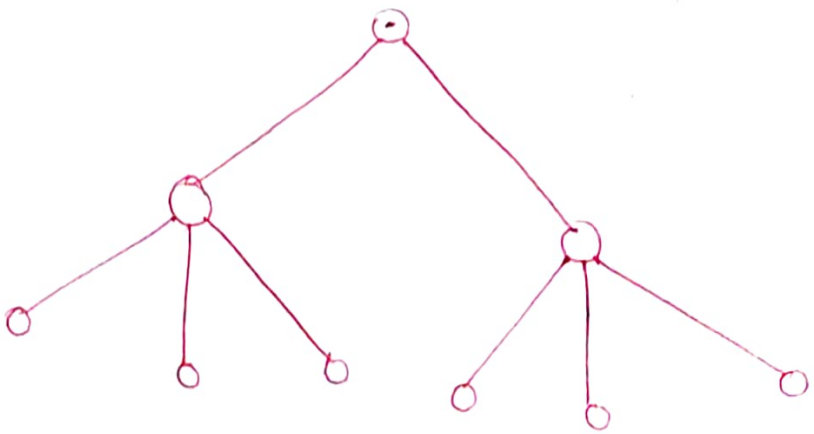
INTRODUCTION TO COMPUTER NETWORKS



Computer Networks

Networking is everywhere.

Networks support the way we learn

Network support the way we communicate → landline phone, whats app.

Network support the way we work

Network support the way we play.

INTRODUCTION

A computer Network is a set of nodes connected by communication links.

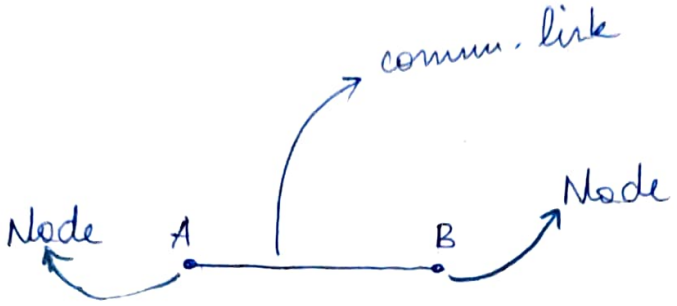
Nodes → Can be a computer, printer or any other device capable of sending & receiving data generated by other nodes in Network

Examples for Node

- → computers
- → Server
- → Printer
- → security camera
- → Many More. (switches Bridges Routers etc)

- A communication link can be a wired or wireless link.
- This links only carry the information.

Ex:



computer A computer B.

These nodes A & B exchange data/information using these links (here it is cable)

↓

physical Med. → wired.

A WIRELESS LINK B

Smartphone A Smartphone B

No physical connectivity

↓

using wireless Tech.

↓

Air is going to carry the signals /data.

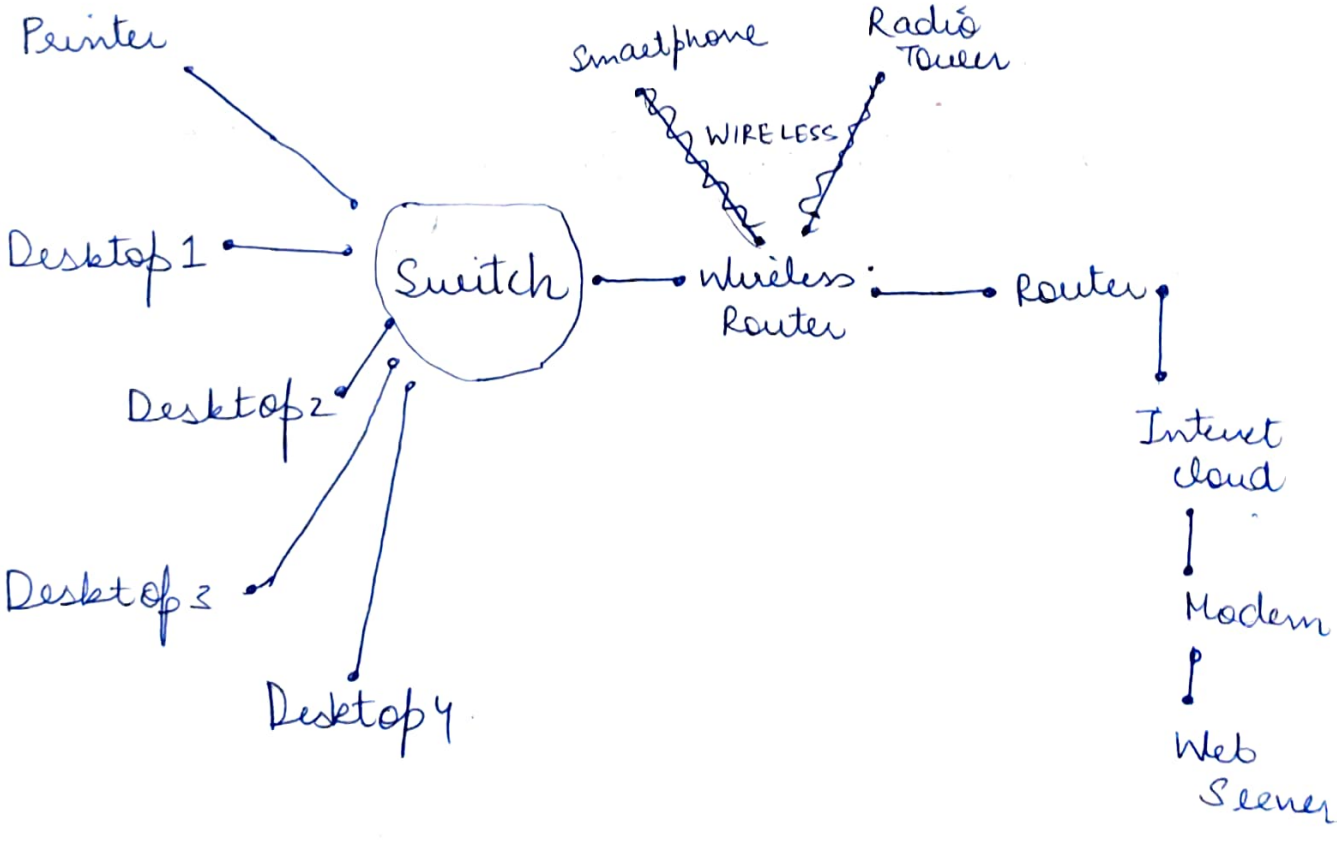
So here Air is the link, to carry the data.

2 types / kinds of communication links :

Links : Wired → cable (Best Ex)

Wireless → Air

An example of CN



• Computer Network is mainly used for Resource sharing

There are 2 types of Nodes / devices

→ End devices

The devices which are the source or destination in the communication are called as end devices.
Ex: Desktops, Printer, Smartphone, Server

→ Intermediary devices

The devices which forwards the data from 1 side to another side are called as Intermediary devices.
Ex: Router, Wireless Router, Cell Tower / Radio Tower.

Basic Characteristic To Judge a CN

① Fault Tolerance

It is:

→ The ability to continue working despite Failure

→ Ensure No loss of service.

Work even after encountering the failures.

Ex: Scenario

You are Going Home from college, & You know very well about the Best Route to reach Home.

& Prefer Taking that route only to Reach Home

But, unfortunately → There is a Blockage.

You cannot take this route further

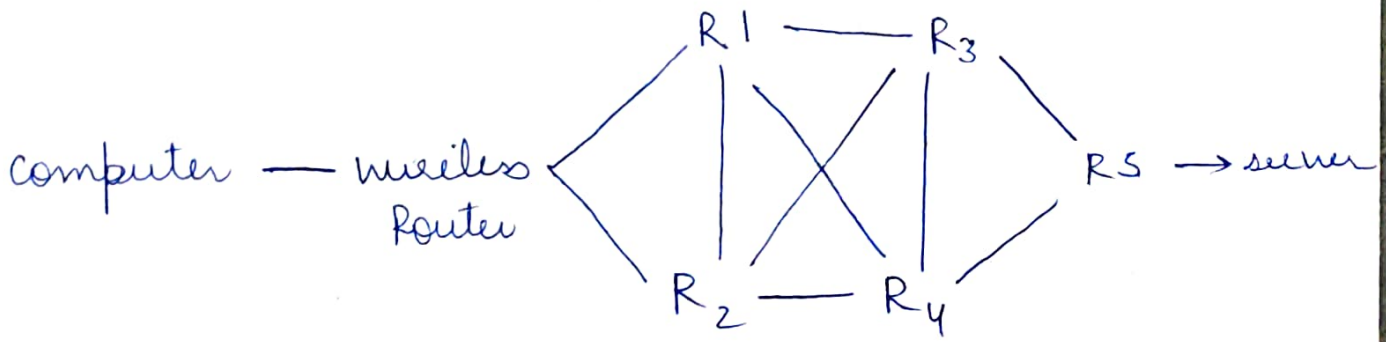
Will you go to your college Back ?

OR

Find another Route to reach your Home ?

→ Fault Tolerance

Ex:



If R1 fails incase while transmitting data from WR to R1, then WR will transmit the data from WR → R2

This is what we call as Fault Tolerance.
or Why we need it ↑.

2. Scalability

It is

→ The ability to grow based on needs.

→ While having good peformance even after growth.

For Ex: 10 computers in a Network

If then 10 computers are added to this Network then this Network should work as like the same as even after adding these 10 computes.

→ Internet → Best Example.

3. QoS (Quality of Service)

It is the ability to set priorities & manage data traffic to reduce data loss, delay etc.

Ex:

(A) 2 Guys are talking to each other using Whatsapp call,

& at the same time,

(B) another guy is sending an email to server,

Now how do you prioritise the network.

or

Which of the 2 is to given more priority?

Ans: → (A) as email can be sent with Teaffic or delay.

But if the voice are sent with delay then there may be loss of signal.

So therefore Router should know that which thing is to be more prioritised. This is QoS.

Main Aspect of QoS → It handle the loss & delay.

4. Security final characteristic & Most Imp

The ability to prevent.

→ Unauthorized Access

→ Misuse

→ forgery. (Making falsy Things) (false doc) (falsification) (fraud)

It should provide →

→ Confidentiality

→ Integrity (Honesty & having strong Moral principles)

→ Availability

Ex:

Computer ⟷ Server

Suppose, someone from computer is sending some confidential infor. to A (amazon).

Once the data leaves our computer, it is not in our hands.

"Internet Has Good Guys & Bad Guys As well"
↳ Attackers

We change the data before sending from our computer. (It is converted to the form, which can be understood by C & the S only) (To prevent forgery & Misuse)

→ This is provided by confidentiality.

Integrity: The should be received by server end point Not any other.

Attacker always tries to deface the web-servers so that this resource ~~of data~~ (server) becomes unavailable for access.

Data - communication

- Data communication are the exchange of data b/w nodes (2) via some form of link (transmission Med.) such as cable, Air etc.

Flow of data

Data flow means the data is going to flow from 1 Node to another.

There are 3 different flows.

1. Simplex
2. Half Duplex
3. full Duplex.

Simplex

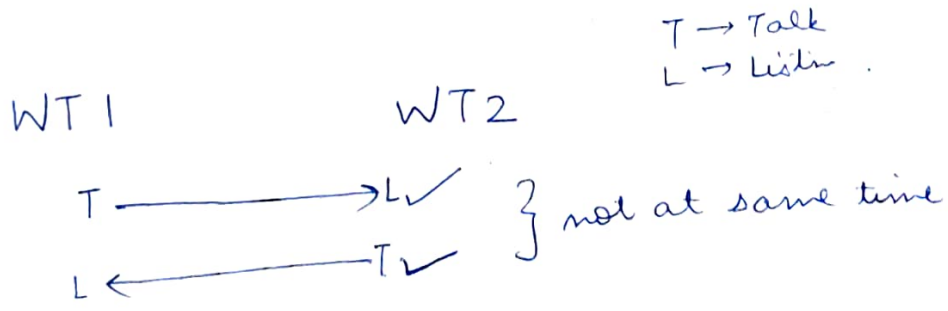
- Communication is always UNI-directional
- one device can transmit & the other device will reciene.

Ex: Keyboards, Traditional Monitors.

Half Duplex

- Communication is in Both directions but not at the same time.
- If 1 device is sending, the other can reciene only. & vice versa.

Ex: Walkie-Talkies.



Duplex or Full Duplex

Communication is in both directions simultaneously.

Device can send & receive at same time.

Ex: Telephone line

TL1 ⟷ TL2

Protocols

All communication schemes will have the following things in common

→ Source or Sender

→ Destination or Receiver

→ Channel or Media.

Rules or PROTOCOLS govern all methods of communication

- What if there are no rules / protocols →

GUY 1 ⟶ GUY 2

→ Guy 1 speaks at a High speed, which G2 can't handle this comm. becomes useless.

So they have to Mutually agree on certain Rules.

Now What if G1 speaks in language, which G2 cant understand.

He Maybe Greamatically correct but there is no use in this communication.

These are exampee situation, where the Comm. becomes messy or chaos.

— x — x —

Protocol = Rule, It is a set of rules that govern datal comm.

Protocol determines : →

What is communicated?
When it is communicated?
How it is communicated?

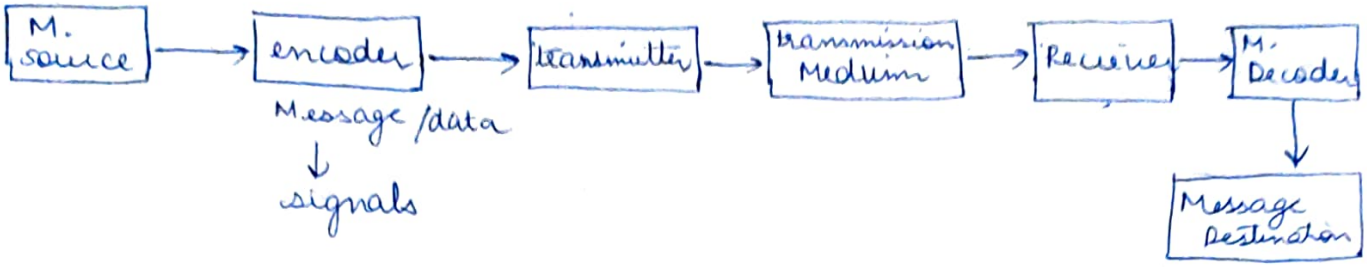
Protocols in context with Human Comm.

→ An identified Sender / receiver
→ common Language & geamar.
→ Speed & timing of delivery.
→ confirmation or acknowledgment requirements.

Protocols in context with Network comm.

→ Message encoding

S → R



2 types of Teansmission Medum → ~~Waves / signals~~. Wired & Wireless

Message source must know about transmission Medum. to which it is connected to.

If Source is connected to Wired Med → data Have to be converted into SIGNALS.

If ------ Wireless Med → data have to be encoded into WAVES as we can't send signals in Wireless Med.

→ Message formatting & Encapsulation

Both sender & receiver must mutually agree upon certain formats, which is → formatting

At the same time, when reciever receives the data, it should identify who has sent the data.

(We as a sender, adds some info with Data (header to identify the S & R)

So we are not going to just send the data as such.

3. Message Size

Humans breaks long messages into smaller parts or sentences.

Long messages must be broken into smaller pieces to travel across a network.

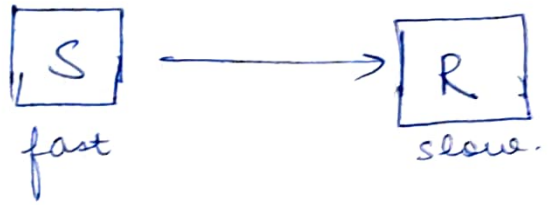
4. Message Timming

Deals with →

(A) → Flow control.

(B) → Response Timeout

(A) →



Since the sender is very fast, it can send data at high speed.

Receiver can't handle the speed

If there is no flow control Mechanism,

S can keep on sending data.

but the receiver cannot receive that data.

ENTIRE COMM. will become useless.

So, It is the responsibility of protocol to provide flow control Mechanism.

At the same time, S sending the data & the receiver has to acknowledge the data. When acknolegdement is sent back to sender, the sender can understand that the data is received by destination. if ack. not received the sender have to wait for a certain period of time.

After Expiry of ~~a~~ exact time, the sender will re-transmit the same so that we can ensure guaranteed delivery.

&

∴, It is the responsibility of protocol to tell, How much time this computer should wait for an acknowledgement.

5. Message delivery Options

There are 3 delivery option →

① Unicast → 1 Sender & 1 receiver only

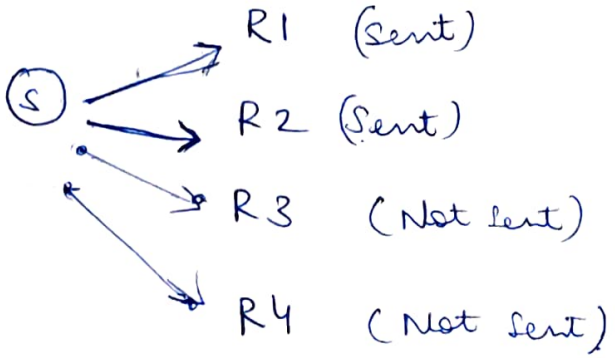
② Multicast → 1 sender & Multiple or a set of receivers (But Not to all receivers)

③ Broadcast → 1 sender & all participants are receivers.

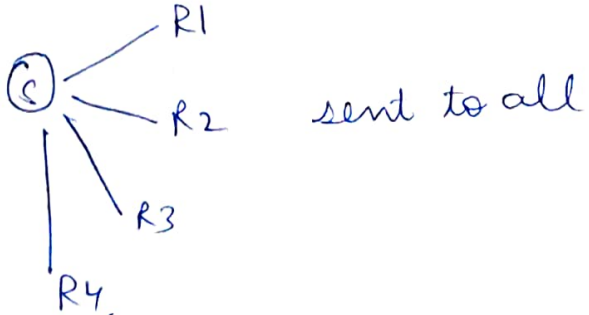
Ex:

① UNI

② MULTI



③ Broadcast



If needed an example :→

NESO ACADEMY

COMPUTER NETWORKING

→ N P & C Part 2 (refer it)
(detailed)

Components of Computer Network

Any computer Network have 3 components:

① Nodes (already seen)

② Media

③ Services

② Media (link)

Wired Medium → (Guided Medium)

Wireless (Unguided)

① In wired Med., there will be a cable that connects two nodes whereas in unwired/wireless medium, cables can't be present.

cable → used to guide the data flow,
∴, wired → guided.

Ex: Wired

→ Ethernet cable (straight through & crossover)
  - straight lines → different devices
  - variations
  - crossover → (dashed lines) (devices of same kind)
→ Fibre optic
→ coaxial cable → Audio/Video comm.
→ USB cable → connect computer to other device.

Wireless → 

→ Infrared → Short Range comm → (TV RC)
→ Radio → Bluetooth / WIFI
→ Microwaves → Cellular System
→ Satellite → Long Range Comm. → GPS

(3) Services

email
storage services
Voice OverIP (whatsapp call)
Video telephony
World Wide Web
Instant Messaging
File sharing.
online games

Classification of Computer Networks

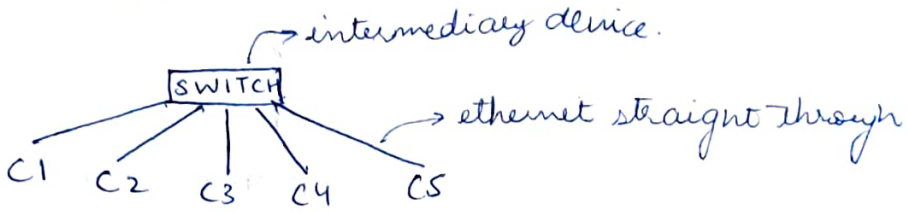
① Local Area Network (LAN)

(Restricted to a limited Area)

A (LAN) is a computer Network that interconnects commuters within a limited area such as residence, school, laboratory, university campus or office Building.

Ex:

A school



We can setup (lan) in 2 ways :-

① Wired → Ethernet - Hub, Switch

② Wireless → Wifi

② Metropolitan Area Network (MAN)

A (MAN) is a computer Network that interconnects users with computers resources in a geographic region of the size of a Metropolitan area (city)

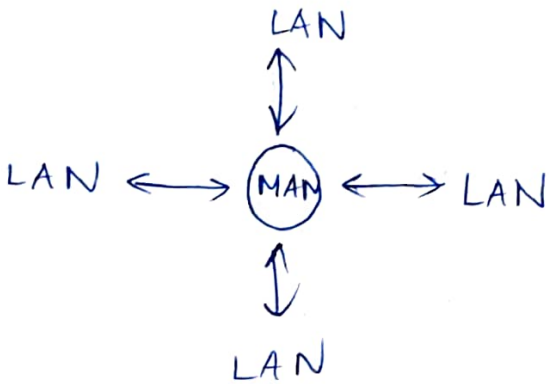
2 LAN are connected to each other in a City

- devices involved in MAN are :→

  Switches / Hub

  Routers / Bridges.

Ex:

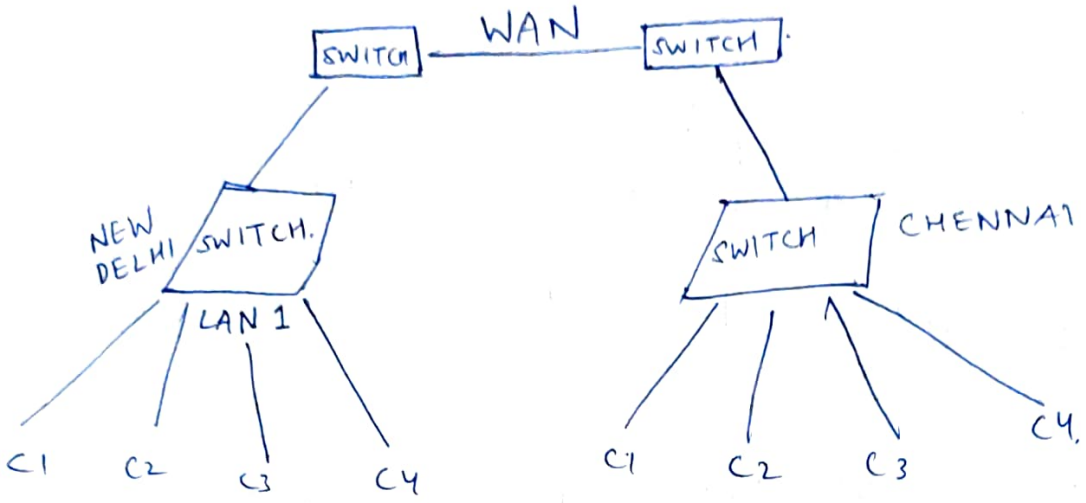


③ Wide Area Network (WAN), any comm. at a distance

A (WAN) is a telecommunication Network that extends over a large geographical area for primary purpose of computer networking i.e resource sharing

devices involved in (WAN)

→ End devices & intermediary devices



THE INTENET

It is Wide Wide Area Network
i.e Wide-WAN

There are so many LAN's, MAN's & WAN's across the world are connected to each other.

New Trends in CN's

Online collaboration (any place person can connect to all part of world)

Bring your own device (BYOD) → Employee can connect his/her device with office Network

Cloud computing → (Storage Area Network)

It is the on demand availability of computer resources, especially data storage & computing power, without direct active management by the user.

Ex: Google drive

Network Topology

Arrangement of nodes of a CN. (so that we can establish commun. among all the Nodes)

Topology → Layout

Physical Topology → Placement of Various Nodes

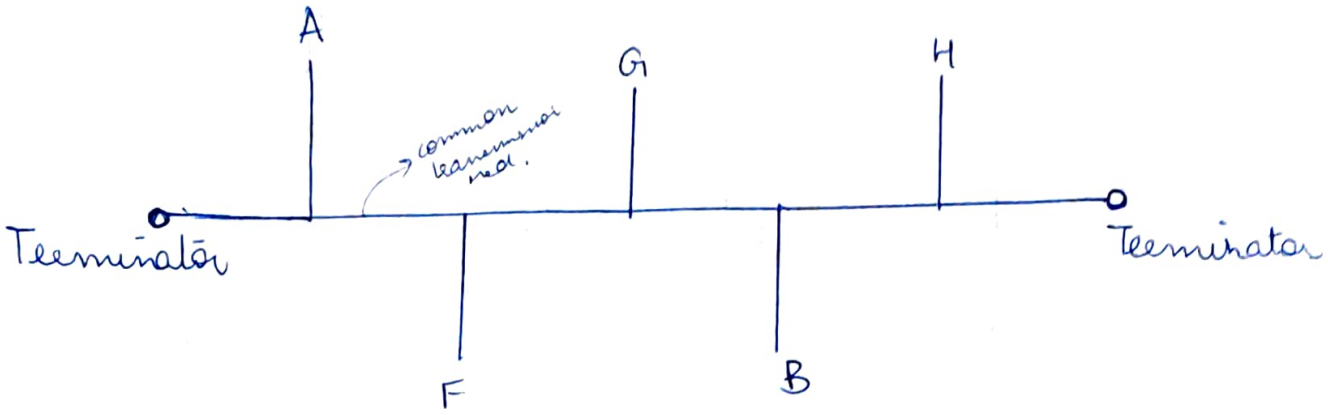
Logical Topology → Deals with data flow in Network

Various Topologies

Bus Topology

- All data transmitted b/w nodes in the network is transmitted over this common Transmission Medium & is able to be recieved by all nodes in Network simultaneously.
- A signal containing the address of the intended recieving machine travels from a source Machine in Both Directions to all Machines connected to the bus until it finds intended recipient.

Ex: data flow → Bi-directional.



Problem → If A sends a data to B, then everyone will receive a copy of data.

Advantages

- Only 1 wire.
  → less expensive
- Suited for Temporary Network
- Node failures does not affect others

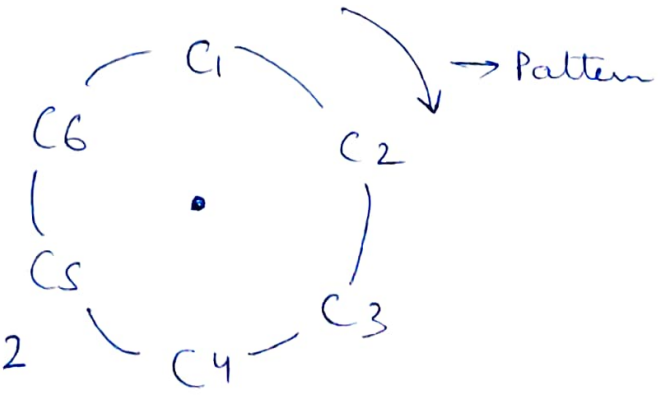
Disadvantages

- Not fault Tolerant (No redundancy)
- Limited cable length
- No security.

Ring Topology

- A ring topology is a bus topology in a closed loop.
- Peer-to-Peer LAN Topology is another Name
  (No one superior, No one inferior)
- Two connections: one to each of its nearest neighbours.
- Unidirectional (A → F) (as communication pattern of ring Topology is always UNI-DIR)
- Sending & Receiving data takes place with help of TOKEN
  (Whoever Node has the Token, it's his/her turn to send data)
  After sometime Token will be Moved to other Node (Next).

No of Nodes = N
No of cables = N
No of ports/device = 2 (NOP)
No of ports in network = N × 2



Advantages

- Performance better than bus topology
- Can cause (bottleneck) due to weak links
- All Nodes with equal access.

Disadvantages

- Unidirectional. Single Point of failure will affect the whole Network
- ↑ in load – ↓ in performance
- No security

Star Topology

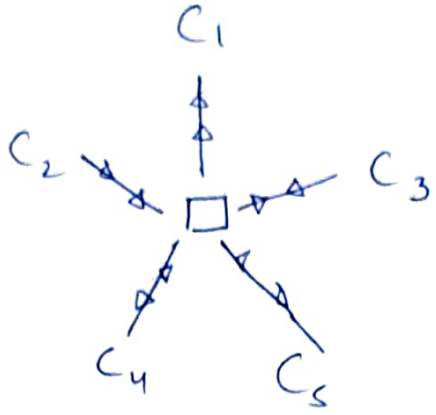
- Every Node is connected to a central Node called a hub or switch.
- Centralized Management
- All traffic must pass through the hub or switch

Advantage: No copy is received as in case of Bus Topology.

No of Nodes = N , No of Cables required = N No of ports in Network 2N

No of ports per device = 1

Example



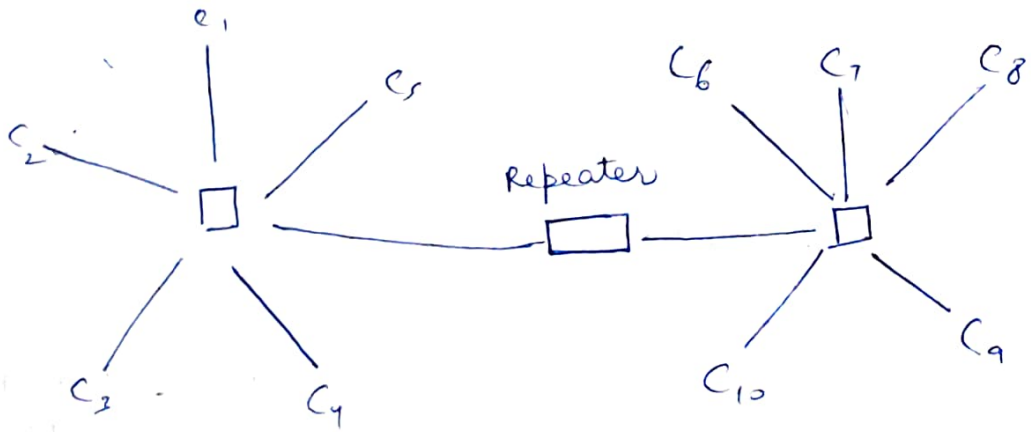
Advantages

- Easy to design & implement
- Centralized administration
- Scalable

Disadvantages

- Single point of failure affect whole Network (central Node failure)
- Bottlenecks due to overloaded switch / hub
- Increased costd due to switch / Hub.

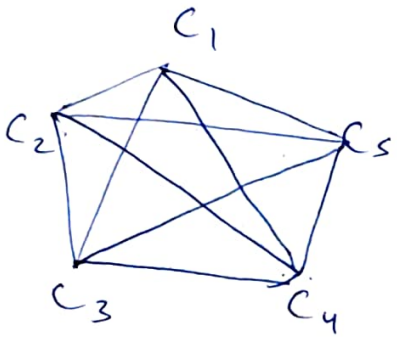
✡ Extended Star Topology



Mesh Topology

- Each Node is directly connected to every other nodes in the network.

- Fault Tolerant & reliable.
  ↳ (somehow your data will reach the destination)



If C_1 fails, there are somany ways to reach other nodes.

advantages

- Fault Tolerant
- Reliable

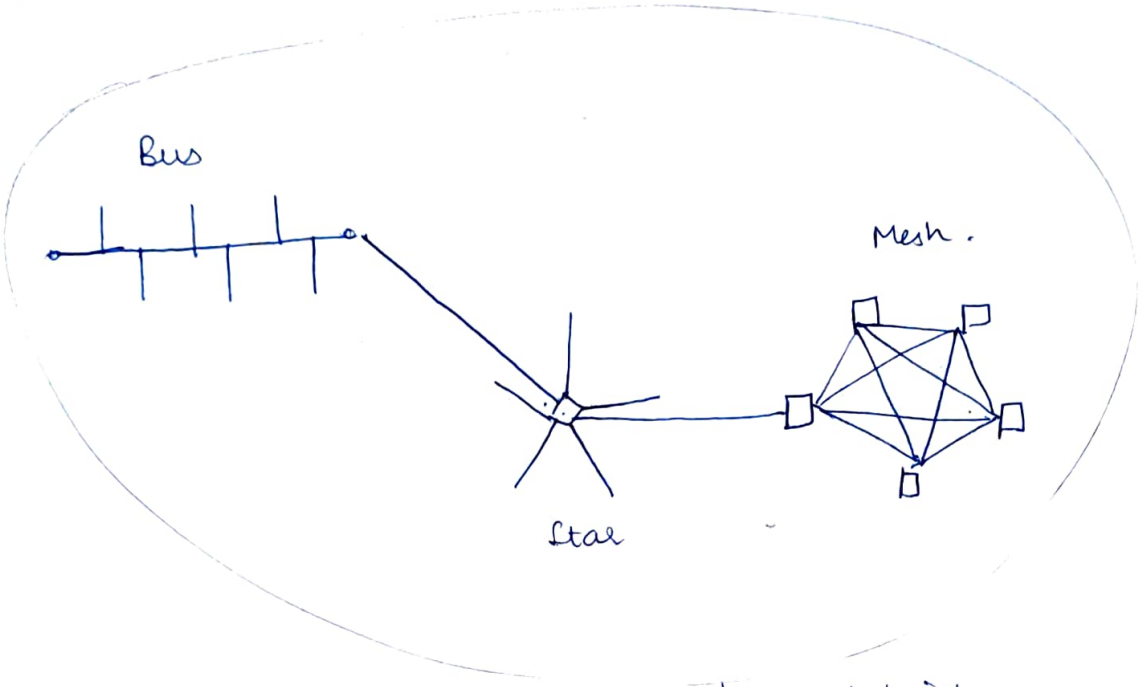
disadvantages

- Issues with Braadcasting Messages.
  (Receiver again sends the message to other Rec)
- Expensive & impractical for large Networks.

Hybrid Topology

More than 1 topology is there in CN.

Ex:



↳ Hybrid.

How to see IP addres in Real device

Start Menu → Cmd prompt

→ type :

ipconfig

under Ipv4 addres

→ u see the addres.

If any data goes from this comp., then this Ip is used for identification of device.

Ex of Valid IP addres

a) 24.25.26.8

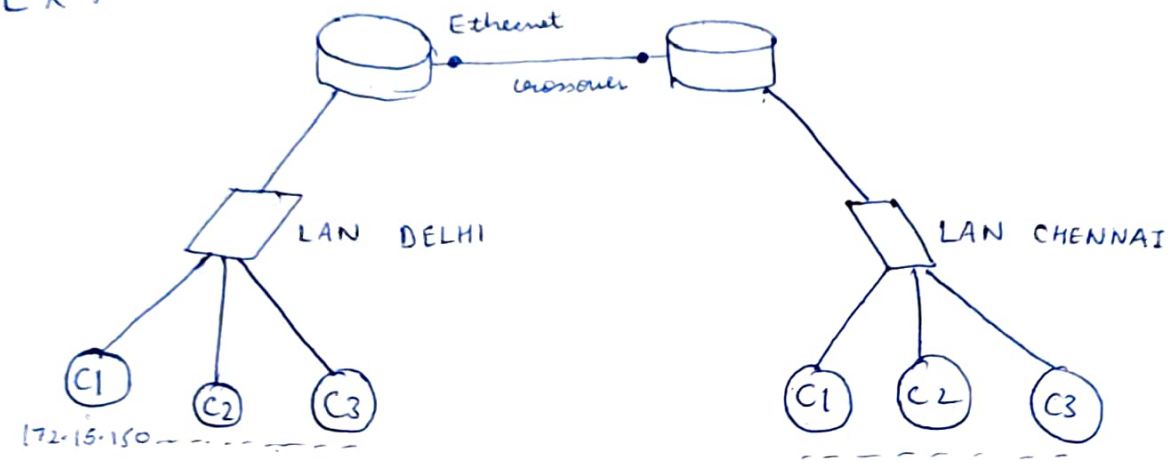
b) 0.0.0.0

d) 255.255.255.255

IP Address

- IP stands for Internet Protocol
- Every node in the computer network is identified by the help IP address.

Ex:



There are 2 variation of IP address

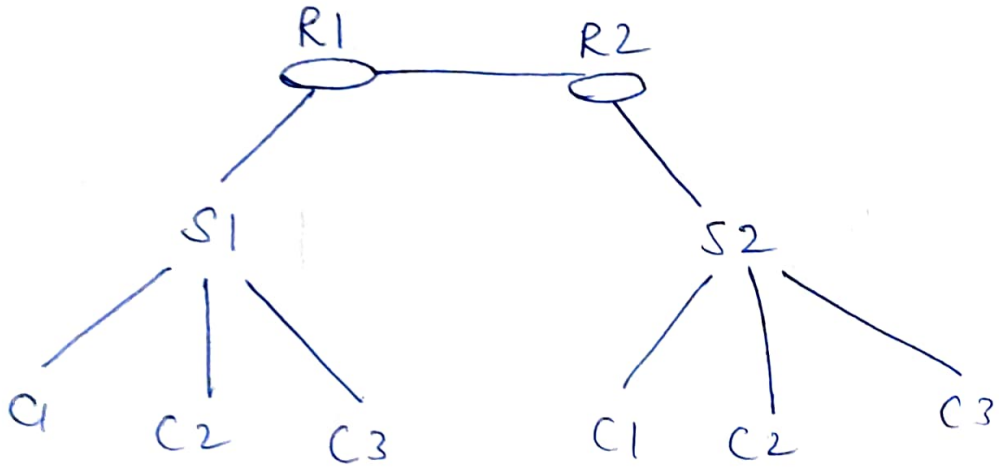
① IP v4

- Every node in computer is identified with help of IP address.
- Logical address because ↓
- can change based on location of the device
- Assigned by manually or dynamically
- Represented in decimal & it has (x.x.x.x) 4 octets
- 0.0.0.0 to 255.255.255.255 (32 bits)

MAC Address

- Mac stands for Media Access Control
- Every node in LAN is identified with help of MAC addres
- IP address = Location of Person (Delhi, Mumbai, London)
  (Wherever the person goes his location gets changed)
- MAC address = Name of Person
  (Name will not get changed)

Routers need IP address, MAC address used by SWITCHES.



Routers identify location, & Switches based on MAC identify device using MAC address to which data is to be received.

- Physical addess or Hardware Address
  ↳ MAC
- Unique
- Cannot be changed
- Assigned by Manufacturer.
- Example : 70-20-84-00-ED-FC (48 Bits)
- Seperator : (-) hyphen, period(.), colon(:)

IP Addess	MAC Address
• Needed for comm.	• Needed for Comm.
• 32 bits	• 48 bits
• Represented in Decimal	• Represented in Hexa decimal
• Router need IP to foward data	• MAC is needed by switches to foword data

How to see Mac addess

→ ipconfig/all

physical addess

Port Addressing : Analogy

Suppose your freind wants to send you a parcel & she lives in CANADA. Lets assume that u are in Mumbai. We need complete address for parcel to reach you. (In complete address details, 1 part of address will Make the parcel reach Mumbai & another part of addres will make the parcel reach your appartment.

If somehow your parcel has reached your appartment, then the last part of this address will Make the parcel to reach you residing in (17th floor) example.

derivations regarding CN

Reaching our city = Reaching our Network (IP Address)

Reaching our appt. = Reaching the Host (MAC Address)

Reaching the Right person = Reaching the right ~~position~~ process (Port Address)

Port addres or Port Number

- In a node, many processes are being running & data which is sent/recieved must reach the right process.

- Every process in a node is uniquely identified using port numbers.

- Port = communication endpoint
- There are fixed port numbers & dynamic P N (0 — 65535)

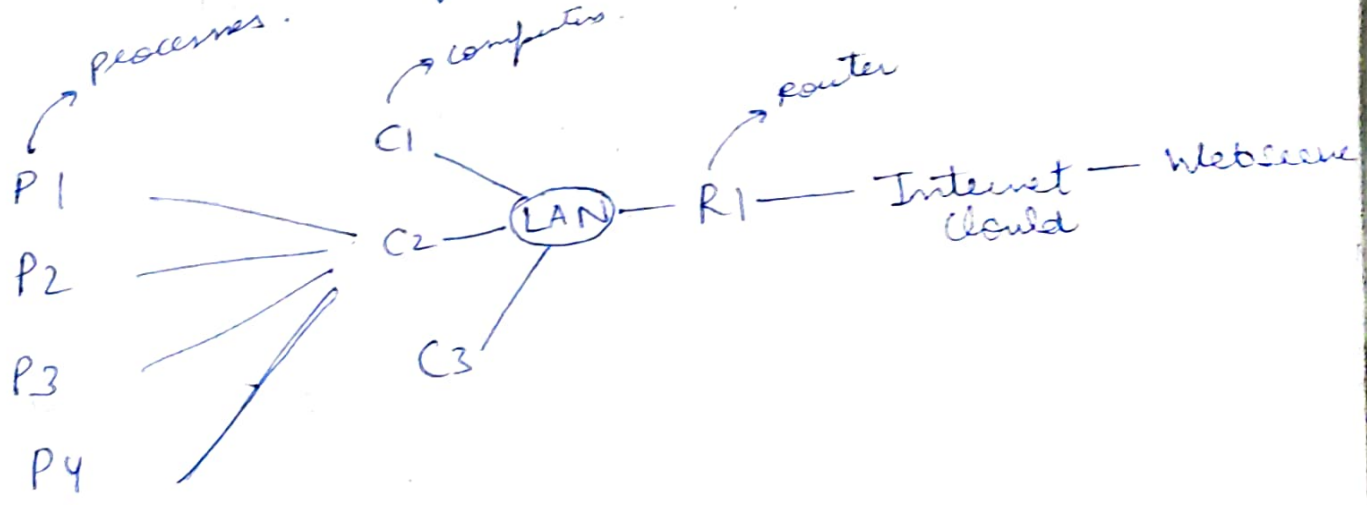
Example

FPN → 80, 25

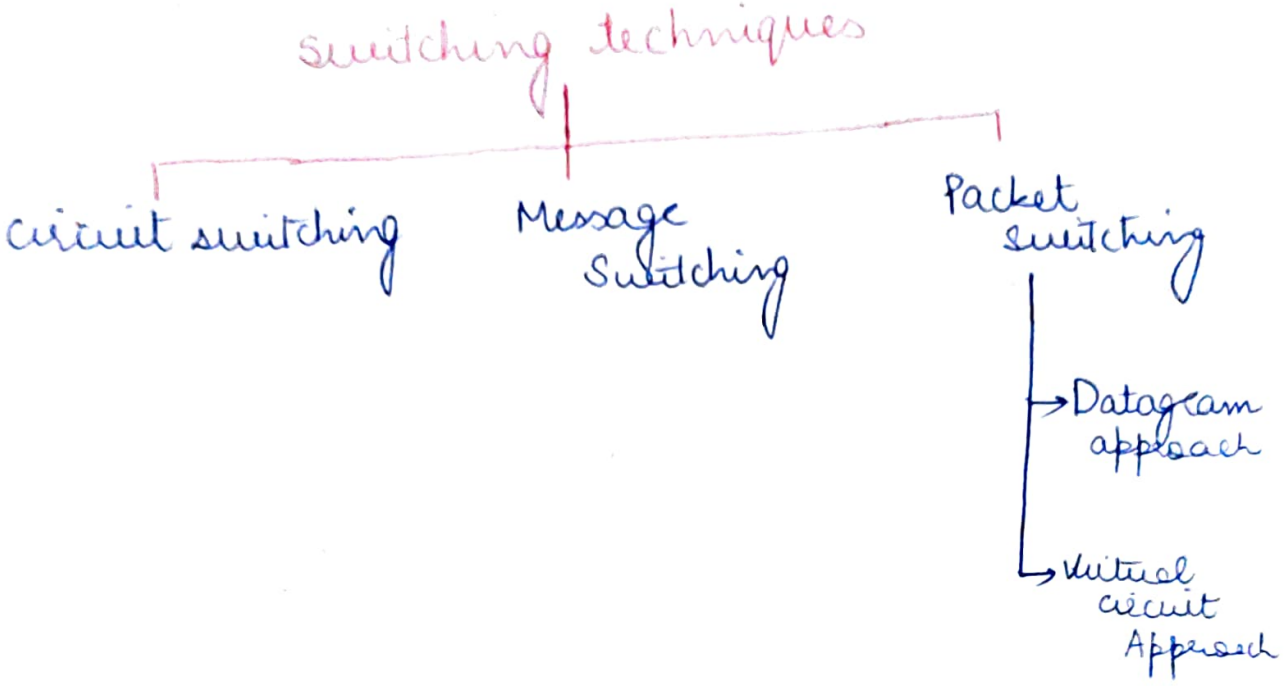
OS assigned dynamic pN → 62414

(If you open Google chrome / fiefox, (a new process), ss, it will be assigied with a pN by OS)

Ex:



Various Switching Techniques



Circuit Switching

- There is always a dedicated path that is established b/w the sender & receiver
- Before Data Transfer, connection will be established first
- Ex: Telephone Network
  Sender first dials the number, once the connection is established, then they can talk to the receiver

3 phases:

1. connection establishment
2. Data transfer
3. connection disconnection

3 pointes to ponder / remember

Before sending data, any node must

- Attach source IP addres & destination IP address (Router)
- Attach source MAC & destination MAC (switch)
- Attach source Port Number (OS) & destination port Number.

Switching

- Switching in computer network helps in deciding best route for data transmisson. if there are multiple paths in a larger network
- It also provide a feel like 1-to-1 connection.

Message Switching

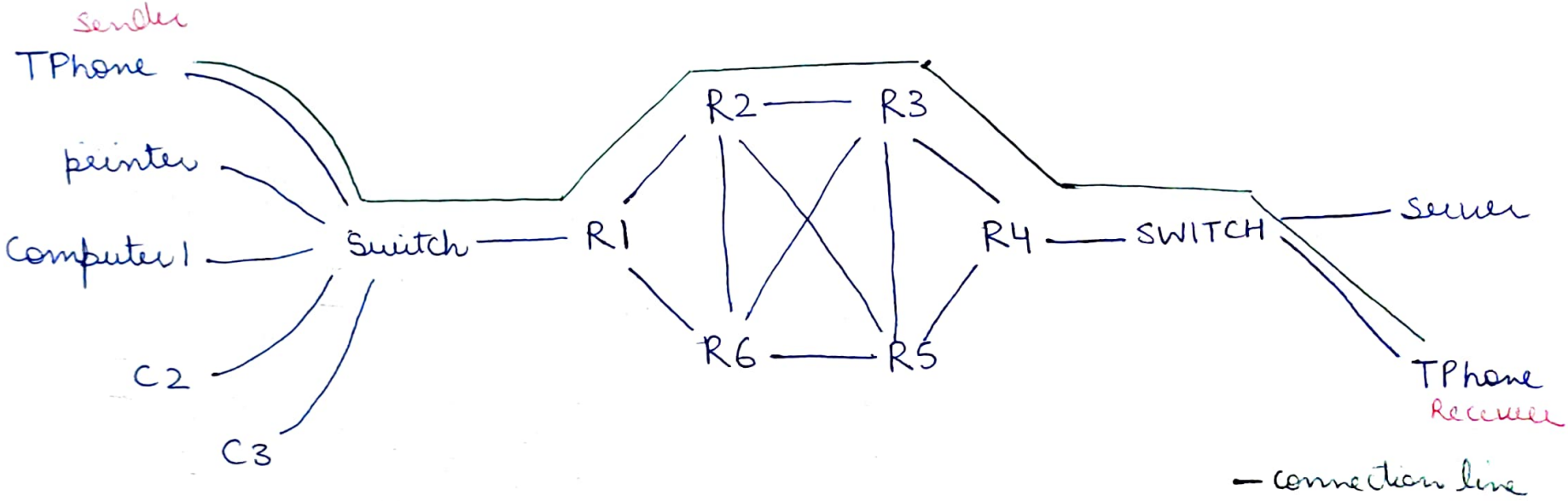
- It uses store & forward Mechanism.
- It means the Message is transfered as a complete unit & forwarded using store & forward Mechanism at the Intermediary Node

Ex: Suppose if sender wants to send a BIG DATA & this BD cannot be transfered in a single stretch. So it is broken into individual pecies/ entities. Each of these pieces are transmitted to intermediary node & this Node receives all the small chunks & constructs the full Mesage. After this, then only it forwards the data.

- It is not suited for real time apps & steaming Media

Ex: Suppose, 2 people are talking over VoIP phone. So we can't expect intermediary node to collect all the data i.e sent by the person & forward it. Because it is a Real time App., message switchy cannot be used.

Example :



1st, connection is established, 2nd data is transfered, all the communication uses this channel or connection line to do all the comm.

After data transmission, connection is closed.

Packet Switching

The INTERNET is a packet switching network.

Here the message is broken into individual chunks called as PACKETS & (Just like Message switching) here the difference is that each packet is sent individually.

So, each of these packets have some information that uniquely identifies the source & the destination

- → source IP address
- → destination IP address
- → Sequence Number

} → Each Packet.

- Sequence Number help the receiver to :→
  1. Reorder the Packets.
  2. Detect missing Packets
  3. Send acknolegdement.

(If a packet gets lost, sender will wait for its acknolegment expiration time & then, sender will re-transmit that packet)

Packet switching : DATAGRAM APPROACH

It is also known as connectionless switching

→ Each independent entity is called as datagram
(if the message is broken into 5 pieces/entity, then each of these 5 pieces are datagram)

→ Each datagram contains destination info & the intermediary devices uses this info to forward datagrams to right distination.

→ In this approach, path is not fixed.
(each datagram may take different routes)
(unlike circuit switching)

→ Intermediary Nodes takes the routing decisions to forward the packets.

Packet switching : VIRTUAL CKT APPROACH

- It is also known as connection-oriented switching.
- In this approach, a preplanned route is established before the messages are sent. (using Virtual circuit Identifier)
- Call accepts & call request packets are used to establish the connection b/w sender & receiver.
- In this app., the path is fixed for the duration of a logical connection.

- The route is decided based on the availability, we can't guarantee that the same route will be used for the next data transfer.

Layering in Computer Networks

Layering means decomposing the problem into more manageable components (Layers)

Advantages

- It provides more modular design
- Easy to troubleshoot

The protocols in each layer governs the activities of the data communication.

(In each layer, we are going to add address of each of these addressing & each of these addressing are taken care by different protocols.)

Different Layered Architecture:

1. The OSI Reference Model
2. The TCP/IP Model

The OSI Model

- OSI stands for Open system interconnection.
- It is a model for understanding designing (reliable) a network architecture i.e flexible, robust & interoperable (If one computer is sending data (generated by WINDOWS OS), this data should be acceptable by other computer in LINUX) (Not only on Architecture But also OS)
- Developed by ISO (International standards for Organizations)
- The OSI Model is not a protocol
- It is only a guidline & hence it is reffered as OSI reference Model.
- The purpose of having this OSI Model is to show how to facilitate communication. b/w different system without requiring changes to the logic of underlying hardware & software.
- The OSI Model was never fully implemented. (guidlines only)

The TCP/IP Model

- TCP/IP = Transmission Control Protocol / Internet Protocol
- The TCP/IP protocol suite was developed prior to OSI model, ∴, the layers in TCP/IP protocol suite do not exactly match those in OSI model
- TCP/IP is a hierarchial protocol made up of interactive modules, each of which provides a special f^n ality (or specific).

So for any comm. to be happen, we need IP, MAC & port addrs. So each layer will take care of each of these addresses so each of these are interactive modules, and each of them does a specific f^n ality.

— x — x —

The OSI Model : Detailed

There are 7 layers in the OSI reference Model.

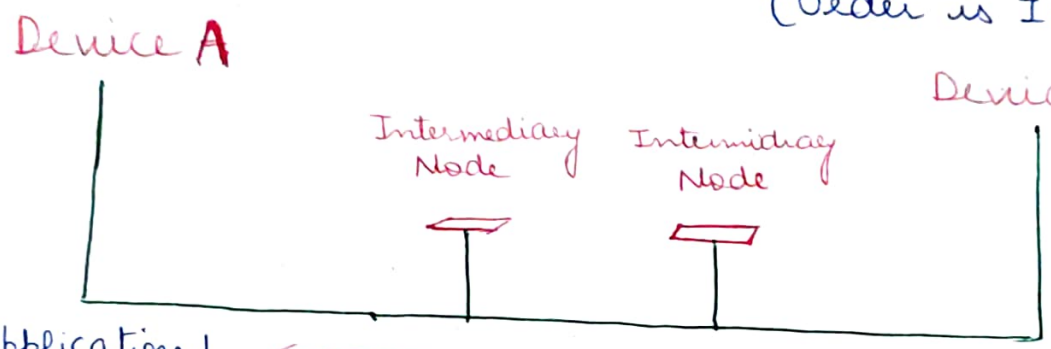
Ex

Away
Pizza
Sausage
Throw
Not
Do
Please

Bottom Up

1. Application layer
2. Presentation layer
3. Session layer
4. Transport layer
5. Network layer
6. Data link layer
7. Physical layer

(Order is IMP)



7 Application L ↕ 7-6 Interface
6 Presentation ↕ 6↔5 Interface
5 Session ↕ 5-4 Interface
4 Transport ↕ 4-3 interface
3 Network ↕ 3-2 interface
2 Data Link ↕ 2-1 interface
1 Physical

peer-to-peer protocol (7th layer) Application 7
peer ..... (6th layer) Presentation 6 (same as peer)
- - - - - - - - (5th layer) Session 5
..... (4th layer) Transport 4
3rd Network ↔ Network ↔ Network 3rd Network 3
2nd Data Link ↔ Data Link ↔ Data Link 2nd Data link 2
1st Physical ↔ Physical ↔ Physical 1st Physical 1

physical communication

The user sitting at Dev A (7 → 1), will open an Application & that application is going to the generate the data. This data is handed over to presentation layer, & then this layer hands over to session layer. then comes the very important point / layer, (The TPT layer) ---- Network ---- Data link ---- then finally it goes to physical layer.

Each layer has its own set of f^n alities.

The Intermidiary Nodes will process the pertaining data only in 3 layers (last, physical, Data link, Network).

Because, we don't want the App data to be accessed by the routers (If someone does that, he is an attacker or a bad guy)

Whatever the data is recieved by Dev B, it is given to physical ⟶ App layer. (1 → 7)

The layers will interact with consequitive layers by the interface provided b/w the layers.

Example

Application layer has generated a confidential data, lets suppose a user sitting at 1 computer wants to send this information to the user who is working in the other computer.

Example Info → My password is Rahul@123.

So the user wants to send this info to other user, this info is given to the presentation layer. It modifies the or converts the content into some format, After the conversion it is then given to session layer (for the session layer activities to carry out) then this info is given to tpt layer, with the data it receives it adds the data or transport layer info, after that this entire content is given to network layer, This layer also adds network layer information & then passes it to Data link layer (it does the same) as above), then it is passed to physical layer, & ∴, it converts the entire content into 0's & 1's. This is sent to the other side of Network or dest. computer. (The physical layer knows, what to which med. it is connected, if wired → it converts entire 0's & 1's into signals; else if ethernet → electrical signals
if fibre optic → light waves.
if wireless → waves.

Application Layer

It enables the user to access the network resources.

Services offered by Application layer:

- File transfer & Access Management (FTAM)
- Mail services
- Directory Services

File transfer & Access Management (FTAM)

lets say Dev A wants to send a file from Dev A to Dev B or Dev A may need a file from Dev B

Dev B → Remote computer
Dev A → Local computer

The user working at Dev A can access a file from Remote computer

MAIL service

The user working at Local computer may need to access email, so again we need the CN to send or recieve emails

Directory services

The application provides access to the data globally.

Presentation Layer

It is concerned with the syntax & semantics of the information exchanged b/w 2 systems.

Services offered

① Translation

→ If devA going to send some data & this data (sender dependent) & we want receiver dependent data also, so converting the data into common format, where that common format is acceptable by both sender & receiver, i.e what Translation is.

② Encryption

→ if devA is sending a confidential Info & we dont want others to see this communication & know the communcation topic, so we want the data to be protected from disclosure or unauth access.

plain Text ⟶ unreadable Text
only sender & receiver can understood

→ senders does encryption & sends the data. receiver does decryption & understands whats the Message is.

③ Compression (very Imp while sending Multimedia Messages)

Reducing the number of bits contained in the info.

Session Layer

It establishes, maintains, & synchronises the interaction among communicating devices.

Services offered

① Dialog control

If we say 2 computers going to communicate with each other, it means 2 processes in these 2 computers are going to communicate with each other,

Session layer allows two systems to enter into a dialog (Dialog means, it is a communication between 2 process to take place in a half duplex (1 way) or full duplex (2 Way)).
at a time

This is what we call as DC.

② Synchronization

The session layer allows a process to add checkpoints or synchronization points

For Ex: If devA is going to send a big file which is of 2000 pages, & it is advisable to insert a checkpoint after every 100 pages to ensure

that the 100 page unit is recieved & acknowledge independently.

In this case if a crash happens during a transmission of a particular page, only that pages can be re-sent.

So this is synchronization; So sender & Receiver must mutually be in a relationship.

Transport Layer

It is responsible for process to process delivery of entire Message.

Services offered

① **Port addressing**

When dev A is sending a message, it uses the source port number & sends the data, upon reception, it is going to reply & that reply is going to reach the sender; after reaching dev B, dev B's OS must handover the data to the right proces This is dont by TPT layer.

② **Segmentation & Reassembly**

Suppose dev A has a very big message. & if this MSG cannot be sent as such. So it can break this Big message into smaller messages, where each MSG can be numbered & after reception of all the indivical messages, this dev B can reassemble the message & construct the oigiral data.

③ Connection control (connection oriented or connectionless oriented)

④ End to End flow control.

→ If the sender is a faster & receiver is a slow receiver so receiver cannot handle the speed, so we are in a need to handle this, or to have a speed Matching Mechanism Where sender & receiver are going to agree upon a common speed matching mechanism, so that whatever the sender sends, the receiver is able to receive it without any loss. (This flow control is b/w end devices, not the intermediary devices)

⑤ Error control

Checking for errors in whatever the tpt layer generates. (transmission errors)

Network Layer

It is responsible for the delivery of data from original source to the destination network.

Services offered

① Logical addressing (IP addressing)

It helps the router to take decision, so when a packet is received by this router, it will have source IP & destination IP. So this router knows, what is the source of that packet & what is the destination of that packet

② Routing

It means finding the best route for the packet to be transmitted, there will be obviously many routes to reach the dest^n. & it is the responsibility of router to find best route, By IP address.

Data link layer

It is responsible for moving data (frames) from one node to another ← in DL Layer only

Services offered

① framing

The DL layer of nodes, it groups the bits of zero's & one's, & we call that grouping as frames.

② physical Addressing (MAC addressing)

When the network layer hands over the data to DL layer, it is the responsibility of DL layer to port the source MAC address & the destination MAC so that the intermediary node/device can take decision by help of MAC address also.

③ Flow control (Same as Tpt layer)

④ Error control

If the frame is corrupted, lost or damaged, it can be easily identified with help of error control techniques

of this layer.

⑤ Access control

When 2 or more devices are connected to same link, then DL layer protocols are necessary to determine which device has control over the link at that time.

Ex: If 3 devices connected to common link The DL layer determines which devices has control over this line only, at that particular time. After the time is over, then it means, it is the turn of other computer to use it.

Physical layer

- It is responsible for transmitting the bits over a medium.
- It also provides electrical & Mechanical specification

Ex:
Suppose if there are 2 computers, after creating the frame (Dev A) & then it is the responsibility of physical layer to place that frame on channel or on the Medium.

- physical layer knows that what is the kind of Medium (wired or wireless).

Services offered

① Physical characteristics of Media.

→ 2 kinds of Media (defines the type of Media)

② Representation of bits
or
Encoding → The physical layer defines the type of encoding (how those zeros & 1's are converted into signals).

③ Data Rate or Transmission Rate

No of bits sent each second.

④ Synchronization b/w bits

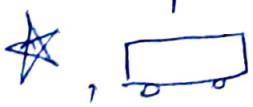
→ The clock b/w sender & receiver must also be synchronized

⑤ Line configuration

determines whether it is a point to point communication (b/w 2 nodes (1 channel exclusively for these 2 Nodes)) or it is a point to multipoint communication

↳ common channel or medium is accessed or shared by Many Nodes

⑥ physical Topology



, Mesh etc.

How devices are connected to Make a Network.

⑦ Transmission Mode,

Simplex, Half Duplex, full Duplex.

Working of OSI Reference Model

Sender's comp. → Receiver's comp.

The sender computer & receiver computer are connected via a network. (so obviously there is a transmission Medium → layer number) So the data generated by App layer is named as D7, & some activity is carried out through (Header 7) app layer (H7) it is then given to Presentation layer, similar process is carried out by all further layers, untill it reach Data link layer & other control related things are added to Trailer part (T2). And finally in physical layer all the data is converted into bits/frames. (zeros & ones)

& thereby it is the responsible of physical layer to take the frames generated by DL layer & place the frames on transmission medium & upon the reception, all the data are received in the form of bits only in receiver side (physical layer of receiver) & it gives the data to DL layer ---- & so on to app layer.

Now whatever data generated by the sender's app layer is transfered to app layer of receiver.

Addressing in Network

IP & Port addressing

Let assume that A ⟶ IP address of sender's computer

P ⟶ IP address of receiver's computer

In sender's computer there are 3 processes running with port Number, a ⟶ ?, b ⟶ ?, c ⟶ ? } port Numbers.

Similarly in receiver's computer, there are 2 processes are running,

with port address → j
k

The data i.e generated at 'a' process must reach at 'j' process.

The data is generated under application layer in 'A' it is added with source port number & destination port number (in Transport layer) as shown (aj)

a → sending
j → recieving

After this, this content is given to Network Layer (Here the source IP & destination IP are added)

Then the entire content is given to data link layer & this layer adds source MAC & destination MAC with it (added in Header H2) & the error control related thing are added to trailer part (T2).

Now the entire content is converted into 0's & 1's & then given to router, this router will forward to other router..... & finally it will received by destination computer (from transport layer in receiver part, it finally delivers the data to process 'j'.

IP & MAC Addressing

IP ← A / 10 → MAC

IP ← Z / 66 → MAC

If the sender computer wants to send the data. (A/10) (A → IP, 10 → MAC), Network layer part is similar as before. In DL layer, in Header particularly, it will add source Mac Address & the destination MAC (20) (In all cases in our networking, we will never try to communicate using MAC addresses, we will leave the computer networking to take care of MAC Addressing, we will always ~~send~~ communicate using names or IP addresses). So what is sender does that, it knows the default gateway for entering into other network For Ex: LAN 1 is Local Area N. ∴, lets imagine there are

are 100 of computers, & this sender's comp. in 1 of the computers in LAN, when this computer wants to send the data in other LAN, it has to hit router port (Interface - 20). So, therefore the MAC address of this interface is 20 & IP → F

i.e Why 20 10 MAC

20 → Interface is called as default gateway as this is the interface or the entrance for this comp. to reach other network (sender ke liye default gateway)

Now once the packet is received by this router, it opens the packet, it collects all the Info in physical layer & Now constructs the data link layer part. Now it opens & sees what is the destination MAC address which is (20). ∴ this router gets to know, this content is for this router. Now it opens N. Layer info & finds different IP address (P). Now router concludes that this packet is not for this router ∴ it removes the old source & destination MAC & puts new source & destination MAC there (33/99) (physical addresses are changed during transmission).

Similarly again this Happens untill it finds same IP address of destination. (i.e P)

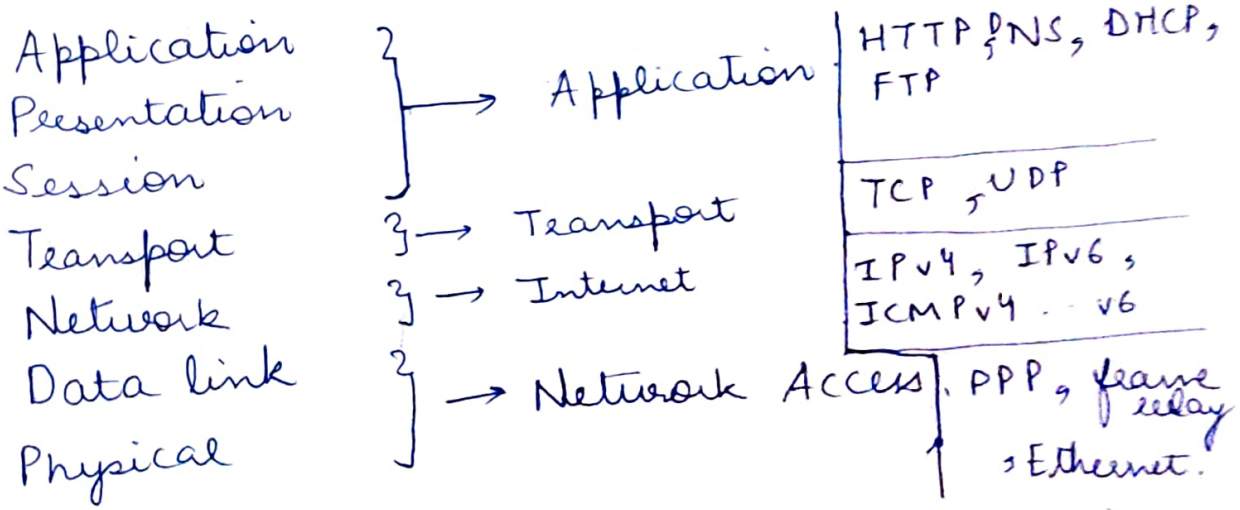
Now receiver computer knows that this is the packet of his own & then it gives the data to APP LAYER.

To reply the sender, the receiver changes the MAC addresses / swap the MAC addresses.

The routers are concerned with collecting the physical layer info, & constructs the data layer part & checking the data layer part whether it is for this router & then it goes to network layer part. So swapping is done only in physical layer part. But the router also checks the Network layer Info / Header N. Layer) i.e why we say that (Router checks PL, NL, DL Layer = NPD) any INTERMEDIARY NODE will always process 3 layer Info. (P, N, DL layer)

TCP/IP Layer or Protocol Suite

We have 4 layers. Network Access, Internet, transport & Application



It is actual Implemented Model, OSI was just a reference Model.

Application Layer

It represents data to the USER, plus encoding & dialog control

Protocols

Name system	Host Config	EMAIL	File Transfer	Web
DNS	BOOTP DHCP	SMTP POP IMAP	FTP TFTP	HTTP

Transport Layer

Supports communication b/w diverse devices across diverse Networks.

Protocols : UDP TCP

Internet

Determines the best path through Network

Protocols (For Routing) : IP (NAT) IP Support (ICMP) Routing Protocols (RIP, OSPF, EIGRP, BGP)

Network Access

Control the Hardware devices & Media that make up the network

Protocols : PPP (Point to point protocol) Ethernet ↓ Wired LAN TECH Interface Drivers

PDU Protocol Data Unit

These are named accd. to the protocols of TCP/IP suite: data, segment, packet, frame, & bits

PDUs can be

Whatever the user generates i.e from APP layer:
The application layer Info / application layer PDU

↓
data

Layer	PDU
Application Layer	Data
Transport layer	Segment
Network layer	Packet
Data link layer	Frame
Physical layer	Bits

Basic Networking Commands

ipconfig → To get IP configuration of the computer

ipconfig/all → give MAC address details also.

nslookup → DNS, Domain Name Server.

→ gives the IP address of server.
type the full address of server in > ⟶

ping domainfull/ipaddress. →

→ Checks whether our computer is able to reach other computer/server.

→ It sends 4 packets to other computer server & then we recieve replies from that computer

It gives details about

→ Packet recieved
→ Palket sent
→ Packet loss.
→ Time.

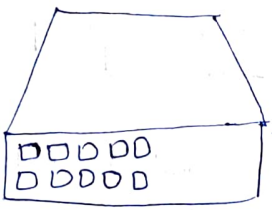
tracert ipaddress/domainName

→ It shows several details about the path, that a packet takes from 1 device to another. (from our comp. to server)

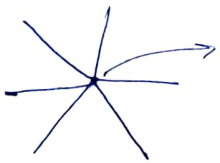
Network devices

HUB

- a.k.a network Hub
- This hub works at the physical layer of OSI Model.
- Used to set-up LAN
- has Multiple ports



- Star Topology



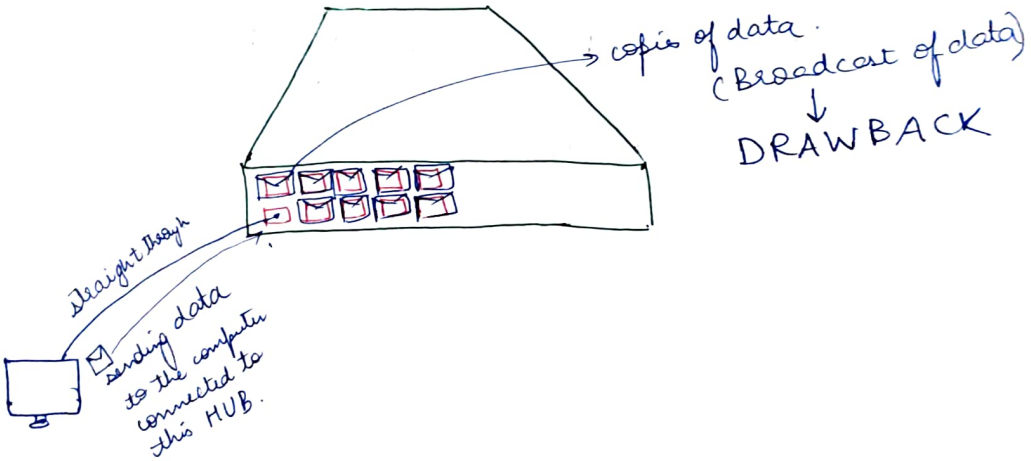
- When a packet arrives at one port, it is copied to the other ports so that all segments of the lan can see all packets

For Ex:

If there are 10 ports in Hub, if a computer is sending a packet in 1 port, then that data is copied in all the remaining 9 ports.

If a computer is receiving an incoming packet & that packet is forwarded to the remaining 9 ports of the HUB, This is the working principal of HUB.

Working



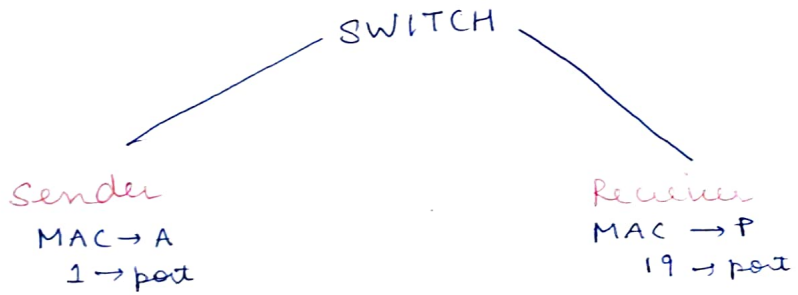
SWITCH

- A switch is a networking Hardware that connects devices on a CN to establish a LAN

- HUB has No Memory, Switch has Memory.
  ↓
  Stores MAC ADDRESS TABLE

- Layer 2 Device (Data link Layer)

Working of a SWITCH



Switch uses some number in order to identify or recognise each of this individual port or interface in switch

MAC ADDRESS TABLE

MAC ADDRESS	INTERFACE/PORT
A	1
P	19

- Less efficient
- Half Duplex

- More Efficient.
- Full Duplex.

Router

A router is a networking device that forwards data packets b/w computer networks.

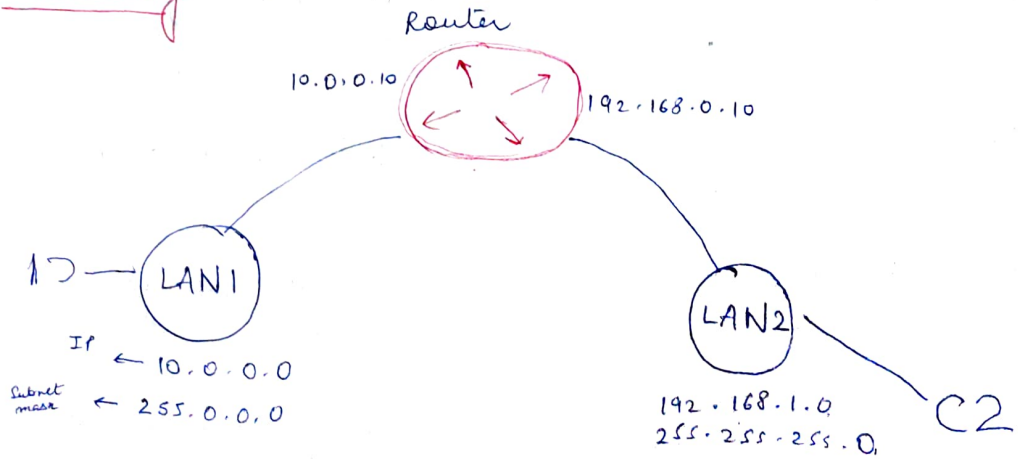
↓

There are 2 different LAN, when these 2 need to communicate with each other, they need a router in order to do this communication.
(unlike switches)

- A router router is connected to at least 2 networks commonly, 2 lans, wans or a LAN & ISP's network (Internet)

- It is a layer 3 (Network layer) device
- Stores routing table in its Memory.

Working



The sender wants to send any data, it sends to port 1 & Now pN 1 received data (if it was HUB) it should have Broadcast it), it knows the destination MAC ADDRESS is connected to which interface i.e 19. So it just forwards the data or the packet to only that interface & the receiver computer now receives this packet. Switch does not flood the entire network (sends exactly).

SWITCH can do UNI, MULTI, BROAD also based on the need

But HUB always Does.

HUB	SWITCH
• Layer 1 device	• Layer 2 device
• Works at physical Layer	• Works at DL layer
• Has No memory	• Has Memory which stores MAC Addr. Table.
• Not an intelligent device	• Intelligent device
• Floods the Network	• can do UNI, MULTI, BROAD casting
• Security risks are High	• Security risks are low

lets say 1 interface (10.0.0.10) is connected to LAN 1 & another is to LAN 2. (→ 192.168.1.19)

Let there are 2 computers (C1: 10.0.0.8 → LAN 1; C2: 192.168.1.5 → LAN 2)

If C1 wants to communicate with C2 (different IP scheme) (these two computers are belonging to 2 different Network) (so switch can't establish communication). (so we need a router for this comm)

Suppose C1 wants to send a message to C2,

→ the data will be received at (10.0.0.10 Interface)

→ Now after receiving, this router will send the data to other LAN (192.168.1.0).

→ & hence the data is received by 192.168.1.5

default gateway → IP address of the first router that is going to hit first.

LAN 2 → 192.168.1.10

LAN 1 → 10.0.0.10

Switch

- A network switch is a compute networking device that is used to connect to many devices together on a CN.
- Operates at DL layer (2nd)
- Has Memory & Stores MAC address table.
- Decisions are taken based on MAC
- Half/full Duplex
- LAN

Router

- A router is a N device that connects a local network to other networks.
- Operates at Network layer.
- Has Memory & stores routing table.
- Decisions are taken on IP address.
- Full Duplex
- WAN, MAN, LAN

Repeater

Suppose, if a proffesor is delivering a lecture in class-room (students at 1st row can Hear > ..... at last Row).

Reason: The speech of proffesor is an alaog ~~digited~~ signal. The signal what gets generated from his mouth tend to loose its stength when it travels a long distance.

Likewise:

The data signals generally become too weak or corrupted if they tend to travel a long distance.

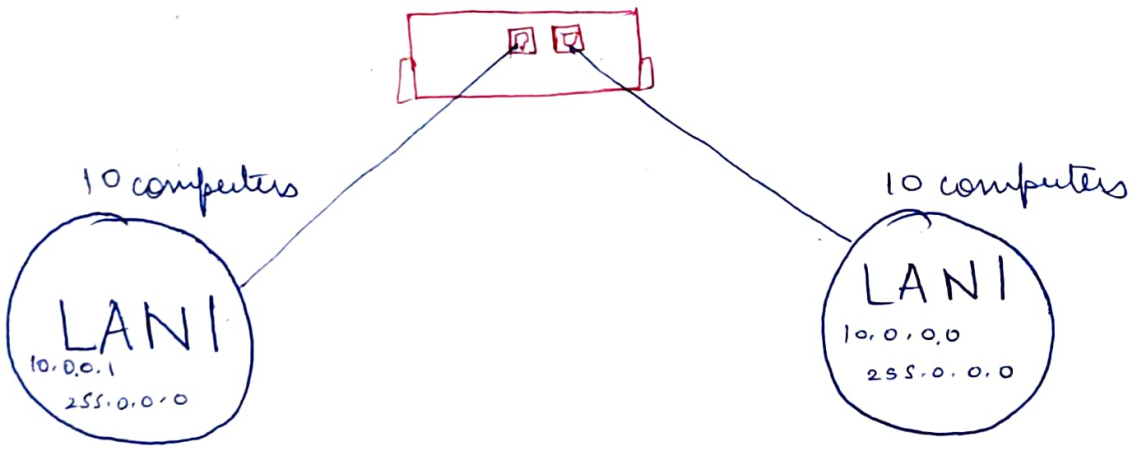
& hence, we need a device to regenerate the signals.

- Repeater regenerates the signal over the same network
  ↓
  same Network

- Layer 1 device ⟶ physical layer
- They donot amplify the signal
- 2 port device

Working of repeater

(organisation
2 different Buildings
at some dist.



This organisation does not want to establish 2 diffeent networks for these 2 diffeent buildings, It means they dont want 2 diffeent LANs

The repeater solves the problem Here,

If LAN1 (left) which has a computer wants to send data to LAN1 (right) then

The repeater gets the signal from LAN1 (left) & regenerates the signal & send it to building 2 NO. (right) LAN.

Bridge (Bridge = Repeater)

- A bridge is normally a repeater but with some additional functionalities.

Bridge = Repeater + f"ality of reading MAC addresses)

- Layer 2 device (Whenever a device deling with MAC, it is a layer 2 Device).

- It is also used for interconnecting 2 LAN's on the same protocol

- It is a 2 port Device

Types of Bridges

1. Transparent Bridges

These are the bridge in which stations or nodes are completly unaware of bridge's existence.

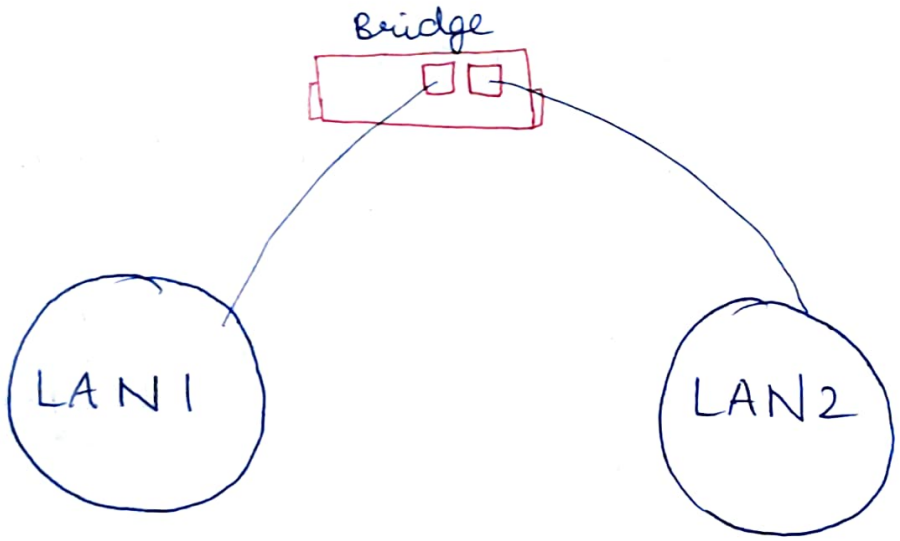
Reconfiguration of the stations is unecessary even if the bridge is added or removed from Network.

Source Routing Bridges

In these bridges, routing operation is performed by source node & the frame specifies which route to follow.

For Ex: In a LAN, there is a source Node/station, if that node is going to send some data to other node, then this Node, that is source stn. will have the routing info., how this frame has to reach the destination.

Working of a Bridge



This bridge extends the range of LAN & interconnects these 2 Networks. (running on a same protocol)

Bridge

- On same protocol (connects 2 different LAN)
- LAYER 2 device MAC ADDRESS

Router

- two different Protocol (2 different LAN)
- LAYER 3 device (IP address)
- Changes physical address in a packet

Multilayer Switch (Layer 3 switch)

- Generally switches are layer 2 devices, (stakes decision on IP addresses) (routing)
- A multilayer switch can be a layer 2/3 device as well as
  → It does the f^n ality of switch as well as a Router to some extent.

Brouter (Bridge + Router)

A bridge can connect 2 different LAN segments of same protocol, a router can connect 2 or more different protocols.

But brouter is a combination of Both.
It can act as a Layer 2 Bridge or Layer 3 router.

Modem

Modulator & Demodulator.

↓ the digital info is going to be carried on an analog carrier signal

& demodulator first retrieves the transmitted signal.

Ex: In a Traditional LANDLINE phones (voice signals Analog.) Modem does both modulation & demodulation. tasks.

Firewall

It is a networking device only (mainly used for providing security to Network.

For Ex: If we deploy a firewall in our campus this firewall filters the packet, it filters the packet based on IP address, port Numbers, application data. (In a network, you dont want any malicious thing to happen)

A firewal filters the incoming traffic as well as outgoing traffic