COMPUTER NETWORKS

- **What is computer Network.**

Computer network is just computers connected together which communicate with one another.

- **Basic Terminologies**

(1) What is Client?

Client is a computer hardware device or a software that accesses the service made available by the server.

(2) What is Server?

A server is a physical computer dedicated to run services to serve the need of other computers (Clients). It can be a physical device or software

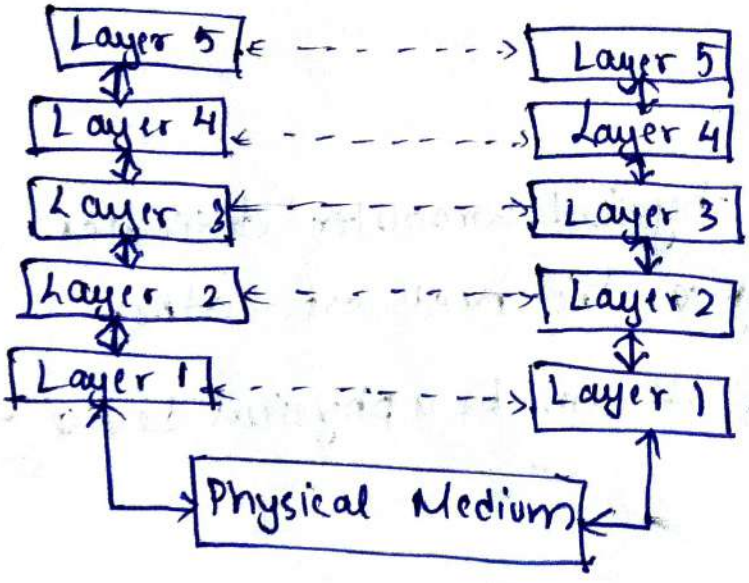
(3) What is host?

Host is any computer connected over the network. It is always a physical device.

Server	Host
* Physical device or Software	* It is always a physical device
* Installed on host computer	* can be both a server (while providing service) and client (while requesting for service)
* Serves only clients	* Serves ~~only~~ multiple users & devices.

4) What is peers?

The entities comprising the corresponding layers on different machines are called peers.



- Layer 5 of host 1 is a peer to Layer 5 of host 2
- ||ly Layer i of host 1 is peer to Layer i of host 2

Peer is not always a layer.

If I talk to you on a mobile phone, you & I are peers in that communication.

The mobile phones each convert audio to/from radio

waves. In this case mobile phones are peers on the phone network.

However, I am not a peer with mobile phone because we are on different levels.

5) Bandwidth

It is maximum rate at which data transfer occurs ~~at~~ any particular path of the network. It is basically the measure of amount of data that can be sent and recieved at an instance of time.

> Bandwidth $\propto$ Data that can be sent

Bandwidth can be compared to volume of water that can flow through the pipe. Wider the pipe, more water can flow.

Cost of network connection goes up as bandwidth increases.

> Bandwidth != Speed

Speed = rate at which data can be sent

Bandwidth = Capacity of speed.

Speed refers to how quickly water can be ~~pushe~~ pushed through the pipe

Bandwidth refers to quantity of water that can be moved through the pipe. Over set time frame.

[6] Jitter

Jitter is time delay in sending data packets over the network connection. This is often caused by network congestion.

Eg: Delay in sending audio/video packets on video/phone call

Jitter is measured in ms. A delay around 30ms or more can cause distortion and disruption.

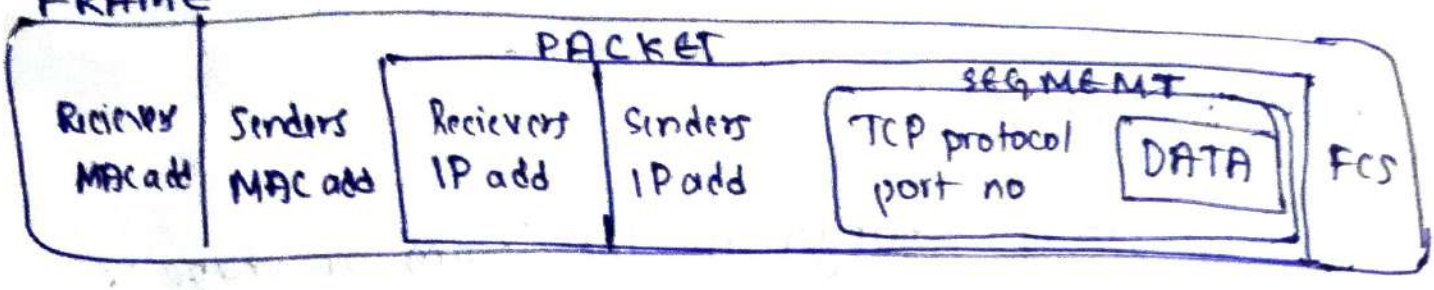
[7] Packet

Packet is a small segment of large message. Data sent over computer network are divided into packets. Packets are combined by reicving computer.

[8] Frame

Frame is a unit of data. Frame works to help identify data packets used in networking and telecommunication.

The crucial difference between frame and packet is that frame is a serial allocation of bits and it encapsulates packets whereas packets are fragmented form of data and it encapsulates segment.



[9] Localhost

Local host is your own computer.

When you call an IP address on your computer, you try to contact another computer on the internet, but when you call the IP address 127.0.0.1 you are communicating with the local host (i.e your own computer). Localhost can be seen as a server that is used on your own computer.

[10] Bit rate

No of bits of data sent per second.

[11] Noise

Noise is undesired signal in communication circuit.

[12] Attenuation

It refers to loss of signal strength due to internal or external factors.

It is measured in dB (decibels)

Eg: WiFi signal strength decopping as distance from router increases

13) Distortion

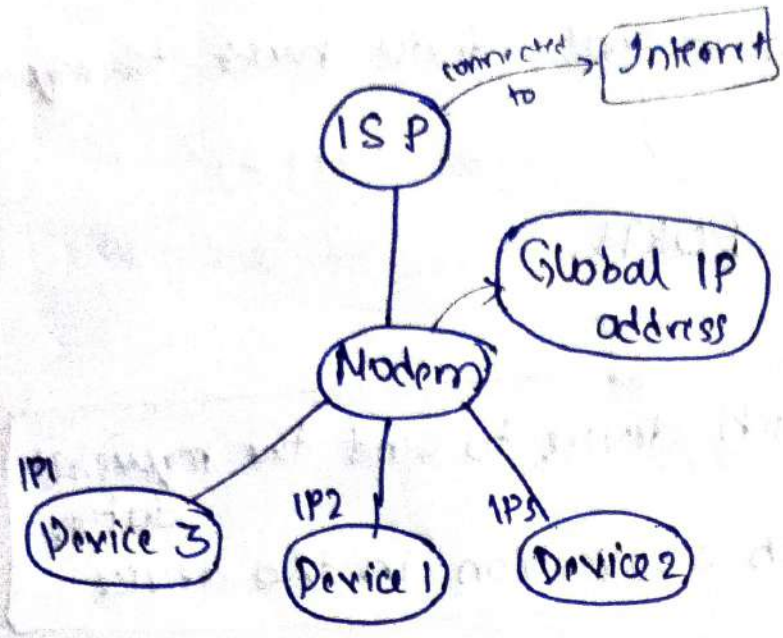
It is changes in the form or shape of signal that is transmitted. (Signal at reciever side is different in shape than ~~that~~ what what was sent).

This is generally seen in composite signals made up with different frequencies.

What is Web? Difference b/w Web & Internet

Internet	Web (world wide web)
* It is global network of networks	* It is collection of information that is accessed via internet
It can be viewed as a huge book store	Web can be viewed as as collection of books in the book store.
* Use TCP or UDP protocol	* Use HTTP protocol which is a layer over TCP protocol

- IP address & Port NO



* An ISP gives you a modem/Router. This is going to have a ~~global~~ GLOBAL IP address; all the devices connected to this WIFI are going to have the same IP address. Modem will give IP address to the devices connected as well and these are known as LOCAL IP ADDRESS.
* If any of the connected device makes request to google.com, google sees only the GLOBAL IP address ~~the~~ Google returns the service requested to modem.
* Modem now decides which device to serve using LOCAL IP Address. (it knows which device requested service from google).

* Modem knows which device made the request.

But which application in that device made the request is to be known.

We do this using PORTS.

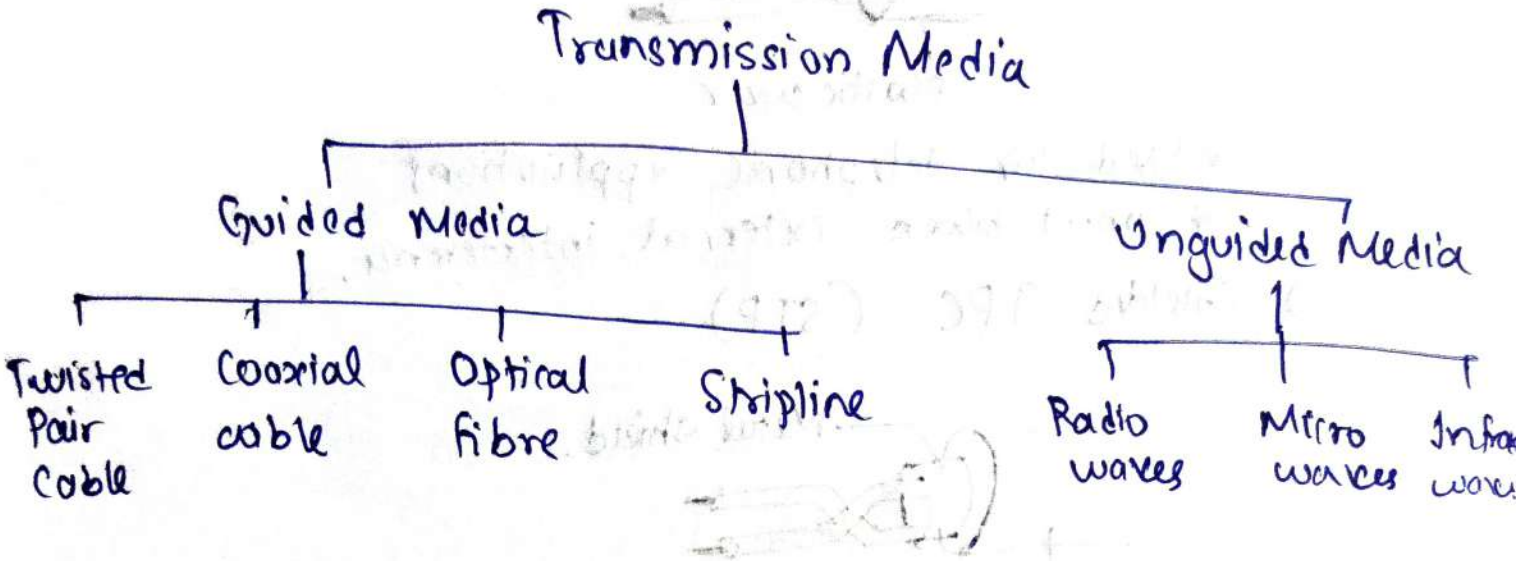
IP address decides which device to send the requested data.

PORT no decides which application in the device

- **Port NO**
  - * Used to identify an application
  - * It is a 16 bit no ⇒ 0 - ≈65000
  - * Port No's from 0-1023 → Reserved Port No's
    All the HTTP stuffs you do happen on PORT 80
  - Port No's from 1024 - 49152 → Reserved for Applications
    Eg: for mongoDB, for VS code etc...
  - You can use the rest of them for your own use

- Types of Transmission Media

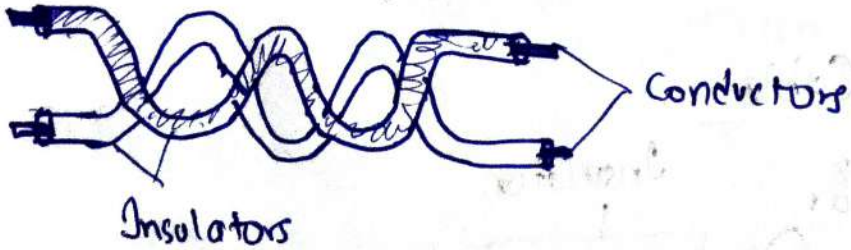
It is a physical path b/w sender and receiver. ie it is the channel through which data is sent from one place to another.



[1] Guided Media

It is also refered as wired or Bounded transmission media. Path b/w communicating devices is already fixed.

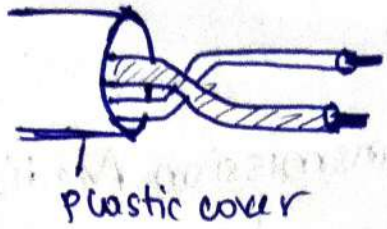
- Twisted Pair Cable



It consists of 2 separately insulated conductor wires wound over each other.

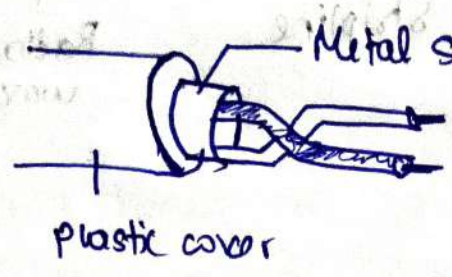
* One of them is used to transmit data while the other is used only for ground reference.

1) Unshielded Twisted Pair Cable (UTP)



* Used for telephonic applications
* Cannot block external interference.

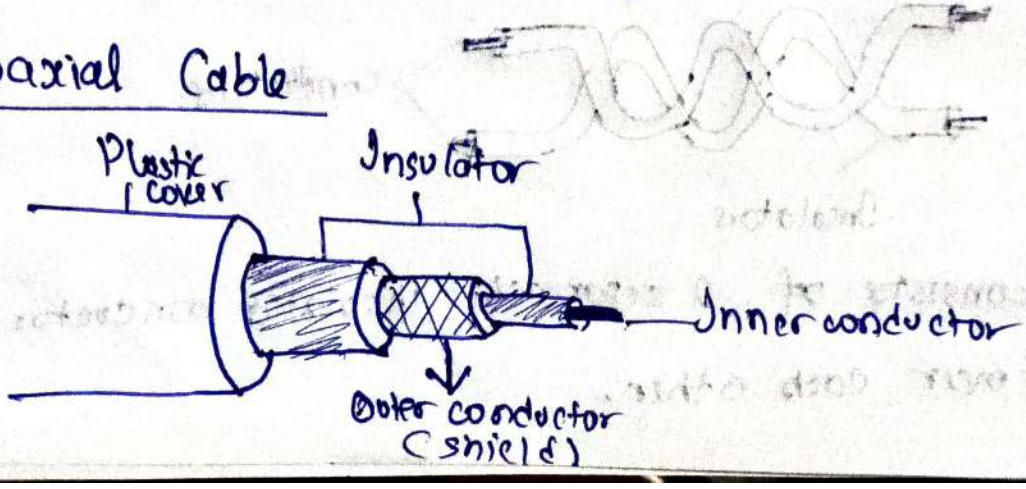
2) Shielded TPC (STP)



Cable consists of special jacket (copper braid covering) to block external interferences.

* Used in fast data-rate ethernet
* Faster than UTP.
* More expensive & bulky

- Coaxial Cable



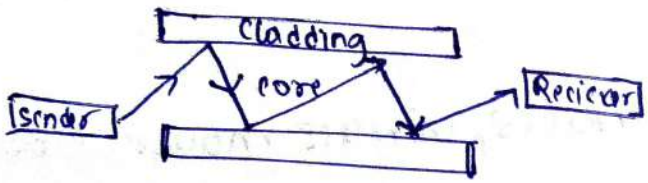
* It transmits information in two modes

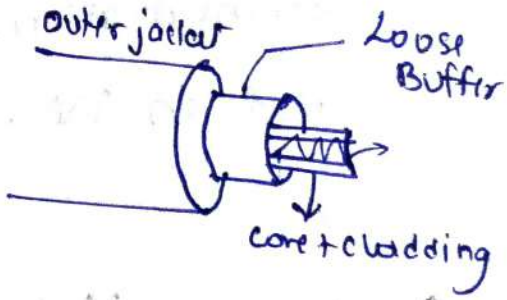
1) Base band mode (dedicated cable bandwidth)
2) Broad band mode (cable bandwidth split into separate ranges)

* Cable networks and television networks use coaxial cables.

- * It is inexpensive and easy to install and expand
  * It has better noise immunity.

- Fibre Optic cable





Advantages

* Increase bandwidth
* Light weight
* Less signal attenuation
* Immune to electromagnetic interference.

2 Unguided media

Also referred to as unbound or wireless transmission. No physical medium is required and has no fixed path b/w sender & receiver.

1) Radio Waves

They are easy to generate and can penetrate through buildings. The sending & recieving antennes has to be alligned.

2) Microwaves

It is line of sight transmission.

Used in mobile phone communication and television distribution

3) Infrared waves

Infrared waves are used for very short distance communication.

Used in TV remotes, wireless mouse etc.

- Computer Network Devices

1) Repeater

It operates at a physical layer. Its job is to regenerate the signal over the same network before signal becomes too weak or corrupted.

An important point to be noted about repeaters

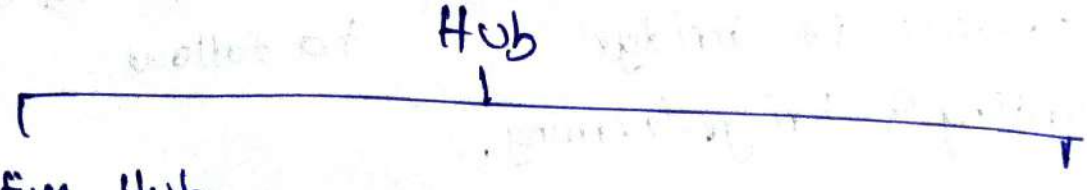
is that they donot amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at original strength. It is a 2 port divice

2) Hub

It is basically a multiport repeater. A hub connects multiple wires coming from different branches.

Eg: Connecter in star topology.

* Hubs cannot filter data, so data packets are sent to all connected devices.



Active Hub

These are hubs which have their own power supply and can clean, boost and relay the signal along the network. They provide path for the data signals also regenerate, strengthen the signal before sending them to destination.

Passive hub

They collect power from active hub. They do not modify the signals.

3) Bridge

Bridge operates at data link layer. Bridge is a repeater with add on functionality of filtering content by reading the MAC addresses of source and destination. It has single i/p and o/p port making it a 2 port device.

Bridges

- Transparent Bridges
  - *Bridges in which the stations are completely unaware of the bridge's existance.
  - * These bridges makes use of two processes i.e bridge forwarding & bridge learning.
- Source Routing Bridges.
  - In these bridges, routing operation is performed by source station and the frame specifies which route to follow.

4) Switch

A switch is a multiport bridge with a buffer and an design that can boost its efficiency (Large no of ports ⇒ less traffic) and performance. Switch is a data link layer device. Switch can

perform error checking before forwarding data. It forwards only data which is error free making it more efficient.

5) Router

A router is a device like switch that routes data packets based on their IP addresses. Router is mainly network layer device. Routers normally connect LAN and WANs together

6) Gateway

A gateway is a passage to connect two networks together that may work upon different networking models. They basically work as ~~message~~ messenger agents that take data from one system, interpret it and transfer it to another system.
They are also called PROTOCOL CONVERTERS.

7) Brouter (Bridge + Router)

It is known as bridging router.
It can work either in data link layer or physical layer. Working as router, it is capable routing packets across the network.

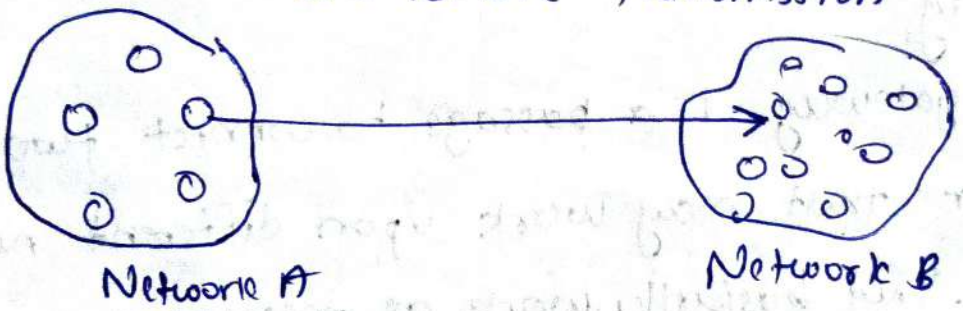
working as bridge, it is capable of filtering local area network traffic.

- **Unicast, Multicast & Broadcast Communication**

cast → means data is being transmitted ~~from~~

[1] Unicast Communication

* Single sender and single receptant
* Called one-to-one transmission



[2] Broadcast

* one to all transmission

- **Limited Broadcasting**

~~Suppose~~ ~~given~~ Data is transmitted from single source host to all other hosts residing in the same network.

- For this to achieve, it will append 255.255.255.255 called as Limited Broadcast Address in destination address of datagram header.

- Directed Broadcasting

  Transmits data from one source host to all other hosts that exist in some other network.

3) Multicast

One/more senders and one/more recievers participate in data transfer.

It is used in internet streaming of audio or video teleconference, sending email to group of people.

- Network Topology

Topology: It describes the methods in which all the elements of network are mapped. The topology term refers to the physical and logical layout of a network.

Topology

Physical Topology

↓

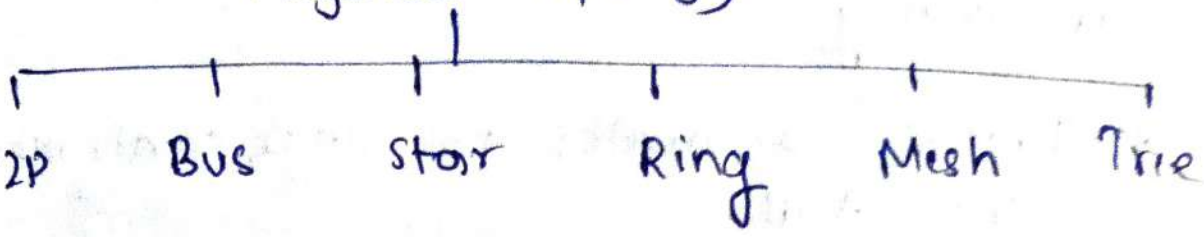
Layout of the computer cables and other network devices

Logical Topology

↓

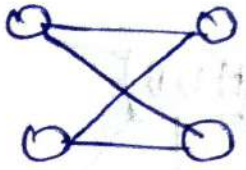
It gives insights about networks physical design.

Physical Topology



1) P2P

* Network consists of direct link b/w devices



Advt

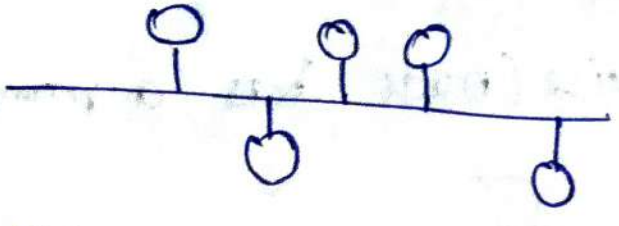
* ↓ cost
* ↓ maintanance
* ↑ Reliable & faster
* Doesnot need an expensive server as individual stations are used to access the ring

Disadvt

* Only used for small network
* Cannot backup files & folders centrally

2) Bus topology

* All nodes are connected to single bus
* Data from source → to all devices, only intended reciever whose physical address matches recieves data.



Advt

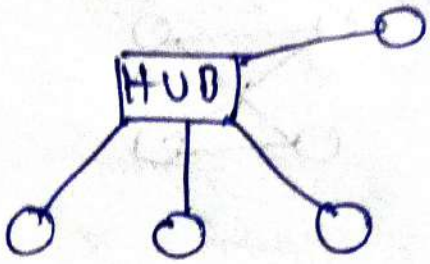
* Easy installation
* ↓ cable & ↓ cost
* Widely used in small networks

Disadvt

* If bus fails → Entire system fails
* ↓ security

[3] Star topology

* All node → connected to singe controller called HUB
* All devices are not directly linked to one another. They are indirectly connected through hub



Advt

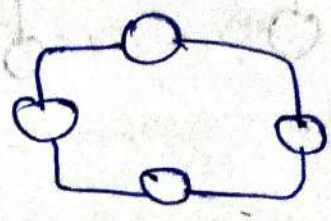
* ↓ Expensive
* Easy to install
* Addition & deletion of devices is easy

Disadvt

* Hub fails → Entire network fails
* ↑ cable length
* No of node depend on capacity of the hub

[4] Ring topology

* Each node is connected to next node
* Data travels in one direction until reciever is reached
* Each device/node has a repeater



Advt

* Easy installation
* Fault detection is simple
* Faster error checking & acknowledgement

Disadvt

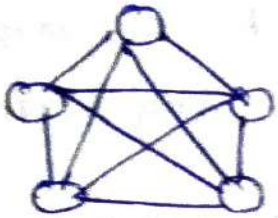
* Troubleshooting difficult
* Unidirectional traffic
* 1 Fault stops all transmission
* Slower

5) Mesh topology

* All devices connected to each other. It develops P2P connection b/w all devices.

$n(n-1)$ channels for n devices

$\frac{n(n-1)}{2}$ duplex links



Advt

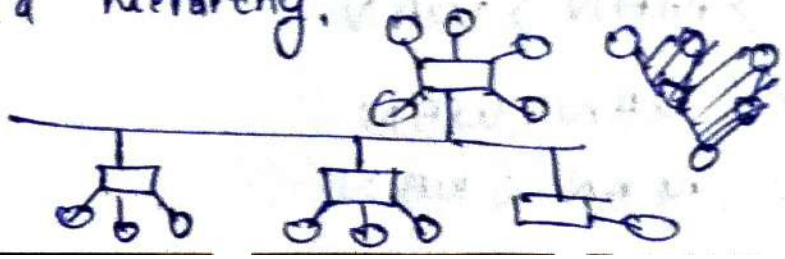
* Congestion reduced
* Faster
* Secure
* Easy fault detection
* Robust

Disadvt

* ↑ cable length
* Difficult installation
* Expensive
*

6) Tree topology / Hierarchial topology (Bus + Star)

Has a root node and all others are connected in a hierarchy.



Advt

* Failure of 1 node doesnot affect other nodes
* Node expansion is easy
* Easy to manage

Disadvt

* Cable length

- **LAN, WAN & MAN**

LAN: Local area network. It is a group of network devices that allow communication b/w various connected devices. Private ownership has control over LAN. It covers small areas like office, school etc. using ethernet, wifi etc.

MAN: Metropolitan area network. It covers larger area than LAN such as town, city. Ownership can be private or public

WAN: Wide area network. It covers larger area than MAN such as country or continent or whole globe. It is expensive and might not be owned by one organization. Connected using optic fibres PSTN or satellite is used for WAN's.

Speed: LAN > MAN > WAN

propogation delay: LAN < MAN < WAN

congestion: LAN < MAN < WAN

WAN

SONET
(Synchronous Optical Networking)
↓
uses optic fibres to carry data

Frame relay
It is a way to connect your LAN to WAN

- **OSI Model**

* Open system Interconnection model.
* Communication b/w computing system are split into seven different abstraction layers

Physical Layer, Data Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer, Application Layer

* It was developed so that there is some standard way about how two or more computers communicate with each other.

OVERVIEW OF ALL LAYERS

- **Application Layer**

  * Related to software (web or android)
  * Interaction b/w application and user.

  Eg: whatsapp, amazon website etc.

Say you send a message to another user

The message is sent to presintation layer

- **Presentation Layer**

  It will get whatever data is sent from application layer and convert into machine readable format. (binary) → Called **Translation**

  The translated data is encrypted and provides abstraction.

In this layer data from application layer is translated → encrypted → compressed and sent to session layer

- **Session Layer**

  It helps in setting up and managing connections between different computers.

  A session b/w machine is set up, managed and terminated.

  Before a session is established, it does authentication,

Eg: When you try to place an order on amazon.

Before placing order ⟶ It ask you your login credentials

↓

Authentication

After you log in, a session is create b/w your computer and the amazon server → You place order → session is terminated.

~~• Transport Layer~~

- Transport Layer

It has its own protocol of how data will be transferred ~~from sender to receiver~~. (TCP and UDP)

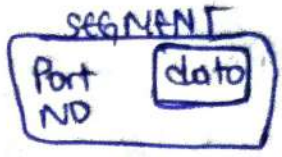
TCP and UDP employ different strategies on how data streams are transferred.

This layer is responsible for SERVICE TO SERVICE DELEVERY

Transport Layer is also responsible for distinguishing network streams. At a given time on a user's computer there might be an Internet browser open, while music is being played, while a chatting app is open. Each of these applications are sending and recieving data from the internet and all this data is arriving

in the form of 0's and 1's.

Something has to exist ~~which~~ in order to distinguish which 1's and 0's belong to the messinger or the browser or music.



This is done by this layer.
The data ~~[redacted]~~ are divided into segments which contains source & dest port no's & sequence no

- Network Layer

It is responsible for transmission of recieved data segment from one computer to another that is located in a different network.

Till now (Application → Transport Layer) we were talking about our own network. Talking about network layer we talk about communicating with computers in other network.

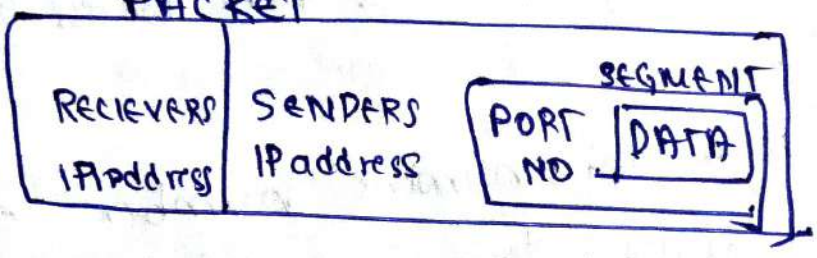
Routers are network devices that operate in this layer. Its primary responsibility is to facilitate communication b/w networks.

How does network layer do this?

Using logical address i.e IP addresses (Internet Protocol Address)

It helps logically identify each node present / connected to the internet. It is considered logical because IP address is not permanent identification of a computer. Unlike the MAC address which is considered a physical address, IP add is not borned into any computer by manufacturer.

Network layer assigns senders and recievers IP address to every segment and forms an IP Packet so that every segment reaches the correct destination.



- It also performs Routing → Moving one data packet from source to destination.

Network layer is responsible for END to END DELEVERY using logical address

- Data Link Layer

Data link layer works with physical addressing ie MAC address. (Media Access Control address)

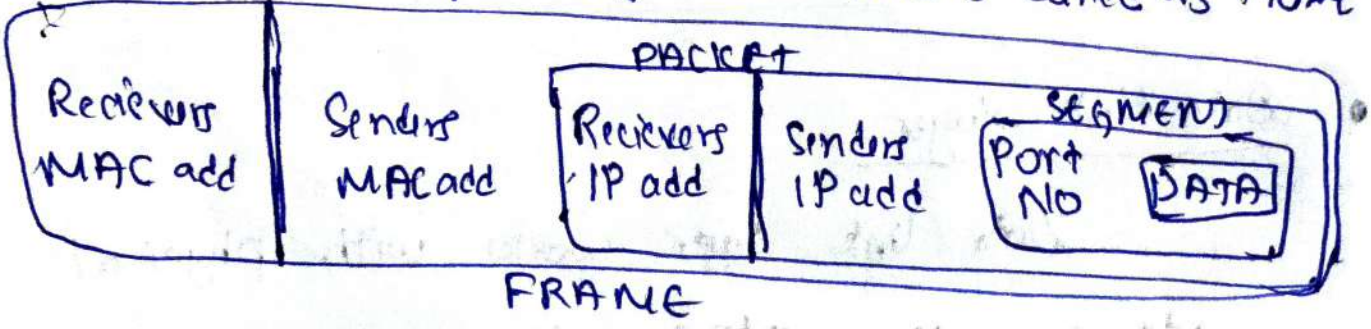
Data link Layer is responsible for interfacing with the Physical Layer

The Network Interface Card (NIC) that is plugged in with Ethernet wire handles Data link Layer functionality. It recieves signal from wire and transmit signals to the wire.

The MAC Address uniquely identifies each individual NIC Each NIC is pre configured with a MAC address by the manufacturer.

MAC is a 12 digit alpha numeric number of network interface of a device. Your computer doesnot have only one MAC address, its WIFI has one MAC address, its bluetooth has another MAC add etc.

The data link Layer adds sender's and reciever's MAC address to the packet. This is called as frame



Layer is Responsible for HOP to HOP transmission

- Physical layer

  * This is the hardware section (wired / wireless).
  * It carries traffic between two nodes.
  * It is anything that carries bits (0 or 1) between two nodes.

  wired → Ethernet → carries bits in form of electric pulses

  wireless → WIFI → Carries bits in form of radio waves

Apart from wires and cables, repeaters and hubs also work in this layer.

Network Layer (L3) Vs Data Link Layer (L2)

Layer 3 / Layer 2

Differentiating these two layers is quite confusing. For example if we already ~~know~~ have a unique L2 addressing scheme on every NIC (like MAC address) why do we need another addressing scheme at L3 (IP address) or vice versa?

The answer is that both addressing schemes accomplish different functions

DLL → uses MAC address and is responsible for packet delivery from hop to hop

NL → uses IP address and is responsible for packet delivery from end to end

when a computer has data to sent, it encapsulates it in a IP header which will include information like the source and destination IP address of two 'ends' of communication.

IP header and data are further encapsulated in a MAC address header, which include source and destination MAC address of current 'hop' in path towards final destination

Between each router in the network, MAC address header is stripped and regenerated to get (it) to the next hop.

The IP address generated by the first computer is only stripped off by the final computer.

Hence IP address handles end to end delivery
MAC address handled hop to hop delivery

Each layer assumes that it is talking to same layer of other computer.

Eg: Session layer thinks that it is talking to session layer of other computer

- Key Players

1 Host

Host is generic term that implies any sort of end device on internet. (Any device in internet is host)
Eg: TV, washing machine, laptop etc.

In typical internet communication, two hosts in communication are often labled Client or Server.

- Client → Entity initiating request
- Server → Entity serving request.

2 Network

Network is simply two or more connected devices. Depending on purpose of each network, the devices within them will communicate with other devices in the same network or devices in other network.

Internet is nothing but series of interconnected network.

3 Switch

It is a device whose primary purpose is to facilitate communication within the network.

Switches operate in layer 2 (DLL).

A switch operates by maintaining MAC address table. It maps MAC addresses of devices plugged into each switch port. A switch has many ports from 24 to 48 upto 96 or more.

MAC address table is populated by looking at source MAC address field of any recieved frame.

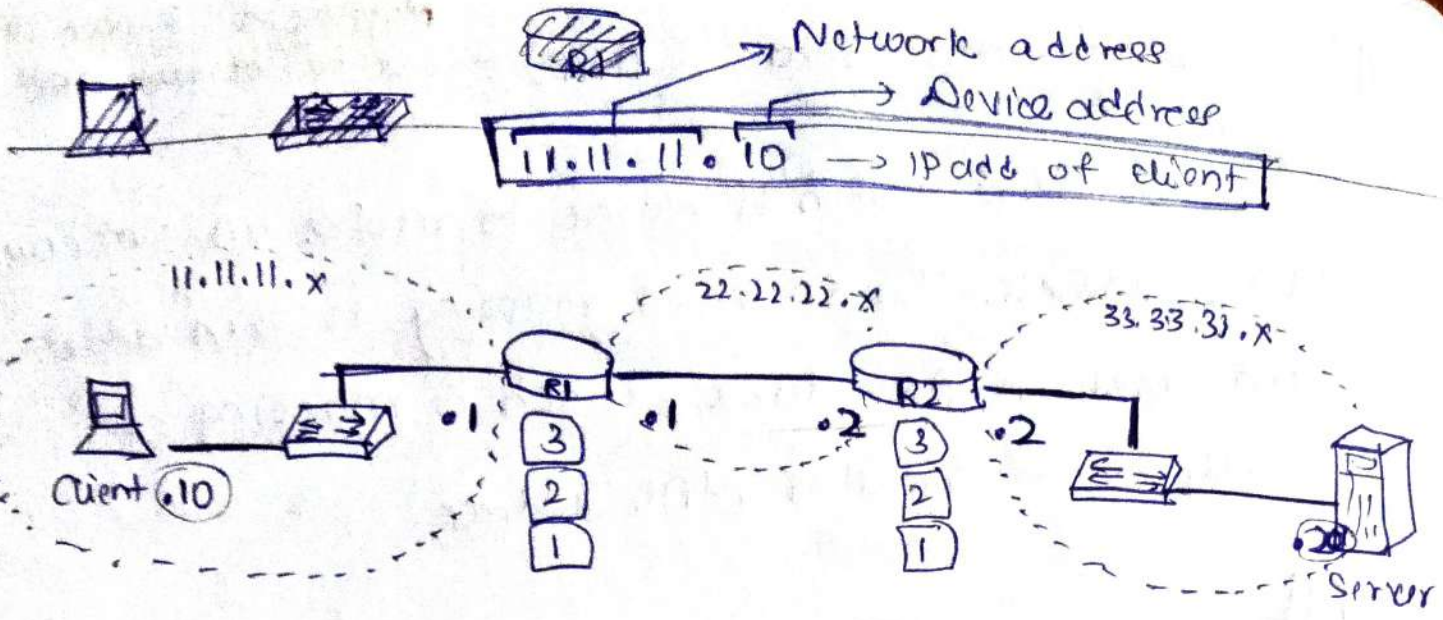
Inorder to forward the frame, the switch will lookup at ~~Source~~ Destination MAC address in MAC address table to determine what port to use.

If switch encounters a frame which it doesnot know the location of destination MAC address, it simply duplicates and floods the frame out each switch port (except the port it was recieved on)

4 Router

Its primary purpose is to facilitate communication between networks. Each interface on a router creates a network boundary.

Routers at Layer 3 (Network).



R1 and R2 (Routers) create 3 separate networks (11.11.11.x, 22.22.22.x and 33.33.33.x). R1's right interface and R2's left interface are both same networks.

The only way for Client in 11.11.11.x to speak to server in 33.33.33.x network is to forward packet to R2, which will finally forward this packet to Server.

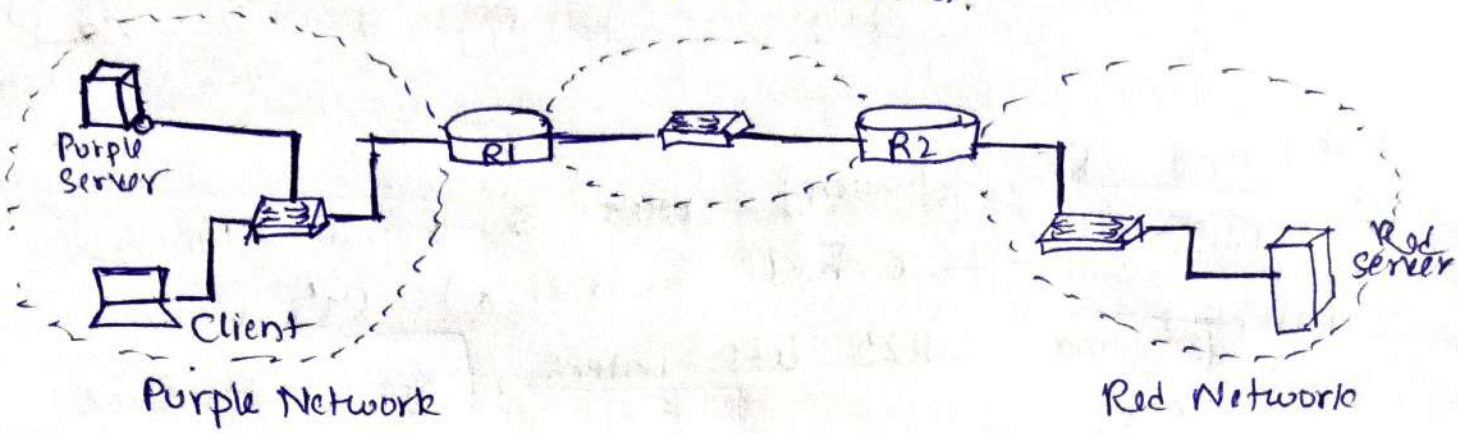
A router accomplishes all this by maintaining Routing Table This is a table that contains paths to all the networks a Router knows. These paths are called Routes.

From the perspective of router, the Routing Table is a map of every network that exists. If a router recieves a packet destined to a network it doesnot know, then as per router that network ~~that~~ doesnot exist. ⇒ the packet is discarded.

5 Address Resolution Protocol (ARP) –

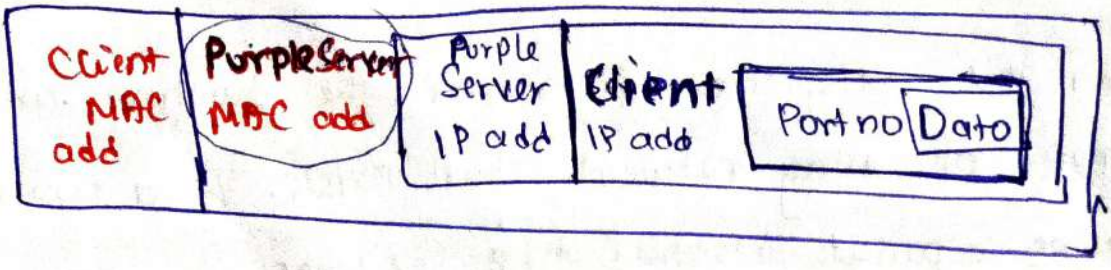
Mapping of known IP add to unknown MAC address

ARP uses a known IP address to resolve an unknown MAC address. The discovered mapping is then added and stored in ARP table, which is mapping of IP address to correlated MAC address.



1) host speaking to another host in same network

When client needs to speak to purple server, it will know Purple Servers IP address and from that it will determine that Purple Server exists in local network. When client is attempting to speak with a host in same network, the client will issue an ARP request for ~~host~~ host's MAC address

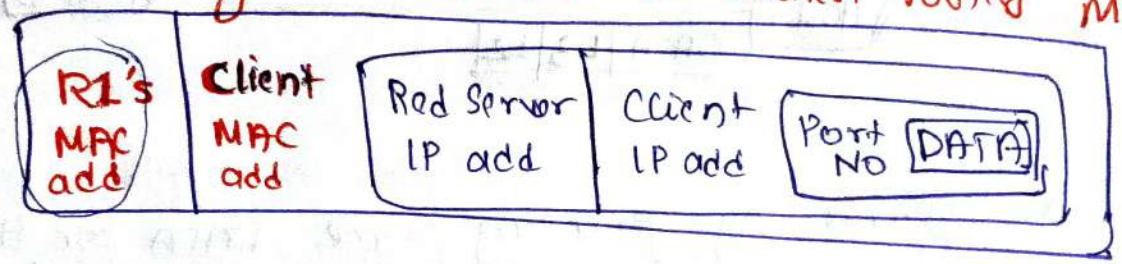


2) host speaking to another host in another network

When Client needs to speak with Red Server, it will know IP add of Red server from which it will get to know that Server exists in foreign network. Implies the packet must be delivered to nearest router

This is called as DEFAULT GATEWAY

When a client is trying to speak to host in a foreign network, the Client will issue an ARP request for Default Gateway's MAC address ie nearest router MAC add.



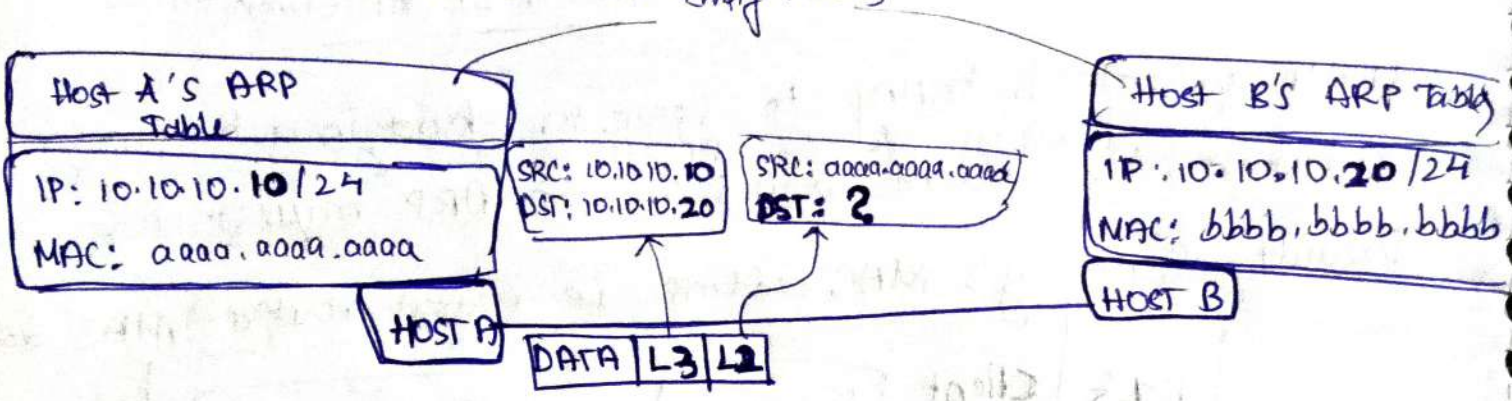
ARP's Role is to create proper L2 header (MAC) based on L3 header (IP) to get packet from one hop to next hop

HOW A PACKET TRAVELLS

VVVIP

1) HOST TO HOST COMMUNICATION

In this section we are discussing about communication happening within the network. Therefore Host A & Host B are configured with IP addresses that belong to the same network.



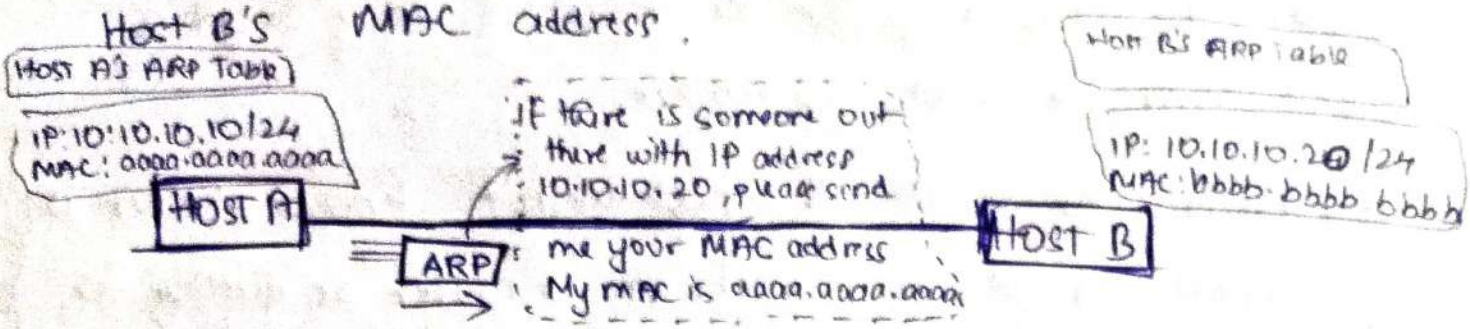
Host A starts by generating some DATA for Host B. Host A knows final destination for data will be the IP address 10.10.10.20 (Host B). Host A knows its own address (10.10.10.10), and is able to create L3 header.

But packet delivery is job of layer 2, despite hosts being connected to one another over the same network, L2 header must be created.

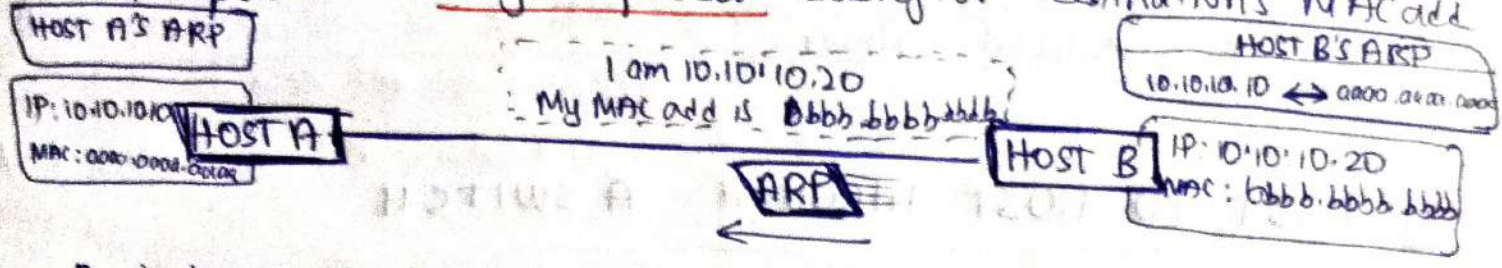
Source of L2 header: HOST A's MAC address → Known

Destination of L2 header: Host B's MAC address → Host A does not have entry in its ARP Table. ⇒ Host B's MAC address is unknown.

Host A will initiate an ARP Request to acquire Host B's MAC address.



ARP request is a single packet asking for destination's MAC add

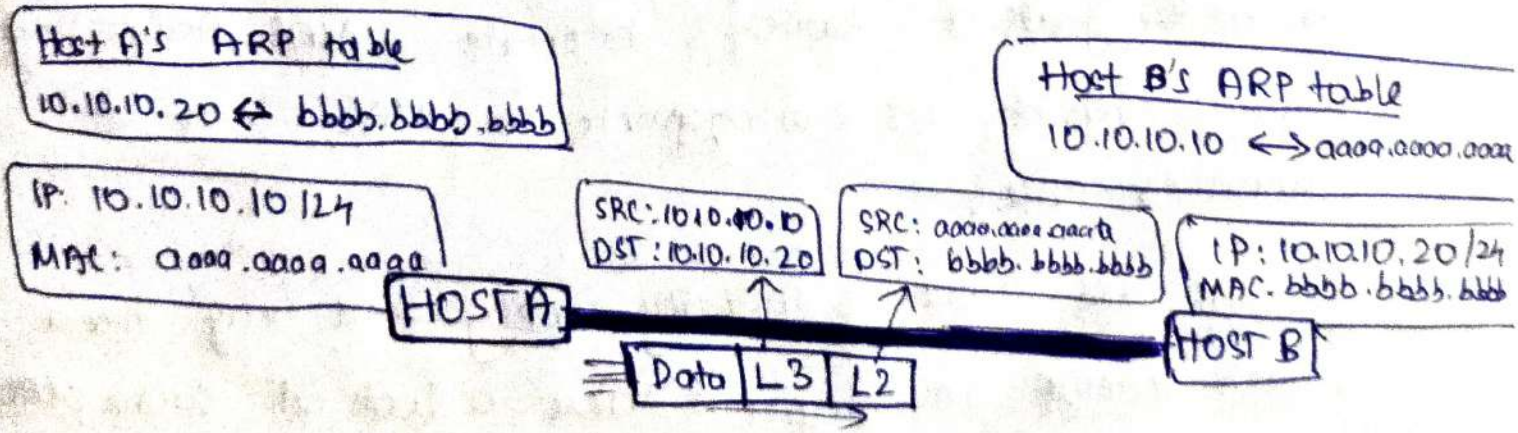


Receiving an ARP request allows Host B to know that Host A's IP add is 10.10.10.10 and MAC add is aaaa.aaaa.aaaa. This entry is added to Host B's ARP table. Host B uses this information to directly reply to A. ARP Request is sent as Unicast Message directly to Host A's address.

ARP response information that HOST A Requested:

MAC address is bbbb.bbbb.bbbb for IP address 10.10.10.20

Host A will update its ARP table with this information



It is rare to find two hosts directly connected to each other (As in this case). But we understood how to get a packet from one host to another.

KEY THING TO NOTE IS host doesn't know whether it is connected to a switch or a router or directly to another host. In either case, host will follow the same procedure discussed above

2 HOST TO HOST THROUGH A SWITCH

SWITCH FUNCTIONS: Learning, Flooding, Forwarding & Filtering

- Learning

Being a layer 2 device, a switch will make all decisions based upon information found in the L2 header.
It will use Source & Dest MAC address to make forwarding decisions.
One of the goals of switch is to create a MAC Address Table mapping each of its switch ports to MAC address of connected devices
The MAC add Table is initially empty and every time a switch receives anything, it takes a look at Source MAC address of incoming frame. It uses Source MAC address

and switch port the frame was recieved on to build an entry in MAC address Table.

After the Table is populated, it can be used to smartly forward frames to intended destination.

- Flooding

However dispite of learning process, it is unavoidable that a swith recieves a frame destined to a MAC address of which the switch doesnot know the location. In such cases, Switch only option is to simply duplicate the frame and sent it out all ports. → FLOODING

It assures that if intended divice existe and is connected to the switch, it will definately recieve the frame.

When intended reciever recives the frame, a response will be genrated which when sent to the Switch will allow to learn and create a MAC Address Table mapping of that unknown divice to switch port.

- Forwarding

There are 3 methods of forwarding frames

1) Store & Forward :- The switch copies the entire frame (header + data) into a memory buffer and inspects the frame for errors before forwarding it.

This method is the slowest but allows for the best error detection and additional features like prioritising certain types of traffic for faster processing.

2) Cut-Through : The switch stores nothing and inspects only the bare minimum required to read the destination MAC address, and forwards the frame. This method is the quickest but provides no error detection or additional features

3) Fragment-Free : This is blend of the above two. The switch inspects only the first portion of the frame (64 bytes) before forwarding the frame. If transmission error occured, it is typically noticed within the first 64 bytes. As such, the method provides good enough error detection, while gaining the speed and efficiency of avoiding storing the entire frame in its memory before forwarding it.

In modern days, with line-speed-switching, the difference in the speed between these 3 methods is negligable. Most of the switches operate in Store & Forward mode.

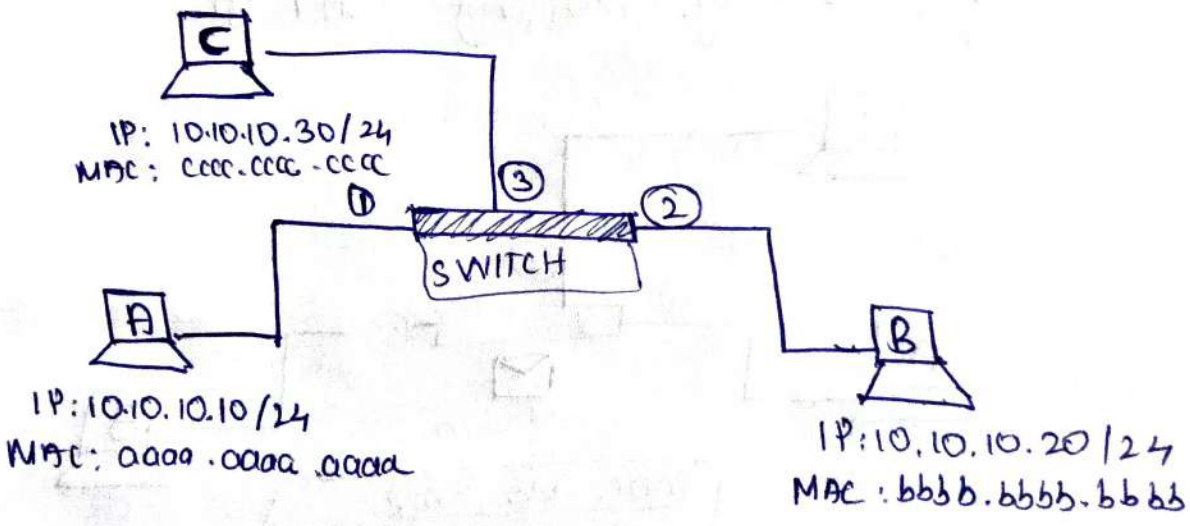
- Filtering

Switch will never forward a frame back to the same port which recieved ~~to~~ the frame.

Most commonly, this happens when Switch needs to flood- the frames will get duplicated and sent out every switchport exapt the switchport which recieved the frame.

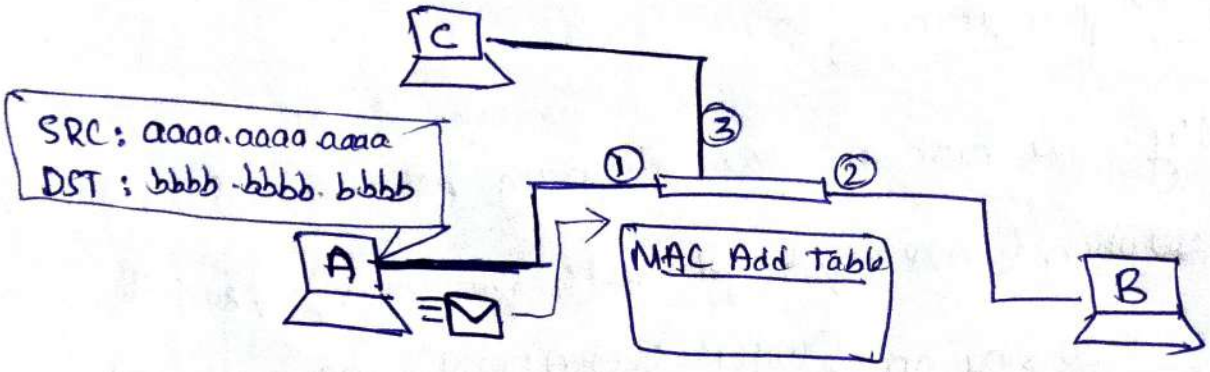
Switch Operation

originally, the host in the diagram below need to perform ARP resolution (ARP req to get dest's MAC add), but for sake of focusing on SWITCH OPERATION, we will skip ARP and ~~focus~~ proceed as if all the hosts already knew each others IP and MAC address.

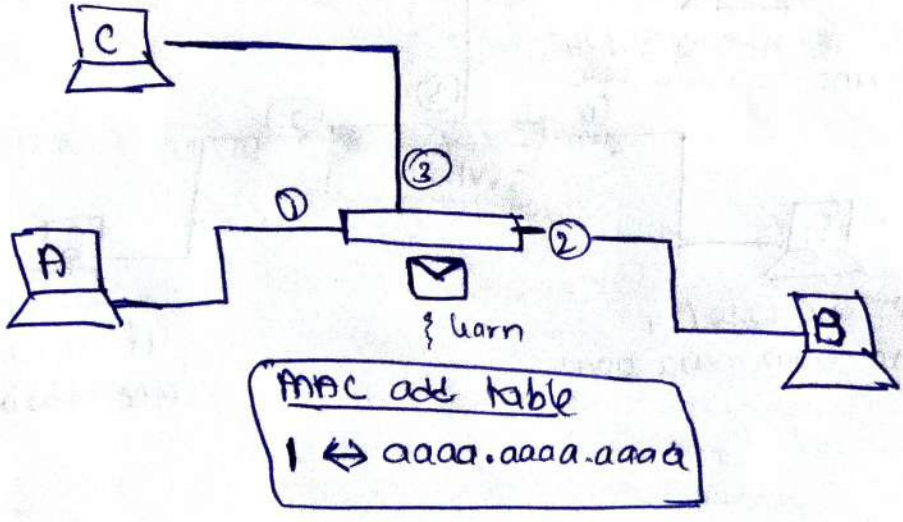


Host A has "something" to sent to Host B. The Contents of "something" is entirely irrilavent so as long its understood that the frame has L2 header which issues Source and Dest MAC address.

Initially MAC Address Table of Switch is empty, it only gets populated when frame is recieved.

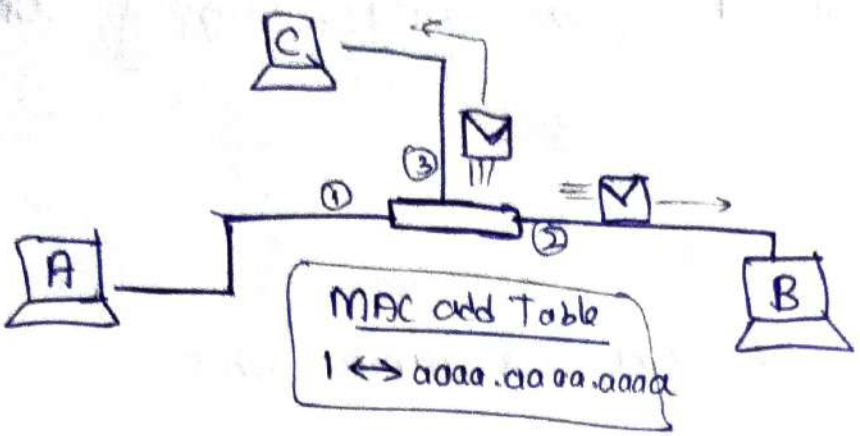


Host A sents a frame to switch, it includes a Source MAC address of aaaa.aaaa.aaaa. This prompts the switch to **learn** a MAC add Table entry mapping Port 1 to aaaa.aaaa.aaaa

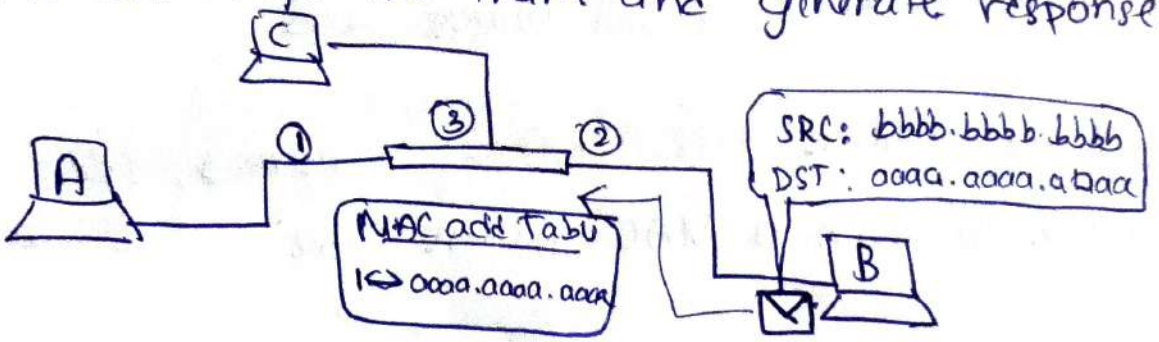


Now we decide how to forward the frame, the switch has no entry to bbbb.bbbb.bbbb in table. The switch

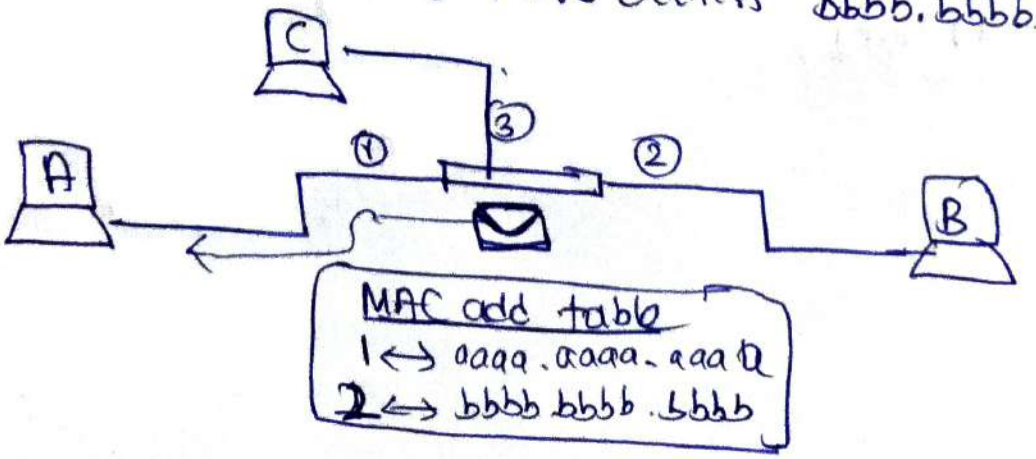
duplicates and **floods** the frames out all ports.
It is duplicated to all ports except port 1 - **filtering**.



The frame will be recieved by host C and host B.
Host C when inspecting the L2 header will realize the frame is not intended for it and will simply discard it, When Host B recieves the frame and realises the frame is intended to it, it will accept the frame and generate response.



When response arrives on switch, another MAC address mapping is learnt: Port 2 contains MAC address bbbb.bbbb.bbbb.



The switch looks at the destination MAC address (aaaa.aaaa.aaaa) and realizes that this address exists out Port 1. The switch simply forwards the frame.

- **Broadcasts**

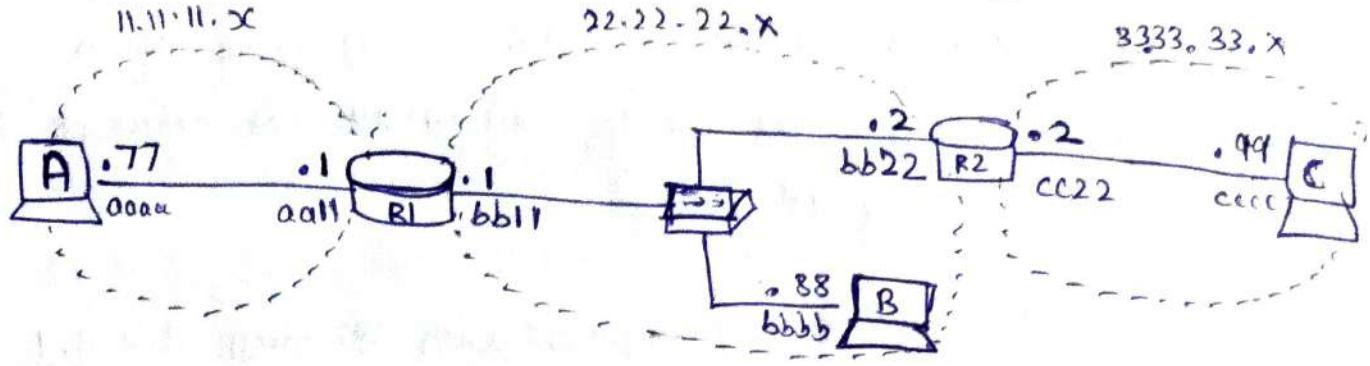
A Broadcast frame is a frame which is addressed to everyone on the local network. This is done using the same Ethernet header, except the Destination Mac address is populated with ffff.ffff.ffff ⟶ this address is specially reserved for broadcasting.

If switch recieves a packet with destination MAC address of ffff.ffff.ffff, it will always flood the frame.

Since the address ffff.ffff.ffff is reserved, the switch is unable to learn a MAC Address Table mapping for it.

In Sommary, a Broadcast is a frame addressed to everyone on the local network and Flooding is an action a switch can take.

[3] HOST TO HOST THROUGH A ROUTER



- **Router Functions**

Routers primary purpose is to facilitate communication between networks. As such, every router creates a boundary between two networks, and their main role is to forward packets from one network to next.

In order to forward packets b/w networks, router must perform two functions

1) Populate and maintain a Routing Table
2) Populate and maintain an ARP table.

- **Populating Routing Table**

Routing table is a map of all networks in existance The table starts empty and learns of new routs to each network and populates the table.

There are many ways a router can learn the routs to each network.

1) The simplest method is known as **Directly Connected Route**.

Essentially when a Router Interface is configured with particular IP address, the router will know the network to which it is directly attached.

Eg: R1's left interface is configured with IP address 11.11.11.1. This tells R1 the location of the 11.11.11.x network exists out its left interface. The same way, R1 learns that the 22.22.22.x network is located on its right interface.

The above method is useful when network is directly connected. When networks are not directly connected we use other ways.

2) Another way is known as **Static Route**. A static route is a route which is manually configured by an Administrator. It would be as if you explicitly told R1 that 33.33.33.x network exists behind R2, and to get to it, R1 has to send packets to R2's interface (22.22.22.x).

In the end, after R1 learned of the two directly connected routes, and after R1 was configured with one static route R1 would have 'routing table which looks like this.

R1's Routing Table

Method	Network	Interface / Next hop
DC	11.11.11.x	Left
DC	22.22.22.x	Right
Static	33.33.33.x	22.22.22.2

Everytime a router recieves a packet, it will consult Routing Table to determine how to forward the packet.

If a router recieves a packet destined for a network it doesnot have a route for, then as far as the router is concerned that network must not exist. ⇒ Packet is discarded

3) There is a third method known as Dynamic Routing. This involves the routers detecting and speaking to one another automatically to inform each other of their known routes. There are various protocols each representing different strategies. (Dijkstras algo, Bellmanford algorithm)

The routing table will tell the router which IP address to forward the packet to.

But packet delivery is always job of Layer 2. And in order to create the L2 header which will get the packet to next L3 address, the router must maintain an ARP table. → Because Routing is Based on IP address (L3) and to forward packets we need MAC address.

• Populating an ARP Table

ARP is a bridge b/w layer 2 and layer 3. When provided with an IP address, ARP resolves the correlating MAC address. Devices employ ARP to populate ARP table or sometimes called ARP cache.

A router will use its Routing table to determine next IP address which should recieve a packet. Using ARP ~~protocol~~ resolution we will obtain MAC address to that IP address.

Unlike the routing table, the ARP Table is populated only when needed. For example R1 will not initiate an ARP request for HOST B's MAC address until it has a packet which must be delivered to HOST B.

When ARP Table is populated it will look like

R1's ARP Table

IP address		MAC address
11.11.11.77	⟷	aaaa
22.22.22.88	⟷	bbbb
22.22.22.2	⟷	bb22

How will the table get filled?

We discussed earlier how ARP ~~req~~ resolution is done b/w two hosts belonging to different network.

First Host A does ARP resolution with RT.
R1 does it with R2 and Host B.
R2 does it with Host 3
~~INTERFACE REQUIRED~~

• ROUTER OPERATION

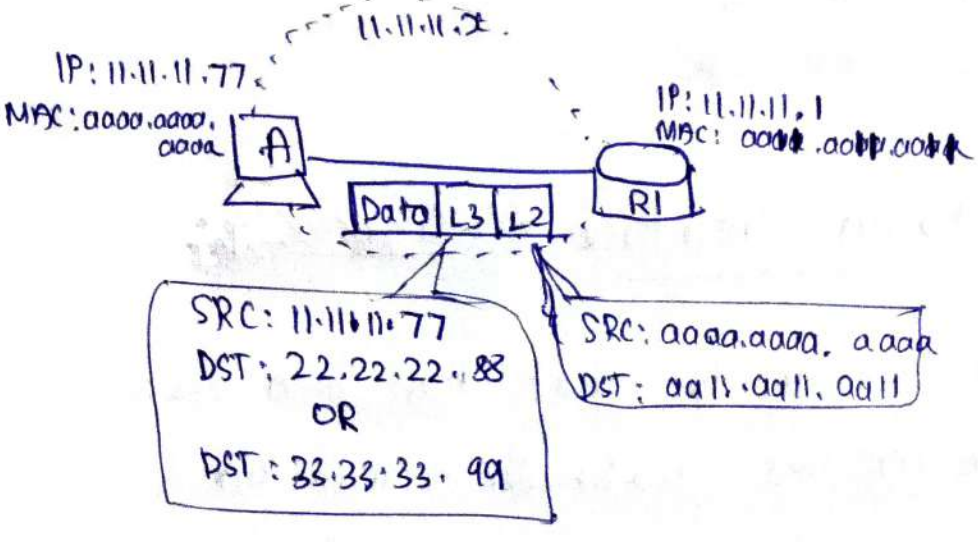
We can know how these two tables are used practically for communication b/w networks.
↳ ARP & Routing Tb

In R1's routing table above, you can see there are two types of routes.

1) pointing to an interface (Left/Right)
2) pointing to next hop (Next router)

First let us discuss how Host A delivers Packet to Default GATEWAY (R1). Then we will Look at what R1 does with packet sent from Host A → Host B and then another packet from Host A → Host C.

1) HOST A GETTING PACKET TO R1



Host A will create L3 Header with Source IP address (11.11.11.77) and Destination IP address (22.22.22.88 (for Host B) or 33.33.33.aa (For Host C). This L3 header will serve the purpose of getting data from end to end

Host A will encapsulate the L3 header in a L2 header which will include Source MAC address aaaa.aaaa.aaaa and Destination MAC address aall.aall.aall. This L2 header will serve the purpose of getting data ~~from Hop to Hop~~ across first hop

The above happens if Host A already has ARP Table entry with R1's MAC address. Else forming L2 head would have been preceded with an ARP request to discover R1's MAC address.

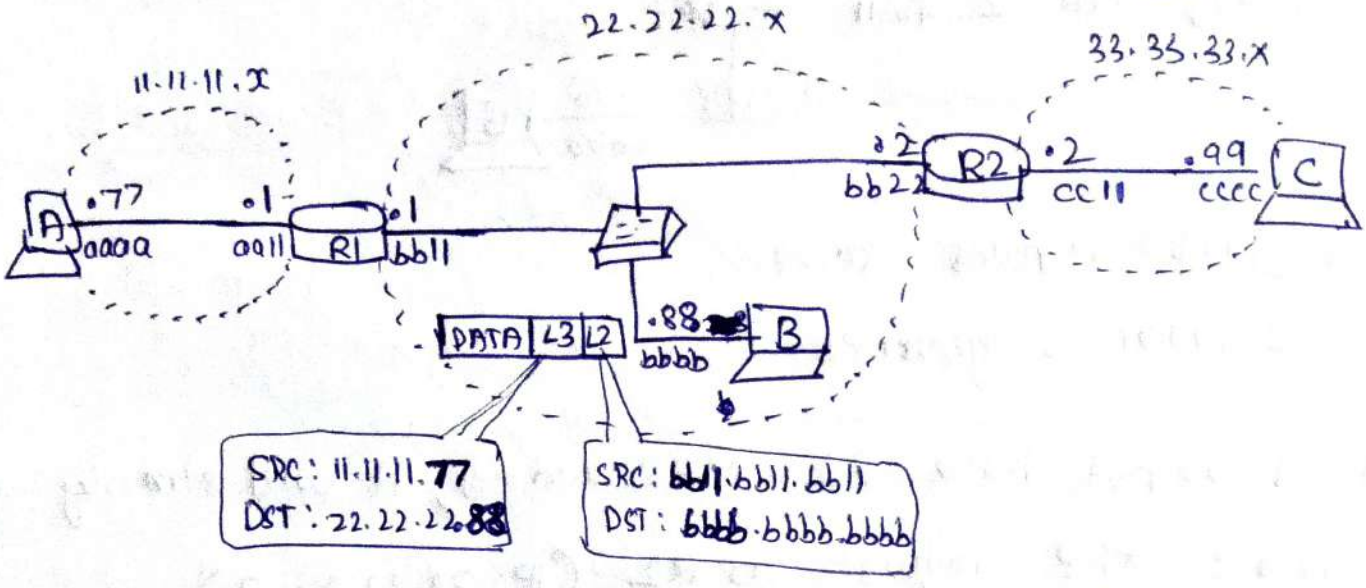
At this point R1 will have the packet. Both destination's (Host B & Host C) exist in R1's Routing table.

To Host B → Points to interface
To Host C → Points to next Hop.

(2) Routes Pointing to an Interface

The process is similar to what has been discussed before. The Router uses L3 Header information to determine

where to send packet next, then creates a L2 header to get it there. In this case the next (& final) hop this packet must take is to the NIC on Host B.



The L3 header will remain unchanged.

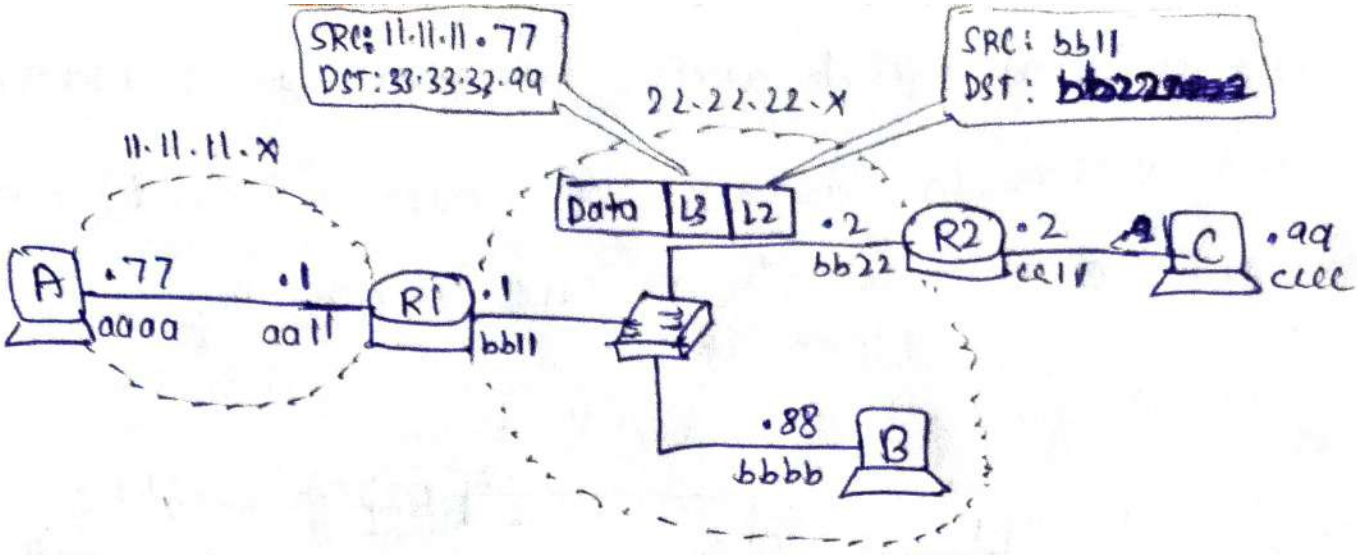
L2 header gets updated with SRC = MAC add of R1 (bb11) (Right interface of R1 (as shown in Routing Table))

DST = MAC add of Host B (bbbb)

2.2 Router Pointing To Next-hop address

For the packet from Host A → Host C, the Destination IP address will be 33.33.33.99. When R1 consults its Routing table, it determines that the next hop for the 33.33.33.[redacted]X network exists at IP address 22.22.22.2 - R2's left interface.

Effectively, this tells R1 to use a L2 header which will get packet to R2 in order to continue forwarding the packet



L3 header remains same

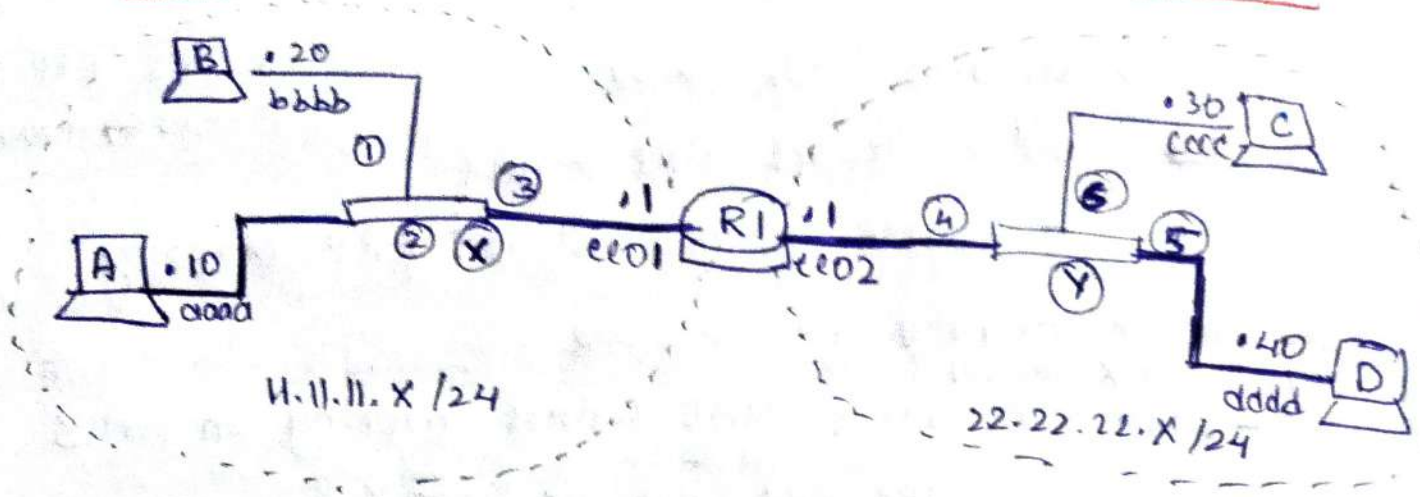
L2 header is regenerated

If R1 doesnot have R2's MAC address, it will simply generate ARP request to R2 (IP: 22.22.22.2).

As process continues R2 will recieve the packet and then be faced with same situation R1 was in for example above (HOST A - B).

This process continues. Had HOST A been trying to speak to Host * 10 routers away in the path, the process would have been identical.

- HOST → SWITCH → ROUTER → SWITCH → ROUTER



HOST A → HOST D

Before ~~the~~ ~~the~~ network handles traffic, Router must populate its Routing table with all paths.

Routing Table

Method	IP add	Interface / next hop
DC	11.11.11.X/24	Left
DC	22.22.22.X/24	Right

1. Host A has data for Host B
   - Host A already knows Host D's IP address
   - Host A creates L3 ~~ether~~ header
   - Host A needs to learn it Default Gateway (R1)'s MAC address
2. Host A sends an ARP request for 11.11.11.1 (R1)
3. Switch X received frame
   - Switch X learns MAC address mapping on port 2

2 ↔ aaaa ~~MAC address~~

- Switch X floods frame out of all ports (except 2)

4. Host B discards the frame

5. Router recieves ARP request

Router's ARP Map
11.11.11.10 ↔ aaaa

- Router learns HOST A's ARP Mapping

6. Router generates ARP response

7. Switch X recieves frame

8. - Switch X learns MAC address mapping on port 3

MAC Add Table for Switch X
2 ↔ [redacted] aaaa
3 ↔ [redacted] ee01

- Switch X forwards frame out port 2

8. Host A recieves ARP response

Host A ARP
11.11.11.1 ↔ eeee

- Host A learns Router's ARP mapping
- Host A creates Layer 2 header

9. Host A sends packet

10. Switch X recieves frame

- Switch X already knows mapping for port 3
- Switch X forwards frame out port 3

11. Router R1 recieves the packet and strips L2 header

12. Router consults Routing Table

- 22.22.22.X/24 networks on right interface
- Router needs to learn MAC address of 22.22.22.40

13. Router Sends an ARP request for 22.22.22.40

14. Switch Y recieves frame

- Switch Y learns MAC address mapping on port 4

MAC Add Table of Y

4 ↔ eeO2

- Switch Y floods frame out all ports (except 4)

15. Host C recieves frames and discards it

16. Host D recieves the ARP request

17. Host D generates ARP response
    - Host D learns R2's ARP mapping

Host D's ARP

22.22.22.1 ↔ eeO2

18. Switch Y recieves frame
    - Switch Y learns MAC address mapping on port 5

MAC add Table of Y

4 ↔ eeO2

5 → dddd

- Switch Y forwards frame out port 4

Routers ARP

11.11.11.10 ↔ aaaa

22.22.22.40 ↔ dddd

19. Router recieves the response
    - Router learns ARP mapping
    - Router creates L2 header

Router ARP

4 ↔ eeO2, eeO2

eeO2

20. Router sends frame to Host D

21. Switch Y recieves the frame
    - Switch Y already knows mapping for port 4
    - Switch Y forwards frame out port 5

22. Host D recieves the frame.
    - Host D strips L2 and L3 Header and recieves Data

23. Host D generates the Respons and it travels all the back to HOST A.

ALL layers in Detail

1) Application Layer

* Layer in which user interacts with each other
  Eg: Whatsapp, Browsers etc.
* Process sends a request to other process and recives a response.
* Process to process communication is duty of application layer.

Protocols of Appln layer

1) TELNET : TELetype NETworking. It allows Telnet client to access TELNET server. Used to manage files on internet, It is used for initial setup of devices such as switches
2) FTP : FILE TRASSFER PROTOCOL. It is a protocol that lets you transfer files.
3) SMPT : Simple Mail Transfer Protocol. It is a part of TCP/IP protocol. Using "store & forward" SMPT makes your email on and across network.
5) DNS : Domain Name System
   Whenever you use a domain name DNS server translate

the name into corresponding IP address.

6) SSH: When you want to login to a terminal you use SSH protocol.

~~etc~~

7) HTTP: Hyper Text Transfer Protocol

In server Client↔Server arechetectur, we know that client sends a request to server and server analyses the request and sends back the response to client.

Client sending request $\xrightarrow[\text{HTTP protocol}]{\text{uses}}$ HTTP request

Server sending response $\xrightarrow[\text{HTTP}]{\text{uses}}$ HTTP response

~~HTTP~~ methods

1) GET: Get something from server
2) POST: Client sending something to server (usir registration details)
3) PUT: Put something at spelfied URI. URI refers to an already existing resource.
4) DELETE: Delete something from server.

Status codes

1n100's: Informational
2xx: Success
3xx: Redirection purpose
4xx: Client error
5xx: Server error.

HTTP is a Stateless protocol. ie it doesnot save the client information/state, every time you visit a website, you are a completely new user to it.

- **Cookies**

HTTP is stateless protocol, but when you Login to Amazon and leave the website without logging out. and go revisit the website again later, you will find you are still logged in to Amazon. If HTTP is stateless, how is this happening → **Cookies**

It is a unique string stored in the browser. When you visit a browser or a website for the very first time, it will set a cookie. After that, whenever you make a request, in that request's header a cookie will be sent.

Eg: Your user value of a Website (Amazon).

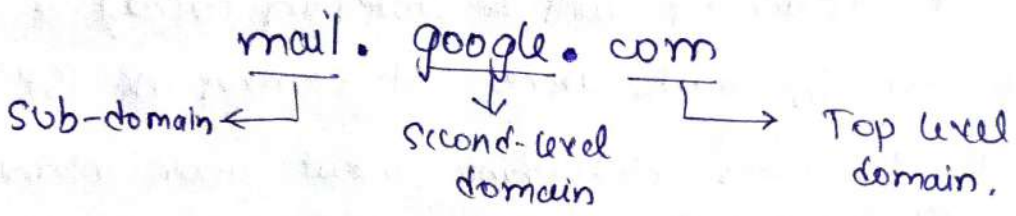
Each cookie has an expiry date.

• DNS (Domain Name System)

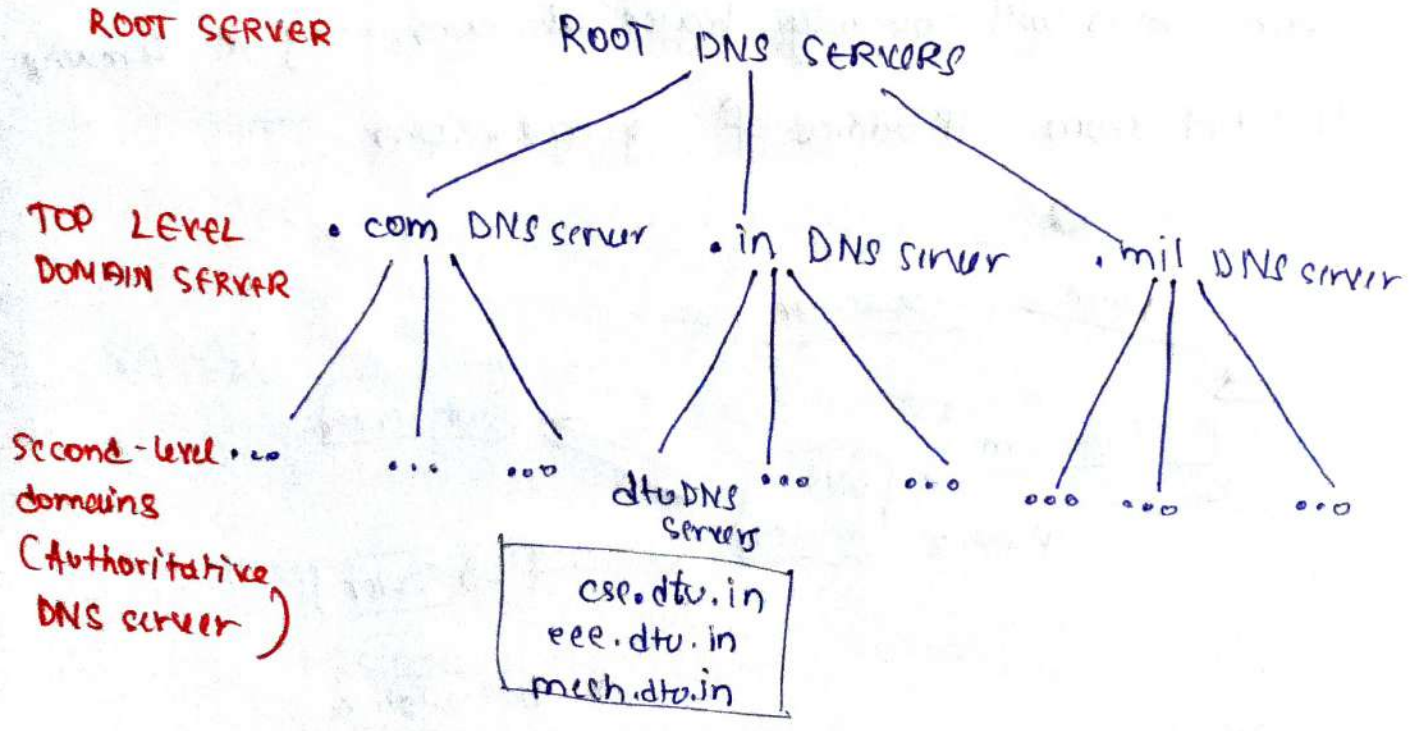
DNS is used to convert the domain name of websites to their numerical IP address.

1) Generic Domain: .com (commercial), .edu (educational),
.mil (military) .org (non profit organization)
.net (similar to commercial)

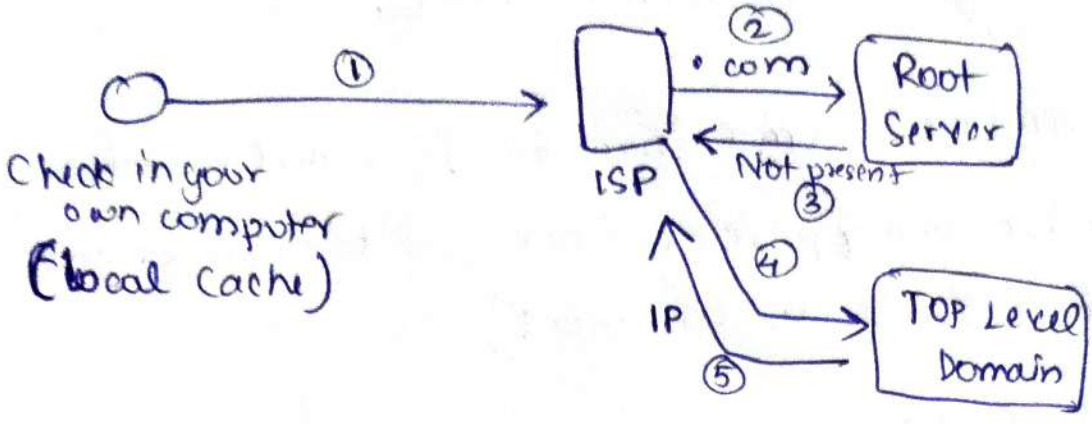
2) Country Domain: .in (India), .us, .uk



Instead of storing everything in a single database, we subdivide the task into a hierarchy



Whenever you search for a website say google.com, the following will happen



1) It checks in your own computer's local cache. (Whenever you visit a website, its IP address will be stored in cache)

2) If not present in local cache, it searches in ISP's server. (ISP knows everything about your internet activity, which website you visit etc)

3) If not present there, it will search in ROOT server.

4) If it is not present in Root server, it will search in TLD ~~which~~ which will obviously have all .com, .org etc domains TLD will return IP address of google.com

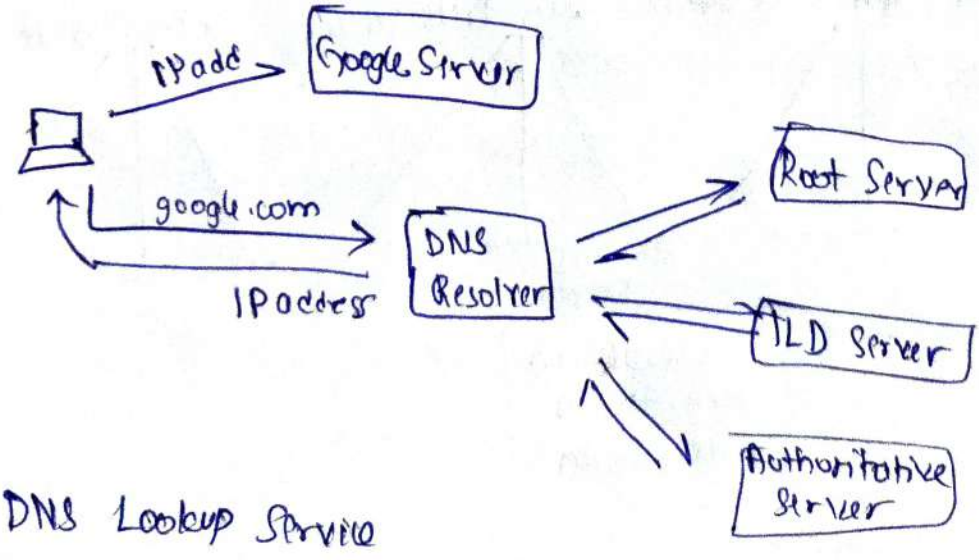


Fig: DNS Lookup Service

2) Presentation layer

It is mainly conserned with syntax and symantics of the data.

It does the following things

1) Translation :- User readable data ⇌ Machine Readable Code

2) Encryption : Encryption at sender & Decryption at reciever

3) Compression : To reduce size of data to be transmitted.

3) Session layer

It maintains and synchronises the interaction b/w two interacting systems. (As we discussed earlier using amazon.com example)

4) Transport layer

There is a very small difference b/w network and transport layer.

When you send a message to your friend. The transportation of message from you → your friend is done by NETWORK LAYER. But within your computer, transportation of data from application to network is done by TRANSPORT LAYER.

TRASPORTATION B/W COMPUTERS → NETWORK LAYER

TRANSPORTATION FROM APPLICATION TO NETWORK (WITHIN COMPUTER) → TRANSPORT LAYER

Protocols of Transport Layer — TCP (Wired)
UDP (Wireless)

Transport Layer is responsible for SERVICE TO SERVICE DELEVERY. By that we mean that it provide service to the upper layer applications, ensuring their data is delevered to the intended receptant in reliable and efficient manner

Other Responsibilities

1) Flow Control
2) Error control (CRC, checksum)
3) Congestion control (Leaky bucket & Token bucket algorithm)

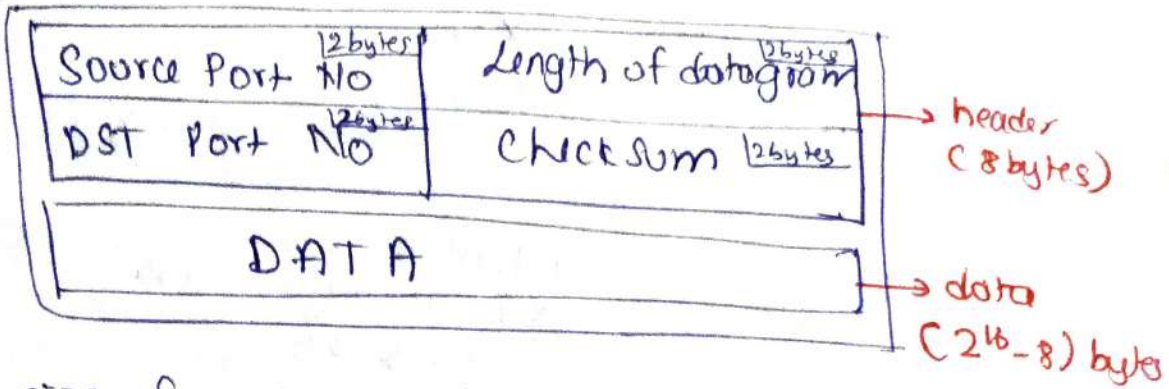
- UDP (User Datagram Protocol)

* Data may / may not be delevered
* Data may change/corrupted
* Data may not be in order

} PROBLEMS

* It is a connectionless protocol and is FASTER
* UDP uses checksums to check if data got corrupted while getting transmitted. But it dosnot do anything about, it will just discard the packet

UDP Packet



Total size of packet = 2^{16} bytes (64KB)

Use Cases

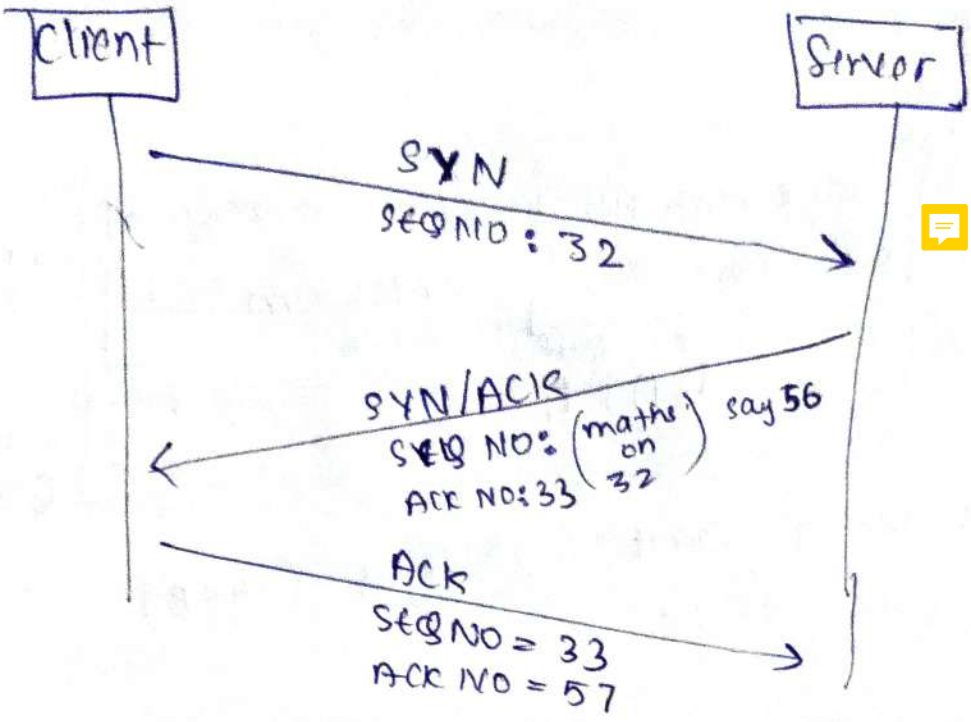
* Very Fast
* Gaming
* DNS
* Video conferencing apps

• TCP (Transmission Control Protocol)

TCP is a connection oriented protocol and every connection-oriented protocol needs to establish a connection in order to resource both the communication ends. TCP is a full duplex protocol.

3-way handshake protocol

This is a way in which connection is established between the communicating systems.



1) Client sends a connection request to your server. In your request it contains a flag called as synchronization flag (SYN FLAG). It means that a new connection is being established. It is just a value inside the header. A sequence no (Random) is also sent along with it.

2) Server gets the request and responds with an SYN/ACK flag. This also contains a sequence no. (Random)

Syn & ack flag

This time, seq no is not random. Server takes clients seq no, does some mathematical calculations on it which will give the sequence no. ACK NO = Prev seq no + 1

3) Client will send an acknowledgement back to server with seq no = Prev Client seq no + 1

ACK no = Prev seq no + 1

After connection is established, data is sent.

Features of TCP

* Connection oriented
* Full duplex protocol
* More reliable (Guarantees data transmission)
* Error checking using Checksum.
* Flow and error control.

5 Network layer

Responsible for end to end delivery

* We have already diswssed a lot about IP address and Routing tables.

Say. 198.68.10.11 → IP address of some device

198.68.10 → Network address (Subnet ID)

11 → Device address (Host ID)

IPV4 : 32 bit numbers (4 words) eg 5.6.9.14

IPV6 : 128 bit numbers (8 words)

Each is 16 bit hexadecimal

8 bits each

eg: 12.0.0.0/31

This mean first 31 bits of IP address is subnet part

- **TTL** (Time To Live) : Max no of of hops a packet can take before reaching its destination.

[5] Data link layer

* Responsible for hop to hop delivery.
* All contents of MAC address and framing which we have already discussed comes here.
* ARP
* It transfers the frame into physical layer

MISCELLENIOUS & SYSTEM DESIGN

- Common Networking Commands

[1] Ping

Ping is used to test a network host's capacity to interact with another host.

ping | target hosts IP address → command.

This is performed using Internet Control Message Protocol (ICMP). It allows the echopacket to be sent to the destination host. If the destination host replies to the requesting host, that means the host is reachable. This command usually gives a basic image of where there may be specific networking issue (if any)

2) ~~Netstat~~ ping

target : destination IP address
-a : This resolves the hostname of an IP add.
-t : will ping the target until you stop it with Ctrl+C
-n count : Set no of ICMP Echo request to send from 1 to 4×10^9 request.

2) Netstat

It is a common TCP/IP networking command prevent in all OS's. It provides statistics and information of networks.

-a : Will display all connections and ports
-n : Will display address and port number in form of numerical.
-r : Will display the routing table.

3) IP config

Will display basic details about the device's IP address configuration.

ip config → Will display IP, subnet mask and default gateway
IP config -all → Full information.

[4] Hostname

Hostname is a human readable lable that is assigned to a device connected to a computer network and used to identify the device on the network. It is a unique name used to identify it such as computer, server or printer.

The main difference b/w hostname and IP address is that hostname is a memorable name used to identify a divice on network, while IP address is a numerical lable assigned to a divice to locate it on the network. Host names are easier to remember for humans, while IP addresses are used by computer networks to locate and communicate with divices on the network.

Q) Why is hostname used when we already have IP address to locate a divice on the network?

1. Usability :- Hostnames are easier for humans to remember.
2. ~~Reliability~~ Scalability : Easy creation of a naming convention of multiple devices on a network
3. Flexibility : Hostnames can be changed if necessary, unlike the IP address.

Q) Where is hostname used in OSI model?

Hostname is used in application layer. Here, hostname is used to identify the device in human-readable format, and is often used to establish a communication channel between two devices. Once the connection is established, hostname is not used in communication process as the data is transferred b/w the devices using IP address which is handled by lower layers of OSI model.

Eg: ~~For~~ when a client requests a web page for a server, the hostname of the server is used to make connection, and client uses the hostname to ensure it is communicating with right device. i.e server.

hostname → will provide name of computer & domain
hostname -s → output will be ~~xxxx~~ host name only
hostname -i → IP add for hostname
hostname -a → hostname and DNS alias
hostname -d → DNS ~~xxxxx~~ domain name

5) Tracert

Tracert (or traceroute) command is used to visualize the path that packet takes from source host to destination host. through intermediate routers.

The tracert command displays IP add of each hop (router) along the path. This information can be useful in trouble shooting network problems.

tracert [-d] [-h Max Hops] [-w TimeOut] target

target : Destination IP add / hostname
-d : prevents tracert from resolving IP add to hostname to get faster results.
-h MaxHops : Max no of hops that the packet can take.
-w TimeOut : It adjusts the amount of time in ms.

[6] nslookup (name server lookup)

It is used to obtain information about internet servers. It helps resolve domain name to IP add and IP add to domain name.

Nslookup [domain.name]

[7] Route

It is used to view and modify the IP routing table on a computer. route command can be used to add, delete or modify entries in the routing table and to display information about existing routes.

[8] ARP

It is used to view and modify ARP table. It can be used to add, modify and delete entries of the table.

[9] path ping

It is used to diagnose network connectivity and packet lose issue in a network path. It combines functionality of 'path' and 'tracert' commands and provides additional information about quality of route b/w source and destination host.

The pathping command sends multiple ping packets to each hop along the path and calculate the packet loss percentage for each hop.

The out put of path ping command gives information about ~~route~~ round-trip time for packet to travel from source to each hop, no of hops along the path and packet loss percentage.

- Who assigns IP address to a device?

1. Static assignment : Manually assigned by network administrators. This method is often used for servers or other central devices.
2. Dynamic assignment : They are automatically assigned to a device when it connects to a network. This method is often used for laptops, smartphones etc
3. DHCP(Dynamic Host Configuration Protocol)

   It is a network protocol used to dynamically assign IP addresses to device on a network. DHCP servers are responsible for allocating IP addresses to devices on the network.

- SSL and TLS

SSL (Secure Socket Layer) and its successor TLS (Transport Layer Security) are protocols for establishing authenticated and encrypted links between networked computers. SSL protocol was depricated on release of TLS protocol.

What is SSL certificate?

An SSL certificate (also known as SSL/TLS certificate) is a digital document that binds the identity of a website to a cryptographic key pair consisting of a public key and private key. The public key included in the certificate allows a web browser to initiate an encrypted communication session with a web server via TLS and HTTP protocols. The private key is kept secure on the server, and is used to digitally sign web pages and other documents (JS files or images).

SSL/TLS and Secure web browsing

Most common use of SSL/TLS is secure web browsing via HTTPS protocol. A properly configured public HTTPS website include a SSL/TLS certificate that is signed by a publicity trusted CA (certificate authority). User visiting a HTTPS website can be assured of

- Authenticity
- Integrity : Documents signed by certificate have not been altered by man-in-middle.
- Encryption : Comm b/w client & server is encrypted

- Difference b/w HTTP and HTTPS

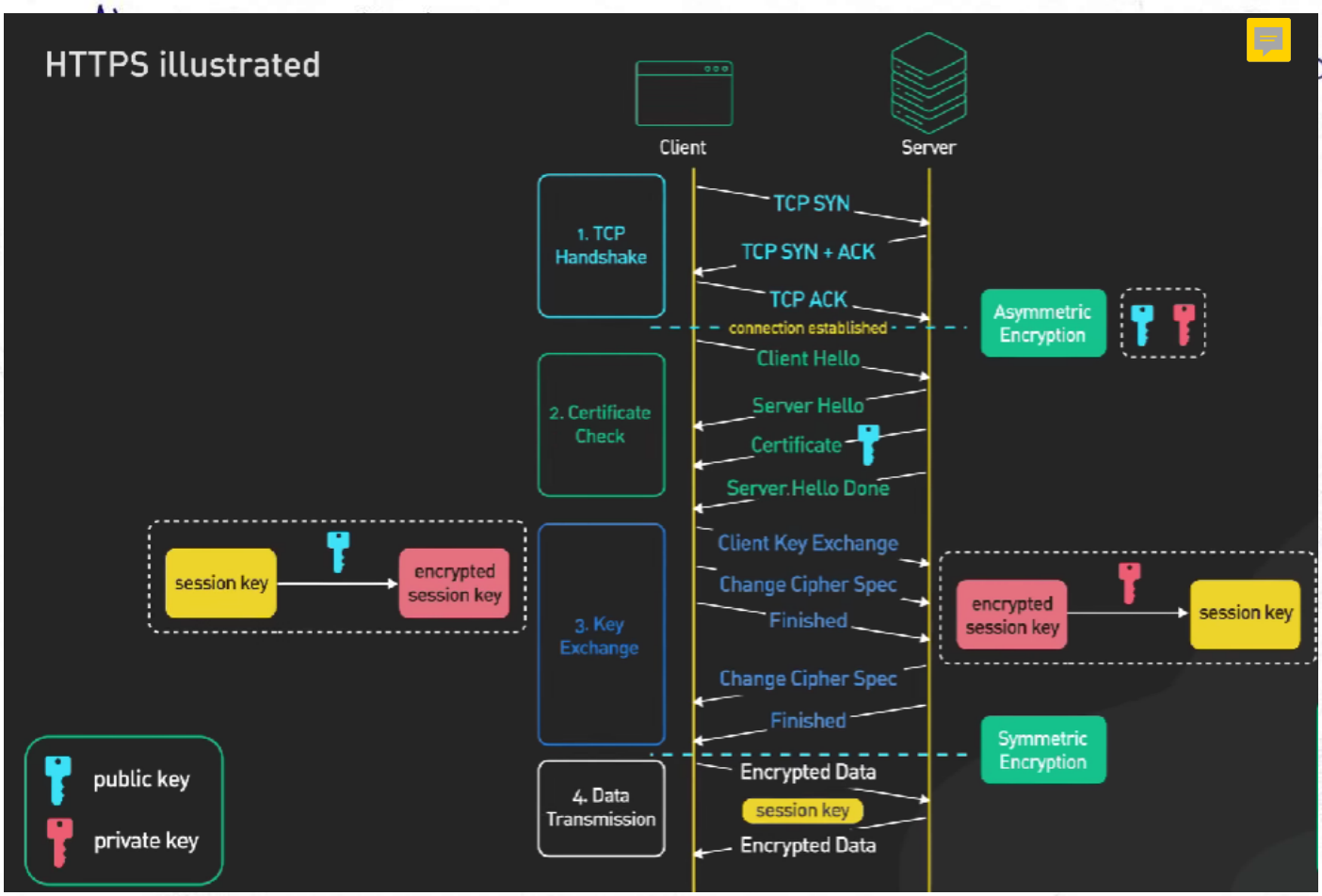
Both of these are protocols using which information of website is exchanged between Web server & Web browser.

1) HTTP (Hyper text transfer protocol)

It is a protocol using which hypertext is transferred over the web. but it is not secure. the data (hypertext) exchanged using http goes as plain text ie anyone between the browser and server can read it..

2) HTTPS

https = http + cryptographic protocols



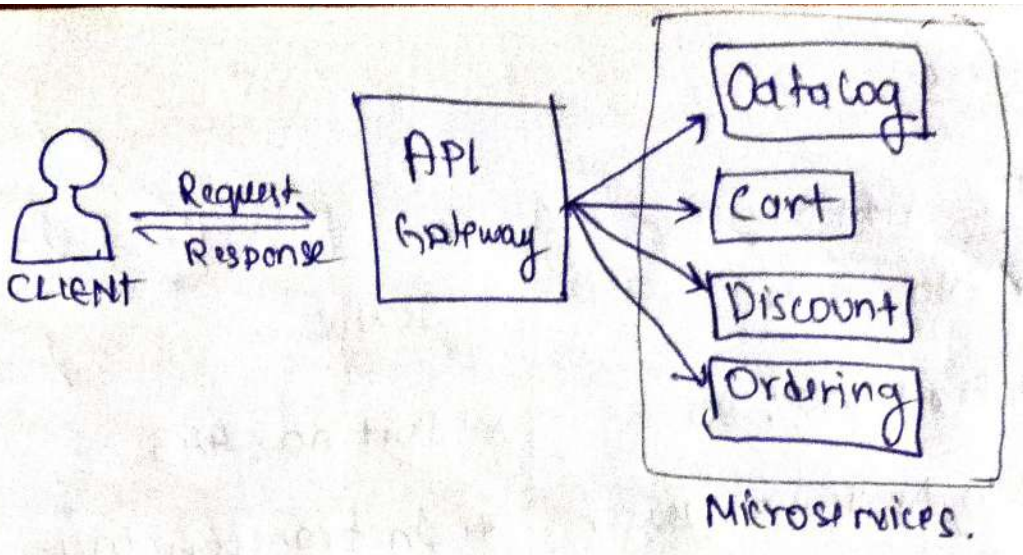
Differences

Http	Https
* not secure	* Secure
* Port no: 80	* Port no: 443
* In Application layer	* In transport layer
* Faster	* Slower
* No certificate	* SSL/TLS certificate.

- What is API gateway?

API Gateway is a server that acts as a bridge between an application and multiple micro servers (API)

* It provides single entrypoint for external clients to access internal microservers.
* It handles tasks such as request routing, security and performance optimization.
* By using API Gateway, system becomes more scalable flexible and resilient.
* The client sends the request to API gateway, which then forwards the request to API. API processes the request and returns a response which the API gateway forwards back to client.



- **Reverse Proxy**

Reverse proxy is a server that sits in front of web server and forwards client requests to those web servers. Rever proxies are implimented to help increase security, performance and reliability.

What is proxy servir?

A forward proxy, often called proxy server or web proxy is a server that sits in fron of group of client machines. When those machines makes request to sites and services on internet, the proxy server intercepts those requests and then communicates with webservers on behalf of those clients (middleman).

Why is this required?

1) To impliment restrictions : Some governments, schools and other organizations use firewall to give

their users access to limited version of the internet, A forward proxy can be used to get around these restrictions

2) To block access to certain content: Proxies can also be used to block a group of users from accessing certain sites.

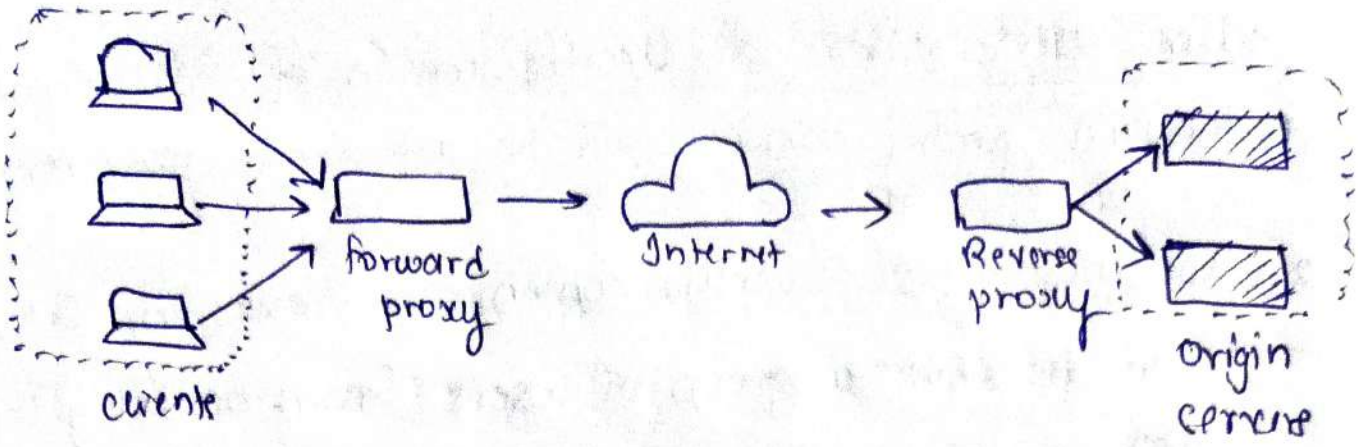
3) To protect their identity online.

How is reverse proxy different?

Reverse proxy is a server that sits in front of one or more web servers. This is different from forward proxy, where it sits in front of the clients. With reverse proxy, when client sends request to origin server of a website, those requests are intercepted by reverse proxy server. The reverse proxy server will then send request to and recieve responses from the origin server.

Forward proxy server: Sits in front of clients and makes sure no origin server communicates directly with specific client.

Reverse proxy server: Sits infront of origin server and makes sure that no client directly communicates with origin server.



Uses of reverse proxy server

1) Load balancing : Reverse proxy distributes incoming requests to multiple servers to balance load and improve performance.

2) Caching : It can cache content, resulting in faster performance.

3) Security : In presence of reverse proxy, client can never access origin server ⟹ Attacker can never) impossible to get IP add of servers ⟹ No attack

4) Hiding backend servers

- Load Balancing

It refers to efficiently distributing incoming network traffic across a group of backend servers.

It acts as a traffic-cop sitting in front of servers

and routing client requests across all servers, and ensures that no one server is overworked. If a server goes down, the load balancer redirects traffic to the remaining online servers. When a new server is added to server group, the load balancer automatically starts to send requests to it.

Benefits of load balancing

1) Scalable
2) Flexible
3) Efficiency

Load Balancing Algorithms

1) Round Robin
2) Hash :- Distributes requests based on key you define such as client IP address or request URL.
3) IP hash :- IP address of client is used to determine which server recieves the request.
4) Least Time :- Sends request to server selected by a formula that combines the fastest response time and fewest active connections.
5) Least connections :- A new request is sent to client with least client connections.

Scaling → Vertical & Horizontal Scaling

Scalability is the ability to expand from existing configuration of system for handling the increasing amount of load. Scaling can be done by either adding extra hardware or by upgrading current system configuration.

1) Horizontal Scaling / Scaling out

Process of adding more nodes to a syetem to handle increasing workloads.

* This approach is useful for systems that experience unpredictable and rapidly growing workloads, as it allows quick and flexible expansion of resource.
* Horizontal scaling can be done by adding more servers, databases or other components.

Use

- Cloud computing

Advantages

* Easily scalable
* Easy to upgrade
* Better use of smaller systems

Disadvantages

* High license fees
* High utility costs (cooling, electricity etc)

[2] Vertical Scaling / Scaling-in

It is process of increasing the capacity of an individual node in a system. such as CPU, memory or storage to handle increasing workloads.

* This approach is useful for systems with predictable and stable workloads, where capacity of a single node can be easily increased to meet dimand.
* It is often used for small to medium sized systems where cost and complexity of adding additional nodes to the system may be prohibitive.

Advt

* Reduad s/w costs
* Easy implimentation
* Licna fee is less
* Consomption powir is Uss (Celectricity and cooling)
* Less expensive

Disadvt

* Limited scaling
* Risk of downtime is much higher
* [redacted]

	Horizontal Scaling	Virtical Scaling
Flexibility	Quick and flexible expansion.	Limited expansion
Cost	More expensive	Less expensive
Complexity	More complex	More simple
Resilience	Even if one node fails, others can handle	If one node fails, everything fails.

• Caching & How is website Cached?

Caching is a process of storing copies of files in a cache, or temporary storage location, so they can be accessed more quickly. Technically, a cache is any temporary storage location for copies of file or data. Web browsers cache HTML files, JS files and images inorder to load websites more quickly, while DNS servers cache DNS records for faster lookups and CDN servers cache content to reduce latency.

What does a browser cache do?

Every time a user loads a web page, their browser has to download quite a lot of data in order to display that webpage. To shorten page load times, browser's cache most of the content that appears on the webpage, saving a copy of the webpage's content on the device's drive. This way, the next time user loads the page, most of the content is already stored locally and page will load much quicker.

Browsers store these files until their time to live (TTL) or until the hard drive cache is full. User can also clear browser's cache if desired.

What does clearing a browser's cache accomplish?

Once a browser cache is cleared, every webpage that loads will load as if it was visited first time by the user. However, clearing ones browser cache can also temporarily slow page load time.

What is CDN (Content Delevery Network) Caching?

A CDN caches content (such as images, videos or webpages) in proxy servers that are located closer to end users. Because the servers are closer to the user making the request, a CDN is able to delever content more quickly.

When you request content from a website using a CDN, the CDN fetches content from origin sirver, and then saves a copy of the content for future ~~purpose~~ purpose.

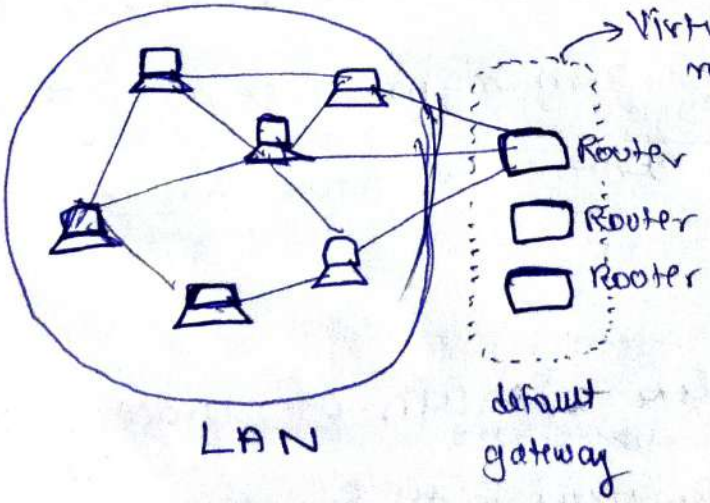
Think of CDN as being like a chain of grocery stores. Instead of going all the way to the farms where food

is grown, which could be hundreds of miles away. Shoppers go to their local grocery store, which still requires some travel but is much closer.

CDN: It refers to geographically distributed groups of servers which work together to provide faster delivery of Internet content.

- **Virtual IP address (VIP)**

VIP is a concept used in layer 3 to provide a backup mechanism for default gateway functionality in the LAN. A set of routers work together to create a virtual router, which acts as default gateway for all device connected to LAN.



In this, each device has its own IP and MAC address and the group has a VIP address.

By group having VIP, we mean that there is each priority given to a router in the group and when a client in LAN request for ~~router~~ default gateway, it requests ~~for~~ using a VIP. the router in default gateway (group) with highest priorite will have the VIP address. when this router is heavily loaded / fails, the VIP address will be given to next priority router.

It is commonly used in network configurations that require high availability, such as load balancer or server clusters.

- What is Container Networking?

Containers are full featured Linux environment with its own users, file systems, processes and network stack. All applications inside the container are permitted to access or modify files or resource available inside the container only.

Containirization: Software deployment process that bundles an applications code with all the files and libraries it needs to run on any infrastructure.

Container networking ~~is~~ refers to connecting containers to each others and to the outside world. This involves creating virtual networks, configuring network settings and assigning IP addresses to containers.

- Performance v/s Scalability

Performance refers to the efficiency and speed with which a system performs its tasks, often measured in terms of ~~network~~ time and resource utilization response

High performance is desirable for ensuring quick & smooth execution of applications.

Scalability on the other hand, refers to the ability of a system to handle increased workloads and maintain performance levels as demand grows.

- **Latency V/S Throughput V/S Bandwidth**

1) **BW:** No of packets that can be transferred through the network at once.

2) **Latency:** Indicates how long it takes for packets to reach their destination.

3) **Throughput** :- No of packets that are processed within a specified period of time.

- **2G V/S 3G V/S 4G V/S 5G**

G → Generation

While you connect to the internet, the speed of your internet depends on the signal strength that is shown using 2G, 3G, 4G or 5G.

1G - First Generation

* 1G was an analog technology to transmit voice and data.
* 1G had limited capacity, low data transfer rates and poor sound quality due to use of analog signals.
* Its maximum speed was 2.4 Kbps.

2G - Second Generation

* It was transition from analog signal to digital signal in mobile networks.
* It uses digital signaling to transmit voice and data, allowing more efficient bandwidth and improved network capacity. This also introduced encryption technique to enhance security.
* Introduced Short Message Service (SMS). & mms
* Mobile data services were introduced → browsing internet, email etc.
* Maximum speed was 64 Kbps.

2G represented a major step forward in development of mobile communication.

* 2G introduced many of the fundamental services such as SMS, internal roaming, conference calls, call hold and billing based on service.

3G - Third generation

* This generation set standards for most of the wireless technology we have come to know. web browsing, email, video downloading, picture sharing and other Smartphone technologies.

* Goals: Facilitate greater voice and data capacity, support a wider range of applications and increase data transmission at lower cost.

* 3G uses new technology called UMTS (Universal Mobile Telecommunication System). It combines aspects of 2G and with some new technology that comply with International Mobile Telecommunication (IMT - 2000).

* One of most significant advancement of 3G was the ability to support video streaming

one mobile video calls.

* 3G offered 144 Kbps – 2 Mbps

4G- Fourth Generation

* 4G is very different from 3G.
* Goals: High speed, high quality and high capacity while improving security and lower cost of voice and data services.
* Key technologies that made it possible is MIMO (Multiple input & Multiple Output) and OFDM (Orthogonal Frequency Division Multiplexing).
* 2 important 4G standards are WiMAX and LTE (widespread deployment). WiMAX has now fizzled out
* LTE (Long term Evolution) is series of upgrades to existing UMTS technology.
* Max speed of 4G: 100 Mbps - 1 Gbps.

5G- Fifth Generation

* 5G is currently under development.
* Offer faster data rates, higher connection densities

much lower latency etc.

* Max speed of 5G is aimed to 35Gbps.

* Technologies used : Massive MIMO, Millimetre Wave Mobile Communications etc.

- **What is VPN and how it Works?**

VPN stands for Virtual Private Network and describes opportunity to establish a protected network connection when using public networks. VPN encrypts your internet traffic and disguise your online identity. This makes it more difficult for third party to track your activities online. Encryption takes place in realtime.

How does it work?

When a user connects to a VPN, their internet traffic is routed through an encrypted tunnel to the VPN server. The VPN server acts as an intermediatery, forwarding the users internet traffic to destination website or service. The destination website/service

then sends its response back through VPN server to the user.

Because users internet traffic is encrypted and routed through VPN server, the users ~~data~~ ISP and anyone else monitoring the internet connection cannot see the users internet activity. This provides high level of privacy and security.

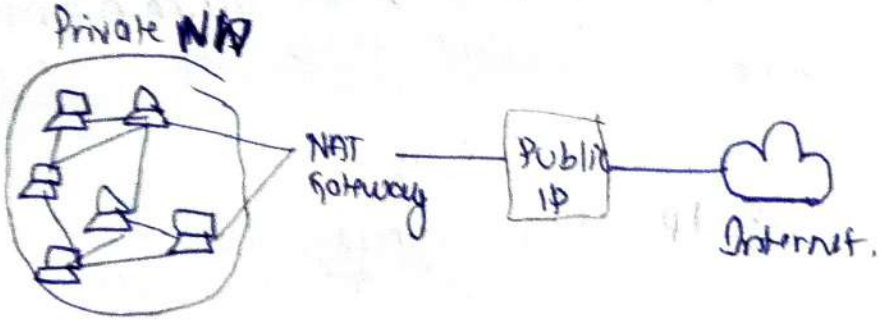
- **Router and Gateway**

Router :- Router is basically a device or hardware which is responsible for recieving, analysing and forwarding data packets to other networks using Routing tables.

Gateway :- Gateway is basically a device ~~that is used for communication among other networks~~ or a hardware that acts like a gate among the networks. It acts as an intermediatey between two networks. A gateway is used to connect two networks that use different protocols and manage to flow data b/w them.

A Gateway is responsible for routing data between two networks and converting data into a format that can be understood by the recieving network. It also perform other functions such as security and Network Address Translation.

NAT: Technique used in computer Networking to allow multiple devices on a private network to share a single public IP address. This allows devices on private network to communicate with the internet while hiding their individual private IP address. The NAT gateway acts as an intermediatary between private & public networks translating private IP add to public IP add.



Main Diff b/w router & Gateway

A router is primarily responsible for forwarding packets between networks while gateway is responsible for connecting networks and converting data between different protocols.

- Public VS Private IP address

Public IP address: IP address that is assigned to a device or a network by an ISP and is used to communicate with devices on the internet, Public addresses are globally unique and are used for communication b/w devices on the internet.

Private IP address: IP address assigned to a device within a private network such as home or office. Private IP addres are not globally unique and are not intended to be used for communication with devices on the internet. They are used for communication within the network.

Private ip address range

10.0.0.0 - 10. 255.255.255
17.16.0.0 - 17.16.255.255
192.168.00 - 192.168.255.255

Rest of the IP address is for Public use.

- ## Modem v/s Router

Modem: (Modulator-demodulator) is a device that connects a LAN to the internet. It is responsible for converting the digital data of a computer into analog signals that can be transmitted over a telephone and vice versa. The modem is connected to the ISP and connects internet and computer.

Router: Device that forwards packets ~~wise~~ between computer networks, and is responsible to determine best paths for data travel based on its routing table.

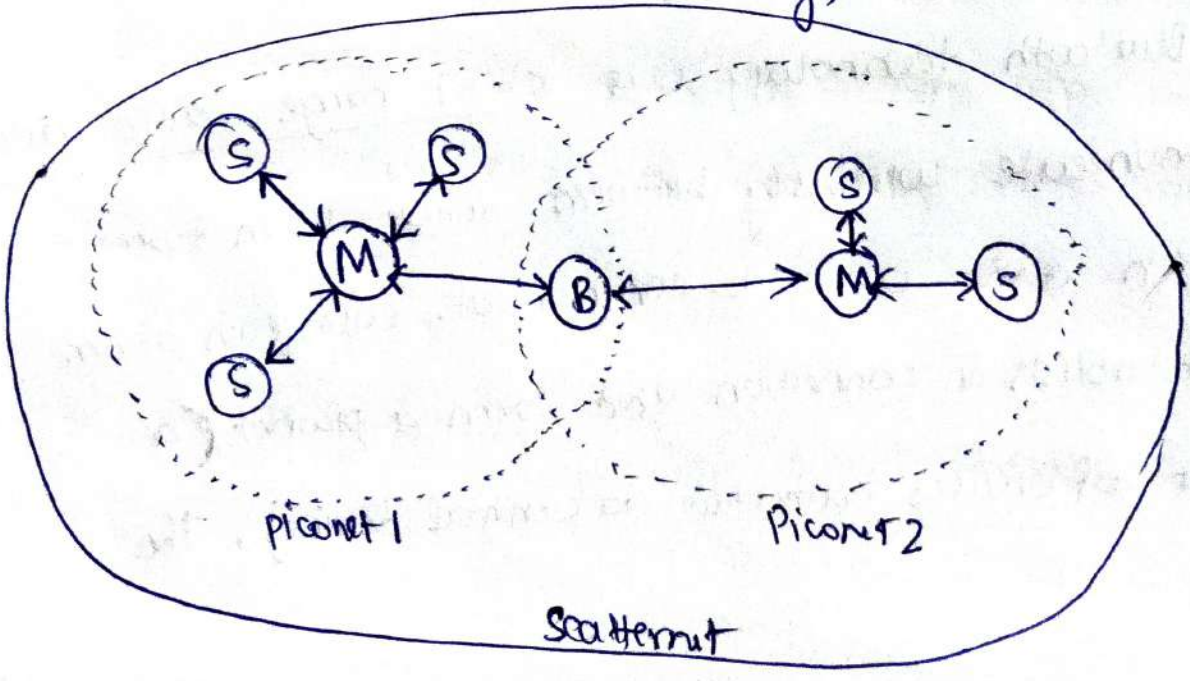
- ## How bluetooth works?

Bluetooth technology uses short range radio waves to communicate wirelessly between devices, when two bluetooth devices want to communicate with each other, they establish a connection and form a piconet (a network of devices connected to central device). The

Central device acts as master and others act as slave. Data is transmitted wirelessly in packets, and the master device determines when each slave device gets to transmit. This allows efficient and secure communication without need of wires.

Piconet and scatternet

Piconet is a network of upto 8 Bluetooth devices connected to a single central device also known as master. The master controls the timing of data transmission, deciding when each slave device ~~decides~~ gets to transmit. The slaves are assigned unique address and can only communicate with master. Each device can communicate with several piconets simultaniously.



Scatternet is a network of multiple piconets that are interconnected, allowing devices in one piconet to communicate with ~~other~~ devices in another piconet. A master of one piconet can act as slave in another piconet. They are useful when there are more than 8 devices that need to communicate with each other.

Eg: A smart phone can be a master in piconet with headset and slave in piconet with smartwatch.

How it works

1) Device discovery :- This is done by process called as inquery scanning, where initiating device sends out a special signal called inquiry. Any other bluetooth device in range will respond with the device name and address.

2) Pairing : Once two devices have discovered each other, they constitiate pairing process. This involves exchanging a unique code between the devices to ensure that they are communicating with the right device.

3) Connection establishment :- Paired device establish connection by creating a piconet. Device which initiated the connection acts as master and other as slave.

4) Data transmission: Master device determins which slave device gets to transmit, allowing efficient and secure communication. Data is transmitted through air in packets and a special protocol called as link controller ensures that data is transmitted reliably and accurate.

5) Disconnection:- when devices are finished ~~computing~~ communicating they can disconnect from each other. This breaks the piconet.

How hotspot works?

Wifi hotspot is a physical location where people can access the internet using WiFi, a wireless networking technology that allows devices to communicate with each other without cables. Wifi hotspot typically consists of a router connected to an ~~internet~~ ISP and WiFi network that users can connect to with their devices.

How does it work?

1. Internet connection :- The WiFi hotspot is connected to the internet through ISP. This provides the

necessary bandwidth for multiple users to access the internet.

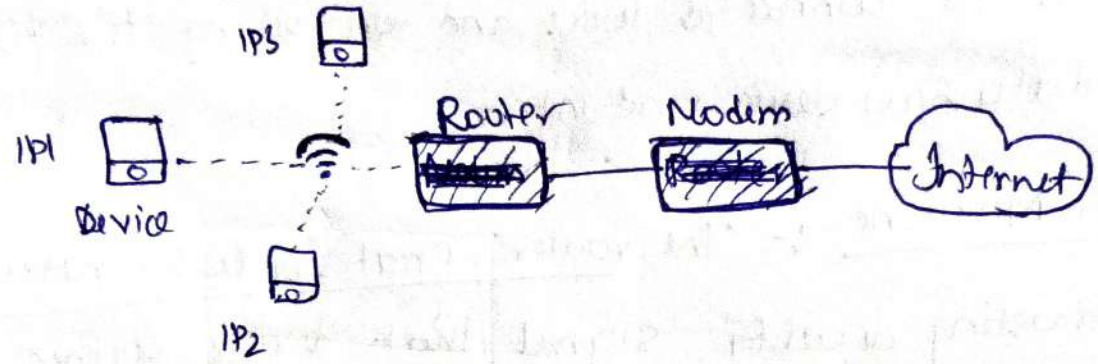
2) Router :- The internet connection is then connected to a router, which serves as the hub for WiFi hotspot. The router manages the network, allocating IP address to connected device and controlling the flow of data b/w device and internet.

3) WiFi Network :- The router creates a WiFi network, broadcasting a wifi signal that devices within range can pickup.

4) Device connection :- When a device wants to connect to WiFi, it searches for available networks and displays a list of them. The user connect to a network using the password.

5) Data transmission : Once connected, user can communicate with the internet and other devices on the WiFi network. Data is transmitted in air through in packets and router manages the flow of data between device and internet.

The device that is installed by the ISP in our homes is typically a combination of modem and router. This device combine the functionality of modem and router into one device, without the need for separate devices for each function



- How Email works ?

Email is a communication method that allows users to send and recieve messages electronically over the internet. SMTP (Simple Mail Transfer protocol) is a standard protocol for transmitting electronic mail from one computer to other over the internet.

SMTP

1) Composing : The sender uses email client such as Gmail / Outlook / Applemail to compose a message. The email client creates a plain text or HTML message and includes the receptant email address, senders

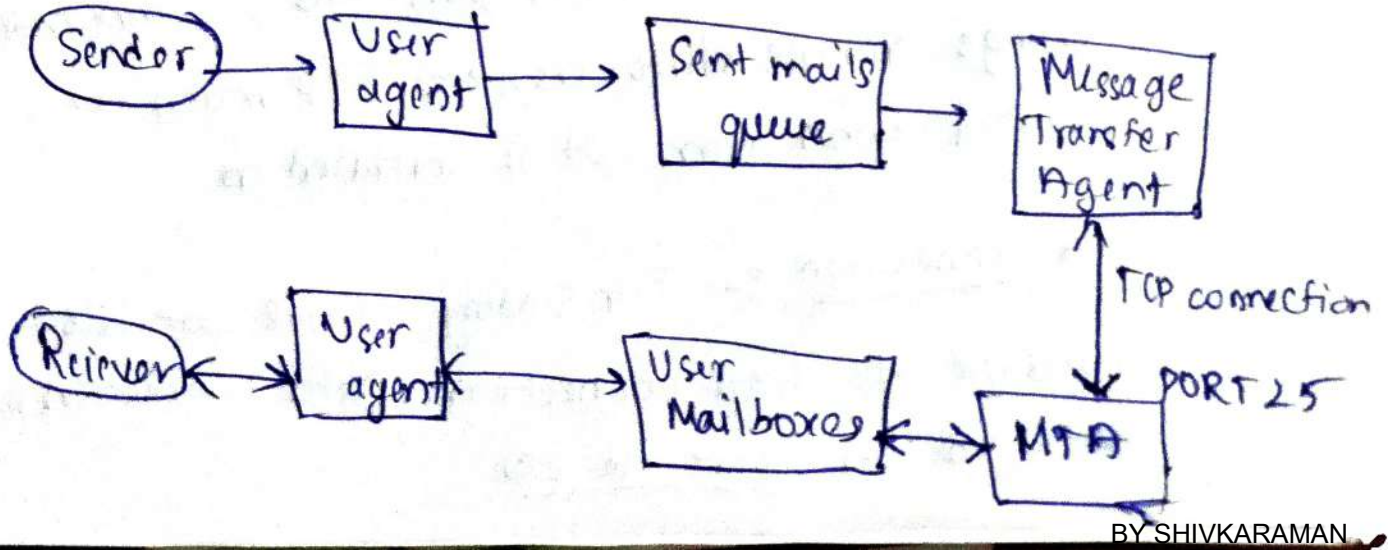
email address and any attachments.

2) Encoding :- The message is encoded in a standardised format ie SMTP, which includes dividing the message into small packets and adding header information such as receptants email address to each packet.

3) Transmission, The encoded message is transmitted from sender to reciever over the internet using TCP to ensure reliable delivery of message. TCP is initiated on PORT NO 25.

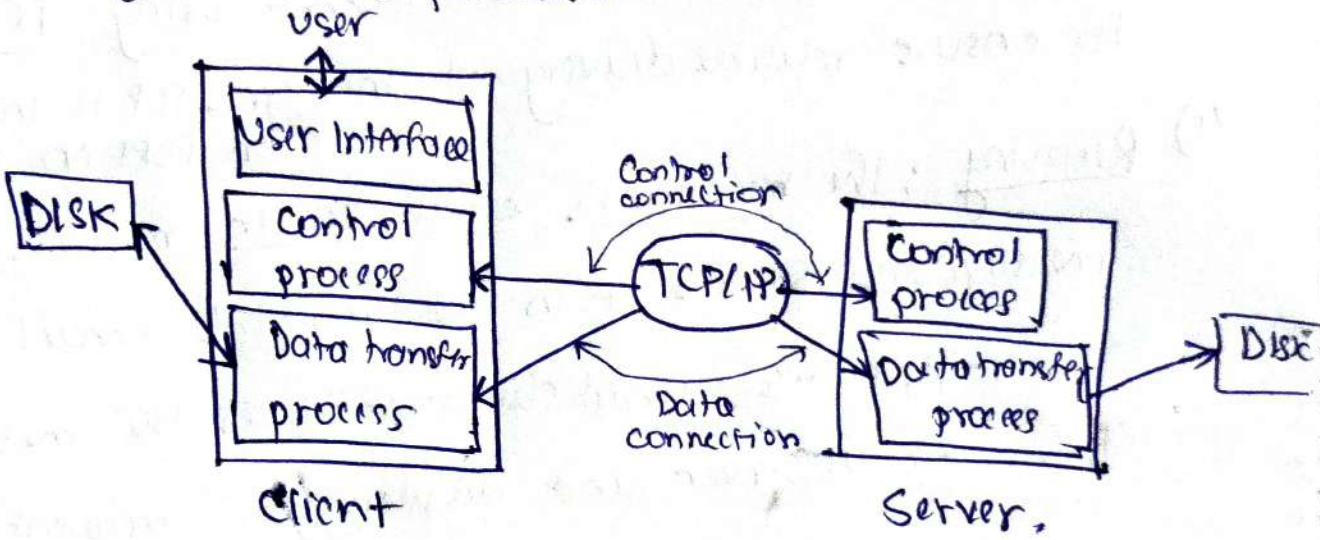
4) Recieving : The receptant's email servir recieves the message and stores it in the recipients email inbox. The receprent's email client retrieves the message from email sirver and displays to recipient.

5) Reply : If recipient wants to reply, he uses senders email address. The process of SMTP repeats.



- ## How FTP works?

File Transfer Protocol is an application layer protocol that moves files between local and remote file systems over a TCP based network, such as internet. FTP is commonly used for transfering large files or group of files. 2 TCP connections are used by FTP in parallel.



- Control Connection :- For sending control information like user identification, password, commands to change remote directory, etc FTP makes use of control connection. It is initiated on PORT NO 21.

Data connection :- For sending actual ~~con~~ file, FTP makes use of data connection. Data connection is initiated on port no 20

FTP Session

When an FTP session is started between a client and server, the client initiates a control TCP connection with server side. The client sends control information over this. When the server recieves this, it initiates a data connection to client side. Only one file can be sent over one data connection. But the control connection remains active throughout the session. FTP needs to maintain a state about its user throughout the session.

* FTP supports only upto 2GB data transfer
* Multiple recievers are not supported by the FTP.
* FTP doesnot encrypt data → Biggest disadvantage.