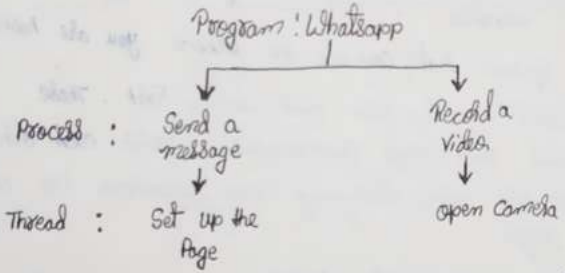
Protocols :—

* TCP/IP
  - HTTP – Hyper text transfer Protocol
  - DHCP – Dynamic Host Control Protocol
  - FTP – File transfer Protocol
  - SMTP – Simple mail transfer Protocol
  - POP3 & IMAC – (used to receive mail)
  - SSH – Secure Shell
  - VNC – Virtual network computing

* Telnet – Terminal immulation 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 or a running instance. One Program can have many Processes running at once.

→ Thread lighter version of Process one Process can have multiple multiple running threads.

Sockets
-> Interface between Process and Internet

Ports
IP address tells us which devices 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 tells 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 ~~REQEST~~ REQUEST, When a Server sends back response to the Client. it is known as HTTP RESPONSE

→ These are application Layer Protocols.

→ HTTP uses TCP

→ 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 : Put data at a specific location.
*DELETE : To delete data from the Server.

Error / Status code :
When you ~~need~~ 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

Computer Networking

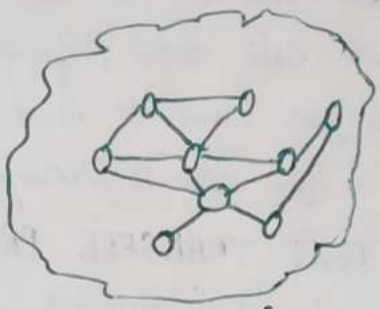
What is computer Network? —

→ In simple terms, it just means computer ~~connect~~ connected together.

Internet

→ A collection of these computer Network

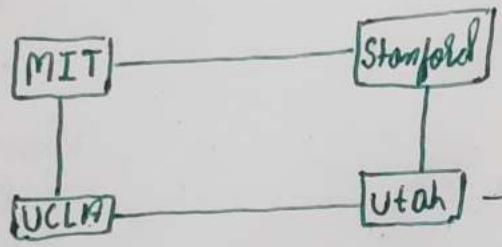
Network



Internet

How ~~did~~ did it start ?

ARPA - Advanced Research Projects Agency (US)



→ They are connected using ARPA net

→ TCP/IP

- Protocol —

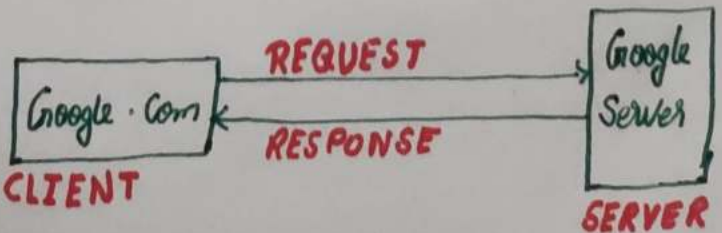
The rules that are set up by People how a Particular data is being send. These are known as Protocols

Eg. UDP, IP, TCP

- 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 accessibles over the internet.

- Internet Society — They are responsible for creating these Protocol.
- Client - Server Architecture —



- Some ~~bd~~ basic Protocols

* TCP → TRANSMISSION CONTROL PROTOCOL
  → It will ensure that the data will reach its destination and 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: Vide Conferencing

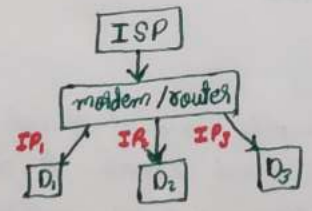
* HTTP → HYPER TEXT TRANSFER PROTOCOL
  → This is being used by web browsers
  → The data that is being transferred between client and servers.

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

- Format of IP Address

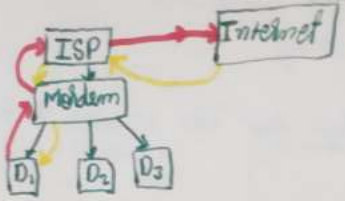
  X . X . X . X
  ↓
  can have value between 0 - 25

- To check the IP address of your computer
  Command :- curl ifconfig.me -S



GLOBAL IP ADDRESS

→ IP1, IP2, IP3 - Local IP Address
→ DHCP - Dynamic Host Configuration Protocol
* modem assign these IP Addresses through DHCP



→ Modem / Router will decide who requested it Does that using NAT (Network Access translator)

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

→ Ports are basically 16 bit numbers.

→ All HTTP stuffs happens at Port 80

65535 Port in Device

→ mongoDB Port - 27017

- 0 - 1023 => Reserved Port
- 1024 - 49152 => Registered for application
- Remaining for use

Speed

1MbPS = 1000000 bits/s
1GbPS = 10^9 bits/s
1KbPS = 1000 bits/s

Submarinecable.com

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

METROPOLITAN AREA NETWORK - Interconnects user with computer resources in a geographic region of the size of a metropolitan area (cities)

WIDE AREA NETWORK - Extends over large geographical area. (countries)

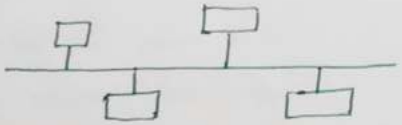
A lot of local area network that are connected to each other using metropolitan area network that are connected to each other using wide area network is a internet.

- SONET – Synchronous optical networking
- Frame relay – A wave for connecting local area network to the wide area network. (like internet)
- Modem –
  → Modulation demodulation
  used to convert digital to analog and vice versa.
- Router
  → A device that forward data packets between computer networks.
- ISP (Internet Service Providers) are companies that provides us access to the internet

  Tier 1 – TATA
  Tier 2 – Airtel, Idea

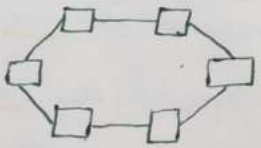
Topologies

1. Bus topologies – They are connected to a single backbone



→ If one part gets broken entire system will fail.
→ Only one person at a time can send information.

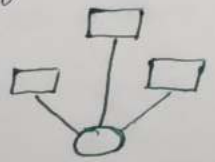
2. Ring topologies –



Every system communication with one another.

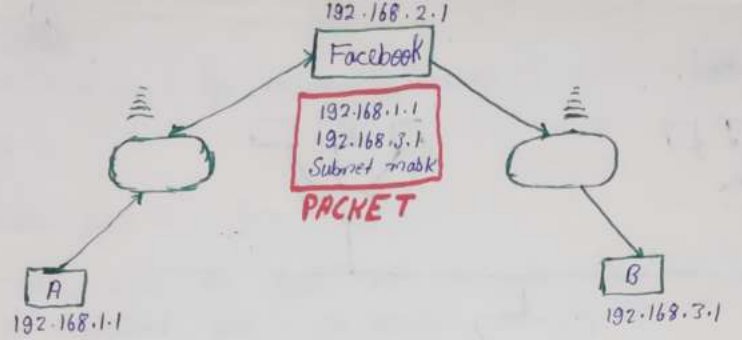
→ If one of the cable break you won't be able to send data
→ lot of unnecessary calls are made.

3. Star topologies –

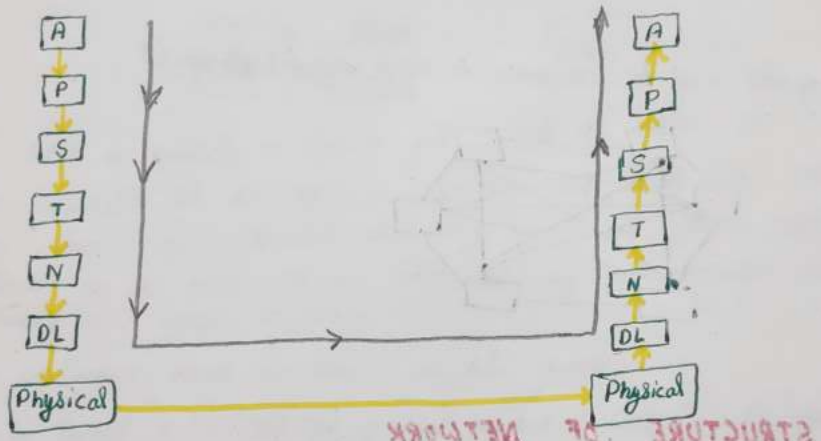


There will be one central device that will be connected to all computers

→ If central device fail then the system will go down



EXECUTION



TCP/IP MODEL

Basically known as INTERNE PROTOCOL SUITE

There are 5 layer

Application Layer

↓

Transport Layer

↓

Network Layer

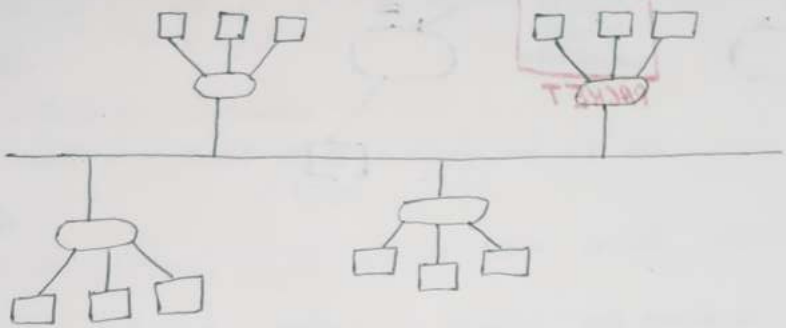
↓

Datal-link Layer

↓

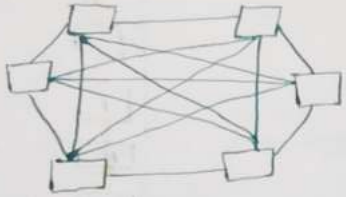
Physical Layer

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 SYSTEM INTERCONNECTION MODEL

There are 7 layer in the OSI Model.

Application Layer	Implemented in Software It is just the application like browsers. Chat app.
Presentation Layer	It converts those messages, data into machine representable binary format Encoding, Encryption happens. Provides Abstraction, Compression, translation
Session Layer	Help in setting up and managing the connections and enables sending and receiving of data followed by termination of connection session. Authentication and Authorization takes Place
Network Layer	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 Packet call frames
Physical Layer	Hardware like Cable, Wire

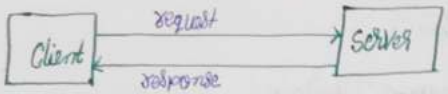
* Mac address
  → It is a 12 digit alphanumeric number of network interface of computer.

Layers :-

Application Layer —

This is the Layer where the users interact with it. It consist of applications like web browsers, chat Application etc It lies on our devices

Client - Server Architecture

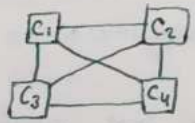


→ A Server is basically a system that controls the website you are hosting
→ The application has two Parts :- Client Part and Server Part. These are known as Processes and they communicate through each other.
→ Clients are the ones who are using/consuming these resources like we making a request to google
→ 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.

Cookies :

→ It is a unique string stored on a client browser

→ When you visit the web page for the first time, the cookies 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.

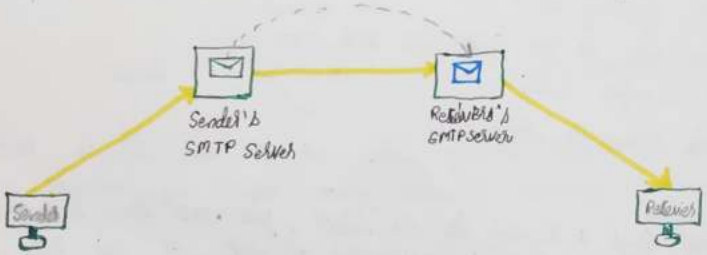
Third Party cookies :

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

How Email works ?

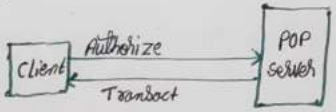
Application Layer Protocol : SMTP (Simple mail transfer Protocol)
POP3

Transport Layer Protocol : TCP



Command ! nslookup - type = mx gmail.com

POP Post office Protocol



IMAP Internet message Access Protocol

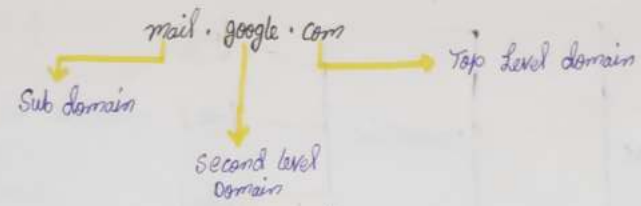
→ Allows to view emails on multiple devices

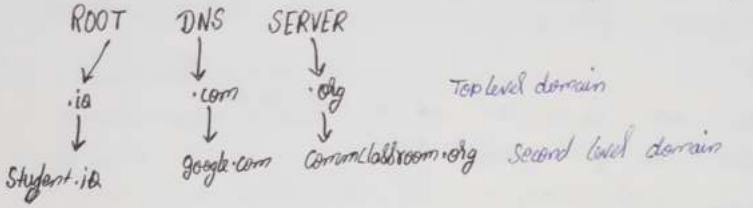
DNS - Domain name System

→ 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 the domain name and use DNS to find the IP address and afterward it connects to that exact server.

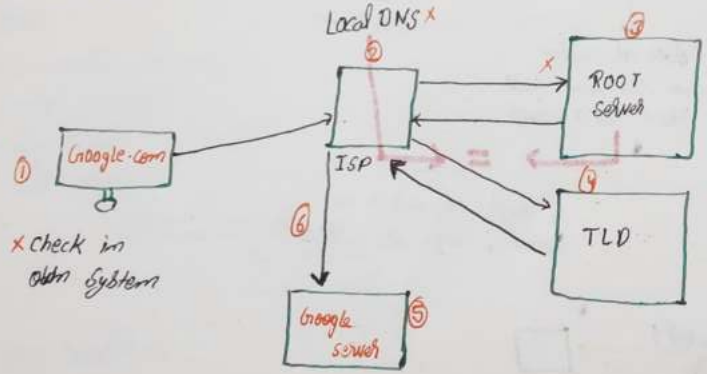
→ It is a directory / database





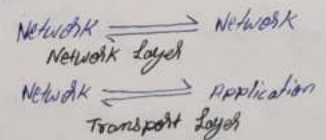
Top Level domain they are like organisation specific for example .com for commercial .edu for education .uk, .in for country specific

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

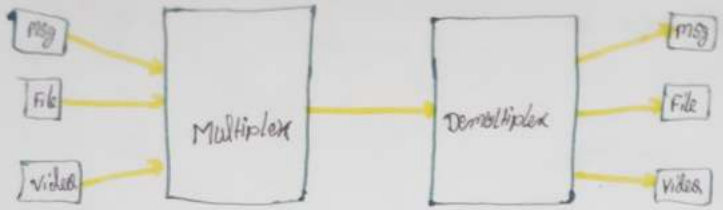


Transport Layer:

→ 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

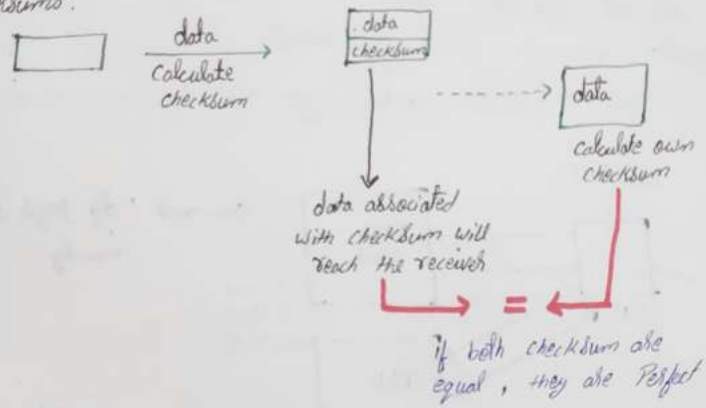


→ Provides Abstraction
→ Located on the devices

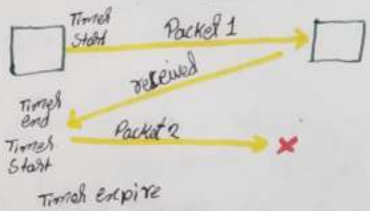


-> Data travels in Packets
-> Transport Layer will attach these Socket Port no to that Packets
-> Transport Layer also takes care of congestion control.
-> Congestion control Algorithms built in TCP

Checksums:

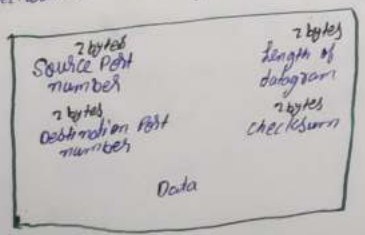


Timer:



Transport Layer Protocol.

UDP: User datagram Protocol
-> Data may or may not delivered, may change, may not in order
-> connectionless Protocol
-> UDP uses checksums and if there is any error it won't care



HEDI
HEADER (8 bytes)
Total Size = $2^{16} - 8$

Use Cases of UDP :

→ Its very fast
→ Video conferencing apps
→ DNS uses UDP
→ Gaming

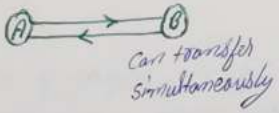
· Command : Sudo tcpdump -c 5 (to see only 5 Packet).

TCP : Transmission Control Protocol.

→ Transport Layer Protocol
→ Application Layer sends lots 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 numbers)

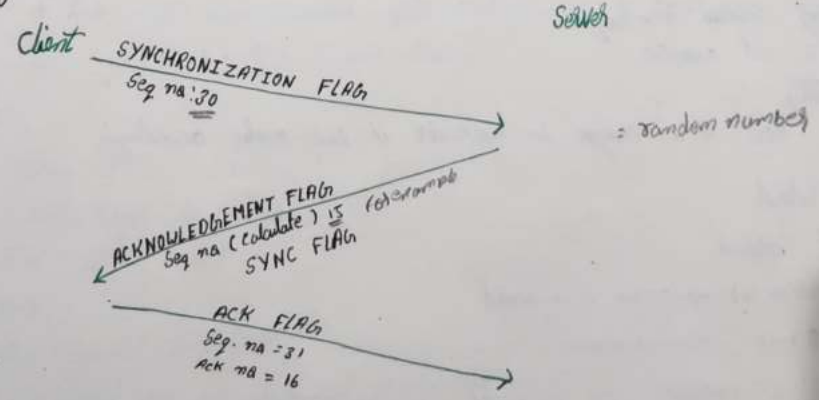
Features :

→ connection oriented
→ error control
→ ~~seg~~ congestion control
→ full duplex



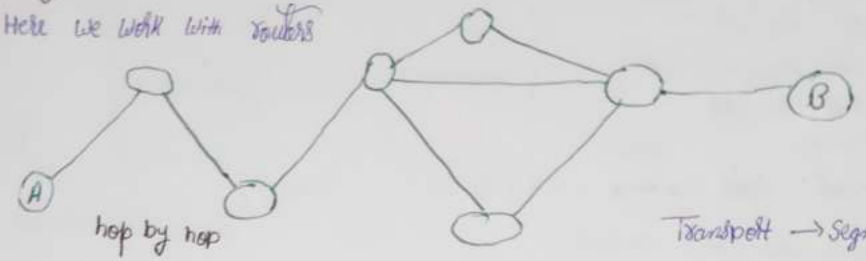
Can transfer simultaneously

3 - way handShake



Network Layer

→ Here we work with routers



Transport → Segment
Network → Packets
Data Link → Frames

* Every routers has a NETWORK ADDRESS
* Every router will check wheather 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

192.168.2 → NETWORK ADDRESS (Subnet id)
30 → DEVICE ADDRESS (host id)

Control Paremel Plane
used to build these routing tables

Router → Nodes
Links → Edges

There are two types of Routing used to create tables

1. Static routing
   → Adding Address manually
   → It's not adaptive
2. Dynamic routing
   → When there is a change in network it will evolve accordingly

Network Layer Protocol
IP Internet Protocal
IPv4 (IP version 4) → 32 bit, 4-word
IPv6 → 128 bits, alphanumerical
→ Blocks of IP addresses are assigned to the ISP. This is known as SUBNETING

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. Local host : 127.0.0.1 (Client also server also)

Loopback address

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 : $2^{32} \simeq 4.3$ billion
→ 4 time Larger than IPV4
→ IPV6 : $2^{32 \times 4} = 2^{128}$

Cons:

* Not Backward Compatible
* ISP's would have to shift. Lot of hardware works

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

1. Firewall
   - → connected to Global ~~network~~ Internet
   - → your local network.

→ It filters out IP Packets based on various rules

- Address
- Modify Packet
- TTL no.
- flags
- Protocols

~~Stall~~

Stateless firewall

→ doesn't maintain a state

Statefull firewall

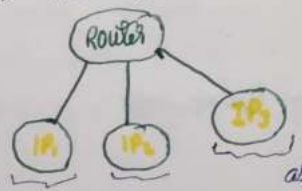
→ See the Packet and maintain its state
→ more efficient

Network address Translation (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 ~~are~~ across a traffic routing device.

Data Link Layer

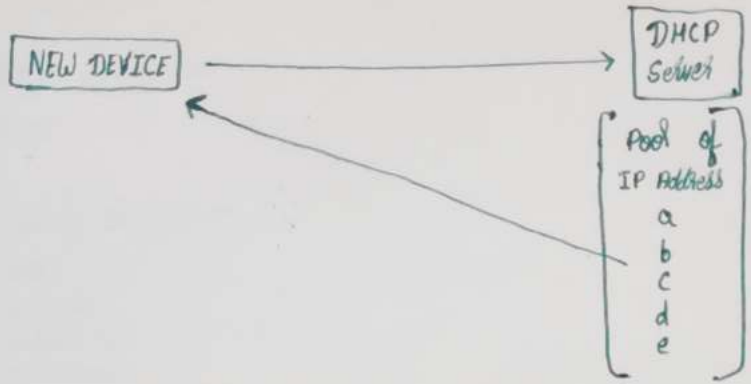
→ The data Packets that we receive from the network layer the data link layer is responsible to send these Packets over a Physical Link.



IP address → ISP
Subnet

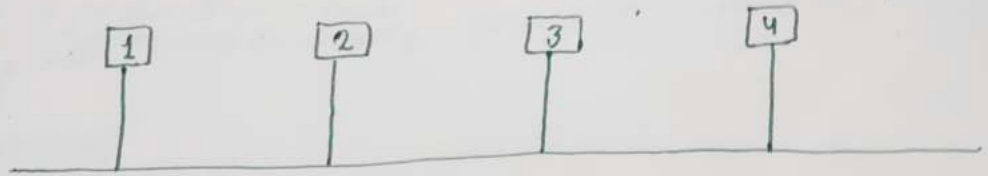
assigned using DHCP

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 ~~see~~ send something to device it, 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

→ IP Address of destination

→

MAC - Media Access Control