1) LAN : small house/office(Ethernets /wifi)

   (local area network)

2) MAN: Across the city

   (Metropolitan area network)

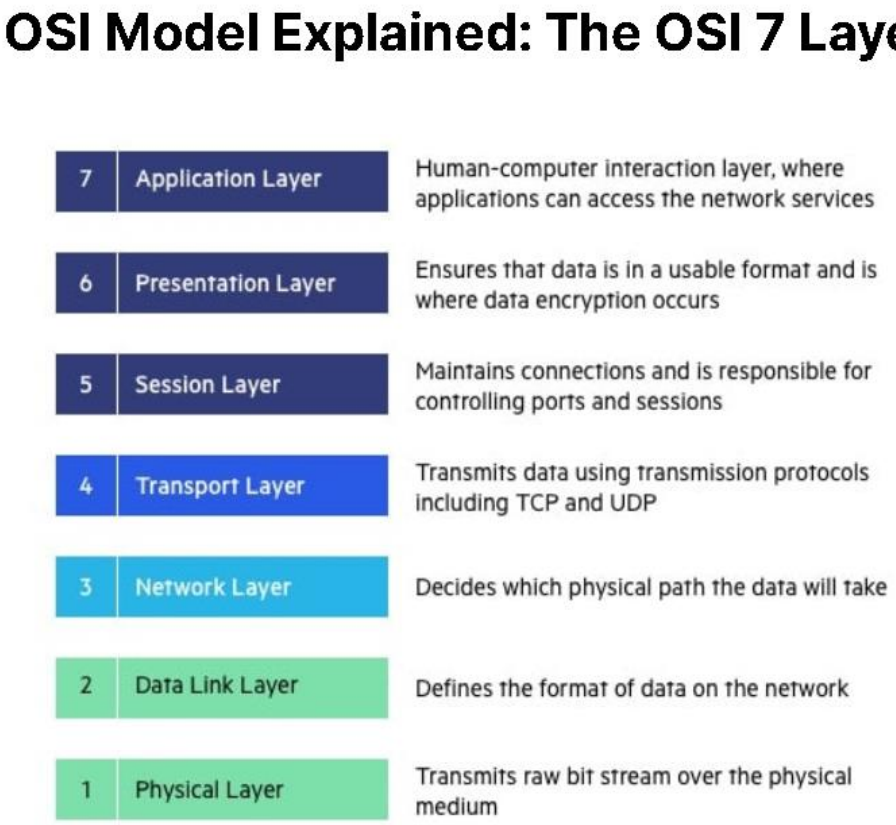
3) WAN: Across countries(optical fiber cables)
   i)Sonet -**Synchronous Optical Network ---- it carries the data** the data using optical fiber cables and it can cover larger distances.
   ii)Frame relay – it's a way to connect the local area network to the wider area like internet.

   (Wide area network)

4) Tropologies- BUS,RING,STAR,TREE,MESH
5) OSI MODEL—open systems inter connection model
   OSI MODEL LAYERS – 1)application layer 2) presentation layer 3)session layer 4) transport layer 5)network layer 6)Data link layer 7)physical layer

Application layer- its implemented into software.

Presentation layer- its encrypt the data, it also provide abstruction.



OSI model

Open Systems Interconnection model

Applical layer :- Its implimented in software.

You send the your data over Application layer to presentation layer.

Presentation layer :- It will take the data from Application layer, presentation layer is going to convert this data into machine representable binary formant. Form ascicy to Ebedic this is know as traslation. before data is going further then its goes under encording, encryption. Changing the data, to readable for only the person the data is send into. It also provide abstraction. Here SSL protocal is used for encryption and decryption.

Session layer protocal :-

Session layer protocal helps in setting up and manageging the connections. And it enabels sending and reciving the data followed by termination of the connected seossions. Here Authentication and othonisation take place.

Transport layer → To work with the data and make sure it transported to the next layer easily. Data will be transport in protocol like UDP and TCP. It dose it in three ways — ① segmentation — Data that transported from session layer it will be divided it to small segments data unit called segments. Every segment will contain the source and destination port numbers and sequence numbers. (sequence numbers basically helps to re-assemble the segments in the connect order.)

② flow control — flow control basically transport layer controls the amount of Data that is being transport, it adds ③ something known as checksome to every data segments that way it figure out the data whether the data that was receive by the friend is good or not.

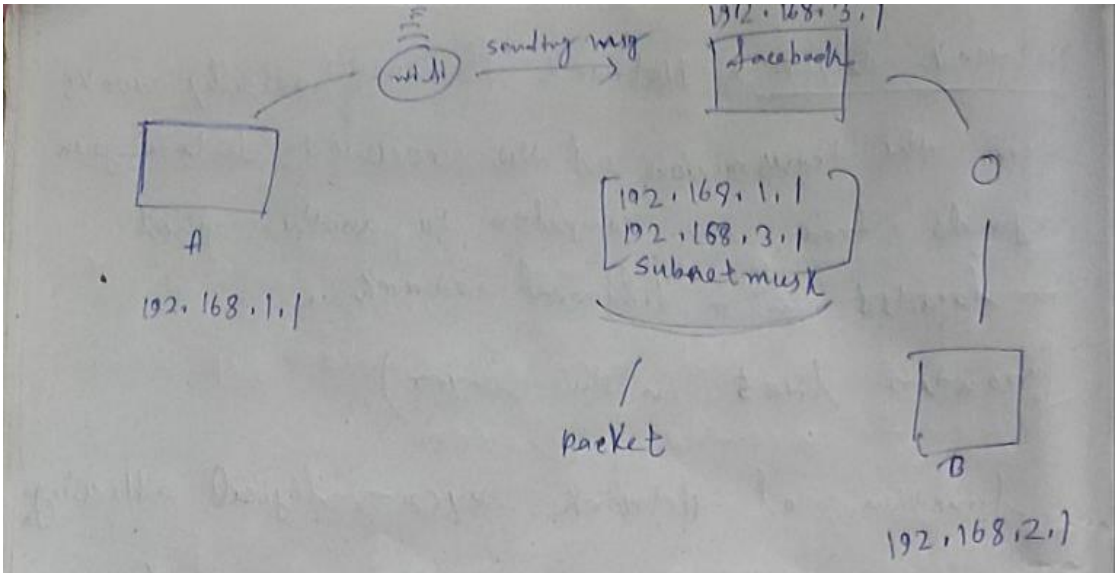
TCP (connection oriented transmission)
UDP (connection less oriented transmission)

Network layer → Network layer basically works for the transmission of the received data segmen segments from one computer to another that is located in a different network.
(router lives in the layer)

function of Network layer – logical addressing.

Ip addressing done in the network layer is known as logical addressing. Network layer assign the senders and recievers ip address to every segment and it forms an ip packet. And also it perform routing so one data packet from source to destination, load balancing also happens here.

Data link layer : Data link layer basically allows you to Directly communicate with the computers and the hosts. Data link layer will receive the data packet from the network layer and this data packets contains the ip address of senders and receivers. Physical addressing is done at Data link layer (like mac addressing) macAddress of sender and reciver is assigned to the data packet to form a frame. frame



is the data unit of the data link layer.

(mac address - mac address is a 12 digit alpha newmanic number of ~~your computer~~ the network interface of your computer)

data link layer performs two functions -

it will allow all the upper layer of the osi model to access this frames and stuf.

and it also controls how the data is placed and recived from the medias using things known as media access control.

Basically technic used to get the frame ~~the~~ and ~~at~~ like error detection.

* data link layer acctually adds mac address ~~in a frame~~ in packet it called

frame and pushes ~~it like~~ that frame like you can transport that frame.

Physical layer → This the hardware section, Here you acctually have ~~wave and~~ something like wire and stuff like that. And here it transmits the bits from electrical signal, we work with cabels and stuff like this. You get data from above layes, will be the form of like 0 and 1 physical layer is going to convert ~~it like~~ this into, transport it into wires and local media it can be eletrical signal and light signal in optical fiber cable or radio signal in case of wifi.

TCP/IP model

It's kind a similar like OSI model but it has only 5 layers

The layers are-

1)application layer 2)Transport Layer 3)Network layer 4)Datalink layer 5)Physical layer

1) Application layer-

Protocols:

Web protocols:

TCP/IP:

HTTP= hyper text transfer protocol : it defines how the data is transferred, html pages and stuff like that

DHCP= Dynamic host control protocol : it basically allocates ip address that people or devices allocated to your network.

FTP= file transfer protocol: how file can be transferred

SMTP= simple mail transfer protocol : it used to send the email.

Pop3 and IMAP = to receive the email we use pop3 & Imac.

SSH= Secure shell : if you want to login to someone else's computer you need to use SSH

VNC= virtual network control : for graphical control

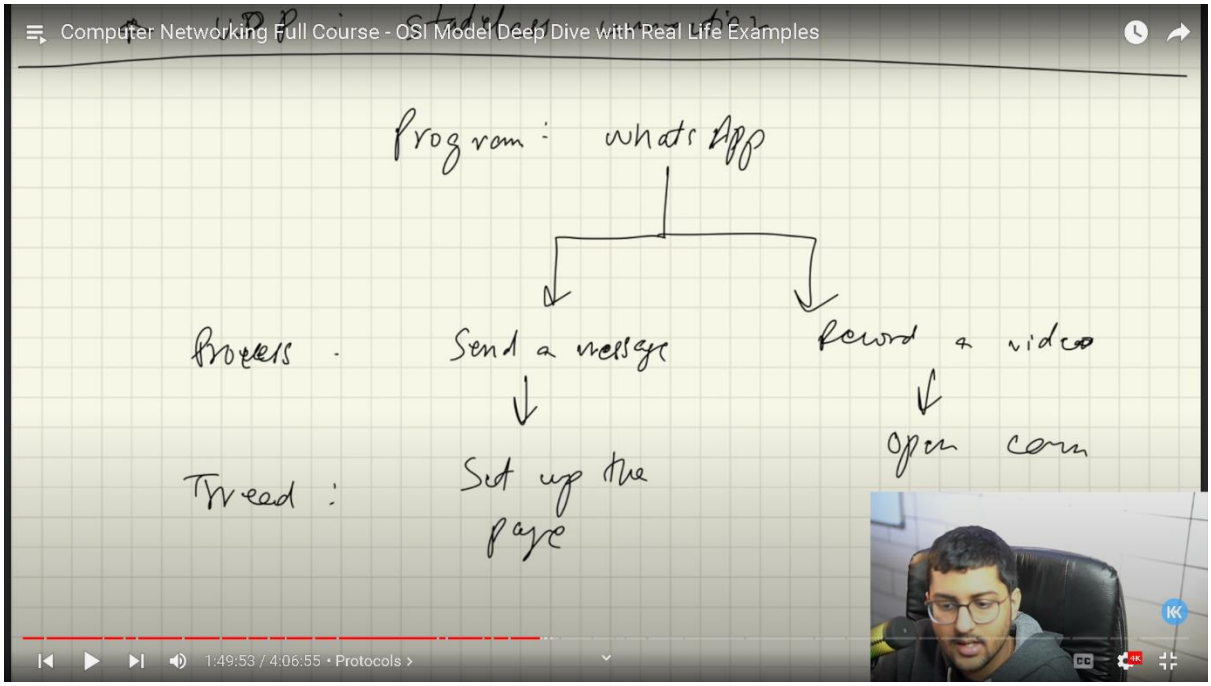
Telnet = Telnet basically a terminal emulation that enable a user to connect to host or device via telnet client : usually its over port "23"

Command- Telnet Hostname lands you in the hostname

HTTPS = Here "s" means secure. Here we get data which is encoded or encrypted.

UDP= state less connection : data may be lost in this like video call.

Socket = interface between process and the internet.



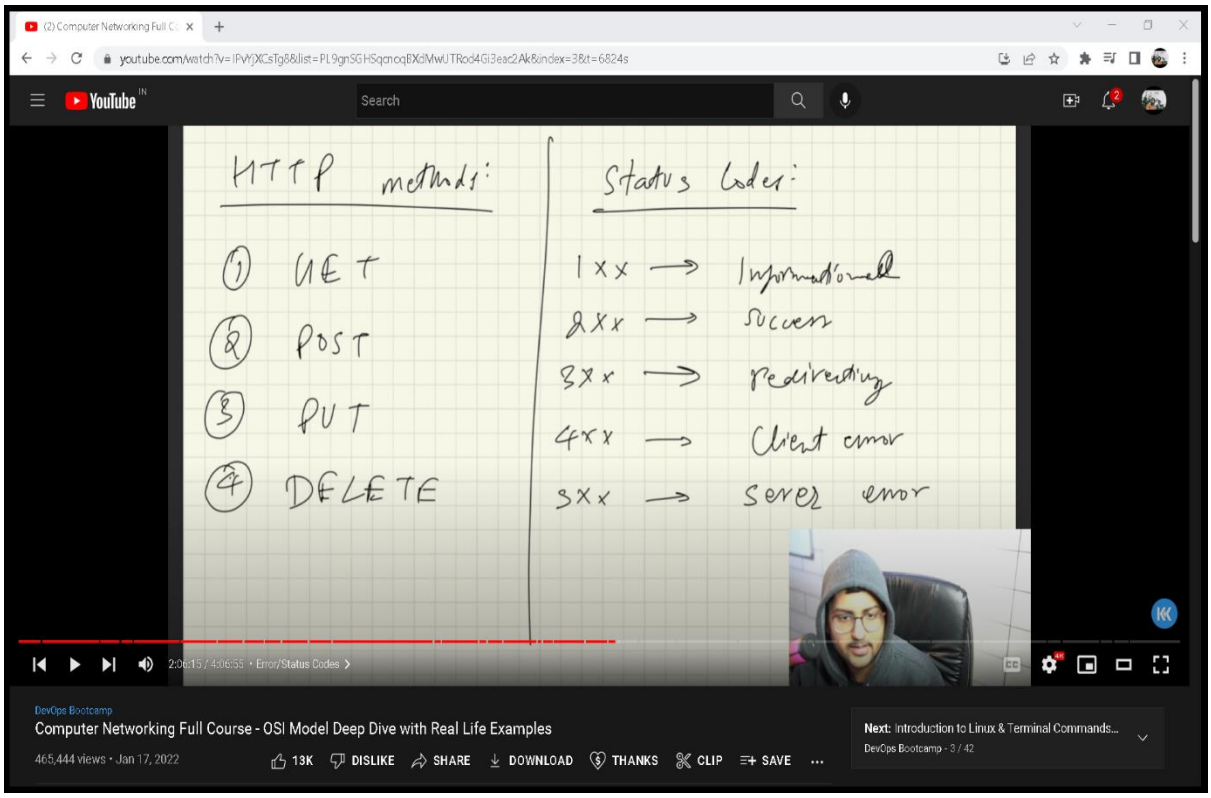
Thread: Thread is a lighter version of a process.

Ports : ephemeral ports.

HTTP= http is a user client protocol. HTTP used tcp(transmission control protocol) : it's actually a stateless protocol .server will not save any information about the user.

("HTTP is a application layer protocol and TCP actually is Transport layer protocol.")

HTTP METHODS = 1)GET 2)POST 3)PUT 4)DELETE



COOKIES = unique string

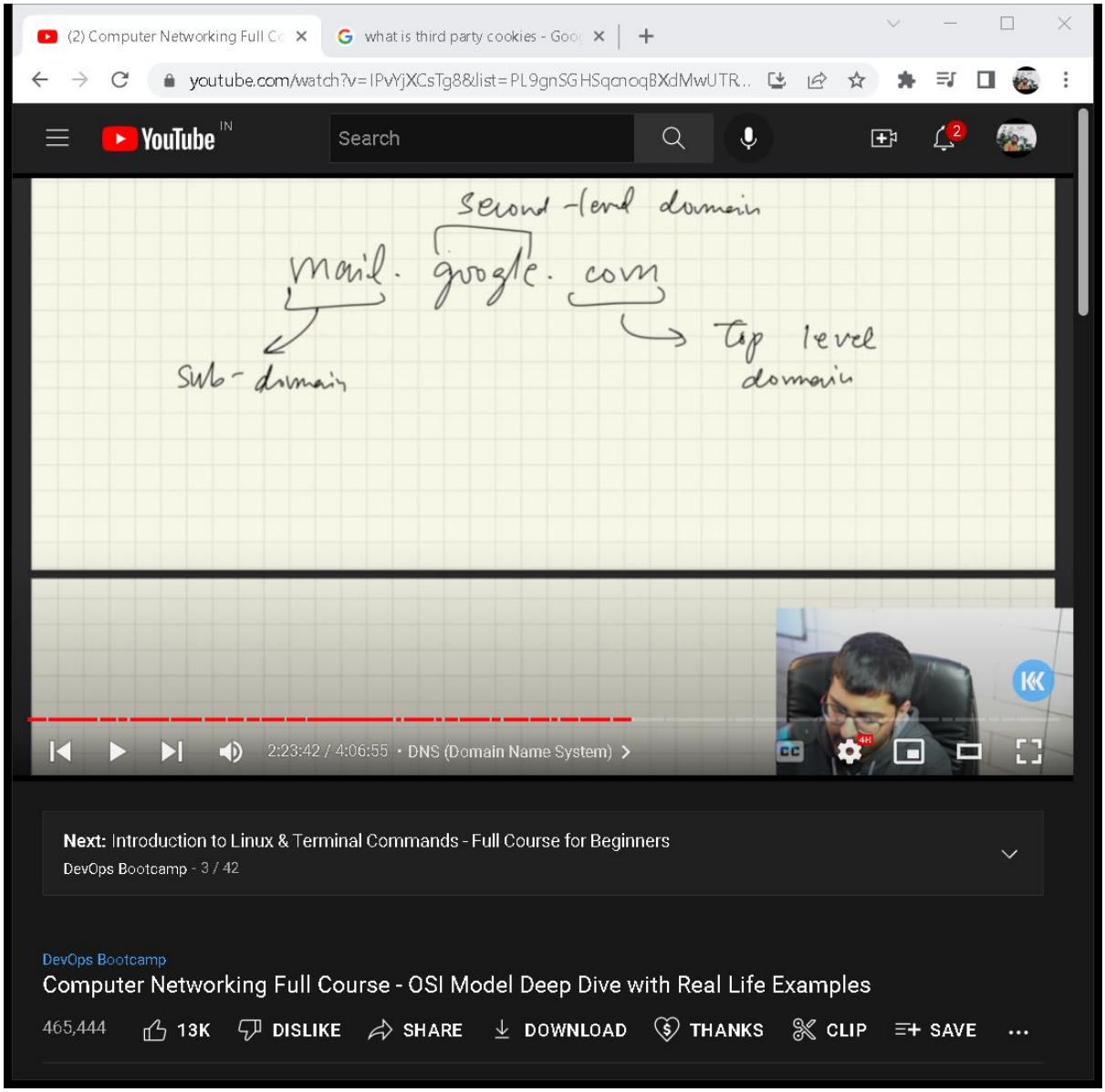
Stored in users browser. And cookies are send as a header of request.

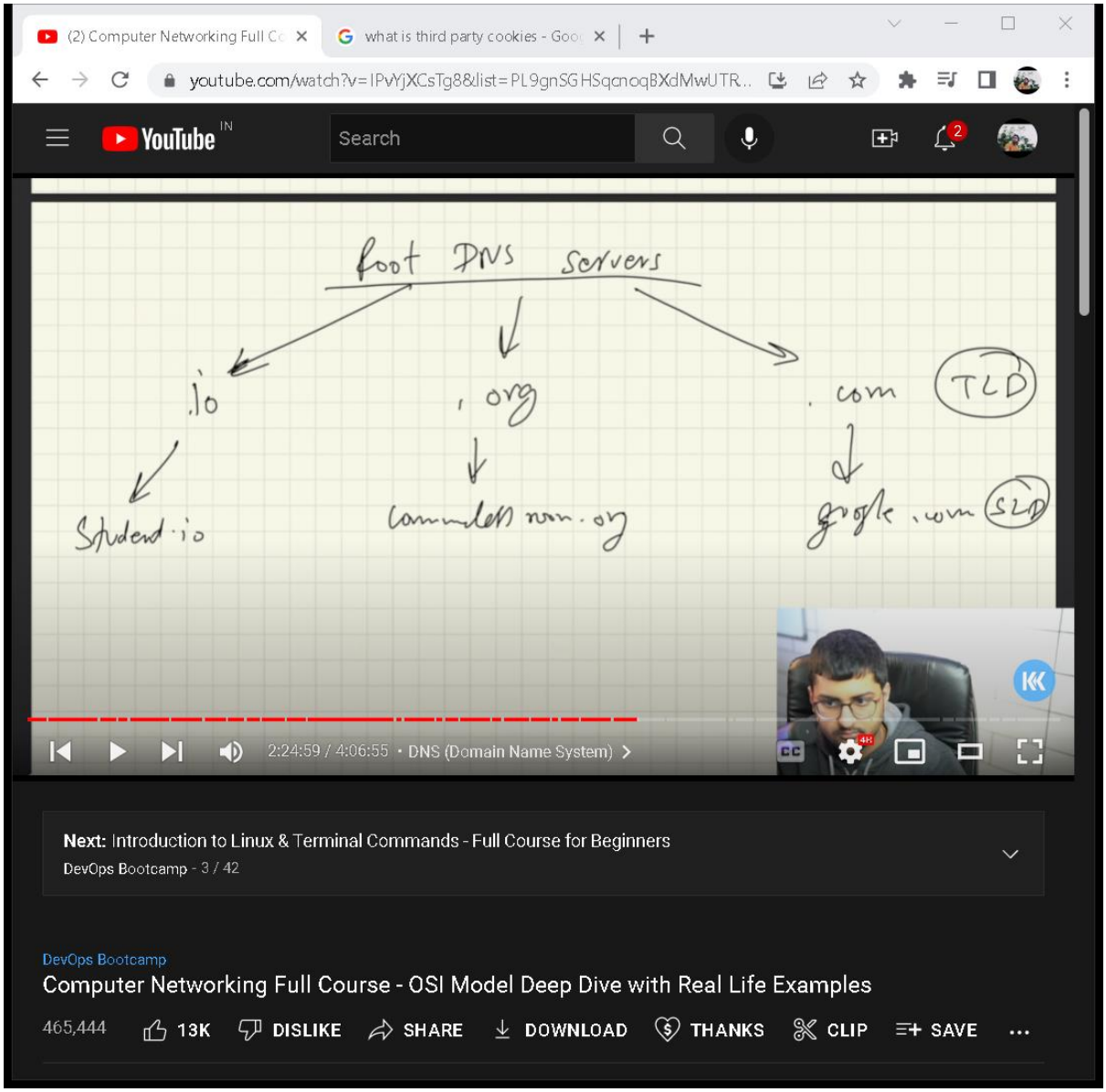
Third party cookies = A third-party cookie is placed on a website by someone other than the owner (a third party) and collects user data for the third party.

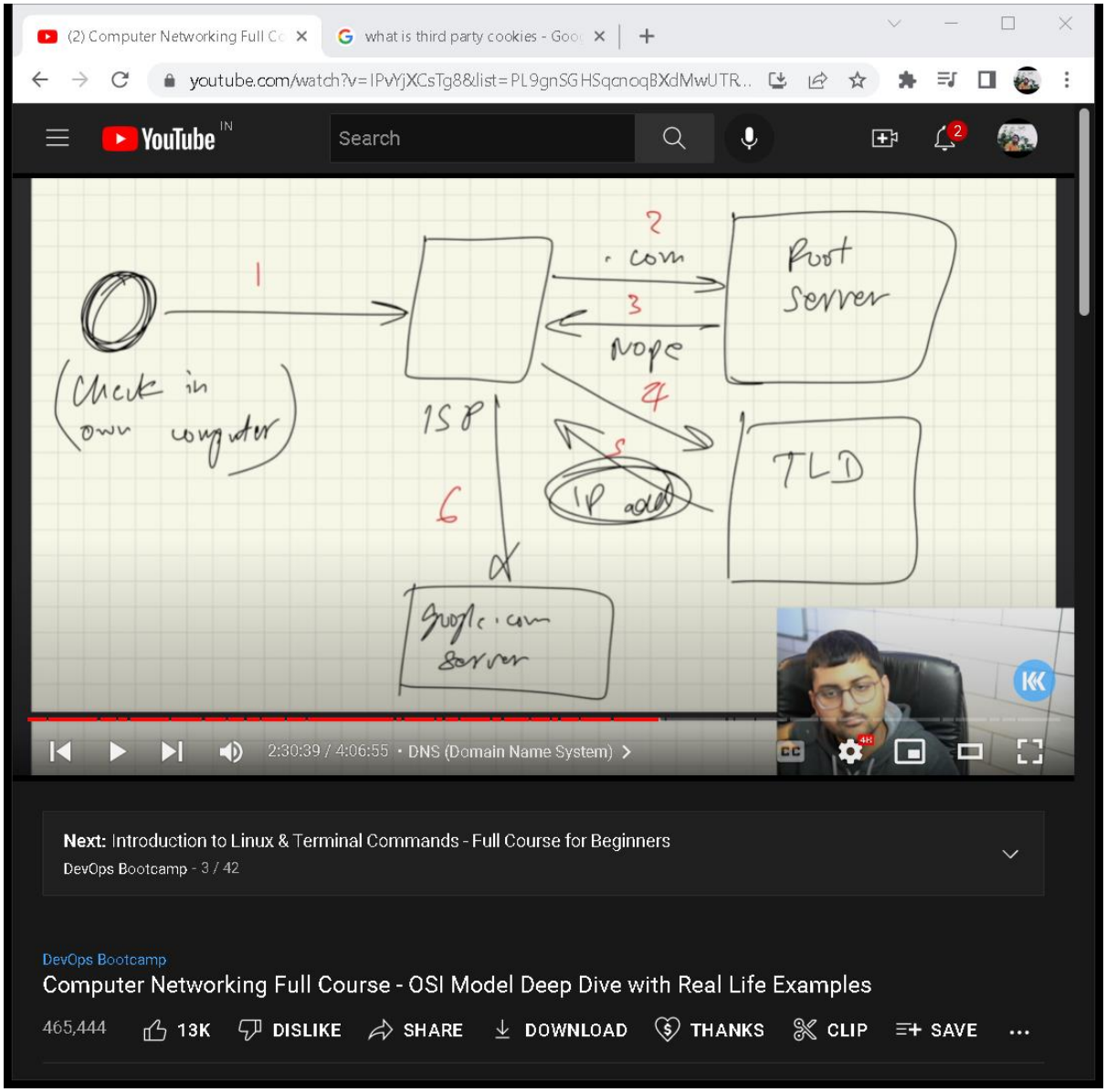
Email works : in this protocols like SMTP(simple mail transfer protocol) , pop3 (post office protocol) and imap(it allows you to see your emails on multiple servers).

*DNS = Domain name system.

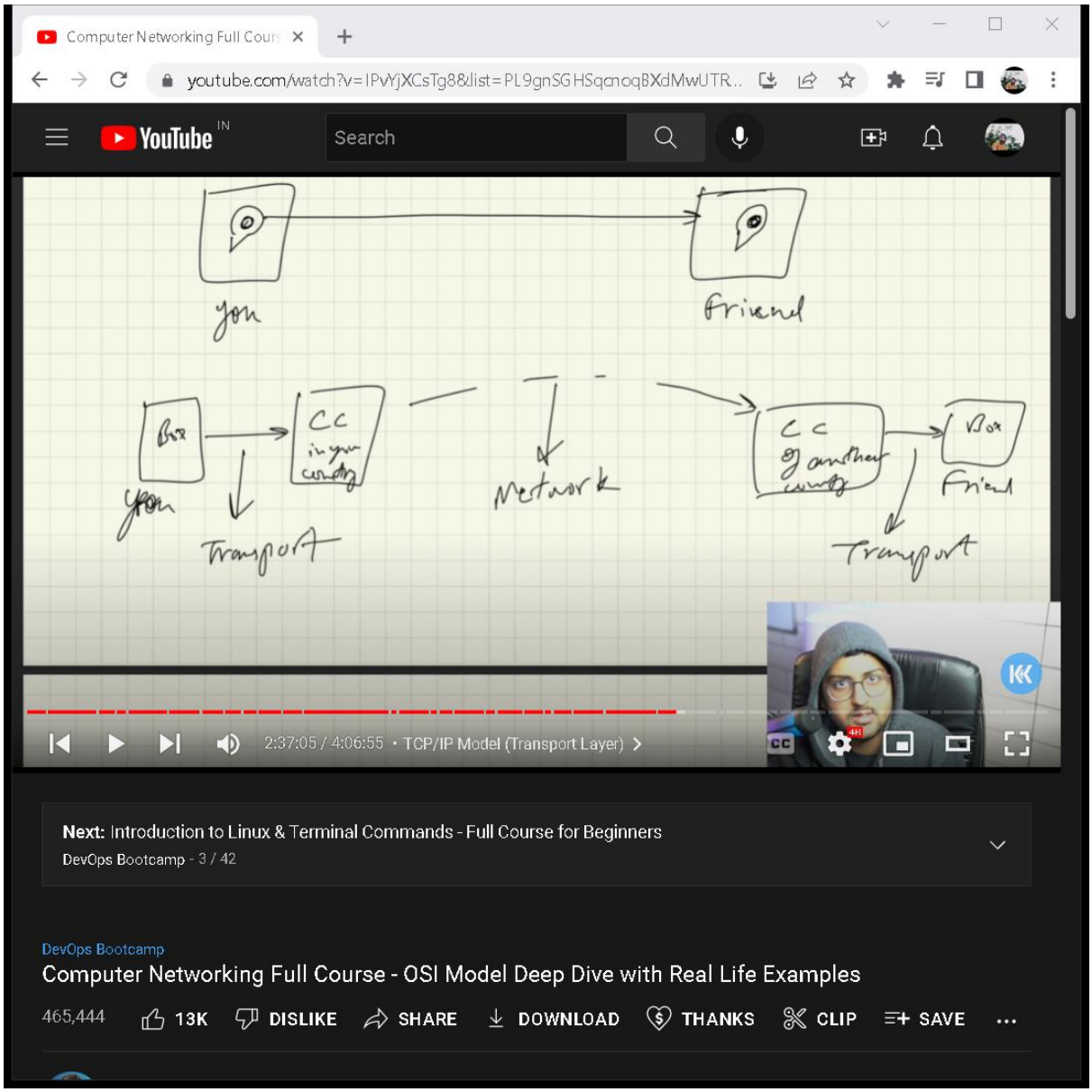
Basically domain names are mapped to ip address.



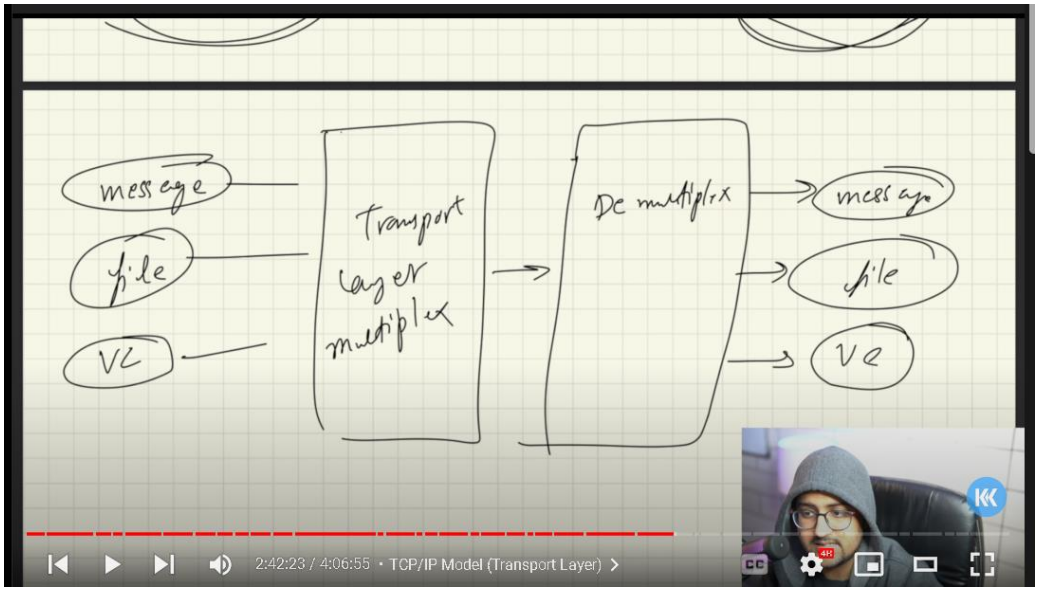

(2) Computer Networking Full C
what is third party cookies - Goo
youtube.com/watch?v=IPvYjXCsTg8&list=PL9gnSGHSqcnoqBXdMwUTR...
YouTube IN
Search
Root DNS servers
.io
.org
.com
TLD
Student.io
.com
SLD
2:24:59 / 4:06:55 • DNS (Domain Name System)
Next: Introduction to Linux & Terminal Commands - Full Course for Beginners
DevOps Bootcamp - 3 / 42
DevOps Bootcamp
Computer Networking Full Course - OSI Model Deep Dive with Real Life Examples
465,444
13K
DISLIKE
SHARE
DOWNLOAD
THANKS
CLIP
SAVE



2) Transport Layer:



Transport layer multiplexer and de multiplexer :



Socket = A socket is one endpoint of a two-way communication link between two programs running on the network. A socket is bound to a port number so that the TCP layer can identify the application that data is destined to be sent to. An endpoint is a combination of an IP address and a port number.

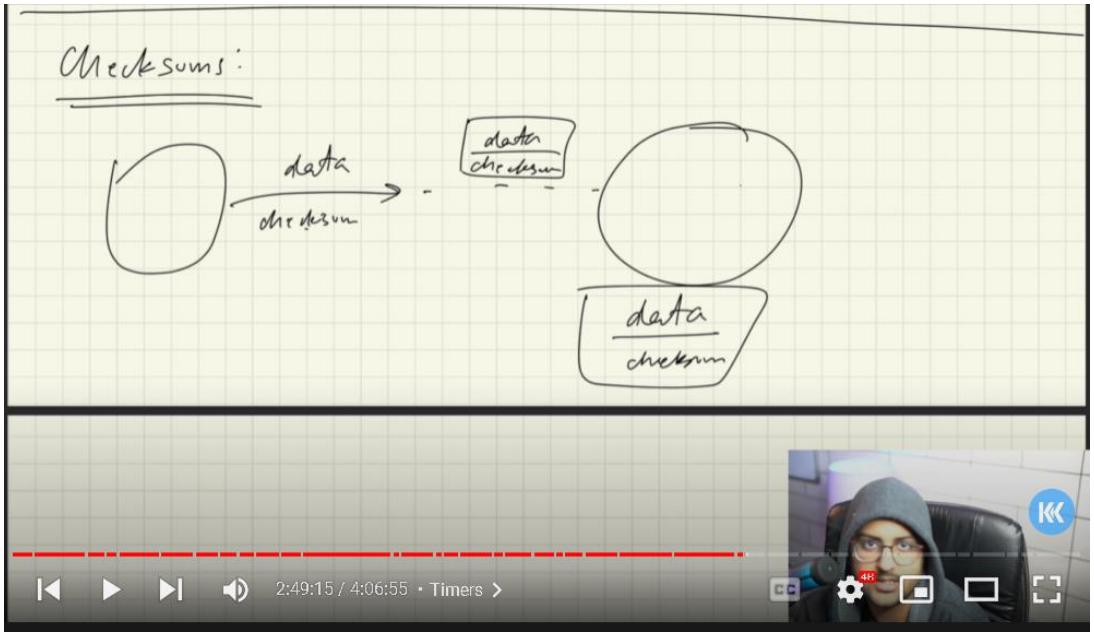
*Data travels in packets, this transport layer will attach socket ports with it.

*Transport layer also takes care of congestion(/traffic) control.

(congestion control= a mechanism that controls the entry of data packets into the network, enabling a better use of a shared network infrastructure and avoiding congestive collapse.)

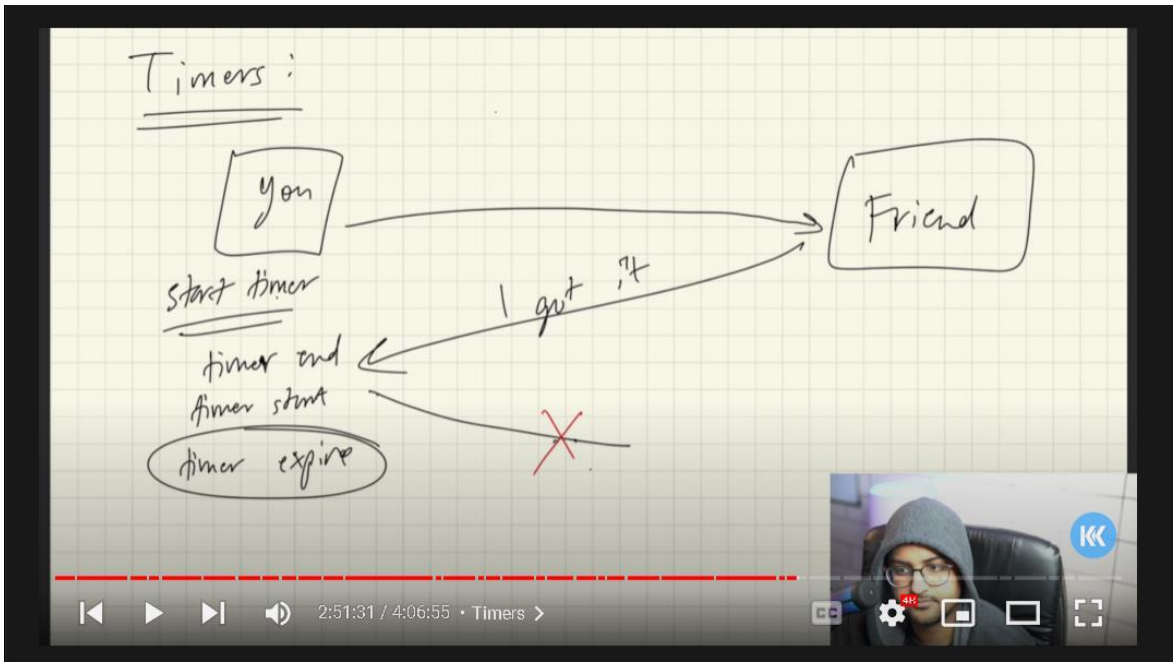
*congestion control algorithms built in tcp.

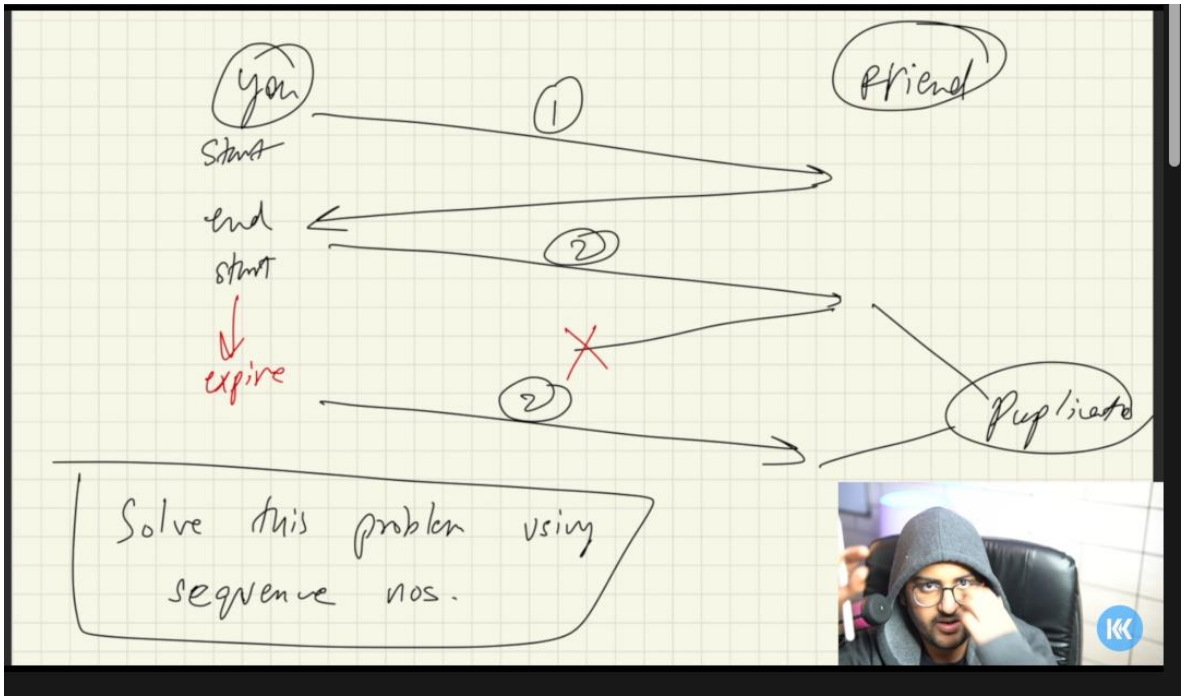
*checksum = value that represents the number of bits in a transmission message and is used by IT professionals to detect high-level errors within data transmissions.



Timers :

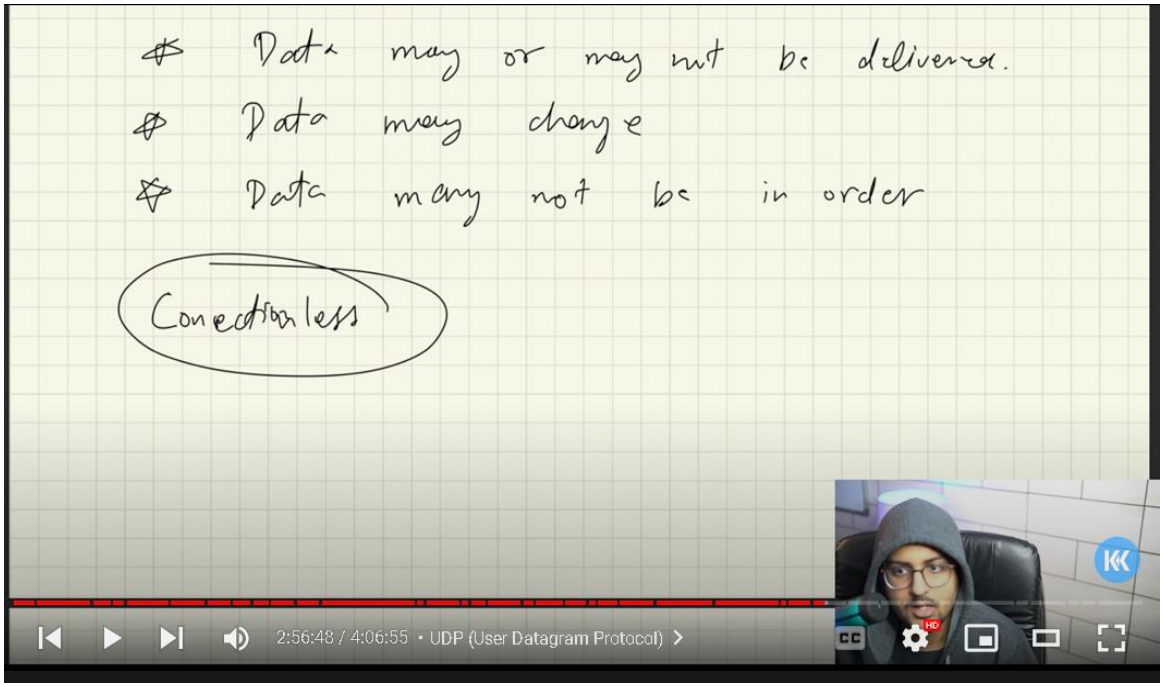
Retransmission Timer – To retransmit lost segments, TCP uses retransmission timeout (RTO). When TCP sends a segment the timer starts and stops when the acknowledgment is received.



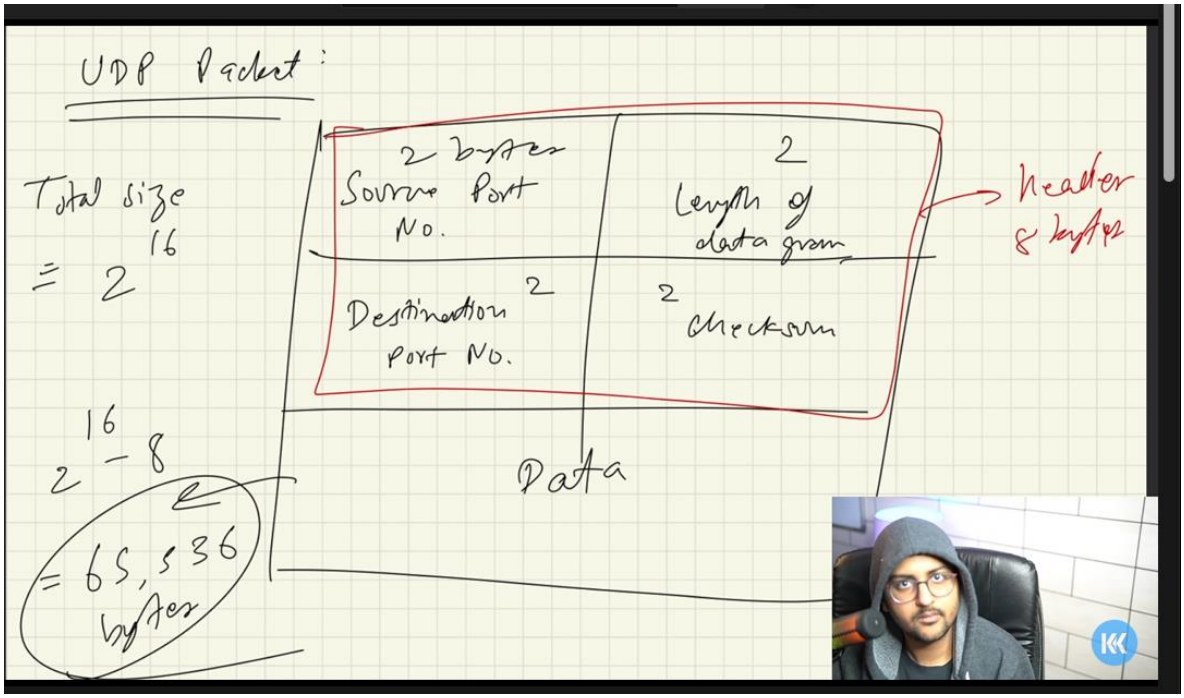


(sequence numbers)

UDP(user datagram protocol) =



UDP uses chechssum.



Uses cases of udp=

It's very fast

Video cong apps

DNS → udp

Gaming

TCP (transmission control protocol) =

1) Its in Transport layer protocol.
2) Application layer sends lots of raw data, tcp segments this data -> divide into chunks add headers, checksum etc. it may also called the data network layer(basically it put together data, which is came from network layer in more smaller chunks)
3) Congestion control.
4) It takes care of --- when data does not arrive

--- maintain the order of data(using the sequence number)

Features =

1)it's connection oriented(first connection get established then file get transferred)

2) its also provide Error control

3) congestion control

4)full Duplex (both computers can send simultaneously)

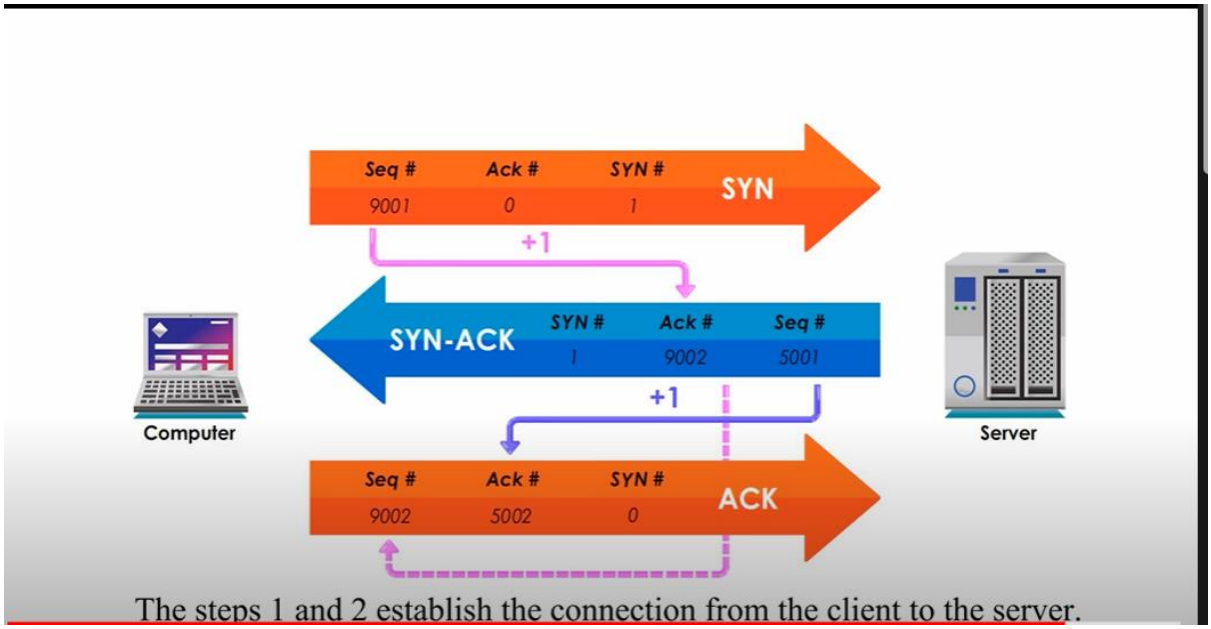
5)it will add sequence number and acknowledgement number and checksum and stuff.

3-way handshake:

Step 1 (SYN): In the first step, the client wants to establish a connection with a server, so it sends a segment with SYN(Synchronize Sequence Number) which informs the server that the client is likely to start communication and with what sequence number it starts segments with

Step 2 (SYN + ACK): Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segments with

Step 3 (ACK): In the final part client acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer.

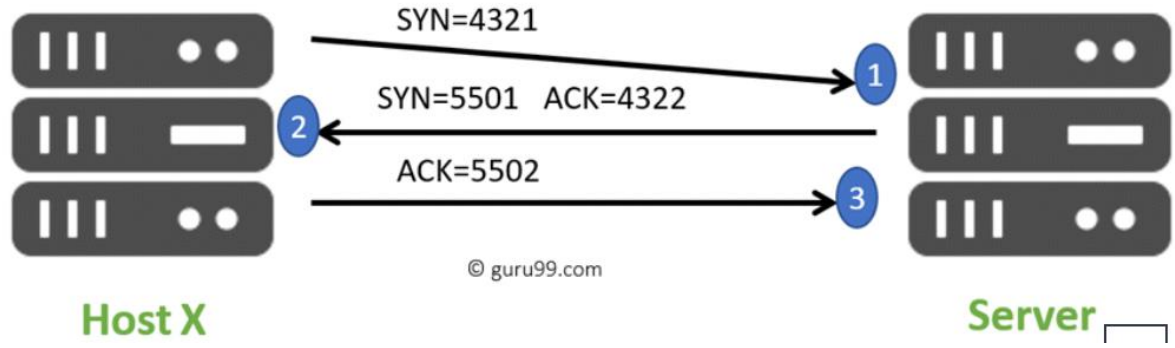


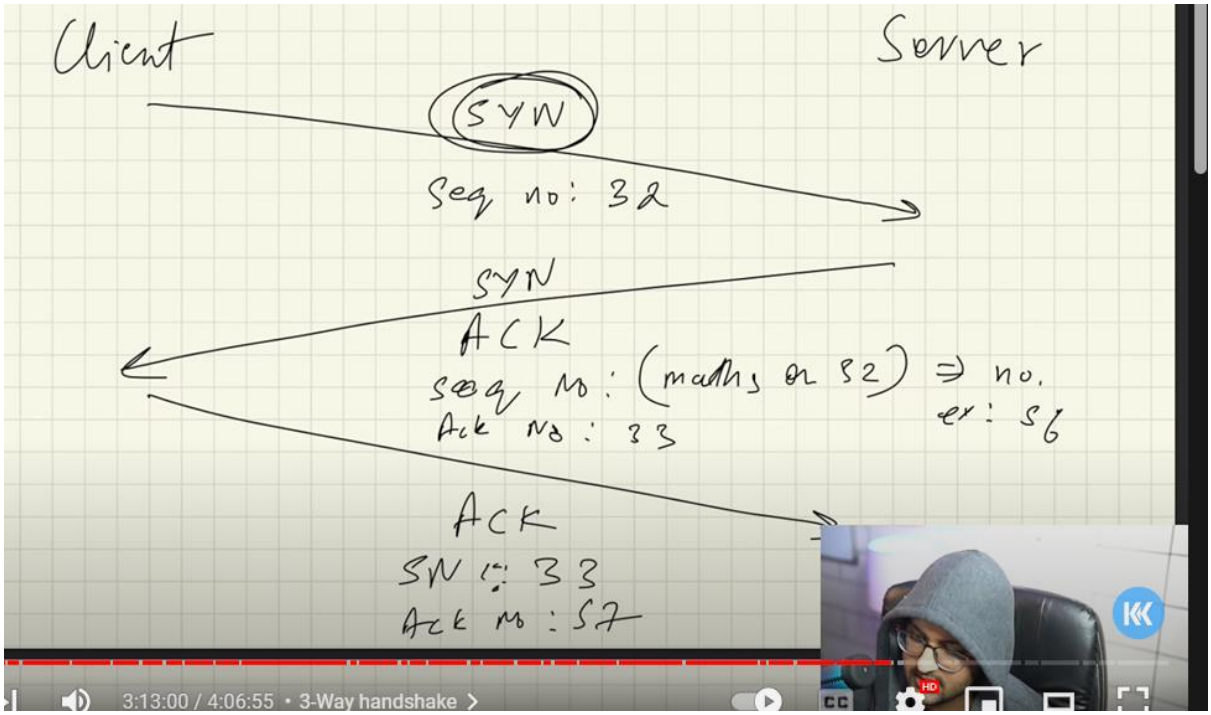
The steps 1 and 2 establish the connection from the client to the server.

The steps 2 and 3 establish the connection from the server to the client.

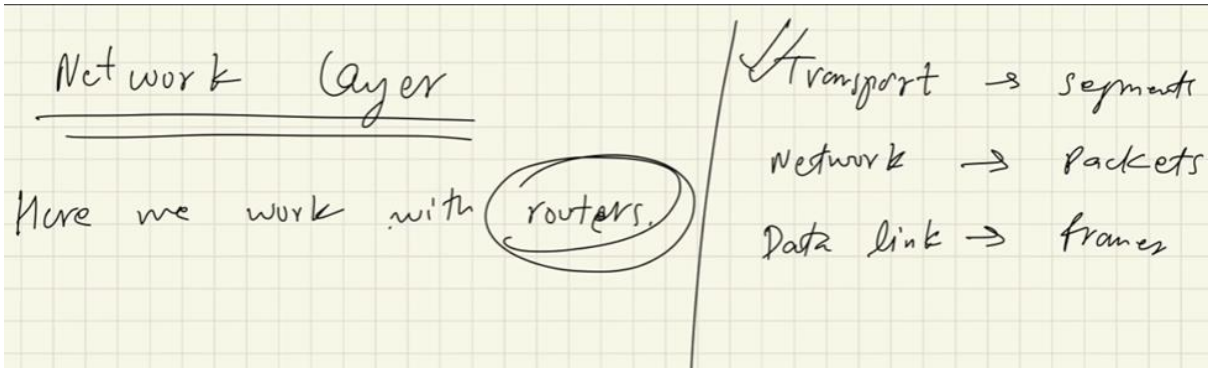
Thus, two-way communication channel is established.

Real-world Example





Network layer

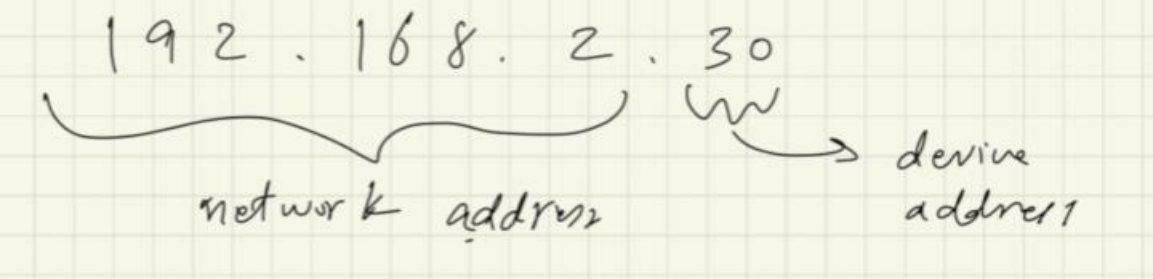


Packet = contains network layer address of destination , network layer address of the person who is sending it and what information you wanted to send.

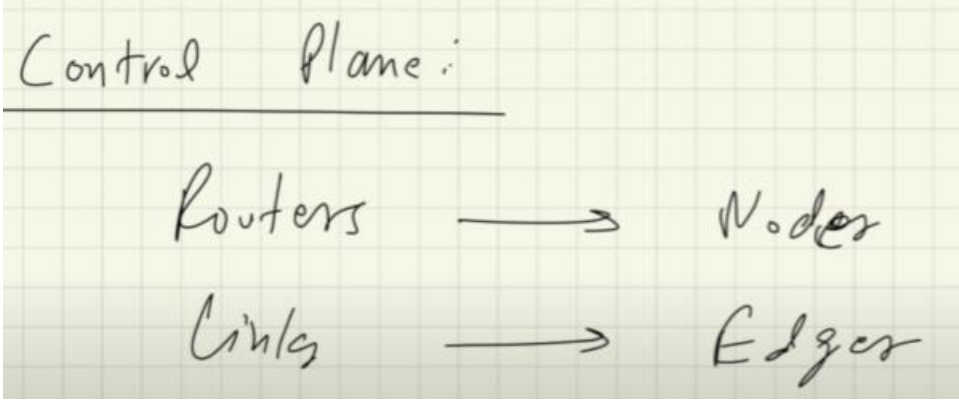
*routing table –

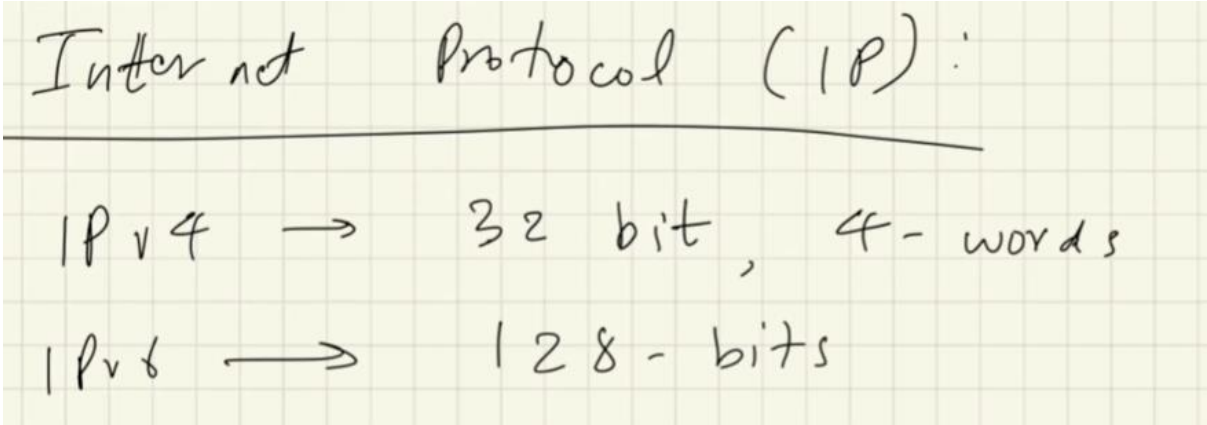
*forwarding table

IP address =



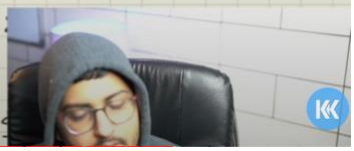
Control plane =





Class 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



D=239.255.255.255

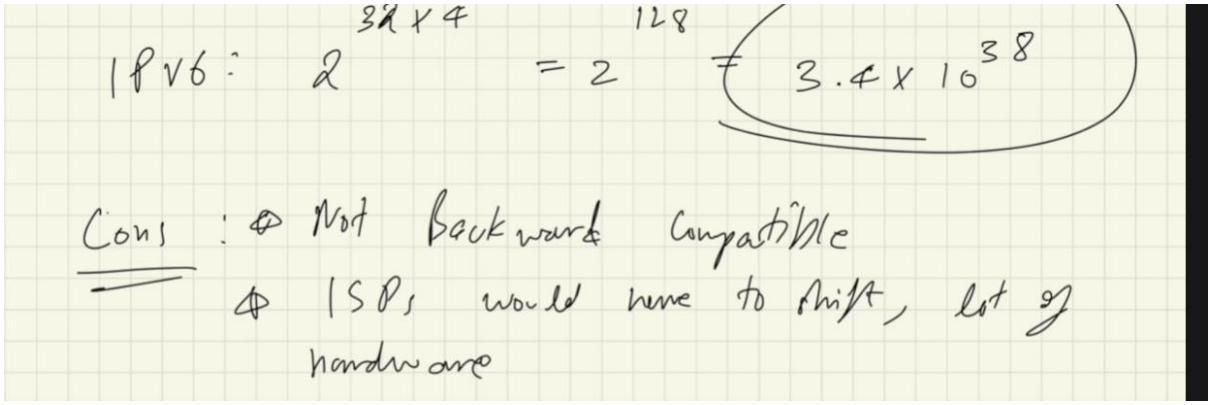
E=255.255.255.255

Packets: Header is of 20 bytes.

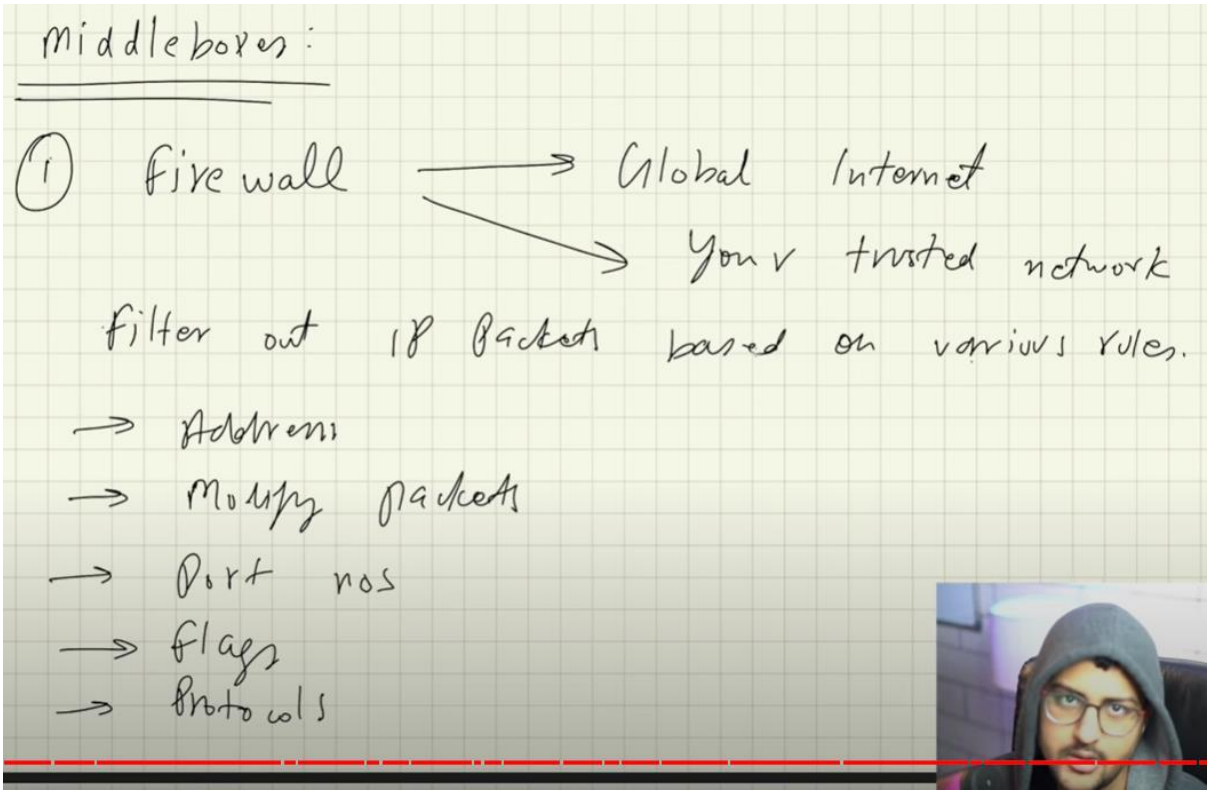
IPV, length, Identifications, flags, protocols, checksum, address, TTL, etc

IPV6

ipv4: $2^{32} \approx$ 4.3 billion



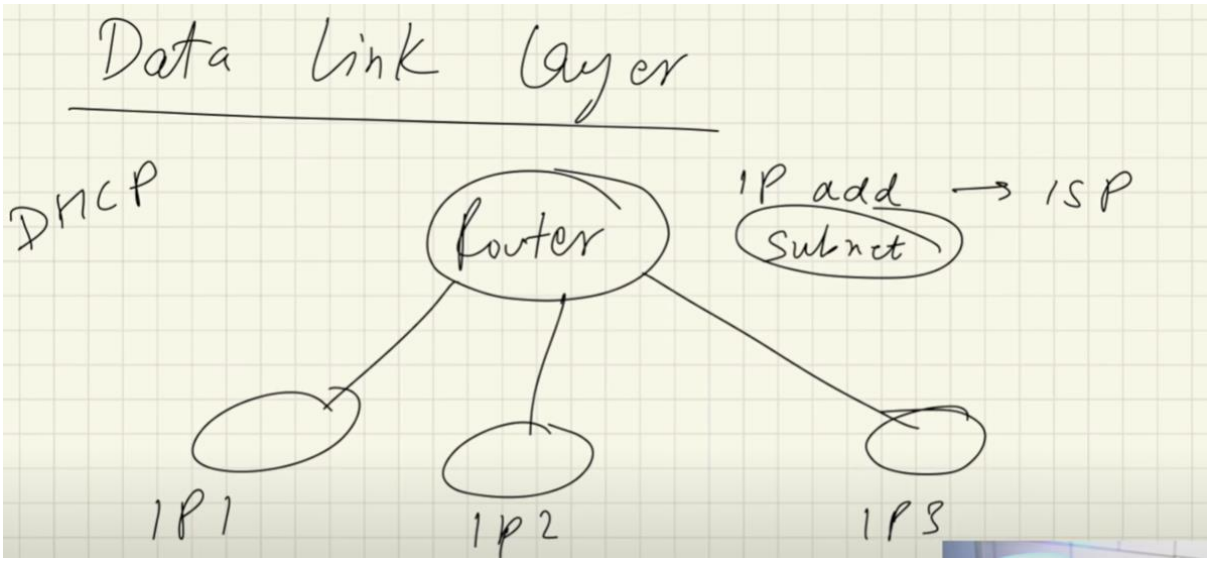
*lots of hard work



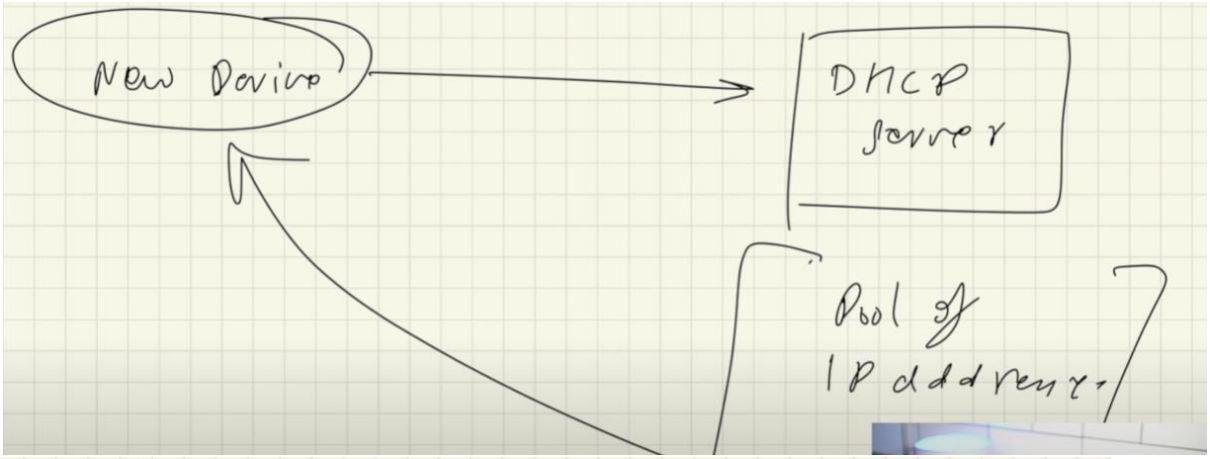
NAT=

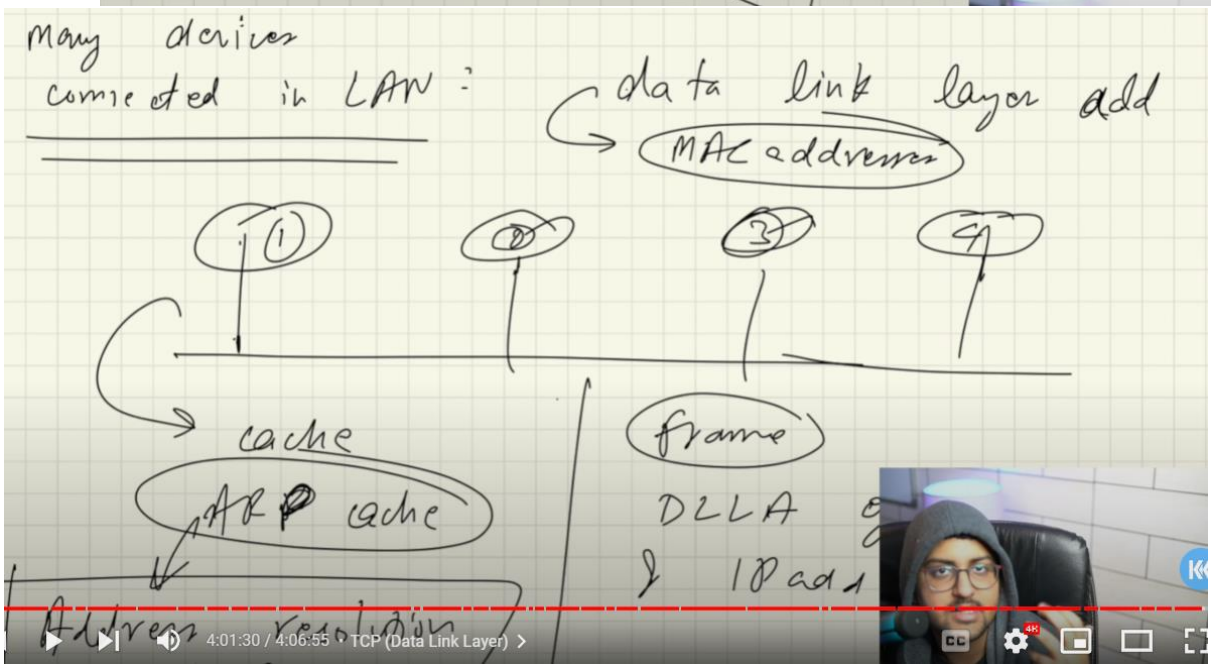
NAT stands for network address translation. It's a way to map multiple local private addresses to a public one before transferring the information. Organizations that want multiple devices to employ a single IP address use NAT, as do most home routers.

DATA link layer:


Data Link Layer
DHCP
Router
IP add
Subnet
ISP
IP1
IP2
IP3

(Subnet=)


New Device
DHCP
Server
Pool of
IP addresses


Many devices
connected in LAN:
data link layer add
MAC addresses
1
2
3
4
cache
ARP cache
frame
DLLA
IP add
Address resolution
4:01:30 / 4:06:55 • TCP (Data Link Layer) >