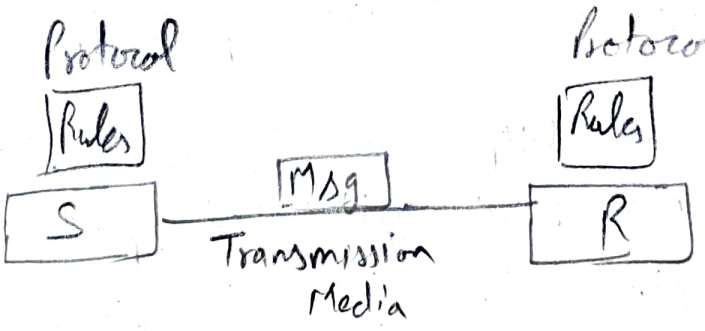
UNIT - I

Introductory Concepts

* **Introduction to Computer Network:** A Comp. n/w is a group of devices connected with each other through a transmission medium such as wires, cables etc. These devices can be comp., printers, scanners, Fax m/c etc.

→ The purpose of having comp. n/w is to send & receive data stored in other devices over the n/w. These devices are often referred as nodes.

Five Basic Component of a Comp. N/w:



- **Message:** It is the data or info. which needs to be transferred from one device to another device over a comp. n/w.

- **Sender:** Sender is a device that has the data and needs the data to other device connected to the n/w.

- **Receiver:** A receiver is the device which is expecting the data from other device on the n/w.

- **Transmission Media:** In order to transfer data from one device to another device we need a transmission media such as wires, cables, radio waves etc.

- **Protocol:** A protocol is a set of rules that are agreed by both sender and receiver, without a protocol two devices can be connected to each other but they cannot communicate.

In order to establish a reliable comm^n or data sharing b/w two diff. devices we need set of rules that are called protocol.

Eg: http and https are the two protocols used by web browsers to get and post the data to internet.

Similarly smtp protocol is used by email services connected to the internet.

→ It can provide connection authentication, transmission, encryption and compression.
Eg. telephone call

→ Point-to-point transmission with one sender and one receiver is sometime called as unicasting.

→ The Connection of two or more n/w is called an Internetwork. Eg. Coorldwide internet.

1) Local Area Network:

→ LAN is a comp. n/w that interconnects comp. within a limited area such as a residence, school, laboratory, office and college, to share resources (eg. printers) and exchange info.

Characteristics of LAN:

→ It is a private n/w, so an outside regulatory body never controls it.

→ LAN operates at a relatively higher speed compared to other WAN Sys.

→ There are various kinds of media access control methods like token ring and ethernet.

- In a Token Ring n/w, all devices are connected to the n/w, with empty data frames circulating around the ring.
- In Ethernet, data travels through the n/w inside units called frames, with each frame containing source & destination address.

LAN's are distinguished from other kinds of n/w by three characteristics:

1) Their transmission technology
2) Their size
3) Their topology

Advantages of LAN:

1) Resource sharing: printers, scanners, modems etc.
2) S/w app. sharing: use same s/w in a many comp. instead of purchasing the separate licensed s/w.
3) Easy & cheap Comm^n: data can shared easily.
4) Centralized data: data is stored on hard disk of the central/server comp.
5) Data security: data is only stored on server. So easily manage the data, data will be not secure.

6) Internet sharing: share a single internet connection among all the LAN users.

Disadvantage of LAN:

1) High setup cost: special s/w required to make a server. Also, comm^n devices like an ethernet cable, switches, hubs, routers are costly.

2) Privacy violations: LAN administrator can see & check personal data files of each LAN user.

3) Data security threat: unauthorised users can access imp. data of an office or a campus if a server hard disk is not properly secured by LAN administrator.

4) LAN maintanance Job: LAN requires a LAN administrator because there are prob such as s/w installation, prog. faults, h/w failures or cable disturbance in LAN.

5) Covers small / Limited Area: restricted in size

2) Metropolitan Area Network:

→ MAN covers a larger area than LAN & smaller area as compared to WAN.

→ It connects to two or more comp. that are apart but resides in the same or diff. cities.

→ It covers a large geographical area and may serve as an ISP (Internet service providers).

→ MAN is designed for customers who need a high-speed connectivity.

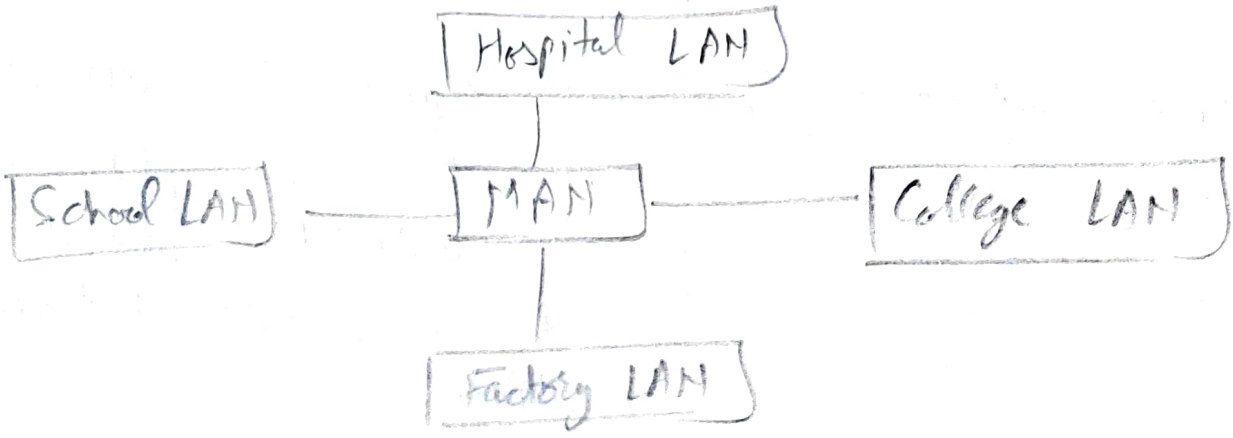
→ Speed of MAN ranges in terms of Mbps.

→ Its hard to design & maintain a MAN.

→ Fault Tolerance of MAN is less.

→ Data Transfer rate and propagation delay of MAN is moderate.

→ Devices used for transmission of data through MAN are: Modem and wire/cable.



Advantages of MAN:

1) less expensive to attach MAN with WAN.
2) MAN gives good efficiency of data
3) Easily ~~centralized~~ manage in a centralized way.
4) Send local email fast & free.
5) High speed than WAN upto 1000 Mbps.
6) Sharing of Internet.
7) Conversion from LAN to MAN is easy means Connecting two LANs ~~to~~ together fastly.

Disadvantages of MAN:

1) Difficult to manage
2) Internet speed difference
3) Hackers attack
4) Technical people required to set up
5) More wires required.

3) Wide Area Network

→ It covers a large geographical area such as a region, a country or whole world.

→ WAN includes the technologies to transmit data, image, audio and video info. over long distances and among diff LANs and MANs.

Features:

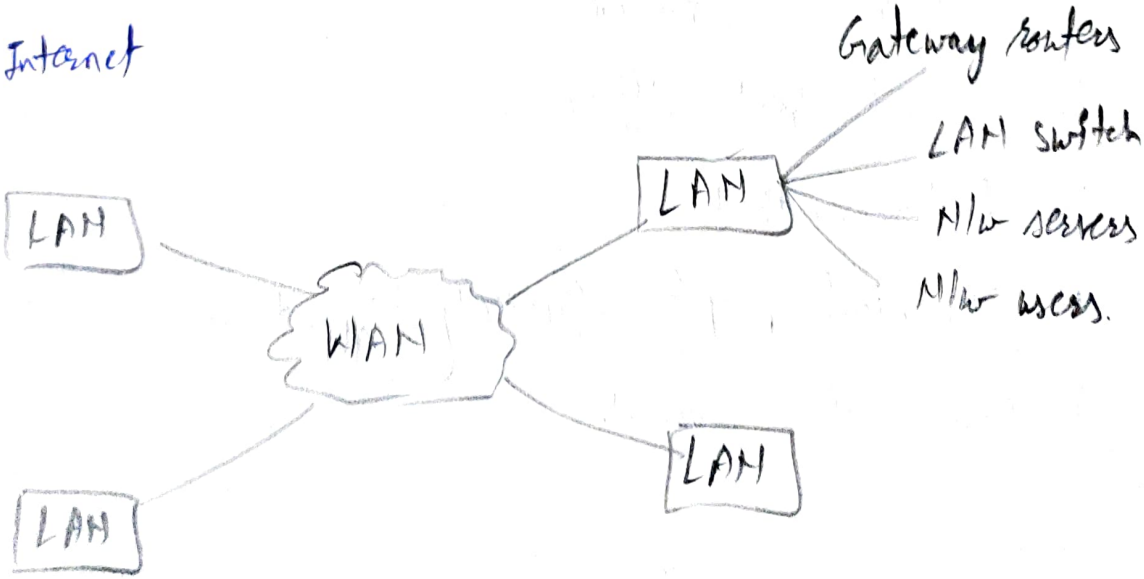
1) WAN has a large capacity, connecting a large no. of comp. over a large area.

2) They provide uplinks for connecting LANs and MANs to the internet.

3) Comm' links are provided by public carriers like telephone n/w, n/w providers, cable sys., satellites etc.

4) they have low data transfer rate & high propagation delay i.e. they have low comm' speed.

Eg. Internet

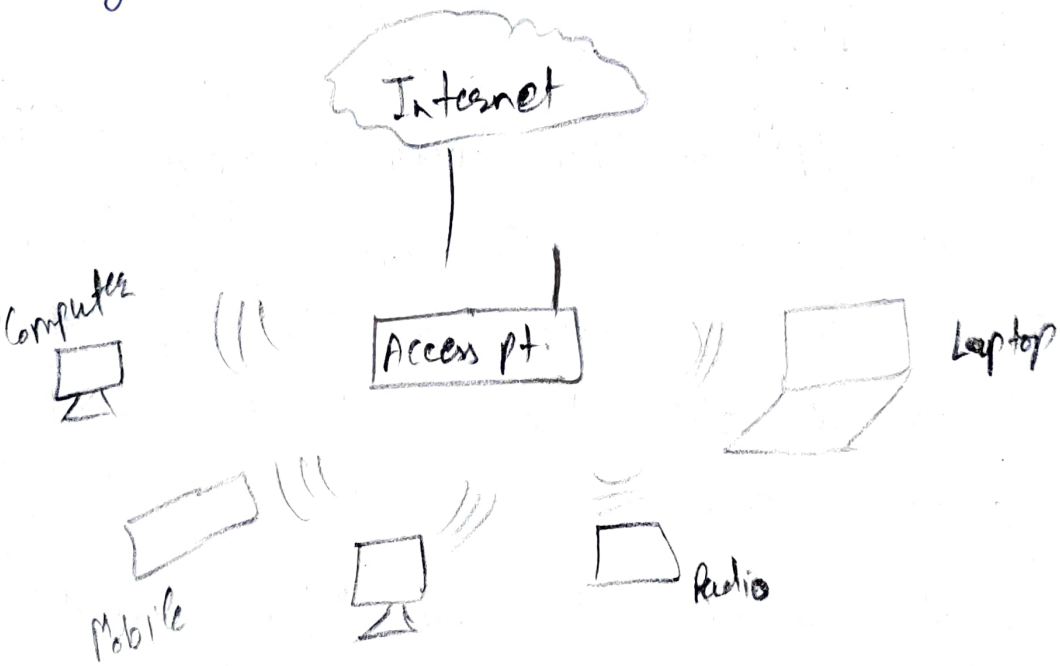


4) Wireless Networks:

→ Comp. N/w that are not connected by cables are called wireless n/w.

→ They generally use radio waves for comm^n b/w the n/w nodes.

→ They allow devices to be connected to the n/w while roaming around ~~the~~ within the n/w coverage.



Types:

1) Wireless LANs: Connects two or more n/w devices using wireless distribution techniques.

2) Wireless MANs : Connects two or more wireless LANs spreading over a metropolitan area.

3) Wireless WANs: Connects large areas comprising LANs, MANs and personal n/w.

Eg: Mobile ph n/w, wireless sensor n/w, satelite.

Advantages of Wireless N/w:

→ installation & setup is easy.
→ Require very limited or no wire.
→ Reduce equipment or setup cost.
→ New devices can be easily connected to existing setup.

5) Home Network:

→ A home LAN or home n/w is a type of network that connects two or more comp. to each other.
→ In this we can share files b/w comp., sharing printer or other devices that are connected to a single comp.
→ In this we can share the Internet connection with multiple comp. by use of a router.
→ If a n/w router in the home or have multiple comp. that share the same network, than home call as a home n/w.

6) Internetworks:

→ Interconnecting multiple comp. n/w such as any pair of hosts in the connected n/w can exchange msg. irrespective of their H/w level n/wing technology.

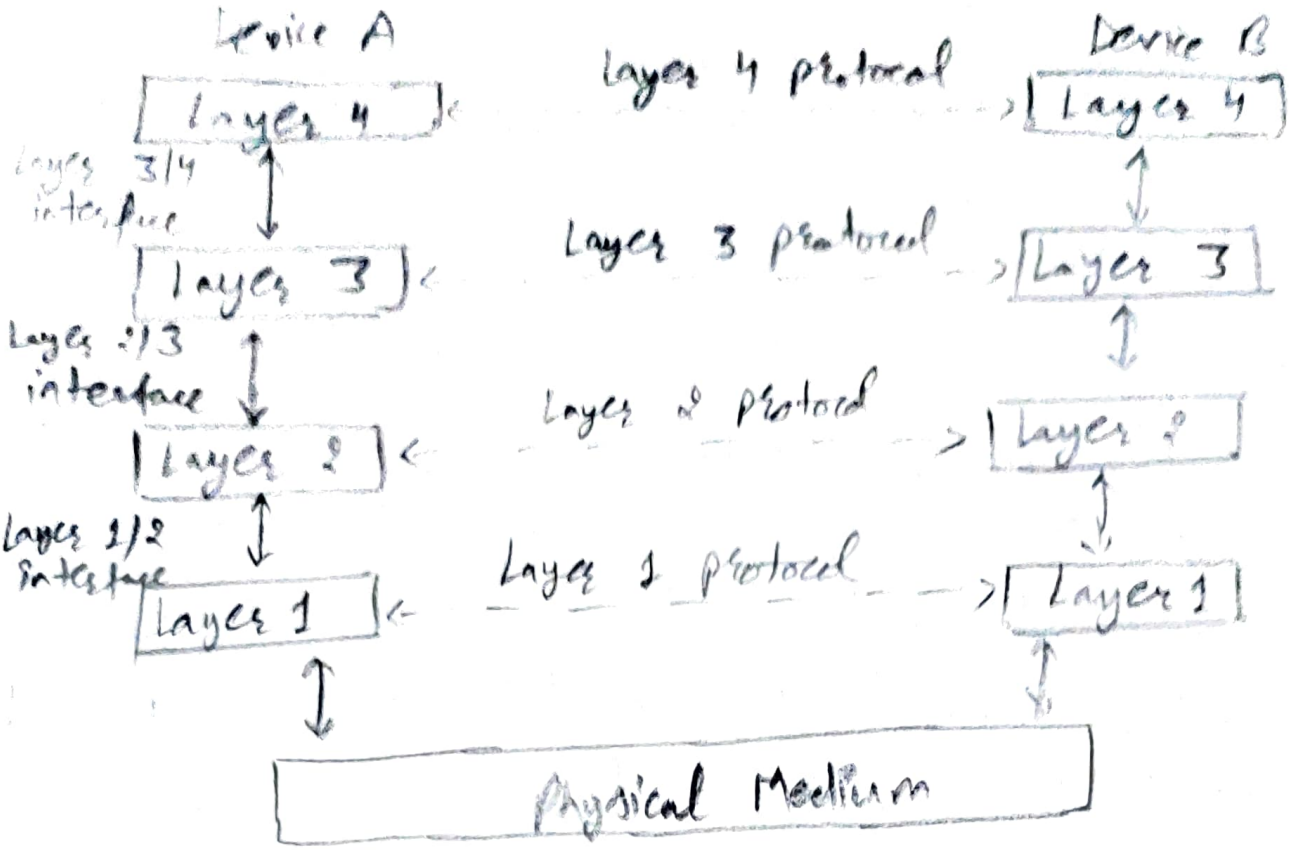
→ The resulting sys. of interconnected n/w are called an Internetwork or Internet.

* Network Software:

1) Protocol Hierarchies:

→ A Protocol is defined as a set of rules & regulations for data comm^n. Rules are defined for each & every step and process at the time of comm^n among two or more comp.

→ Most n/w are organized as a stack of layers, one on top of another. The no. of layers & their names vary from n/w to n/w. Each layer has a specified fun^n & protocols. Thus we obtain a stack of protocols.



→ It represents Comm^n b/w device A and device B. The data from one device to other is not sent directly but has to pass through a no. of layers.

→ The layers called as peers & have a set of protocols for Comm^n.

→ B/w each adjacent layer is an interface that defines the services that are being offered by a lower layer to the next higher layer.

- Device A wants to send a msg. to device B. device A passes its info. to the highest layer, than perform some specified fun^n on it & passes it to layer below. This continues until data reaches to the lowest layer.

- Layer 1 passes a bit stream of 0s and 1s to the physical medium that communicates it to the layer 1 of the receiving end. than perform some fun^n on data stream to support the protocol with its peer & passes it to layer above.
- This continues until the info. reaches the highest layer.
- The highest layer convey the msg to device B in same format sent by device A.

2) Design Issues for the layers:

- Reliability: operates correctly even when it is made up of unreliable components.
- Addressing: multiple processes are running on one m/c. Every layer needs a mechanism to identify senders & receivers.
- Error Control: It is an imp. issue bcoz physical Comm^n circuits are not perfect. Many error detecting and error correcting codes are available. Both sending and receiving ends must agree to use any one code.

- Flow Control: If there is a fast sender who is sending data to a slow receiver, then there must be flow control mechanism to control the loss of data by slow receivers. Mechanism are increasing buffer size at receivers, slow down the fast sender, etc.
Some process will not be in position to accept arbitrarily long msg. This property leads to mechanism for disassembling, transmitting and reassembling msg.

- Mux & Demux: If the data has to be transmitted on transmission media separately, It is inconvenient or expensive to setup seperate connection for each pair of comm^n processes. So multiplexing needed in the physical layer at sender and demultiplexing needed at receiver end.

- Scalability: If n/w gets large, then n/w can continue to work by using scalability.

- Routing: When multiple path b/w source & destination so choose only one route, by using any routing algo.

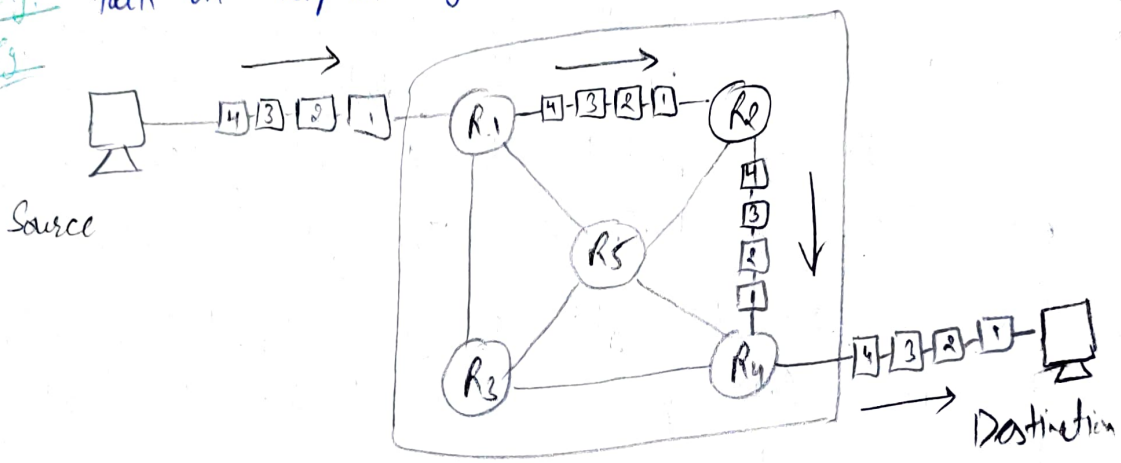
- Confidentiality & Integrity: n/w security is most imp. So Confidentiality defends against threats like eavesdropping. and Integrity prevent faulty changes to msg.

3) Connection Oriented & Connection-less services? [TCP protocol]

Connection Oriented: establish a connection prior to sending the packets belonging to same message from source to destination.

eg. talk on telephone sys.

eg.



[Connection Oriented Service]

To establish a conn' a source sends a request pkt to the destination. Then destination sends acknowledgement pkt. to the source confirming that destination is ready to accept the data from the source

Meanwhile, the routers involved in exchange of request and ack. pkt b/w source & destination.

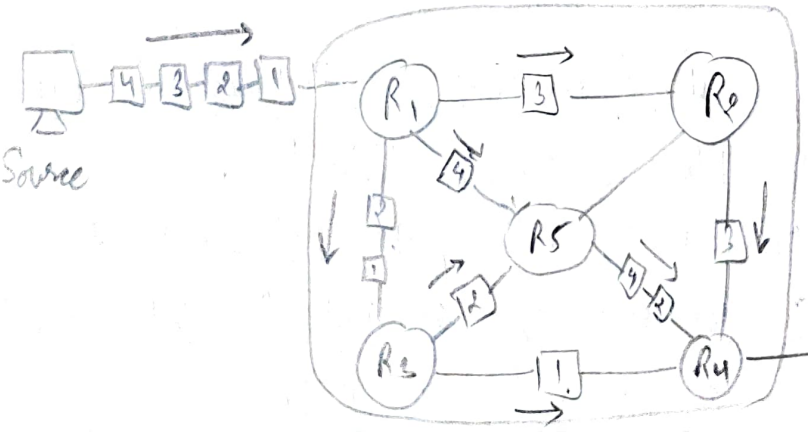
Virtual path followed by all pkts. belonging to the same msg. So resources are reserved for data transfer before transferring all pkt. in a msg.

Connectionless Service: Each pkt. belonging to the same msg. as a diff. & independent entity and route them with a diff. path.

→ It is a method of data transmission b/w two comp. in a diff. n/w. Connectionless service also called as a datagram service. This service look like a postal sys. where each letter carries its source & destination addr. and each one of them routed through a diff. path.

→ The source divides the msg into small acceptable pkt. these pkts known as datagram. The datagrams are individually pushed into the n/w, each datagram may travel a diff. path. The n/w considers each datagram or data pkt as an independent entity i.e. no relationship is considered b/w the pkts belonging to the same msg.

→ Each datagram carries its source and destination addr. The router uses the destination addr. to route the datagram to its destination. The pkt received at the destinat^n may be received out of order. Hence, the datagram are assembled to recreate the original msg.



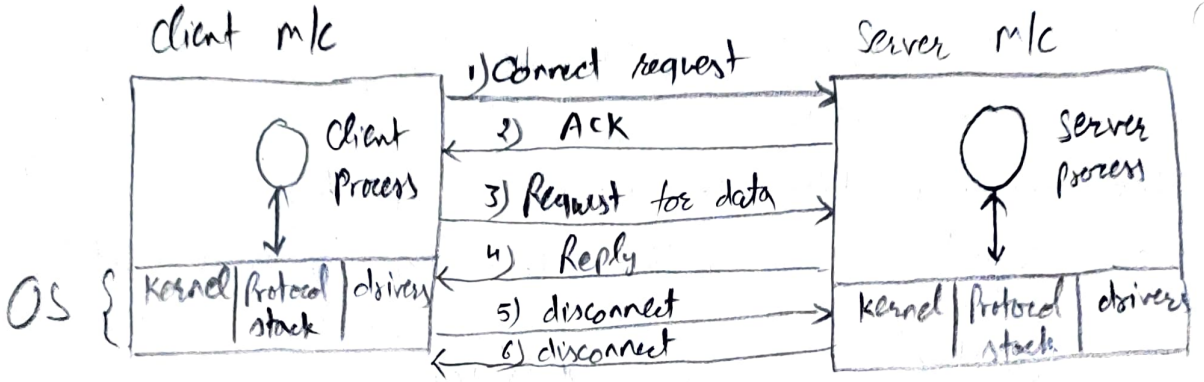
UDP Protocol

→ Primitive can have parameters such as Connect, Data, Disconnect to established a connection, to send data and disconnect a connection through these four primitive

→ Services can be either Confirmed or unconfirmed.

→ In a Confirmed service, there is a request, an indication, a response and a confirm.

→ In an unconfirmed service, there is just a request and an indication.



[Pkt sent in a client-server interaction on a connection oriented n/w].

* Topologies: It is a arrangement in which comp. sys. or n/w devices are connected to each other.

1) Bus topology: all devices share single comm^n line or cable. In this we have a prob. while multiple hosts sending data at the same time. Therefore, It uses Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue. So that failure of a device does not affect the other device. But failure of shared comm^n line can make all other devices stop

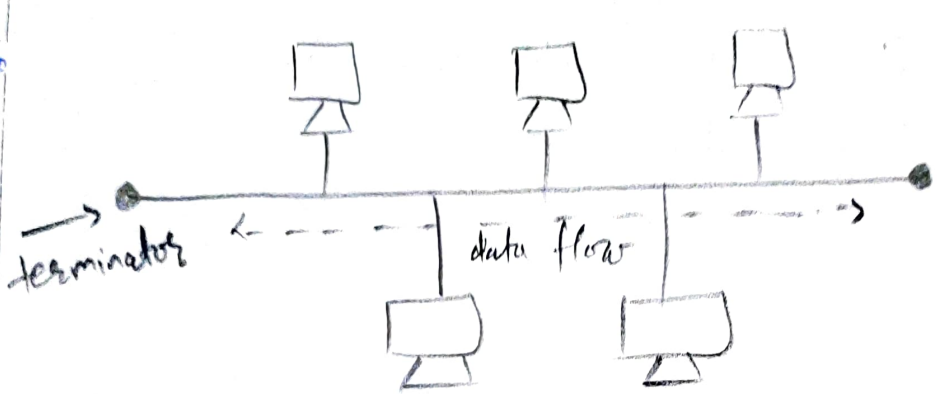
4) **Service Primitives:** In the n/w layer architecture, when one layer requires another layer to carry out a service, the comm" b/w the layers is carried out by service primitives.

→ A service is formally specified by a set of primitives (operations) available to a user or other entity to access the service.

→ These primitives tells the service to perform some action or report on an action taken by a peer entity.

Primitive	Meaning
Request	An entity wants the service to do some work
Indication	informed that someone wants to set up a connection.
Response	An entity wants to respond to an event accept it or reject it.
Confirm	The response to an earlier request has come back.

functions. Both ends of the shared channel have line terminator. The data is sent in only one direction and as soon as it reaches the extreme end, the terminators removes the data from the line.

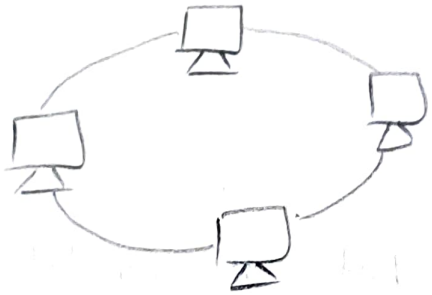


2) Star Topology: All hosts are connected to a central device, known as hub device, using a pt.-to-pt. connectn. b/w host & hub. The hub device can be any of the following:

- Layer 1 device such as hub or repeater
- Layer 2 device such as switch or bridge
- Layer 3 device such as router or gateway

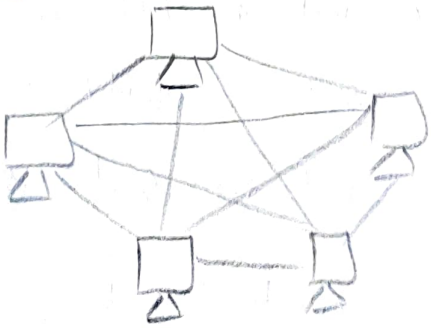
→ If hub fails, then connectivity to all hosts fails.
→ Every comm^n b/w hosts, take place through only the hub.
→ It is not expensive to connect one more host, only one cable is required and configuratn is simple.

3) Ring topology: each host mlc connects to exactly two other mlc, creating a circular nlw structure. When one host fails to comm^n or send a msg to a host which is not adjacent to pt, the data travels through all intermediate hosts.



Failure of any host results in failure of whole ring.

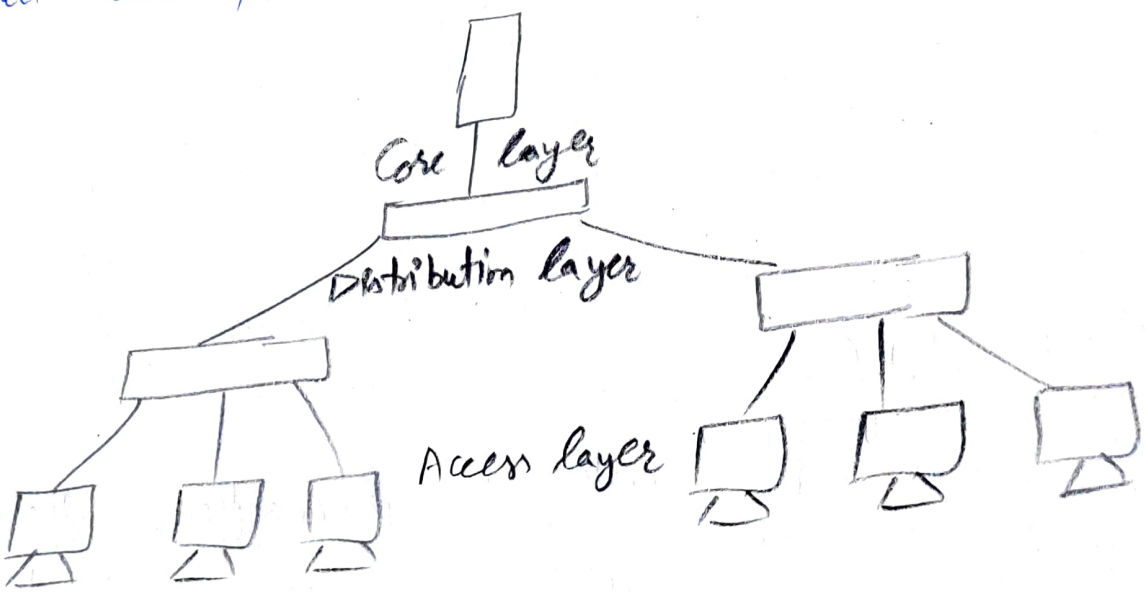
4) Mesh Topology: A host is connected one or multiple hosts



Types: Full Mesh & Partially Mesh

- Full Mesh: all hosts have pt.-to-pt. connectn to every other host in the nlw.
- Partially Mesh: Not all host.

5) Tree Topology: 3 types of nw devices.
- Lower layer is access layer where comp. are attached
- Middle layer is known as distribution layer, which work as mediator b/w upper layer and lower layer
- Higher layer known as core layer and. It is a central pt. of nw, ie root of the tree from which all nodes ~~for~~ work.

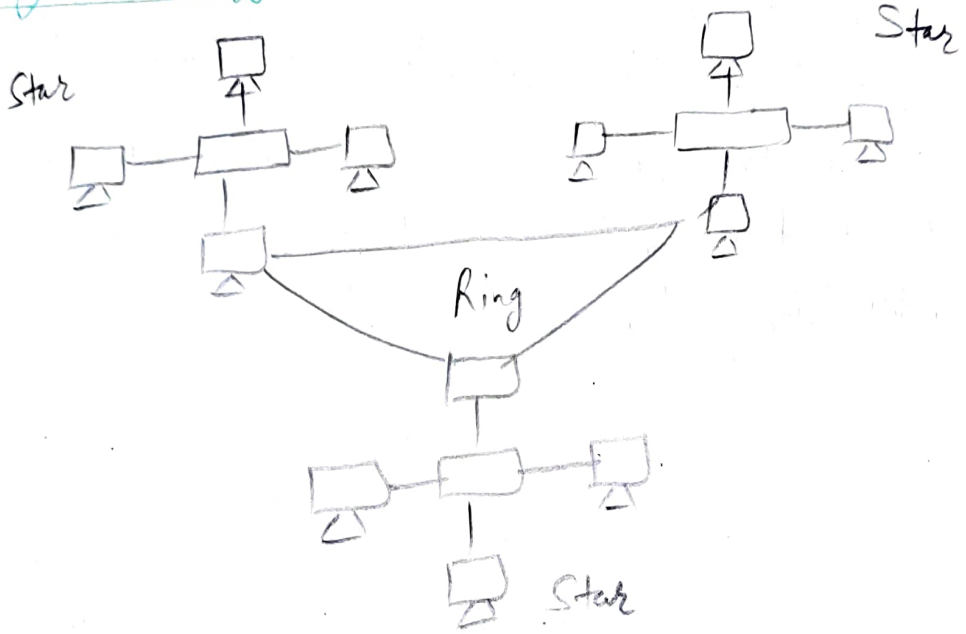


→ All host have pt.-to-pt. conn.
→ Similar to Bus topology, if the root goes down, then the entire nw suffers, even though it is not the single pt. of failure.

6) Daisy chain: all hosts connect in a linear fashion. Similar to Ring topology, all hosts are connected to two hosts only, except the end hosts.

- Each link in daisy chain topology represent single point of failure.
- Every link failure splits the n/w into two segments.
- Every intermediate host work as relay for the intermediate hosts.

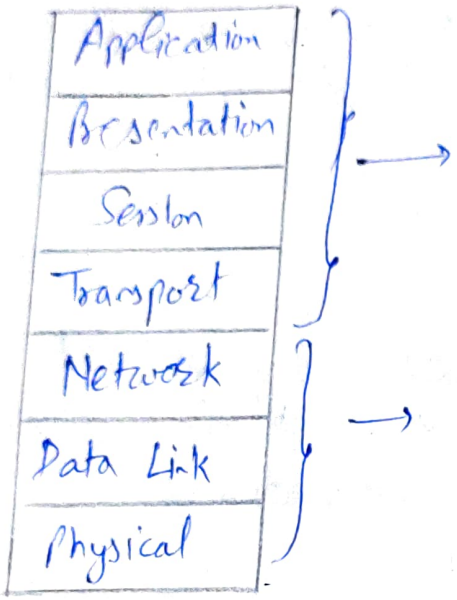
7) Hybrid Topology: More than one topology.



* OSI Model:

- Stands for Open System Interconnection, describe how info. from a S/w app. in one comp. moves through a physical medium to the s/w app. in another comp.
- Consist of 7 layers, each layer performs a particular n/w fun^n.
- developed by ISO (International Organization for Standardization) in 1984, and it is now considered as an arch. model for the inter-comp. comm^n.

Characteristics of OSI Models



- The OSI model is divided into two layers: upper layers and lower layers.
- Upper layer deals with app. related issue and implemented only in S/w. App. layer is closest to end user. Both the end user and app. layer interact with the s/w app.
- Lower layer deals with data transport issue. Data link layer & physical layer are implemented in H/w and S/w. The Phy. layer is the lowest layer & closest to phy. medium. Phy. layer is mainly responsible for placing the info. on the physical medium.

Functions of OSI layers

1) Application

Application → This layer provide the services to the user.

Presentation ← It is responsible for translation, compression & encryption

Session → It is used to establish, manage and terminate the sessions.

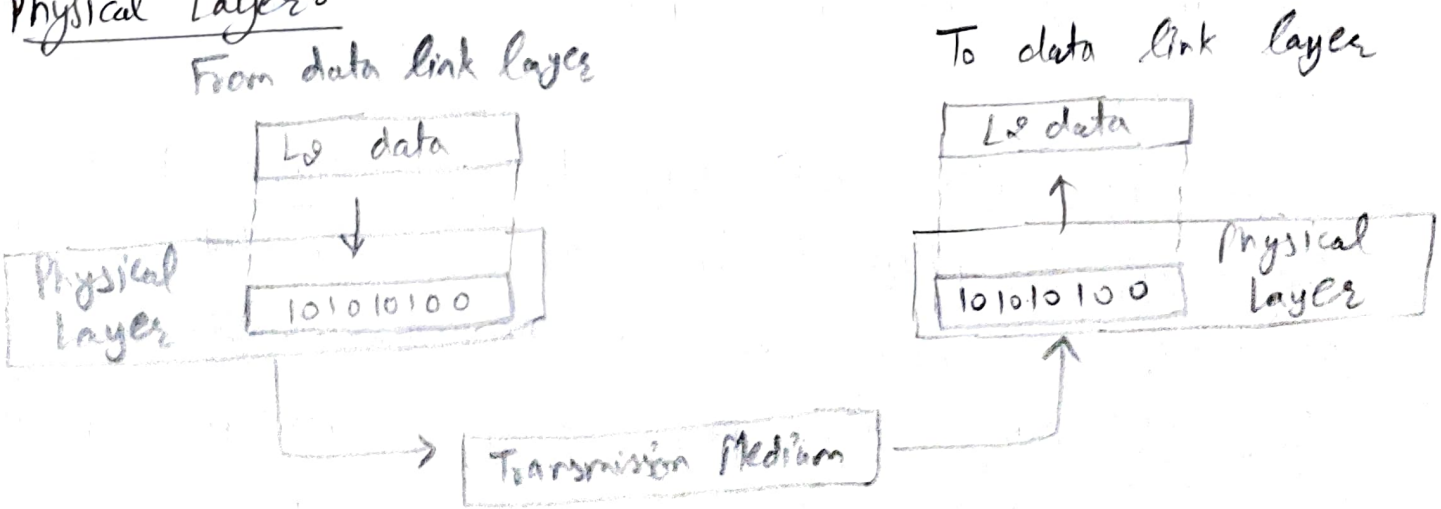
Transport ← It provides reliable msg delivery from process to process

Network → It is responsible for moving the pkts from source to destination

Data Link ← It is used for error free transfer of data frames

Physical → It provides a physical medium through which bits are transmitted

1) Physical Layer:



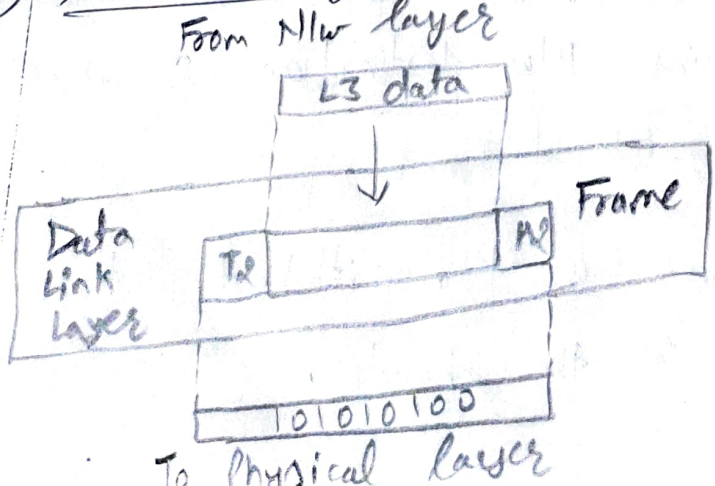
- Main functionality: transmit the individual bits from one node to another node.
- lowest layer of OSI model.
- It establishes, maintains & deactivates the physical connection.

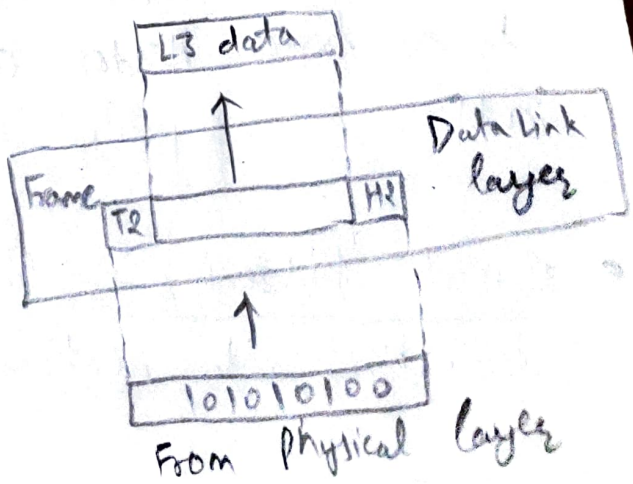
Functions:

- Line Configuration: how to connect more devices can be connected physically.
- Data Transmission: define the transmission mode whether it is simplex, half-duplex or full duplex mode b/w the two devices on the n/w.
- Topology: How n/w devices are arranged.
- Signals: determines type of signal used for transmitting the info.

2) Data Link layer:

From N/w layer





- Responsible for error free transfer of data frames.
- defines format of data on the n/w.
- provides a reliable or efficient comm^n blw two or more devices.
- Mainly responsible for unique identification of each device that resides on a local n/w.
- It contains two sub-layers:

↳ Logical link Control layer

- Responsible for transferring the pkts to N/w layer of the receiver that is receiving.
- Identifies the addr. of the n/w layer protocol from the header.
- also provides flow control.

↳ Media Access Control Layer

- It is a link blw logical link control layer and the n/w's physical layer.
- transferring the pkts over the n/w.

Functions:

- Framing: translates the physical's raw bit stream into pkts known as frames. It adds header & trailer to the frame. Header contains H/w destination & source addr.

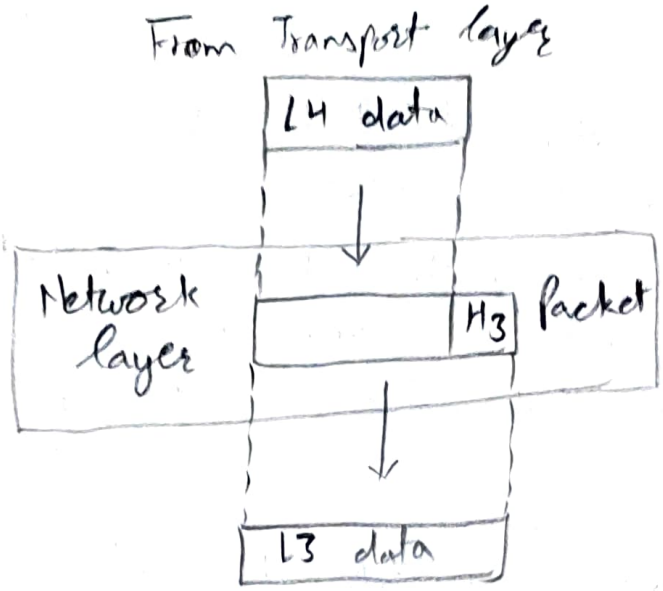
- Physical Addressing: frame is transmitted to the destination addr. mentioned in the header.

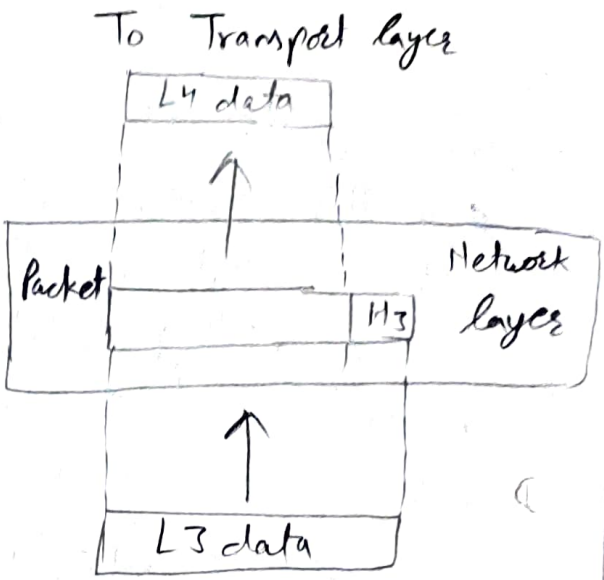
- **Flow Control:** It is a main fun^n of Data link layer. In this constant data rate is maintained on both sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- **Error Control:** achieved by adding a calculated value CRC (Cyclic Redundancy Check) i.e. placed to the DLL's trailer which is added to the msg frame before it is sent to the phy. layer.
  If any error occur, then receiver sends the ack. for the retransmission of the corrupted frames.
- **Access Control:** When two or more devices are connected to the same comm^n channels then the data link layer protocols are used to determine which device has control over the link at a given time.

3) Network layer:

- Layer 3 manage device addressing, tracks the location of devices on the n/w.
- determines best path to move data from S to D based on n/w cond^n, priority of service & other factors.

- DLL responsible for routing & forwarding the pkts.
- protocols used to route the n/w traffic are known as Nlw layer protocols. Eg. of protocols are IP and IPV6.

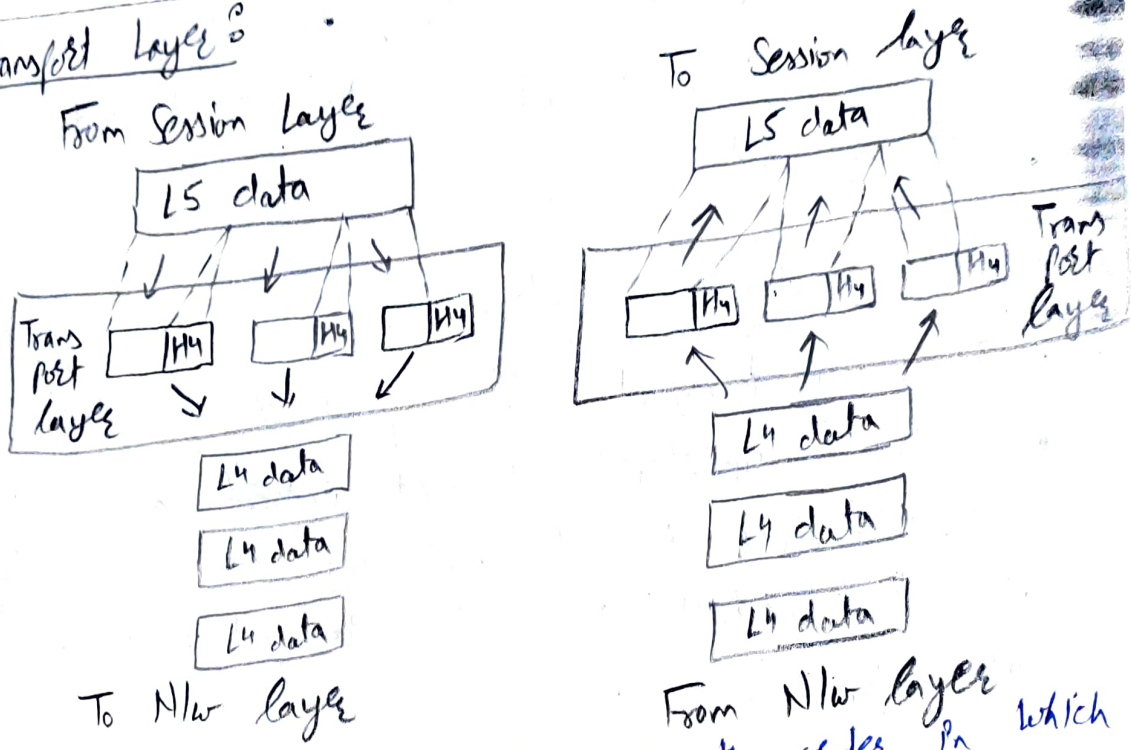




Functions:

- Internetworking: This is a main responsibility of Nlw layer. provides a logical connectn blw diff. devices.
- Addressing: adds S and D add. to the header of the frame. Addressing used to identify the device on the internet.
- Routing: Determines best optimal path out of the multiple paths from S to D.
- Packetizing: Nlw layer receive the pkts from the upper layer and converts them into pkts. It is achevicled by Internet Protocol (IP).
- Fragmentation: breaking the pkts into smallest individual data units that travel through diff. n/w.

4) Transport Layer:



- Ensures that msg are transmitted in the order in which they are sent and there is no duplication of data.
- Responsibility is transport the complete data.
- Receive the data from upper layer & converts them into smaller units known as segments.
- This layer can be termed as end to end layer as it provides a pt.-to-pt. connectn b/w source & destination to deliver the data reliably.

Two Protocols used:

1) Transmission Control Protocol: standard protocol that allows the sys. to comm^n over the internet.

- Establish & maintain a connectn b/w hosts
- When data is sent over the TCP connectn, then the TCP protocol devicides the data into smaller units known as segments. Each segment travels over the Internet using multiple routes, and they arrive in diff. orders at the destination. The transmission Control Protocol reorders the pkts. in the correct order at receiving end.

2) User Datagram Protocol:

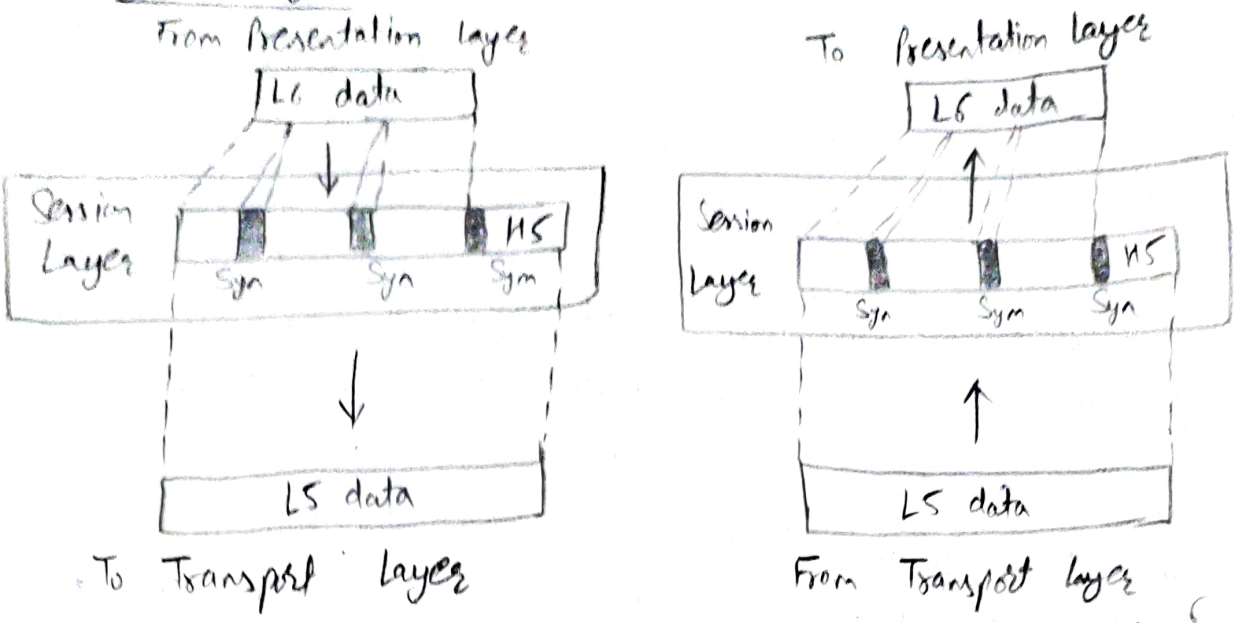
- It is a transport layer protocol.
- It is an unreliable transport protocol as in this case receiver does not send any ack. when the pkt is received, the sender does not wait for any ack.

Functions:

- **Service-point addressing**: Comp. run several prog. simultaneously. The transmission of data from S to D not only from one comp. to another comp. but also from one process to another process. The TL adds the header that contains the addl known as service pt. addl. or port addl.
  - ↳ The responsibility of N/w layer is to transmit the data from one comp. to another comp.
  - ↳ The responsibility of TL is to transmit the msg to the correct process.

- Segmentation & Reassembly: When the TL receives the msg from the upper layer, it divides the msg into multiple segments, and each segment is assigned with a sequence no. that uniquely identifies each segment. When the msg has arrived at the D, then the TL reassembles the msg. based on their seq. no.
- Connection Control: TL provides two services Connectn oriented service & Connectionless service.
  - ↳ A connectionless service treats each segment as an individual pkt. & they all travel in diff. route to reach the D.
  - ↳ A Connectn oriented service makes a connectn with the TL at the D m/c. before delivering the pkt. All the pkt. travel in the single route.
- Flow Control: perform end-to end rather than across a single link.
- Error Control: Same as flow control. & ~~error~~ & ensures that msg. reach at the D without any error.

5) Session Layer:



- used to establish, maintain & synchronizes the interact^n b/w comm^n devices.

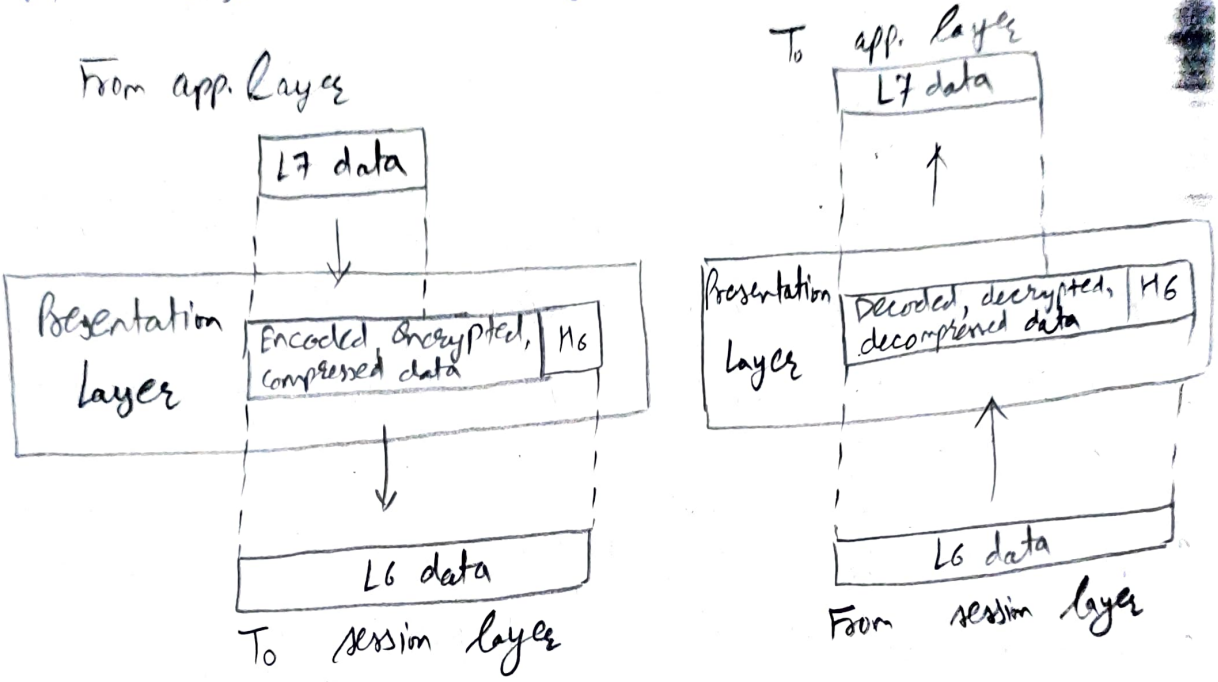
Function:

- ~~Digital Control: Comm^n b/w two process~~
- Dialog Control: Comm^n b/w two processes which can be either half-duplex or full-duplex.
- Synchronization: SL adds some checkpt. when transmiting the data in a seq. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpt. This process is known as Synchronizatn & Recovery.

6) Presentation Layer:

- It concerned with the syntax and semantics of the info. exchanged b/w two sys.
- Act as a data translator for a n/w.

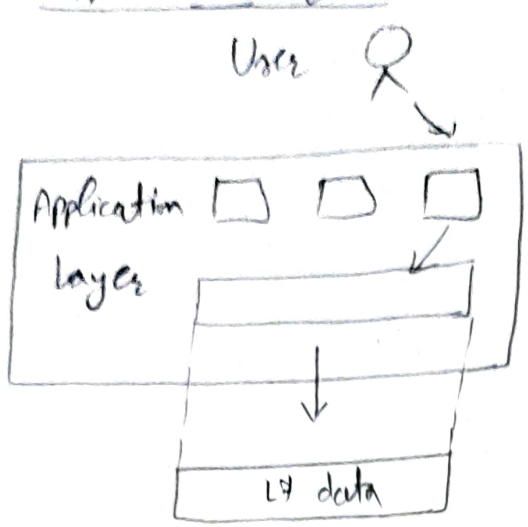
- It is a part of OS that converts the data from one presentation format to another format.
- It is also known as Syntax layer.



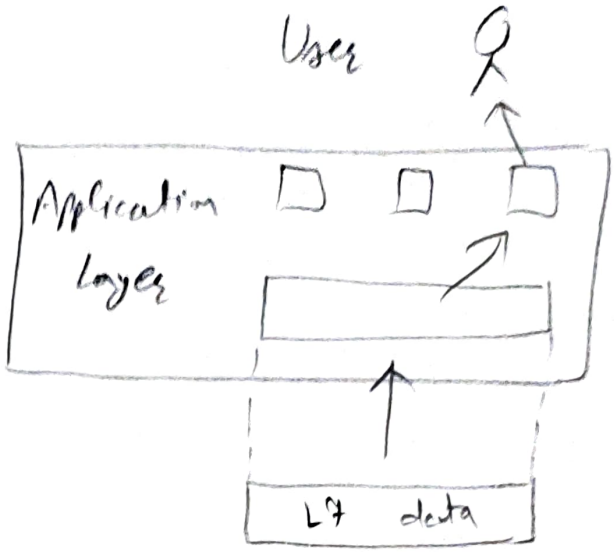
Function:

- Translation: Two sys. exchange the info. in the form of character strings, no. & so on. Diff. comp. use diff. encoding methods, the presentatn layer handles the interoperability b/w the diff encoding methods. It converts the data from sender-dependent format into a common format & changes the common format into receiver-dependent format at the receiving end.
- Encryption: maintain privacy.
- Compression: Reduces the no. of bits to be transmitted.

7) Application Layer:



To Presentation Layer



From Presentation Layer

- This layer serves as a window for users and app. processes to access n/w service.
- Handles issues such as n/w transparency, resource allocation etc.
- performs app. layer fun".
- provides n/w services to end user.

Functions:

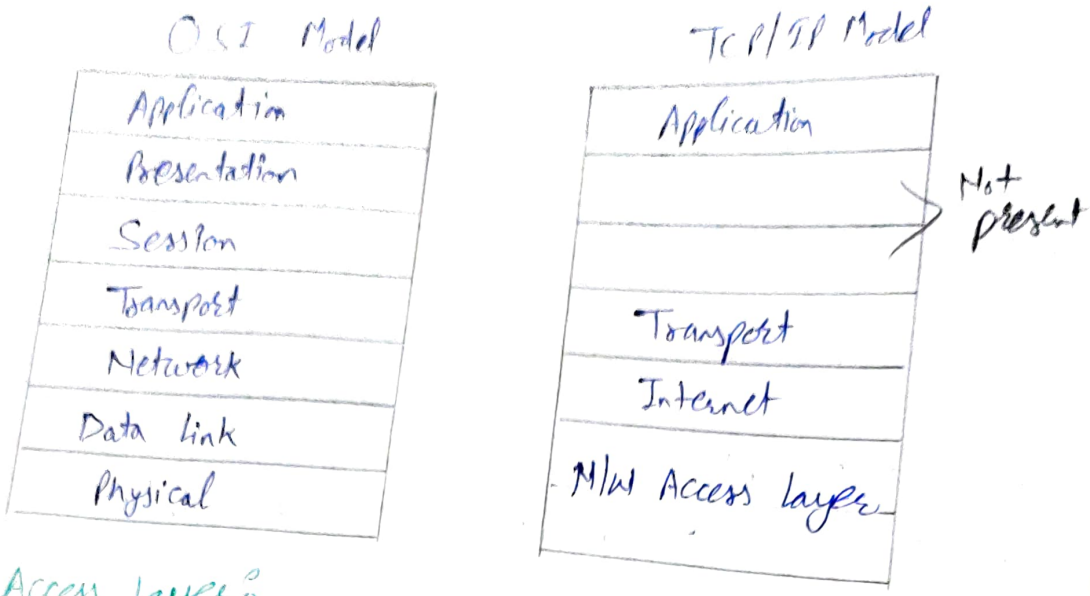
- File Transfer, Access and Management (FTAM): Access the files in a remote comp., retrieve the files from a comp. & to manage the files in a remote comp
- Mail Services: facility for email forwarding & storage.
- Directory Services: provides distributed DB sources and is used to provide that global info. about various obj.

TCP/IP Model:

- Stands for Transmission Control Protocol / Internet Protocol.
- It is a set of conventions or rules and methods that are used to interconnect n/w devices on the Internet.
- OSI was designed to describe the fun^n of the comm^n system by dividing the comm^n procedure into smaller and simpler components.
- TCP/IP was designed and developed by department of defense (DoD) in 1960s and is based on standard protocols.
- TCP/IP is a concise version of the OSI model.

4 Layers:

1) Process / Application Layer
2) Host - to - Host / Transport Layer
3) Internet Layer
4) N/W Access layer / Link layer



1) N/w Access layer:

- It is a combinat^n of DLL and Phy. layer. of the OSI.
- It looks out for H/w addressing and protocols present in this layer allows for the physical transmission of data.

2) Internet Layer:

- This layer parallel to OSI n/w layer.
- It is responsible for logical transmission of data over the entire n/w.

Protocols are:

1) IP:

↳ Stands for Internet Protocol.

↳ responsible for delivering pkt. from S host to D host by looking at the IP addresses in the pkt headers.

↳ IP has two versions: IPv4 & IPv6

IPv4: most of the websites are using currently.

IPv6: limited in no. when compared to the no. of users.

ii) ICMP:
- Stands for Internet Control Msg. Protocal.
- Encapsulate with IP datagrams.
- Responsible for providing hosts with info. abt n/w prob.

iii) ARP:
- Stands for Address Resolution Protocal.
- find h/w add. of a host from a known IP add.
- Types of ARP: Reverse ARP, Proxy ARP, Gratuitions ARP and Inverse ARP.

3) Transport Layer:
- Responsible for end-to-end Commⁿ and error-free delivery of data.
- It shields the upper-layer app. from the complexities of data.

i) Transmission Control Protocal (TCP):
- It is known to provide reliable and error-free commⁿ b/w end sys.
- performs sequencing & segmentation of data.
- It has ack feature & control the flow of data through flow control mechanism.

- ↳ very effective but lot of overhead.
- ↳ ↑↑ overhead, ↑↑ cost. ↳ Connection oriented protocol.

ii) User Datagram Protocol (UDP):

- ↳ It is the go-to protocol if your app. does not require reliable transport as it is very cost-effective.
- ↳ Connectionless protocol.

4) Application Layer:

- performs the fun^n of top three layers of OSI model: Application, Presentation & Session.
- responsible for node-to-node comm^n.
- protocols present: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD.

i) HTTP and HTTPS:

↳ stands for Hypertext transfer Protocol.

↳ used by the World Wide Web to manage comm^n b/w Web browsers and servers.

↳ HTTPS stands for HTTP - Secure.

↳ It is a combinat^n of HTTP with SSL (Secure Socket Layer).

↳ efficient in cases where browsers need to fill out forms, sign in, authenticate and carry out bank transactions.

ii) SSH:

↳ stand for Secure Shell.

↳ It is a terminal emulation slw similar to Telnet.
↳ maintain encrypted connectn.
↳ Set up a secure session over a TCP/IP connectn.

iii) NTP?

↳ Stands for Network Time Protocol.
↳ used to synchronize the clocks on our comp. to one standard time secure.
↳ useful in Bank transactn.

* Difference b/w TCP/IP and OSI Model?

TCP/IP	OSI
1) Transmission Control Protocol.	Open System interconnection.
2) has 4 layers.	has 7 layers.
3) More reliable	less reliable.
4) does not have very strict boundaries.	has strict boundaries.
5) Horizontal approach.	Vertical approach.

6) uses both session and presentation layers in app. layer	uses diff session & presentation layers.
7) developed protocols then model.	developed model then protocol.
8) TL does not provides assurance delivery of pkts.	provide.
9) N/W layer provides only Connect^less servie.	Connect^ Oriented, Connect^ less
10) protocols cannot be replaced easily	protocols are better covered and is easy to replace.

6