Contents

* Introduction to Networks

Data communications.

- When we communicate, we share information. It can be local or remote.
- local communication usually occurs face to face, while remote communication takes place over distance.
  ex:- telephone, telegraph & television → "telecommunication"
  tele means far
- The word "data" refers to information presented in whatever form is ~~agg~~ agreed upon by the parties creating & using the data.
- "Data communications" are the exchange of data b/w two devices via some form of transmission medium such as a wire cable
- For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) & software (program)
- The ~~effectiv~~ effectiveness of a data communications system depends on four fundamental characteristics:

i. Delivery: The system must deliver data to the correct destination, to intended device/user only by that device/user.

ii. Accuracy: The system must deliver the data accurately.

iii. Timeliness: The system must deliver the data in a timely manner.
   ↳ Data delivered late are useless.
   ↳ In case of video & audio, timely delivery means delivering data as they are produced & with out significant delay. This kind of delivery is called "real-time transmission".

iv. Jitter: Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets.

Ex: one packet 30ms delay & other 40ms delay, an uneven quality in the video is the result.

Components of data communication

↳ It has five components

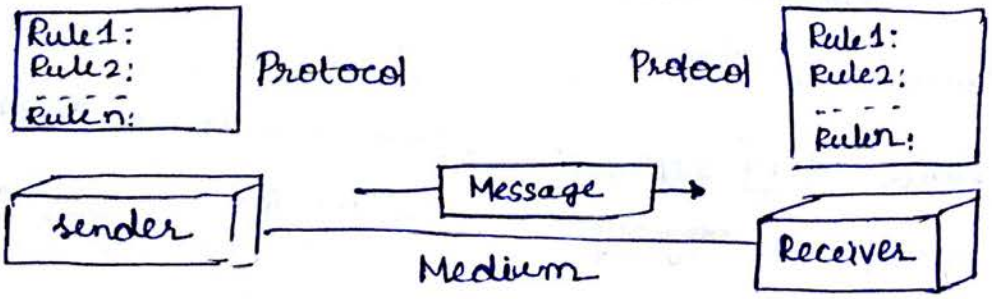


Fig: Five components of data communication

1. Message: The information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio & video.

2. Sender: The sender is the device that sends the data message. It can be a computer, workstation, telephone ~~head~~ handset, video camera, so on.

3. Receiver: The receiver is the device that receives the message.

4. Transmission medium: This is the physical path by which a message travels from sender to receiver. Examples are twisted-pair cabel/wire, coaxial cable, fiber-optic cable & radiowaves.

5. Protocol: A Protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices.

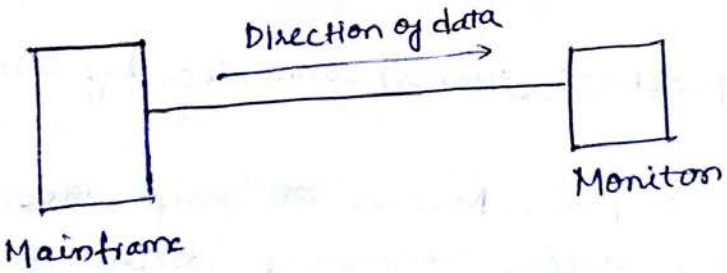
↳ without a protocol, two devices may be connected but not communicating, just a person ~~Sepatts~~ speaks to another person of different language.

Data Representation:

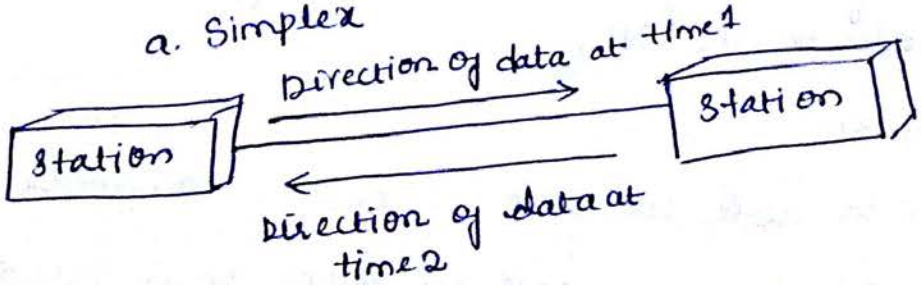
→ Text, numbers, images, audio & video.

Data Flow:

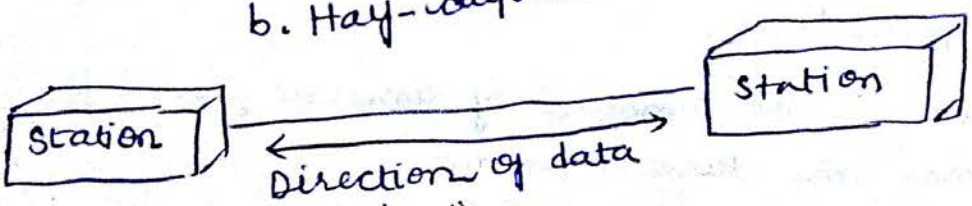
→ Communication between two devices can be simplex, half-duplex, or full-duplex.



a. Simplex



b. Half-duplex



c. Full-duplex

Fig: Data flow (Simplex, half-duplex & full duplex)

Simplex: The communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive.

ex:- keyboards & traditional monitors are examples of simplex devices.

Half_duplex: Each station can both transmit & receive, but not at the same time. When one is sending, other can receive & vice versa.

↳ walkie-talkies & CB (Citizens band) radios are examples.

Full_duplex:

↳ Also called duplex, both stations can transmit and receive simultaneously.

ex: telephone Network. Two people can communicate by a telephone line, both can talk & listen at a same time.

NETWORKS

↳ A N/w is a set of devices (Nodes) connected by communicating 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 N/w.

Network Criteria

↳ A N/w must be able to meet a certain number of criteria.

i) **Performance:** Can be measured in many ways, including transmit time & 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 b/w an inquiry and a response.

↳ The performance of a N/w depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the S/w.

↳ Performance is evaluated by two Networking metrics:
Throughput & delay

* More throughput & less delay.

Reliability: It is measured by the frequency of failure, the time it takes a link to recover from a failure, & the Network's robustness in a catastrophe.

Security: It includes protecting data from unauthorized access, protecting data from damage & development, & implementing policies & procedures for recovery from breaches & data losses.

* Computer Network: It is a connected set of autonomous computers. Normally each computer has its own operating system that is basically a Network operating system.

↳ A CN refers to the collection of several computing machines, Peripherals, & Storage Unit.

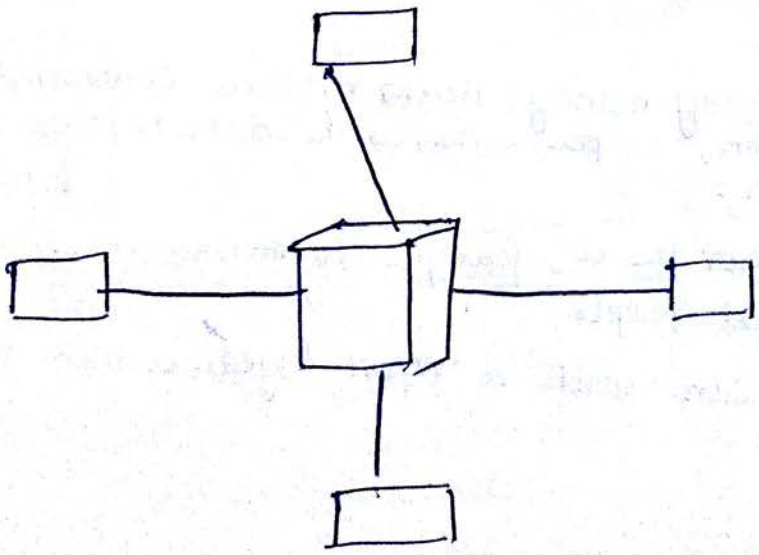


FIG: Computer Network

* Need of Computer Network

1) Provide sharing of resources such as information / processors.
2) Provide inter-process communication among users & processors.
3) To provide distribution of processing functions.
4) To provide centralized control for geographically distributed system.
5) To provide centralized management & allocation of H/w resources
6) To provide compatibility of dissimilar equipment & S/w.
7) To provide N/w users with maximum performance at minimum cost.
8) To provide an efficient means of transport large volumes of data among remote location.

↳ Advantages:-

1. Resource Sharing: The goal is to make all programs, data & equipment available to anyone on the N/w without regards to the physical Location of the resource and the user.

2. High Reliability: N/w provides high quality alternative sources of supply.

Ex:- Replication of two or more files in machines, failure of one machine data available in another.

3. Low cost / Saving money: Build systems consisting of powerful Personal computers, as per user, with data kept on one/more shared file server machines

4. Communication:

It can provide a Powerful communication medium among widely separated people.

Ex:- Two people can write a report together who live far apart on Online.

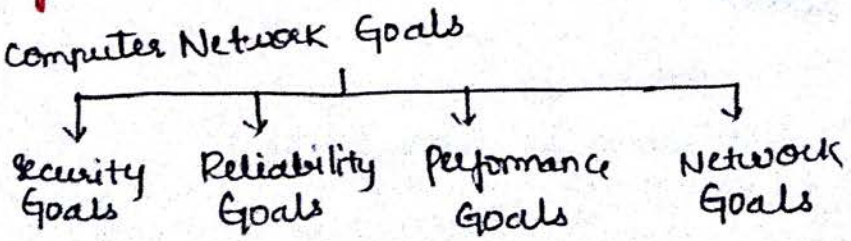
* Uses/Applications:

1) Access to remote programs :- BMI & Owner client > Same site / Program access
2) Access to remote data bases :- Railway Reservation at home
3) Value - added communication facilities: High-quality communi-cation facilities tend to reduce the need for physical proximity. Everyone in the world, have an ability to send & receive electronic mail.
4) Using for entertainment Purpose.
5) Accessing the information systems like world wide web, which contain -s almost any information.

* Disadvantages

1) Set up cost (Hardware / software) in Network: Setting up a N/w requires an investment in h/w & s/w, as well as funds for Planning, designing & implementing the Network.
2) Security concerns: More systems are connected to the internet, the more potential exposure to security risk. {unauthorised, hackers}
3) Unwanted sharing: It also allows sharing of undesirable data. "sharing problem" in this regard means viruses, which can spread easily over Network.
4) Illegal behaviour: Like unwanted sharing of information or data, N/w facilities useful connecting & communication but also brings difficulties with it problems including abuse of resources distractions that reduce productivity, downloading of illegal or illicit materials & S/w piracy.

* Goals of CN



1) Security Goals: N/w security issues comprises of prevention from virus attacks & protecting data from unauthorized access.

* Viruses:
  - ↳ As a N/w is accessible from many points, it can be susceptible to computer viruses.
  - ↳ A virus is an illicitly introduced code to damage the function -ality of a system.
  - ↳ A Good Network is protected from viruses by s/w & h/w designed specifically for that purpose.

* Unauthorized access: protection from unauthorized access of sensitive data is mandatory for any N/w to be useful.
  - ↳ protection can be accomplished at a number of levels.
    - lowest level → User login codes & Passwords.
    - High level → encryption techniques.

2) Reliability Goals: It is measured by failure frequency average down time of N/w & the N/w's robustness in a catastrophe.

a) Failure frequency: It is always a possibility. A N/w fails rarely is good for a user, but if it fails oftenly is of little value to a user.

b) Average Down Time: How long does it takes to restore service is known as down-time for the N/w. A N/w with less average down-time is more useful than one that does not.

c) Catastrophe: N/w must be protected from catastrophe event such that earthquake or theft. One protection against these is a reliable system to backup N/w software.

3) Performance Goals: The N/w performance can be measured by its Transit time & response time.

↳ N/w performance depends on a number of factors including, N/w transmission medium, Network hardware, N/w software & traffic load.

(a) N/w Transmission Medium: A N/w medium may be wired (optical fiber, copper cables, etc..) or wireless (microwave, satellite etc.,).

↳ As N/w are increasing, fastr & faster transmission media is required for Network; such as fiber optic cabling.

(b) Hardware: The types of hardware included in a N/w affect both speed & capacity of transmission. A higher speed system with greater storage capacity provides better performance.

(c) Software: Moving a message from node to node through a N/w requires processing for transformation of raw data into transmittable signals, to route these signals to the proper destination, to ensure error free delivery & to recast the signals into a form the receiver can use.

↳ The S/w that provides these services affects both the speed & the reliability of a N/w link.

↳ Well-designed S/w can speed the process & make transmissi -on more effective & efficient.

(d) Traffic Load: The design of a N/w is based on an assessment of the average Number of users that will be communicating at any moment of time. Having a large number of concurrent users can slow response time in a N/w not designed to coordinate heavy traffic loads. In peak load periods however the "actual Number of users" may exceed the "average Number of users" and thereby detoriate the performance. How a N/w

responds to peak loads is a measure of its performance.

e) N/w cost: N/w cost is import for designing.

N/w cost < fixed cost
Runtime cost.

a) fixed cost: The cost of medium & devices.

b) Runtime cost: To maintain a H/w functionally strong, very good maintenance is required and as much complexity we increase in design chances of failure increases accordingly which in turn leads to more down time & maintenance cost of N/w.

↳ so increasing the runtime cost of N/w. so while designing not only fixed cost but runtime costs must be taken into account for minimization of total cost.

Physical Structures.

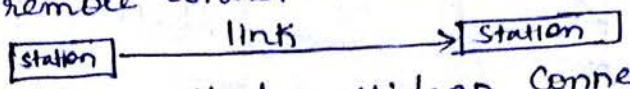
↳ Types of Connection

* A N/w is two or more devices connected through links.
* A link is a communications pathway that transfers data from one device to another.
* 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
  2) Multipoint.

Point-to-point: provides a dedicated link between two devices. ~~must be connected in some way to the same link at the same time~~ The entire capacity of the link is reserved for transmissi-on b/w those two devices.

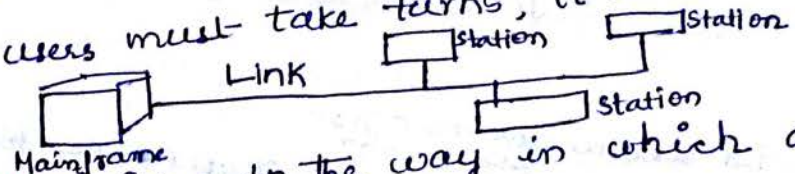
↳ Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible.

Ex: When you change television channels by infrared remote control, you are establishing a point-to-point connection b/w the remote control & the television's control system.



Multipoint: Also called multidrop connection is one in which more than two specific devices share a single link.

↳ In a multipoint environment, the capacity of the channel is shared, either spatially or temporarily. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a time shared connection.



Physical topology: Refers to the way in which a N/w is laid out physically. Two or more devices connect to a link; two or more links form a topology.

↳ The topology of a N/w 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: Mesh, star, bus & ring.

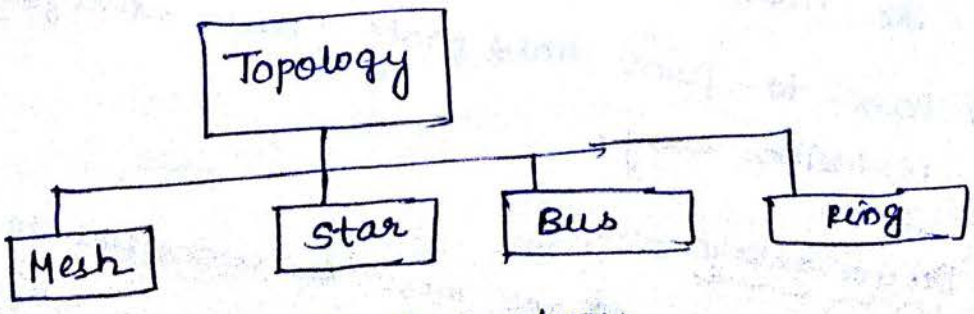


Fig: Categories of topology

↳ Mesh Topology: Every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only b/w the two devices it connects.

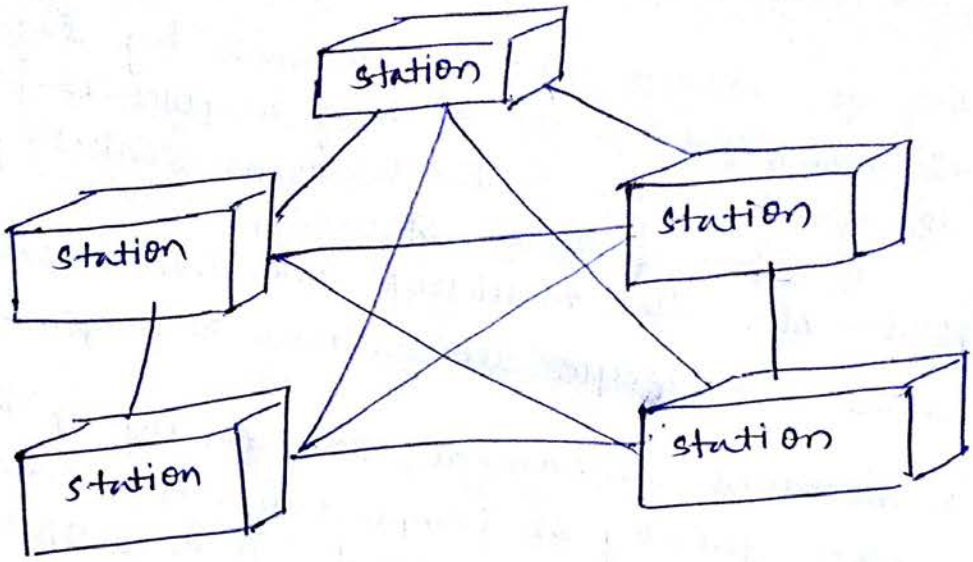


Fig: Mesh Topology

↳ It provides several advantages:

1) The use of dedicated links guarantees that each connection can carry its own data load, thus elimination of traffic problems.
2) It is robust. If one link becomes unusable, it does not incapacitate the entire system.
3) There is the advantage of privacy or security. when every message travels along a dedicated line, only the intended recipient sees it.
4) Point-to-point links make fault identification & fault isolation easy.

↳ Disadvantages:

1) Because every device must be connected to every other device, installation and reconnection are difficult.
2) the sheer bulk of the wiring can be greater than the available space can accomodate.

3) the h/w required to connect each link (I/O ports and cable) can be prohibitively expensive.

↳ Star Topology: Each device has a dedicated point-to-point link only to a central controller, usually a hub.

↳ The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.

↳ A star topology is less expensive than a mesh topology.

Advantages:

1) Each device needs only one link and one I/O port to connect it to any number of others.

2) Robustness: If one link fails, only that link is affected. All other links remain active.

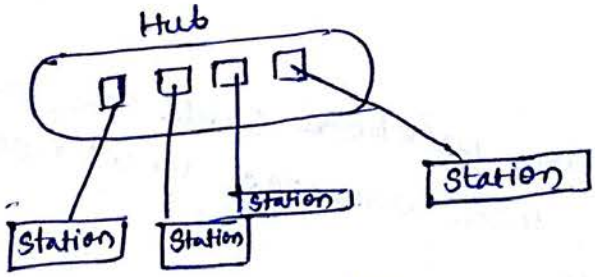


Fig:- Star topology

disadvantages:

1) Dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.

↳ Star topology is used in Local-area networks (LANs) High-speed LANs often use a star topology with a central hub.

↳ Bus topology: A bus topology, on the other hand, is multipoint. One long cable acts as a backbone to link all the device in a N/w.

↳ Nodes are connected to the bus cable by drop lines & taps.

↳ A dropline is a connection running b/w the device & the main cable.

↳ A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.

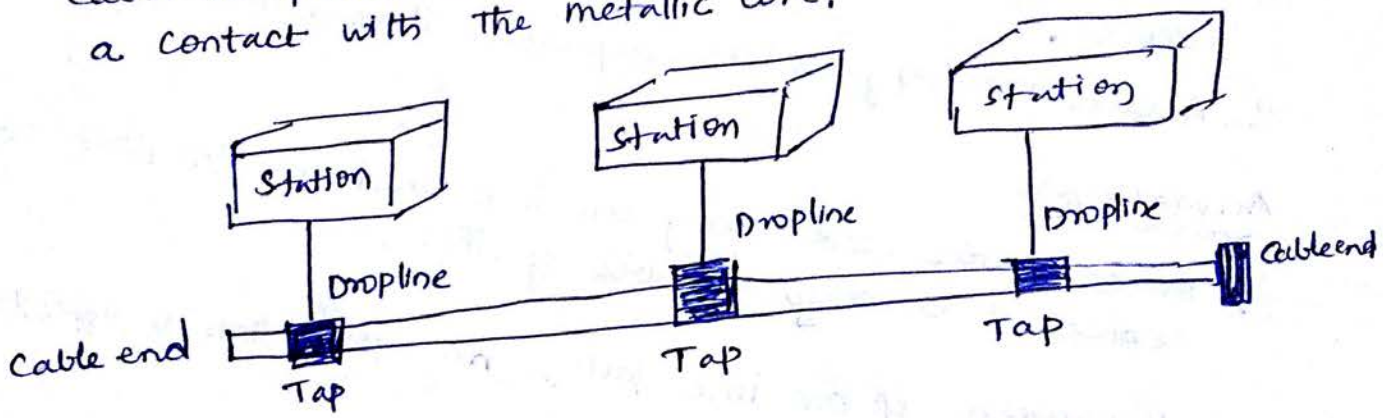


Fig:- Bus topology

advantages:

1) Ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop line of various lengths.

2) redundancy is eliminated.

disadvantages:

1) Difficult reconnection & fault isolation.

2) A fault or break in the bus cable stops all transmission, even between devices on the same side of the problem.

3) Bus topology was the one of the first topologies used in the design of early local area Network.

↳ Ring Topology: Each device has a dedicated point-to-point connection with only the two devices on either side of it.

↳ A signal is passed along the ring in one direction, from device to device, until it reaches its destination.

↳ Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits & passes them along.

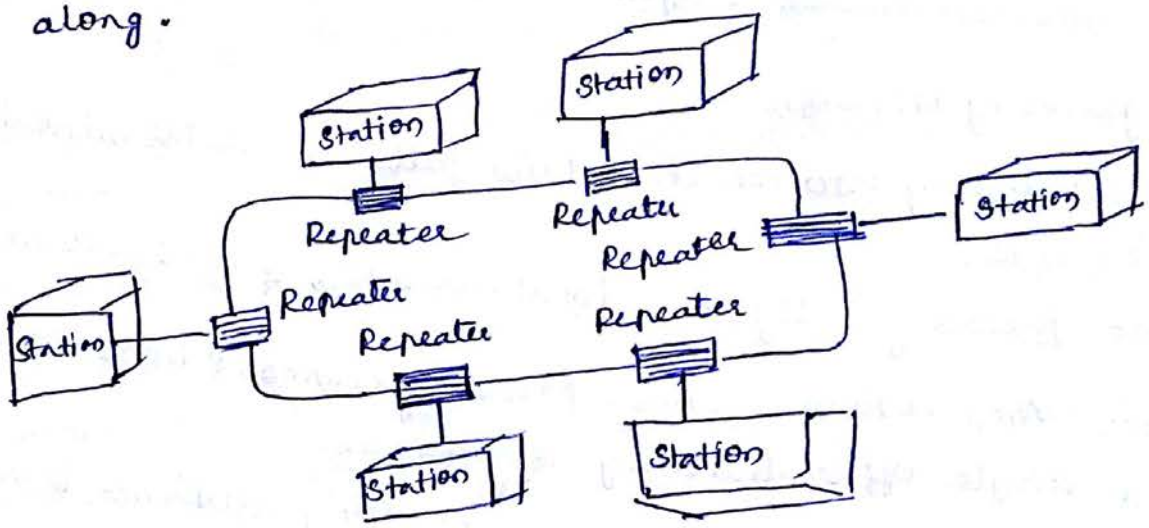


FIG: Ring topology

advantages

1) A ring is relatively easy to install & reconfigure.
2) Fault isolation is simplified.

disadvantages

1) Unidirectional traffic can be a disadvantage.

↳ Hybrid Topology: A N/w can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology.

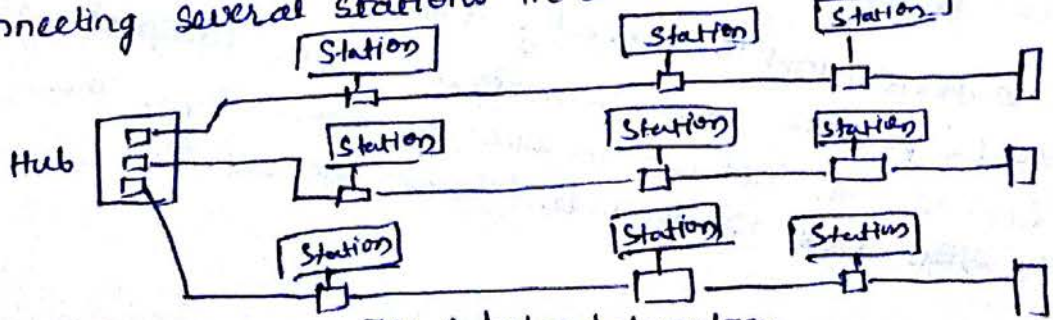


Fig: A hybrid topology

* Network Models

↳ standards are needed so that heterogeneous N/ws can communicate with one another.

↳ the two best-known standards are the OSI model & the Internet model.

↳ The OSI (Open Systems Interconnection) model defines a seven-layer N/w

↳ The internet model defines a five-layer N/w.

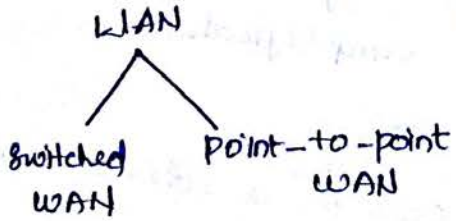
* Categories of Network

↳ the category into which a N/w falls is determined by its size.

↳ two primary categories: Local-area N/w & wide-area N/w.

* Local Area Network (LAN): Privately owned & links the device in a single office, building, or campus.

* Wide Area Network (WAN): provides long distance transmission of data, image, audio & video information over large geographic areas that may comprise a country, a continent, or even the whole world.



↳ the switched WAN connects the end systems, which usually comprise a router (internetworking 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). this type of WAN is often used to provide Internet access.

INTERNET

↳ When two or more Networks are connected, they become an internetwork, or internet.

* The internet

↳ The internet has revolutionized many aspects of our daily lives.

↳ The internet is a communication system that has brought a wealth of information to our fingertips & organized it for our use.

↳ The internet is structured, organized system.

* A brief history

↳ A N/w is a group of connected communicating devices such as computers & printers.

↳ An internet is two or more Networks that can communicate with each other.

↳ The most notable internet is called the Internet, a collaboration of more than hundreds of thousands of interconnected networks.

↳ This extraordinary communication system only came into being in 1969.

↳ In the mid-1960s, mainframe computers in research organizations were standalone devices.

↳ computers from different manufacturers were unable to communicate with one another.

↳ The Advanced Research projects Agency (ARPA) in the department of Defense (DOD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs & eliminating duplication of effort.

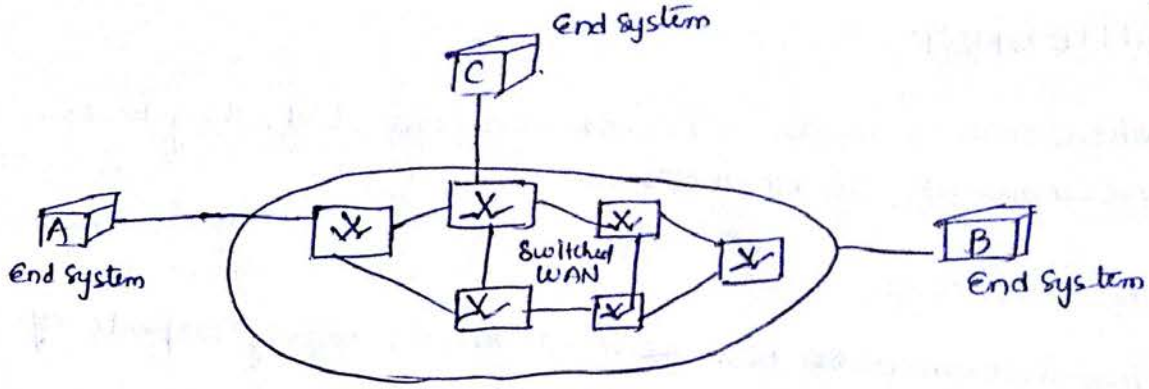


Fig: Switched LIAN

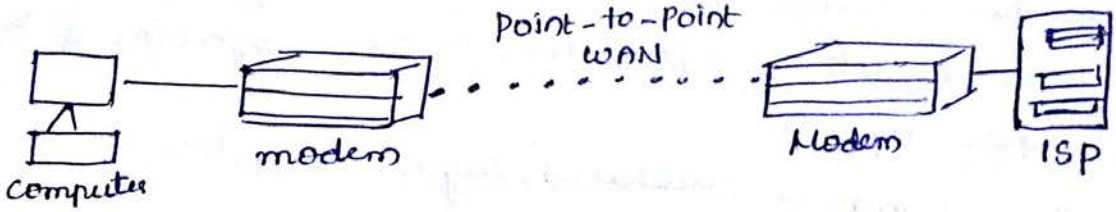


Fig: point-to-point LIAN

Metropolitan Area Network (MAN) is a N/w with a size between a LAN & 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, & have endpoints spread over a city or part of city.

ex:- Telephone company N/w that can provide a high-speed DSL line to the customer.

↳ In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for ARPANET, a small network of connected computers.

↳ The idea was that each host computer would be attached to a specialized computer, called an interface message processor (IMP). The IMPs in turn would be connected to one another. Each IMP had to be able to communicate with other IMPs as well as with its own attached host.

↳ By 1969, ARPANET was a reality. Four nodes at UCLA, UCSB, SRI & University of Utah, were connected via the IMPs to form a N/w. Software called the Network control protocol (NCP) provided communication between the hosts.

↳ In 1972, Vint Cerf & Bob ~~bb~~ Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the Internetting project. Cerf & Kahn's landmark 1973 paper outlined the protocols to achieve end-to-end delivery of packets. This paper on Transmission control protocol (TCP) included concepts such as encapsulation, the datagram, and the functions of a gateway.

↳ Shortly there after, authorities made a decision to split TCP into two protocols:

↳ Transmission Control protocol (TCP)
↳ Internetworking protocol (IP).

↳ IP would handle datagram routing while TCP would be responsible for higher-level functions such as segmentation, reassembly, and error detection. The internetworking protocol becomes known as TCP/IP.

⇒ The Internet Today

↳ The Internet has come a long way since 1960's.

↳ The Internet today is not a simple hierarchical structure.

↳ It is made up of many wide- and local-area Networks joined by connecting devices & switching stations.

↳ TO day most 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.

↳ The Internet today is run by private companies, not the government

* International Internet Service providers :-

At the top of the hierarchy are the international service providers that connect nations together.

* National Internet service providers :- These are backbone N/w's created & maintained by specialized companies. There are many national ISPs Operating in North America.

↳ TO provide connectivity blw the end users, these back bone N/ws are connected by compter switching stations called Network Access points (NAP)s.

↳ Some national ISP n/w are also connected to one another by private switching stations called peering points. These normally operate at a high data rate.

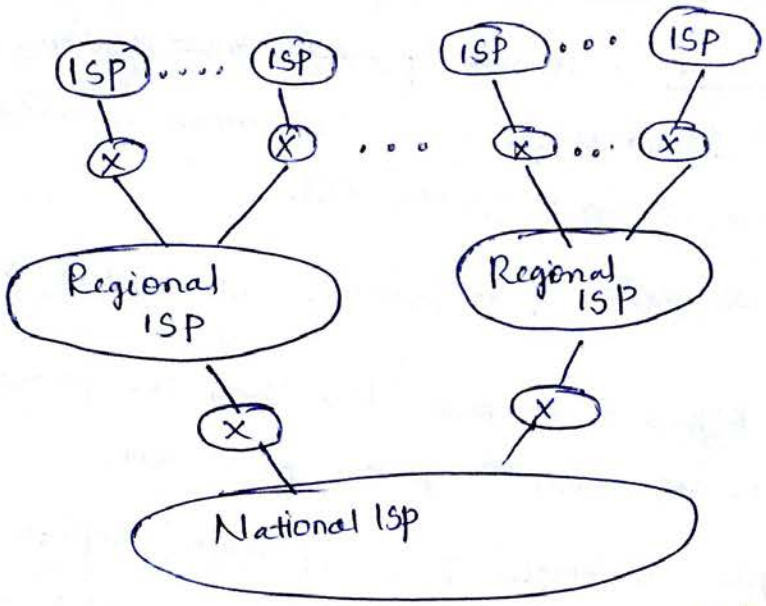
* Regional Internet Service providers

↳ Regional ISPs are smaller ISPs that are connected to one or more national ISPs.

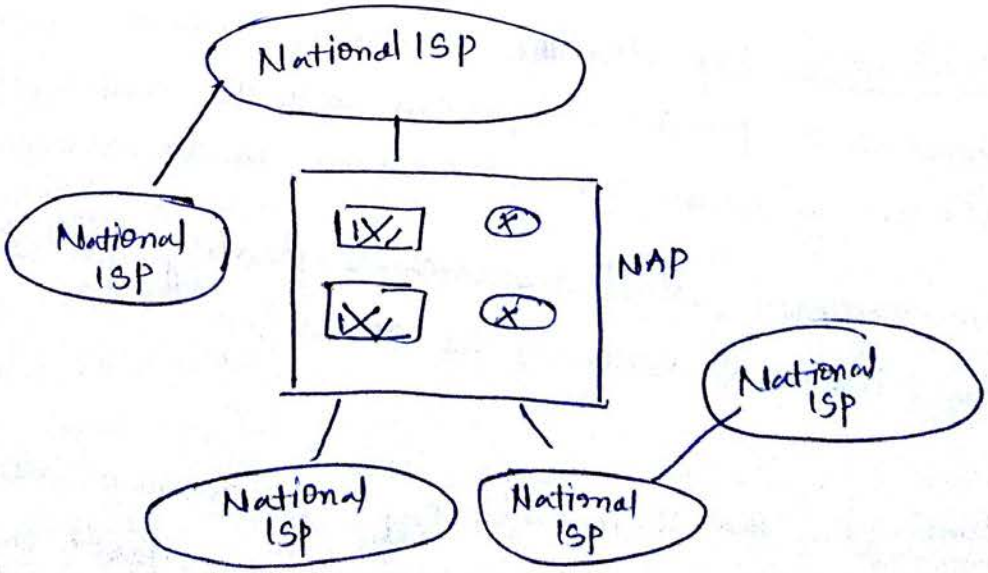
↳ They are at the third level of the hierarchy with a smaller data rate.

* Local Internet Service Providers

↳ Local Internet service providers provide direct service to the end users. The local ISPs can be connected to regional ISPs or directly to national ISPs. Most end users are connected to the local ISPs. These local ISPs can be connected to a regional or national service provider



a: Structure of a national ISP



b: Interconnection of national ISPs

Fig: Hierarchical Organization of the Internet

PROTOCOLS AND STANDARDS

* Protocols

↳ In computer N/ws, communication occurs b/w entities in different systems.

↳ An entity is ~~any thing~~ anything capable of sending or receiving information.

↳ For communication to occur, the entities must agree on a protocol.

↳ A protocol is a set of rules that govern data communications.

↳ A protocol defines what is communicated, how it communicated, and when it is communicated.

↳ The key elements of a protocol are syntax, semantics, & timing.

* Syntax :- Refers to a ~~the~~ structure or format of the data, meaning the order in which they are presented.

For Example, a 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 :- Refers to the meaning of each section of bits. ~~How~~ How is a particular pattern is to be interpreted, and what actions is to be taken based on that interpretation?

For Example, does an address identify the route to be taken or the final destination of the message?

* Timing :- The term timing refers to two characteristics: when data should be sent and how fast they can be sent.

↳ For example, if a sender produces data at 100Mbps but the receiver can process data at only 1Mbps, the transmission will overload the receiver & some data will be lost.

* Standards

↳ standards are essential in creating & maintaining an open & competitive market for equipment manufacturers & in guaranteeing national & internal interoperability of data & telecommunications technology and processes.

↳ They provide guidelines to manufacturers, vendors, government agencies and other service providers.

↳ Data communication standards fall into two categories: de facto (meaning "by fact")

de jure ("by law" or "by regulation")

* Defacto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.

* De jure. Those standards that have been legislated by an officially ~~creation committees, &~~ recognized body.

* Standard organizations

↳ standards are developed through the cooperation of standards creation committees, forums, and government regulatory agencies

Standards Creation committees

1) International organization for standardization (ISO).
2) International Telecommunication Union - Telecommunication standards Sector (ITU-T).
3) American National Standards Institute (ANSI)
4) Institute of Electrical & Electronics Engineers (IEEE)
5) Electronic Industries Association (EIA).

~~* Forums Forum~~

* Forums

The Forms work with universities & users to test, evaluate & standardize new technologies. By acceptance & use of those technologies in the telecommunications community. the forums present their conclusions to the standard bodies.

* Regulatory Agencies.

All communications technology is subject to regulation by government agencies such as the Federal Communications commission (FCC) in United states.

↳ the purpose of these agencies is to protect the public interest by regulating radio, television & wire/cable communication.

Internet Standards

↳ An Internet standard is a thoroughly Tested specification that is used to and adhered to by those who work with the Internet.

↳ An Internet draft is a working document with no offical status and a 6-month lifetime.

↳ Upon recommendation from the Internet authorities, a draft may be published as a Request for Comment (RFC).

↳ Each RFC is edited, assigned a number, and made available to all interested parties.

↳ RFCs go through maturity levels & are categorized according to their requirement level.

The OSI Model

↳ A N/w is a combination of hardware & software that sends data from one location to another.

↳ The hardware consists of the physical equipment that carries signals from one point of the Network to another.

↳ The software consists of instruction sets that make possible the services that we except from a N/w.

Hierarchy

↳ The Open Systems Interconnection (OSI) model was first introduced in the late 1970's.

↳ An Open System is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.

↳ The purpose of the OSI model is to show how to facilitate communication b/w different systems without requiring changes to the logic of the underlying hardware / software.

↳ The OSI model is not a protocol; it is a model for understanding & designing a N/w architecture that is flexible, robust and interoperable.

↳ The OSI model is a layered framework for the design of Network systems that allows communication b/w all types of computer systems.

↳ It consists of seven separate but related layers, each of which defines a part of the process of moving information across a N/w.

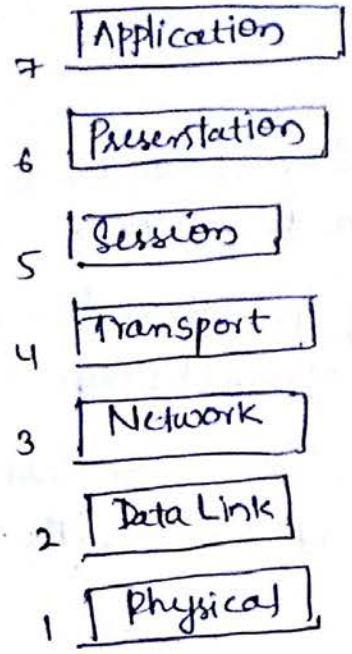


Fig: Seven Layers of the OSI model

* Layered Architecture

- The OSI model is composed of seven ordered layers:
  physical (layer 1)
  datalink (layer 2)
  network (layer 3)
  transport (layer 4)
  session (layer 5)
  presentation (layer 6) &
  application (layer 7)
- The layers involve when a message is sent from device A to device B. As the message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model.
- within a single machine, each layer calls upon the services of the layer just below it.
- Between machines, layer x on one machine communicates with layer x on another machine. This communication is governed by an agreed-upon series of rules & conventions called protocols.
- These processes on each machine that communicate at a given layer are called peer-to-peer processes.

↳ Communication b/w machines is therefore a peer-to-peer process using the protocols appropriate to a given layer.

* peer-to-peer processes

↳ At physical Layer, communication is direct. Device A sends a stream of bits to device B (through intermediate nodes).

↳ At the higher layers, however, communication must move down through the layers on device A, over to device B, and then back up through the layers.

↳ Each layer in the sending device adds its own information to the message it receives from the layer just above it & passes the whole package to the layer just below it.

↳ At layer 1 the entire package is converted to a form that can be transmitted to the receiving device. At the receiving machine, the message is unwrapped layer by layer, with each process receiving & removing the data meant for it.

Interfaces b/w Layers

↳ The passing of the data & N/w information down through the Layers of the sending device & back up through the layers of the receiving device is made possible by an interface b/w each pair of adjacent layers.

↳ Each interface defines the information and services a layer must provide for the layer above it.

↳ well-defined interfaces & layers functions provide modularity to a N/w.

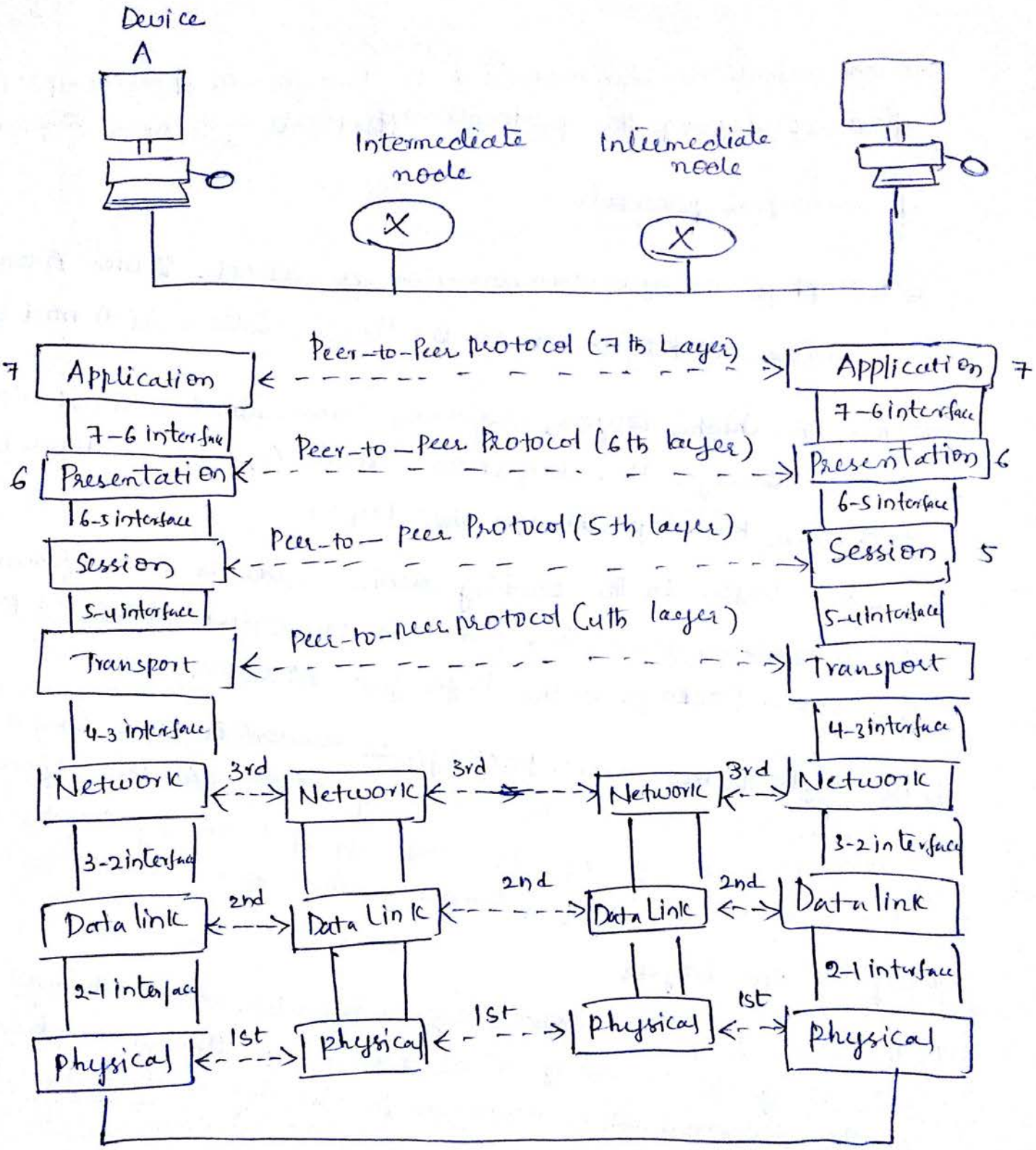


Fig: The interconnection b/w layers in the OSI model

Organization of Layers

↳ The seven layers can be thought of as belonging to three subgrou -PS.

↳ Layer 1, 2 & 3 – physical, datalink & Network – are the Network support layers.

↳ They deal with the Physical aspects of moving data from one device to another

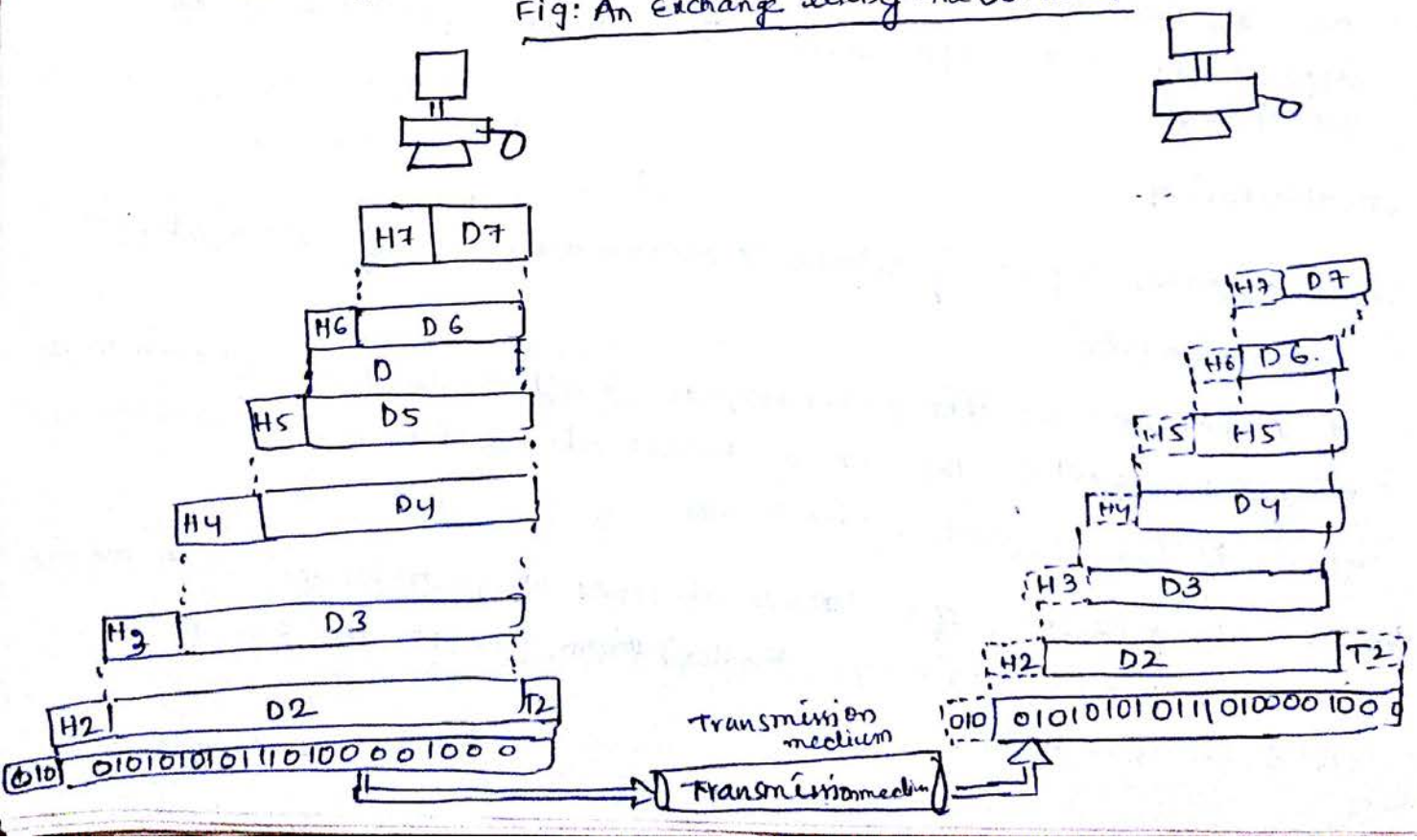
↳ Layers 5, 6, & 7 – session, presentation, and application – can be thought of as the user support layers; they allow interopera -bility among unrelated software systems.

↳ Layer 4, the transport layer, links the two subgroups & ensures that what the lower layers have transmitted is in a form that the upper layer can use.

↳ The upper OSI Layers are almost always implemented in software.

↳ The lower layers are a combination of h/w & s/w, except the physical layer, which is mostly hardware.

Fig: An Exchange using the OSI model



↳ The figure shows the overall view of the OSI layer, DT means the data unit at layer 7

↳ The process starts at layer (7), then moves from layer-to layer in descending, sequential order.

↳ At each layer, a header, or possibly a trailer, can be added to the data unit.

↳ Commonly, the trailer is added only at layer 2. when the formatted data unit passes through the Physical layer (layer 1), it is changed into an electromagnetic signal & transported along a physical link.

↳ Upon reaching its destination, the signal passes into layer 1 and is transformed back into digital form. The data unit then moves back up through OSI layers.

↳ As each block of data reaches the next higher layer, the headers & trailers attached to it at the corresponding sending layers are moved, and actions appropriate to that layers are taken.

↳ By the time it reaches layer 7, the message is again in a form appropriate to the application & is made available to the recipient.

Encapsulation

↳ The another aspect of data communication. is the OSI model is Encapsulation.

* A packet (header & data) at level 7 is encapsulated in a packet at level 6. The whole packet at level 6 is encapsulated in a packet at level 5, and so on.

↳ The data portion of a packet at level N-1 carries the whole packet (data & header and may be trailer) from level N. the concept is called encapsulation.

Layers in the OSI Model

* Physical Layer

↳ The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical & electrical specifications of the inter-face & transmission medium.

↳ It also defines the procedures and functions that physical devices & interfaces have to perform for transmission to occur.

* ↳ The physical layer is responsible for movements of individual bits from one hop (node) to the next.

1) Physical characteristics of interfaces & medium: The physical layer defines the characteristics of the interfaces blw the devices & the transmission medium. It also defines the type of transmission medium.

2) Representation of bits: The physical layer data consists of a stream of bits (sequence of 0s or 1s) with no interpretation. To be transmitted, bits must be encoded into signals - electrical or optical. The physical layer defines the type of encoding (how 0s and 1s are changed to signals).

3) Data rate: The transmission rate - the number of bits sent each second - is also defined by the physical layer.

4) Synchronization of bits: The sender & receiver not only must use the same bit rate but also must be synchronized at the bit level.

5) Line Configuration: The physical layer is concerned with the connection of devices to the media.

In point-to-point configuration two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.

6) physical topology → defines how devices are connected to make a Network. Devices can be connected by using a mesh topology, a star topology, a ring topology, or a hybrid topology.

7) Transmission mode → The physical layer also defines the direction of transmission b/w two devices: Simplex, half-duplex, or full-duplex. In simplex mode, only one device can send; the other can only receive. The simplex mode is a one-way communication

↳ In half-duplex mode, two devices can send & receive, but not at the same time.

↳ In a full-duplex mode, two devices can send & receive at the same time.

* Data link layer

↳ The Data link layer transforms the physical layer, a raw transmission facility, to a reliable link.

↳ It makes the physical layer appear error-free to the upper layer

1) Framing — The data link layer divides the stream of bits received from the N/w layer into manageable data units called frames.

2) Physical addressing: If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame.

↳ If the frame is intended for a system outside the sender's N/w, the receiver address is the address of the device that connects the N/w to the next one.

3) 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 overwhelming the receiver.

4) Error Control: The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.

5) Access Control: When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

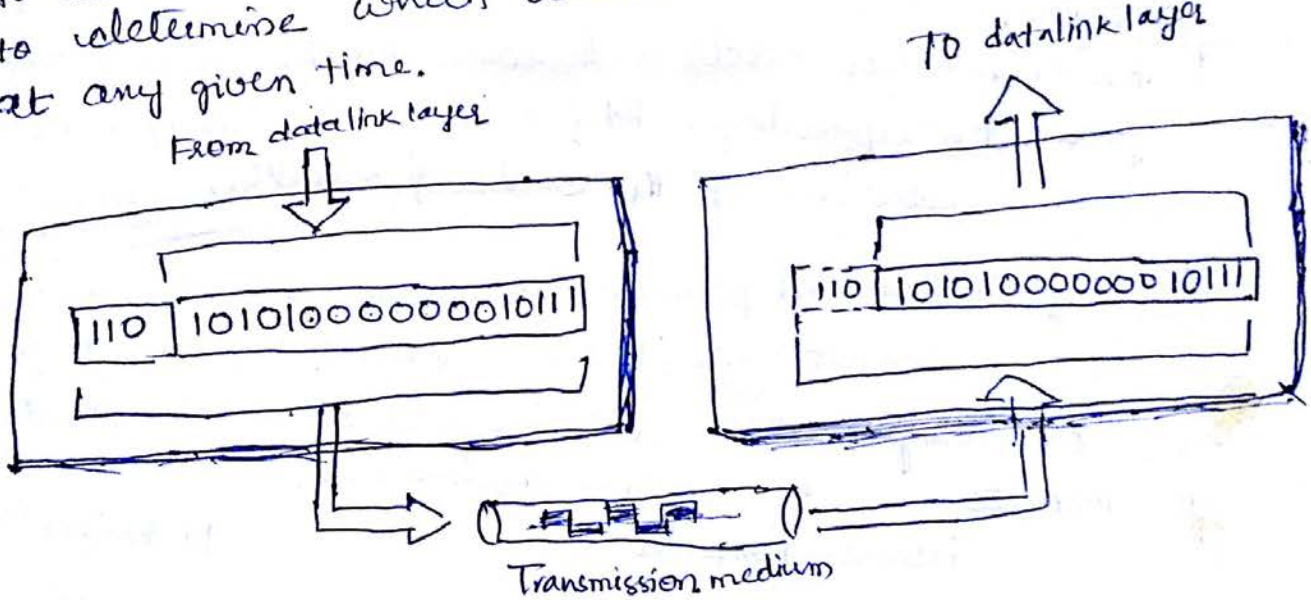


Fig: Physical Layer

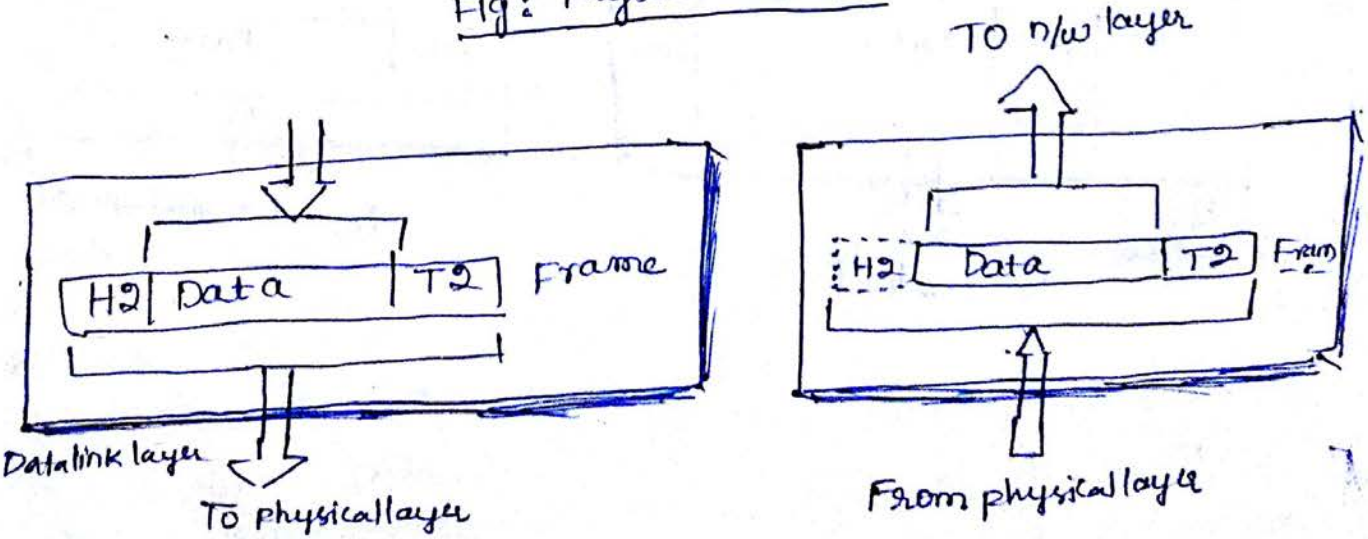


Fig: Datalink layer

Network Layer

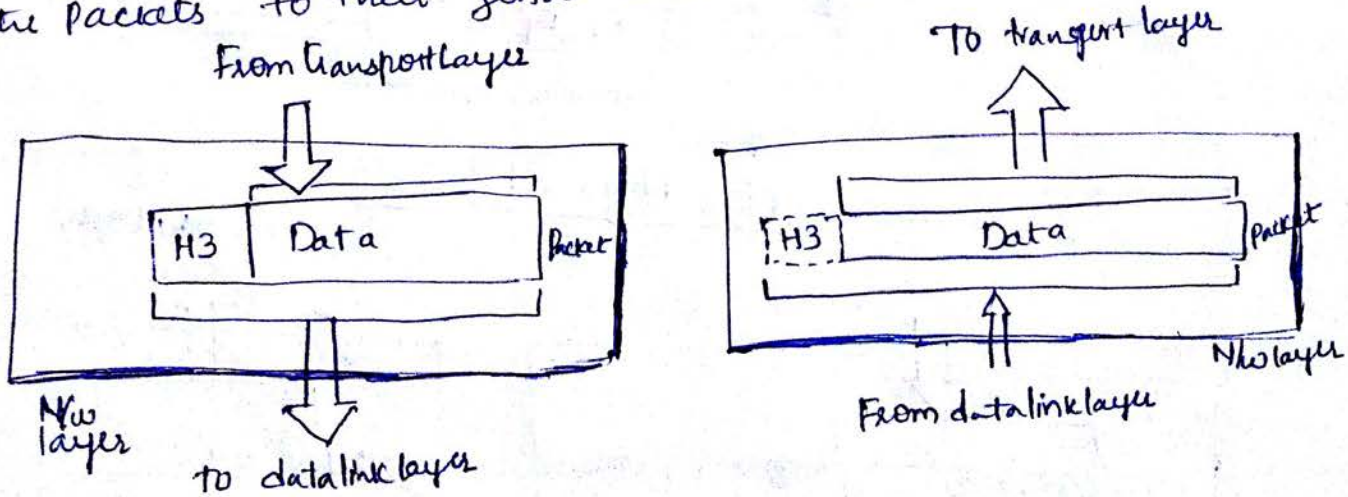
↳ This layer is responsible for source-to-destination delivery of a packet, possibly across multiple N/w (links). whereas the data link layer oversees the delivery of the packet b/w two systems on the same (Network (links), the N/w layer ensures that each packet gets from its point of origin to its final destination.

* Responsibilities

Logical addressing: The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the N/w boundary, we need another addressing system to help distinguish the source & destination systems.

↳ The N/w layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender & receiver.

Routing: When independent Networks or links are connected to create internetworks (network of networks) or a large N/w, the connecting devices (called Routers or Switches) route or switch the packets to their final destination.



Transport layer

- The transport layer is responsible for process-to-process delivery of the entire messages.
- A process is an application program running on host. Whereas the N/w layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship b/w those packets.
- It treats each one independently, as though each piece belonged to a seperate message, whether or not it does.
- The transport layer, on the other hand, ensures that the whole message arrives intact & in order, overseeing both error control & flow control at the source-to-destination level.

Responsibilities

* **Service-point addressing:** Computers often run several programs at the same time. For this reasons, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process on one computer to a specific process on the other.
- The transport layer header must therefore include a type of address called a service-point address (or port address).
- The N/w layer gets each packet to the correct computer, the transport layer gets the entire message to the correct process on that computer.

* **Segmentation & reassembly:** A message is divided into transmitta-ble segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination & to identify and replace packets that were lost in transmission.

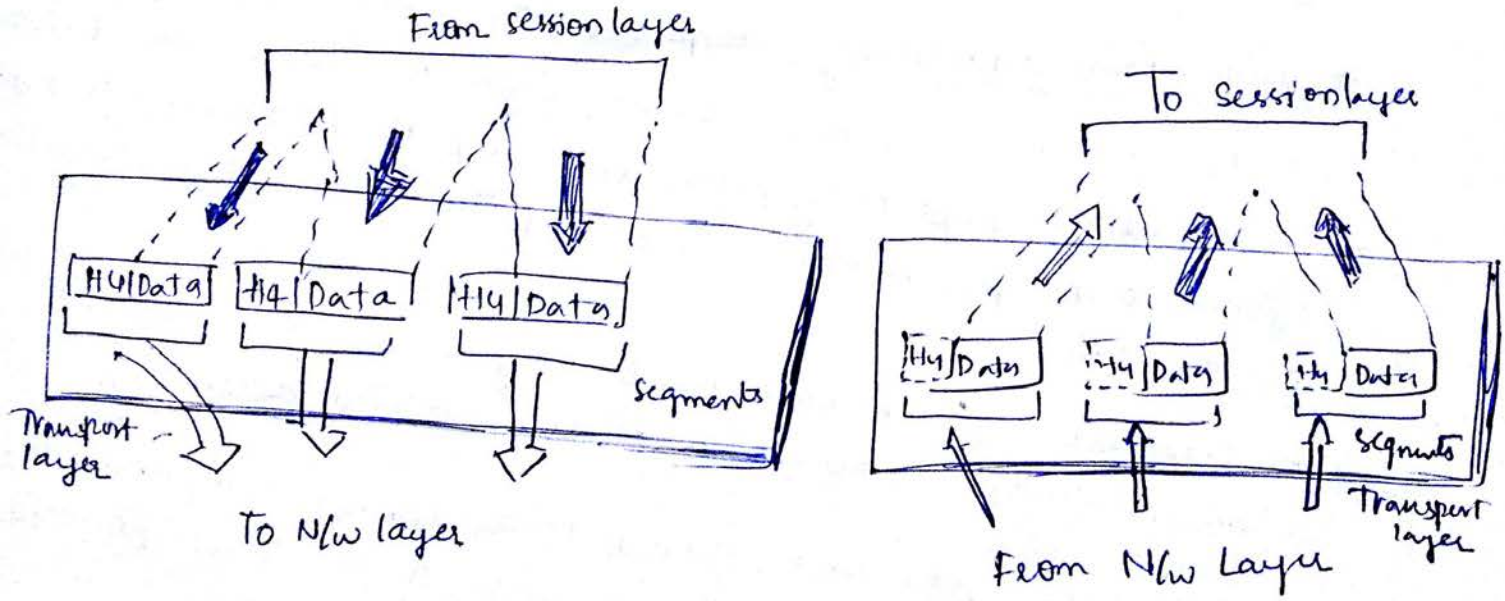
* Connection Control: The transport layer can be either connectionless or Connection oriented.

↳ A connectionless transport layer treats each segment as an indepe-ndent packet & delivers it to the transport layer at the destination machine.

↳ A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transfered the connection is terminated.

* Flow control: The flow control at this layer is performed end to end rather than across a single link.

* Error control: Error Control at this layer is performed process-to-process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error. Error correction is usually achieved through retransmission.



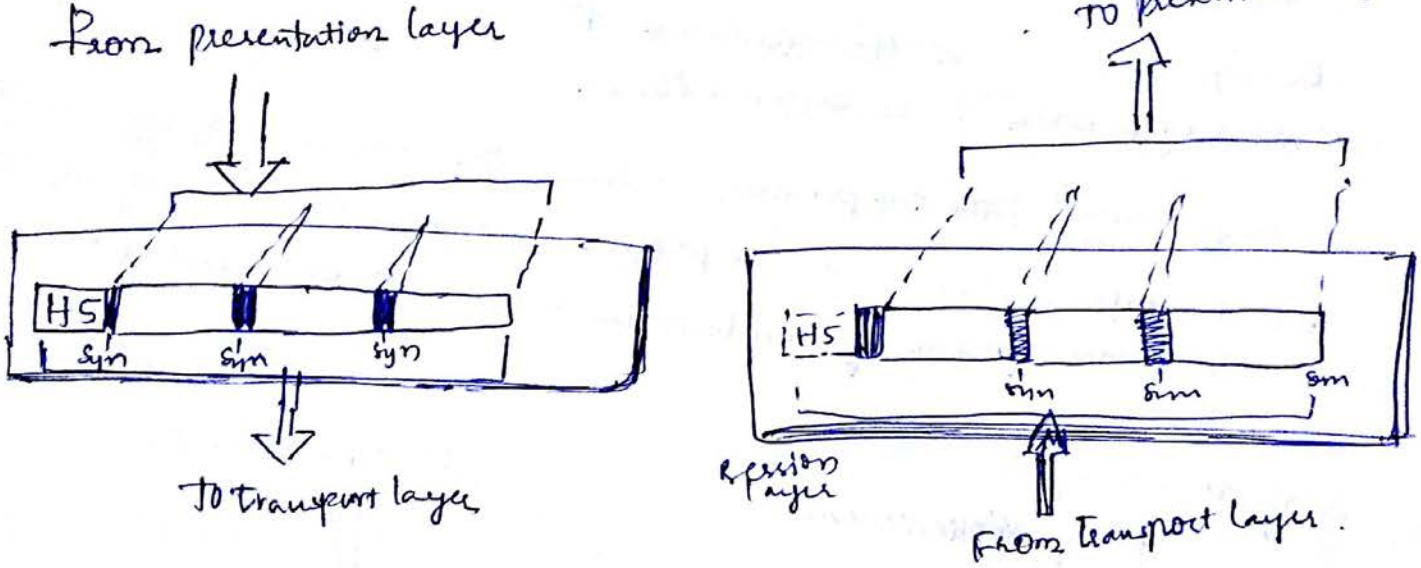
Session Layer

↳ It is the N/w dialog controller. It establishes, maintains, & synchroni-zes the interaction among communicating systems,

* Responsibilities

Dialog control: The session layer allows two systems to enter into a dialog. It allows the communication b/w two processes to take place in either half-duplex (one way at a time) or full-duplex (two ways at a time) mode.

Synchronisation: The session layer allows a process to add checkpoints, or synchronization points to a stream of data.



Presentation layer

- This is concerned with the syntax & semantics of the information exchanged b/w two systems.

* Responsibilities

- Translation: The processes in two systems are usually exchanging information in the form of character strings, numbers, & so on.
- The information must be changed to bit streams before being transmitted. Because different computers use different

encoding systems, the presentation layer is responsible for interoper-ability b/w these different encoding methods.

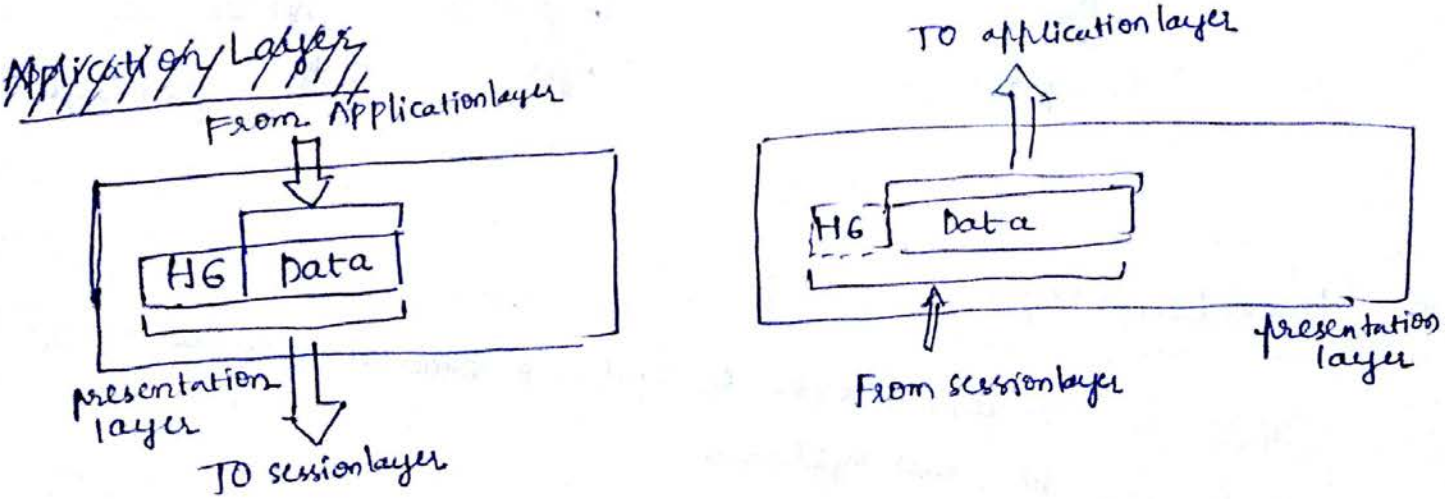
↳ The presentation layer at the sender changes the information from its sender-dependent format into a common format.

↳ The presentation layer at the receiving machine changes the common format into its receiver-dependent format,

Encryption: To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form & sends the resulting message out over the network.

Decryption reverse the original process to transform the message back to its original form.

Compression: Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio & video.



Application Layer

↳ The application layer enables the user, whether human or software, to access the Network. It provides user interfaces & support for services such as electronic mail, remote file access & transfer, shared database management, and other types of distributed information services.

* Services

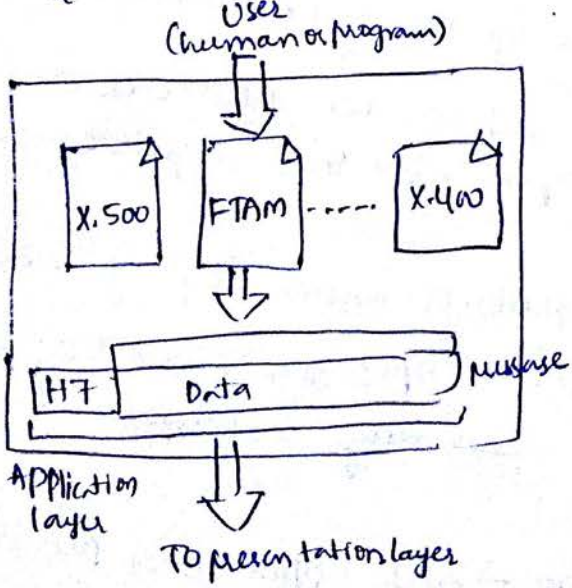
↳ **Network Virtual terminal** : A Network Virtual Terminal is a s/w version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a s/w emulation of a terminal at the remote host.

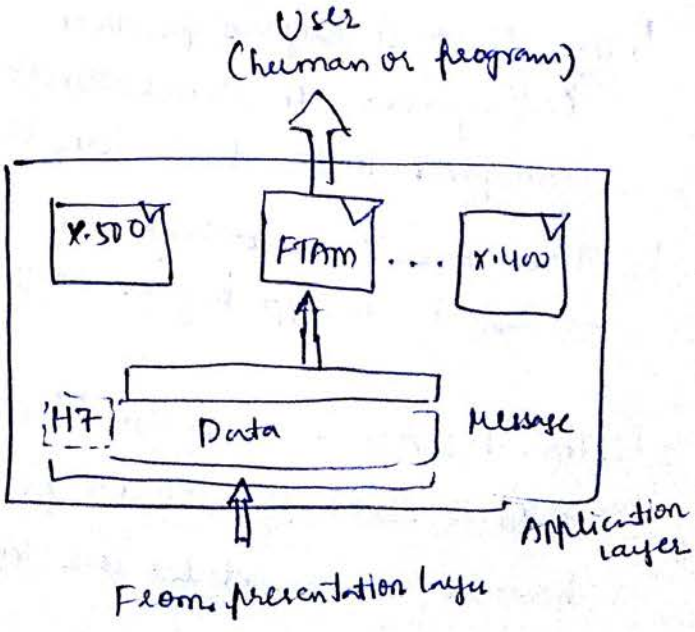
↳ The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host belives it is communicating with one of its own terminals and allows the user to log on.

↳ **File transfer, access, and management** : This application allows a user to access files in a remote host, to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.

↳ **Mail services** : This application provides the basis for e-mail forwarding & storage.

↳ **Directory services** : This application provides a distributed database sources & access for global information about various objects & services.





- X.400 → message-handling services • file transfer access & Management (FTAM)
- X.500 → directory services

TCP/IP Protocol Suite

↳ The original TCP/IP protocol suite was defined as having 4 layers: host-to-Network, internet, transport & application.

↳ when TCP/IP is compared to OSI, the host-to-Network layer is equivalent to the combination of the physical & datalink layers.

↳ The internet layer is equivalent to the network layer. The applicati -on layer is roughly doing the job of the session, presentation & application layers with the transpost layer in TCP/IP taking care of part of the duties of the session layer.

↳ We Assume that the TCP/IP protocol suite is made of five layers:

1) physical
2) data link
3) Network
4) transport
5) Application

↳ The first 4 layers provide physical standards, Network interfaces, internetworking, and transport functions that correspond to the first four layers of the OSI model.

↳ The three topmost layers in the OSI model, however are represe -nted in TCP/IP by a single layer called the application layer.

↳ The TCP/IP is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality; however, the modules are not necessarily interdependent.

↳ the Term hierarchical means that each upper-level protocol is supported by one or more lower-level protocols.

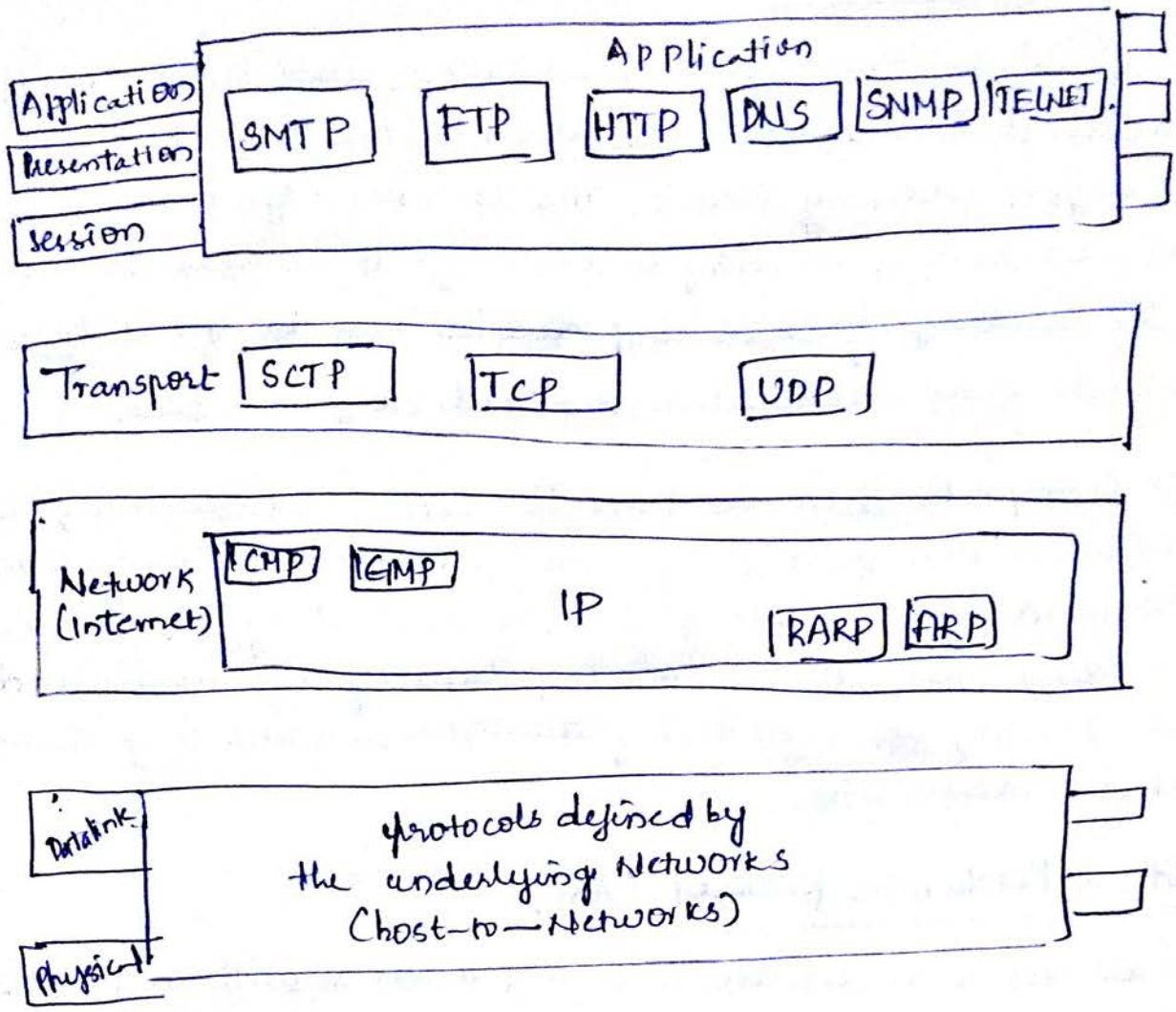


Fig: TCP/IP & OSI model

Physical & Data link layers

At the physical & data link layers, TCP/IP does not define any specific protocol. It supports all the standard & proprietary protocols. A N/w in a TCP/IP internetwork can be a local-area Network or a wide-area Network.

Network layer

At the Network layer, TCP/IP supports the internetworking protocol. IP, in turn, uses 4 supporting protocols: ARP, RARP, ICMP & IGMP

* Internetworking protocol (IP)

↳ The IP is the transmission mechanism used by the TCP/IP protocols. It is an unreliable and connectionless protocol — a best-effort delivery service. The term best effort means that IP provides no error checking or tracking. IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.

↳ IP transports data in packets called datagrams, each of which is transported separately. Datagrams can travel along different routes & 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 arrive at their destination.

* Address Resolution protocol (ARP)

It is used to associate a logical address with a physical address. On a typical physical N/w, such as a LAN, each device on a link is identified by a physical or station address, usually imprinted on the N/w interface card (NIC).

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

* Reverse Address Resolution protocol (RARP)

It allows a host to discover its Internet address when it knows only its physical address. It is used when a computer is connected to a network for the first time or when a diskless computer is booted.

* Internet Control Message protocol (ICMP)

It 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)

The IGMP is used to facilitate the simultaneous transmission of a message to a group of recipients.

Transport layer

The transport layer was represented in TCP/IP by two protocols:

TCP & UDP. Ip is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another. UDP & TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process. A new transport layer protocol, SCTP, has been devised to meet the needs of some newer applications.

* User Datagram protocol

↳ UDP is the simpler of the two standard TCP/IP transport protocols. It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.

* Transmission Control protocol

↳ It provides full transport-layer services to applications. TCP is a reliable stream transport protocol. The term stream, in this context, means connection-oriented: A connection must be established b/w both ends of a transmission before either can transmit data.

↳ At the sending end of each transmission, TCP divides a stream of data into smaller units called segments.

↳ Each segment includes a sequence number for reordering after receipt, together with an acknowledgement number for the segments received. Segments are carried across the

internet inside of IP datagrams. At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

* Stream Control Transmission protocol (SCTP)

Provides support for newer applications such as voice over the Internet. It is a transport layer protocol that combines the best features of UDP & TCP.

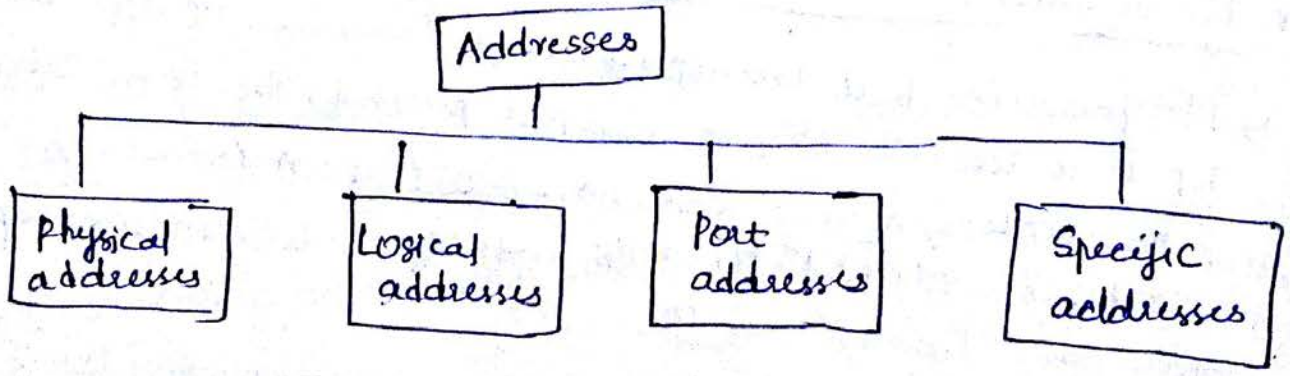
Application Layer

The application layer in TCP/IP is equivalent to the combined session, presentation, & application layers in the OSI model.

Addressing

↳ Four levels of addresses are used in an internet employing the TCP/IP protocols:

1) physical (link) addresses,
2) logical (IP) addresses
3) port addresses
4) specific addresses



↳Each address is related to a specific layer in the TCP/IP architecture.

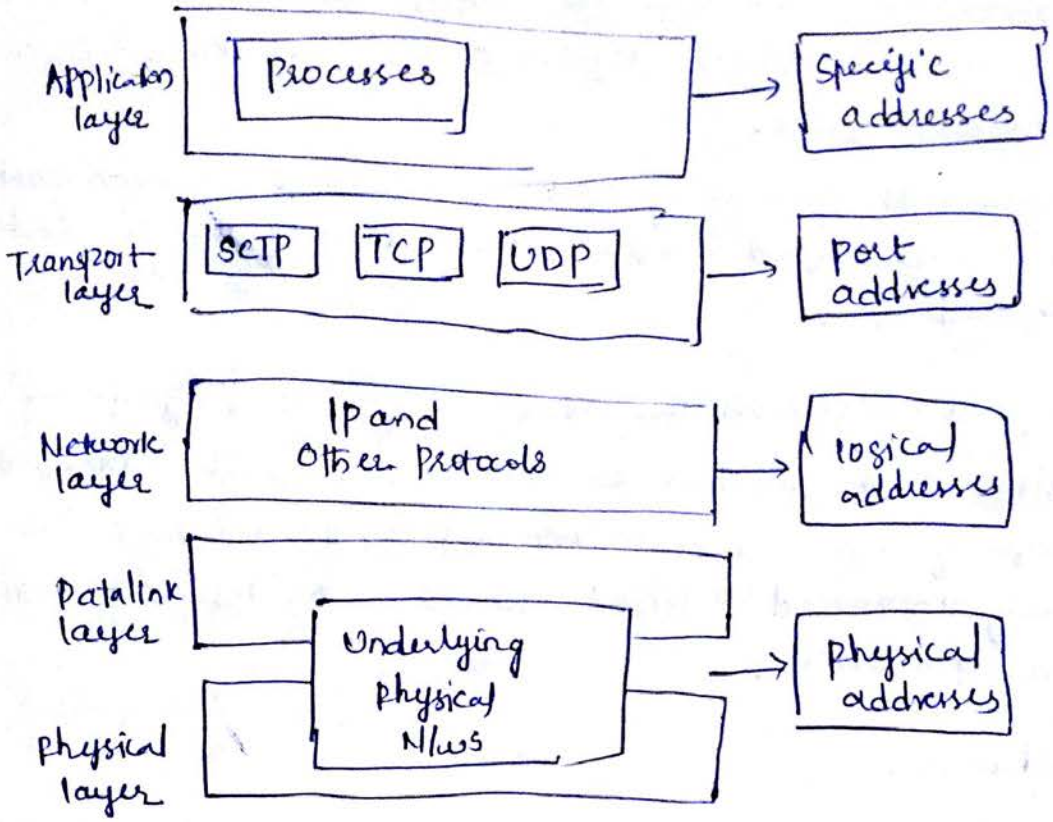


Fig: Relationship of layers & addresses in TCP/IP.

* Physical Addresses.

↳ The physical address, also known as the link address, 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 physical addresses have authority over the Network (LAN or WAN). The size & format of these addresses vary depending on the N/w. For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the N/w interface card (NIC). LocalTalk (Apple), however, has a 1-byte dynamic address that changes each time the station comes up.

* Logical Addresses

↳ Logical addresses are necessary for universal communications that are independent of underlying physical networks. physical addresses are not adequate in an internetwork environment where different n/ws can have different address formats.

↳ A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical N/w.

↳ The logical addresses are designed for this purpose. 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.

* Port Addresses

↳ The IP address & the physical address are necessary for a quantity of data to travel from a source to the destination host. However, arrival at the destination host is not the final objective of data communications on the Internet. A system that sends nothing but data from one computer to another is not complete.

↳ Today, computers are devices that can run multiple processes communicating at the same time. The end objective of Internet communication is a process communicating with other process.

↳ ex: Computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP).

↳ In the TCP/IP architecture the label assigned to an process is called a port address. A port address in TCP/IP is 16 bits in length.

Specific Address

↳ Some applications have user-friendly addresses that are designed for that specific address.
Examples include email address (forouzan@fhda.edu) & the Universal Resource Locator (URL) (www.mhhe.com)

↳ The first defines the recipient of an e-mail; the second is used to find a document on the World Wide Web.

↳ These addresses, however, get changed to the corresponding Port & logical addresses by the sending computer

Analog & digital signals

↳ Analog and Digital Data

Both data & the signals that represent them can be either analog or digital in form.

↳ The term analog data refers to information that is continuous
Ex:- Sounds made by a human voice.
↳ The digital data refers to information that has discrete ~~sets~~ states.
Ex:- Data stored in computer memory in the form of 0's & 1's

↳ Analog and Digital Signals

↳ An Analog signal has infinitely many levels of intensity over a period of time.
↳ A digital signal, on the other hand, can have only a limited number of defined values. Although each value can be any number, it is often as simple as 1 and 0.

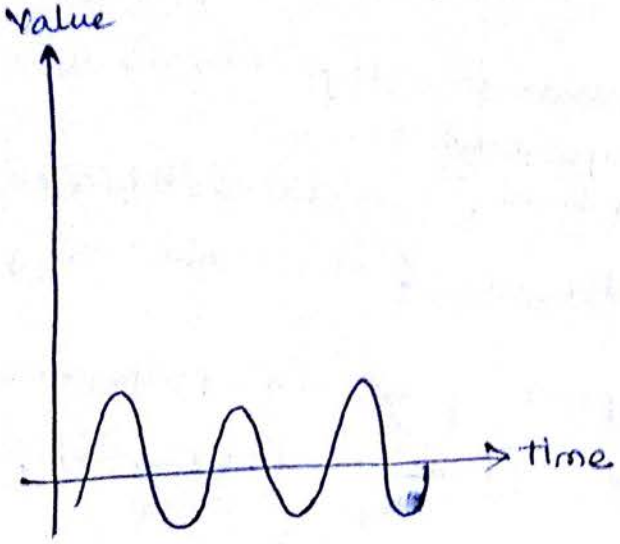


Fig: Analog signal

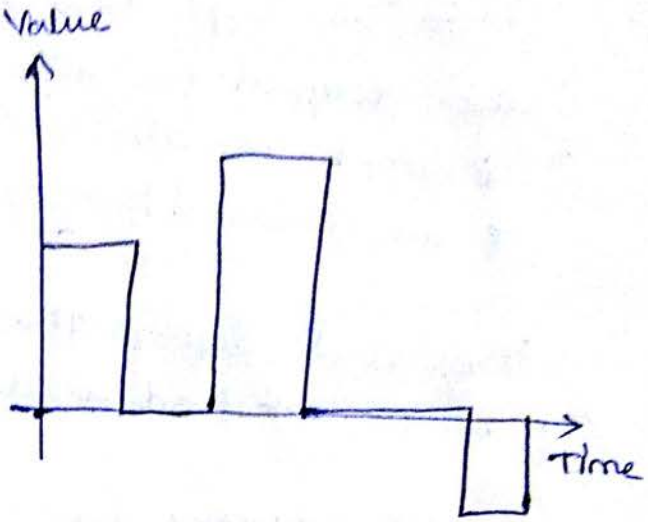


Fig: Digital signal

↳ Periodic & Non periodic Signals

Both analog & digital signals can take one of two forms: periodic or non periodic.

↳ A periodic signal completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical periods.

↳ The completion of one full pattern is called a cycle. A nonperiodic signal changes without exhibiting a pattern or cycle that repeats over time.