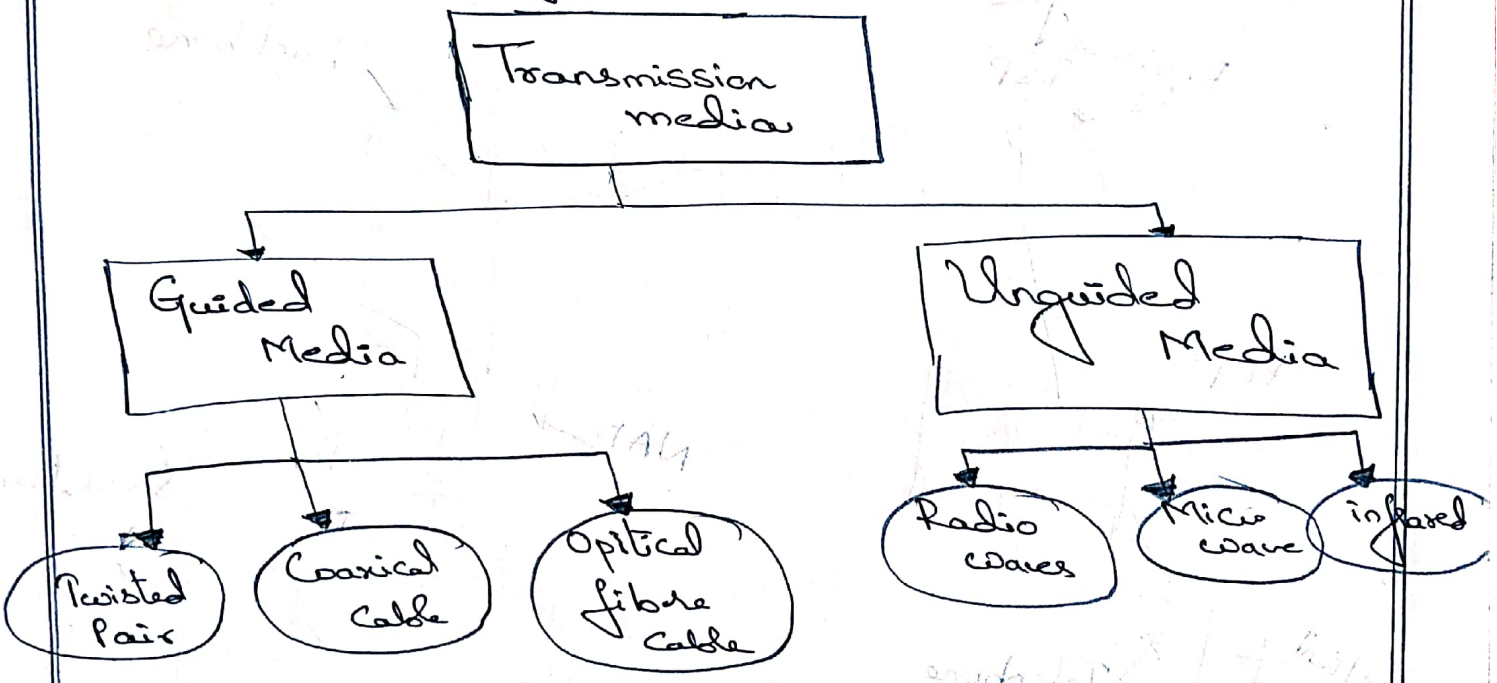
TRANSMISSION MEDIA:-

→ It is a pathway that carries the information from Sender to Receiver.

(or)

→ It is a physical Pathway between the transmitter & the receiver i.e the channel through which data is sent from one place to another.

→ Transmission media is broadly classified into two types. They are.



1. Guided Media :-

→ Signals being transmitted are directed & confined in a narrow pathway using physical links is known as Guided Media.

→ This is also known as Wired or Bounded transmission media.

Scanned by CamScanner

→ High Speed, Secure, Shorter distance (used for) are features of Guided Media.

→ There are 3- major types of Guided Media. They are :-

i. Twised Pair Cable :-

→ This cable is the most Commonly used & is cheaper than others.

→ It is light weight, cheap, Can be installed Easily, & they support many different types of network.

→ Its frequency range is 0 to 3.5 KHZ

→ Typical attenuation is 0.2 dB/km @ 1KHZ

→ Typical delay is 50 μs/km

→ Repeater Spacing is 2km.

→ A twisted Pair Consists of two Conductors (normally Copper), Each with its own plastic insulation, twisted together.

→ One of these wires is used to Carry Signals to receiver, & the other is used only as ground reference.

→ Twisted Pair is of two types. They are:-

(a) Unshielded Twisted Pair (UTP)

(b) Shielded Twisted Pair (STP)

Scanned by CamScanner

* Unshielded Twisted Pair Cable (STP):-

→ This cable has a metal foil or braided-mesh covering which encases each pair of insulated conductors.

→ Electromagnetic noise penetration is prevented by metal chasing.

→ It has same attenuation more expensive than coaxial & unshielded twisted pair.

Adv:-

- Easy to install
- Performance is adequate
- Can be used for Analog or Digital transmission
- Increases the signalling rate
- Higher capacity than unshielded twisted pair
- Eliminates cross talk.

Dis:-

- Difficult to manufacture
- Heavy.

Applications:-

- telephone lines to provide voice & data channels. (DSL lines)
- LAN such as 10 Base-T & 100 Base-T, also use twisted pair cables.

* Unshielded Twisted Pair Cable (UTP):-

→ It is most common type of telecommunication when compared with STP cable, which consists of two conductors usually copper, each with its own colour plastic insulator.

Scanned by CamScanner

→ UTP Cables Consist of 2 or 4 Pairs of twisted Cable. Cable with 2-Pair use RJ-11 Connector & 4-Pair Cable use RJ-45 Connector.

Adv:-

1. Installation is Easy
2. flexible
3. cheap.
4. It has high Speed Capacity
5. 100 meter limit.
6. Higher grades of UTP are Used in LAN technologies like Ethernet.

Dis:-

1. Bandwidth is low when Compared with Coaxial Cable
2. Provide less Protection from interference.

2. Coaxial Cable:-

→ It is called by this name because it Contains two Conductors that are Parallel to Each other.

→ Copper is Used in this as Center Conductor which can be a Solid wire or a Standard One.

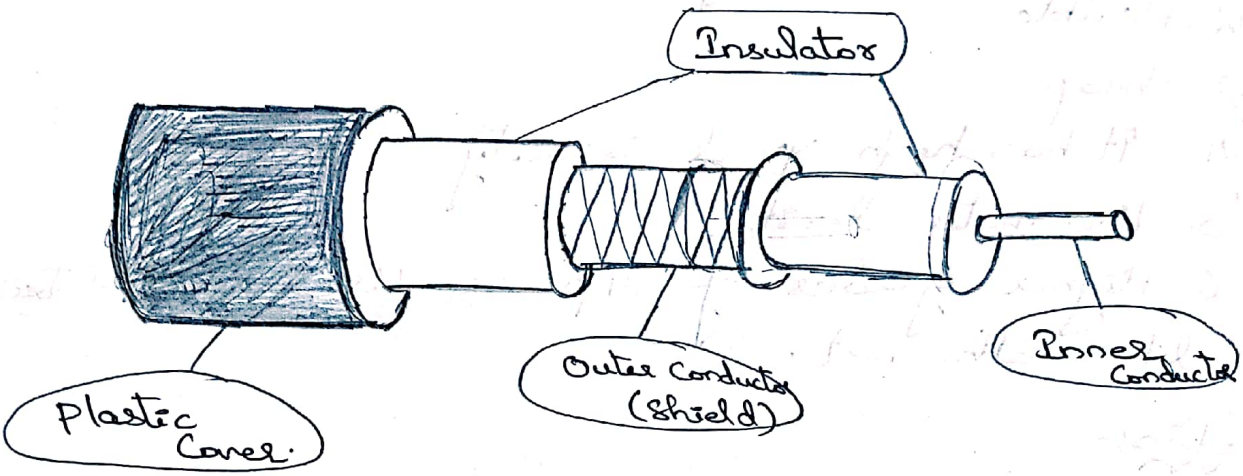
→ It is Surrounded by Pvc installations a Sheet which is Encased in an Outer Conductor of metal foil, braid or both.

→ Outer metallic wrapping is used as a Shield against noise & as the Second Conductor which completes the Circuit. The outer Conductor is also Encased in an insulating sheath. The outermost Part is the plastic Cover which Protects the whole Cable.

Scanned by CamScanner

→ Here the most Common Coaxicial Standards.

- 50-ohm RG-7 or RG-11 : Used with thick Ethernet.
- 50-Ohm RG-58 : Used with thin Ethernet
- 75-Ohm RG-59 : used with Cable television
- 93-Ohm RG-62 : used with ARCNET.



* Coaxial Cable Standards:-

Category	Impedance	Use
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet.

→ There are two types of Coaxial Cables:

1. Base Band:-

→ This is a 50 Ohm (Ω) Coaxial cable which is used for digital transmission. It is mostly used for LAN'S. BaseBand transmits a Single Signal at a time with Very high Speed. The major drawback is that it needs amplification after Every 1000 feet.

2. Broad Band:-

→ This uses analog transmission on Standard Cable television Cabling. It transmists Several Simultaneous

Scanned by CamScanner

Signal using different frequencies. It covers large area when compared with Baseband Coaxial Cables.

Adv:-

1. Bandwidth is high
2. Used in long distance telephone lines
3. Transmits digital signals at a very high rate of 10 Mbps
4. Much higher noise immunity.
5. Data transmission without distortion
6. The can span to longer distance at higher speeds as they have better shielding when compared to twisted pair cable.

Dis:-

1. Single cable failure can fail the entire network
2. Difficult to install & Expensive when compared with twisted pair
3. If the shield is imperfect, it can lead to grounded loop.

Applications:-

1. Analog telephone networks. (i.e 10,000 Voice signals)
2. Traditional cable TV networks (uses RG-59)
3. Traditional Ethernet LAN'S. (10 Base-2, or thin Ethernet uses RG-58).

3. Fiber Optic Cable:-

→ A fiber optic cable is made of glass or plastic & transmits signals in the form of light.

→ fiber optic's propagation can be done in two modes
- Multimode
  - Step-index
  - Graded-index
- Single mode

Scanned by CamScanner

Adv:-

1. Higher bandwidth
2. Less Signal attenuation
3. Immunity to Electromagnetic interference
4. Resistance to Corrosive materials
5. Light weight
6. Greater immunity to tapping

Dis:-

1. Installation & maintenance
2. Unidirectional light Propagation
3. High Cost.

Applications:-

1. often found in backbone networks because its wide bandwidth is Cost-Effective
2. Some Cable TV Cables Companies Uses a Combination of optical fibre & Coaxial Cable thus Create a hybrid network.
3. LAN Such as 100 Base-FX network & 1000 Base-X also use fibre-optic Cable.

2. Unguided Transmission Media:-

→ Unguided medium transport Electromagnetic waves without using a physical Conductor.

→ This is also known as Wireless (or) Un-bounded Transmission Media.

→ Signals are normally broadcast through free space & thus are available to anyone who has a device Capable of receiving them.

Scanned by CamScanner

→ Unguided Signals can travel from the source to the destination in several ways, like ground - Propagation, Sky Propagation & Line - of - Sight Propagation.

→ These Wireless transmission into three broad groups. They are:

1. Radio Waves
2. Micro Waves
3. Infrared Waves.

1. Radio Waves:-

→ Electromagnetic waves ranging in frequencies between 3KHZ & 1GHZ are normally called radio waves.

→ Radio waves are Omnidirectional.

Applications:-

1. The Omnidirectional characteristics of radio waves make them useful for multicasting in which there is one sender but many receivers.
2. AM & FM radio, television, maritime radio, Cordless phones, & Paging are Examples of multicasting.

2. Micro waves:-

→ Electromagnetic waves having frequencies between 1 and 300GHZ are called micro waves.

→ Microwaves are Unidirectional.

Applications:-

1. cellular phones, Satellite networks & Wireless LAN'S.

→ There are 2-types — Terrestrial, Satellite

Scanned by CamScanner

Adv:-

1. Used for long distance telephone Communication
2. Carries 1000's of Voice channels at the same time.

Dis:-

↳ It is Very Costly.

3. Infrared Waves:-

→ Infared waves, with frequencies from 300GHZ to 400THZ, Can be used for short-range Communication.

→ Infrared waves, having high frequencies, Cannot Penetrate walls.

~~Applications:-~~

~~*~~ SWITCHING AND ENCODING ASYNCHRONOUS COMMUNICATION:-

→

SWITCHING:-

→ ~~The~~ In design of phone system, it is Principal Parts are divided into two Parts

* Outside plant (i.e local loops, trunks, etc)
* ~~Inner~~ Inside plant (i.e switches)

→

Scanned by CamScanner

SWITCHING :-

→ To Establish a network

→ A network Consists of many Switching devices.

→ In Order to Connect multiple devices, One Solution Could be to have a Point-to-Point Connection in between Pair of devices, but this increases the no. of Connection.

→ The other Solution Could be to have a Central device & Connect Every device ~~which is~~ to Each other Via the Central device [∴ i.e Star topology].

→ Both these methods are wasteful & impractical for Very large network.

→ The other topology also Cannot be Used at this Stage. Hence a better solution for this Situation is SWITCHING

→ A Switched network is made up of a Series of interconnected nodes Called Switches.

Eg:- In order to design a phone System, it's Principal Parts are divided into two Parts

* Outer Part (i.e local loops, trunks etc)
* Inner Part (i.e Switches)

Scanned by CamScanner

→ Switching Techniques are classified into three types. They are:-

1, Circuit Switching
2, Packet Switching
3, Message Switching.

1. Circuit Switching:-

→ The Process of Establishing a physical Path between Sender device & Receiver device is Known as Circuit Switching.

Eg:- When you & your Computer places a telephone call, the switching Equipment within the telephone system seeks out a physical path all the way from your telephone to receiver telephone.

→ It is generally used in the Public networks.

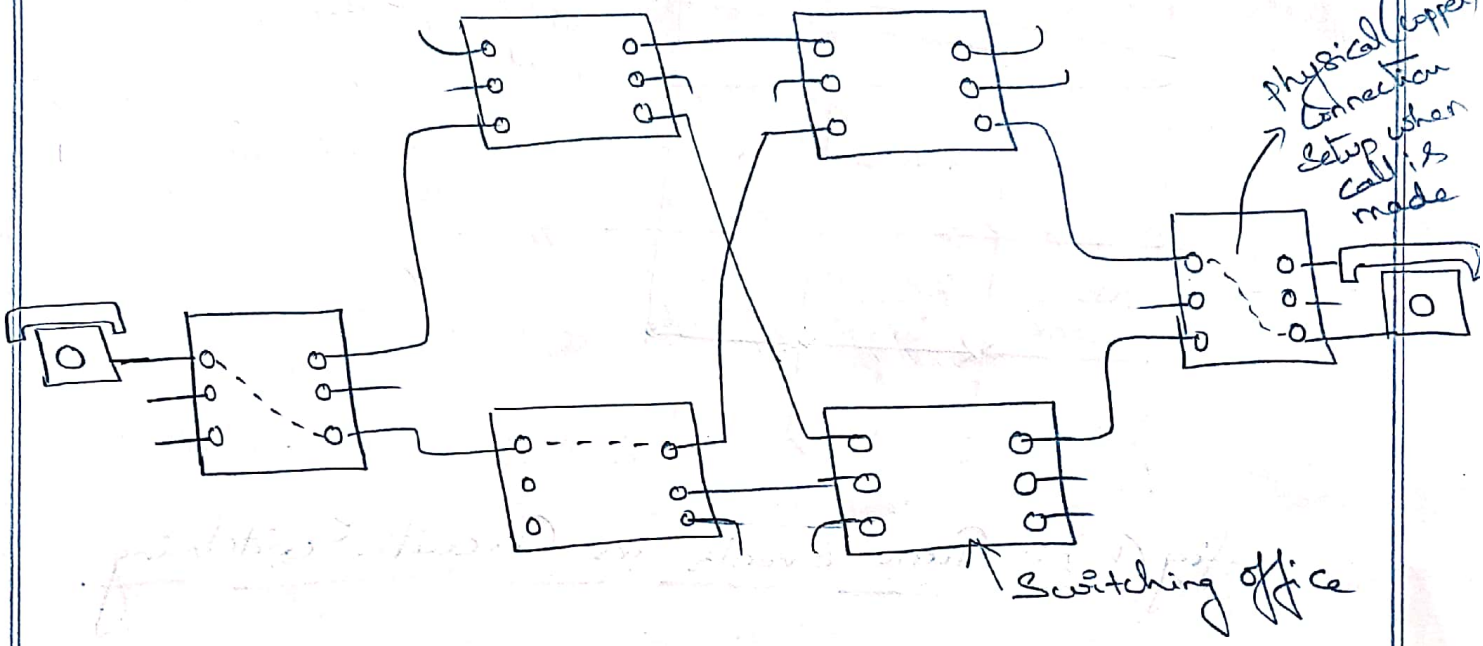
→ It Comes into Existence for handling Voice traffic in addition to digital data.

→ However digital data handling by the use of Circuit Switching methods are proved to be inefficient.

→ The below fig(a) shows, how a physical link (i.e Circuit Switching). Each of the Six rectangles represents a Carrier Switching office (End offices, toll office etc).

Scanned by CamScanner

→ Here, in this Example, Each office has three incoming lines & three outgoing lines. When a call Passes through switch office, a physical connection is (Conceptually) Established between the line on which the call came in and one of the output line. (i.e shown in dotted lines).



→ Here the network connection allows the Electrical Current & the associated voice with it to flow in between the two respective Users. The End to End Communication is Established during the call.

→ Here, the routing decision is made when the path is set up across the given network. After the link has been sets in between the Sender & the receiver then the information is forwarded Continously Over the Provided link.

→ In Circuit Switching a dedicated link/Path is Established between across the Sender & Receiver which is maintained for Entire duration of Conversation.

Scanned by CamScanner

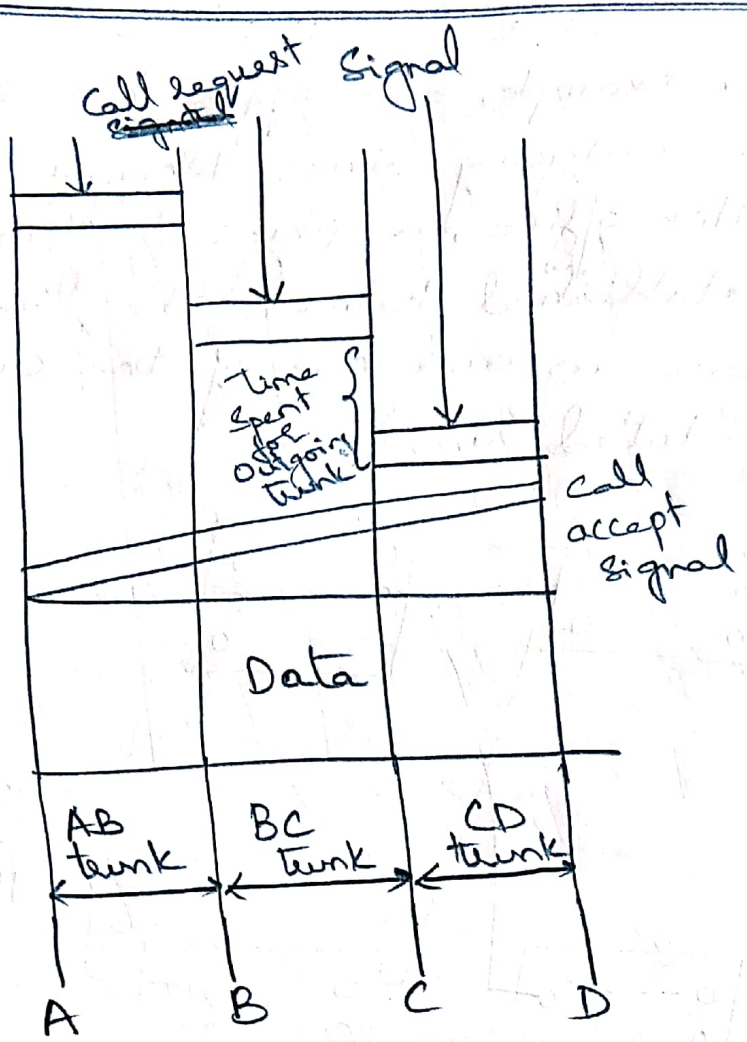


fig (b) :- Time Events in Circuit Switching.

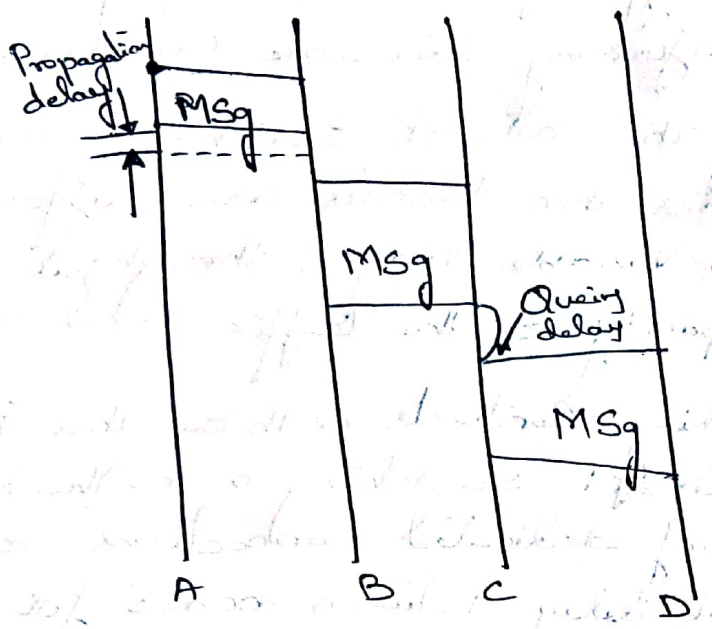
(b) Message Switching:-

→ An alternative switching strategy is message switching.

→ When this form of switching is used, no physical path is established in advance between sender & receiver.

→ Instead, when the sender has a block of data to be sent, it is stored in the first switching office (i.e router) & then forwarded later, one hop at a time. Each block is received in its entirety, inspected for errors, & then retransmitted. A network using this technique is called a store-and-forward network.

Scanned by CamScanner



eg:- telegrams, Paper tape,

fig b: Message Switching

ⓒ Packet Switching:-

→ Here, messages are broken up into Packets & each of which includes a header with Source, destination & intermediate node address information.

→ Individual Packets in Packet Switching technique take different route to reach their respective destination.

→ Independent routing of Packets is done in this case for following reasons:

1. Bandwidth is reduce by the Splitting of data onto different routes for a busy circuit.
2. For certain link in the network, the link goes down during transmission the remaining Packet can be sent through the another route.

Scanned by CamScanner

→ The major advantage of Packet Switching is that they are used for performing data rate conversion.

→ When traversing the network switches, routers or the other network nodes then packets are buffered in the queue resulting in variable delay & throughput depending on the network's capacity & the traffic load on network.

→ Packet switching contrasts with another principal networking paradigm, circuit switching a method which setup a limited no. of dedicated connections of constant bit rate & constant delay between nodes for exclusive use during the communication session.

→ In cases, where traffic fees are charged, for eg in cellular communication, packet switching is characterized by a fee per unit of information transmitted.

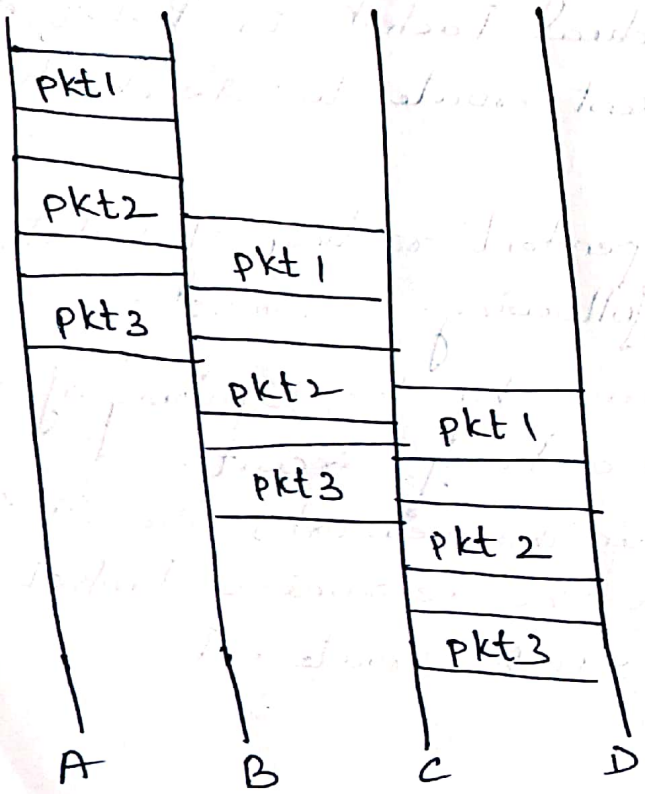
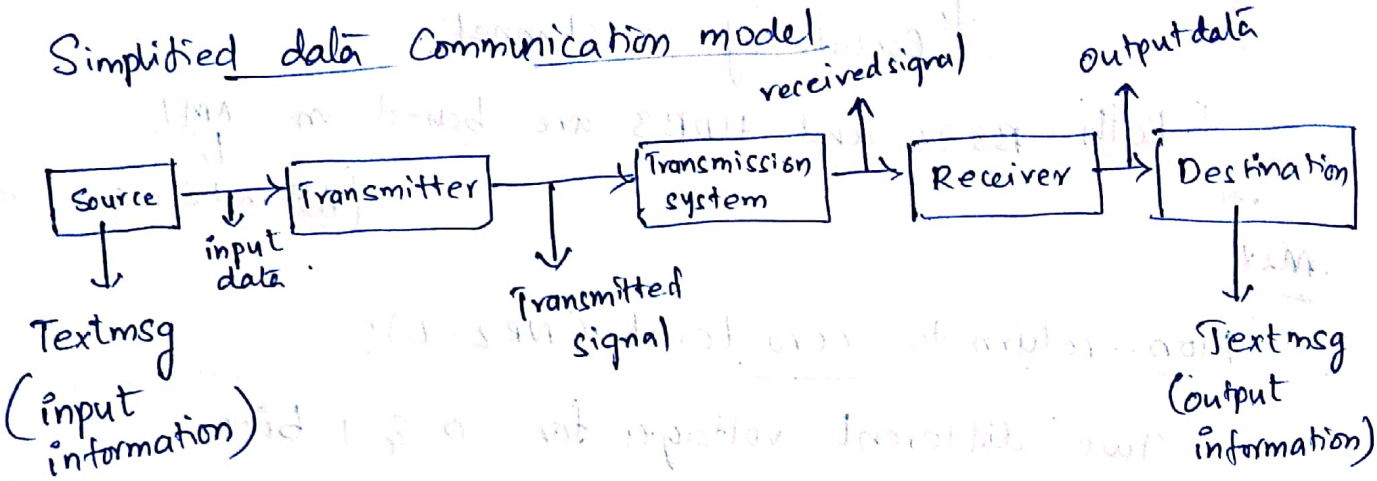


fig (c): Time Event in Packet Switching.

Scanned by CamScanner

Encoding asynchronous Communication:-

Simplified data Communication model



input data → input data is a digital bit stream

Output data → Output data is also digital bit stream

Transmitted signal, Received signal → both are of analog signals

Time period (T) = $\sin(2\pi ft+\phi)$

Analog:- Electric and electromagnetic representation of data

Analog transmission is continous values within some intervals.

Ex:- Sound, video.

Digital:-

Discrete values

Ex:- text, integer.

Encoding schemes:-

Min:-

BSZS:- (Bipolar 8 zero substitution, clear)

Consists of 24 channels

data transmitted through these 24 channels with 64kbps

Scanned by CamScanner

In which 8kbps for synchronous.

HDB3:- High density Bipolar 3.

↓ Consists of 32 channel.

→ Both B8ZS and HDB3 are based on AMI
↓
(Alternate mark Inversion)

Mux:-

→ Non-return to zero-level (NRZ-L):-

→ Two different voltages for 0 & 1 bits

→ voltage constant during bit interval
• No transition (i.e no return to zero voltage)

→ It is used for short distance between terminal and modem or, terminal and computer.

→ NRZ is non inherintly a self clocking signal
addition synchronization → ~~bit~~ bit slips.
ex:- run length limited.

NRZ-I (Non return to zero Inverted)

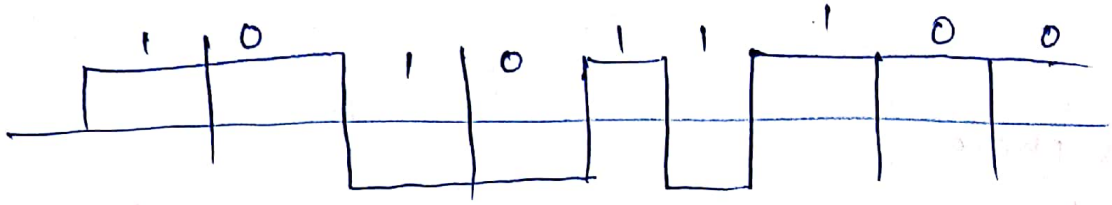
- Non return to zero inverted on ones
- used in bit stuffing
- constant during bit Interval
- Data encoded as presence or absence of signal transtition at begining of bit time.

1 → existence of signal transmission at the begining of the bit time (either low to high & high to low)

0 → no signal transtition at the begining of bit time.

- NRZI is known as differential encoding (i.e signal decoded by comparing the polarity of adjacent signal elements

Scanned by CamScanner



Manchester:

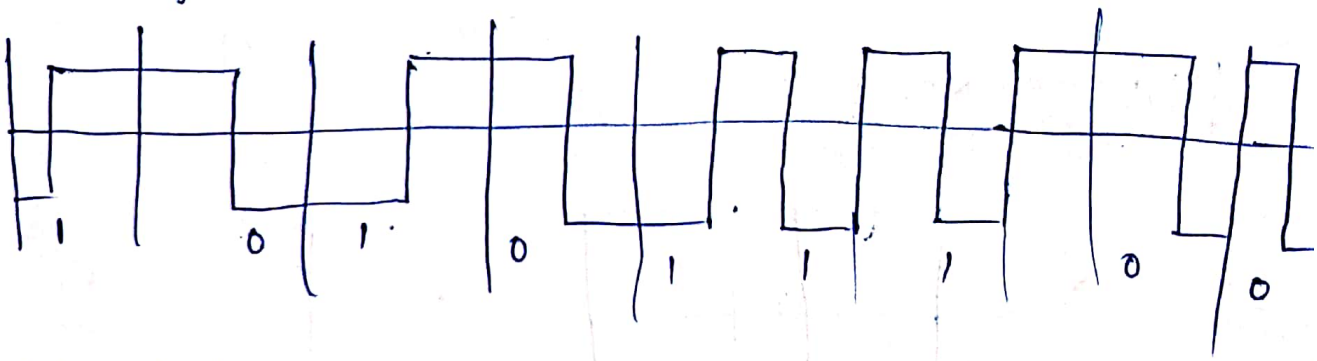
- occur at bit boundary
- transtition at the centre of each bit
- Manchester is also known as Biphase code

  Its two phases are

  1 → low to high

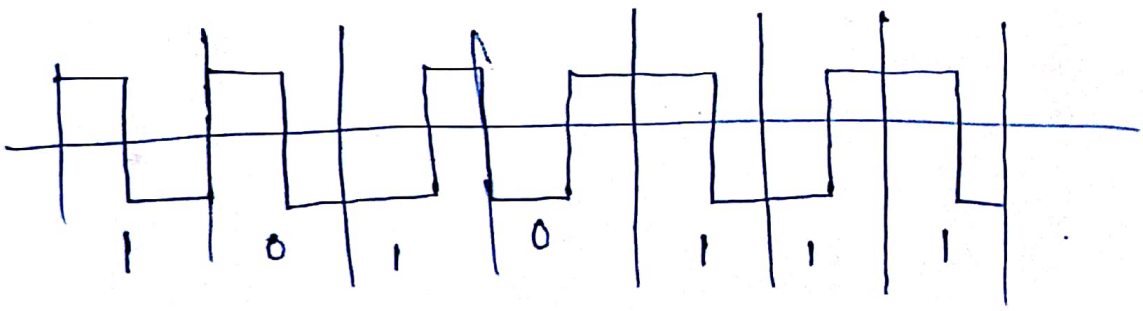
  0 → high to low

- It is a mid bit transtition (used as clocking mechanism)
- The direction of mid-bit transtition represents the digital data.



Differential Manchester

- It is also a mid-bit transtition phase
- In contrast to manchester, in this phase both the ~~course~~ 0's and is are represented in same direction i.e either high to low & low to high. For the next occurance of '0' & '1' direction is reversed.



Scanned by CamScanner

Bipolar :

- In this phase
  '1' → alternating. ~~+1/2~~, ~~-1/2~~ ~~voltage~~ positive and negative voltage
  '0' represents zero voltage
- same issue as NRZ-I
  i.e sequence of 0's
- A systematic problem with ~~pol~~ polar is polarity can be backwards.

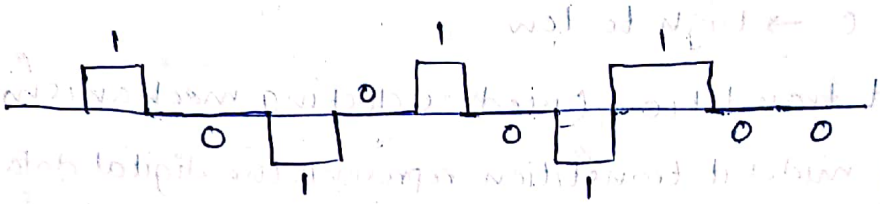
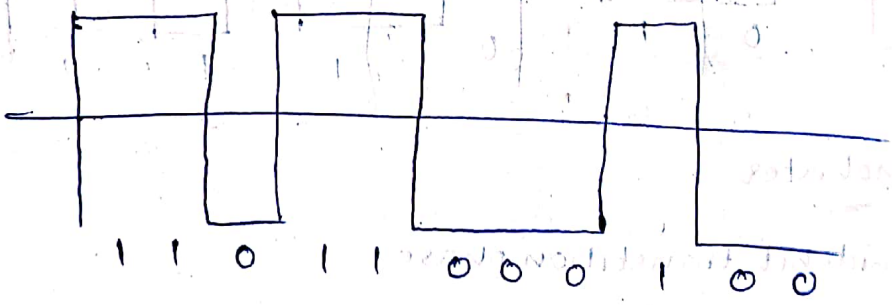


Diagram of NRZ-L



Scanned by CamScanner