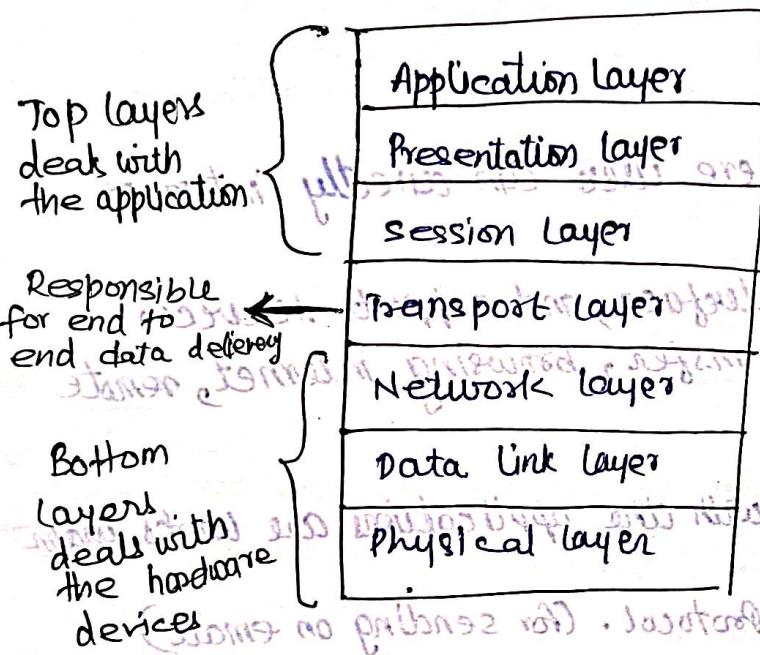
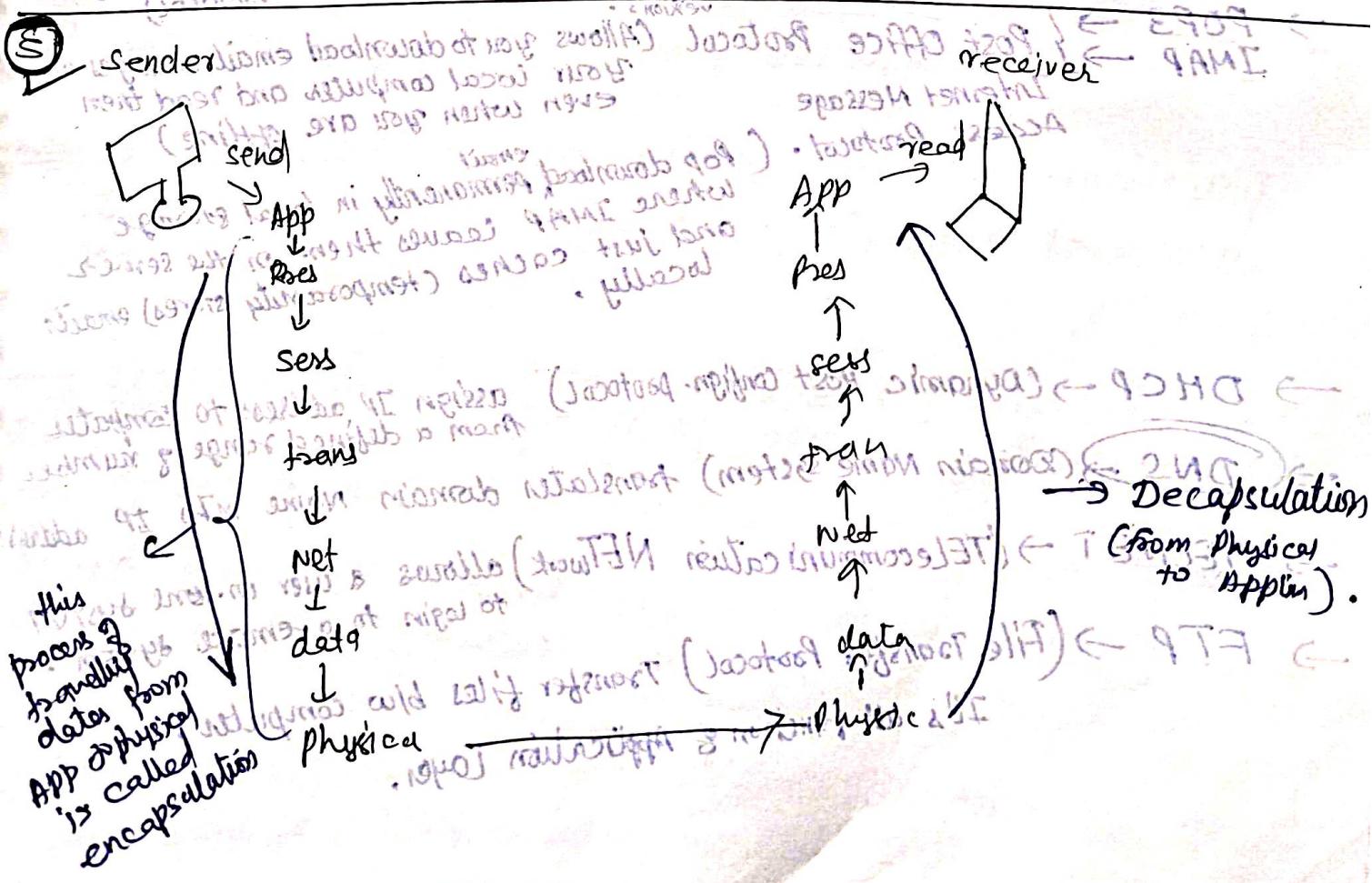


OSI model → Open system interconnection model. Developed by ISO in 1984.

⇒ OSI model has seven layers. It tells how data travel in a network.



↳ Application layer: deals with the application. Presentation layer: deals with presentation. Session layer: deals with session. Transport layer: responsible for end-to-end data delivery. Network layer: deals with network. Data Link layer: deals with data link. Physical layer: deals with physical.



5

so normally we say physical layer is the first layer of OSI model. It's is bcoz all physical connectivity takes place in this physical layer.

If no physical layer then no network at all.

• Protocol in network

③ Functions of each layer :-

① Application layer.

→ Only layer where user can directly interact with the data.

→ This layer provides user interface, and supports services such as mail access, file transfer, browsing internet, remote desktop connection etc.

→ The protocols that communicate with the applications are works under this layer! ex:-

→ SMTP → Simple Mail Transfer Protocol. (for sending an email)

→ HTTP → For Browsing internet via web browser. (Hyper Text Transfer Protocol)

→ POP3 → Post Office Protocol (Allows you to download email messages on your local computer and read them even when you are offline)
→ IMAP → Internet Message Access Protocol. (Pop download emails permanently in local storage where IMAP leaves them on the server and just caches (temporarily stores) emails locally.)

→ DHCP → (Dynamic Host Confign. protocol)

assign IP address to computer from a defined range & number

→ DNS → (Domain Name system) translates domain name into IP address

→ TELNET → (TElecommunication NETwork) allows a user on one system to login to a remote system.

→ FTP → (File Transfer Protocol) Transfer files b/w computer.
It's all function of Application Layer.

2 Presentation Layer :- 6th layer of OSI model.

⇒ This layer is responsible for translation, encryption and compression.



To windows and in term in Linux, both same thing will be
different for windows and emit same sent

⇒ Encryption → Plain text to cipher text.

⇒ Compression → Reducing the size of data by compressing it so that data can travel in the network with superfast speed.

at the border of bnd compression and then streams to Encryption and then Transmission sent

⇒ The protocol works under this layer is SSL

SSL → (Secure Socket Layer) designed for securing connections between web clients and web servers over an unsafe network, such as internet.

3 Session Layer :- 5th layer of OSI Model.

⇒ It is responsible for dialog control, establishing the connection, manage connection and Terminate connection.

⇒ Dialog control :- Enter username & password in the dialog box before secure connection.

⇒ After good authentication connection is established

⇒ If there is some blockage or default then session layer will terminate the connection.

⇒ This layer also controls whether do send the data in Simplex, Half Duplex or Full Duplex form.

Simplex, Half Duplex, Full duplex mode :- (modes of communication)

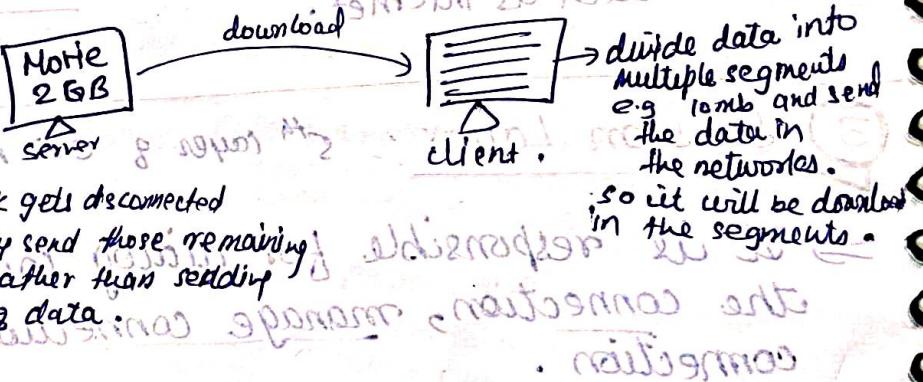
- ⇒ Simplex mode → the signal is sent in one direction
- ⇒ half duplex mode → the signal is sent in both directions, but one at a time.
- ⇒ Full duplex mode → the signal is sent in both directions at the same time. both devices can transmit the signal at the same time.

(4) Transport Layer :- 4th layer of OSI model.

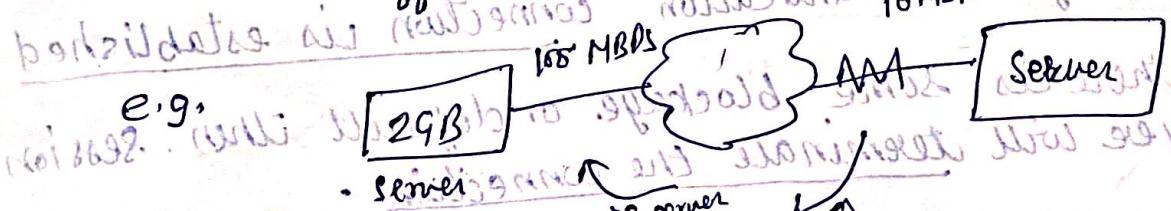
- ⇒ It converts data into segments and forward it to the network layer.
- ⇒ This layer is responsible for segmentation, flow control, error control and sequencing.

Segmentation →

(divide the files into multiple segments)

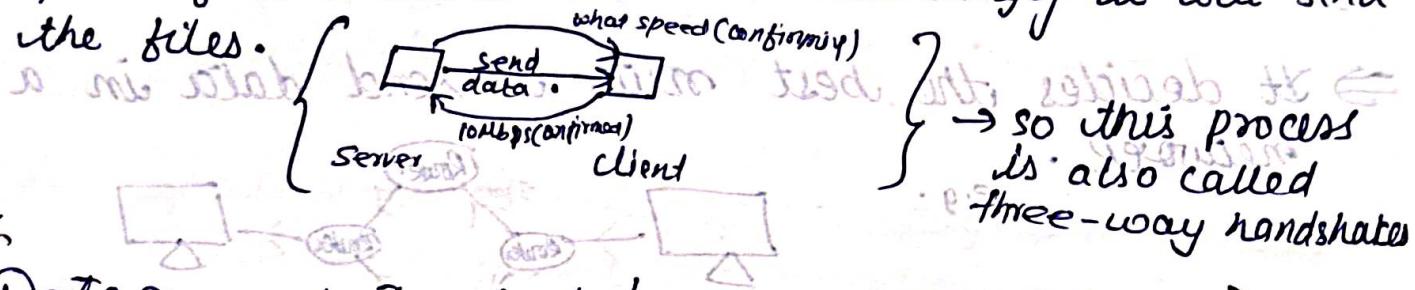


- ⇒ Flow control : There may be chances that server speed is different and client side internet speed is different.



If server continuously keeps sending then there network will be completely jammed. so because of this packets (data) will also get lost.

⇒ So in flow control first server confirms the internet speed & the client and then accordingly it will send the files.



Datagram at Transport layer are called Segments

⇒ Error control :- After sending the file, the server will also check whether all the files have successfully reached to client PC or not.

If there's some packet missing, then server will again send those files. so this process is called as error control.

⇒ Sequencing :- Sequencing occurs in receiver side.

So since data are transferred in the form of segments. So it might be possible that segments reached at Server side in random form (e.g. first 3rd segment then 1st etc). So in this sequencing transport layer will do its job. Once all the data reached to client side it will resequence the data in serial order.

Protocols works under this layer are: TCP & UDP.

⇒ **TCP** → (Transmission Control Protocol) we use this for transferring the files. It also do error checking and guarantee delivery. TCP more reliably. It sends files in form of segments. In arranged order.

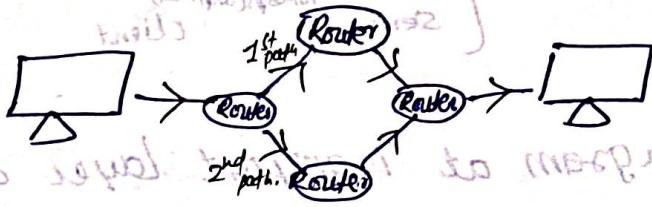
⇒ **UDP** → (User Datagram Protocol) used for video conferencing, playing online games.

It does not perform any error checking.

5 Network Layer :- Third layer of OSI model

⇒ It decides the best route to send data in a network.

e.g.



Which is better and suitable to message?

⇒ It converts the segments into packets and forward it to the Data link layer. (which is coming from transport layer)

⇒ This layer is responsible for logical addressing, routing etc.

⇒ Logical addressing :- (means IP addressing), Network layer adds both the source and the destination IP Address to the packets and forward it to the data link layer.

⇒ Routing :- Means deciding the best route to send the data in the network.

⇒ Devices works under this layer are router, bouler, L3 (Layer 3) switch and etc.

⇒ Protocols used under this layer are :-

⇒ IP Address (IPv4 & IPv6) → (Internet Protocol version 4 & 6)

it is a numerical label assigned to each device connected to a computer network that uses Internet Protocol for communication.

⇒ ICMP → (Internet Control Message Protocol) is an error-reporting protocol network devices like routers use to generate error messages to the source IP address when network problems prevent delivery to a IP packets.

⇒ IGMP → (Internet Group Management Protocol) is used by IP hosts to report their host group memberships to any immediately-neighbouring multicast routers.

⇒ IPsec → (Internet Protocol Security) uses cryptographic security services to protect communications over IP networks.

⇒ Routing Protocols :-

⇒ RIP → (Routing Information Protocol) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network. It uses port number 520.

⇒ IGRP → (Interior Gateway Routing Protocol) is a distance vector interior gateway protocol developed by Cisco. It is used by routers to exchange routing data within an autonomous system.

⇒ EIGRP → (Enhanced IGRP) is an advanced -vector routing protocol used for automating routing decisions and configurations.

⇒ OSPF → (Open shortest Path first) is a routing protocol for Internet Protocol networks. It uses a link state joining flooding algorithm and falls into the group of interior gateway protocols, operating within a single autonomous system.

The router creates a shortest Path first (SPF) tree using Dijkstra's algorithm on the LSDB and a routing table can be derived from the SPF tree which contains the best route to each other.

⇒ Datagram in Networks layer is called as Packets. and forward to data link layer

⑥ Data links layer :- 2nd layer of OSI model

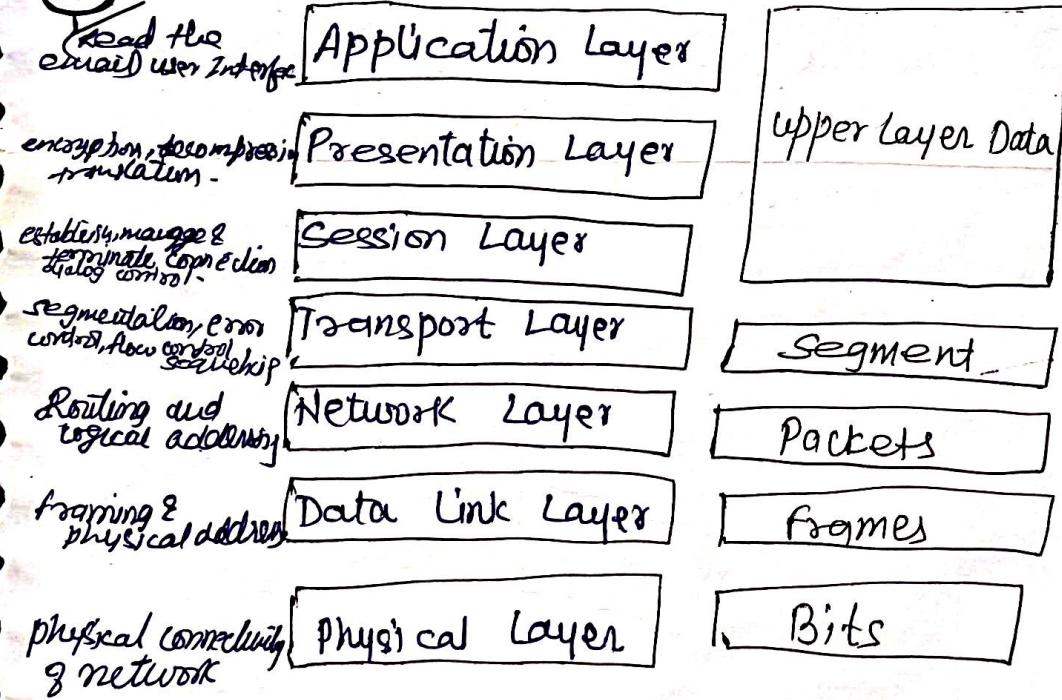
- ⇒ It provides connection between hosts on same network.
- ⇒ It converts the packets into frames and forwarded to the physical layer.
- ⇒ This layer is responsible for framing and physical Addressing. (means add NIC address to the packets)
- * ⇒ Devices works under this layer are Switch, Bridge and NIC.
- * ⇒ Protocols used in this layer are :-
- ⇒ PPP → (Point-to-Point Protocol) is a data link layer communication protocol between two routers directly without host or any other networking in between.
- ⇒ PPTP → (Point-to-Point Tunneling Protocol) is a networking standard for connecting to a virtual private networks, or VPNs.
- ⇒ ARP → (Address Resolution Protocol) is a protocol used by the IP, specially IPv4, to map IP network addresses to the hardware addresses used by a data link protocol.
- ⇒ RARP → (Reverse ARP) is a networking protocol used by a client machine in a local area network to request its internet protocol address (IPV4) from the gateway-router's ARP table.
- * ⇒ Data frame at Data link layer are called as frames.

7 Physical Layer :- 1st layer of OSI Model.

- ⇒ In Physical Layer all the physical connectivity of a network takes place, such as connectivity of devices using wires.
- ⇒ It converts data into bits and forward it to the physical layer available on receiver side.
- ⇒ Devices works under this layer are: Hub, repeaters, cables, etc.
- ⇒ Datagrams at Physical layer called bits.



OSI Model Layers and its datagram



Layers	Protocols	Devices
Application	FTP, TELNET, DHCP, HTTP, DNS, POP3, SMTP etc.	Server, PC
Presentation	SSL	—
Session	NetBIOS and SAP	—
Transport	TCP and UDP	Switch, Router, Firewall
Network (I)	IP Address (IPv4 & IPv6), ICMP, ICNPv6, IGMP, IPsec and Routing Protocols: RIP, IGRP, EIGRP, OSPF etc.	Router, BRouter, L3 switch etc.
Data link (P)	PPP, PPTP, ARP and RARP etc	Switch, Bridge, NIC etc.
Physical	Physical connectivity takes place	HUB, REPEATER, CABLES etc.