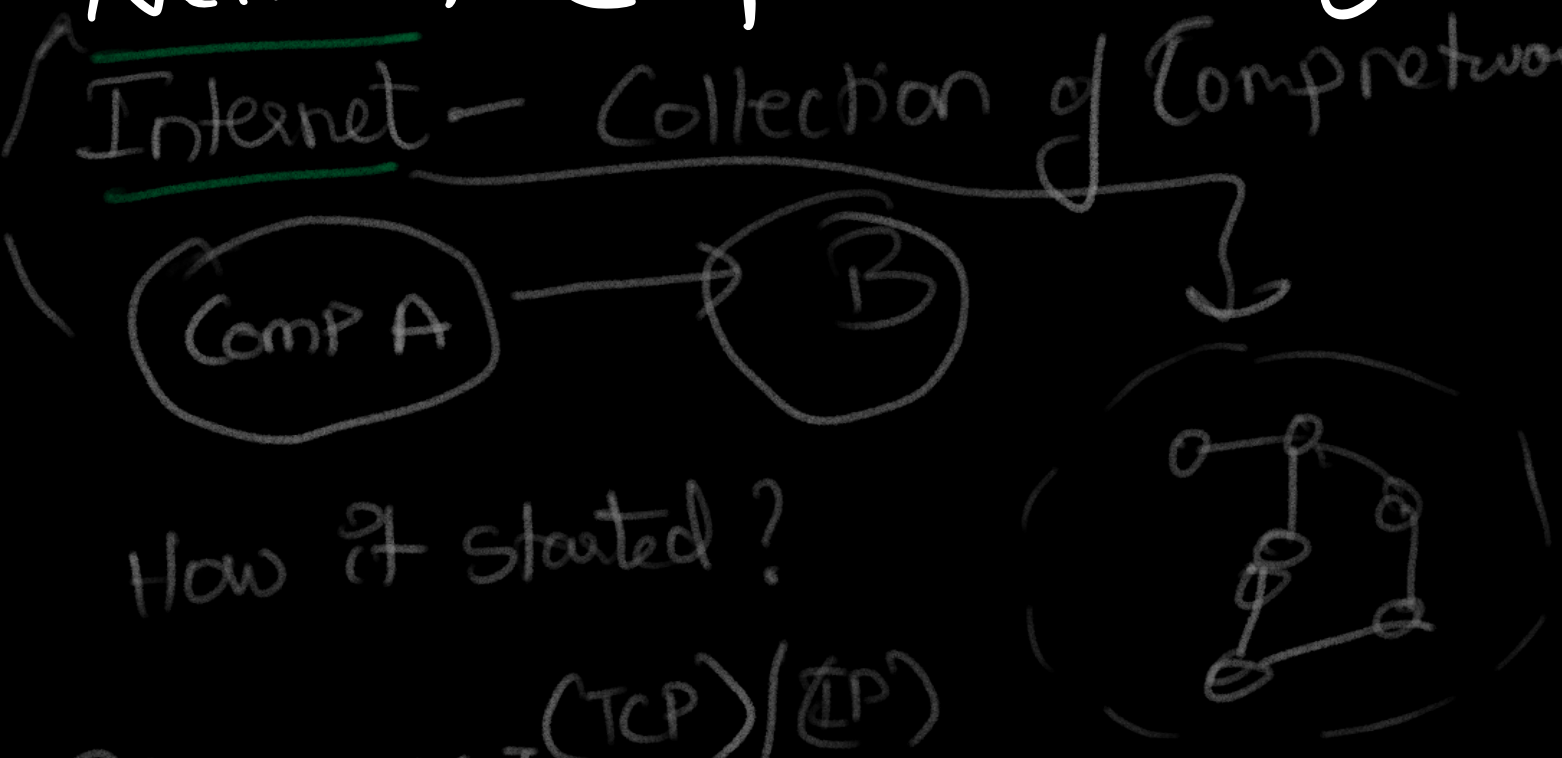
Computer Networking

Network - Comp Connected together

Internet - Collection of Comp networks



How it started?

ARPA-NET (TCP)/(IP)

Initial used to transfer

MIT, Stanford, UCLA, UTAH

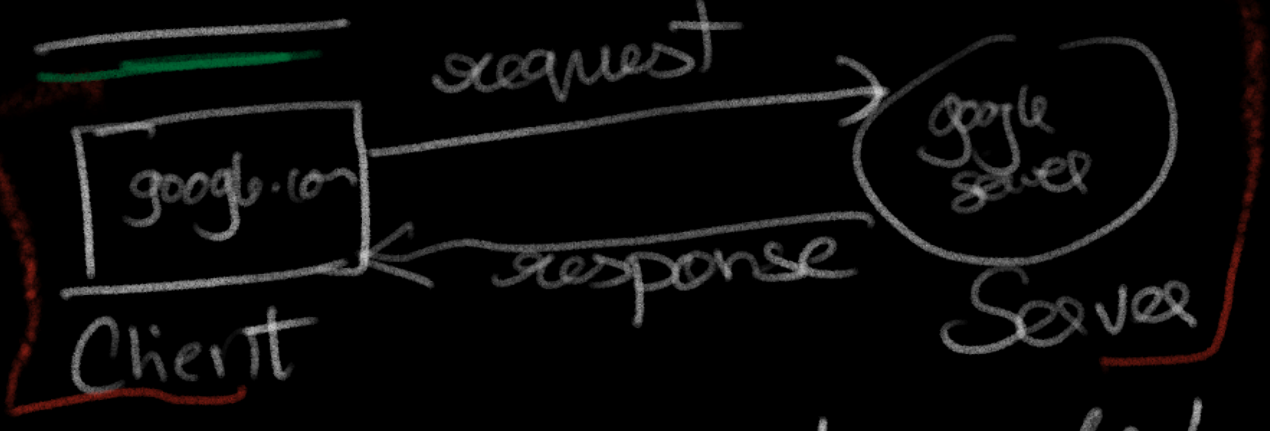
Later Comes www

Protocols (Rules)

→ Imp to have protocols. So, that we can communicate to the entire world.

Check later: RFC - Editor // Internet - Society

Server



- Protocols are rules made by Internet Society.

Some of the Protocols:

TCP (Transmission Control Protocol)

→ It will ensure data will reach it's destination without getting corrupted

(Uses datagram Protocol)

→ UDP - not all data will be reached

ex: Video Conferencing

→ HTTP (Hypertext transfer Protocol)

used by web Browsers

How data is transfered ?

→ Since in Comp everything is 0, 1 it doesn't make sense to send entire data once. You want Send a large file it won't be sent in I go it will come in chunks.

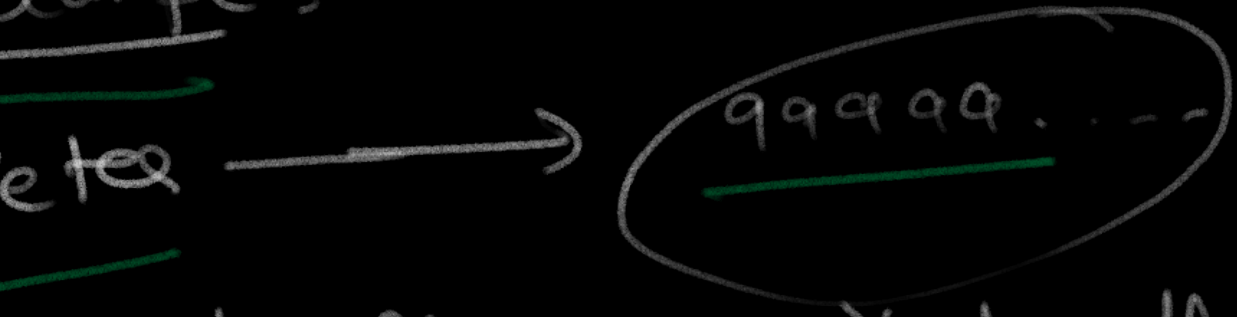
Ex:- loading Webpage, Watching Movie

→ Data we will be getting will be in packets

when you enter google.com how does it find which sever to connect?

→ Basically, these comp & Servers are identified by Ip address think of it as phone Book.

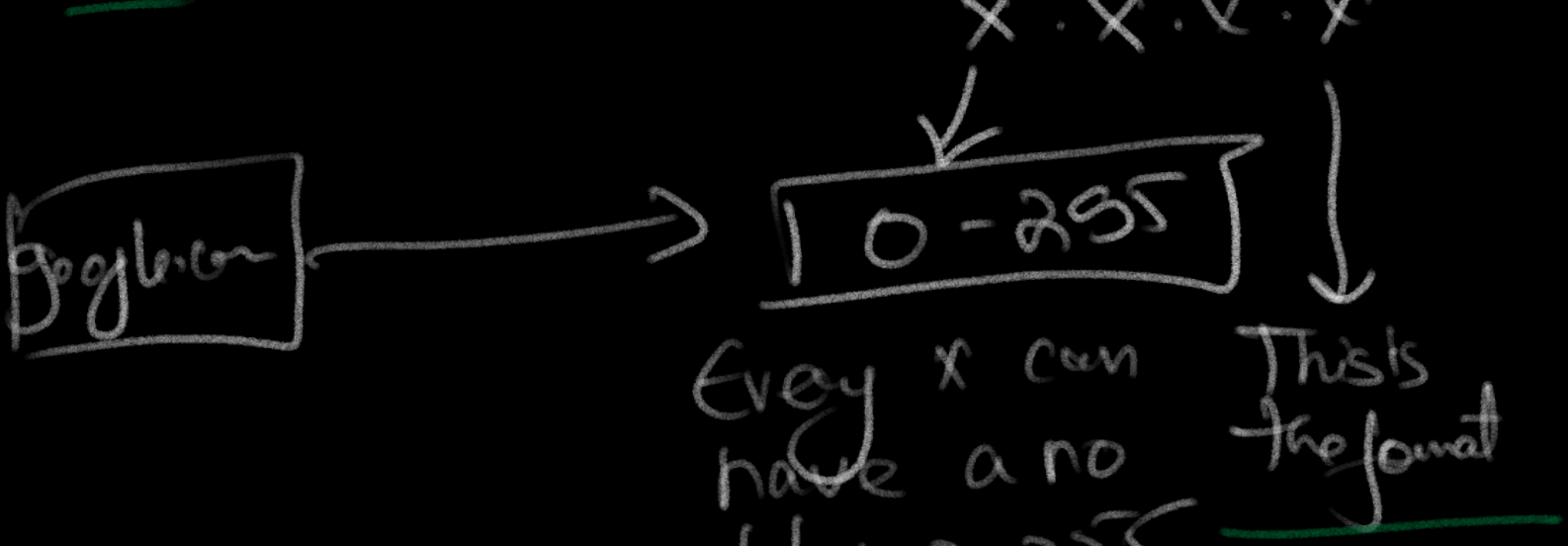
for example:



for example if you want to call peter & hit call peter it will directly call as the number is linked.

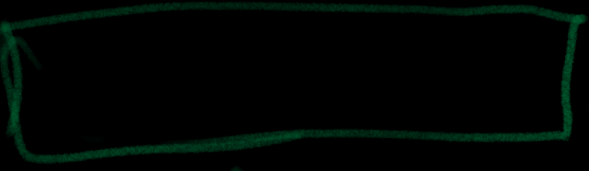
=> Every single device on Internet that can talk to each other has an I.P address.

Ex :-

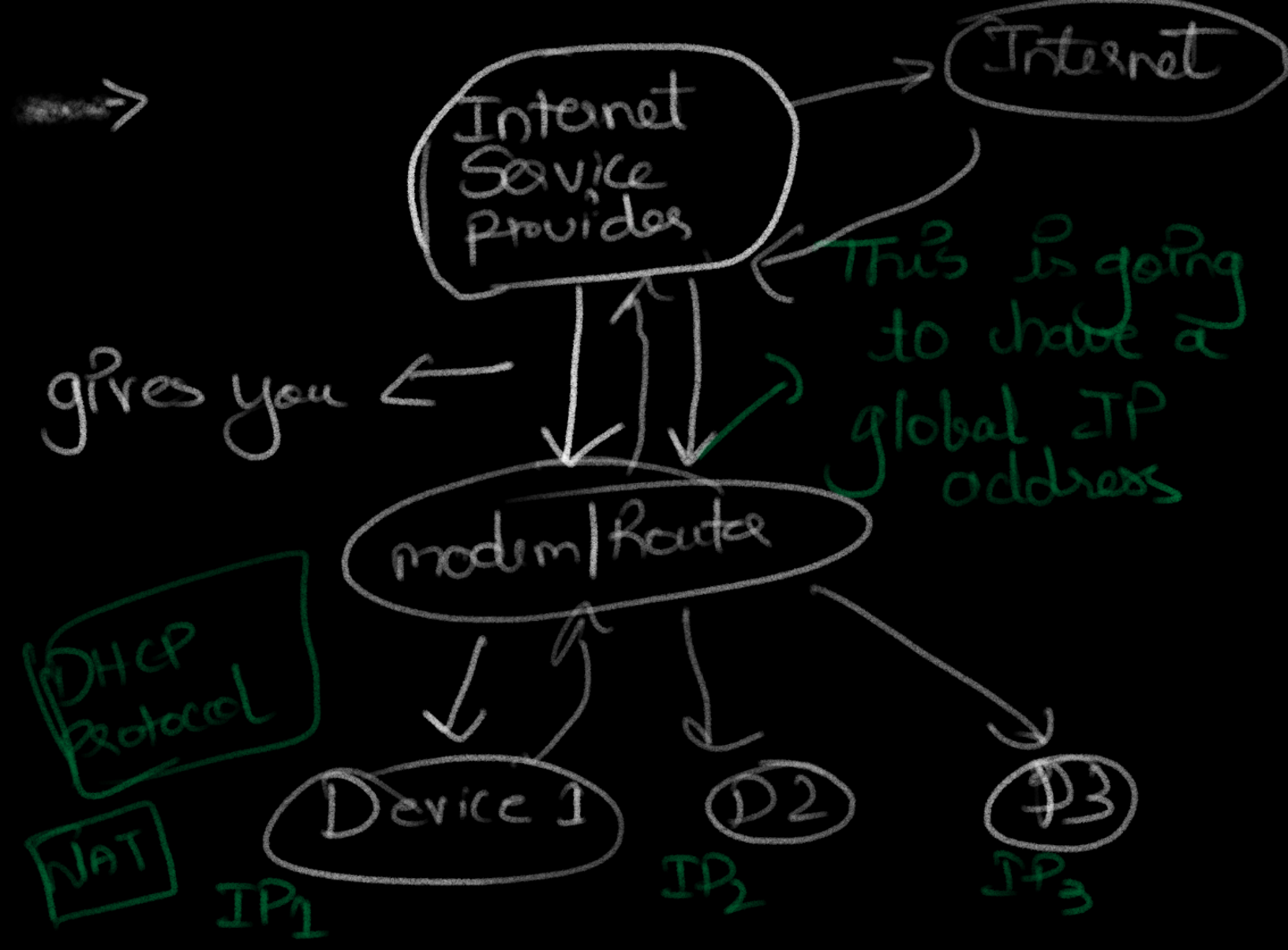


So, when click google.com it will be resolved to a particular IP address

To get the Ip adress of your Internet (or)



Use this command



The modem will assign each device a Ip address known as Local Ip address.

→ It does do it using DHCP Dynamic Host Configuration Protocol

It's also part of rules & regulations.

→ For example you make a request to google.com it will see the global Ip address

from our above example if D1 & D2 make a request for google it will be seen 1 device making a request

→ You send a request to google.com your Isp will send ,, ,, , ,, & then it will return back the response.

→ Now, Modem / Router will decide who was the one who had the request. It does that using NAT

Network Access Translator (NAT)

- It says D1 has a chrome tab open and it's requested for this response

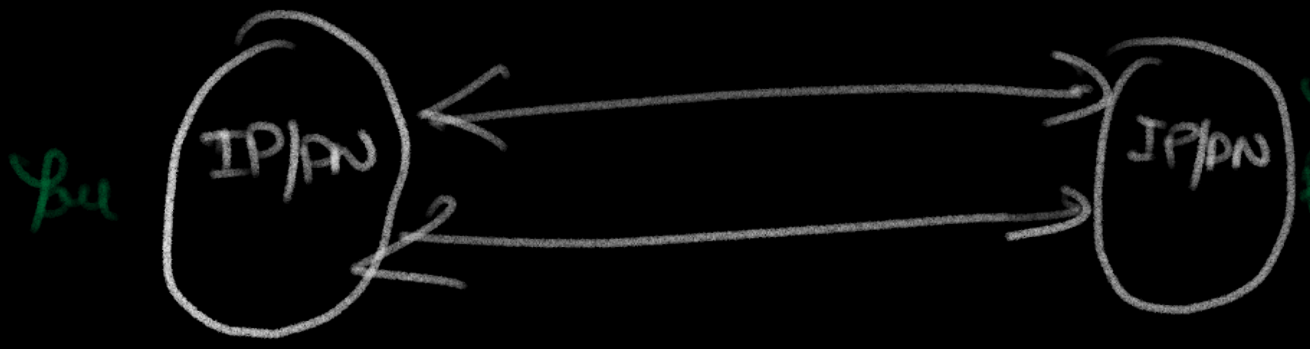
How do Modem/Router figure out which app made the request

We know that Ip address decides which device to send the data.

Since there are many applications running the same device which will have the same Ip address.

It will sending to the exact app which made request using Ports / Port Number

→ Let's say you talking to your friend you & your friend will have IP address & Port Number



IP address - will determine where Comp located

Port Numbers - denoting which app you will be using to communicate

Ports

→ They are Basically 16-Bit numbers.

16-Bit means we can have 16 cells

1 each cell can contain 0 (or) 1

Total port numbers that are possible are : 2^{16} ≈ 65 K.

We know web pages are using HTTP protocol. All HTTP stuff will happen on Port 80 ex: HTTP:80, MongoDB: 27017

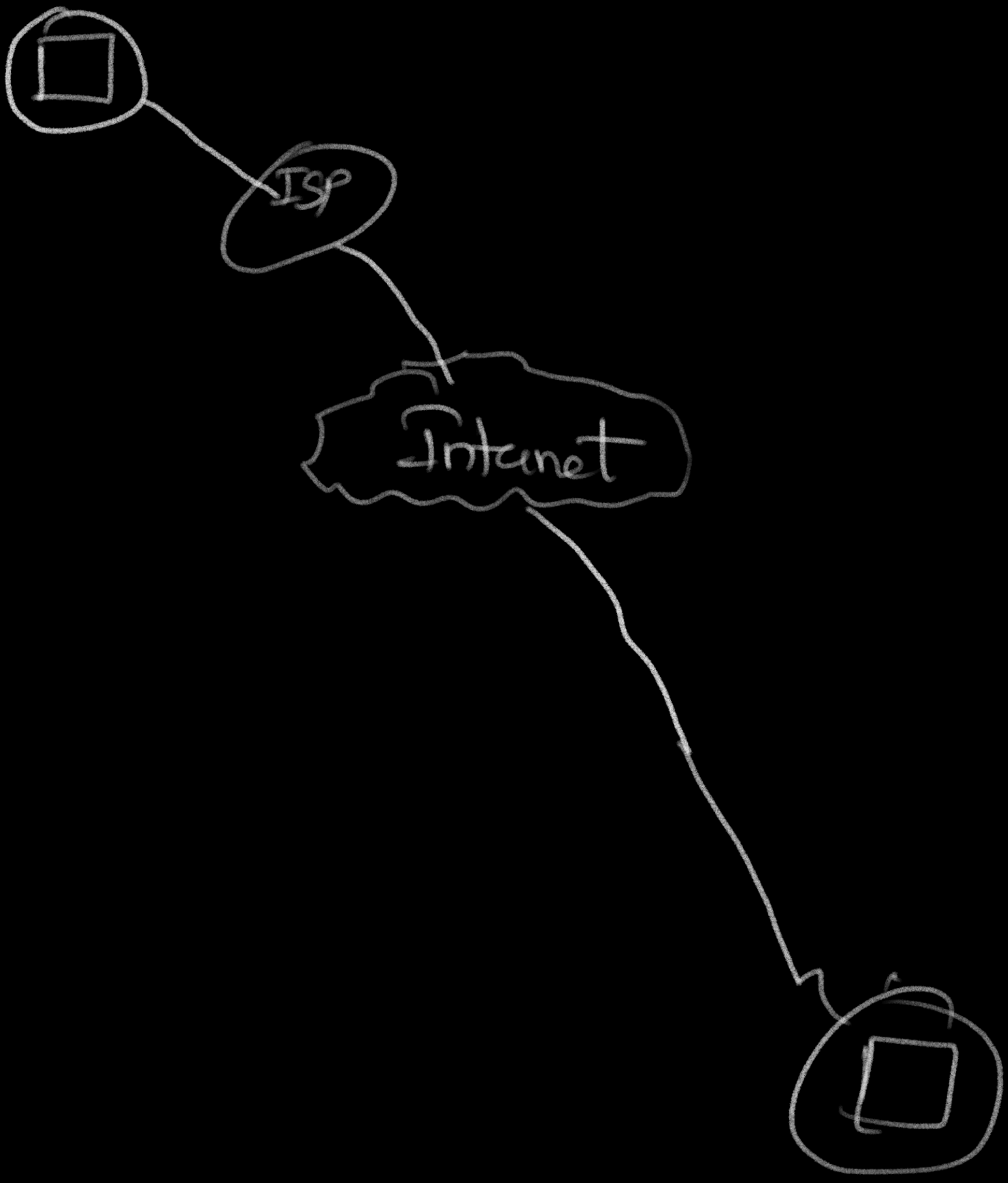
Ports from 0 - 1023 are reserved ports. It means for example you create an app & want to host on port number 80, you can't because it is reserved for http.

Ports: 0 - 1023 - Reserved

1024 - 49152 - Registered left for some specific apps

HTTP: 80
MongoDB: 27017
MySQL: 1433

The remaining ones we can use


ISP
Intanet

Measuring Speed of Internet

1 Mbps = 1 Mega bits per second

Mega means - [1 000 000] bits / sec

1 gbps = 10^9 bits / sec

1 Kbps = 1000 bits / sec

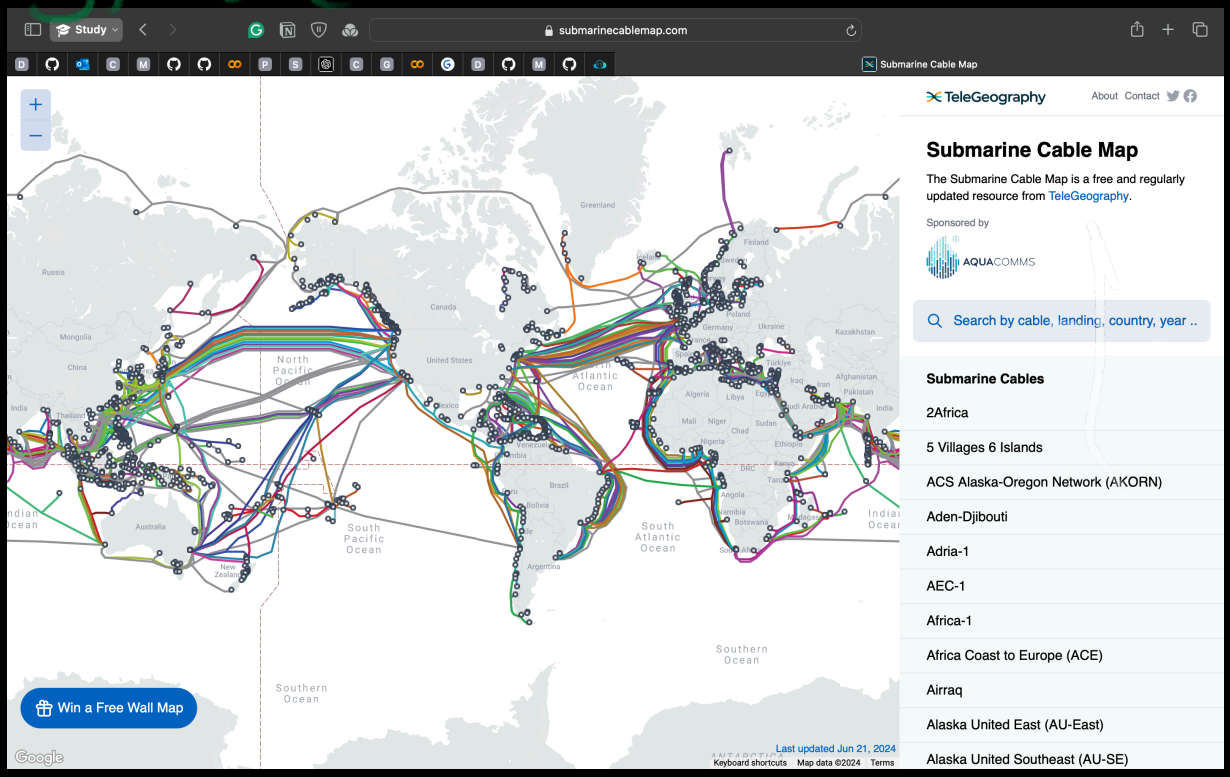
You send data from 1 comp to another — Upload

When someone sends data to you & you download - Download

These are download & upload speeds

You can check fast.com, speedtest.com

How Countries are Connected?



For example from chennai we are connected Srilanka & Mumbai we are connected Dubai, Oman & Singapore.

→ One Big entity (Tata Maybe) give to small entities they give to Internet service Provider & they give it to us this how it works on large scale.

Physically: optical fibre Cable, Coaxial Cables

Wireless: Bluetooth, Wifi, 2TE, 5G

Using these Cables is way faster than using via Satellites.

How various things are Connected?

Local Area Network (LAN): Small house/office

Ethernet, WiFi

Metropolitan Area Network (MAN) - Across the City

Wide Area Network (WAN): Across Countries

using optical fibre Cables.

① Sonet - Synchronous optical networking ② Frame - Relay

Internet is a Collection of all the above 3 LAN, MAN, WAN.

Alot of LAN are Connected to each other using MAN and they are Connected using WAN

WAN

① Sonet - Carries data using optical fibres hence can cover larger distance

② Frame Relay - A way to Connect LAN to WAN.

Now what is a Modem / Router?

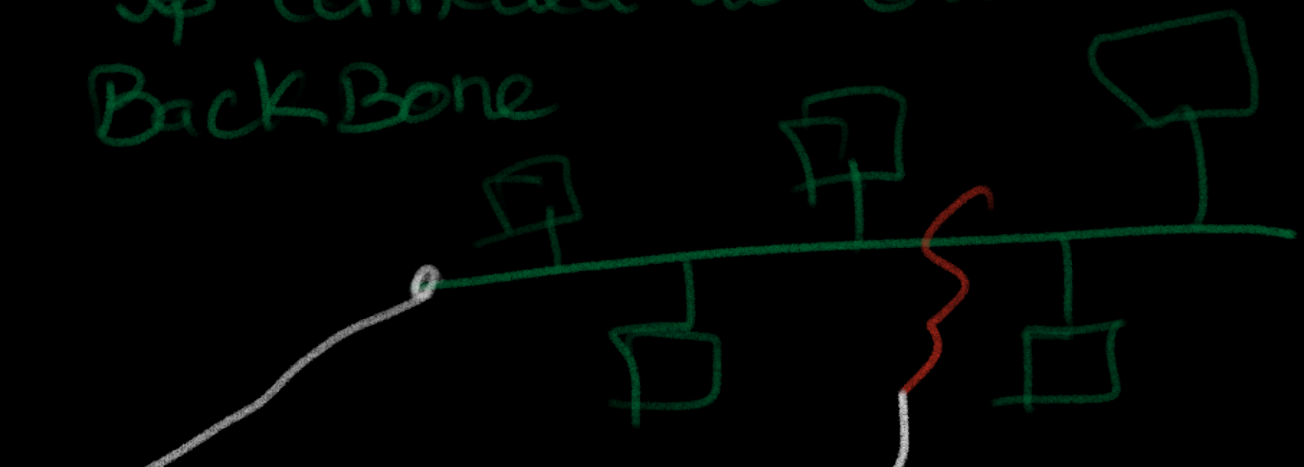
Modem is used to convert digital signal to analog signal & Vice Versa

ex: The digital data in your comp can be transferred to electronic signal so you can transfer it to other modem at the receiving system that will recover the digital data.

Router is basically device that routes the data packets based on IP address.

Topologies → How Computers are Connected

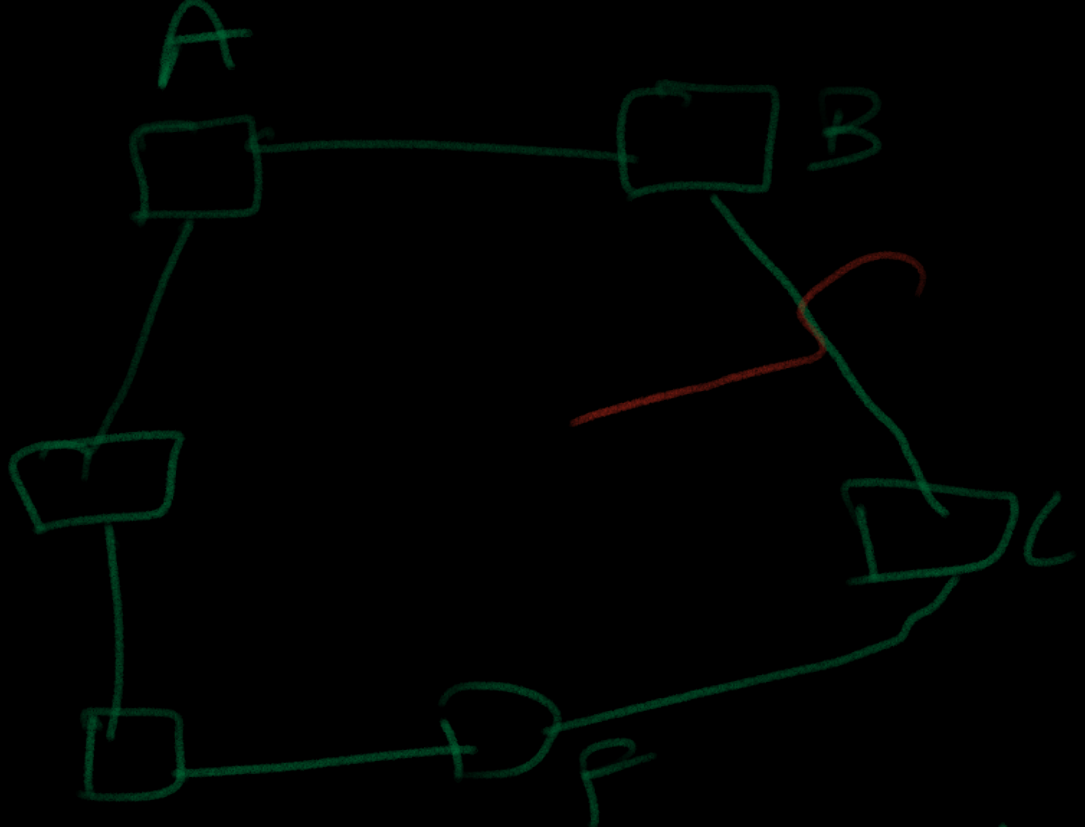
1. BUS → Every system in BUS topology is connected to one chord (or) one BackBone



→ If this link gets broken the entire network is spoiled

→ Since everything is transmitted by this cable only 1 person can send data at particular time.

2. Ring



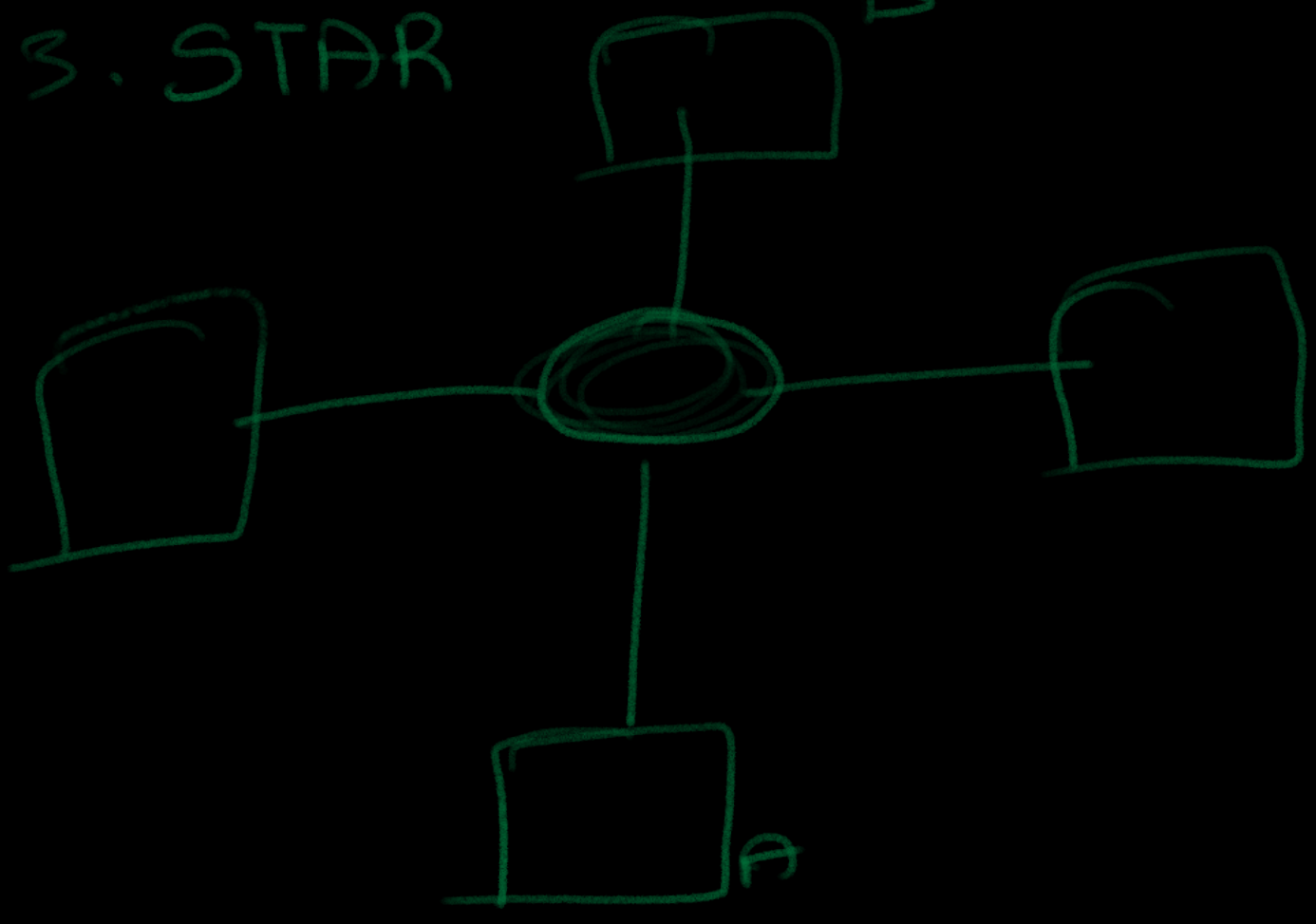
Here, every system communicates with one & other.

So, if I want from A - F It Should go through B & C Also

→ If the cable breaks, you can't transfer data

→ Lot of unrequired calls being made for example you want to send from A to F It makes the calls to B & C Also

3. STAR



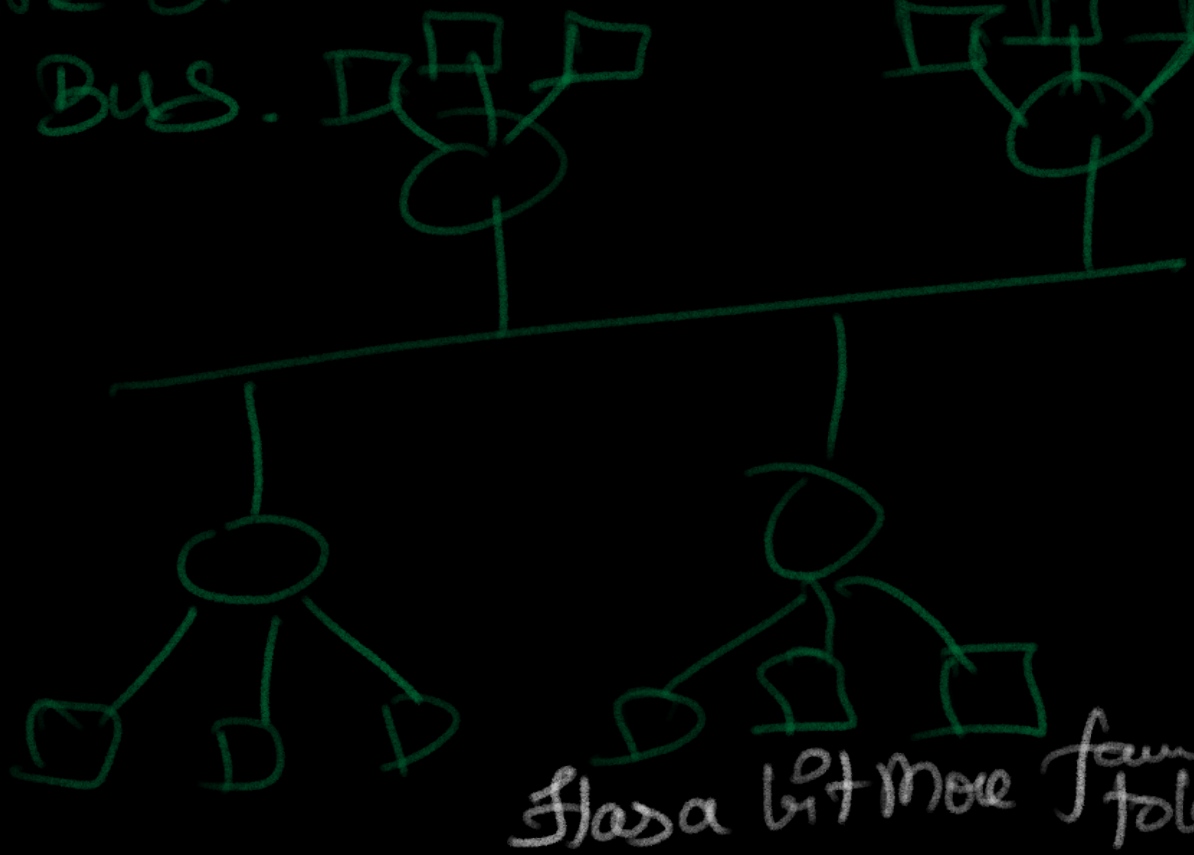
→ There is 1 Controlling / Central device that is connected to all the devices

If want to send from Comp A to Comp B then it will communicate via Central device

→ If Central device fails then Comp will go down.

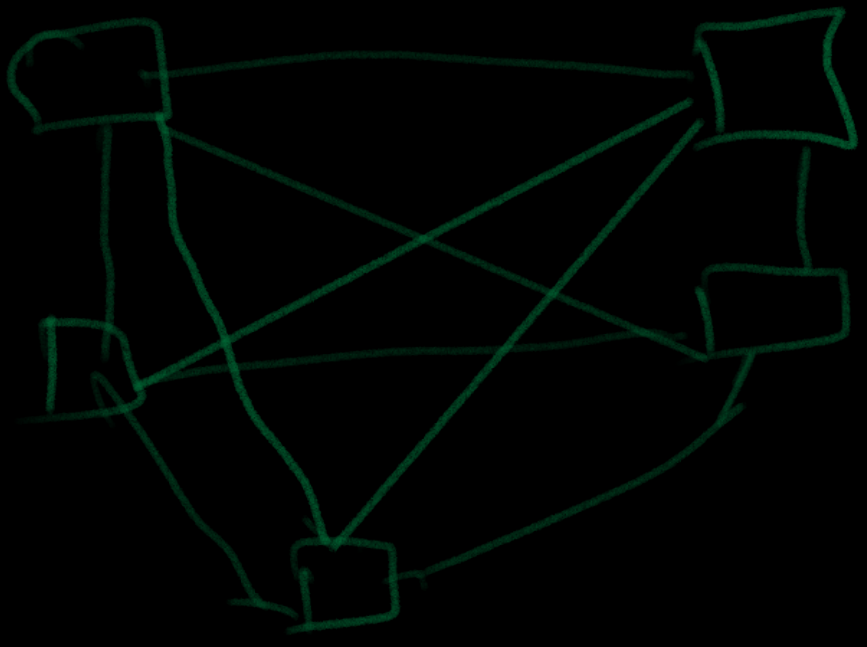
4. TREE (BUS - STAR)

Some Star networks connected like a Bus.



Has a bit more fault tolerance

5. MESH - Every Single Comp is connected to every single comp

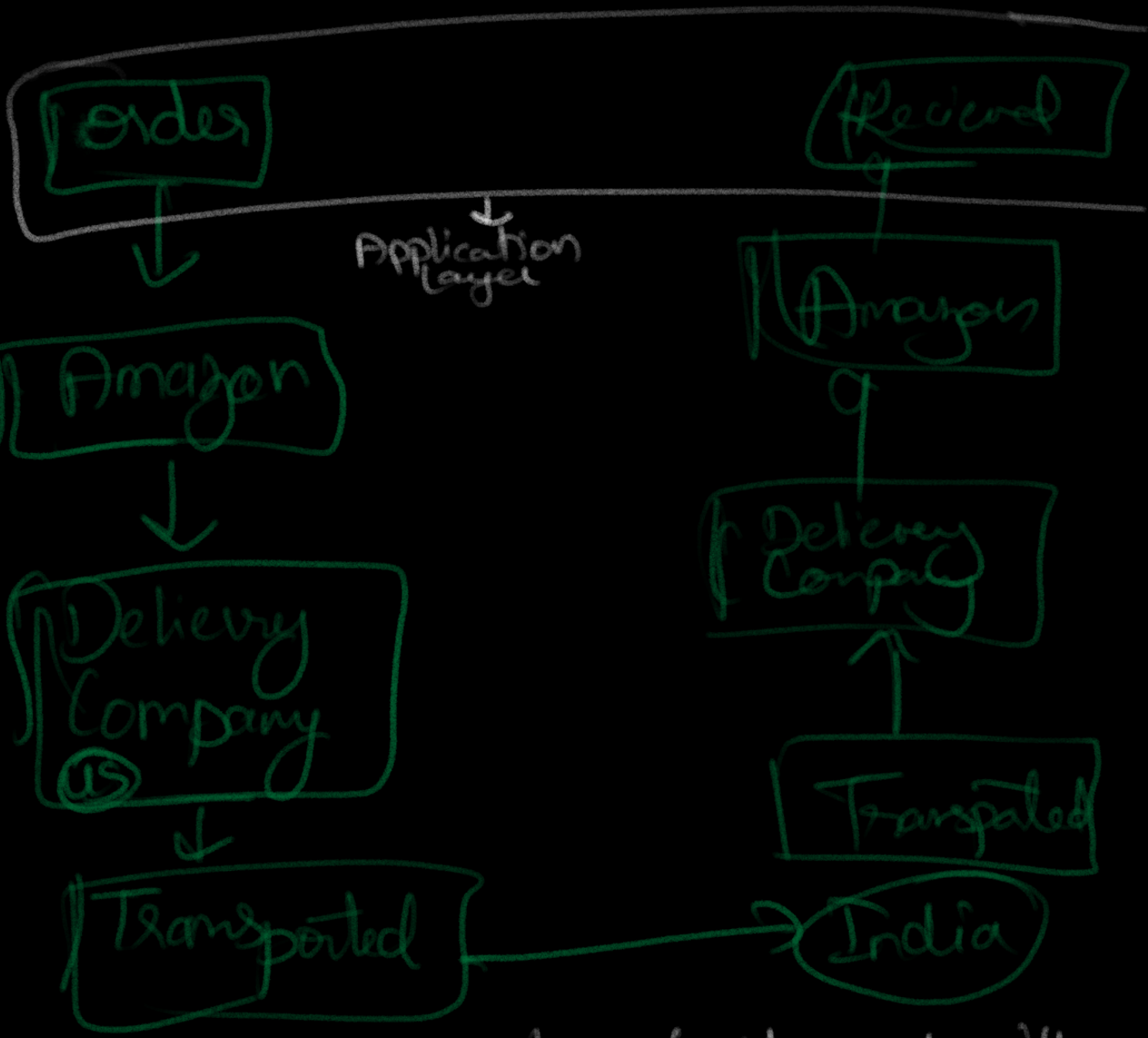


→ Expensive (so much wire used)

→ Scalability (if you add comp then you have to connect that with every Computer).

Structure of Network

Since, Internet is Complex let's break down.



⇒ Basically you request a yt video, yt will take care prepare the data it will give to transportation for it sends to server in your country & now it is recieved to you.

How the Internet Works

OSI Model – Open System Inter Connection Model

⇒ It is developed to ensure a Standard way how to Computers communicate with each other

7 Layers:

Application → Implemented in Software (App)

↓ you sent a message

Presentation ⇒ It will take data & Convert the data into Machine Representable Binary format Known as Translation.

⇒ from ASCII to EBCDIC. Before that data is transmitted it goes through encryption to make it readable to only the person that the data was sent to. Also provides Abstraction.

⇒ The data is also Compressed to send large files & reduce traffic

⇒ Encryption, Compression, Translation

→ SSL protocol is used for encryption & decryption

Session → It helps us setting up & managing connections & it enables sending & receiving data followed by termination of connected sessions.

→ Before a session is established it asks us for authentication like username & password & authorization takes place whether we have access to that file(s) or not.

→ Like how presentation layer assumes when we pass data to the low layer it gets it done similarly the session layer also assumes if it establish a session the data transportation will be done by transport layer.

Transport - Basically, it will work the data transport it to other end easily. It has it's own protocol how data is transfered like UDP & TCP.

It does in 3 ways

Segmentation - data that is recieved from session layer will divided into small data units called segments.

→ Every segment will contain source, destination port No & Sequence No.

Sequence No → helps to reassemble Segments in correct order

Flow Control - It controls amount of data that is being transported.

for example Server is sending at 40mbps & client is recieving at 20mbps it not going to work it will say slow down.

Error Control → It adds checksum to every segment that way whether the data received by friend is good or not.

→ Connection Oriented Transmission
↳ TCP

→ Connection less " " → UDP

⇒ UDP is faster, it doesn't provide feedback if data is lost.

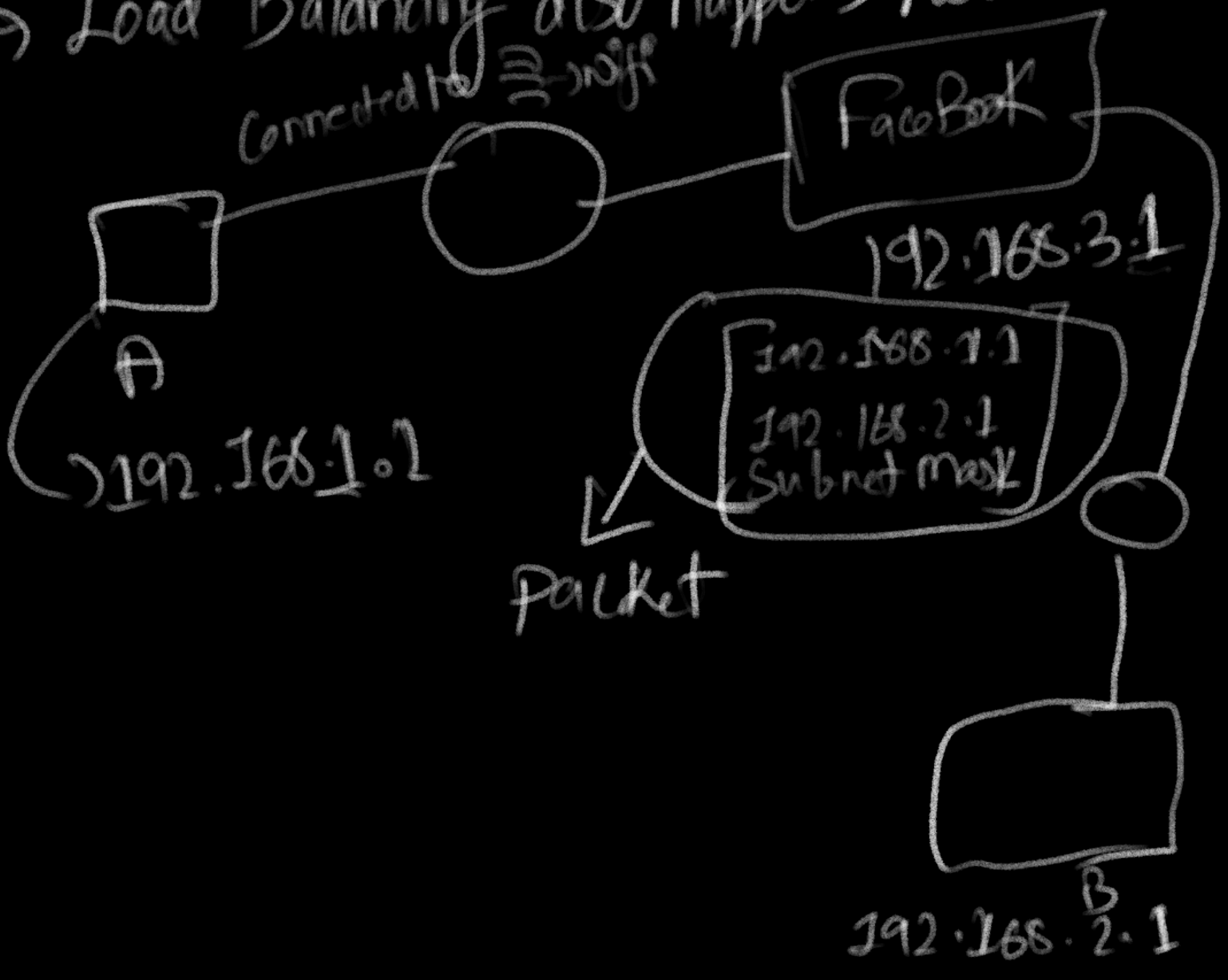
Network - It works for transmission of received data segments from one computer to another that is located in a different network.

⇒ Ip addressing done in network layer
↳ 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 correct destination

→ Also performs routing mooring are data packet from src to destination.

→ Load Balancing also happens here



Data link - Allows to directly Communicate to Computer & hosts.

→ Once it receive data packet from network, it will Contain Ip address of both Sender & reciever. On this layer 2 types of addressing is pejored.

1. Logical addressing - Same as network Layer

2. Physical addressing - MAC Addresses

Here in This layer MAC Address of Sender & Reciver are attached to data packet to form a frame

Frame - A data unit of data link layer

MAC Address - 12 Digit Alpha Numeric of network interface of Computer

→ Each Comp has more than 1 Macaddress like Comp Bluetooth have another ID Comp wifi has another & so on.

→ It allows all upper layers to access frames.

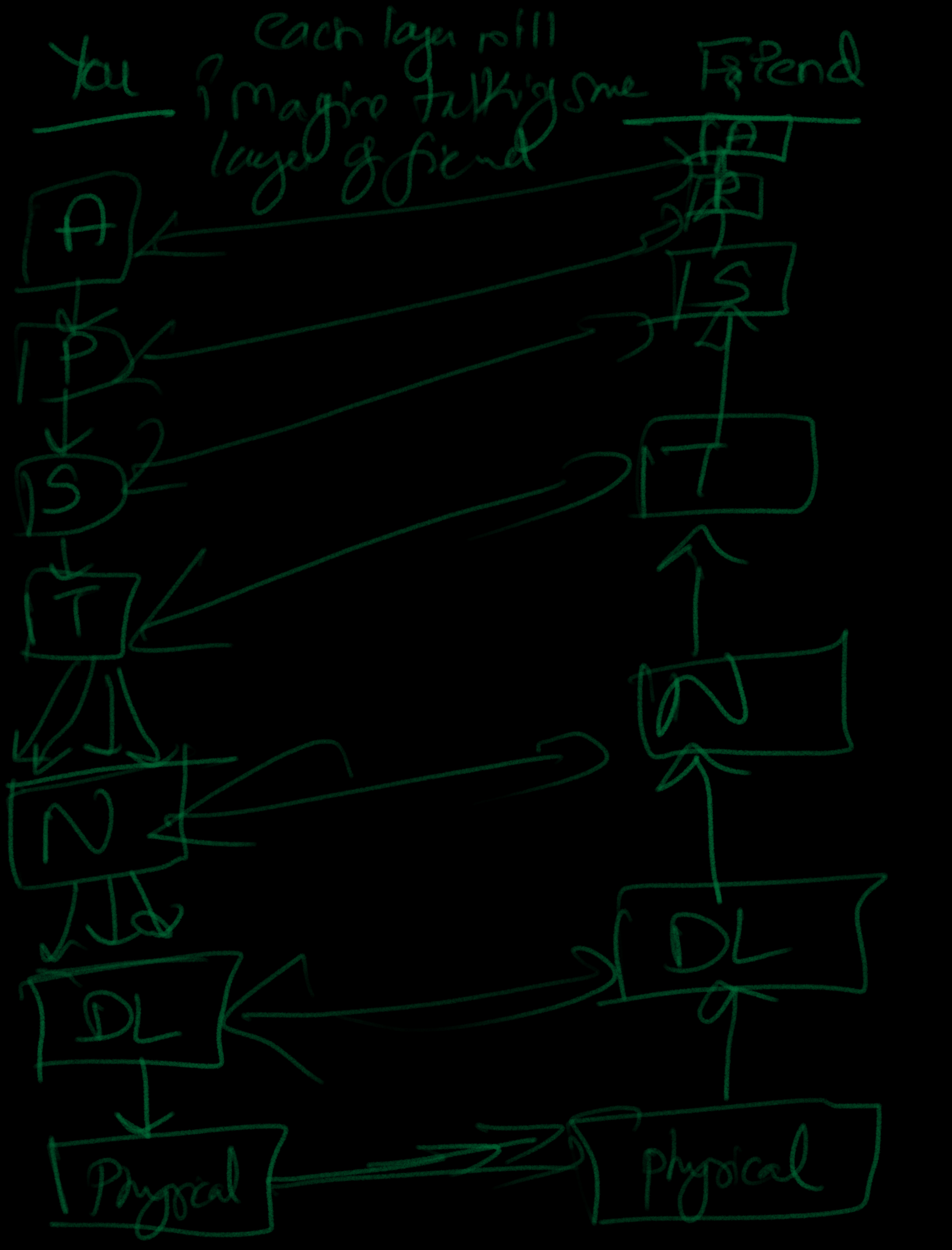
→ It also controls data is placed / received using things knowns as Media Access Control

→ Adds Mac address to packet to make a frame & pushes the frame to transport

Physical

→ It Contains hardware.

→ It transmits bits from electric signals


You
each layer will imagine talking same layer of friend
Friend
A
P
S
T
N
DL
Physical
A
P
S
T
N
DL
Physical

TCP/IP Model

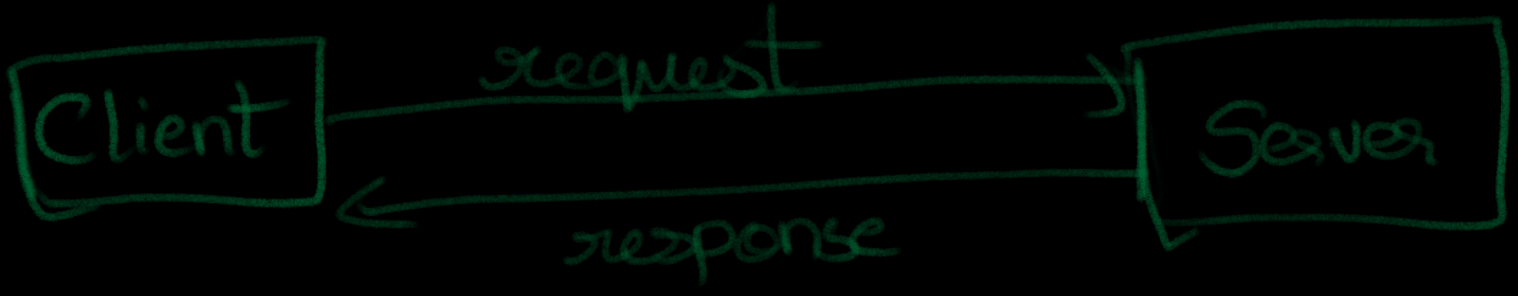
→ Another Model (Reduced to 5 layers)

Application
Transport
Network
Data Link
Physical

} 5 Layers

1. Application Layer:

→ Users interact with it
→ whatsapp, browsers etc
→ where: on your devices.
→ Protocols
→ (1) Client Server Architecture



(server is a system that contains the website you are hosting)

→ The app has 2 ports client port & Server port these are known as processes & they communicate with each other.
→ Server should have reliable IP address & high availability

→ Collection of Servers - Data Centre

```
base ~ (16.305s)
ping google.com

PING google.com (142.250.70.110): 56 data bytes
64 bytes from 142.250.70.110: icmp_seq=0 ttl=118 time=41.728 ms
64 bytes from 142.250.70.110: icmp_seq=1 ttl=118 time=41.650 ms
64 bytes from 142.250.70.110: icmp_seq=2 ttl=118 time=48.493 ms
64 bytes from 142.250.70.110: icmp_seq=3 ttl=118 time=41.887 ms
64 bytes from 142.250.70.110: icmp_seq=4 ttl=118 time=41.847 ms
64 bytes from 142.250.70.110: icmp_seq=5 ttl=118 time=48.181 ms
64 bytes from 142.250.70.110: icmp_seq=6 ttl=118 time=42.193 ms
64 bytes from 142.250.70.110: icmp_seq=7 ttl=118 time=48.558 ms
64 bytes from 142.250.70.110: icmp_seq=8 ttl=118 time=47.579 ms
64 bytes from 142.250.70.110: icmp_seq=9 ttl=118 time=44.465 ms
64 bytes from 142.250.70.110: icmp_seq=10 ttl=118 time=48.643 ms
64 bytes from 142.250.70.110: icmp_seq=11 ttl=118 time=48.204 ms
64 bytes from 142.250.70.110: icmp_seq=12 ttl=118 time=48.932 ms
64 bytes from 142.250.70.110: icmp_seq=13 ttl=118 time=45.670 ms
64 bytes from 142.250.70.110: icmp_seq=14 ttl=118 time=48.528 ms
64 bytes from 142.250.70.110: icmp_seq=15 ttl=118 time=48.039 ms
64 bytes from 142.250.70.110: icmp_seq=16 ttl=118 time=49.159 ms
^C
--- google.com ping statistics ---
17 packets transmitted, 17 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 41.650/46.103/49.159/2.961 ms
```

Command ping from terminal as you can see no packets lost & every packet is 64 bytes.

Here 142.250.70.110 is google's Ip address

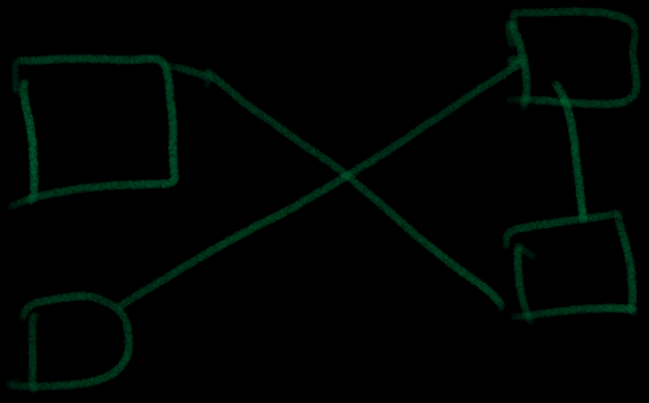
Icmp_seq is the sequence no.

The ping measures the round trip time from message sent from originating host to destination & echoed back

→ (2) Peer to Peer (P2P) Architecture

Apps running on various devices communicate by getting connected with each other. In this case there isn't server (or) data Centre

for ex:- In Colleges

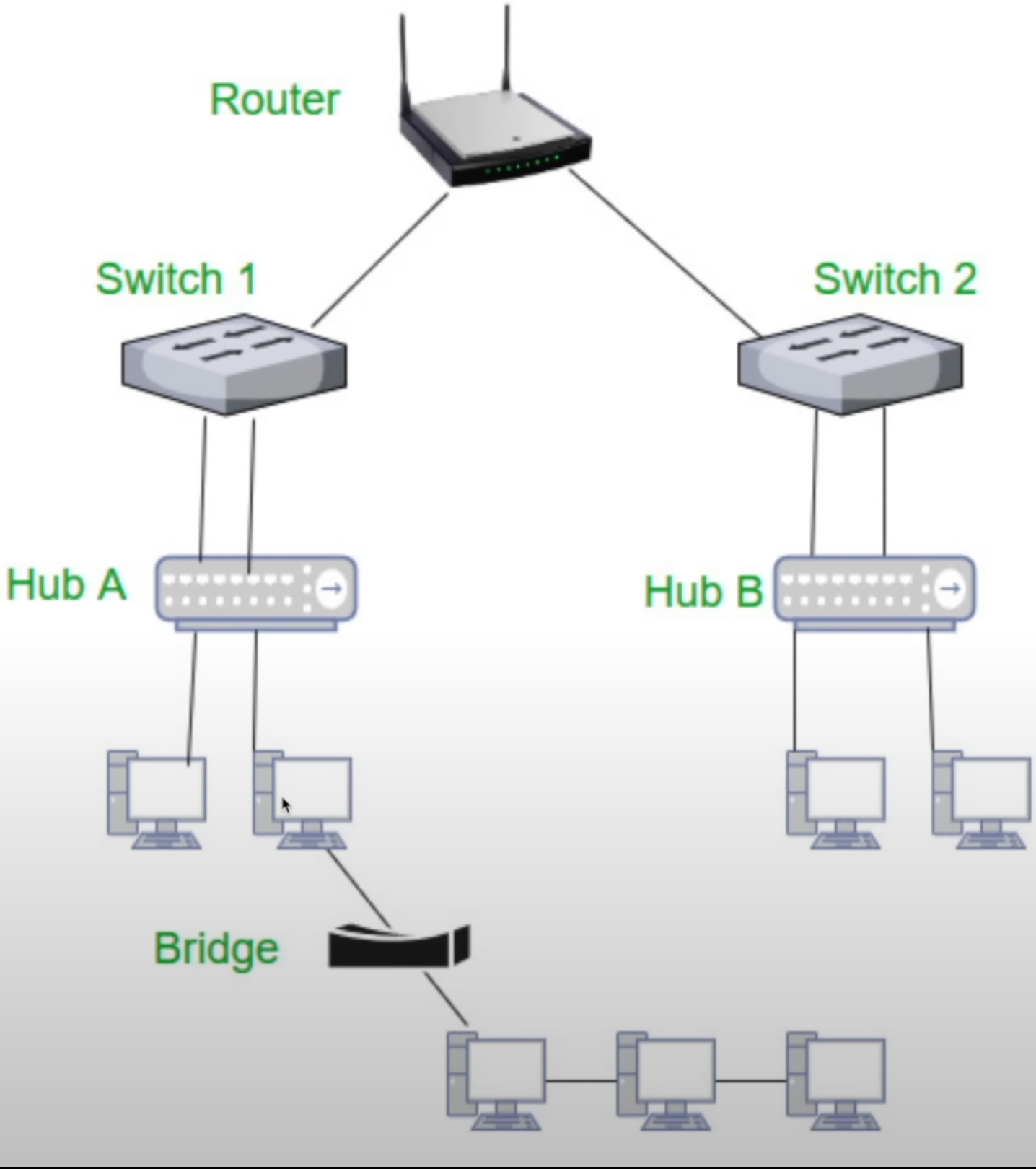


→ Easily Scalable
→ decentralized
→ Every Comp is client & Server
ex:- Bittorrent
→ Hybrid Also exits Some P2P & Some Centralized DB

Networking Devices

→

→ Link to get indepth info


Router
Switch 1
Switch 2
Hub A
Hub B
Bridge

Protocol

Web Protocols

* TCP/IP :
  - → HTTP (hypertext transfer Protocol)
  - → DHCP (Dynamic host Config Protocol)
  - → FTP (File transfer) (not being used anymore)
  - → SMTP (Simple mail transfer)
  - → POP3 & IMAC (To Receive Emails)
  - → SSH (secure Shell protocol)
  - → VNC (Virtual Net Computing) (graphical control)

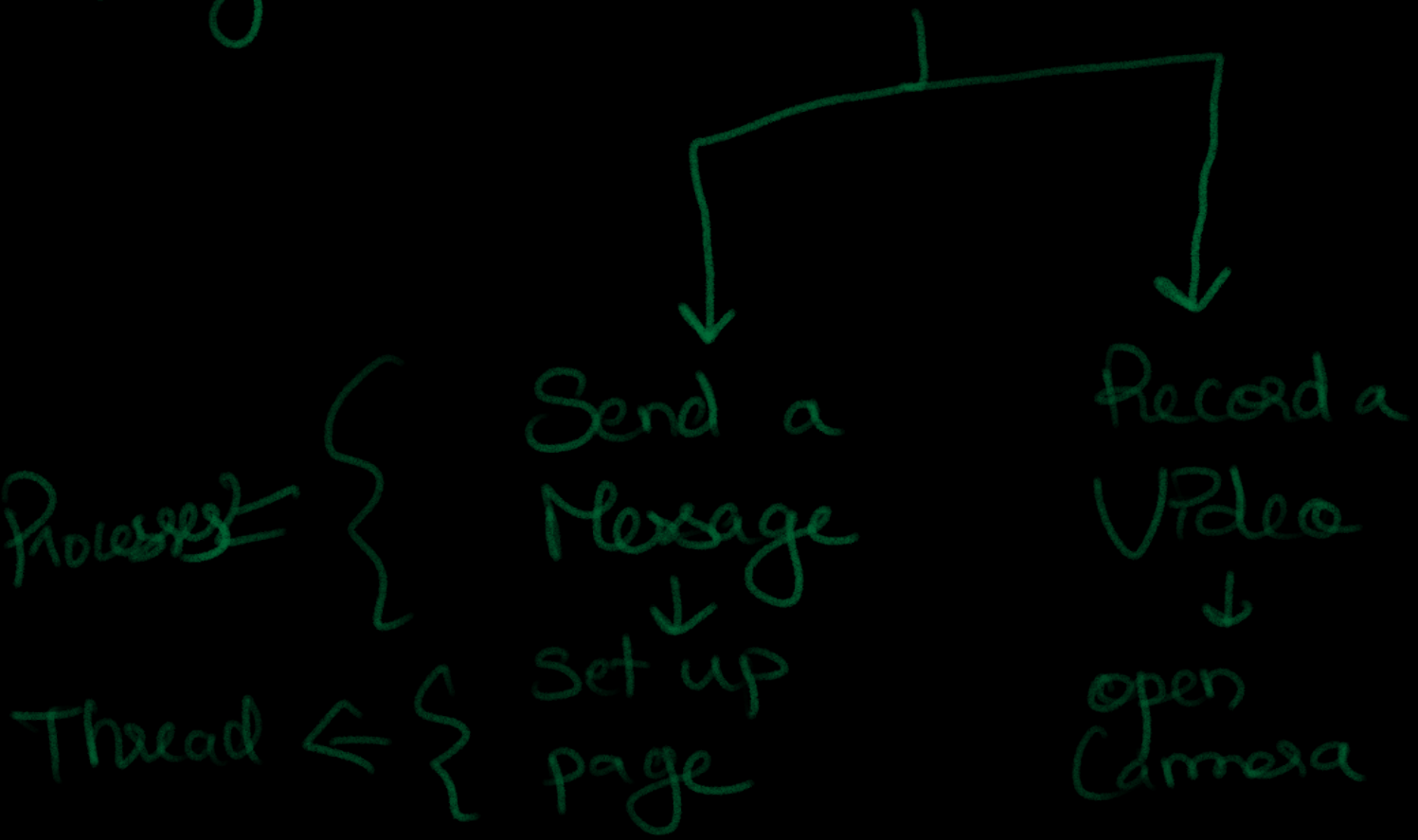
* TELNET : Terminal Emulation

It enables remote host using a telnet client usually port 23.

★ UDP : Stateless Connection

⇒ data may be lost like Video Conferencing.

Program : WhatsApp



→ A program can have multiple processes.

→ One processes can have multiple running threads.

→ Each thread is a lighter version of thread

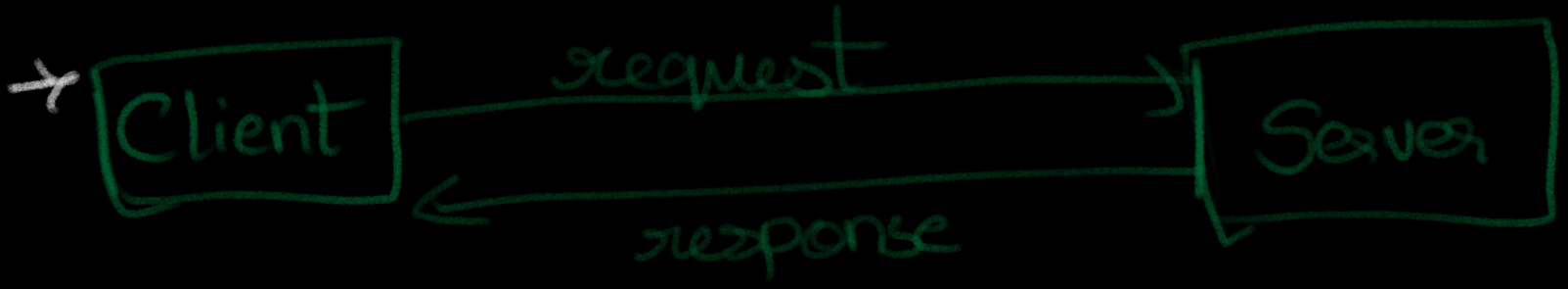
⇒ Thread does only one job unlike process.

→ Sockets: Interface b/w process & Internet

→ ports → Ephemeral Ports → Internally it will assign random portno & work with it.

Basically to which window (or) tab to send to.

HTTP (Hyper text transfer Protocol)



→ It's a client server protocol & it tells us how you request this data from the server & it also tells us how server will send data back to a client.

→ It's an application layer protocol.

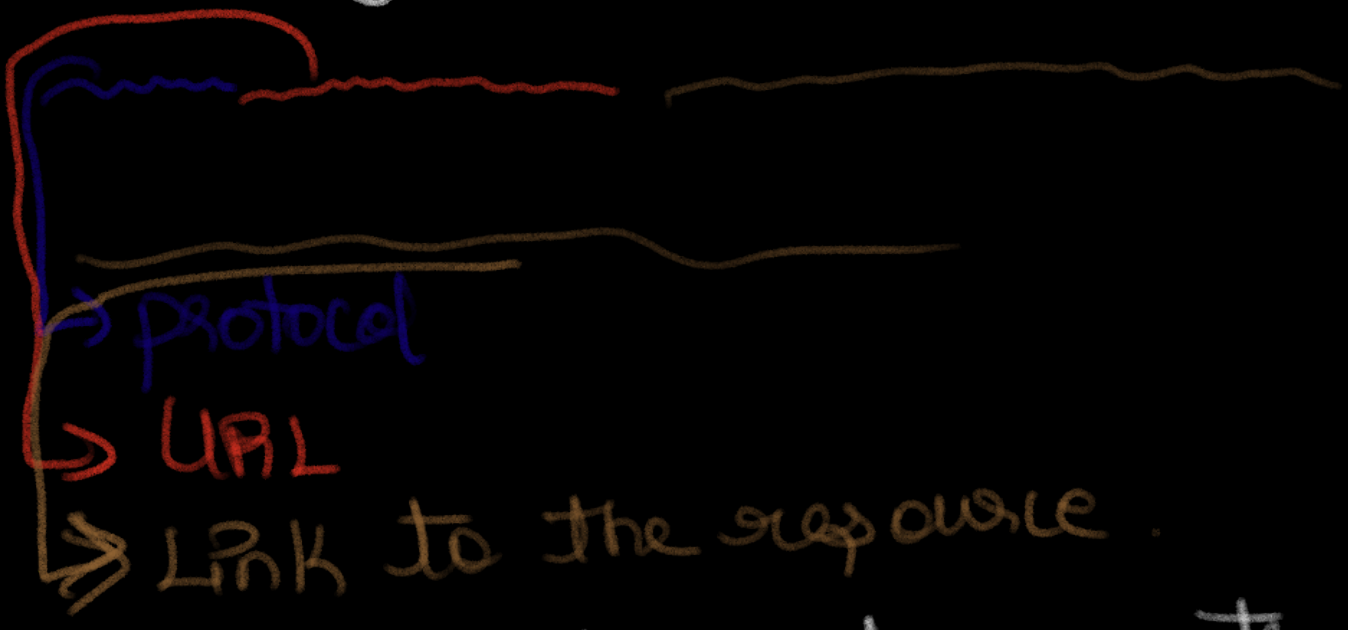
ex:- It has few methods

GET, POST, PUT, PATCH, DELETE.

→ HTTP uses TCP (Transmission Control Protocol) in inside it Transport layer)

→ HTTP is Stateless protocol

→ Server will not store anything sent by client by default.



→ We can also add arguments, for example

→ After ? in Argument

→ Above After question is Argument video = videoId

HTTP Method: It's a method that tells server what to do.

1. GET Method

It means you are requesting the data.

2. POST Method

You are sending the data.

3. PUT Method

puts data at specific location

4. DELETE Method

Delete the data from Server.

Status Codes

when you send a req to server you need a way to know whether it was sent or fail whatever for that the Status Code exists.

200 - Request Successful

404 - Couldn't find it

400 - Bad Request

500 - Internal Server Error

There are classes for these status Code :-

1xx - Informational Category

2xx → Success Codes

3xx → Ridirection

4xx → client error

5xx → Server Error

Cookies :

→ HTTP is stateless as we Know then how do everytime you close Amazon

Tab the Cart items 2 your account is still logged in the answer is Cookies

⇒ It's a Unique string.

⇒ It's stored on client Browser

⇒ When you visit a website for a 1st time it will set a Cookie

⇒ Whenever you make a request After that in the request header a Cookie will be sent then Server will know this request is coming from you & you sent a Cookie & it will check the DB & find a State for that

→ In the response, you can see like below it has tag called Set-cookie it also has url, names & path & also expiration date.

→ Some times cookies can be misused to track the client's data

Third party Cookies

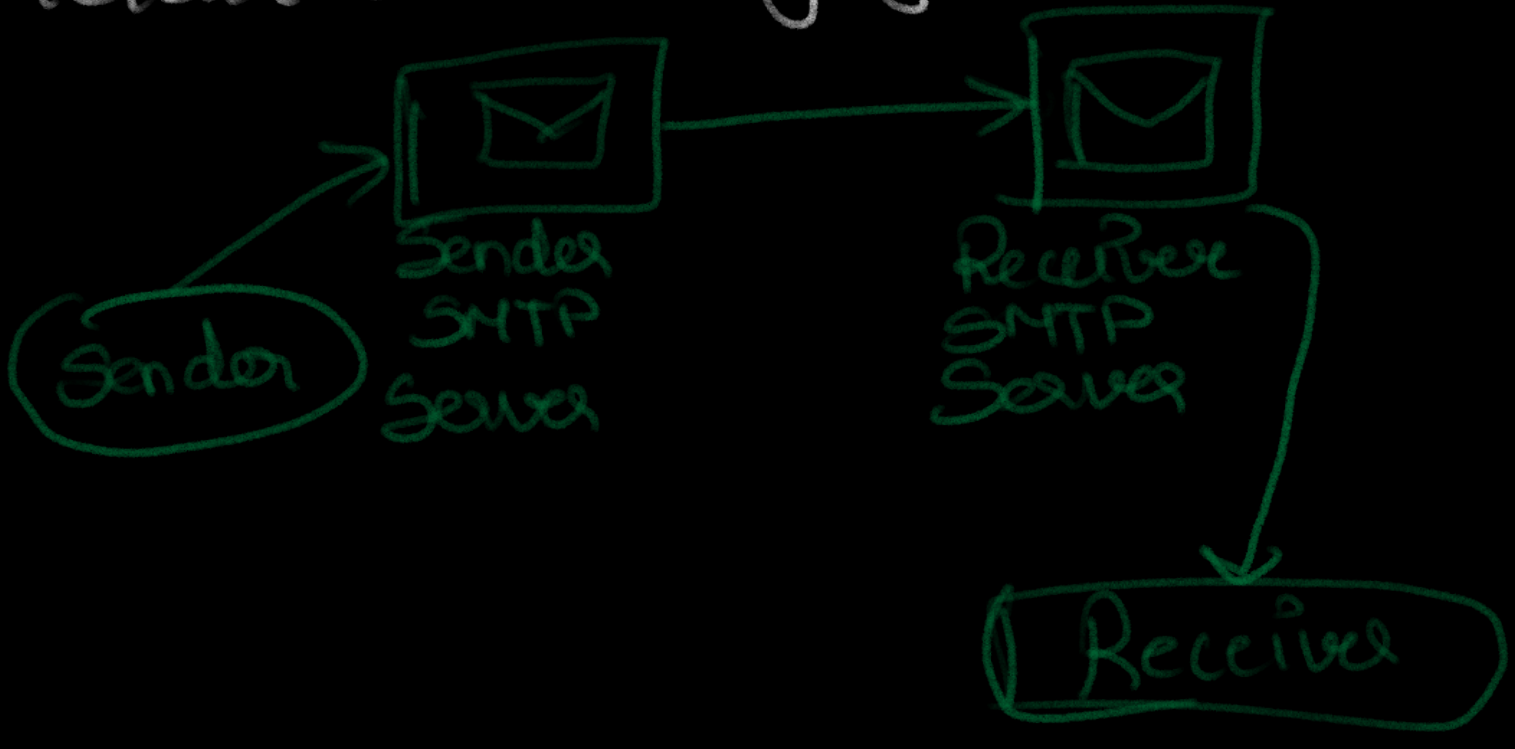
→ Cookies that are set for the URL's you do not visit.

Ex:- A website like youtube has an add of facebook that way FB might use your cookies

How EMAIL Works

→ for sending email SMTP is used & for receiving POP3 is used & this is at Application Layer

→ Let's you are sending mail from icloud.com to google.com



→ Internally it uses TCP.

→ If both are using gmail.service then it directly changes it.

→ Using the Name Server lookup command you can find the name & ipaddres of smptp servers. Check Below

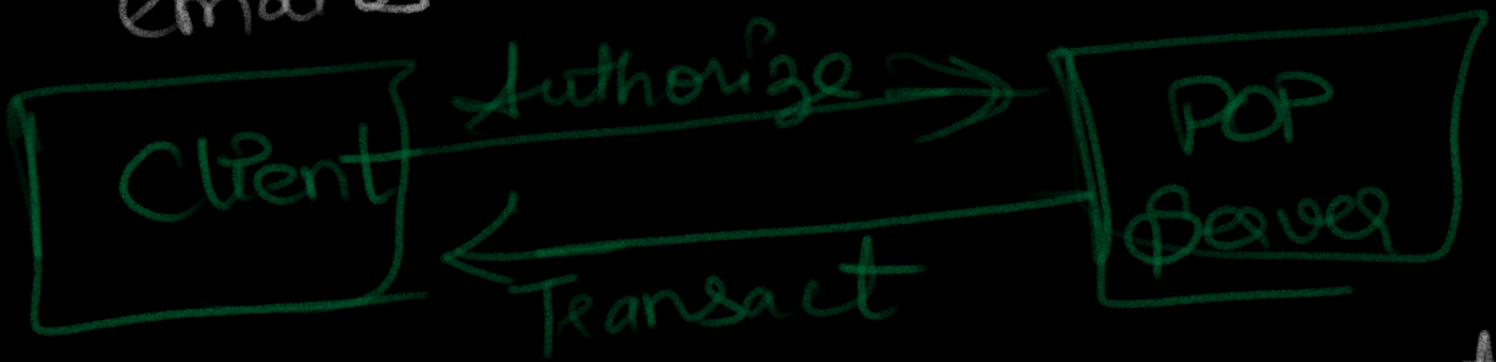
nslookup -type=mx gmail.com
↳ mail exchange

```
base ~ (0.124s)
nslookup -type=mx gmail.com

Server:         10.20.1.1
Address:        10.20.1.1#53

Non-authoritative answer:
gmail.com       mail exchanger = 5 gmail-smtp-in.l.google.com.
gmail.com       mail exchanger = 10 alt1.gmail-smtp-in.l.google.com.
gmail.com       mail exchanger = 20 alt2.gmail-smtp-in.l.google.com.
gmail.com       mail exchanger = 40 alt4.gmail-smtp-in.l.google.com.
gmail.com       mail exchanger = 30 alt3.gmail-smtp-in.l.google.com.

Authoritative answers can be found from:
.       nameserver = h.root-servers.net.
.       nameserver = b.root-servers.net.
.       nameserver = c.root-servers.net.
.       nameserver = a.root-servers.net.
.       nameserver = g.root-servers.net.
.       nameserver = j.root-servers.net.
.       nameserver = f.root-servers.net.
.       nameserver = k.root-servers.net.
.       nameserver = l.root-servers.net.
.       nameserver = d.root-servers.net.
.       nameserver = m.root-servers.net.
.       nameserver = e.root-servers.net.
.       nameserver = i.root-servers.net.
```

```
base ~ (0.191s)
nslookup -type=mx icloud.com

Server:         10.20.1.1
Address:        10.20.1.1#53

Non-authoritative answer:
icloud.com      mail exchanger = 10 mx02.mail.icloud.com.
icloud.com      mail exchanger = 10 mx01.mail.icloud.com.

Authoritative answers can be found from:
.       nameserver = g.root-servers.net.
.       nameserver = j.root-servers.net.
.       nameserver = f.root-servers.net.
.       nameserver = k.root-servers.net.
.       nameserver = l.root-servers.net.
.       nameserver = d.root-servers.net.
.       nameserver = m.root-servers.net.
.       nameserver = e.root-servers.net.
.       nameserver = i.root-servers.net.
.       nameserver = h.root-servers.net.
.       nameserver = b.root-servers.net.
.       nameserver = c.root-servers.net.
.       nameserver = a.root-servers.net.
```

→ To download & receive E-Mails lets look at POP (Post office Protocol)

→ It uses port 110 & it does the authorization & then the client asks the Server for all the new emails



→ After authorizing, You transact all the emails.

→ Then you command the Server like to delete, Archive & So, on.

IMAP (Internet Message Access Protocol)

→ It allows to view Email on Multiple devices.

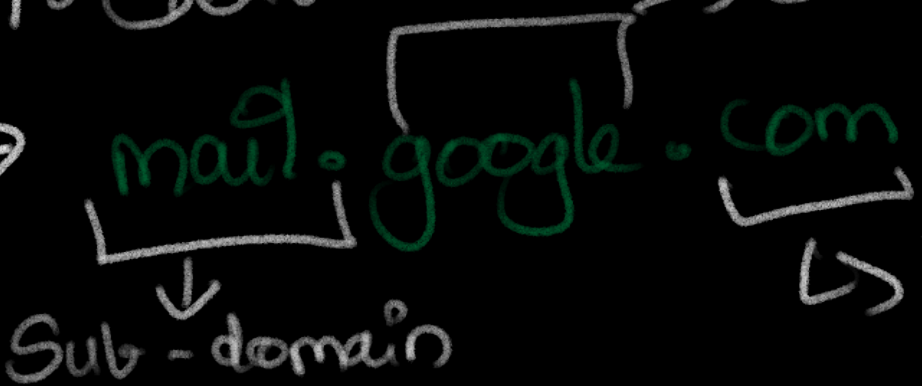
ex:- If you delete an email in your phone it will be deleted in Mac & Ipod as well.

DNS - Domain Name System

→ for example when you enter google.com it will use DNS to find the Ip add of google.com

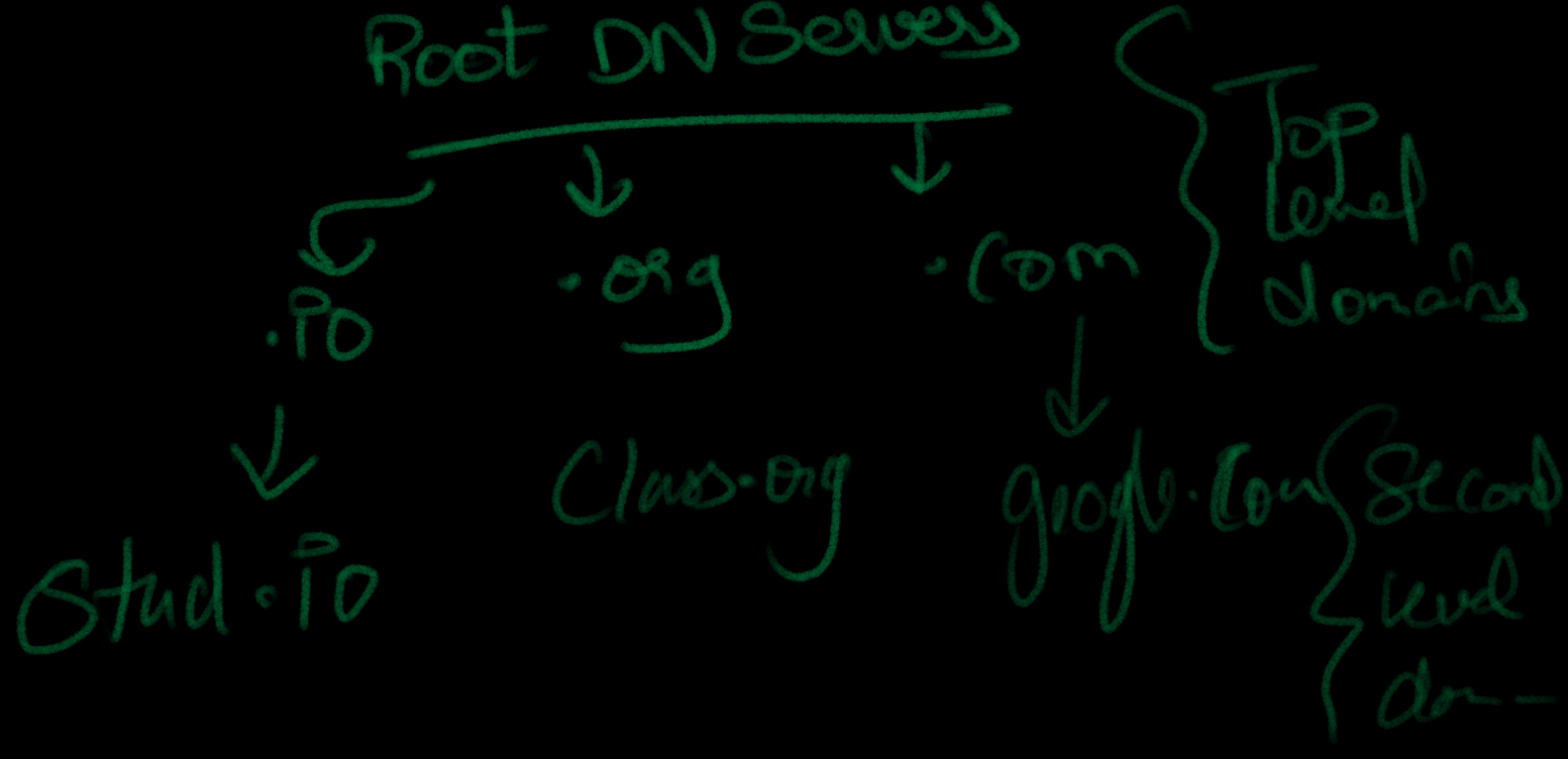
→ part of ~~App~~ Layer.

→ When clicked google.com http protocols uses DNS & Convert the URL into Ip add & then Connect to Server.

→ 

→ Sub-domain is a part of bigger domain

→ Top level are known as Root DNS Servers



→ Root DNS servers are the first point of Contact.

→ to check who is maintaining these servers

→ .com is for Commercial, .edu for educational, .in, .us → Country specific

the above are managed by this ICANN.

→ When you enter a new website, it will store the Ip add in your local Cache/DNS. To make it not search again & again.

(check in own computer)

→ If not found in local system it searches in local dns server.

↳ (ISP)

→ checks own Computer or else local DNS Server (ISP) it checks through Root Server if not there then sends to ISP & ISP sends to Top level domain which send Ip address to DNS.

```
base ~ (0.12s)
 dig google.com

; <<>> DiG 9.10.6 <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51857
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             231     IN      A       142.250.183.142

;; AUTHORITY SECTION:
.                       22083   IN      NS      j.root-servers.net.
.                       22083   IN      NS      f.root-servers.net.
.                       22083   IN      NS      k.root-servers.net.
.                       22083   IN      NS      l.root-servers.net.
.                       22083   IN      NS      d.root-servers.net.
.                       22083   IN      NS      m.root-servers.net.
.                       22083   IN      NS      e.root-servers.net.
.                       22083   IN      NS      i.root-servers.net.
.                       22083   IN      NS      h.root-servers.net.
.                       22083   IN      NS      b.root-servers.net.
.                       22083   IN      NS      c.root-servers.net.
.                       22083   IN      NS      a.root-servers.net.
.                       22083   IN      NS      g.root-servers.net.

;; Query time: 35 msec
;; SERVER: 10.20.1.1#53(10.20.1.1)
;; WHEN: Wed Jun 26 20:05:46 IST 2024
;; MSG SIZE  rcvd: 255
```

To check Messages received by DNS servers you can the clear command

→ This Ip address is what is stored in my local Cache -

$ man dig - manpage of dig

dig - DNS lookup utility

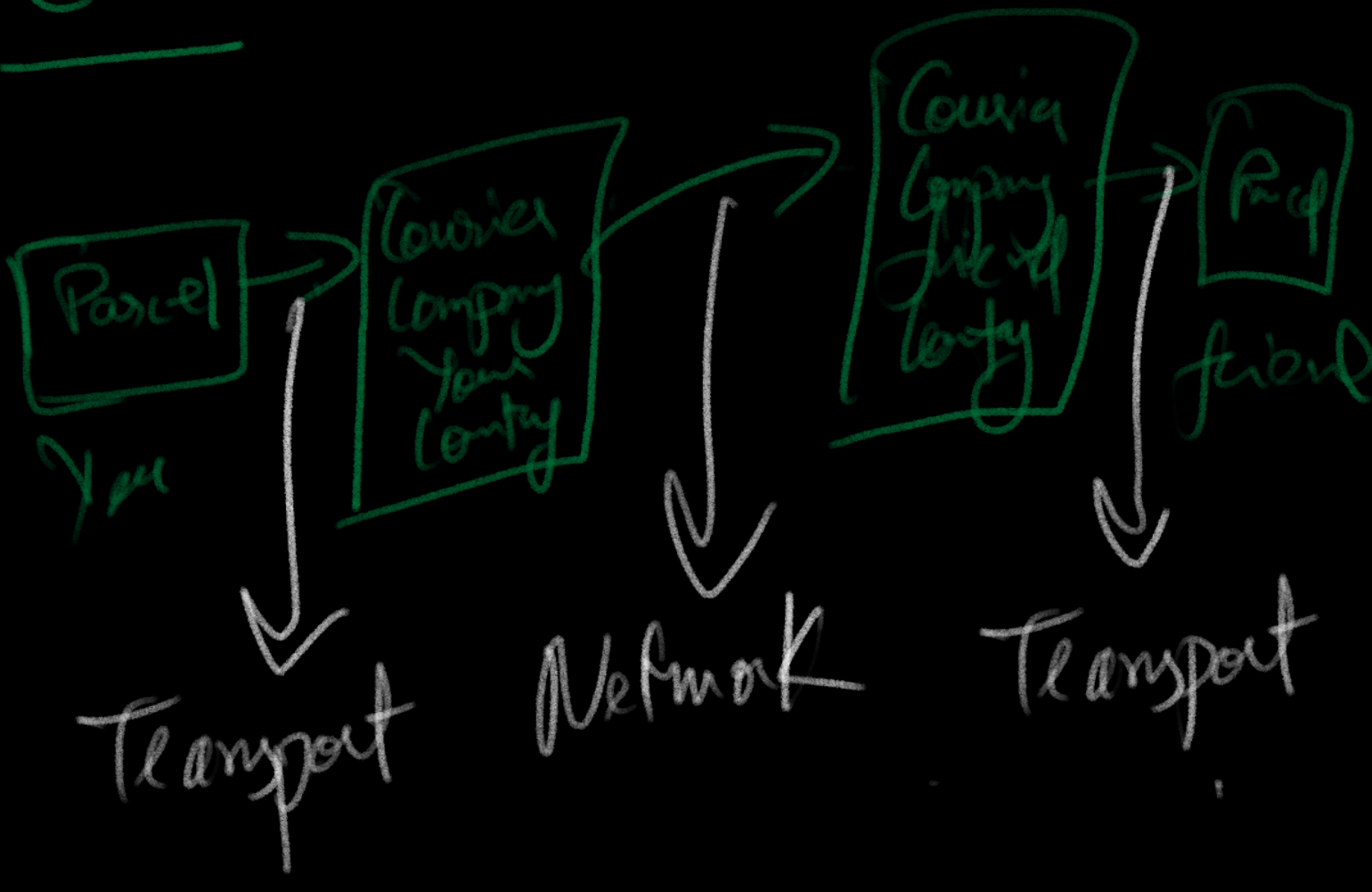
2: Transport Layer

you write a message & send it to your friend.

→ The message transportation from one computer to other is done by Network Layer.

→ The Role of transport layer is to take information from the network layer & send to the correct application. This layer is in the device itself.

Ex:



→ from 1 device to another device it uses Network layer but within each device for the app it uses transport Layer.

⇒ Transport 1 gives → Network 1

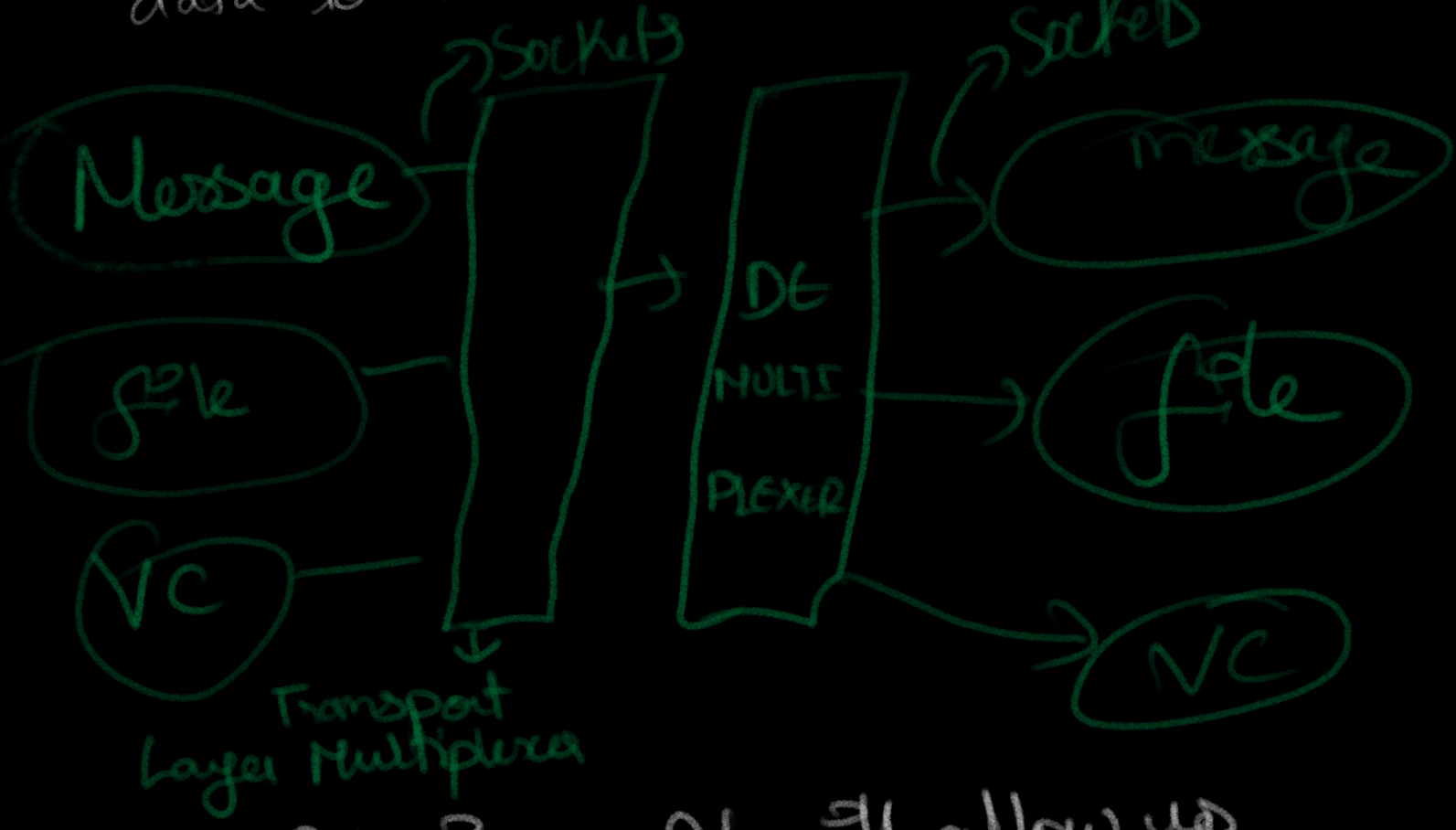
→ Network 2 gives → Transport

→ Transport layer have some protocols

TCP - 100% of data can be sent & in order.

UDP - Some data may not be in order & some data packets maybe lost.

Let's figure out how our Comp will determine to send these types of data to the network.



→ Multiplexing : It will allow up all these messages & things to a lot of destinations in above examples 3 apps 3 destination just via 1 Medium

→ De Multiplexing : opp of Multiplexing It will pass it through apps

→ Data travels in packets

→ Transport layer will attach these socket port no, so we will know where it is coming from & where to send the data.

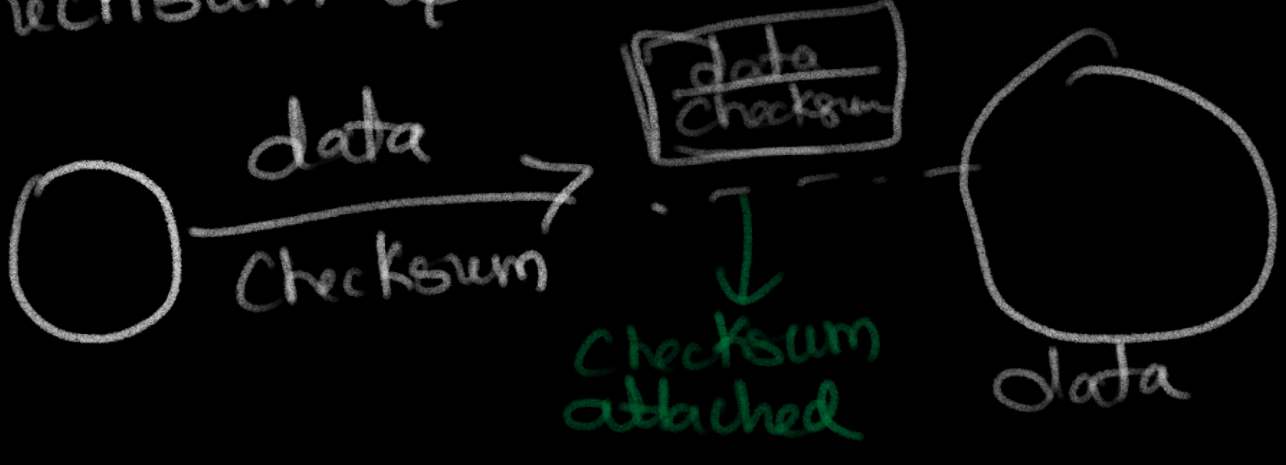
→ This layer also takes care of Congestion Controls. (Traffic)

→ Congestion control algos built in TCP are used.

CheckSums

→ checksum is a random number

→

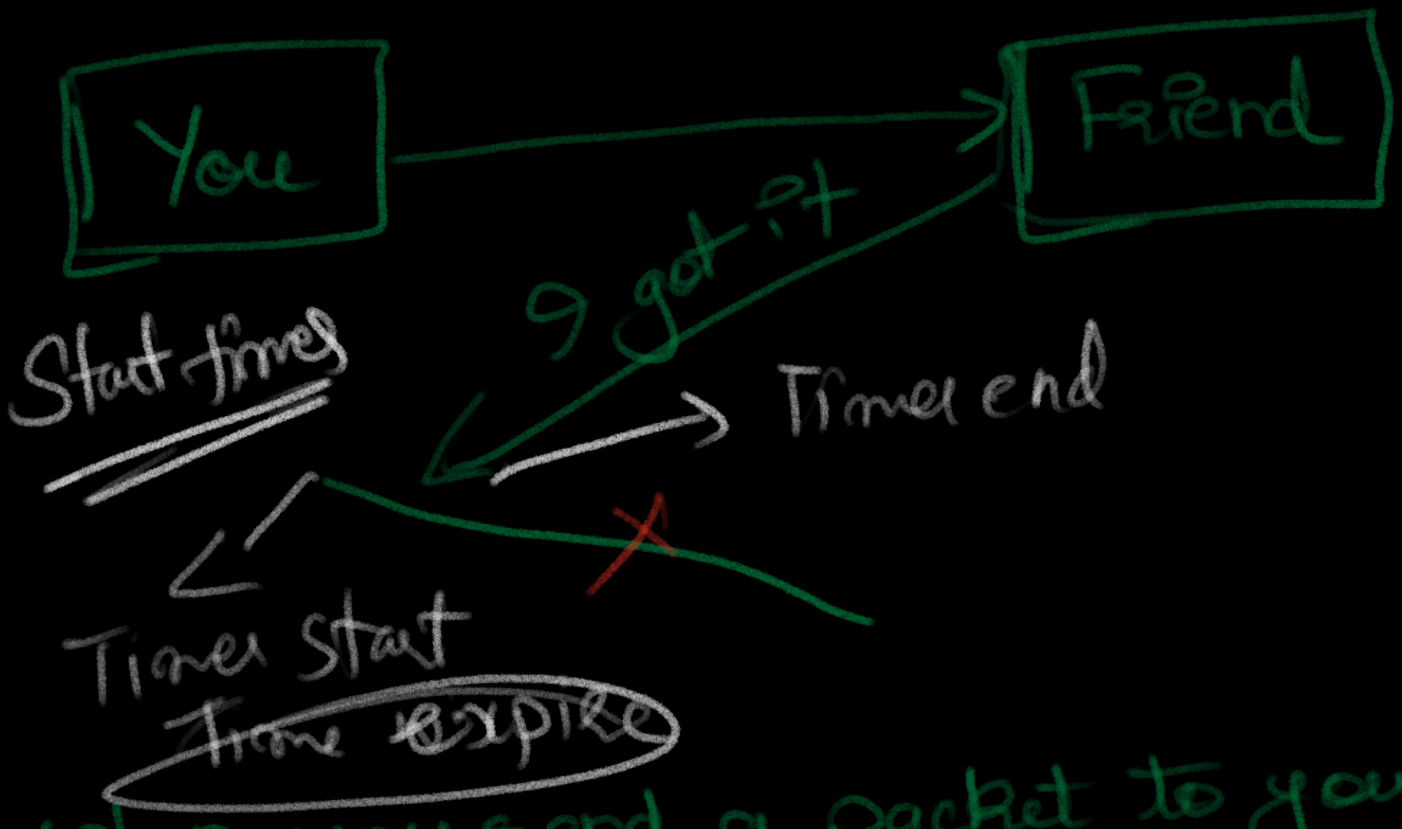


→ you send data to your friend using the data it will calculate a particular string val called checksum then friend get the data & since checksum is calculated using the data. The data will have a checksum associated with it. So, the checksum will be attached & when friend receives data, it will calculate using same Algo.

→ If value is diff something is wrong if value is same then it is correct.

→ How would I know whether my data/packets are received to my friends?

Timers:

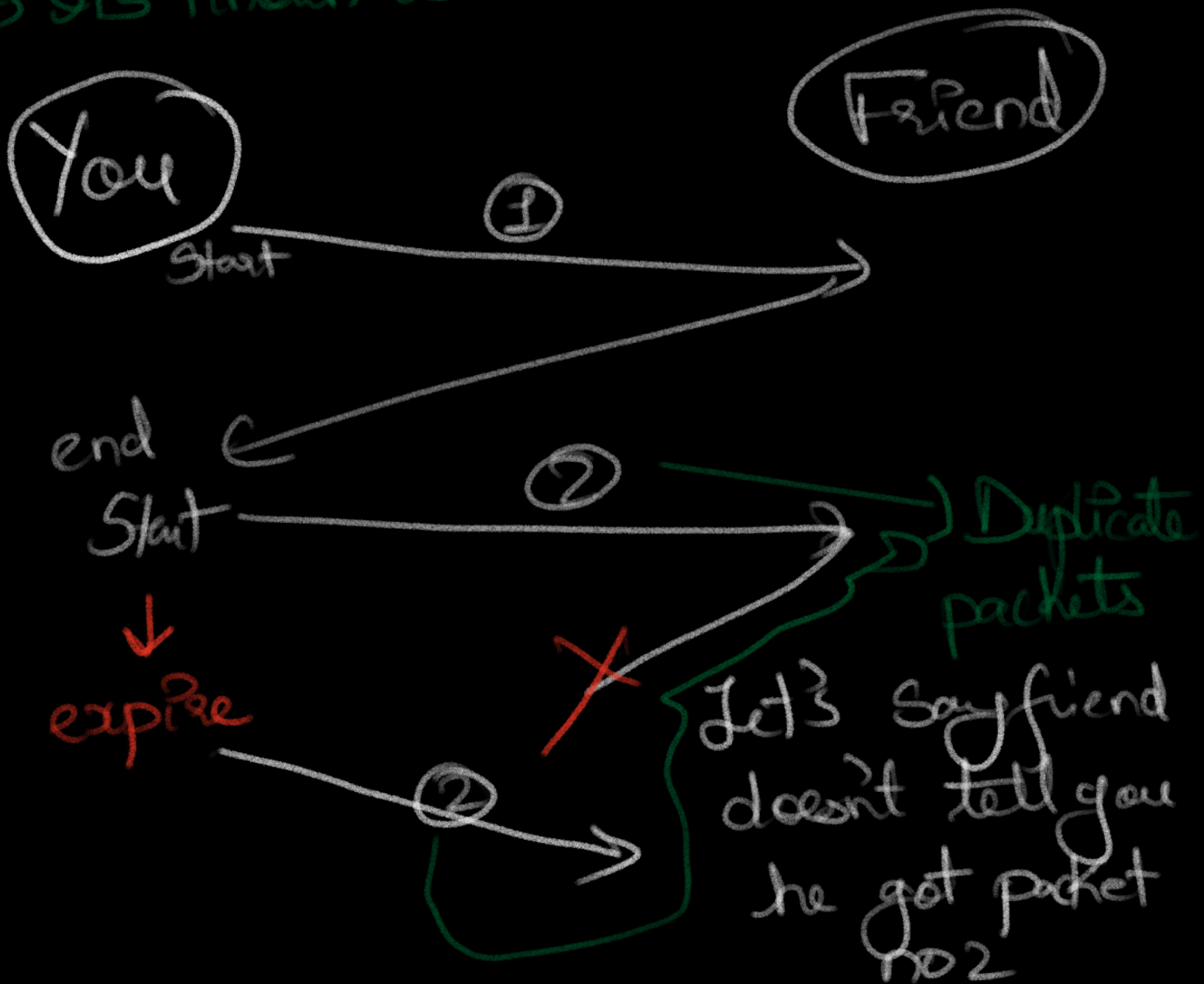


When you send a packet to your friend you will start a timer.. friend will say I got the packet now you will know I got packet & Timer ends.

⇒ You sent another packet & in b/w only another packet is lost, when you send again timer will start again & since it's lost your friend won't be able to say he got the packet now timer will expire.

→ By Timer expiry, you will the packet is not sent.

→ It's known as Re-Transmission Timer



→ So, you have not received that & let's say timer will expire. Since, I don't know whether they received

(or) not & will send packet no ⑤ again. Now the friend has 2 packet no ⑤ a duplicate

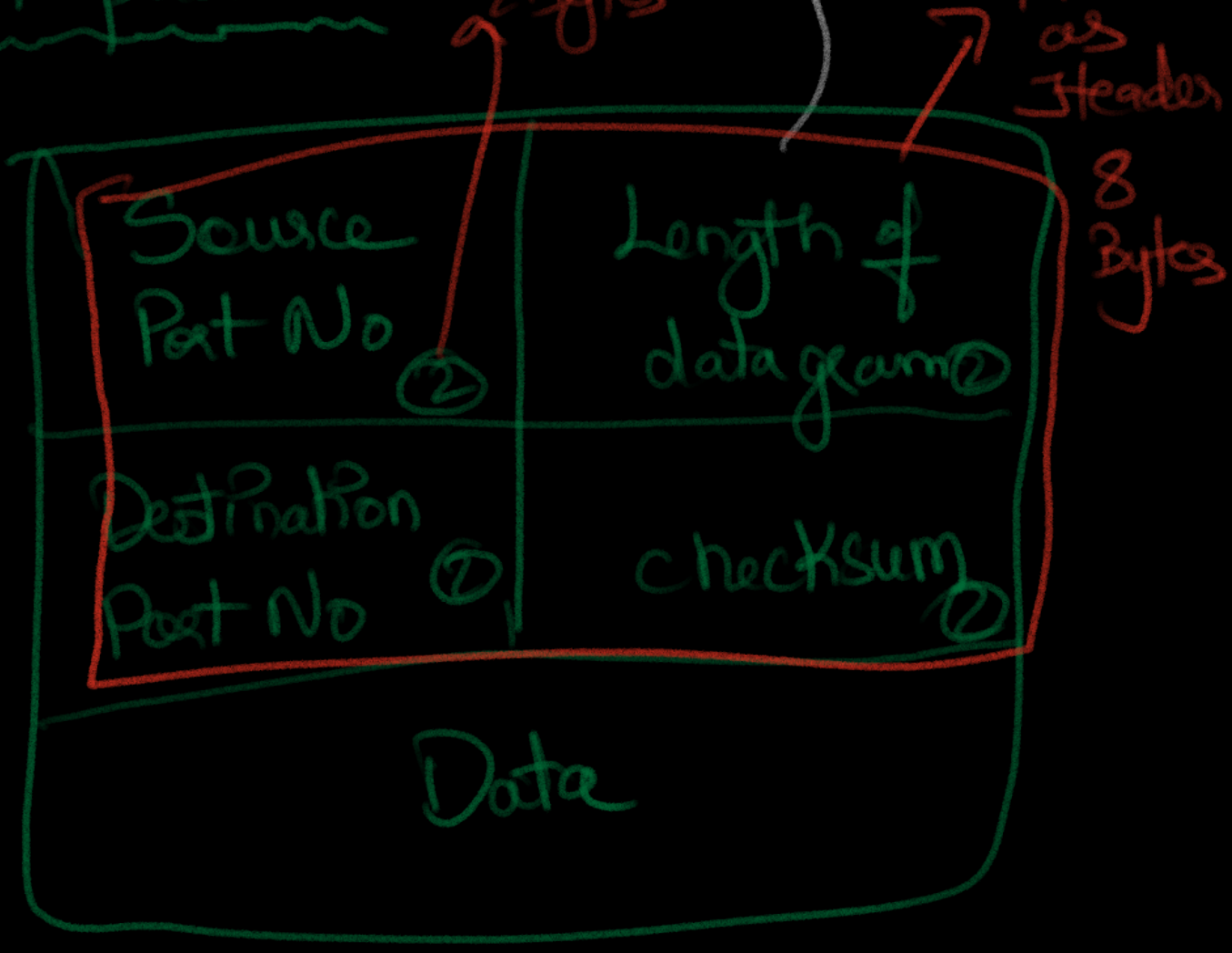
→ We solve the above problem using Sequence Nos.
→ Every segment/packet will get a unique number.

USER DATAGRAM PROTOCOL (UDP)

→ It's a transport layer protocol
→ Data may (or) may not be delivered
→ Data may change
→ Data may not be in order.
→ Connectionless protocol
→ UDP uses checksums but won't do anything when the data is gone

Length of packet

UDP packet



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

$\approx$ 65K Bytes

↳ Size of data you can send in 1 packet.

→ UDP is faster. → Use cases

→ Video-Conferencing
→ DNS Also uses UDP
→ gaming Also uses UDP
} of UDP

```
base ~ (9.66s)
sudo tcpdump -c 5
Password:
tcpdump: data link type PKTAP
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on pktap, link-type PKTAP (Apple DLT_PKTAP), snapshot length 524288 bytes
23:13:00.151515 IP 10.20.1.44.31013 > 10.20.1.1.domain: 17584+ A? www.youtube.com. (33)
23:13:00.151581 IP 10.20.1.44.18210 > 10.20.1.1.domain: 49937+ Type65? www.youtube.com. (33)
23:13:00.159895 ARP, Request who-has 10.20.1.44 tell 10.20.1.1, length 46
23:13:00.159924 ARP, Reply 10.20.1.44 is-at a0:78:17:a1:0e:1f (oui Unknown), length 28
23:13:00.163493 IP 10.20.1.1.domain > 10.20.1.44.18210: 49937 2/13/16 CNAME youtube-ui.l.google.com., Type65 (549)
5 packets captured
20 packets received by filter
0 packets dropped by kernel
```

Command above is to check all the data packets Coming in & out of the Computer. { -c 5 → only 5 packets }

TCP Protocol (Transmission Control Protocol)

→ It's a Transport layer protocol
→ App layer sends a lot of raw data
→ TCP segments This data → divides in chunks & headers.
→ It may also collect data from network layer

Ex: You have data & transport layer passes to network layer, then network layer may divide into more smaller junks. At the receiving end these smaller chunks will be put into one.

↳ [check Kunal's Video 3:01:04 - 3:05:04]

⇒ Congestion Control

⇒ takes care of 2 things:
- ⇒ when data does not arrive &
- ⇒ maintains the order of data using sequence no.

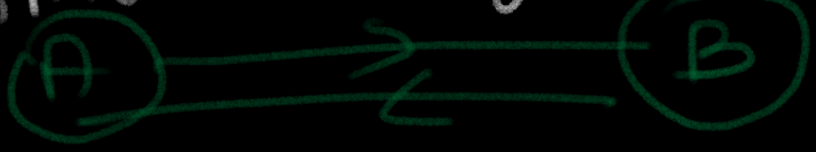
Features:

⇒ Connection Oriented { means 1st connection has to be established then can send data }

⇒ Provides Error Control & Congestion Control

⇒ Full Duplex

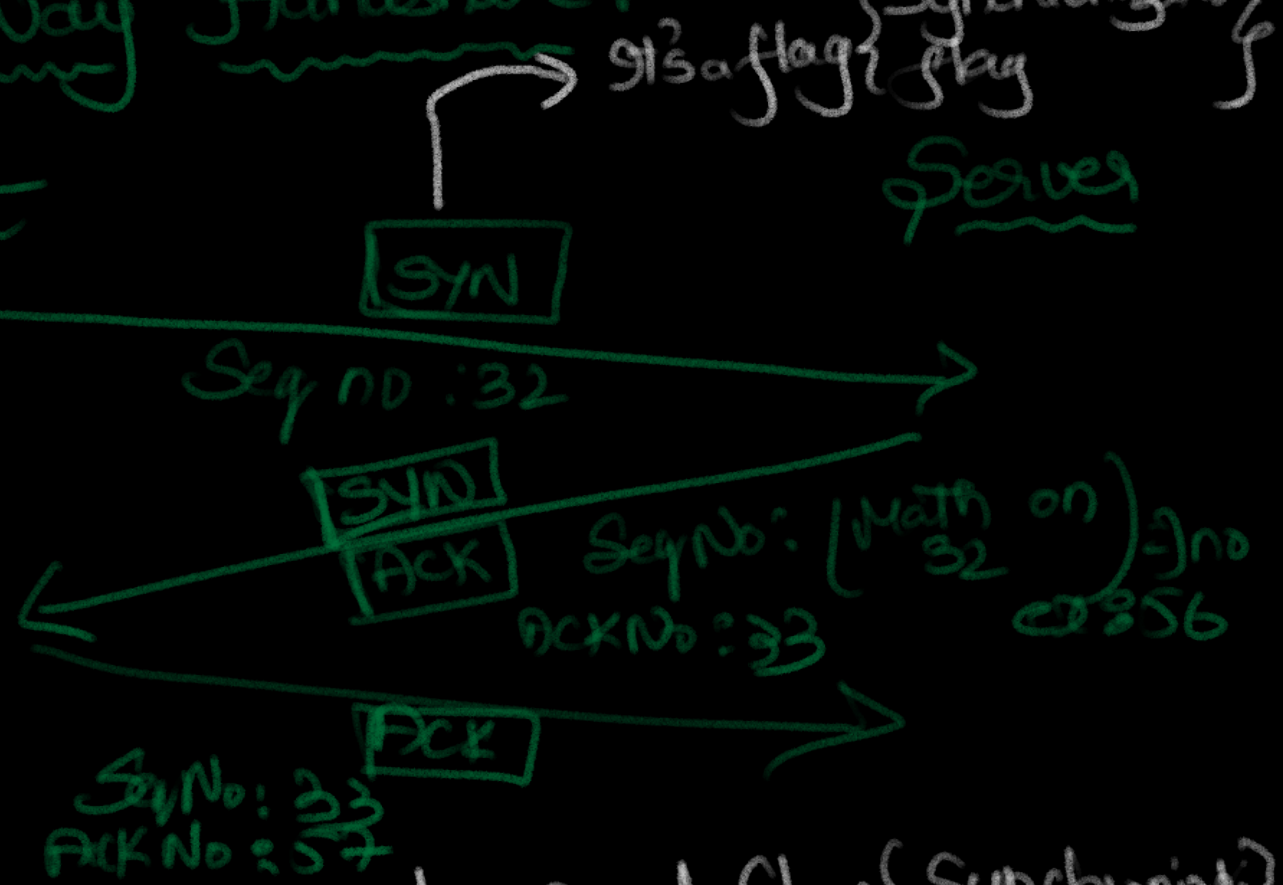
↳ It means 2 Comp connected can send files like Comp A → Comp B, Comp B → Comp A (or) Both can send simultaneously.



Using TCP, you cannot send message to 10 computers.

⇒ When client request the Server, that I want to establish a connection with you then the Server will respond back to you sure I want to. then you will accept & Connection is established this is known as 3 Way handshake

3- Way Handshake:



⇒ You are going to send flag {Synchronization flag} it means new Connection is established

→ Flag is just a value inside a header
→ Along with it Seq no also & next Seq no are random numbers

{ If Seq No aren't random easy to guess & anyone can make connection to server it means prone to Hacking }

→ The server then sends an acknowledgment flag & Sequence no is calculated using the Math on Seq no recieved from client

→ Because it's also starting new connection.

SYN Flag &

→ Then client also sends a ack Flag with Seq no of before adding 1 to it

Acknowledgment No: previous Seq No + 1

→ Network Layer

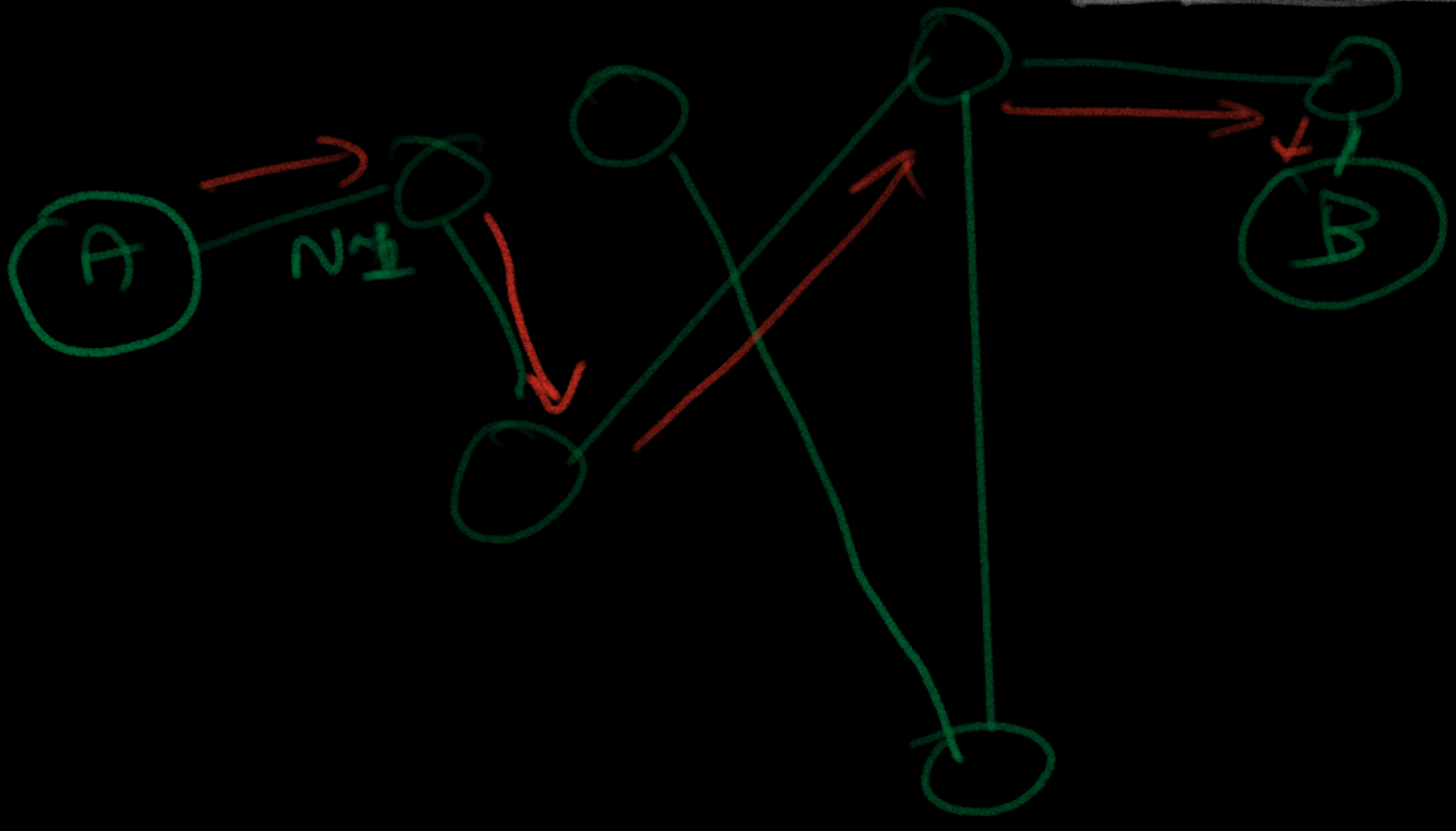
→ We work with Routers in this layer

→

Transport layer → Segments

Network layer - packets

Data link - Frames



→ Routers

→ Every single router has IP's own network address

→ Network address means it allows to send the data packets.

→ for ex: you are sending data packets to N1, then N1 is going to check its Routing table {forwarding Table} that basically consists of every destination address.

→ A packet Contains

- Network layer adds of destination
- " " " " source
- Information {data}

→ When you send a packet, the router will check I have recieved this packet & it should be in this location so let me check my fowading table & check & send it.

⇒ The Above is Known as Hop-by-Hop forwarding. {Hopping routers until it reach the correct router

⇒ 192.168.2.30

192.168.2. → network address / Subnet ID

30 → device address / host ID

In Network layer there is something known as Control Plane.

Control Plane: It's used to build routing tables.

⇒ Think of every router as graph & links b/w the router are edges of the graph.

Routers → nodes

Links → Edges

1. Static Routing

→ Adding addrs manually
→ Time Consuming & not adaptive.

2. Dynamic Routing

→ It evolves when there is a change in network
→ Bellman-Ford, Djisktra's Algos are used in finding to these various network.

IP (Internet Protocol):

→ It's a protocol that resides in network layer.
→ So far we're learning Ip addr version 4.

IPv4 :

↳ 32 Bits, 4 words

↳ what's Ip address we already

it defines a Sever, Client, a node

(or) route

IPv6 → 128 Bits

↳ In future

→ 5 . 6 . 9 . 14 ⇒ 32 Bit

↓ ↓ ↓ ↓

8Bit 8Bit 8Bit 8Bit

↓

00000101

8Bits

↳ Binary

⇒ The hop-by-hop, hopping happens at Internet service providers

⇒ The Routing table doesn't have every address, it has Blocks of Ipaddr these are assigned to ISP called Subnetting.

⇒ So, whenever a router shares to other R it should know it's SubnetID.

⇒ The Internet Society created class for R

Class of Ip addresses:

A	0.0.0.0	—	127.255.255.255
B	128.0.0.0	—	191.11.11.11
C	192.0.0.0	—	223.11.11.11
D	224.0.0.0	—	239.11.11.11
E	240.0.0.0	—	255.255.255.255

Subnet-Masking: It Basically means that subnet mask is going to mask the network part of the Ip address.

ex:

Subnet mask for class 3 ip

255.255.0.0

I can add any numbers here

That means all devices That has Ippadde 255.255 belongs to class 3.

Variable length Subnet:

→ Let's say you have a subnet like below 12.0.0.0/31 It Basically means the first 31 bits are my subnet part.

Ex:- 192.0.1.0/24

Total - 32 Bits

24 - occupied By Subnet remaining 8

Start

192.0.1.0

end

192.0.1.255

} Total 256

=> IETF {Internet Engineering Task Force}
they are the one who assign the Ip address to ISP.

=> They assign Based on region not class to minimise the no of Hops.

⇒ Some of IPv4 are reserved, special addres

Reserved address

⇒ 127.0.0.0 /8

↳ These can be anything only 1st 8 Bits are reserved

ex: localhost : 127.0.0.1

↳ Known as loop Back address

↳ when your device will acts as client & server.

Packets : Header is of 20 Bytes

↳ IpVersion, length, identification, flags, Protocol, Checksum, addresses (TTL), etc

Time To Live (TTL) : When packets are travelling on various routers, it's hopping on & on, sometimes packets may be in a loop & many not reach after so many hop

```
base ~ (8.228s)
ping apple.com

PING apple.com (17.253.144.10): 56 data bytes
64 bytes from 17.253.144.10: icmp_seq=0 ttl=58 time=34.157 ms
64 bytes from 17.253.144.10: icmp_seq=1 ttl=58 time=33.081 ms
64 bytes from 17.253.144.10: icmp_seq=2 ttl=58 time=32.960 ms
64 bytes from 17.253.144.10: icmp_seq=3 ttl=58 time=39.369 ms
64 bytes from 17.253.144.10: icmp_seq=4 ttl=58 time=33.067 ms
64 bytes from 17.253.144.10: icmp_seq=5 ttl=58 time=41.024 ms
64 bytes from 17.253.144.10: icmp_seq=6 ttl=58 time=41.331 ms
64 bytes from 17.253.144.10: icmp_seq=7 ttl=58 time=41.118 ms
64 bytes from 17.253.144.10: icmp_seq=8 ttl=58 time=40.391 ms
^C
--- apple.com ping statistics ---
9 packets transmitted, 9 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 32.960/37.389/41.331/3.695 ms
```

→ It means if after 58 hops it does not reach then the packet will be dropped.

→ Google for more

IPV6

↳ IpV4 : 32bit ⇒ $2^{32} \approx$ 4.3billion Ip addresses

↓

we may run out since usage is growing

IpV6 ip 4 times larger than IpV4

⇒ IpV6 = $2^{32 \times 4} = 2^{128} = 3.4 \times 10^{38}$

↓

unique Ip addresses

Cons: ⇒ not Backward compatible. It means devices that are Configured with IpV4 cannot access website with IpV6.

⇒ ISP's would have to shift, lot of hard coase work.

* 8 numbers & represent 16 Bit hexa-decimal numbers.

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

↓

Hexadecimal

⇒ 32 x 4 = 128 Bits.

⇒ 128/8 = 16 Bit Hexadecimal String.

Ex: ABFE : FOOL : 3210 : 9182 : 0 : 0 : 1 : 3

previous 127.0.0.0/8 → prefix

subnet

→ we can do the same representation here also.

ABFE : FOO1 : 3210 : 9182 : : /60

If all Values are 0000 → 0 is fine

1:0000:0000:0000:9 → 1:0:0:0:9

→ 1::9

2

Btw full of zeros

Middle Boxes

→ Extra devices that interact with Ip packets, most you can find them on network but you can also find them in transport layer.

⇒ They work with packet, You can allow, reject & modify some packets

1. Firewall → types → Global Internet
→ Your trusted Network

⇒ Filter out various Ip packet based on various rules
⇒ Addresses → You can Block specific addres for example
⇒ Modify packets
⇒ port Nos
⇒ Flags
⇒ protocols

Stateless vs Statefull firewall

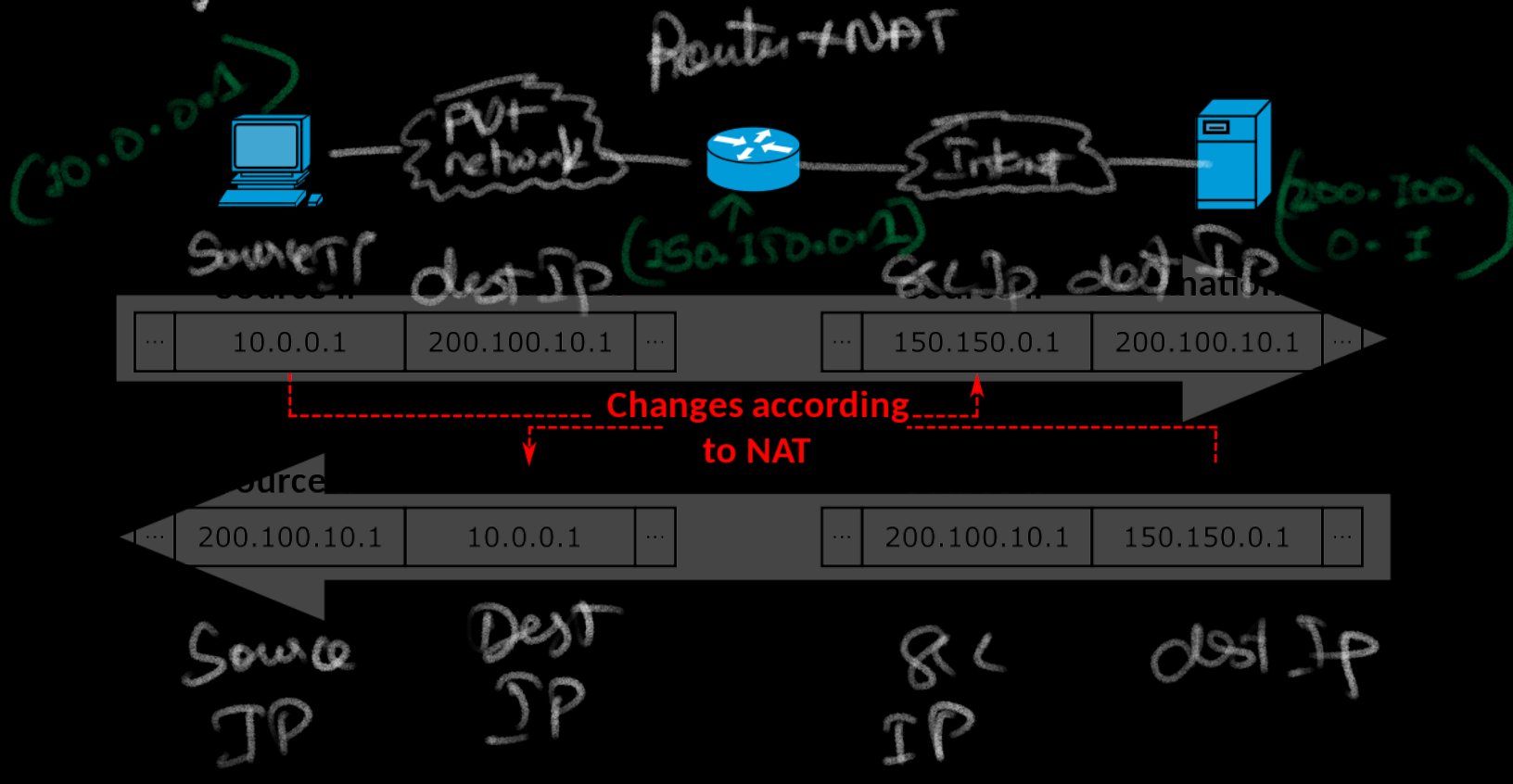
↳ Stateless

↳ It maintains it's state & Store packet in Cache memory
→ more efficient

⇒ It's in the network & transport layer as well

2. Network Address Translation (NAT)

→ Method of mapping Ip add space into another by modifying network addr info in the Ip header of packet.



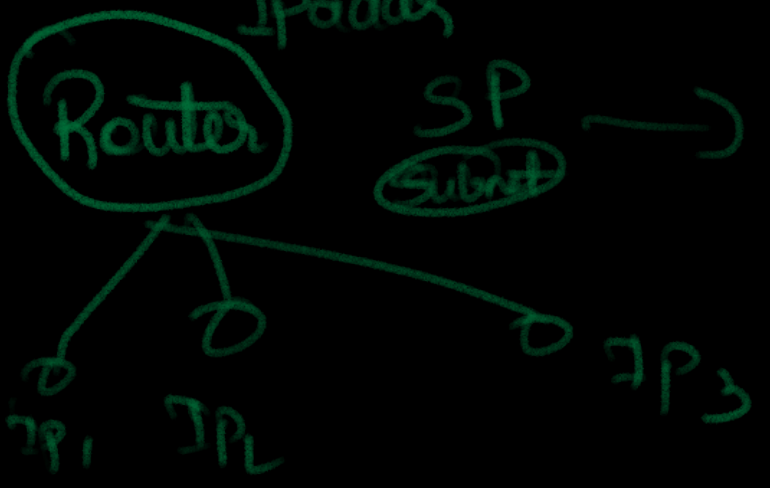
→ NAT will be modifying the addresses To the outside the Ip address of device will look (150.150.0.1)

→ Initially the host Ip was (10.0.0.1) but since NAT modified it's Ip for the internet the Ip is coming from (150.150.0.1). So, Now all the Ip's in your network can work as private Ip.

→ To slow down the Consumption of Ip addresses it's being used.

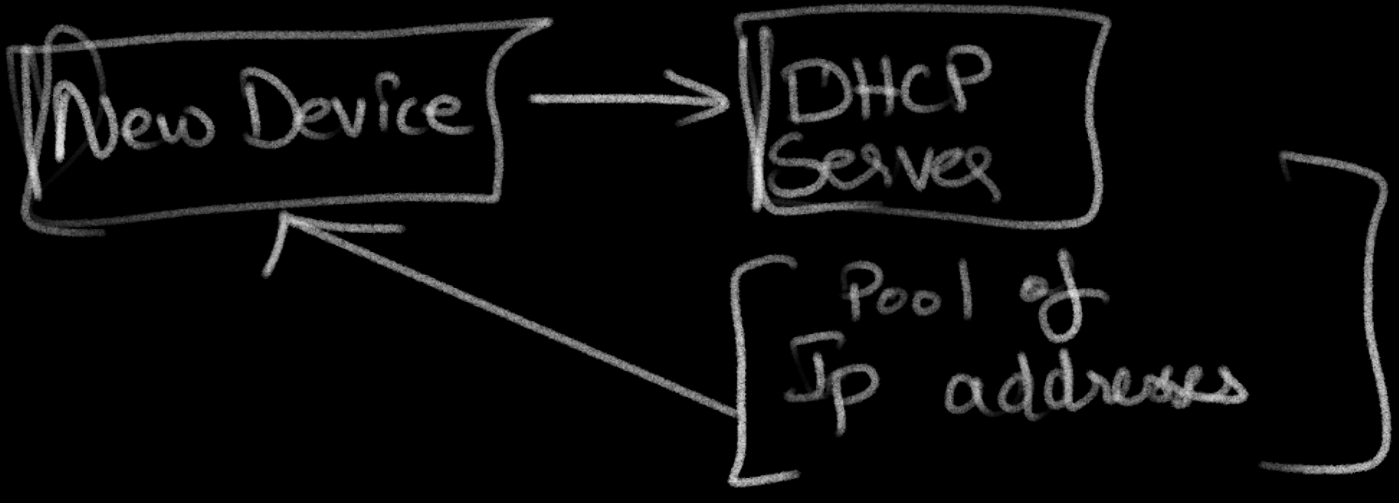
Data Link Layer

→ This layer is responsible to send the packets over a physical link.

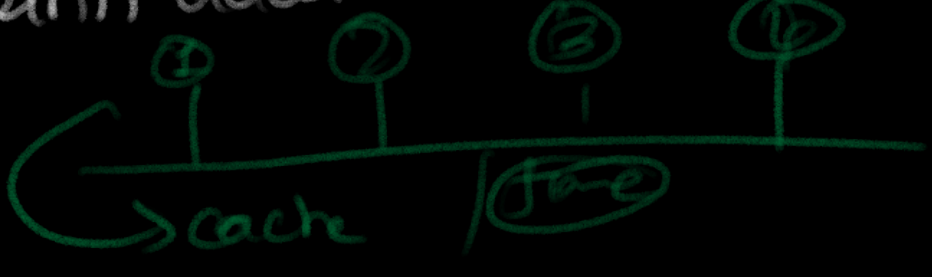


⇒ There is a router & it has an Ip addr that is provided by ISP. Some devices are connected to the router & they each have Ip addresses

⇒ There is going to be a subnet to allocate new Ip addresses. It happens via DHCP (Dynamic host Configuration Protocol)



⇒ many devices connected in LAN:
Every device that has Ip addr have data link addr



→ If device 1 wants to send to device 4, it will check in its own cache does it have data link addr of device 4 when it does not have it is going to ask the devices that are connected its known as ARP Cache

(Address Resolution Protocol)

→ Frame
- DL Addr of Sender
- IP " " dest

→ Data link layer adds it also known as MAC Address.

→ So, MAC adds when you request & when the data comes back to your router, the Router will attach the private IP addr to the data packets ensuring they got to the Computer & device.

→ All Pvt Ip addr Correspond to Local Mac addr only

→ Using MAC addr you can Block access & it's a 12 digit Alphanumeric thing, used by ethernet, wifi, Bluetooth