


Computer Networking Notes



Dhurika V

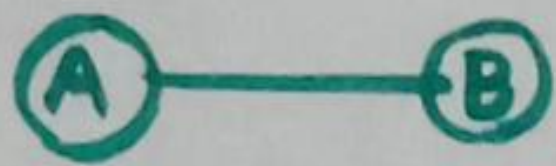
Computer Networking

What is Network?

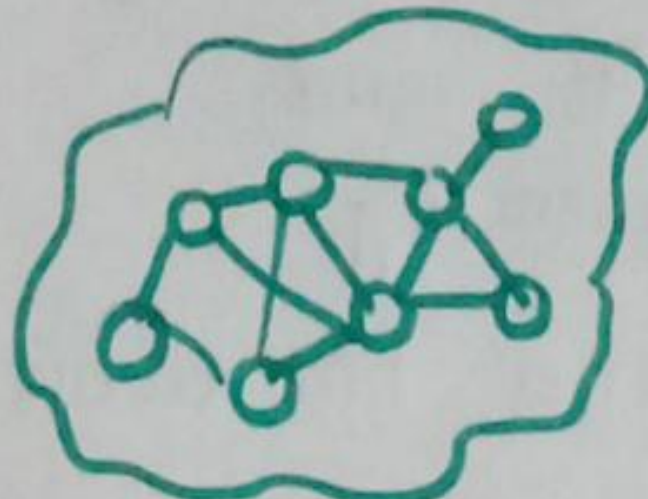
→ In simple terms, it just means computers connected together

Internet

→ A collection of these computer networks



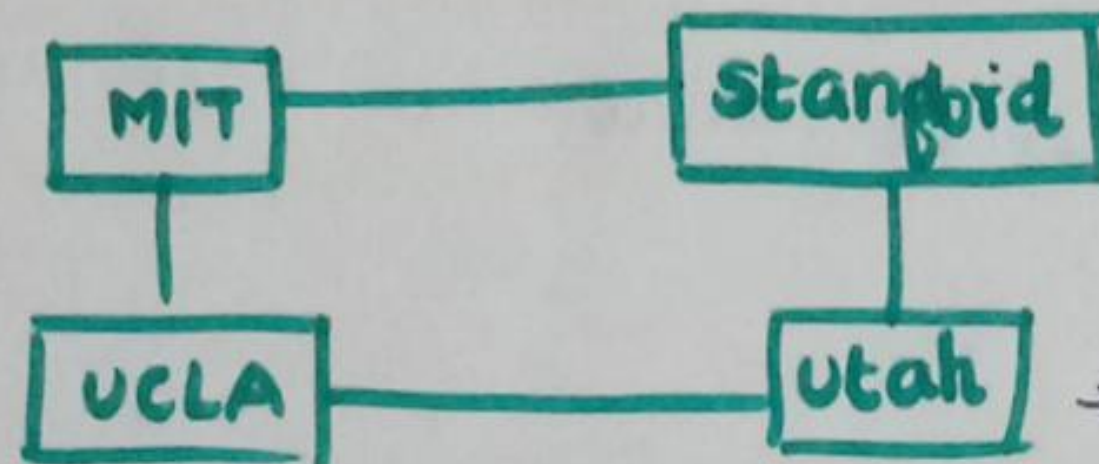
Network



Internet

How did it start?

ARPA - Advanced Research Projects Agency (US)



→ They were connected using ARPA net.

→ TCP / IP

- Protocol

Protocol
The Rules that are set up by people how a particular data is being send. These are known as PROTOCOLS.

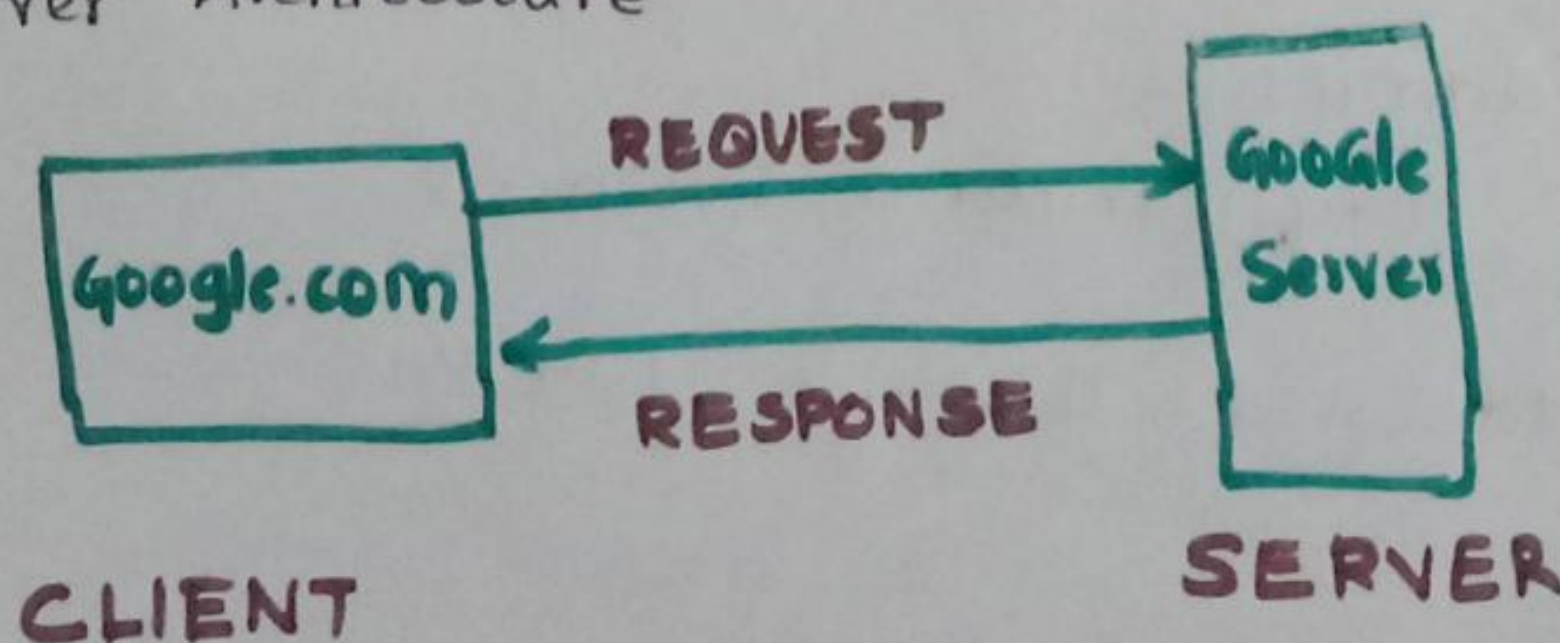
Eg. TCP, IP, UDP.

- World wide web

The world wide web (WWW), commonly known as the web, is an information system where documents and other web resources are identified by URLs, which may be interlinked by hyperlinks and are accessible over the internet.

- INTERNET SOCIETY, They are responsible for creating these protocols.

- client-server Architecture



(2)

- Some Basic Protocols

- * TCP - TRANSMISSION CONTROL PROTOCOL

→ It will ensure that the data will reach its destination and not get corrupted on the way

- * UDP - USER DATAGRAM PROTOCOL

→ When you don't care about, if 100% of the data is reaching your friend/ whoever you want to send.

Eg. Video Conferencing

- * HTTP - HYPER TEXT TRANSFER PROTOCOL

→ This is being used by web browsers.

→ The data that is being transferred between clients and servers

- Every single device on the internet that can talk to each other. They have an IP ADDRESS.

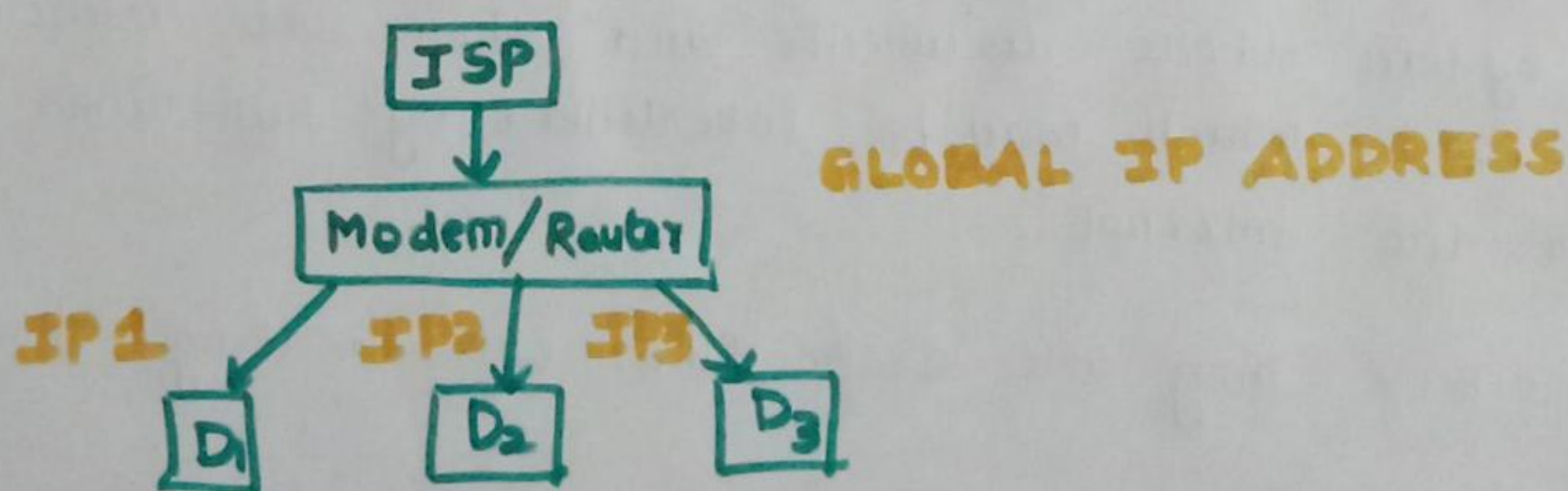
- Format of IP address

X.X.X.X



can have value between 0 - 255

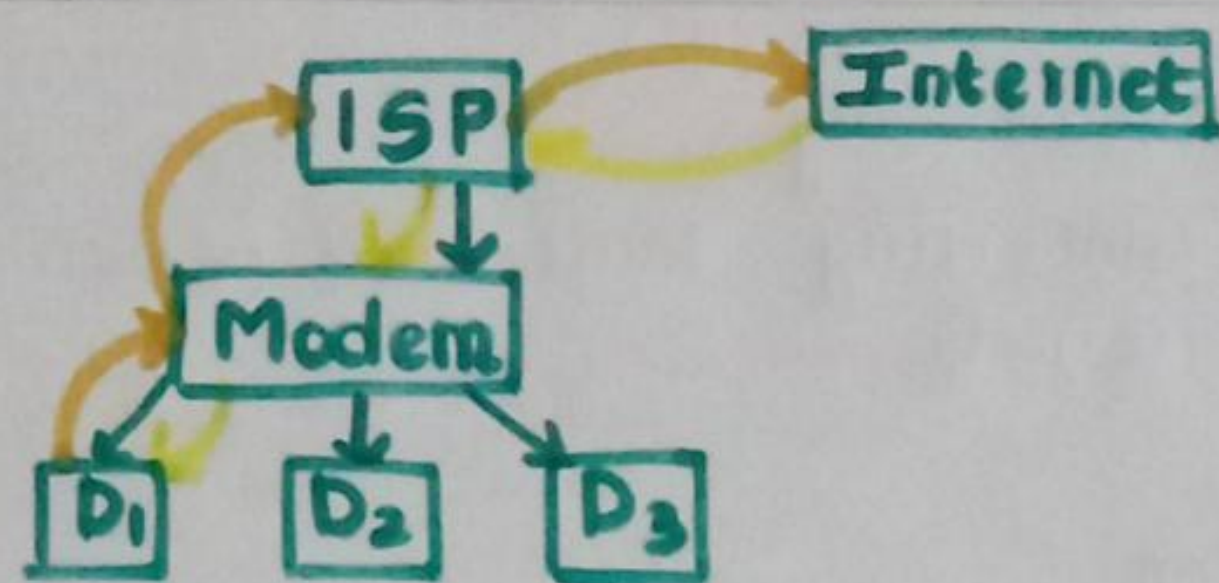
- To check the IP address of your own computer
command :- `curl ifconfig.me -s`



→ IP1, IP2, IP3 - Local IP addresses.

→ DHCP - Dynamic Host Configuration Protocol.

- Modem Assigns these IP addresses through DHCP.



→ Modem/Router will decide who requested it. It does that using NAT - Network Access translator

→ IP address decides which device to send the data whereas Port numbers are used to identify which application made that request.

→ Ports are basically 16 bit numbers.

→ All HTTP stuffs happen at port 80

→ MongoDB port - 27017

→ • 0 - 1023 ⇒ Reserved ports

• 1024 - 49152 ⇒ Registered for Applications

• Remaining ⇒ for our use

Speed

1 mbps = 1000000 bits/s

1 gbps = 10^9 bits/s

1 Kbps = 1000 bits/s

Submarine cable.com

LOCAL AREA NETWORK - Interconnects computer within a limited area such as a residence, school, university campus etc.
Ethernets, wifi

METROPOLITAN AREA NETWORK - interconnects users with computer resources in a geographic region of the size of a metropolitan area. (cities)

WIDE AREA NETWORK - extends over large geographic area (countries)

A lot of local Area network that are connected to each other using metropolitan area network that are connected to each other using wide area network is a internet

④

- SONET - Synchronous Optical Networking
- Frame relay - A way for connecting local area network to the wide area (like internet)

Modem - Modulation demodulation

used to convert digital to analog and vice versa

Router - A device that forwards data packets between computer networks

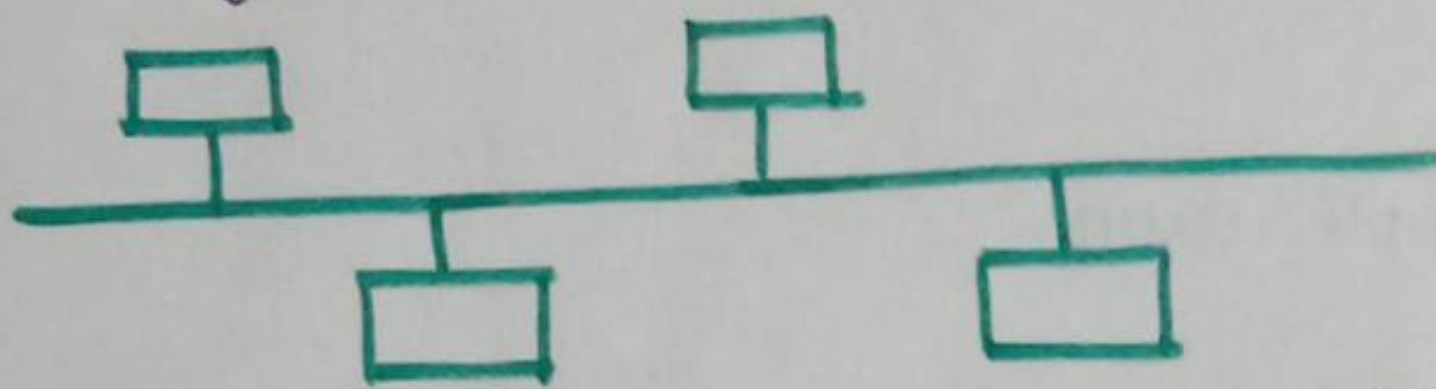
ISP - Internet Service Providers are companies that provide us access to the internet

Tier 1 - TATA

Tier 2 - Airtel, Idea

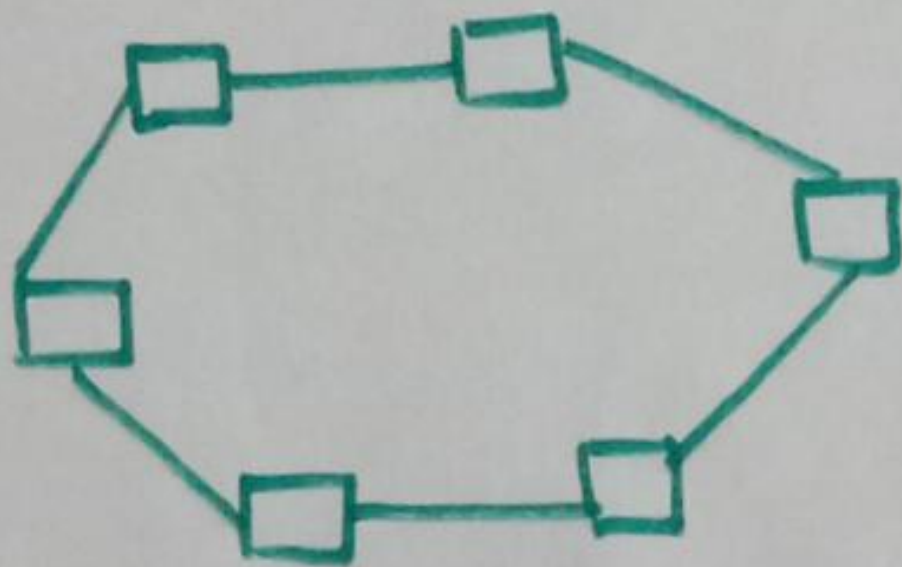
Topologies

1. Bus topology - They are connected to a single backbone



- If one part gets broken entire system will fail.
- only 1 person at a time can send information.

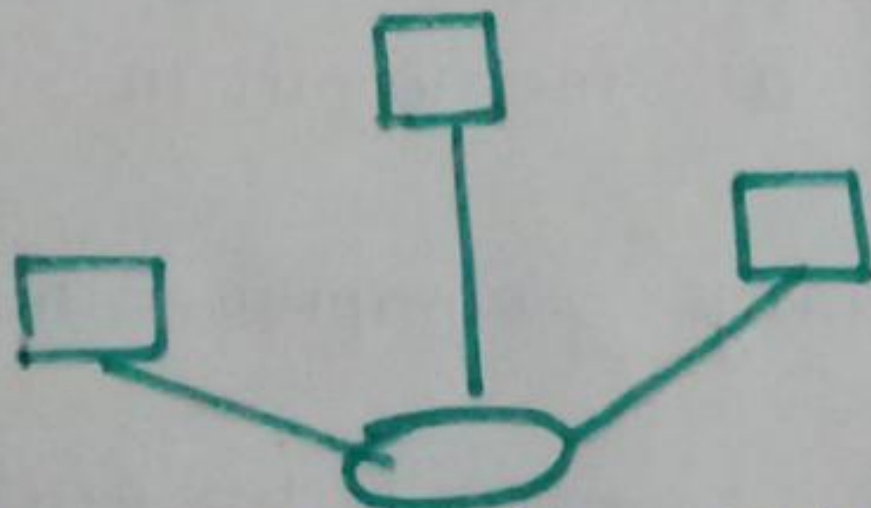
2. Ring topology



Every system communicate with one another

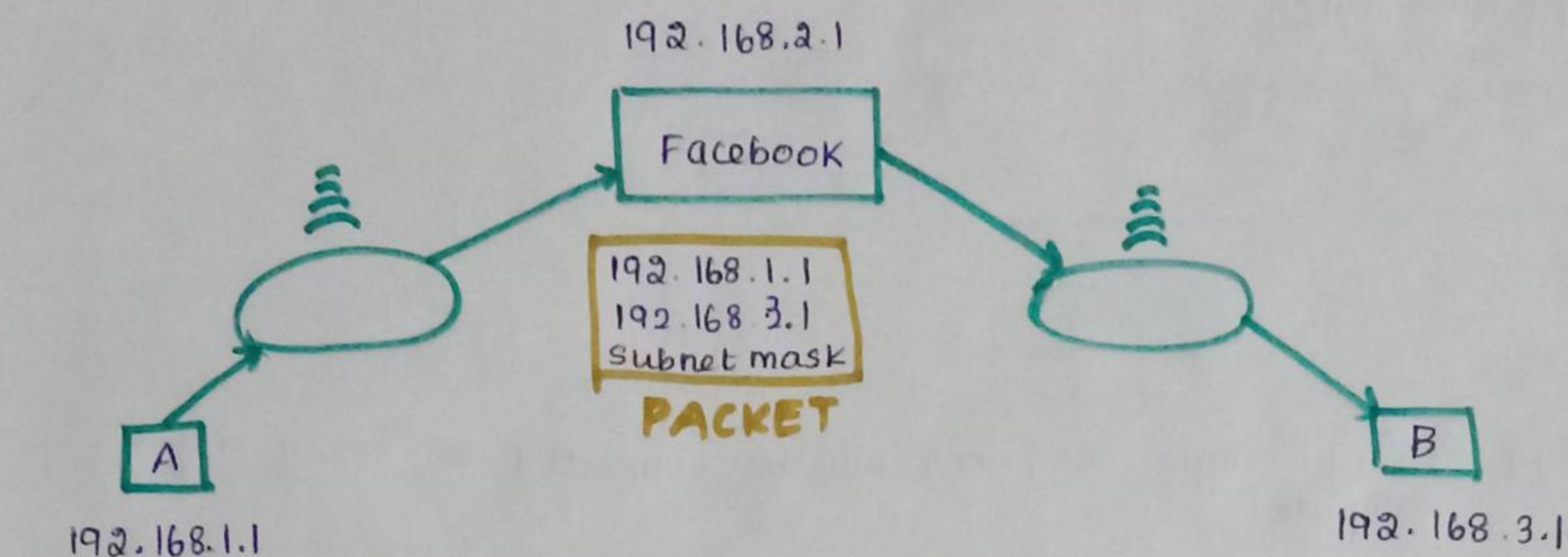
- if one of the cables break you won't be able to send data
- lot of unnecessary calls are made

3. Star topology

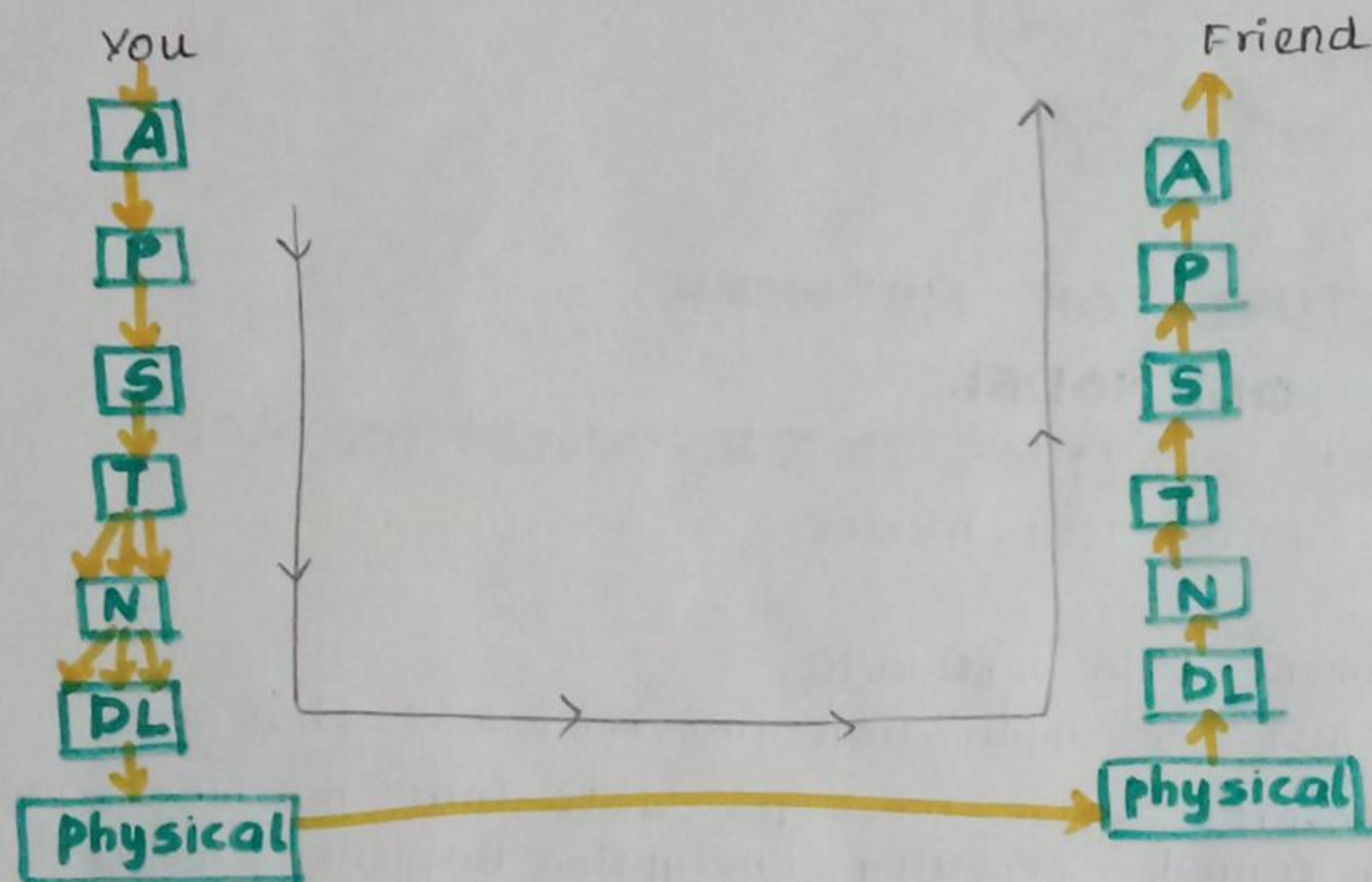


There will be one central device that will be connected to all computers

if central device, then the system will go down.



Execution



TCP/IP MODEL

Basically known as INTERNET PROTOCOL SUITE

There are 5 Layers.

Application Layer



Transport layer



Network layer



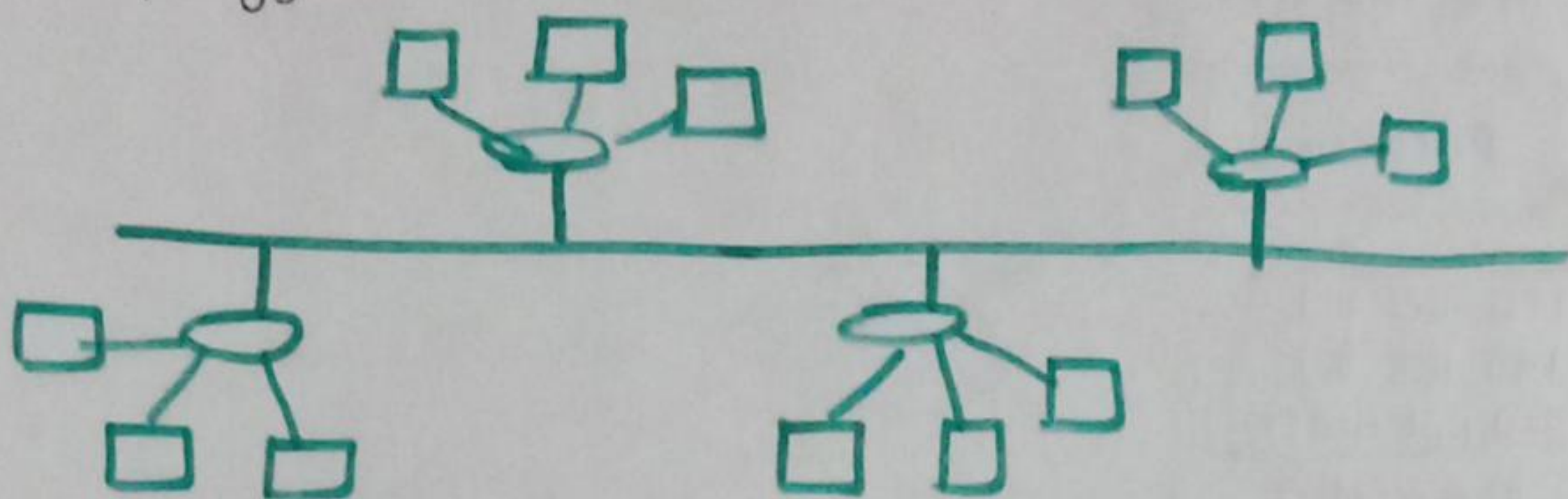
Datalink layer



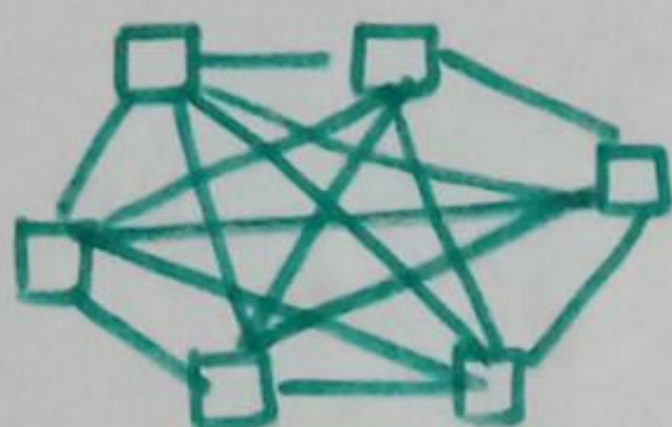
Physical Layer

(6)

4. Tree topology (Bus-star)



5. Mesh topology Every single computer will be connected to every single computer.



→ Expensive
→ Scalability issues.

STRUCTURE OF NETWORK OSI MODEL

OPEN SYSTEMS INTERCONNECTION MODEL

There are 7 layers in the OSI model

Application layer	Implemented in software. it is just the application like browsers, chat apps.
↓	
Presentation layer	It converts those messages, data into machine representable binary format. Encoding, Encryption happens. provides Abstraction. compression, translation.
↓	
session Layer	helps in setting up and managing the connections and enables sending and receiving of data followed by termination of connected session. Authentication and Authorization takes place.
↓	
Transport layer	Data received from session layer is divided into small data units called segment. Every segment has source and destination's port as well as sequence number. Flow control. Error control.
↓	
Network layer (Router lives here)	The transmission of the received data segments from one computer to another that is located in different network. IP addressing done here is called logical addressing. Routing is performed. Load balancing.
↓	
Datalink Layer	Physical addressing is done here. Mac addresses are physical addresses. Now these addresses of sender & receiver are assigned to packets called frames.
↓	
Physical layer	Hardware like cables, wires.

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

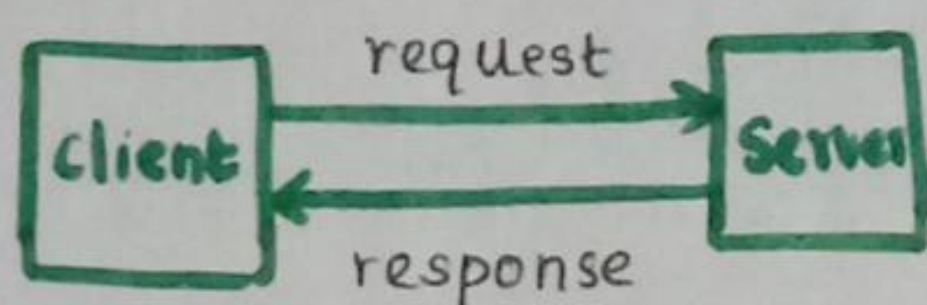
Network Layer

Layers:

Application layer:

This is the layer where the users interact with it. It consists of Applications like web browsers, chat Application etc. It lies on our devices.

Client-server Architecture

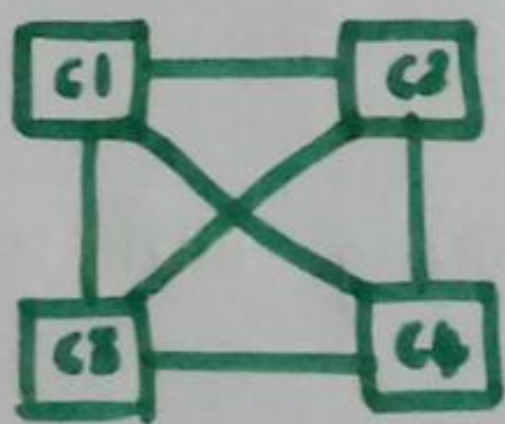


- A server is basically a system that controls the website you are hosting
- The application has two parts: client part and server part. These are known as processes and they communicate through each other.
- clients are the ones who are using/consuming these resources like we making a request to google.
- A collection server is known as data centers.
- Data centers is a collection of huge number of computers. It may have static IP addresses. They have good Internet connection and high upload speed.

Command: ping google.com

- ping measures the round trip time for messages sent from the originating host to the destination computer and are echoed back.

Peer to Peer Architecture



- There is no one dedicated server, they are just connected with each other.
- The key advantage is you can scale it rapidly.
- Here, every single computer can be termed as a client as well as a server.

Protocols:

Web protocols:

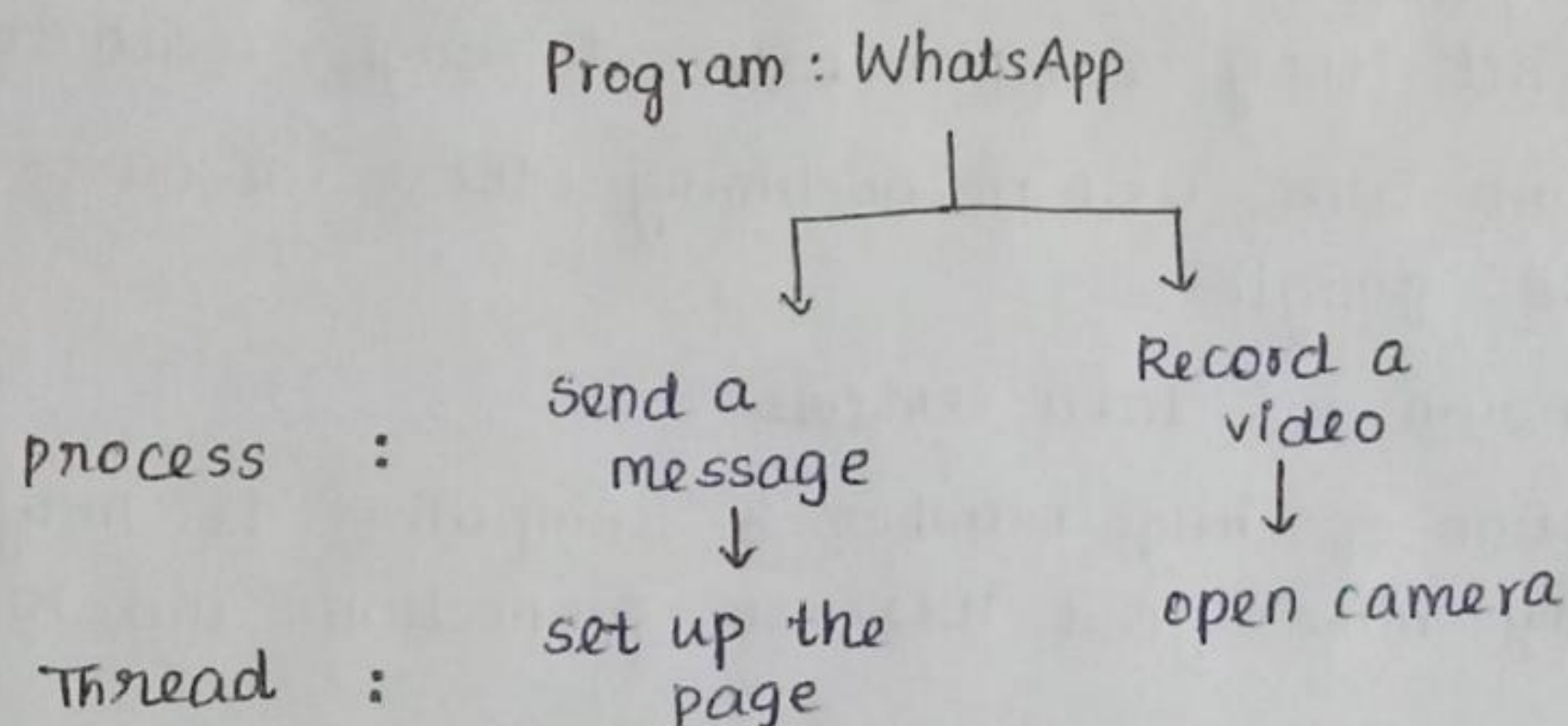
(8)

*TCP/IP :

- HTTP - Hyper Text Transfer Protocol
- DHCP - Dynamic Host control protocol
- FTP - File Transfer Protocol
- SMTP - simple mail Transfer Protocol (used to send Email)
- POP3 & IMAC (used to receive Email)
- SSH - Secure Shell
- VNC - Virtual Network Computing

*Telnet Terminal emulation that enables the user to connect to remote host/device using Telnet client. Port: 23

*UDP → stateless connection



→ process is like one of the feature of the program on a running instance. one program can have many processes running at once.

→ Thread : lighter version of process one process can have multiple running threads

Sockets

Interface between process and Internet

Ports

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

There may be possibility of many processes of single application is running. Like opening up many tabs in chrome when the response is coming back how it will know which tab to give the data. This can be resolved using EPHEMERAL PORTS.

HTTP

- It is a client-server protocol and it tells us how you request this data from the server and also tell us how the server sends back data to the client.
- When a client makes a request to the server, it is known as an HTTP REQUEST, when a server sends back response to the client, it is known as HTTP RESPONSE.
- These are application layer protocols.
(Application layer)
- HTTP uses TCP. (Transport layer)
- It is a stateless protocol: (server will not store any information about client by default).

Method

is basically telling the server what to do.

HTTP methods

- * GET: It means you are requesting some data.
- * POST: client gives some data to the server like web forms.
- * PUT: puts data at a specific location.
- * DELETE: To delete data from the server.

Error/ Status code:

When you send a request to the server, you need some sort of a way to know whether the request is successful or not. For this there exists STATUS CODE.

- Eg. 200 - request was successful
- 404 - not found
- 400 - bad request
- 500 - internal server error

- 1XX → Informational category
- 2XX → success code
- 3XX → Redirecting purpose.
- 4XX → client error.
- 5XX → server error.

Cookies:

- It is a unique string stored on a 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 look into the database and identify the state.

⑩

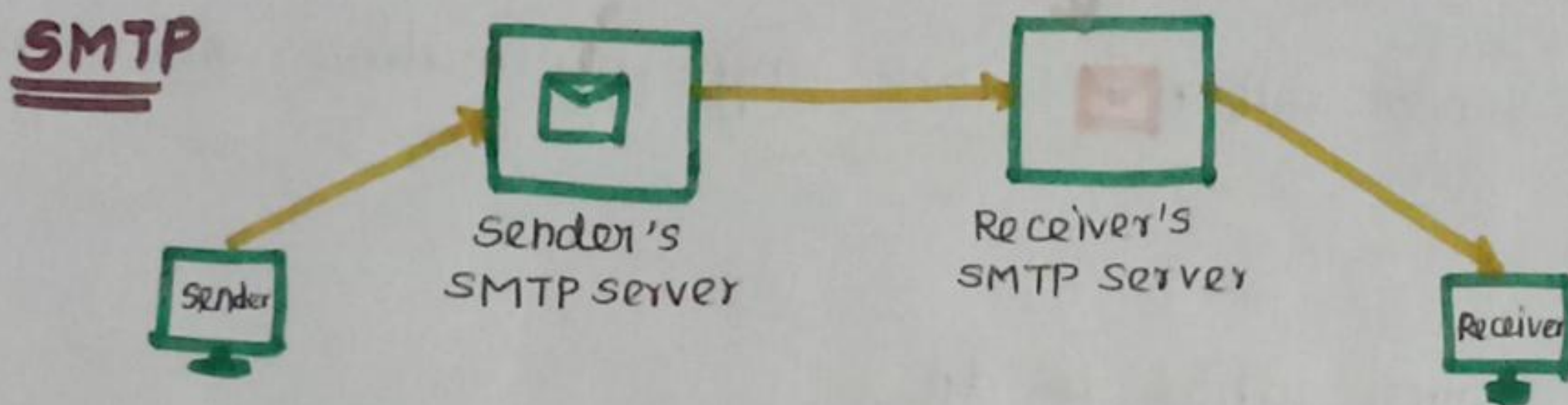
Third party cookies:

These are the cookies set for URL's you don't visit.

How Email works?

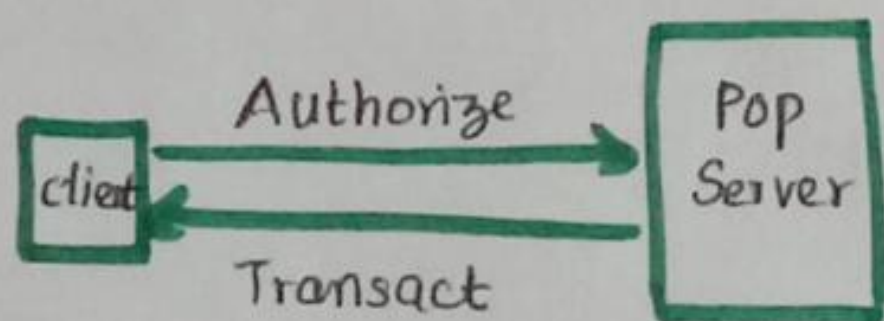
Application Layer protocol: SMTP (Simple Mail Transfer Protocol)
POP3

Transport Layer protocol: TCP.



command: nslookup -type=mx gmail.com

POP Postoffice Protocol.



IMAP Internet Message Access Protocol.

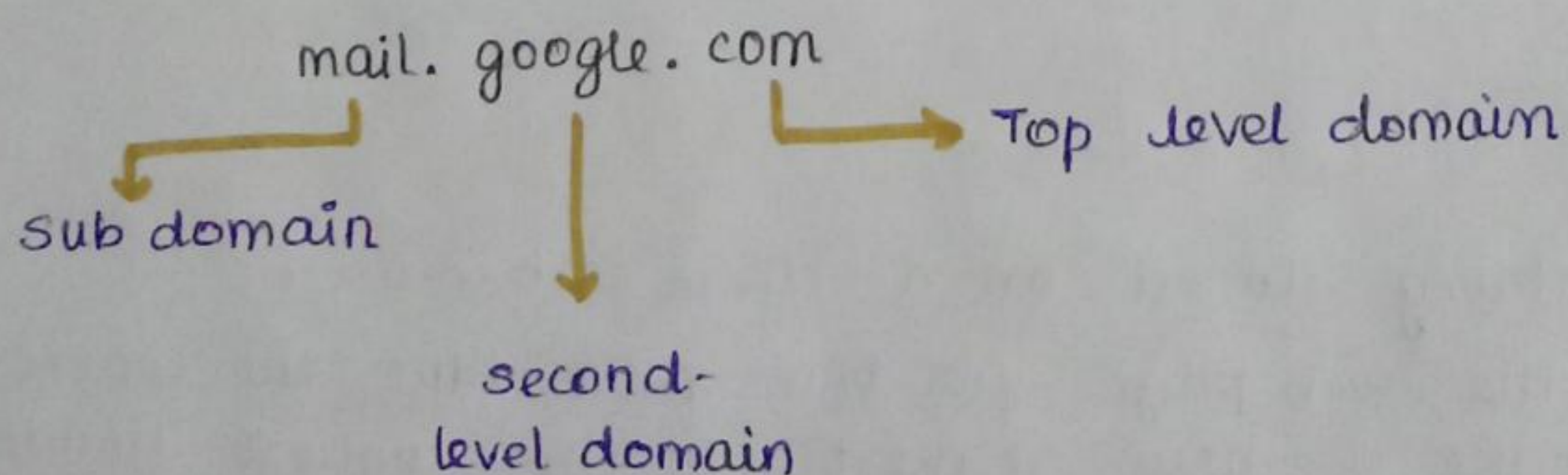
→ Allows to view emails on multiple devices.

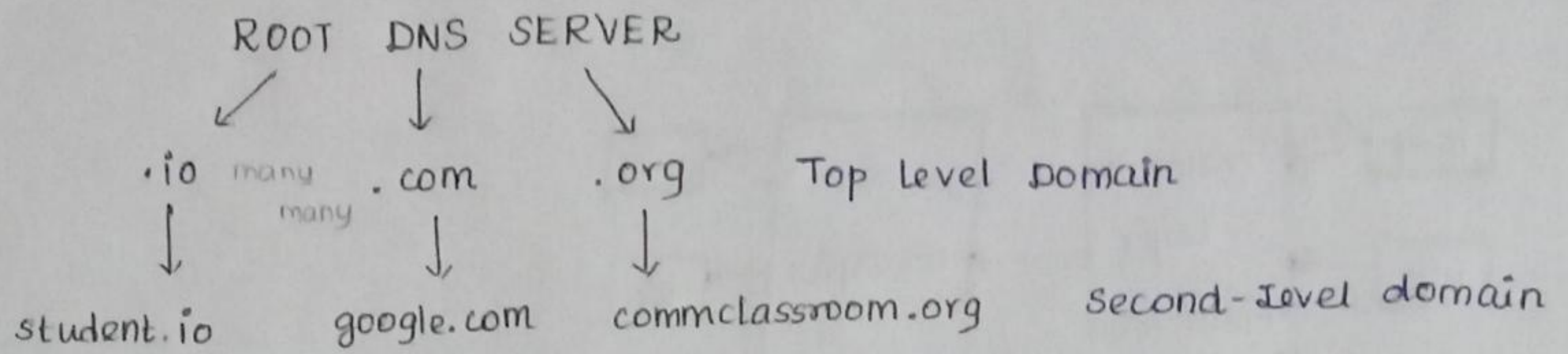
DNS - Domain Name System

→ Domain names are mapped to IP Address. We use services to look up into this. The most popular service is DNS.

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

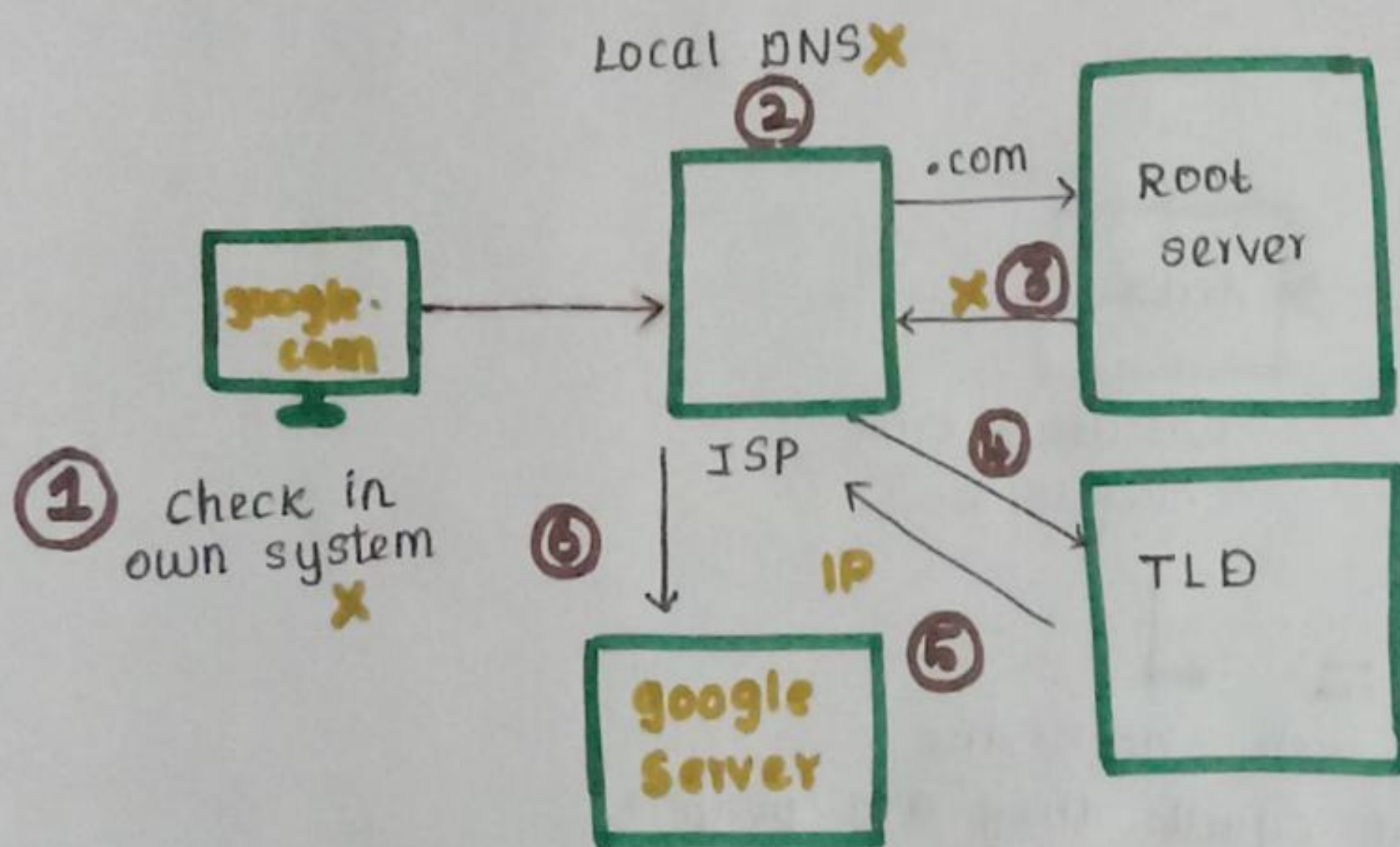
→ It is a directory / database.





Top level domain, they are like organisation specific for example .com for commercial, .edu for education .uk, .in → country specific.

These are managed by ICANN INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS



command: dig google.com
man dig

Transport Layer:

→ data transferred between one computer to another is done by using NETWORK Layer.

→ Transport layer is a layer that lies over devices.

→ The role of the transport layer is to take the data from the network to the Application

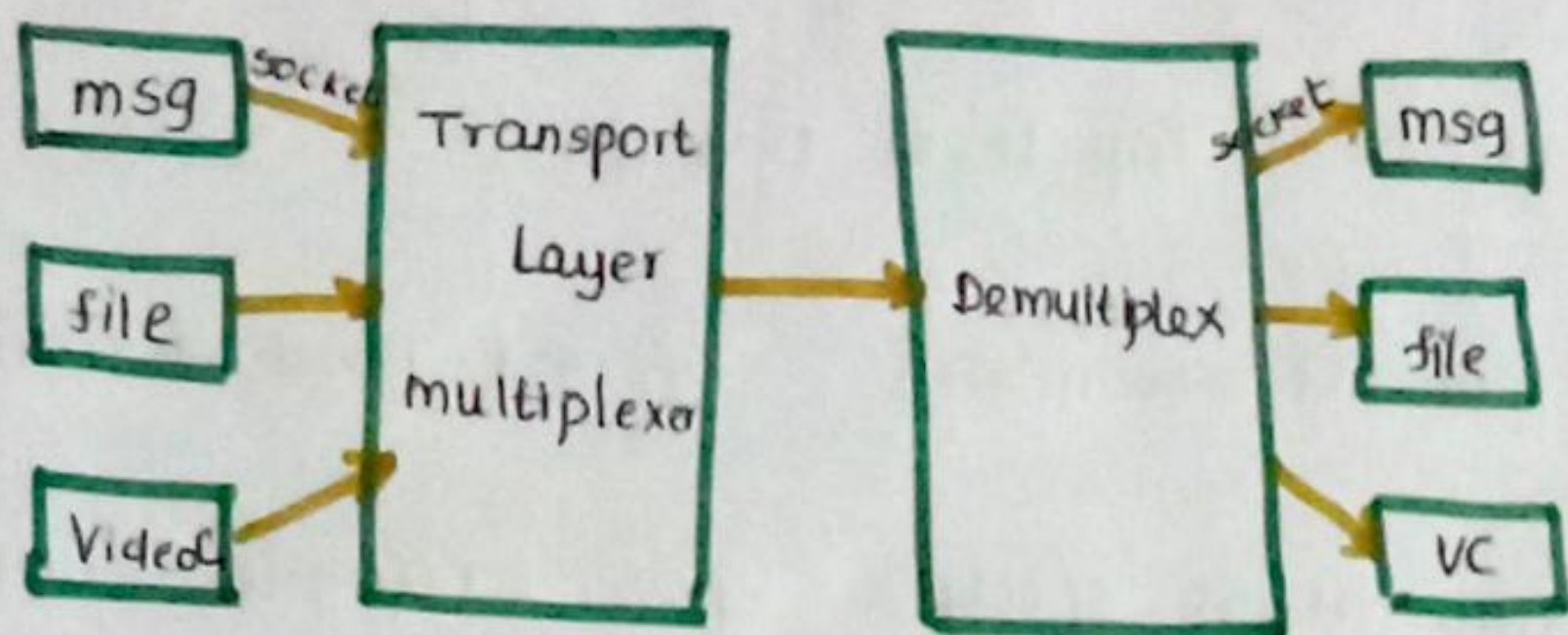
Network \rightleftharpoons Network
Network layer

Network \rightleftharpoons Application
Transport layer

→ Provides Abstraction

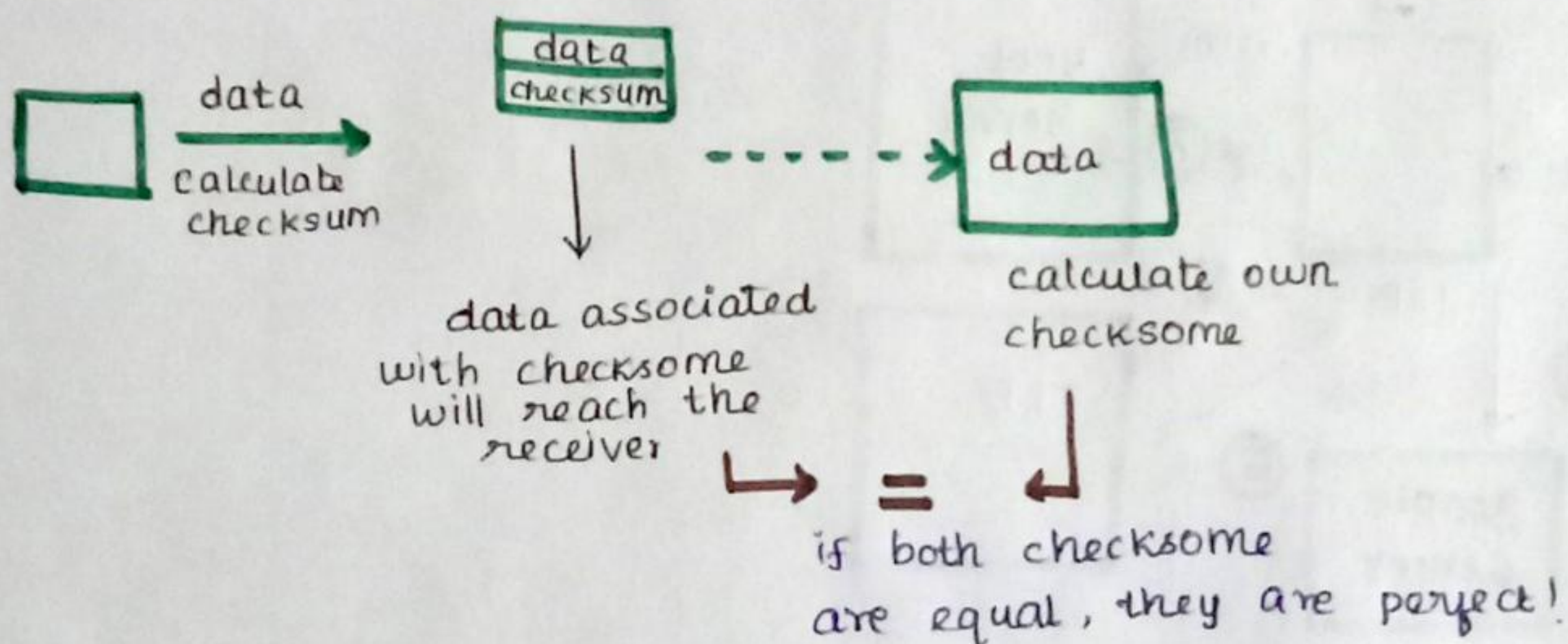
→ Located on the devices.

(12)

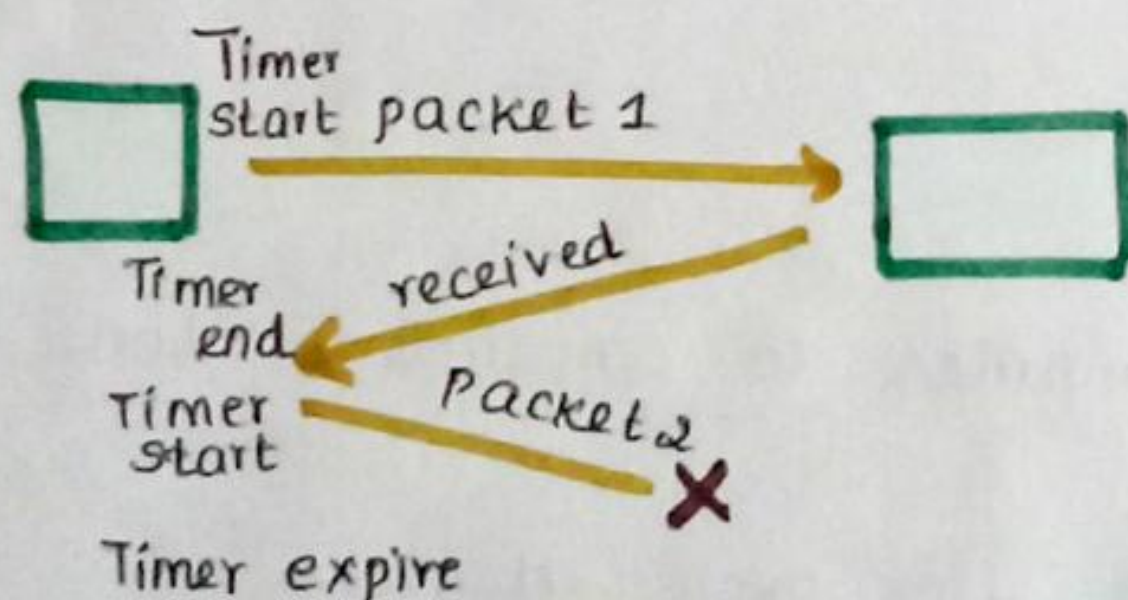


- Data travels in packets
- Transport layer will attach these socket port nos to that packets
- Transport layer also takes care of congestion control.
- congestion control Algorithms built in TCP.

Checksums:



Timers

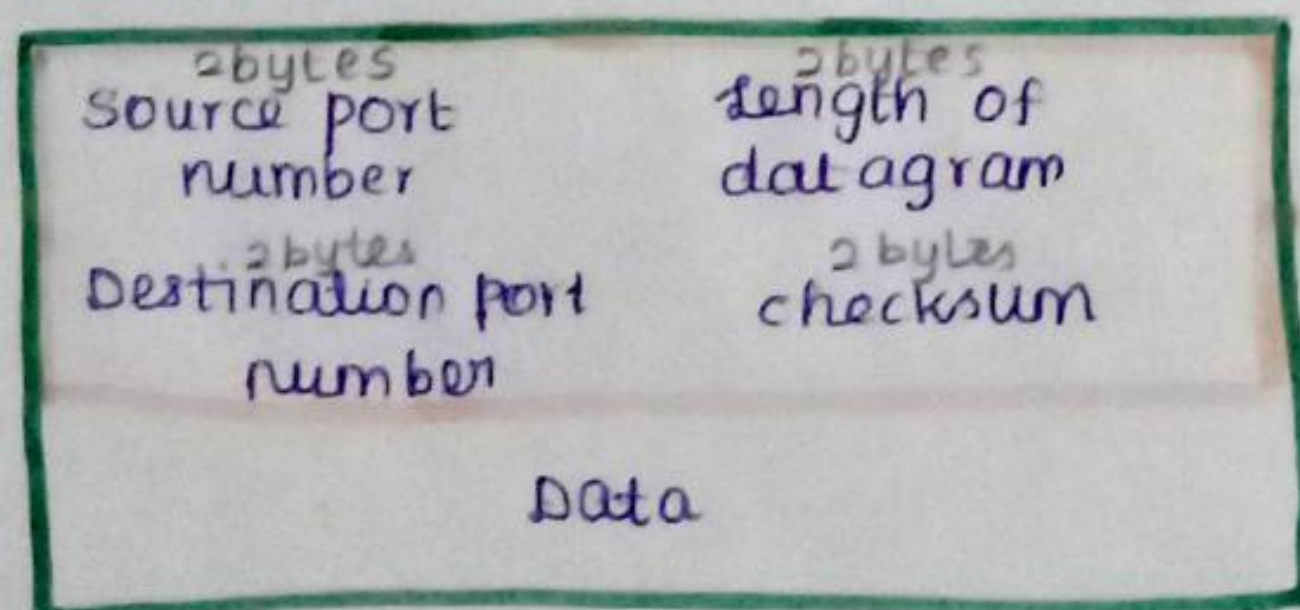


Transport layer protocol.

UDP - user Datagram Protocol.

- Data may or may not delivered, may change, may not be in order.
- Connectionless protocol.
- UDP uses checksums. And if there is any error. it won't care

UDP Packet



HEADER (8 bytes)

Total size = $2^{16} - 8$

Use cases of UDP:

- Its very fast
- video conferencing apps
- DNS uses UDP
- Gaming

Command: `sudo tcpdump -c 5` (to see only 5 packets)

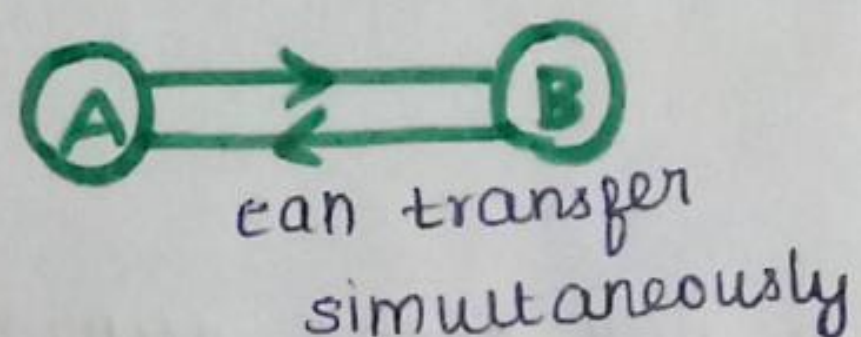
TCP - Transmission Control Protocol.

- Transport layer protocol
- Application layer sends lot of raw data. TCP segments this data, divide in chunks, add headers, etc. It may also collect the data from network layer and the small chunks are put in to one in the receiving end.

- congestion control.
- Takes care of
 - when data does not arrive
 - maintains the order of data. (using sequence number)

Features

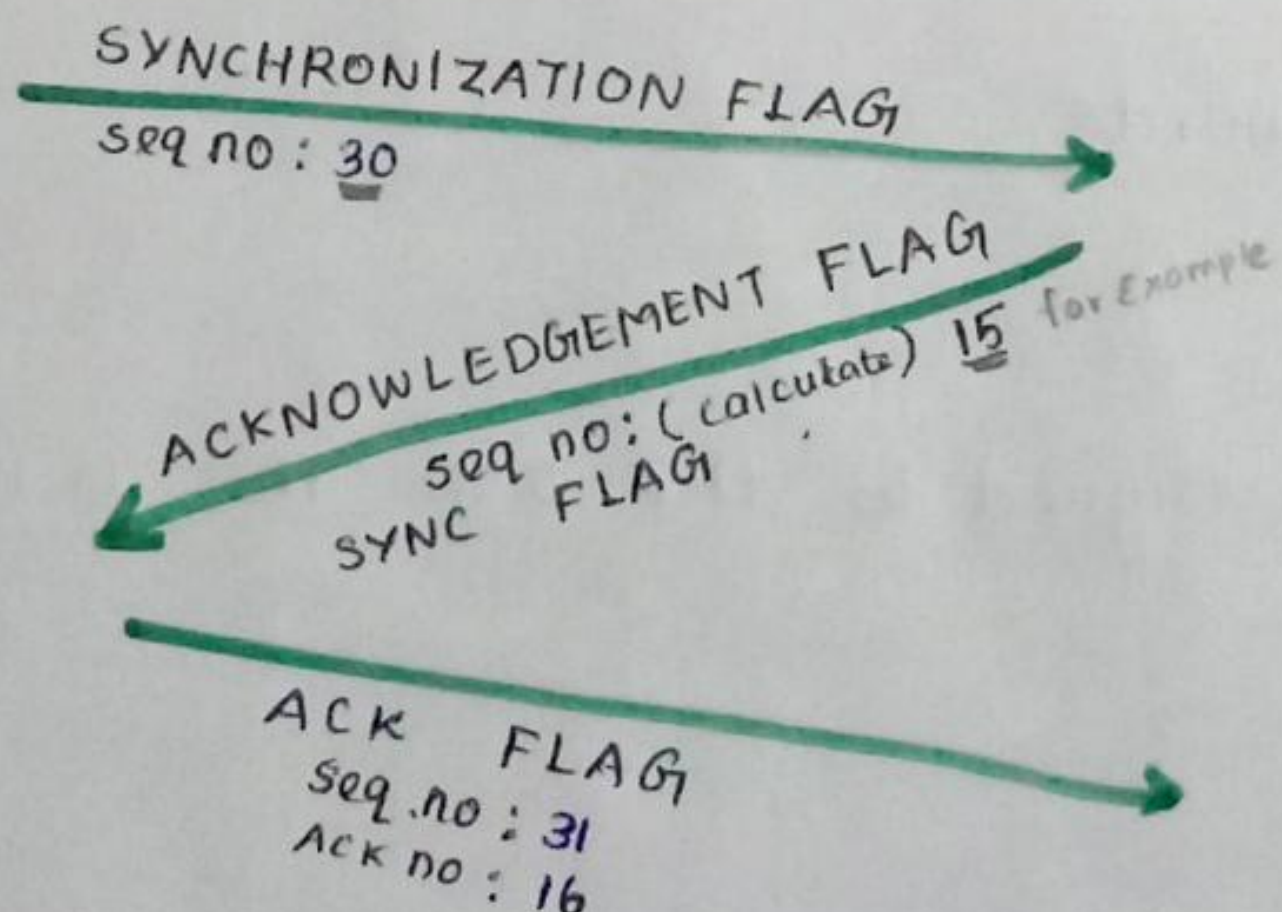
- connection oriented
- Error control
- congestion control
- Full duplex



3-way handshake

Client

Server

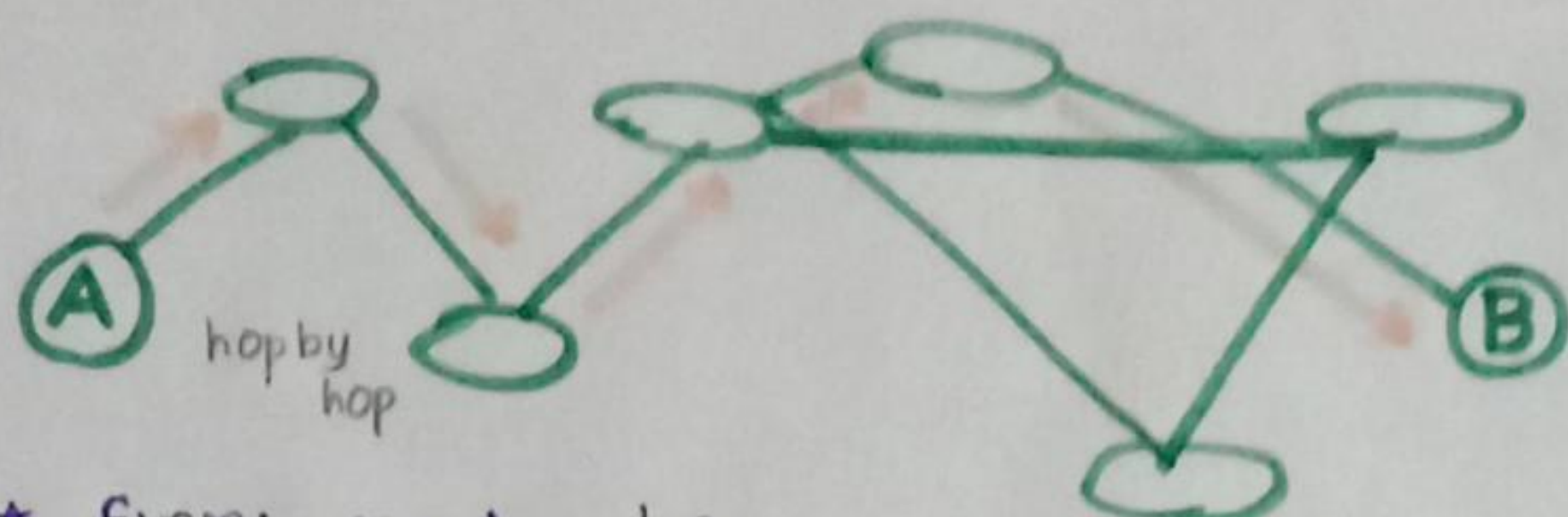


→ random number

Q4)

Network Layer

→ Here we work with routers



Transport → segments

Network → packets

Data link → frames

★ Every router has a NETWORK ADDRESS

★ Every router will check whether the packet is for that router, if not then it will forward that using forward table in routing table

In IP Address

192.168.2.30
└───┬───┘ └─┘
Network address device address
(subnet id) (host id)

Control plane.

used to build these routing tables

Routers → Nodes

Links → Edges

There are two types of routing used to create tables.

1. static routing

→ Adding address manually

→ It's not adoptive

2. Dynamic routing

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

Network layer protocol

IP- Internet protocol

IPv4 (IP version 4) → 32 bit, 4- words

IPv6 → 128-bits

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

Classes of IP addresses:

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 the host part.

Variable length subnets

You can set your own subnet length.

Eg. 15.0.0.0/30 → This basically means first 30 bits are my subnet part.

Reserved addresses:

127.0.0.0/8

Eg. localhost : 127.0.0.1 (client also server also)

loopback addresses.

Packets : Header is of 20 bytes. It contains IPv, length, Identification no, flags, protocols, checksum, Addresses, TTL (Time to live).

Time to live : It is a number, after that number of hops, the packet doesn't reach, then it will leave.

IPv6

→ IPv4 : $2^{32} \approx 4.3$ billion

→ 4 times larger than IPv4.

→ IPv6 : $2^{32 \times 4} = 2^{128}$

Cons:

- * Not Backward compatible
- * ISPs would have to shift, lot of hardware work.

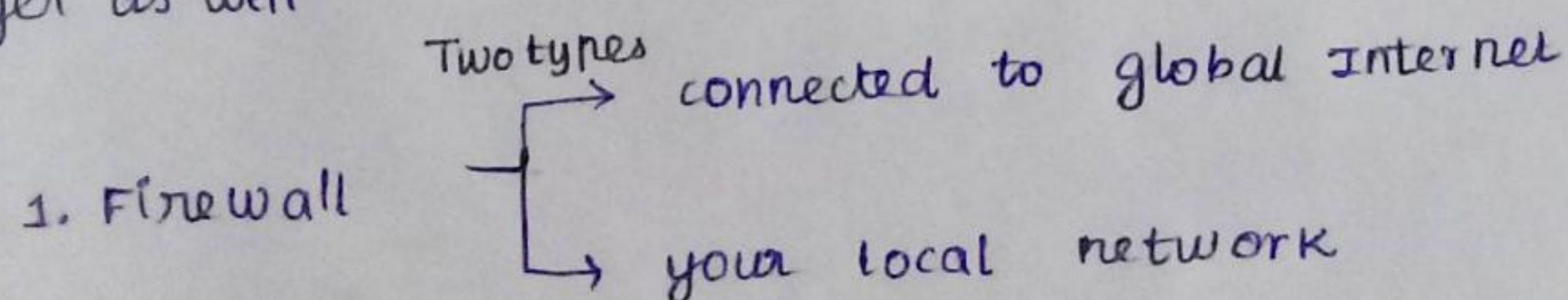
Format:

a . a . a . a . a . a . a . a
↓
Hexadecimal
(16 bit)

Middle boxes:

→ They are extra devices that also interact with IP Packets.

→ Mostly it will be in network layer but it can also be in transport layer as well.



(16)

→ It filters out IP packets based on various rules

- Address
- modify packets
- port nos
- Flags
- protocols

Stateless firewall

→ doesn't maintain a state

stateful firewall

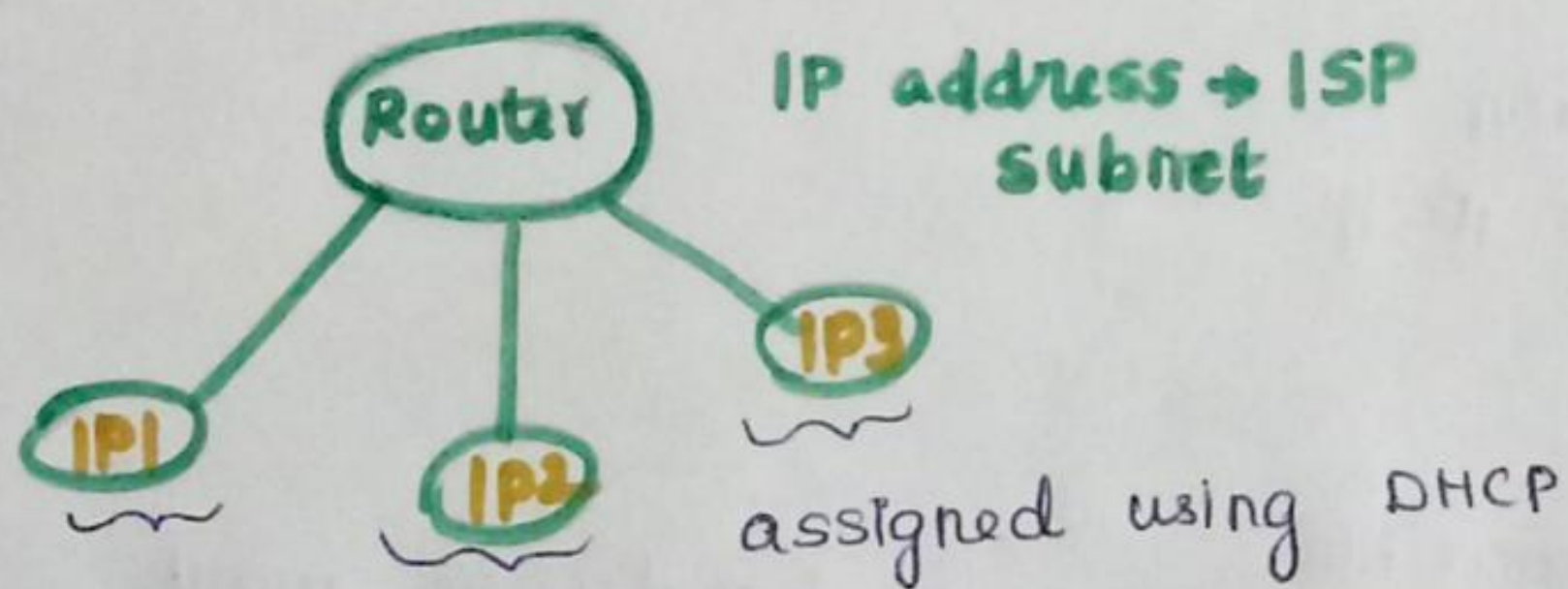
→ see the packet and maintain its state
→ more efficient

Network Address Translator (NAT)

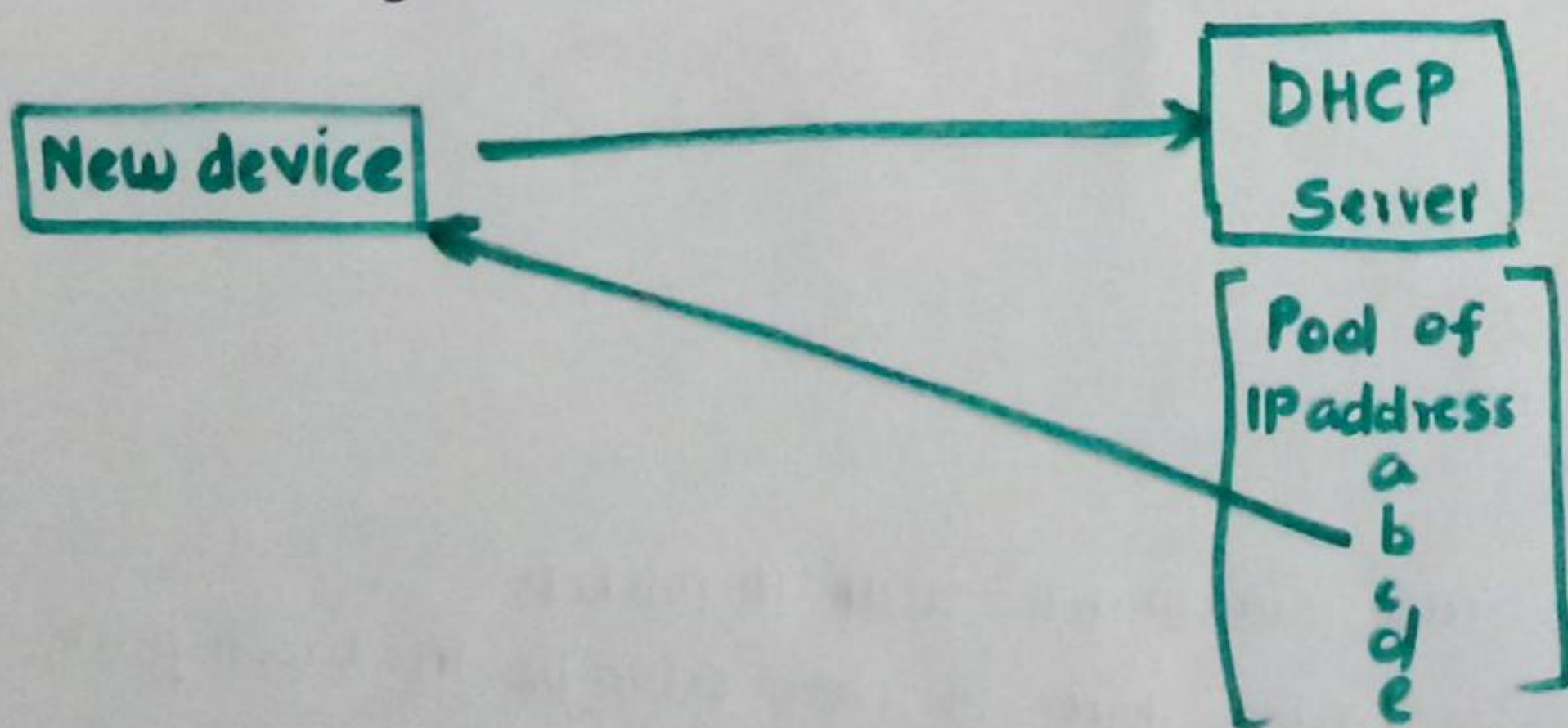
It is a method of mapping an IP address space into another by modifying ^{network} address information in the IP header of packets while they are in transit across a traffic routing device.

Data link layer

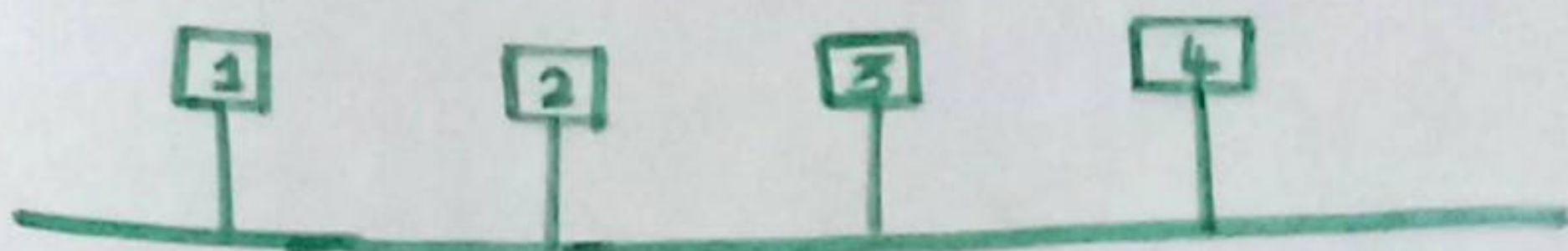
→ The data packets that we receive from the network layer, the data link layer is responsible to send these packets over a Physical link.



DHCP - Dynamic Host Configuration Protocol.



→ In data link layer, the devices communicate with each other using DATA LINK LAYER address, MAC address



Let's say device 1 needs to send something to device 4, first it will look up in its cache. If it does not have then it will ask all other devices. This is known as ARP cache (Address Resolution Protocol)

Frame consists of

- DLLA of sender
- IP address of destination

MAC - Media Access Control