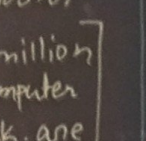
Computer Networking Course

Internet
↓
Collection of many computer networks
[like million of computer network. are interconnected So, we can say it's internet.]

How did it start?
↳ ARPA → Advanced Research Project Agency.
ARPANet → first connected b/w


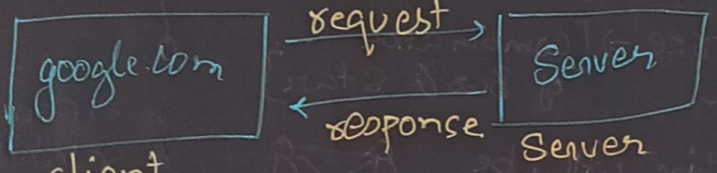
What is protocol?
↳ Set of rules and conventions that define how data is formatted and transmitted in a network or communicat system.

Stanford Research Institute. ⟷ UCLA University of California. Los, Angel
→ funfact → there was no search engine for anything you have to go manually.

Connected with ICP.

↳ Now the issue was they wanted to share research paper?
↓
Solution :- WWW ← By sir tim Berner-lee

Now, let's talk about protocols
↳ need ↳ who set these!
↙
I know
↓
The Internet Society



TCP → Transmission Control Protocol.
UDP → User datagram Protocol
HTTP → Hypertext transfer Protocol.

→ How to check i/p on mac
↳ ipconfig getifaddr en0.

DHCP → Dynamic Host Configuration protocol.

IP → decides who'm to send.
Ports → decides which application to send (game, web etc).
[selection of application]

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

HTTP = 80
mongodB → 27017/ 27018
SQL → 1433

0 - 1023 → reserved Ports.
1024 - 49152 → for applicati

1 mbps → 1000 000 bit's/s
1 gbps → 10^9 bits/s
1 kbps → 1000 bit's/s.

cool website
↳ Submarinecables.com
↓
to see all the connection across the world.

Physically : optical fiber cables., coaxial cables.

Wireless : Bluetooth, wifi, 3G, 4G, LTE, 5G.

☆ LAN → Small house office / Ethernet/wifi
☆ MAN → Across a city
☆ WAN → Across Countries / Optical cable fiber
→ ① SONET
→ ② Frame relay

Internet is collection of LAN + WAN + MAN

☆ Topologies (See the advantages and disadvantages yourself)
① Bus
② Ring
③ Star (central device)
④ tree ⇒ [combination of Bus & Star]
⑤ mesh ⇓ everything will be connected to each other
→ ☆ expensive
☆ scalability issue.

☆ (imp) Structure of the Network [OSI Model] → open system interconnection

↓
7 layers
① → Application → implemented in software
② → Presentation → ASCII to binary. [translation] [encoding] [Abstraction] [compression] [SSL]
③ → session → Connection b/w servers.
④ → transport
⑤ → Network
⑥ → Data link
⑦ → physical.

[I will work in detail later]

① Physical layer → This is the lowest layer and deals with the physical transmission of data over a network medium, such as cables or wireless signal.

② Data Link layer → Responsible for creating a reliable link b/w two directly connected nodes, handling issues like error detection and correction.

③ Network layer → Manages the routing of data packets b/w devices on different network, often using IP addresses.

④ Transport layer → Ensures end-to-end communication, managing data segmentation, flow control, and error checking. Example include TCP and UDP.

⑤ Session layer → Establishes, maintains and terminates connections b/w applications on different devices. It also manages session synchronization.

⑥ Presentation layer → Handles data translation, encryption, and compression, ensuring that data is in a format that both sender and receiver can understand.

⑦ Application layer → The topmost layer that interacts directly with user applications. It provides network services to applications and end-user, like web browsers and email clients.

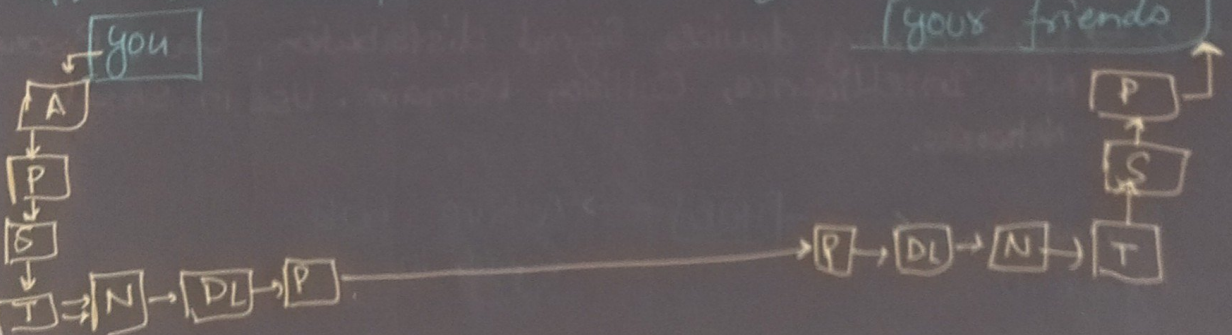
★ What is subnet mask?

→ Separates an IP address into network and host portions.
→ Uses "1s" to represent the network part and "0s" for hosts.
→ Aids in IP address allocation and routing decisions.
→ Is crucial for subnetting and efficient network management.

★ Physical address?

→ A physical address, also known as a MAC (Media Access Control) address:
→ Is a unique hardware identifier assigned to network devices
→ Consists of 12 hexadecimal digits (eg 00:1A:2B:3C:4D:5E)
→ Is embedded in network interface cards (NICs) and used for data link layer communication.

★ let's take example how these layer work



☆ Another mode [TCP/IP model]

↳ Cat in 5 layers!

→ Application layers → This layer remain the same, handling software application and user interaction

→ Physical layer : layer deals with the physical network hardware, including cables, switches, and network interface card.

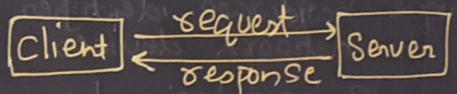
→ Data link layer : Responsible for data framing and transmission over the physical medium. It includes sublayer like LLC (Logical Link Control) and MAC (Media Access Control).

→ Network layer : this layer handles routing and addressing, primarily using the internet Protocol (IP).

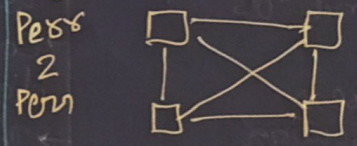
→ Transport layer : Provides end-to-end Communicati and includes protocols like TCP and UDP.

→ Application Layer : This layer encompasses various application-specific protocols and services for tasks like web browsing (HTTP), file transfer (FTP), and email (SMTP).

① client-Server



② P2P [In this case everything is connected to one another



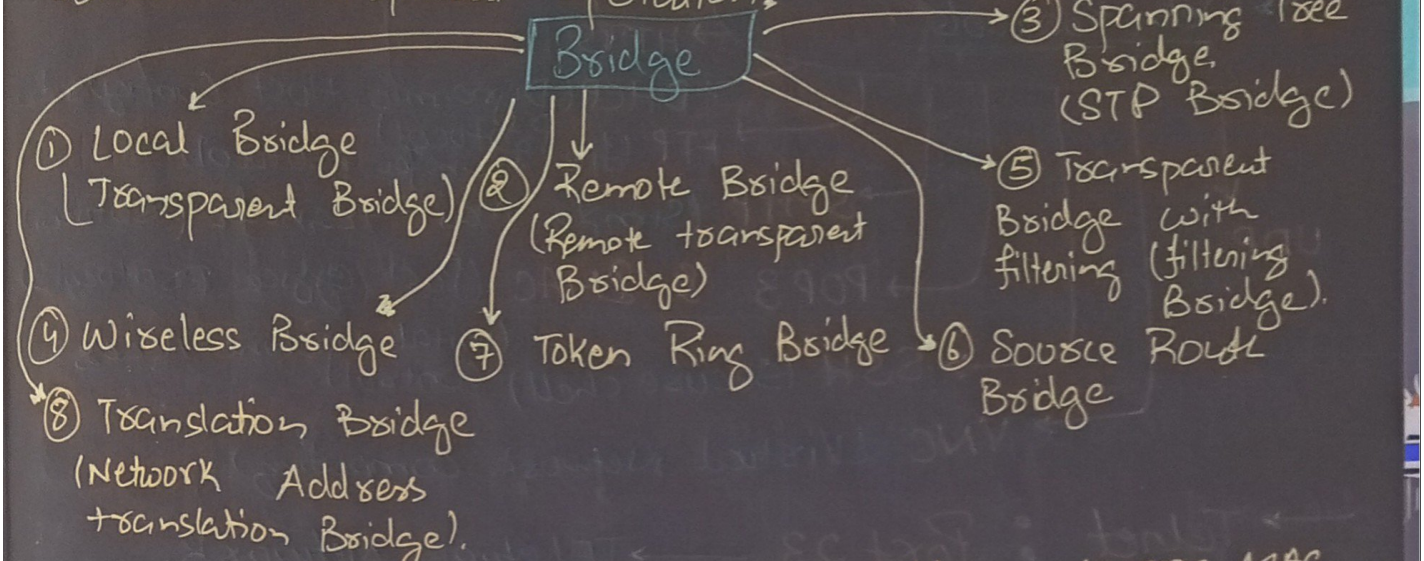
anyone of these can be turned into Client or Server.
eg → torent.

☆ Repeater → Amplifications, Extend Range, Prevents Signal degradation, ~~Common Uses~~, Improves Coverage, Regenerates Signal.

☆ Hub → Networking devices, Signal distribution, Data Broadca NO Intelligence, Collision Domain. Use in small Networks.

Passive hub ← HUB → Active hub
(google it) (google it)

* Bridge → Connect Network segments, filtering traffic, Learning MAC address, Improves Network performance, segragation and Isolation, transparent operation.



* Switch → Device Connection, MAC Address, Learns MAC address, Efficient Data transfer., VLAN. (Virtual LAN), Managed and Unmanaged, QOS and Security, Redundancy, Layer 2 devices, Replace Hubs.

* Router → Network Devices, Interconnects Networks, Routing Decisions, NAT (Network Address translation), firewall capabilities, DHCP Server, traffic management, Wireless Routing, Gateway to the internet, Network segmentation, Protocols, Dynamic Route, static Routing.

* Gateway → Interconnect Networks, protocols translation, Network layer, Internet Access., Security, Bridging different Networks.

* Brouter → Hybrid Devices, Routing capabilities, Bridge capabilities, Flexibility, less Common.

Protocols

→ A protocols is a set of rules and conventions that govern how data is transmitted and received in computer networks or communication systems.

→ Web Protocols
- → TCP/IP
- → HTTPS
- → DHCP (Dynamic Host Configuration Protocol)
- → FTP (file transfer protocol)
- → SMTP (Simple mail transfer protocol)
- → POP3 & IMAC (Post office protocol3) (inital machine Access control)
- → SSH (Secuse shell)
- → VNC (Virtual Network computing).
- UDP

→ Telnet : Port 23 → TELetype Network
- → Network protocol
- → log into remote devices
- → administrative purpose
- → Lacks encryption

thread → Smallest unit of a computer Program's execution allowing for concurrent or Parallel execution of tasks within the same program

Ports : Ephemeral ports dynamically assigned temporary Port no used by client application for outbound network connection to avoid conflict and allow concurrent session.

HTTPS method
- → GET
- → POST
- → PUT
- → DELETE

Status code :-
- 1XX (any 100's) error → imnformational
- 2XX → Success
- 3XX → redirecting
- 4XX → client side error
- 5XX → Server side error.

Socket → endpoint for Sending or receving data across a computer network, often associated with a specified IP address and Port number

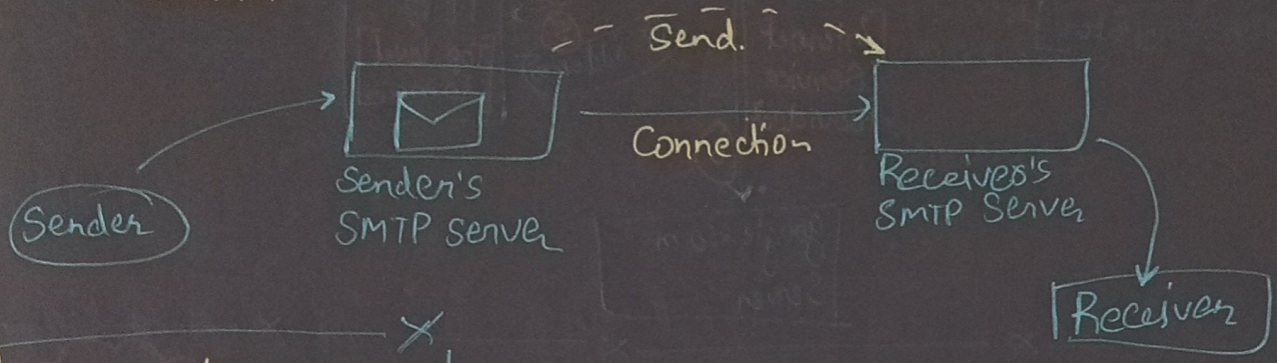
Third party cookies :
- → tracking files used by websites to collect data from users for advertising and analytics, often without their direct consent.

cookies : Small piece of data Stored on a user's devices to enhance website functionality and remember user preferences

How email work?

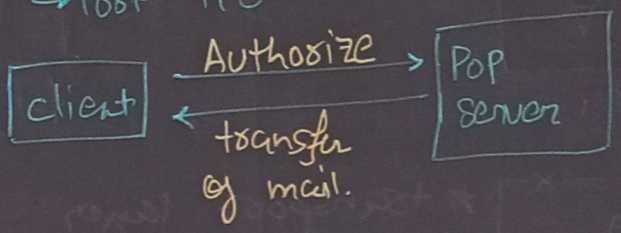
SMTP (Sender)

POP3 (Receive)



fun thing: if both are using same (gmail.com) this connection will not take place it will be sent directly

* POP (Post office protocol)
  ↳ Port 110.



here only data can be downloaded and deleted

* IMAP
  ↳ internet Message Access protocol → is an email protocol that allow users to access and manages their email message stored on a remote email server.

You can see your data on one device only

* DNS:

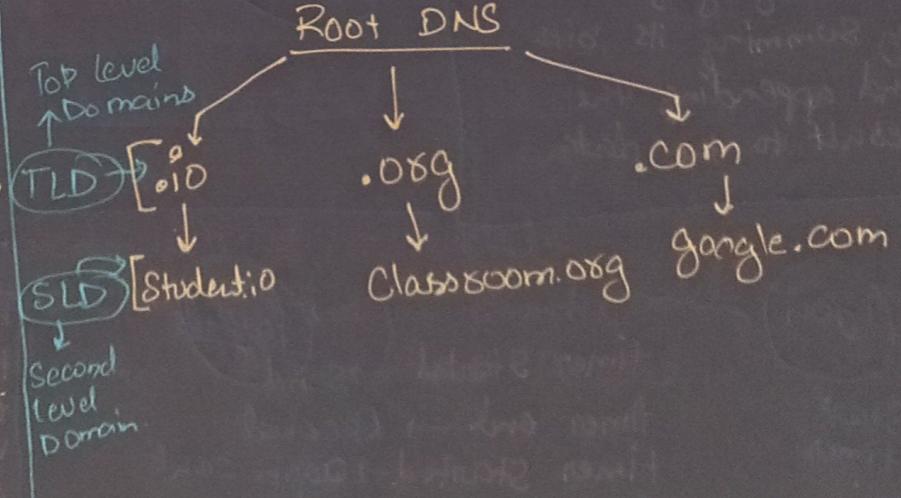
[Domain Name System: mail. google. com

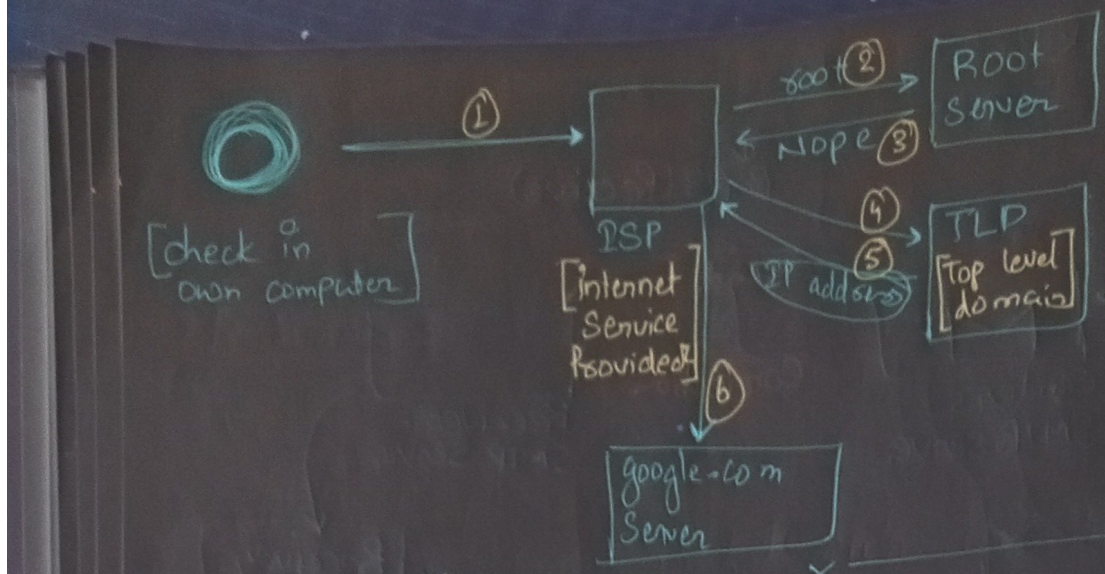
second level domain

TOP level domain

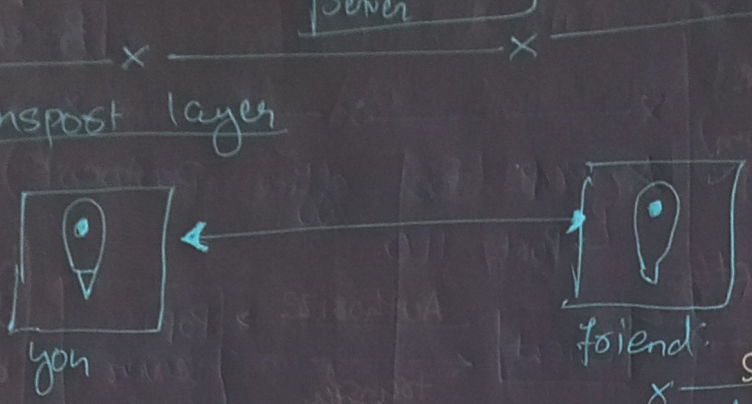
Sub-domain

* Root DNS Server
  ↳ Root DNS server is a critical part of the internet's domain name system, serving as the initial point of contact for resolving domain names into IP addresses.





② Transport layer

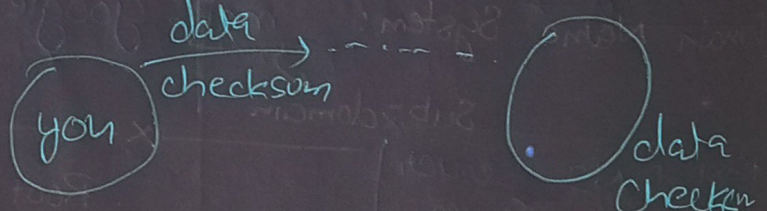


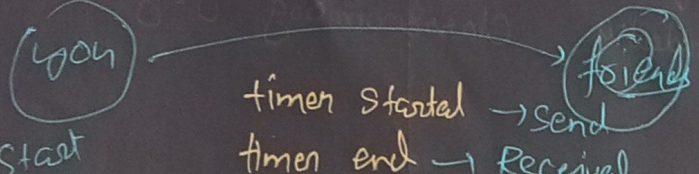
multiplexing
↳ multiple data streams into one for transmission

* transport layer also takes care of congestion control (traffic control).
* Congestion control Algo built in TCP.

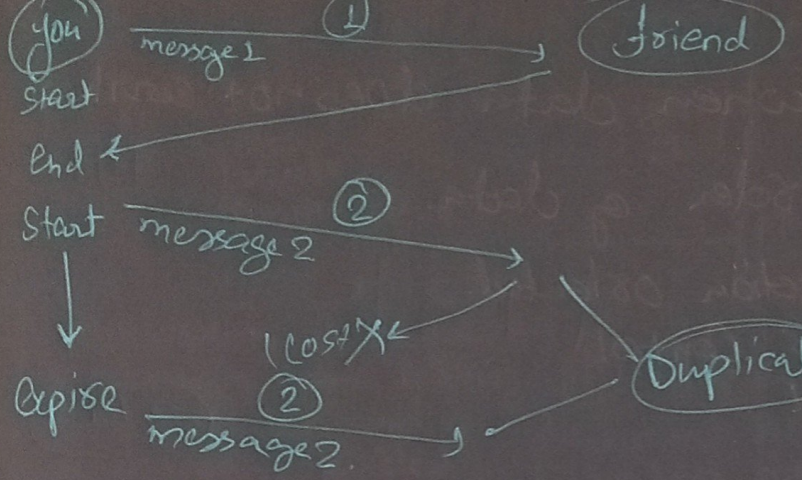
demultiplexing
↳ Separates them back into individual stream upon reception in data communication.

Checksums
↳ a simple error-checking technique used to verify the integrity of data by summing its bits and appending the result to the data.





Timers: Software or hardware mechanisms used to measure and control time intervals for various purpose in computing and electronics.



Solve this problem using sequence nos.

Sequence :-

UDP → User Datagram Protocol (Connectionless)

- Data may or may not be delivered
- Data may change
- Data ~~may~~ may not be in order.

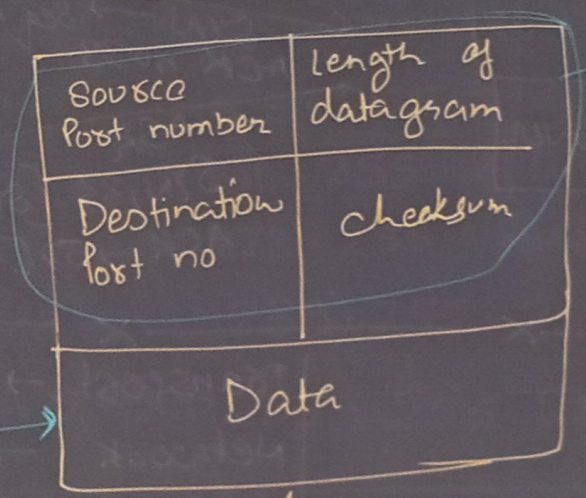
* UDP uses checksum.

* UDP

Total Size $= 2^{16}$

$\Rightarrow 2^{16} - 8$

$\Rightarrow$ 65,536 (approx)



UDP benifit → it's very fast
→ video conferencing application
→ DNS - UDP (cause it's fast)
→ Gaming.

TCP → Transmission Control protocol

* transport layer protocol
* Application layer sends lots of raw data.
  → TCP Segements this data → divide in chunks, add headers.
* It may also called the data network layers.

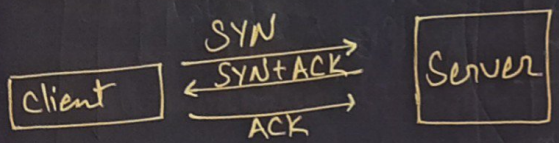
* Congestion Control.
* takes care of → when data does not survive
  ↳ maintain the order of data.

→ features : → Connection oriented.
→ Error Control
→ Congestion Control
→ full Duplex

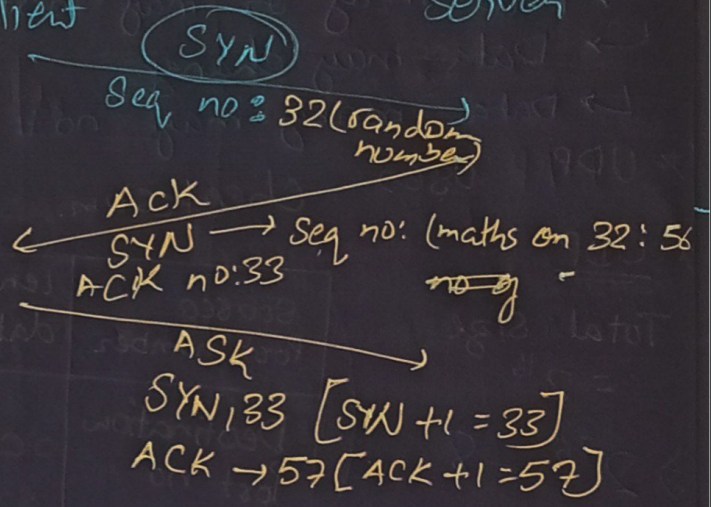
* TCP can be worked only in two computers.
  1 TCP connection b/w two computers.

3-way handshake

↳ fundamental process in establishing a TCP connection b/w two devices, involving three steps : SYN, SYN-ACK, and ACK, to ensure reliable data transmission.



3- way handshake



Network Layers

↳ Here we work with routers :

Transport	→ segments
Network	→ packets
Data link	→ frames.

---

hop-by-hop → networking refers to the process of data being forwarded from one network node to the next in a step-by-step fashion, with each node making individual routing decisions.

192.168.2.30 → example of IP

network address | Also require Subnet ID. | ↳ device address | Host ID.

Control plane

Router → Nodes

Links → Edges

① Static Routing
☆ Manually

② Dynamic Routing
↳ What Algo used for this.
→ best path for data to travel within a network.
→ Dijkstra's algo, Bellman-Ford algo. OSPF's SPF algo

~~Clone~~ Control plane:
→ networking is responsible for managing and setting up the routes and protocols that guided data traffic in the network.

Internet Protocol (IP):

→ eg → 5.6.9.14 → 8 bit + 8 bit + 8 bit + 8 bit = 32 bit (8 bit)

IPv4 → 32 bit, 4 words (we are using)

IPV6 → 128 bits,

Class of IP address: → this is mainly given by internet service provider on first come first serve basis.

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
↳ technique used in networking to divide an IP address into network and host portions by applying a subnet mask, which is a binary pattern that designates which bits represents the network and host portions.

Variable length Subnet
↳ Variable length subnet masking (VLSM) is a technique in IP addressing where different subnet within a network can have different subnet mask lengths, allowing for efficient use of IP address space by allocating more addresses to large subnets and fewer addresses to smaller subnet as needed.

IETF → Internet Engineering task force

↓

they work on region so you can minimize the hoping.

↓

open international community of network designers, operators and researchers

Reserved Addresses:

↳ typically refers to specific IP addresses within a subnet that are not assigned to devices but serves special purpose.

Example → network address, broadcast address.

Additionally, certain IP address are reserved for private network, multicast, loopback and other specialized functions.

loopback address

↳ A loopback address (eg 127.0.0.1 in IPV4) allows a device to communicate with itself for testing and diagnostics.

Packets:

- Header is of 20 bytes
- IP version
- Total length
- Identification number
- TTL (Time to live) →
- Flags
- Protocols
- Checksum.
- Addresses.

IPV

→ IPV4 : $2^{32} \approx 4.3$ billion (approx)

→ IPV6 : $2^{32 \times 4} = 2^{128} = 3.4 \times 10^{38}$

↳ Example :

Cons of IPV6

Pros of IPV6

middle boxes :

def → network devices that sit in the middle of data traffic to perform various function like security, optimization and monitoring.

middleboxes

① firewall → global internet
→ your trusted network.

→ filter out IP packets based on various rules.
- → Address
- → multiplying packets
- → port nos
- → flags
- → Protocols.

Stateless vs stateful firewalls

→ Examines individual Packets	tracks the state of connection
→ static criteria	Consider the state of connection
→ don't track connection	⇒ keep track
→ faster for simple rule sets	slower for complex ruleset
→ less secure against certain attack	often better protection.

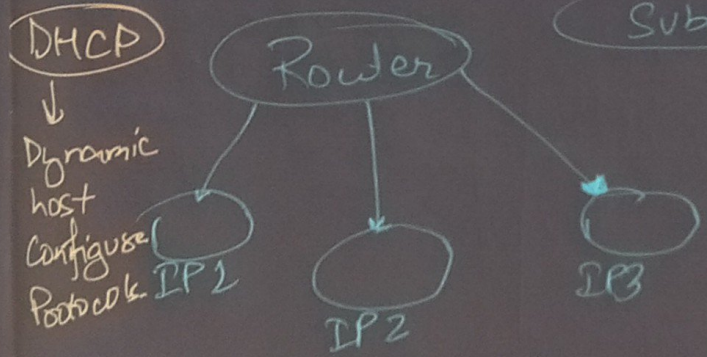
NAT (Network address translation).

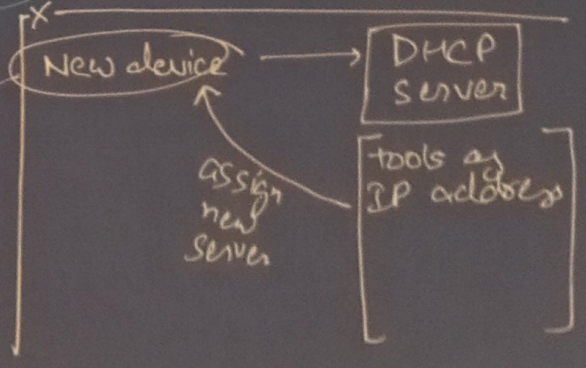
→ NAT conserve IP address and enhances security but can complicate peer-to-peer connections and limit certain applications.

Data link layer

IP address → ISP

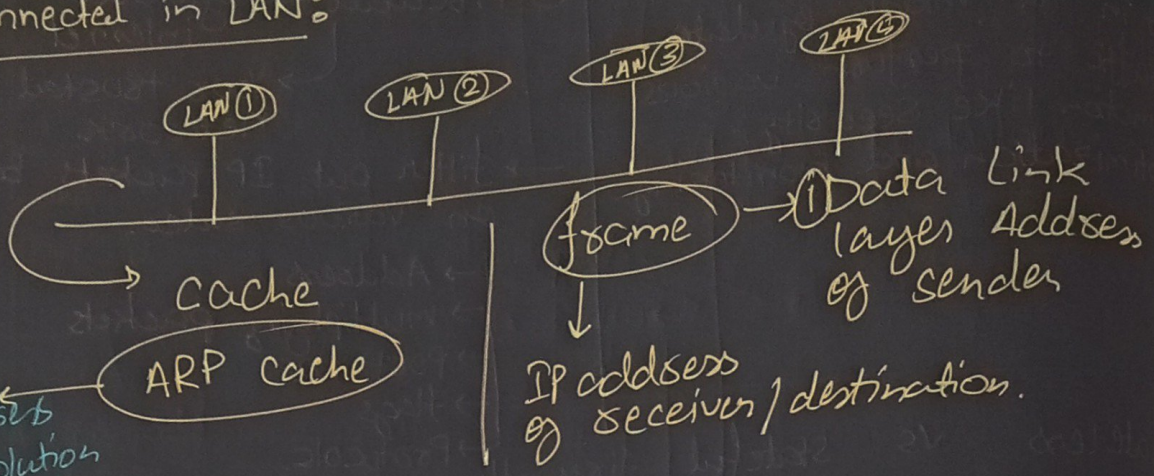
Subnet





Many ~~Active~~ device Connected in LAN:

data link layer addd → MAC addess



✕ framing

↳ networking, is the process of encapsulating data into frames for transmission over a network, adding essential info like source and destination addresses, error-checking, and control information.

MAC Address

↳ address is a unique hardware identifier assigned to a network interface allowing devices to communicate within a local network.

☆ Error Detection: networking refers to mechanisms and techniques used to identify and flag error or corruption in data transmitted over a network, ensuring data integrity. Common method include checksums, cyclic redundancy checks (CRC), and parity bits.