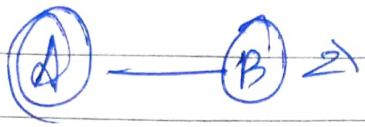
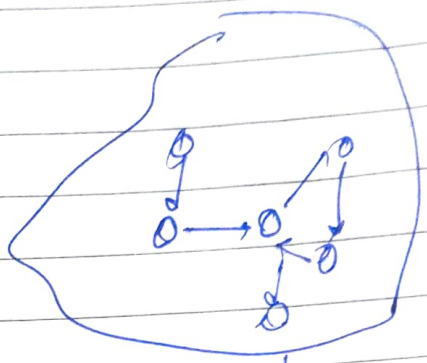
4th Feb

Computer Networking Course

- Computer network → network of computers connected together
- Internet → Collection of computer networks.



Network

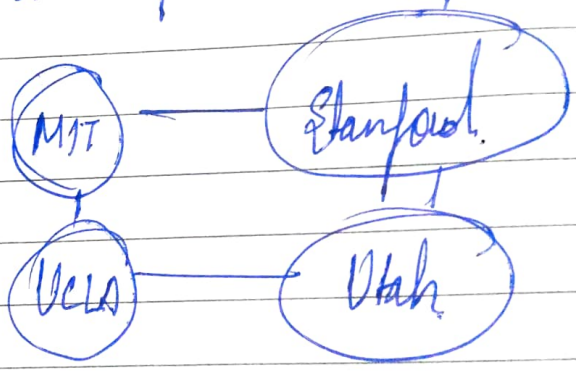


Internet

How did it start?

ARPA. Advanced research projects agency
~~Con~~ made by US as a result of cold war competition

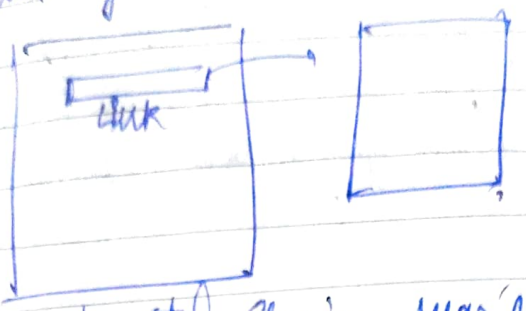
- ARPANET was created.
- They used TCP.
  (Transmission control protocol)



- Rules setup to ~~st~~ transfer securely and efficiently files over the internet is known as protocol.
  - TCP
  - UDP
  - IP.
- This was the first form of internet

classmate
Date
Page

Issue — suppose we want to send some file that references some other file.



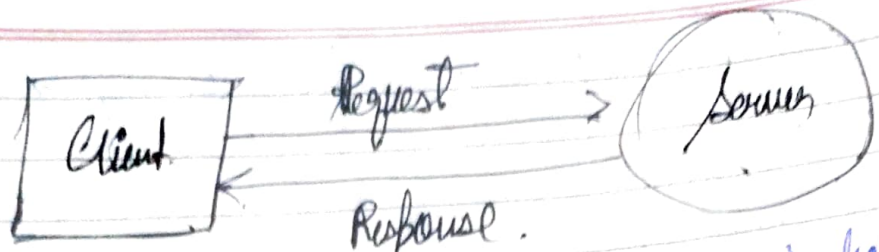
— So this automated sharing was missing.
— came into picture www. (world wide web).
— world's first website — info.cern.ch/hypertext/www/TheProject.html.
— www is a universal collection of all the documents and its allowing us access to them with the help of links.

"It is an information system where documents and other web resources are identified by Uniform Resource Locators (URLs), which may be interlinked by hyperlinks and are accessible over the internet"

— Hyperlinks are relative paths of the URL. When we click a hyperlink they allow us to move to a new location and that location is called a URL.

issue — There's no search engine. So we had to develop search engines. Yahoo was the first one.

— Protocols are decided by 'The Internet Society' internetsociety.org.
— we can also make submissions.



we can see this by typing google.com → inspect → network → Refresh.

- TCP It makes sure that the files are not corrupted while transferring.

UPP When we don't care if 100% of data is transferred eg. video conferencing.

(User Datagram Protocol)

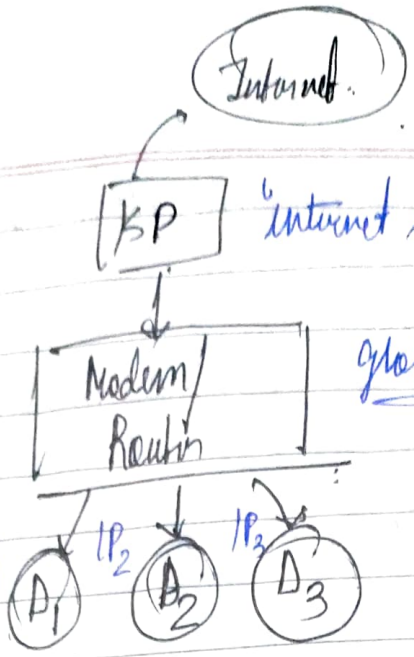
HTTP - HyperText Transfer Protocol
used by web browsers
It defines formats of data transfer.

- Data is always transferred in packets
- All devices that are connected to each other are identified by IP Address. That's how we find the device to send data to.

format → X.X.X.X

Every number can have digits from 0 → 255

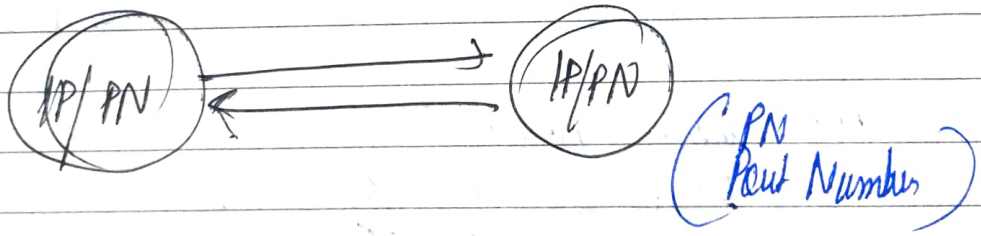
$ curl ifconfig.me → to find your own IP Address.



Modem appoints local IP address to all the devices connected to it. It does so by DHCP (Dynamic Host Configuration Protocol).

When a response is received, the modem decides which was the device that made the request. It does so by NAT (Network Access Translator).

So IP Address decides which ~~data~~ device to send the data, but to decide which application within that device ~~to~~ to send the data, we use ports.



Ports are 16 bits number. We have 16 cells, each cell can have 2 digits → 0 or 1.

Total port no. available → $2^{16} \approx 65000$

- HTTP has port no. 80.
  MongoDB — 27017.

- ports from 0 – 1023 are reserved ports. It can't be used by anyone else

- 1024 – 49152, they are reserved, but they are reserved for applications
  eg. MongoDB
  SQL (P33).

we can use the remaining ports.

- 1Mbps → it means we can transfer 1 Mega bits per second.

- Submarinecablemap.com — how countries are connected to each other via underground sea cables

- So physically computer networks are made up of optical fibre cables, co-axial cables etc.

and wirelessly, we have Bluetooth, wifi, 3G, 4G, LTE, 5G

- LAN Local area networks
  connects small houses (offices. Small in range)
  e Ethernets, wifi

MAN Metropolitan Area Network
in a city

WAN - wide area network
across countries
optical fibre cables.

- bunch of LAN connected via MAN and a bunch of MAN connected via WAN. This collection is the internet

- WAN → SONET Synchronous Optical Network
  it basically carries data via optical fibre cables so it covers a wide area.

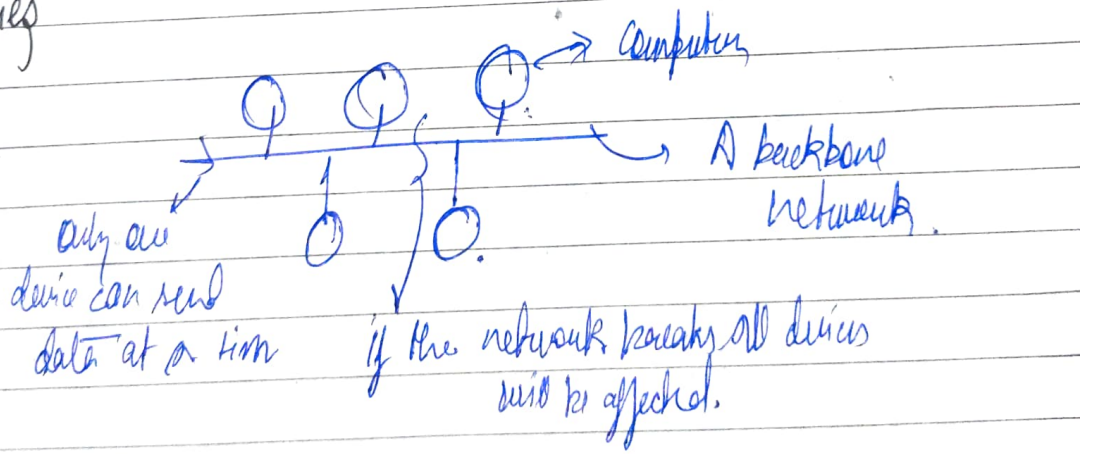
  Frame Relay -- It is a way to connect your LAN to WAN.

- Modem. Converts digital to analog signals & vice versa.
  Router. Routes data packets based on their IP Address.

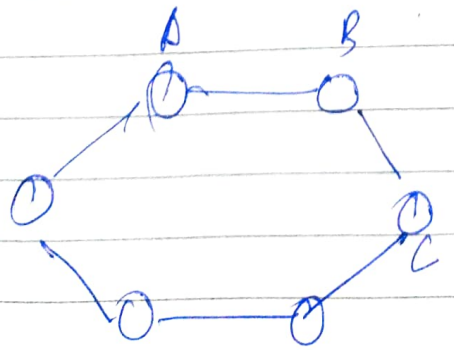
- ISPs are also connected to higher ~~to~~ level of ISP also known as Tier 1 ISPs
  TATA is Tier 1 ISP
  Airtel is Tier 2 ISP.

- Topologies

(1) BUS.



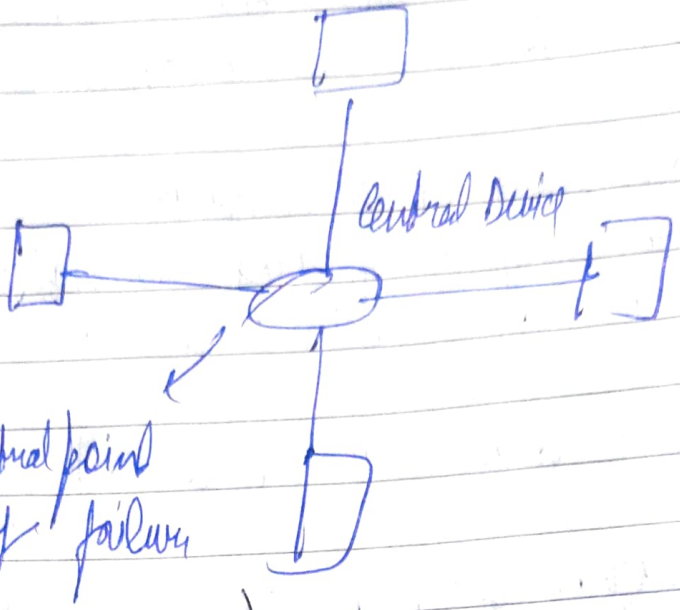
(2) Ring.



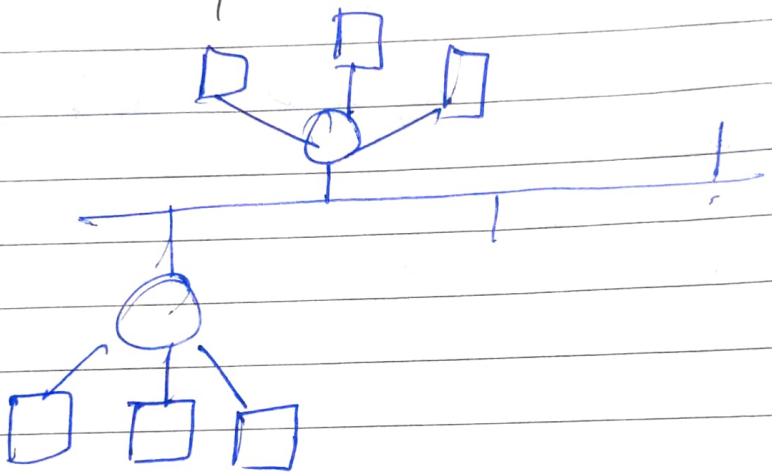
All computers are connected to one another
if we send A to C it'll have to pass through B too.

if one cable breaks, everything will fault

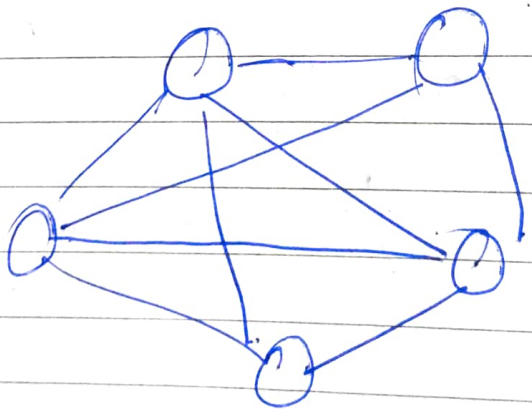
③ Star.



④ Tree. (Bus-star)

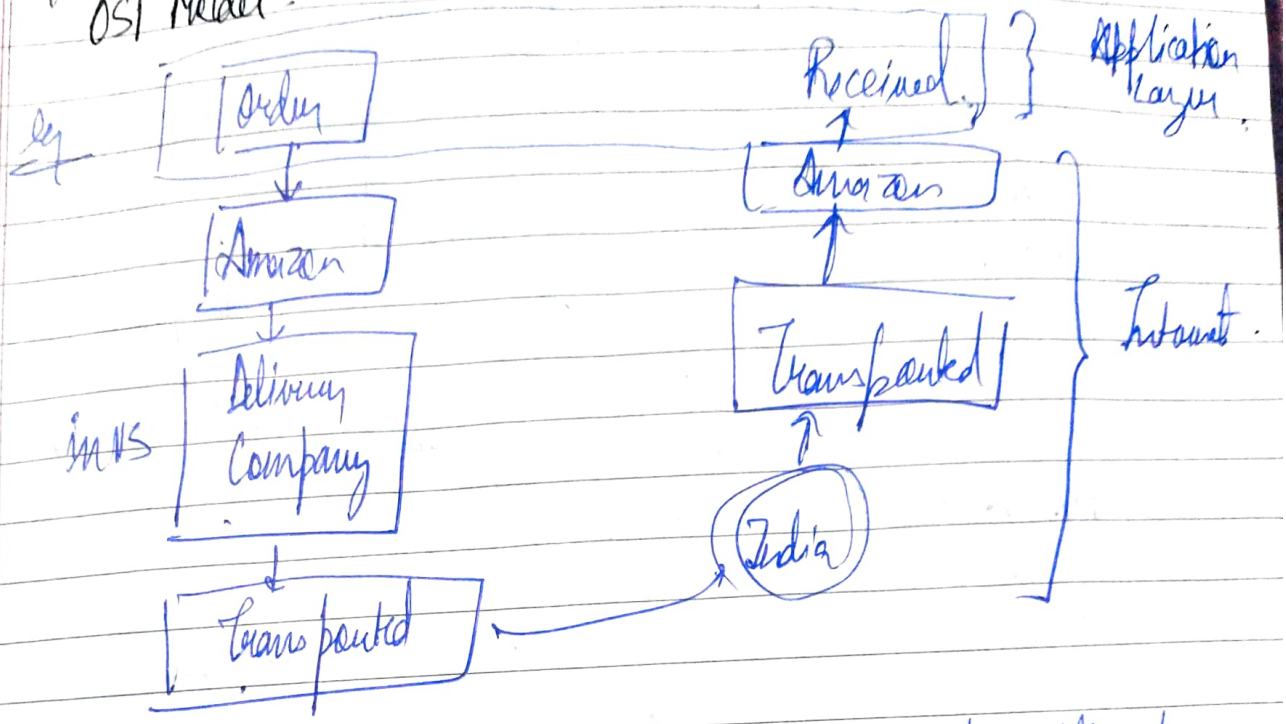


⑤ Mesh.



- Expensive
- Scalability issues

Structure of Network
OSI Model.



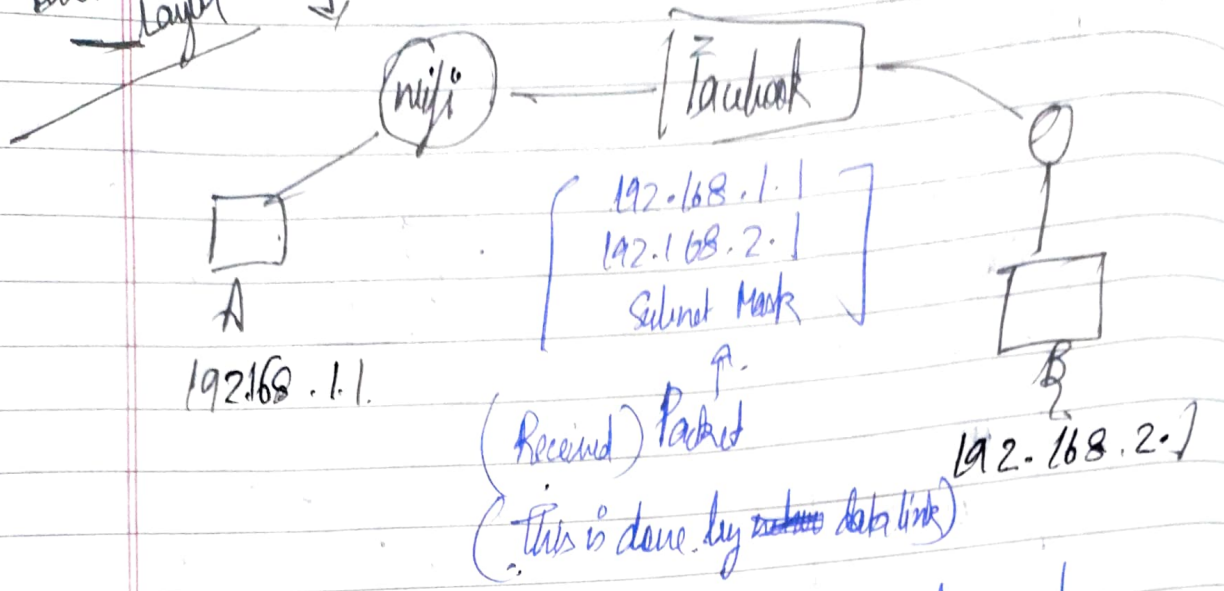
OSI Model → Standard of how devices communicate with each other.

- Application Layer (implemented in software eg. browsers, messaging apps)
- ← Presentation Layer. (Converts / translates data to machine code & / encrypts.)
- Session Layer. (helps in setting up & managing the connections it enables sending/receiving of data then termination of sessions)
- Transport Layer. (segmentation, flow control, error control, checksum)
- Network Layer. (Transmission of segmented data over different devices that are connected over diff. networks)
- Data Link Layer. (allows you to communicate directly with the computer)
- Physical Layer. (Hardware, wiring)

does abstraction
It assumes below layer will take care of it & it does its job

Router.

Data Link Layer



(Received) Packet

(This is done by ~~router~~ data link)

- MAC Address — 12 digit hexadecimal number assigned to each device connected to the network.
(Media Access Control)

- Data Link does the physical addressing (which application to send the data to). These physical addresses are MAC addresses

- MAC address are assigned to the ~~da~~ data packet. to form a frame → data unit of the data link layer.

- your computer's wifi & bluetooth can have different MAC addresses

- Another Model — TCP/IP Model.
developed by ARPA.

Application → Transport → Network → Data Link & Physical

- TCP/IP Model is a practical model while OSI model is a more theoretical way of doing things.

(1) Application Layer

- User Interface
- Whatsapp, Browsers etc.
- located on our devices.
- It has protocols
- Client-Server Architecture.

- Application layer has two parts, client and server, each of which perform their own functions and communicate with each other.

$ ping google.com.
We can see how data is transmitted in packets.

- ping time – it's the time over which data is transferred/received. Round trip time.
  - It can't be reduced as it's the best possible time.

- P2P Architecture (peer to peer) – instead of one dedicated server, all applications are connected to each other.
  - Scalability is easier.
  - decentralised
  - every single computer acts as client/server.
  - Eg. BitTorrent.

Networking devices —

a) Repeater operates at physical layer. Its job is to regenerate the sig 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. ~~Do not~~ They do not amplify the sig. When the signal becomes weak, they copy the signal bit by bit and regenerate it at its original strength. It is a 2 port device.

b) Hub is a multiport repeater. Connects multiple wires coming from different branches. They cannot filter data, so data packets are sent to all the connected devices. In other words collision domain of all hosts connected through Hub remains one. This leads to inefficiencies and wastage.

i) Active Hub. They have their own power supply and can clean, boost and relay the signal along the network. Used to extend max distance b/w nodes.

ii) Passive Hub. They collect wiring from nodes and power supply from active hubs. They relay signals without cleaning/boosting. Can't be used to extend max distance between nodes.

c) Bridge operates at data link layer. Bridge is a repeater, which can filter content by reading content's MAC addresses of source & destination. It is also used for interconnecting two LANs working on the

same protocol. It has a single input & single output, thus it's a 2 port device.

i) Transparent B. Stations are completely unaware of the bridge's existence so reconfiguration of stations is unnecessary.

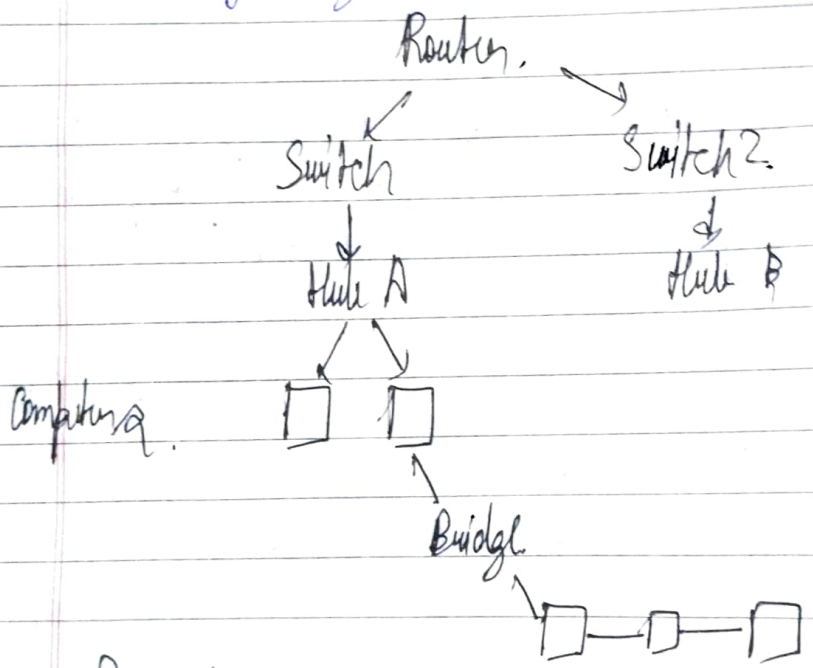
ii) Source Routing B. Routing operation is performed by source station and the frame specifies which route to follow. The host can discover the frame by sending a discovery frame which spreads through the entire network.

d) Switch. It is a multi port bridge with a buffer and a design that can boost its efficiency (large no. of ~~pots~~ ports → less traffic) and performance. Switch is a data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch ~~avoids coll~~ divides collision domain of hosts, but broadcast domain remains same.

e) Routing — It is like a switch that routes data based on their IP addresses. It's a network layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through

f) Gateway is a passage to connect two networks together. They take data from one network, interpret it and transfer it to another system. They are also called protocol converters and can operate at any network layer. Now complex than switch/router.

g) Brouter It is known as a bridging router. Can work at data link layer on network layer. Capable of routing packets across networks (router) and filtering LAN traffic (bridge).



- Protocols

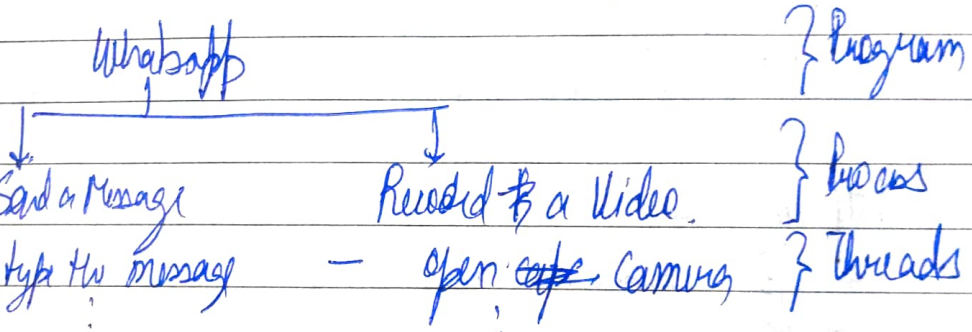
Web Protocols

① TCP/IP
- HTTP
- DHCP
- FTP (files transfer protocol)
- SMTP (Simple Mail Transfer p)

- POP3 & IMAP (for receiving emails)
- SSH (for logging into terminal on someone else's computer)
- VNC (Virtual Network Computing) for graphical control

② Telnet – client/server application protocol that provides access to virtual terminals of remote systems on LAN or the Internet. It has 2 components – protocol and the software application which provides the service.
– Port 23.

③ UDP – Stateless connection, data may be lost.

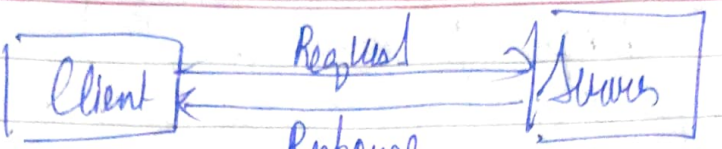


– Sockets – When you need to send messages between devices. Not like client/server, more like software process. Interface between the process & Internet.

– Ephemeral port – Ports identify which application on the device to send data to, ephemeral ports determine which instance of the application to send data to. Eg. different tabs on a web browser.

– HTTP. It is a client server protocol and it tells us how the request is made to the server and it also tells us how the server will send the data back to the client

↗ HTTP Request



↘ HTTP Response.

- it is a application layer protocol. Every application layer protocol needs to have a transport layer protocol.

- HTTP uses TCP (in transport layer)
- stateless protocol. Server will not stores any info about the client

URLs

- http / url / link to the resource (google.com)
  http / url ? argument (yeukuu.com)

http methods

- GET requesting some data
- POST i am the client & i'm giving some data to the server. eg. forms
- PUT puts data at a particular location
- DELETE

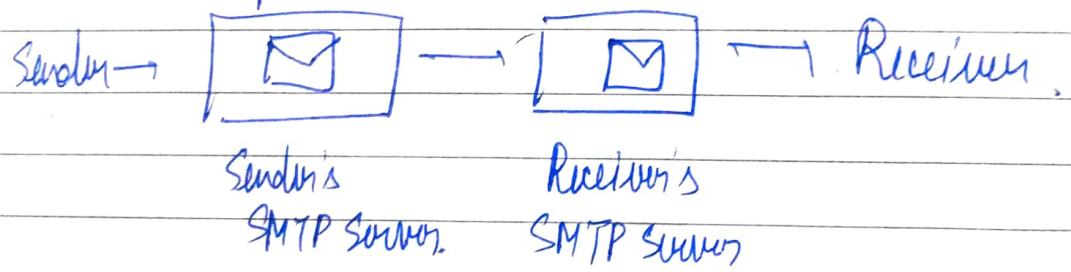
Status / Error Codes —

1XX — Informational codes
2XX — Success codes
3XX — Redirectional codes
4XX — Client Error
5XX — Server Error.

- Cookies – unique string
  - stored in client's browser
  - when you visit a link for the first time, it will setup a cookie and after it whenever we make a new request, this cookie will be sent in the header, the server will check its database's cookie data and it'll know about the client

Third party cookies - It sets up cookies for a url that you didn't visit. Like ads on some website may store your cookie

- Emails in Application layer.
- Use SMTP, Pop3 with TCP

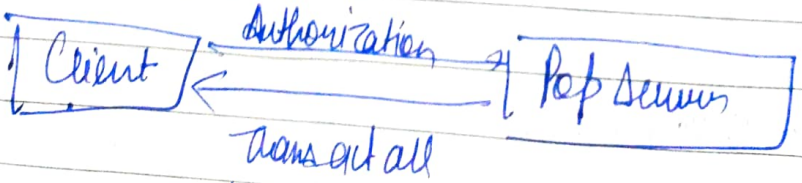


- if SMTP servers are same then data is transferred directly

$ nslookup -type=mx gmail.com.

we can get server and address of an SMTP server.

- POP Post office protocol
  Port 110.

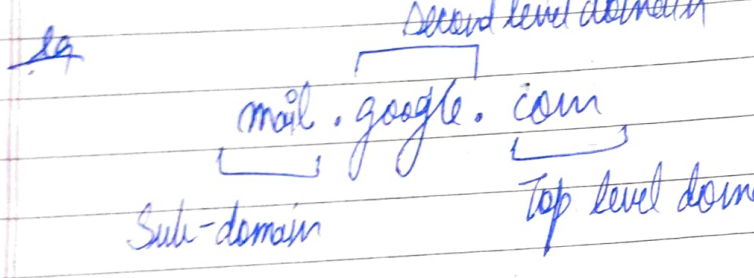


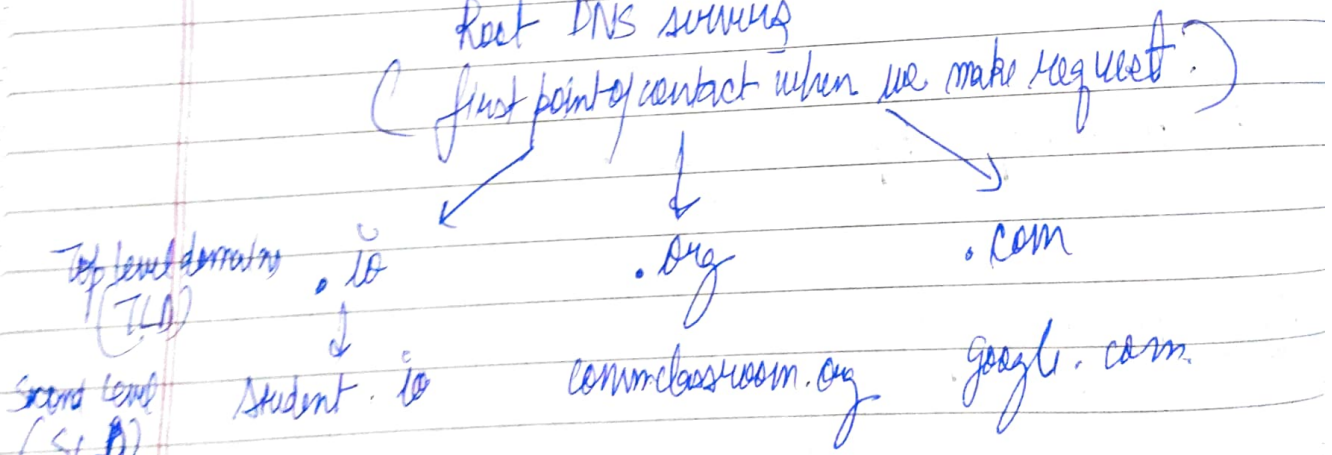
- IMAP (Internet ~~Messaging~~ Message Access Protocol)
  allows to view the emails on various devices

- when we type google.com how does it find the server to link to?

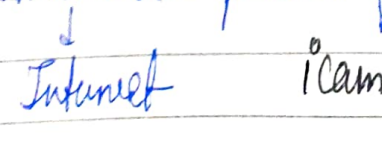
DNS Domain Name System

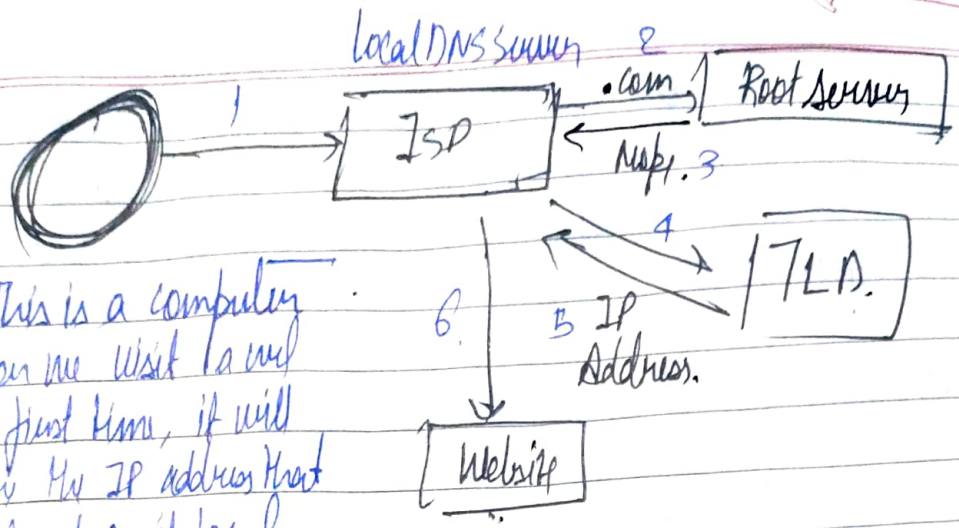
- when we type a url, it uses DNS to find the IP address of that url's server
- It a database service
- These databases are divided into various classes based on domain addresses





- root-servers . org
- TLDs are managed by ICANN (US based)
  (Internet Corporation for assigned Names & Numbers)





This is a computer. When we visit a web for first time, it will store the IP address that is found on its local database / cache.

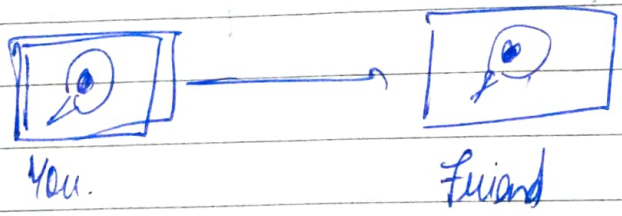
If not found
↳ it'll contact the Local DNS server, if not found, it will check the root server, if not found, it'll check the TLD which will return the ip address and we'll connect to the website.

— we cannot buy a domain name, we can only rent it.

$ dig google.com — we can get info about DNS name servers. It's a DNS lookup utility which queries into our local cache.
$ man dig.

if not working you'll need to install & add it to path.

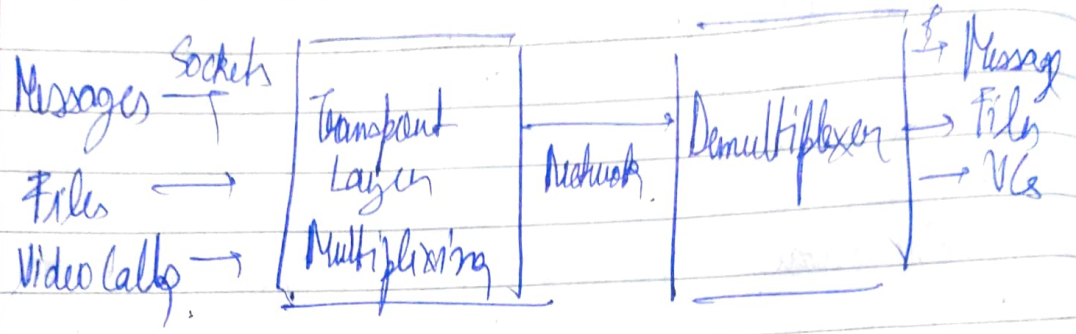
(2) Transport Layer



— Network layer transfers the file from one device to another over the network.

- However once the data is received, which application to send the data to is determined by the transport layer. Therefore, it transfers data b/w the network & application.

- It's also located on client's device.



- We use IP Address to refer to device & port numbers to refer to applications

- These sockets will have port no. ✓.
- ∴ Transport layer attaches these port no. ✓ to data packets & that's how it works internally.

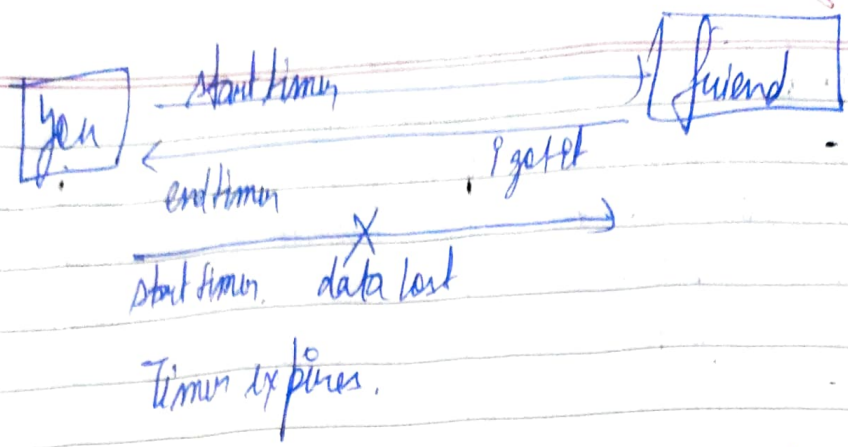
- Transport layer takes care of congestion control.
- Congestion control algorithms are built into TCP.

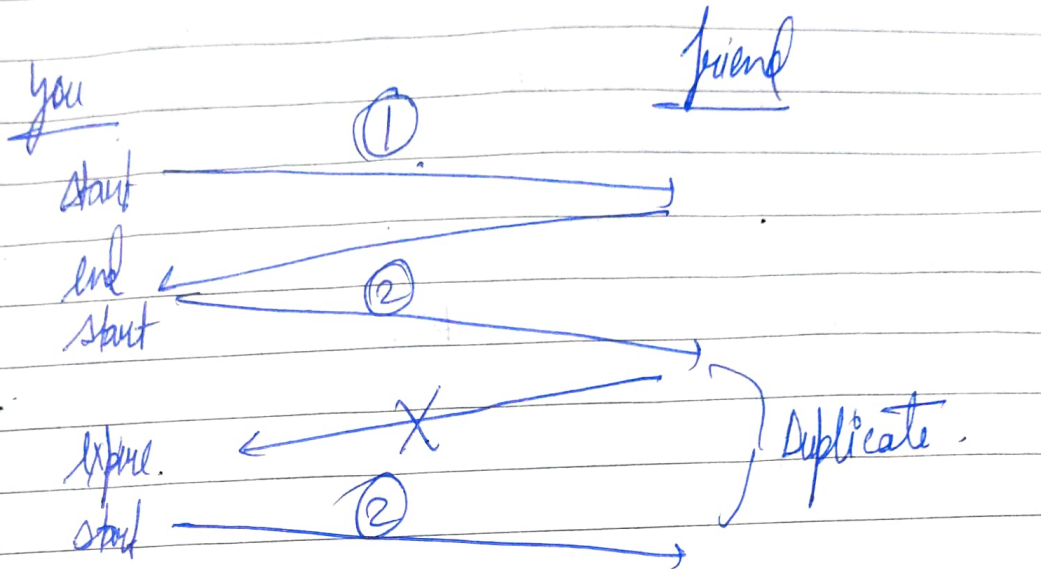
- Checksum

takes care that the data is not corrupted in any way algorithm based

- Timers

tells if the data packets that we sent were lost in the way or not.





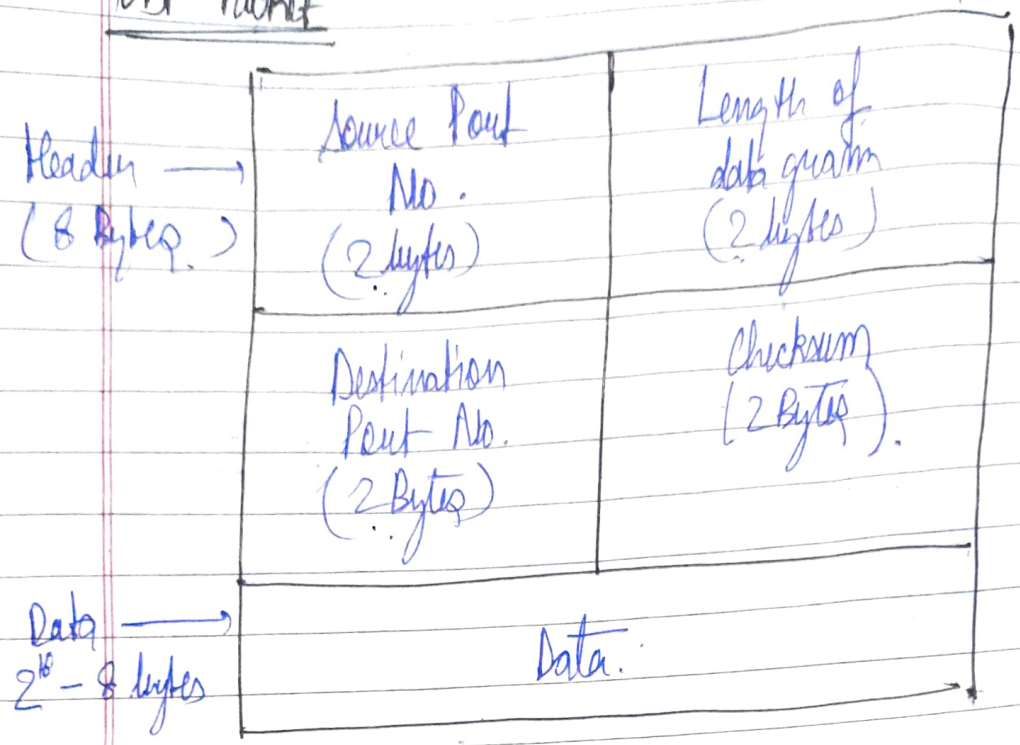
We solve this problem using Sequence Numbers.
No.s which are assigned to every data packet & if a duplicate is received its rejected.

UDP User Datagram Protocol.

- Data may or may not get delivered
- Data may get changed
- Data may get rearranged.
- Connectionless protocol.
- UDP uses checksums. We'll know if the data is corrupted but it won't do anything about it.
- Its fast.
- Video Conferencing Apps
- Gaming
- DNS

} Uses.

UDP Packet



Total = 2^{16} bytes

$ Sudo tcpdum -c 5 — store only 5 packets

we can see UDP packets coming in & out of your computer

TCP (Transmission Control Protocol)

- Application layer sends raw data which is then processed by TCP to create segments of data — divides it into chunks & headers.
- It may also collect the data in network layer as NL may too divide the ~~but~~ data into further chunks.
- Provides congestion Control.

- Takes care of
  - When data doesn't arrive
  - When data is mis-arranged.

- Features - Connection Oriented
  - Error Control
  - Congestion Control
  - Full Duplex :)

A can send file to B, B can send to A
A & B can send simultaneously

Three Way Handshake -

Client → Server

- Connection Request
  - Synchronisation Flag
  - Sequence No. (say 32)

Server → Client

- Connection Accept
  - Acknowledgement Flag
  - No. obtained from doing some maths on seq no. ⇒ eg. 56
  - Synch Flag

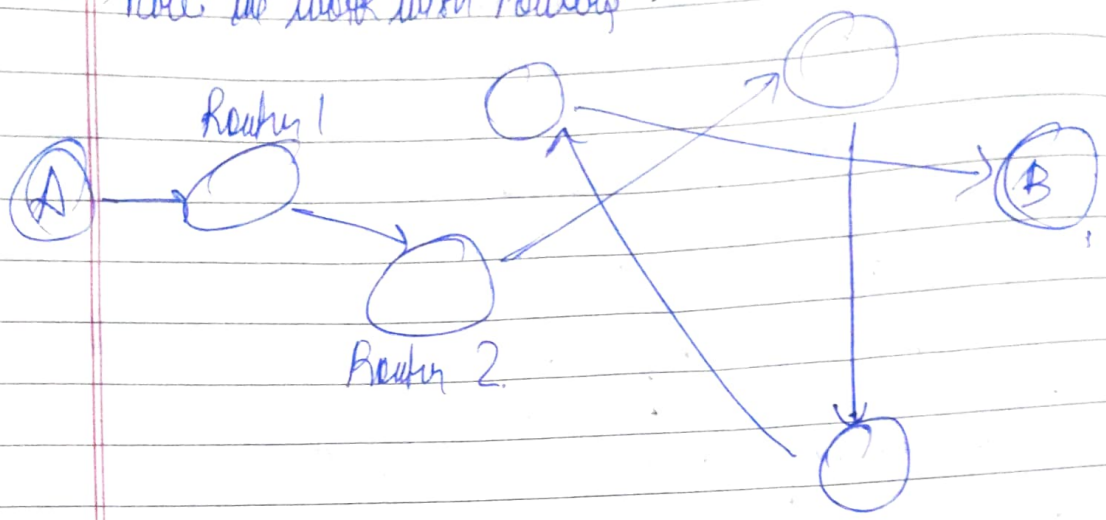
Client → Server

- Acknowledgement flag
  - new seq. no. by doing some maths
    eg. 32+1 = 33
  - Ack No. = prev seq no. + 1
    = 56+1 = 57

TL → Segments
NL → Packets
Data Link → Frames

(3) Network Layer

- Here we work with routers.



- Each router has its own network address and a forwarding table (inside routing table).
- When R1 receives packet from A, it contains Network address of B & A. R1 will check if its Nw data is for him, if not it'll check its forwarding table & send the data to Router 2.
- This is known as hop by hop forwarding.
- 192.168.2.30
  - Network Address
  - Device Address
- Control Plane exists within the NL which creates these routing/forwarding table

- static routing - manually adding routes
- dynamic routing - it'll evolve on its own when there's a change in the network.

IP (Internet Protocol)

- A network layer protocol.

IPv4 - 32 bit no.s with 4 octets
IPv6 - 128 bits no.s.

eg. 5.6.9.14.
8 bits 8 8 8] 32 bits
00000101

Subnetting

- Our router doesn't take part in hop by hop forwarding, it is done by our ISPs.
- Our routers don't count in all the IP addresses it merely contains blocks / chunks of IP.
- eg: 192.168.132.03
  Network A. Device A.
- all the devices within this network will have the same network address. This is known as subnetting.

→ Class of IP Addresses —

A	0.0.0.0	—	127.255.255.255
B	128.0.0.0	—	191.259.255.255
C	192.0.0.0	—	223.255.255.255
D	224.0.0.0	—	239.255.255.255
E	240.0.0.0	—	255.2555.255.255

→ Subnet Masking

Subnet Mask Masks the network address in IP Address & leaves the host/device address for us to use.

→ Variable Length Subnet

You can set your own length of subnet network

eg 12.0.0.0 /31 first 31 bits are part of subnet rest we can use

192.0.1.0/24 first 24 bits are part of subnet rest we can use

→ IETF (Internet Engineering Task Force) assigns IP addresses - they appoint based on regions and not on classes!

Reserved IP Addresses —

→ 127.0.0.0 /8

eg. localhost : 127.0.0.1

→ Known as loopback address

Packets - Header is of 20 bytes.
- IP version
- Length
- Identification
- flags
- protocol
- checksum
- Address
- TTL (Time to Live) etc.
  ↳ It determines the no. of hops after which the packet will be dropped if not delivered.

- IPV6

Comp - Not backward compatible.
IPV4 devices can't connect to IPV6 devices

- IPs would have to shift loads of hardware work.

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

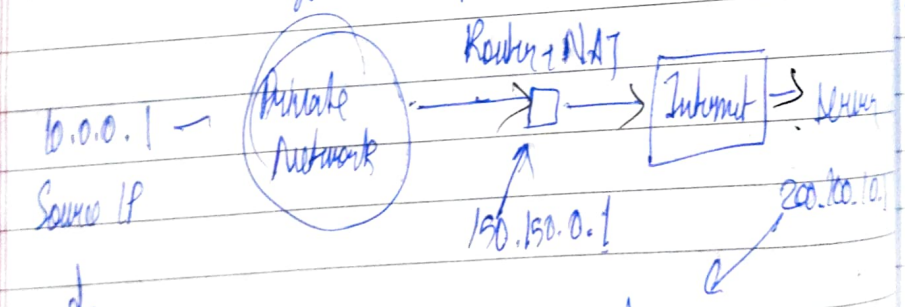
- Middle Boxes - extra devices that also interact with the ~~data packets~~ IP packets. Can be located in transport / network layer.

① Firewall. → two types → connected to global internet
→ to your trusted network

- It filters out IP packets based on various rules & like
  - address
  - Nullify packets
  - Port no. &
  - Flags
  - Protocols.

- Stateless Firewall Vs Stateful Firewall.
  → more efficient.

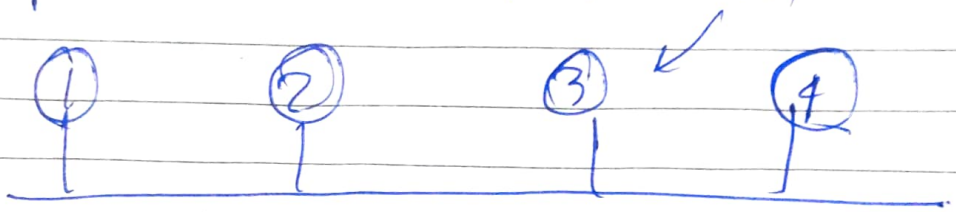
- NAT (Network Address Translation)
  Is a method of mapping an IP address space into another by modifying network address info in the IP header of packets while they are in transit across a traffic routing device.



(4) Data Link Layer.

Data link layer is responsible to send the received data packets over a physical link.

Eg. Multiple devices connected over a LAN network



- suppose (1) wants to send data to (4).
- so it'll check in its local cache if it has the address to 4.
- if not, it'll send request to all the devices over LAN. This request is in the form of frame.
- Frame contains.
  - Data Link Layer Address (DLLA) of the sender.
  - IP address of the destination
- if any device have the DLLA of device 4 it'll send it to it's cache.

This cache is known as ARP Cache

(collection of Address Resolution Protocol entries that are created when an IP address is resolved to a MAC address)

- DLLA is also a MAC Address

(5) Physical Layer.

get admission to electrical and electronics engineering.