Computer Networking

Network : A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications.

In simple word, computers connecting together that is a network.

Internet : The connection of networks is called as Internet.

I.e, the internet is a vast network that connects computers all over the world.

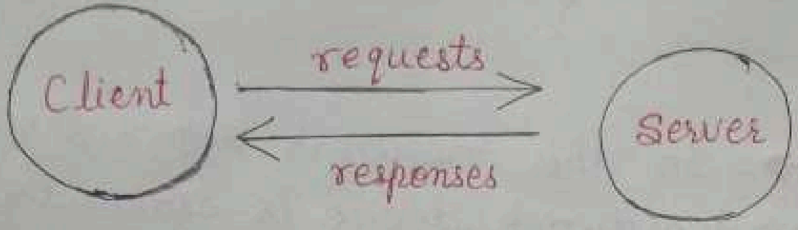
⇒ Through the internet, people can share information and communicate from anywhere with an internet connection. But, there is certain rules and conventions used in this communication, these are called as Protocol.

Protocol : Protocol is a set of rules or an ~~aggreement~~ agreement between the two communicating machines about how the communication link should be established, maintained and released.

Q. Why we need these rules?

→ Protocols are needed because it is important for the receiver to understand the sender.

Clients and Servers



A server is simply a computer, that makes the network resources available and provides service to other computers when they request it.

A client is the computer running a program that requests services from a server.

Packets:

A packet is a small segment of a larger message. Basically, when data is sent across the web, it is sent in thousands of small chunks.

- There are multiple reasons, why data is sent in small packets?

→ They are sometimes dropped or corrupted, and it's easier to replace small chunks when this happens.

→ The packets can be routed along different paths, making the exchange faster and allowing many different users to dowload the same website at the same time. If each website was sent as a single big chunk, one user could download it at a time, which obviously would make the web very inefficient and not much fun to use.

IP address : IP address stands for Internet Protocol address.

It is an identifying number that is associated with a specific computer or computer network.

⇒ Every single device on the internet that can talk to each other they have ip address means, when connected to the internet, the ip address allows the computers to send and receive information.

Each address is a string of numbers separated by periods. There are 4 numbers in total and each number can range between 0 and 255. So, the full IP addressing range goes from 0.0.0.0 to 255.255.255.255

→ Your IP address is assigned to your device by your ISP(Internet Service Provider).

→ All devices which are connected to same modem or router have same IP address.

Port Number : A port number is the logical address of each application or process that uses a network, means, port number identifies which application to send the data in that particular device.

* Ports are basically 16-bit numbers.

→ Total ports number $= 2^{16} = 65,536$

→ Reserved port numbers = 0 to 1023
(used by well-known protocol services like for HTTP = 80)

→ Registered Port numbers = 1024 to 49151

→ Private Port number = 49152 to 65,536
(used by anybody)

# Ways through which communication between devices occurs :—

1> Guided way :- For this there should be a point-to-point physical connection.
for eg. :- Two computers are connected with a wire.

2> Unguided way :- In this way, communication happens but there is no any physical connection. i.e, wireless. e.g → Infrared

* Guided (or wired) :→ Co-axial cable, Twisted pair cable, Optical fiber cable.

* Unguided (or wireless) :→ Infrared , Microwave links

* Classification of Networks :-

- Local Area Networks (LAN) :

LAN is a network which is designed to operate over a small physical area such as an office, factory or a group of buildings.

- Metropolitan Area Network (MAN):
  A MAN is basically a bigger version of a LAN. It is designed to extend over a larger area such as an entire city.

- Wide Area Network (WAN):
  A WAN is a network that extends over a large geographic area i.e, across countries.
  It uses optical fibre cables.

* SONET :

SONET stands for Synchronous Optical Network. It is used to convert an electrical signal into an optical signal so that it can travel long distances.

* Frame Relay :

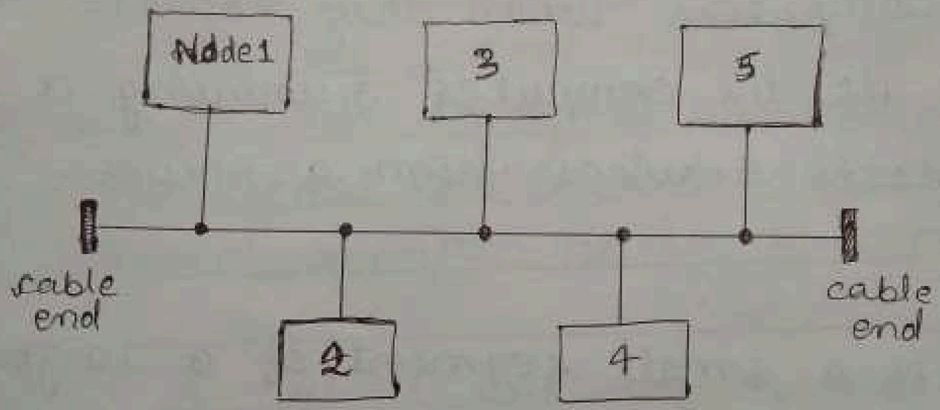
It is used to connect two or more LAN over large distances.

* Network Topology :-

It is used to explain the manner in which a network is physically connected.

Types :

① **Bus Topology :→** In this network ~~setp~~ setup, each computer and network device is connected to a single cable or backbone.



* Advantages :-

→ Best suited for small networks.

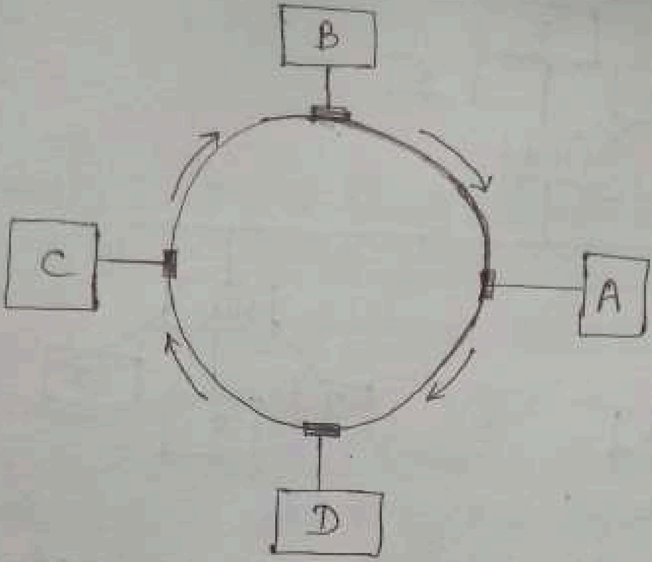
→ Easy to setup, handle and implement.

* Disadvantages :-

→ A fault in this setup leads to entire network failure.

→ Only one computer can transmit at a time.

② **Ring Topology :→** In this network setup, each computer is connected to the next computer, and the last one is connected to the first to form a ring.

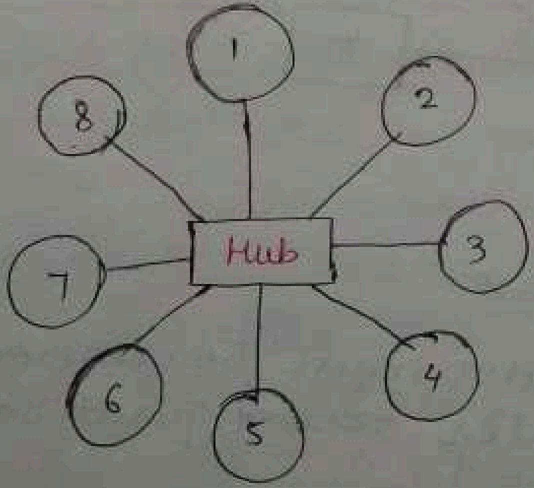


Problems :

→ If any link breaks then the entire network will be disabled.

→ If we want to send any data from one computer to other, it has to pass through all the intermediate computers, which makes transmission slower.

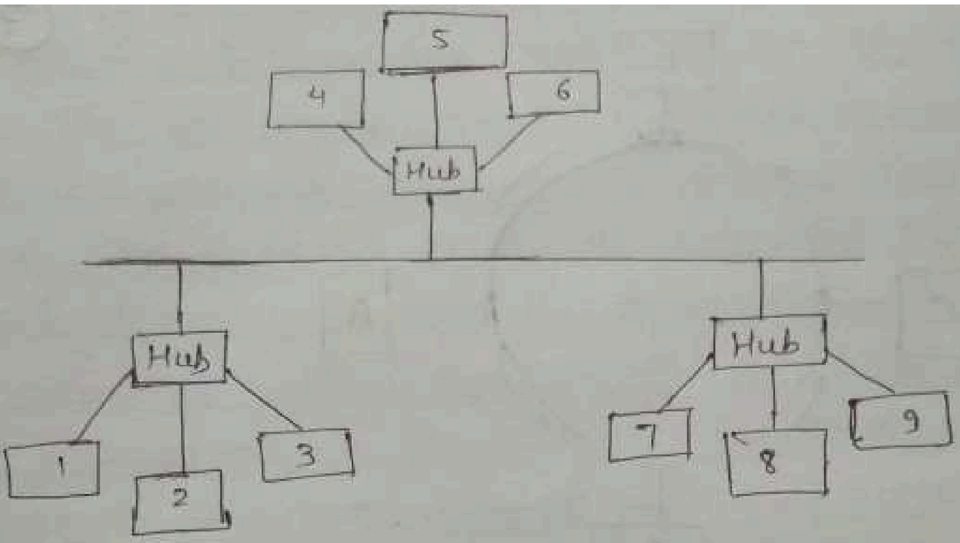
③ Star Topology :- In this, all the computers are connected to a central device called hub. There is no direct connections among the computers.



Problems :

→ If the central hub fails, the whole network fails to operate.

④ Tree Topology :- This network setup is combination of Bus and star topology.

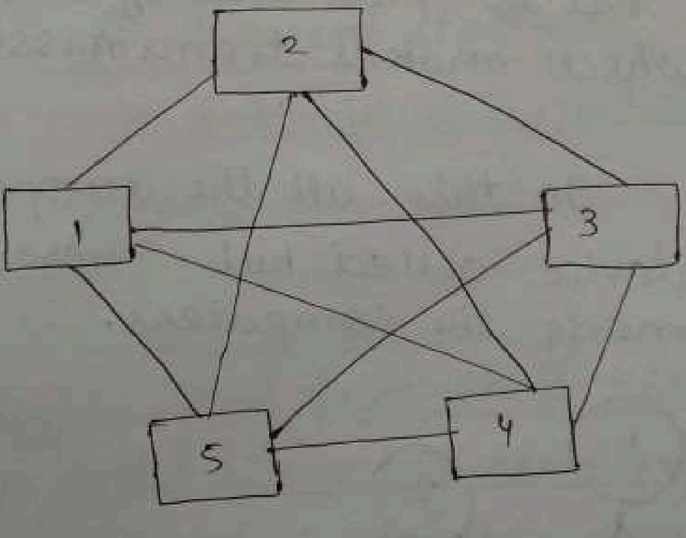


Problems:

→ If main cable breaks, the whole network fails.

→ Difficult to configure.

5 Mesh Topology :- In mesh topology, every device is physically connected to every other device.



Problems:-

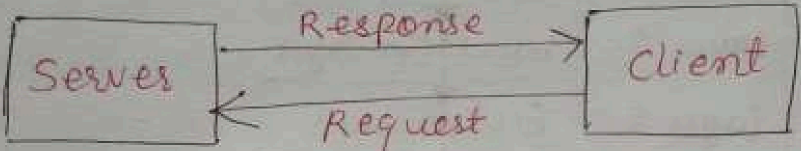
→ Cabling cost is more.

→ Since, every computer must be connected to every other computer reconfiguration is difficult.

* Client - Server Network :

In client-server network relationships, certain computers act as server and other act as clients.

- A server is simply a computer, that makes the resources available and provides service to other computers when they request it.
- A client is the computer running a program that requests services from a server.

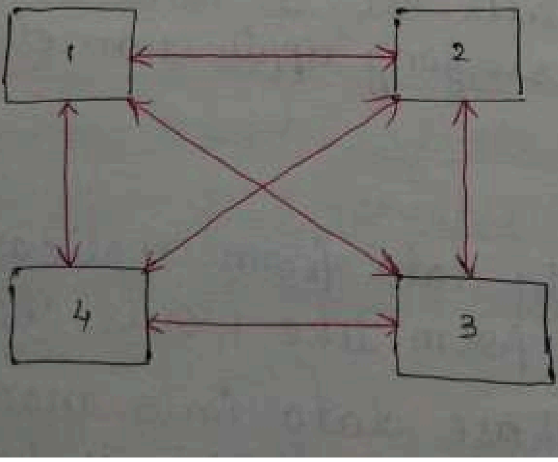


* Data Centre — It is a collection of huge no. of computers.

- It may have Static IP (IP that do. not change).
- They have very good internet connections and have high upload speed.

* Peer-to-Peer Networks :

In Peer-to-Peer network, every computer can function as both a client and server. There are no servers. P2P do not have a central control system.



* OSI Model :—

→ OSI stands for Open System Interconnection.

→ An OSI model is a layered framework for the design of network systems that allows for communication across all types of computer systems.

→ There are 7 layers in the OSI model.

Layer 7	Application layer
Layer 6	Presentation layer
Layer 5	Session layer
Layer 4	Transport layer
Layer 3	Network layer
layer 2	Data link layer
Layer 1	Physical layer

* Application layer :

→ Top-most layer in OSI model.

→ Implemented in software.

→ As the name suggests, it's an application layer. So, the user interact with their applications, send messages, files, emails, etc. It contains the app like browsers, messaging application etc.

* Presentation Layer :

→ This layer receives the data from application layer. These data is of the form like words, characters etc.

→ This layer convert those data into machine representable binary format. This is known as translation.

→ Formatting functions at this layer include Encoding, encryption, compression, etc.

* Session layer :

→ This layer helps in setting up and managing the connections and enables sending and receiving of data followed by termination of connected session.

→ Here, Authentication and Authorization takes place.

* Transport layer :

→ Data received from session layer is divided into small data units called segment. Every segment contains source and destination port as well as sequence number. sequence no. basically helps to reassemble the segments in the correct order.

→ The protocols operating at Transport layer is TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

* Network Layer:

→ Network layer basically works for the transmission of the received data segments from one computer to another that is located in different network.

→ Routers operates in this layer.

→ IP addressing done in this layer called logical addressing. This layer assigns the sender's & receiver's ip address to every segment and it forms an ip packet so that every data packet can reach to its correct destination.

→ Routing is performed here.

→ Load balancing is also done here.

* Data link Layer :

→ Physical addressing is done here.

→ Mac address are physical addresses.

→ Now, Mac addresses of sender and receivers are assigned to the data packet to form a frame. frame is a data unit of data link layer.

Mac address :- It is a 12-digit alphanumeric number of network interface of computer.

* Physical Layer :

→ Contains hardware

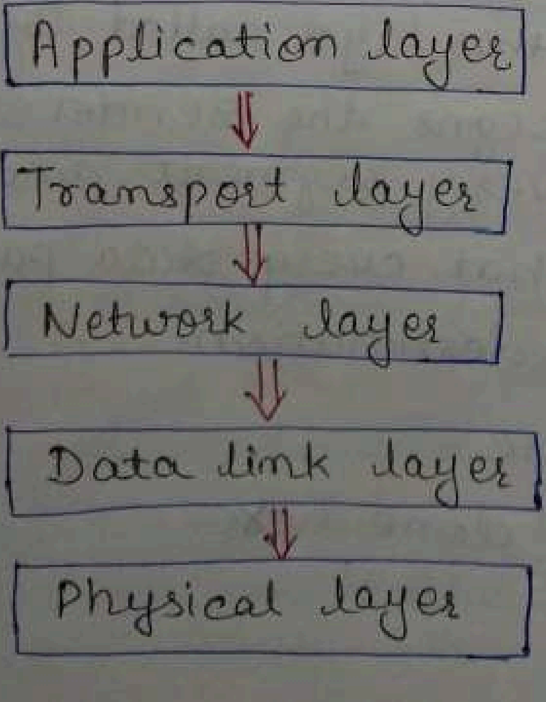
→ converts the digital bits into electrical, radio or optical signals.

* TCP/IP Model :—

→ The Transmission Control Protocol (TCP) and Internet Protocol (IP) are together known as TCP/IP protocol.

→ Developed by ARPA.

→ There are 5 layers in TCP/IP model.



Network Connecting Devices :

1. Repeater — A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. when the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

2. Hub — A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations.

Hubs can't filter data, so data packets are sent to all connected devices.

Types of Hub :-

- Active hub :- They have their own power supply and can clean, boost and relay the signal along the network. It serves both as a repeater as well as wiring center. They are used to extend maximum distance between nodes.
- Passive hub :- These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend distance between nodes.

3. Bridge :- A bridge operates at data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on same protocol. It has a single input and single output port thus making it a 2 port device.

Types of Bridges:

- Transparent Bridges :- In these bridges, the stations are completely unaware of the bridge's existence i.e, whether or not a bridge is added or deleted from the network.
- Source Routing Bridges :- In these bridges, routing operation is performed by source station and frame specifies which route to follow.

4. Switch :- It is a multi-port bridge with a buffer and a design that can boost its efficiency. It operates at data link layer. It can perform error checking before forwarding data, that makes it very efficient as it doesn't forward packets that have errors and forward good packets selectively to correct port only.

5. Routers :— It is a device like a switch that routes data packets based on their IP addresses. It mainly operates at Network layer. It normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets.

6. Gateway — It is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system.

7. Brouter :— It is also known as bridging router. It is a device which combines features of both bridge and router. It can work either at data link layer or at network layer. Working as router, it is capable of routing packets across networks and working as bridge, it is capable of filtering local area network traffic.

** Protocols : Application layer Protocols

web protocols:

* TCP/IP :

→ HTTP — Hyper Text Transfer Protocol
HTTP is designed for transferring a hypertext among two or more systems. HTML tags are used for creating links.

→ HTTPS — Hyper Text Transfer Protocol Secure
It is a standard protocol to secure the communication. Here, the transferring of data is done in an encrypted format.

→ DHCP — Dynamic Host Control Protocol
It basically allocates the IP address

to the devices that are connected to your network.

→ FTP – File Transfer Protocol
FTP allows users to transfer files from one machine to another. Types of files include text files, documents, program files, etc.

→ SMTP – Simple Mail Trasfer Protocol
It is used to send the email

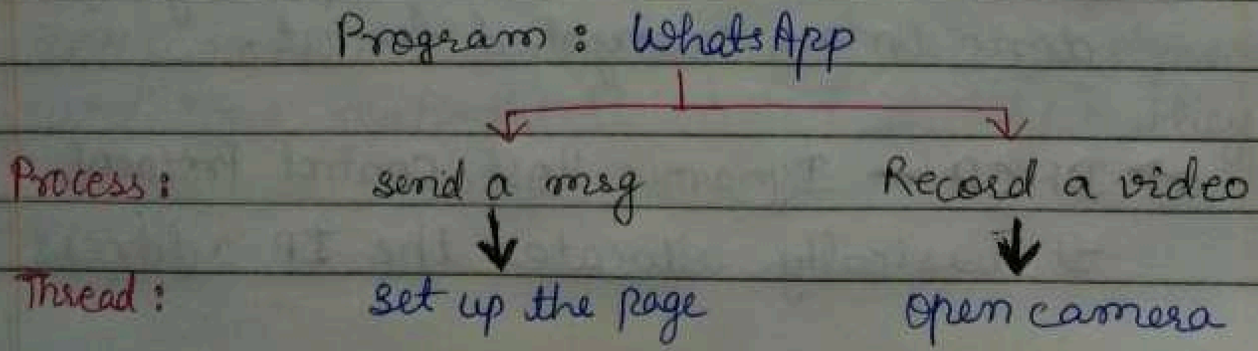
→ POP3 – Post Office Protocol, version 3
→ IMAP – Internet Mail Access Protocol
These protocols used to retrieve emails

→ SSH – Secure SHell

→ VNC – Virtual Network

* Telnet
Terminal Emulation Protocol
It is an application layer protocol that enables a user to communicate with a remote device using a telnet client.
It works on port 23.

How Applications communicates —



Program : WhatsApp

Process : send a msg — Record a video

Thread : set up the page — open camera

→ Process : Process is like one of the feature of the program on a running instance.

- One program can have many processes running at once.

→ Thread : Thread is a lighter version of process.

- One process can have multiple running thread.

Sockets : It is the interface between process and internet.

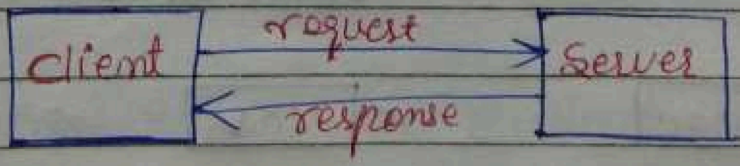
Ports :

⇒ IP address tells which device we are working with while ports tells us which application we are working with.

→ There may be possibility that many process of a single application is running like we have many chrome windows open. Now, the data we requested that is coming from other person that need to go to Google Chrome but which instance/processes of chrome. How it will know that ?

⇒ This can be resolved by using Ephemeral ports.

* HTTP :



→ It is a client-server protocol and it tells us how we request the data from the server and how server sends back data to the client.

→ when a client makes a request to the server, it is known as HTTP Request, and when a server sends back response to client, it is known as HTTP Response.

→ HTTP uses TCP.

→ It is a stateless protocol (server will not store any information about client by default).

HTTP Methods: It is basically telling the server what to do.

① GET : It means you are requesting some data.

② POST : client gives some data to server like in a web form, we give name, password, etc.

③ PUT : put data at a specific location

④ DELETE : delete data from the server.

* Status code / Error Code

when you send a request to the server, you need to know whether the request is successful or not For this, there are Status code like

200	-	request was successful
404	-	not found
400	-	bad request
500	-	Internal Server Error

•

Range		Class
1XX	→	Informational category
2XX	→	success codes
3XX	→	Redirecting purpose
4XX	→	client error
5XX	→	server error

Cookies :

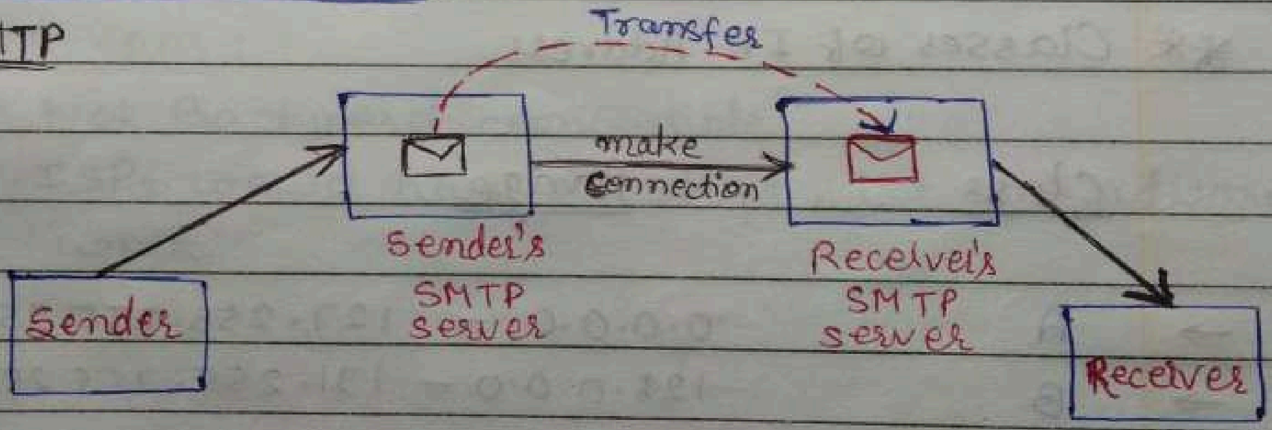
→ It is a unique string that stored on client's browser.
→ when you visit the web page for the first time, the cookie is set and whenever you make a new request, in the request header a cookie will be sent. Then the server will check its database and identify the state for that.

Third-Party Cookies :

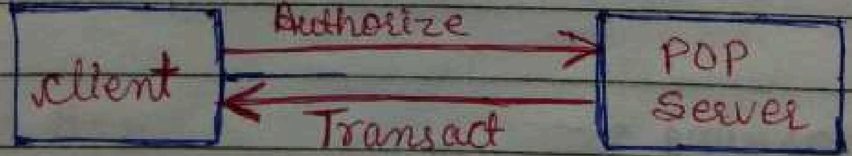
→ These are the cookies that are set for the URLs that you don't visit.

* How Email works :-

SMTP



POP



IMAP

→ Allows to view Emails on Multiple devices

* DNS - Domain Name System

→ Domain names are mapped to IP address.

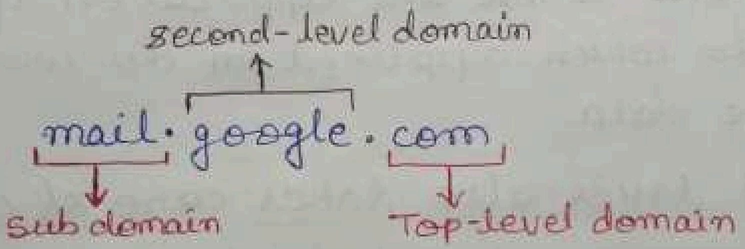
→ We use service to look up into this. The most popular service is DNS

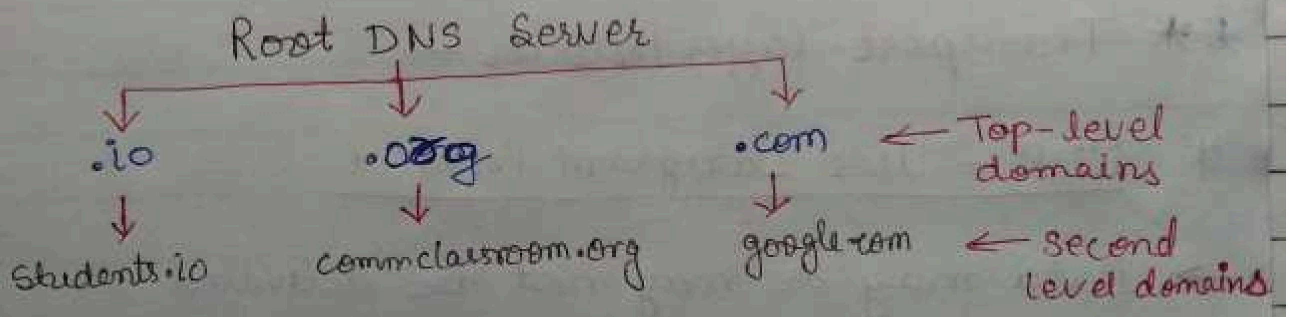
→ when we type google.com, it will use DNS to find the IP address of google's server.

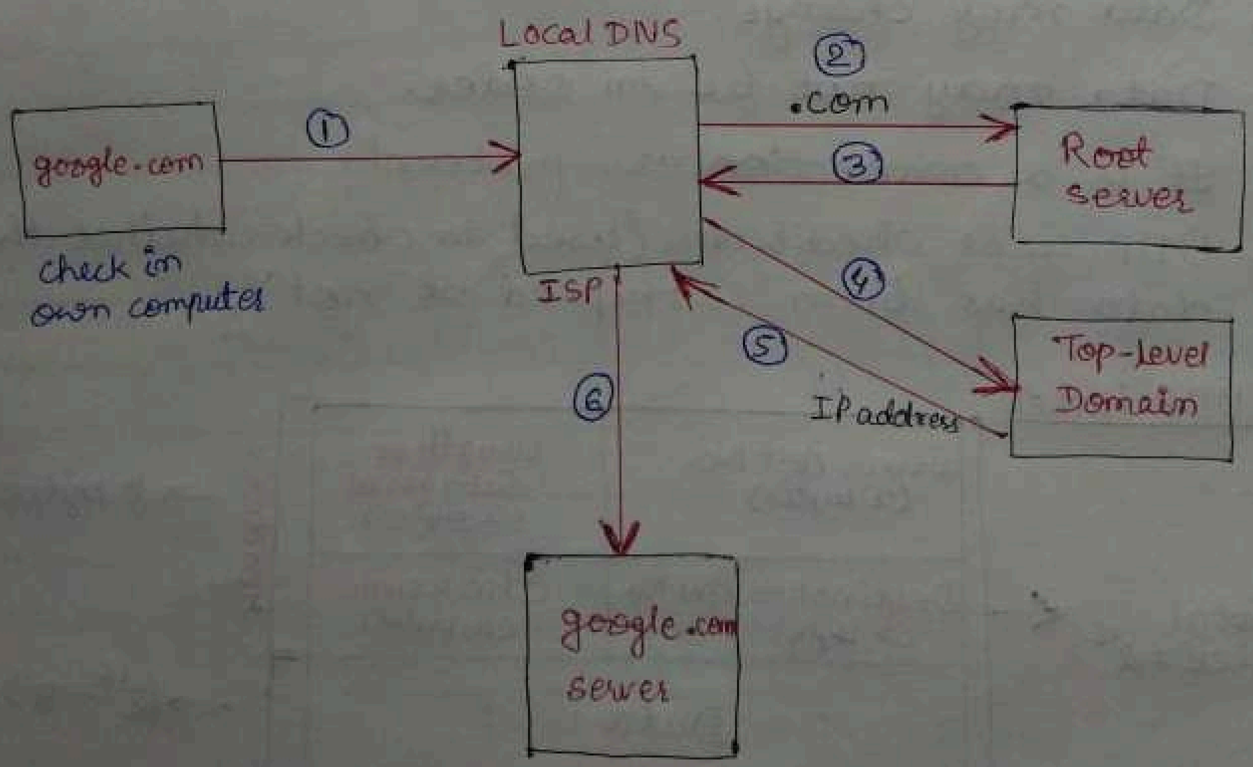
→ DNS are like an address book for websites.

→ when we type google.com, http protocol takes that domain name and use DNS to find the IP address and after that it connects to that server.

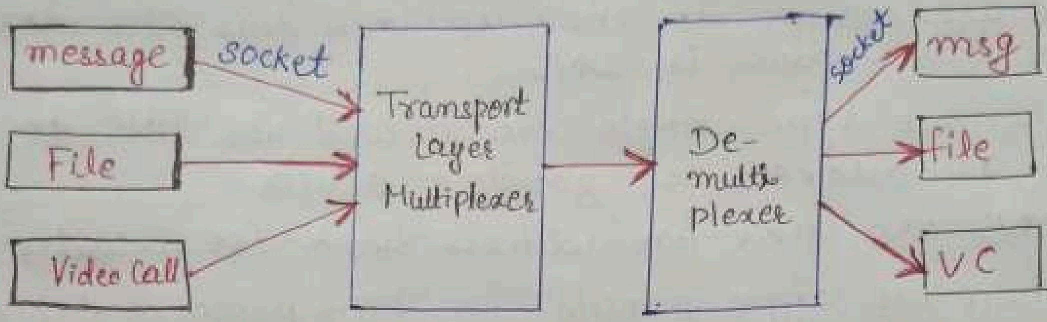
→ It is a directory/database service.







* Transport layer



→ Data travels in packets. Transport layer will attach the socket port nos. to that packet, that's why it knows where the application is coming from & to which application do we need to send the data.

→ Transport layer also takes care of congestion (or traffic).

→ Congestion Control algorithm built in TCP.

** Transport Layer Protocols —

* UDP – User Datagram Protocol

→ Data may or may not be delivered.

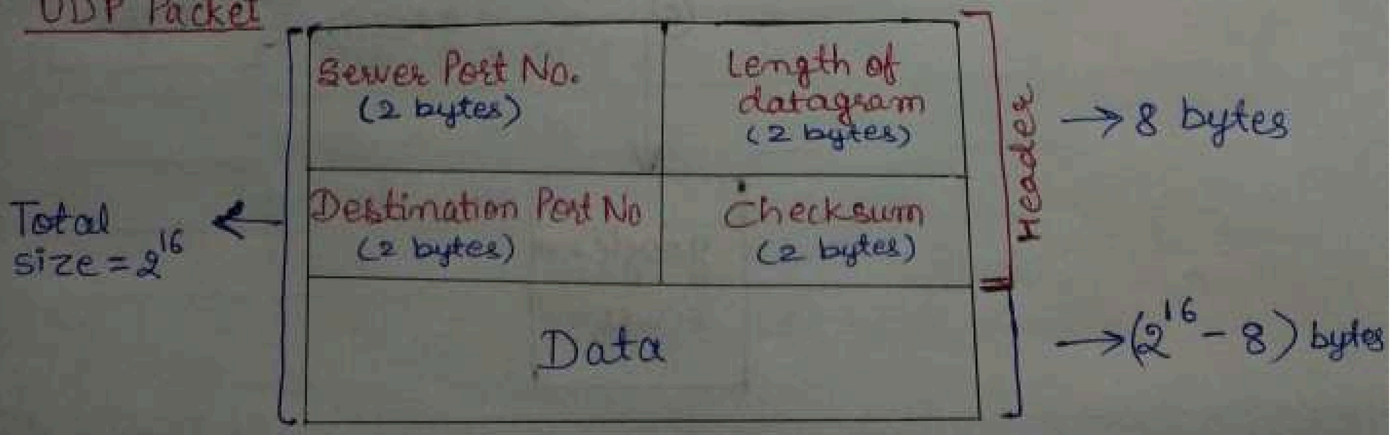
→ Data may change.

→ Data may not be in order.

→ It is a connectionless protocol.

→ UDP uses checksums (used to check whether the data has been corrupted or not).

* UDP Packet



Server Port No. (2 bytes)	Length of datagram (2 bytes)
Destination Port No (2 bytes)	Checksum (2 bytes)
Data	

* Use cases of UDP

- → It is very fast
- → video conferencing apps
- → DNS uses UDP (becoz it's fast).
- → Gaming

tcpdump -c 5 → to see only 5 packets

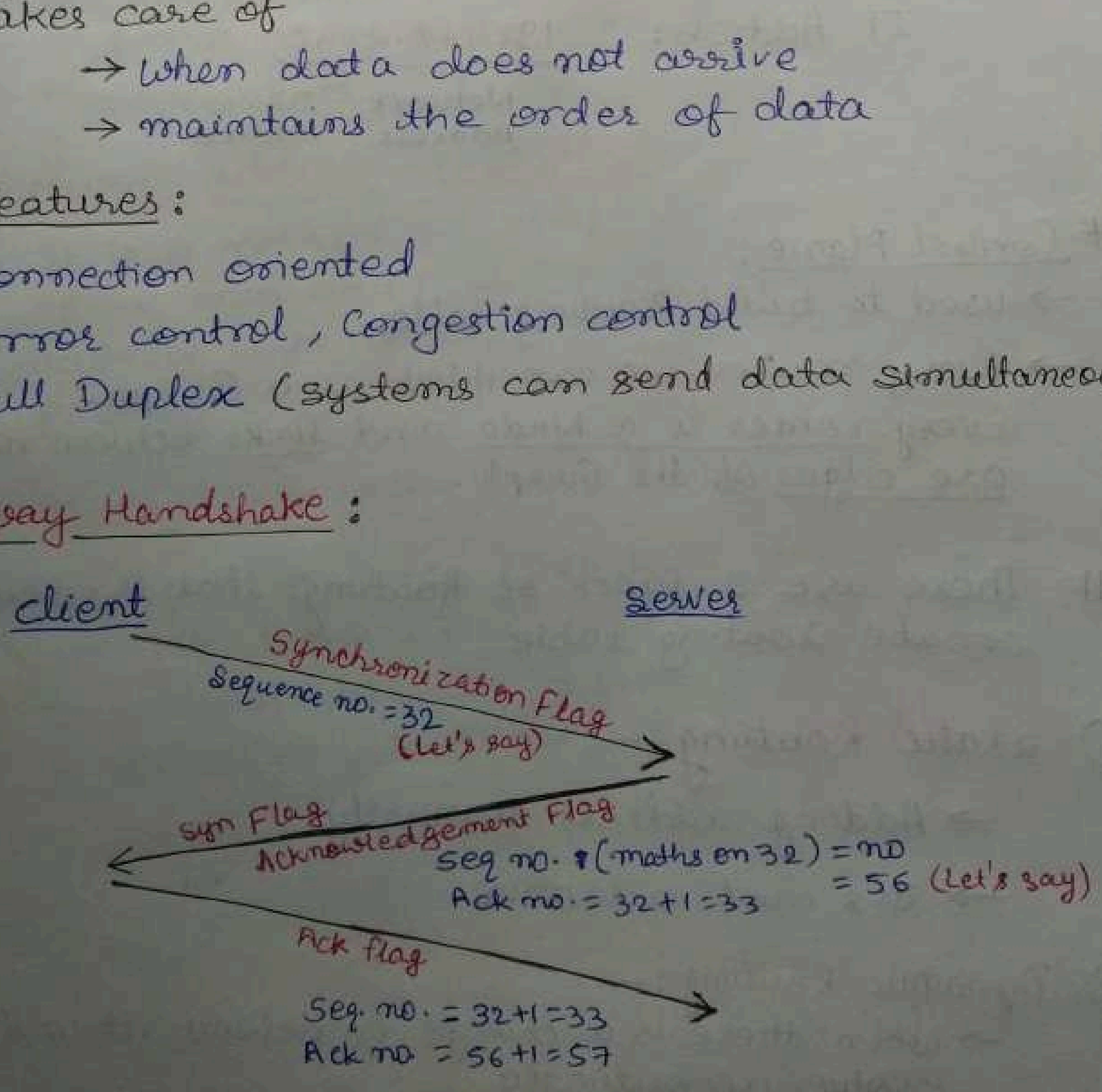
* TCP - Transmission Control Protocol

- → Transport layer protocol.
- → Application layer sends lots of raw data, TCP segments this data means, divide in chunks, add headers, checksums, etc. It may also collect the data from network layer and the smaller chunks are put into one in the receiver's end.
- → provide congestion control
- → Takes care of
  - → when data does not arrive
  - → maintains the order of data

** Features:

- → connection oriented
- → Error control, Congestion control
- → Full Duplex (systems can send data simultaneously).

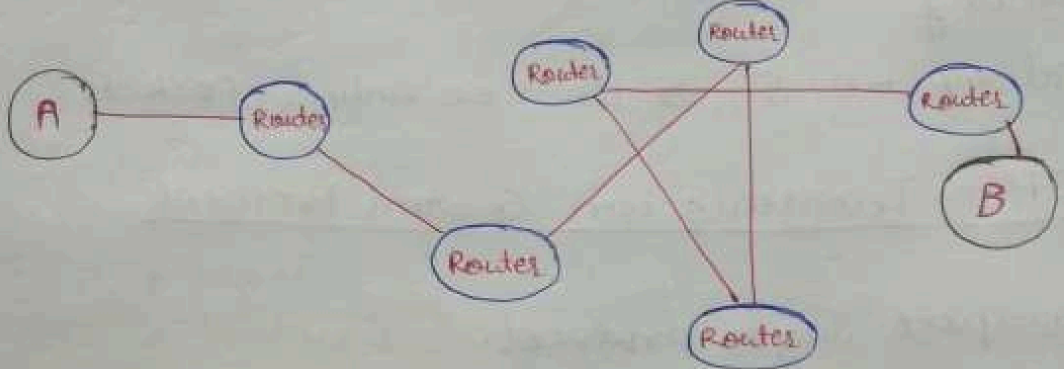
** 3-Way Handshake:



* Network Layer :

→ Here, we work with Router.

Transport → Segments
Network → Packets
Data Link → Frames



→ Every router has a Network Address.

→ Every router will check whether the packet is for that router or not. If not, then it will forward that using forwarding table (a part of routing table).

→ Forwarding table is just a data str.

IP Address: $\underbrace{192.168.2}_{\text{Network Address}}.\underbrace{30}_{\text{Device Address}}$

** Control Plane :

→ used to build Routing tables.

→ Every router, we can think as a Graph. Every router is a Node and links between routers are edges of the Graph.

There are 2 types of Routing that is used to create routing table

① Static Routing :—

→ Adding address manually.

→ It's not adaptive.

② Dynamic Routing :—

→ when there is a change in network, it will evolve accordingly.

* Network Layer Protocol

IP - Internet Protocol

IPv4 → 32 bits, 4-words
IPv6 → 128 bits

→ Blocks of IP addresses are assigned to the ISP This is known as Subnetting.

$$\underbrace{192 . 168 . 2}_{\text{Subnet ID}} . \underbrace{30}_{\text{Host ID}}$$

** Classes of IP Address

	Class	Range
→	A	0.0.0.0 - 127.255.255.255
→	B	128.0.0.0 - 191.255.255.255
→	C	192.0.0.0 - 223.255.255.255
→	D	224.0.0.0 - 239.255.255.255
→	E	240.0.0.0 - 255.255.255.255

Subnet Masking :-

Subnet mask is going to mask the network part of the IP address and leaves us to use host part.

192.0.1.0/24

Total = 32 bit
Subnet = 24
host = 8 ⇒ 192.0.1.0 - 192.0.1.255

Total no. of hosts = 256

Variable Length subnets :

→ You can set your own subnet length.

Eg. 15.0.0.0/30 → first 30 bits are subnet part

Reserved Address :

127.0.0.0/8

Eg → localhost – 127.0.0.1

Loopback addresses

** IPv4 : $2^{32} \approx 4.3$ billion no. of IP addresses

** IPv6 : $2^{32 \times 4} = 2^{128} = 3.4 \times 10^{38}$ no. of IP address

** IPv6 cons :

→ Not Backward compatible

→ ISPs would have to shift, lot of hardware work

** IPv6 Format

a : a : a : a : a : a : a : a

↓

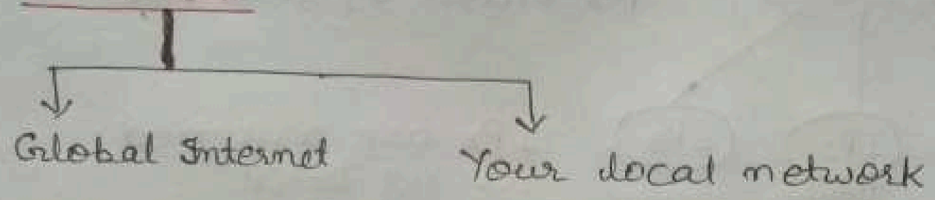
Hexadecimal (16 bit)

* Middle Boxes

→ They are extra devices that interact with packets

→ Mostly a network layer devices but also a transport layer device as well.

* Firewall



→ It filter out IP packets based on various rules.

- Address
- Modify packets
- Port numbers
- Flags
- Protocols

→ Stateless vs stateful firewalls

* Stateless firewalls :

→ doesn't maintain a state

* Stateful firewalls :

→ see the packets and maintain its state
It store in its cache memory

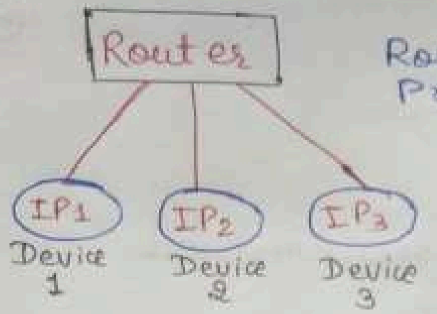
→ More Efficient

* Network address Translation :

→ It is a method of mapping an IP address space into another by modifying network address information in the IP header of packets

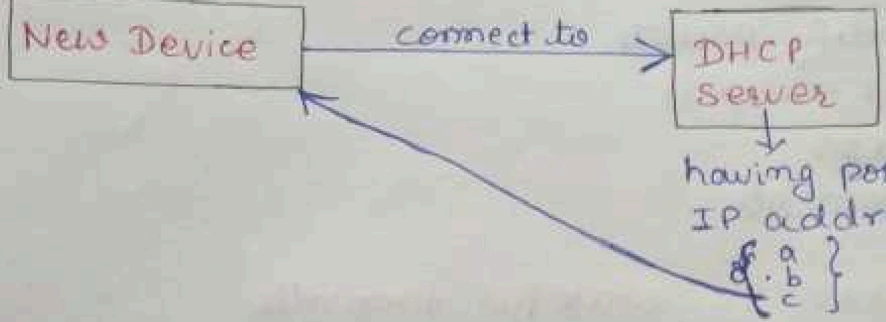
** Data Link Layer :

→ The data packets that we receive from the network layer, the DATA LINK LAYER is responsible to send these packets over a physical link.



Router has some IP address Provided by your ISP

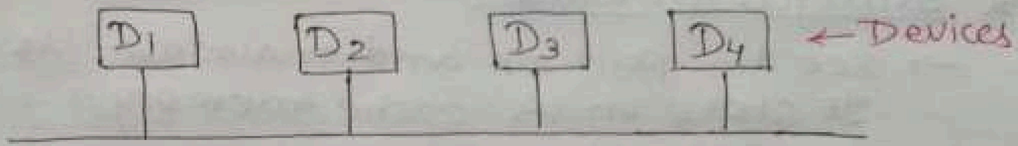
IPs are assigned using DHCP



DHCP assigns IP address to the devices

having pool of IP address

→ In data link layer, the devices communicate with each other using Data link layer address.



→ Let's say, device 1 needs to send some data to device 4. First D1 will check in its own cache. If it doesn't have then it will ask to other devices. This is known as ARP cache (Address Resolution Protocol).

→ All the devices that are connected will receive a message from ARP cache device, the message will be a frame.

→ Frame contains:

- → Data Link Layer address of sender
- → IP address of destination

NOTE: Data Link Layer address are known as MAC address (Media Access Control).