Computer Networks:-

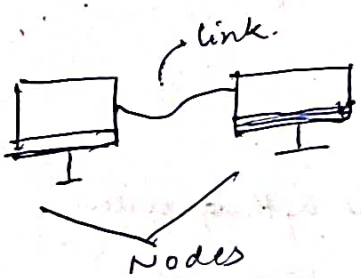
Computer Network:-

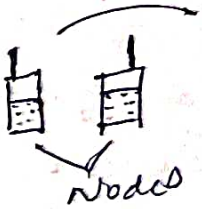
- A computer network is a set of nodes connected by communication links.

A node can be a computer, printer or any other device capable of sending/receiving data generated by other nodes in the network.

eg:- computer, server, printer, security camera and many more (switches, bridges, Routers, etc.)

A comm. link can be a wired or wireless link.
The link carries the information.





Links

medium :- wired - cable
wireless - air.

- A computer network allows resource sharing.

eg: a printer can be connected to different computers

- A networks has:-

1) End devices :- where the flow of data starts or terminates.

2) Intermediary nodes:- through which nodes the data traverses.

Basic characteristics of computer network :-

- Four basic characteristics any computer network should possess :-

1) Fault tolerance
2) scalability
3) ~~Qoss~~ Quality of service (QoS)
4) Security.

Fault tolerance :- The ability of computer network to :-

1) continue working despite failure (choosing other feasible route)
2) ensure no loss of service.

scalability :- The ability to :

1) grow based on needs
2) Have good performance after growth.

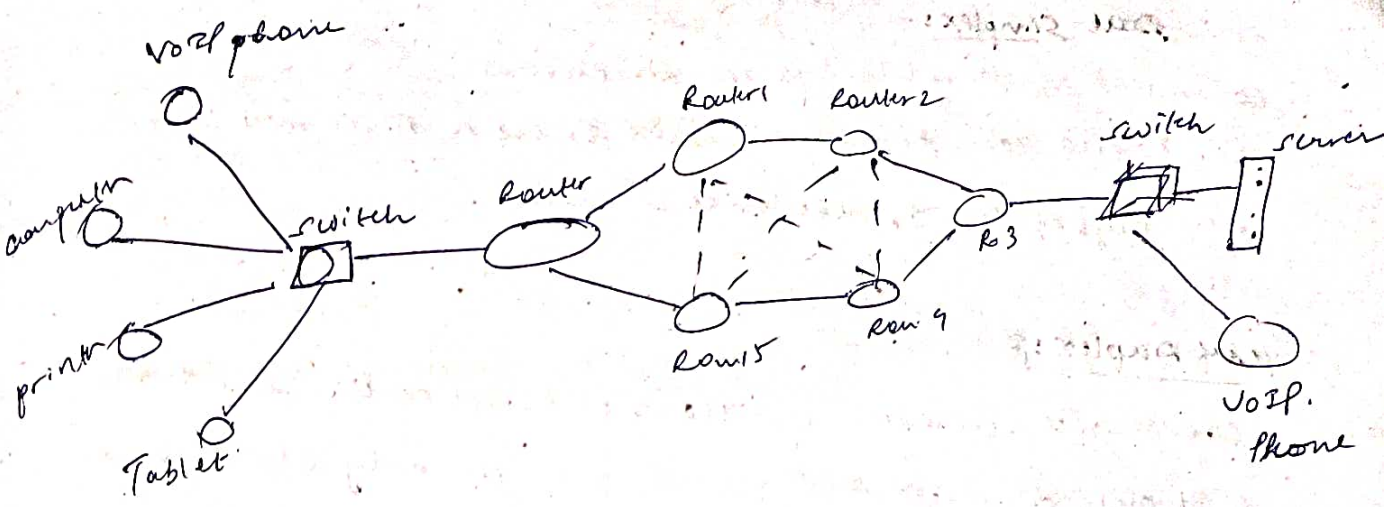
eg: Internet

Quality of service :- The ability to :

1. set priorities
2. manage data traffic to reduce data loss, delay, etc.

Suppose two packets of data arrive, the network should be able to identify which packet should be processed first.

eg: whatsApp call and email communication happen through the same ~~network~~ internet, so the priority should be given to the voice-over → whatsApp call. because delays are not acceptable in real-time comm.



Security:- Ability to prevent:-

1) unauthorized access
2) misuse
3) Forgery

The ability to provide:-

1) confidentiality
2) Integrity → (the data that is sent is not modified or changed)
3) Availability.

Network protocols and communication:-

Data communication:-

* Data communications are the exchange of data between two nodes via some form of link (transmission medium) such as cable.

Data flow:- How the data is going to flow from one node other node. There different ways are:-

1) Simplex
2) Half duplex
3) Full duplex -

~~Dat~~ Simplex :-

- Communication is always unidirectional.
- One device can transmit and the other device will receive.

eg:- Keyboards, Traditional monitors

Half Duplex :-

- Comm. is in both directions but not at the same time.
- If one device is sending, the other can only receive, and vice-versa

eg:- Walkie-talkies.

Full duplex :- Comm. can happen in both directions simultaneously

- Devid can send and receive at the same time.

eg:- Telephone line

~~Protocols:~~ Protocols :

All communication schemes will have following things in common:- (whatsapp, sms, etc.)

1) Source or sender
2) Destination or receiver
3) Channel or media

~~Rules~~ Protocols are rules that govern all methods of communication.

· Protocols determine :-

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

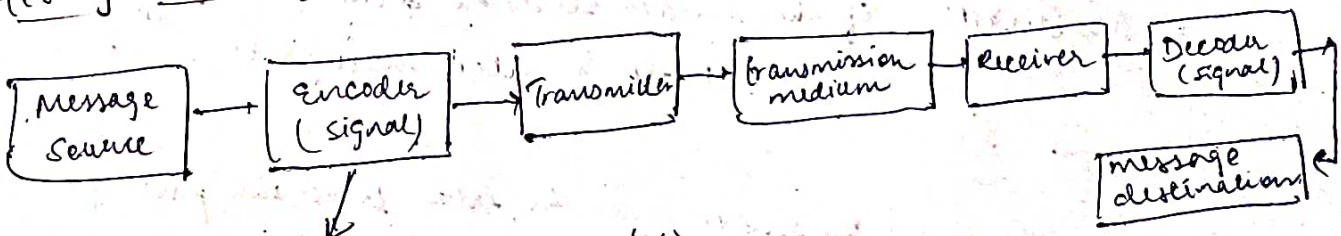
Protocols used in network communication also define :-

* Message encoding
* Message formatting and encapsulation
* Message timing
* Message size
* Message delivery options.

Elements of protocol :-

1. Message encoding
2. Message formatting and encapsulation.
3. Message timing
4. Message size.
5. Message delivery options.

Message encoding :-



waves in case of wireless
electrical in case of wired.

Message formatting and encapsulation :- (If addresses are added [illegible] and data.)

- Agreed format
- Encapsulate the information to identify the sender and receiver rightly

Message sizing :- → each small packet is numbered. So that they get arranged in order upon reaching dest. and a missing packet can be detected.

- Humans break long messages into smaller parts or sentences.
- Long messages must also be broken into smaller pieces to travel across a network.

Message timing : → to avoid data loss.

- * Flow control → sending and receiving speeds.
- * Response timeout. → how much time to wait before sending other data packet if no acknowledgement is received.

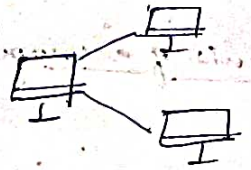
message Delivery options :-

- Unicast :- One sender and one receiver. The sender is going to send data to exactly one receiver

- Multicast: If the sender sends the data to a set of receiver but not all is called multicast

- Broadcast: The sender sends the data to all the participants in the ~~new~~ network

peer-to-peer network

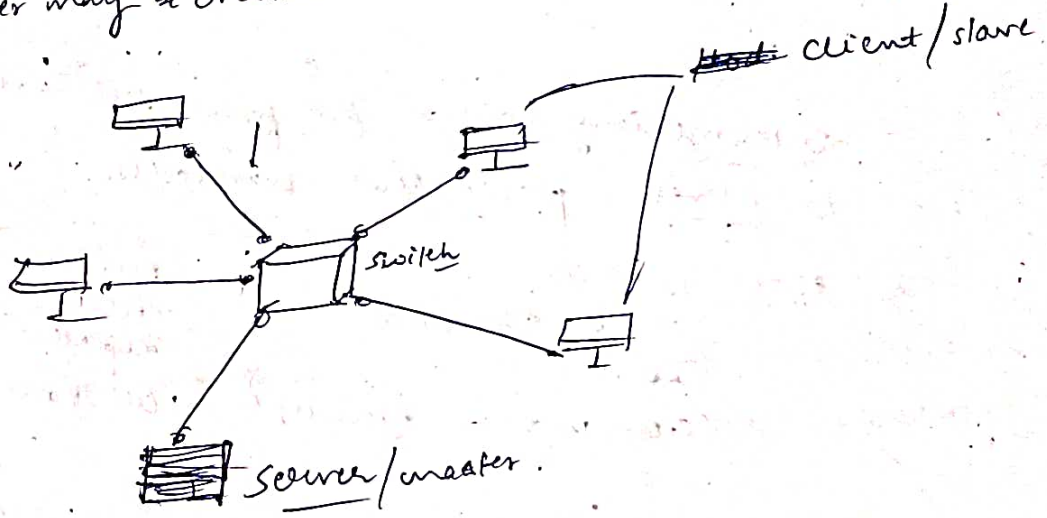


* No centralized administration
* All peers are equal.
* Simple sharing applications.
* Not scalable. (a system has n ports to connect to n number of devices, the network is not scalable.)

→ Every system has all sorts of rights.

client-server network :-

* centralized administration
* Request-response model.
* Scalable
* Server may be overloaded.



Components of a computer network:-

1. Nodes
2. Media
3. services

(1) **Nodes:-** End nodes (End devices)
Intermediary nodes.

~~eg:-~~

End nodes :- eg:- computers
Network printers
VOIP phones
Telepresence endpoint
Security cameras

Intermediary nodes:- that forward the data from one node to other placed b/w end nodes.

eg:- switches
wireless Access Point
Routers
security devices (Firewall)
Bridges
Hubs
Repeaters
Cell Tower

(2) **Media:-** link
- wired medium (guided medium)
- wireless medium (unguided medium)

Wired eg:- Ethernet straight through cable → two different devices
Ethernet crossover cable → two devices of same kind.
Fibre optic cable
coaxial cable (TV.) → for audio and video comm
USB cable

Wireless media:- eg: Infrared (short range comm., eg remote)
Radio (eg:- Bluetooth, Wifi)
microwaves (cellular system)
satellite (long range communication :- GPS).

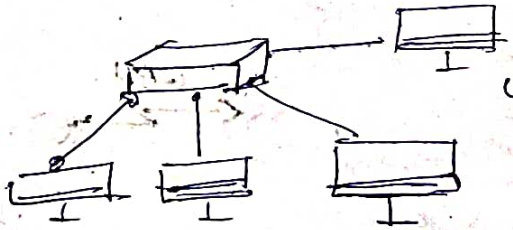
~~Eg:~~ 3 Services:-

email
storage services
file sharing
online game
voice over IP
WWW.

Classification of computer networks :-

1) LAN (Local Area Network)
2) MAN (Metropolitan " ")
3) WAN (Wide " ")

. LAN:- A computer network that interconnects computers within a limited area such as residence, school, laboratory, university campus or office building.



All these comp can communica with each other internally.

LAN devices:-

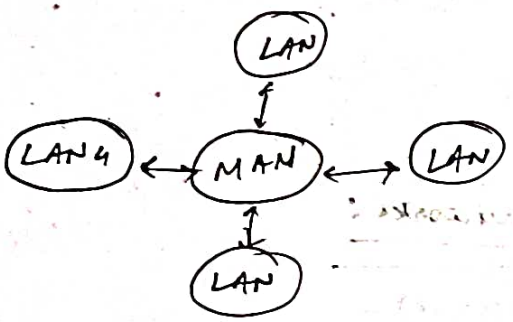
* Wired LAN (Ethernet, Hub, Switch)

x Wireless ~~network~~ LAN (Wifi).

MAN: A metropolitan area network is a comp. network that interconnects users with computer resources in a geographic region of the size of a city.

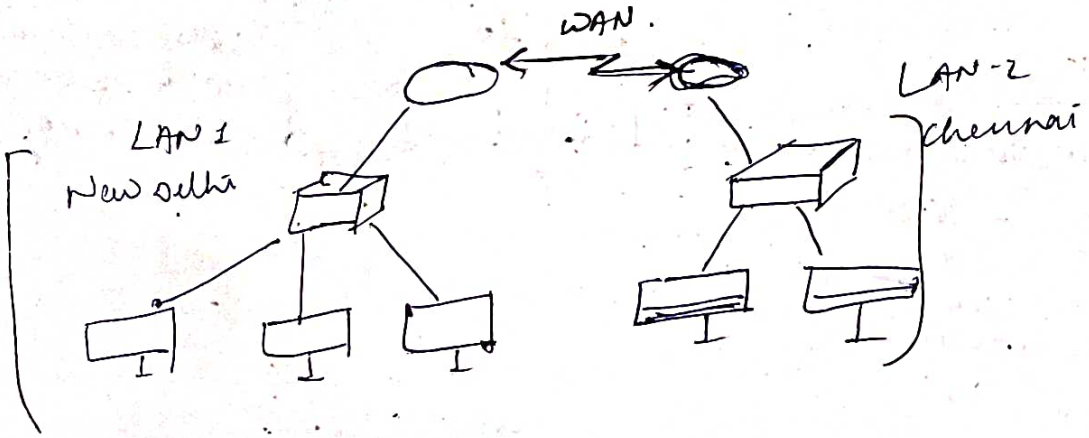
devices used:- · switches / hubs
Routers / Bridges

switches / hubs are used to establish LAN
Router / bridges connect two LANs



WAN:- It is a telecommunication network that extends over a large geographical area for the primary purpose of computer networking. → distant communication

eg: end devices and intermediary devices



- The internet can be called as wide WAN.

SAN :

Cloud computing :- on demand availability of comp-resources, especially data storage and computing power, without direct active management by the user.

Network Topology :-

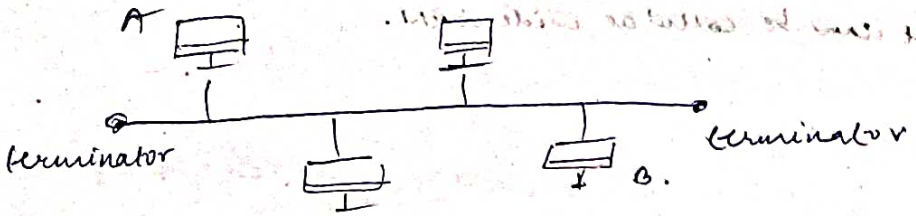
Arrangement of nodes of a computer network so that they can communicate with each others

Topology - layout.

Topology
- Physical top. — Placements of various nodes.
- Logical top — Deals with the data flow in network

Types :-
1) Bus
2) Ring
3) Star
4) Mesh
5) Hybrid

Bus :-
- All data is transmitted b/w the nodes over a common transmission medium and is able to be received by all nodes in the network simultaneously.
- A signal containing the address of the intended receiving machine travels from a source machine in both direction to all machines connected to the bus until it finds the intended recipient.



Advantages

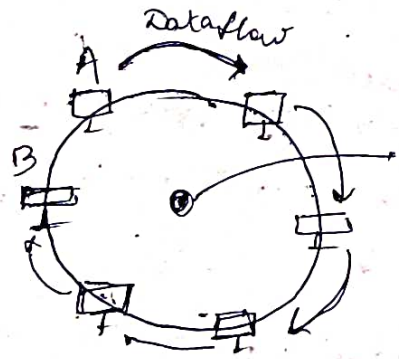
1. Less expensive
2. Suited for temporary network
3. Node failures does not affect others.

Disadvantages

1. Not fault tolerant (No redundancy). If an error occurs in transmission line the complete communication comes to a stand still.
2. Limited cable length. (Scalability problem)
3. No ~~new~~ security.

Ring topology:- A ring top. is a bus top. in a closed loop.

- Peer = to-peer LAN topology
- Two connections = one to each of its nearest neighbours.
- Unidirectional flow of data.
- Sending and receiving data takes places by ~~the~~ the help of token.



If A wants to send data to B,

- The node that has the possession of the token is only allowed to send data. This all the nodes get opportunity to send the data

Advantages

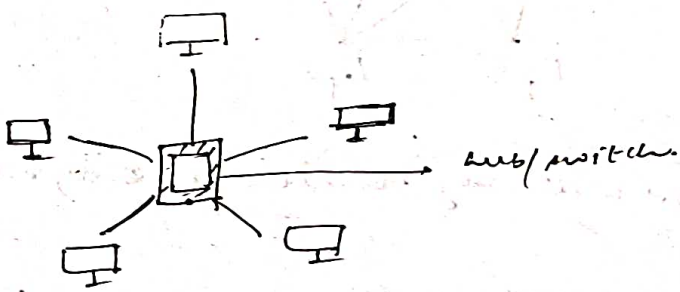
- Performance better than bus topology.
- Can cause bottleneck due to weak links.
- All nodes with equal access.

Disadvantages

1. Unidirection. Single point of failure will affect whole network
2. ↑ in load, ↓ in performance
3. security. (The data needs to pass on from different nodes before reaching the destination.)

Star topology:-

- Every node is connected to a central node called a hub or switch.
- Centralized management. (by hubs and switches)
- All traffic must pass through the hub or switch.



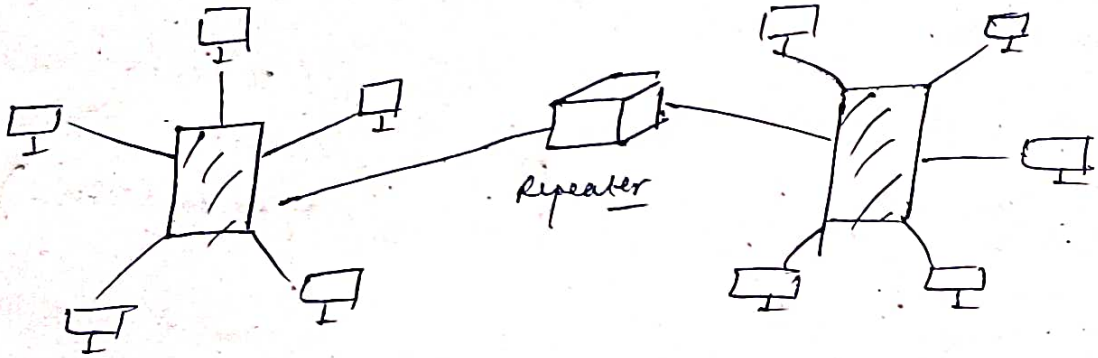
Adva-

- Easy to design and implement
- Scalable
- Centralized administration.

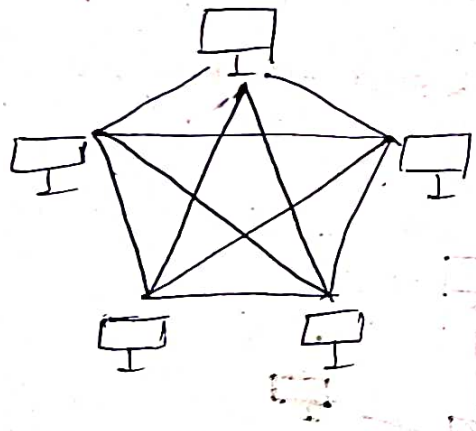
Disad.

- Single point of failure affects the whole network
- Bottlenecks due to overloaded switch/hub
- Increased cost due to hub/switch.

Expanded star topology (combination of two or more star topologies connected by a repeater).



Mesh topology :-



* Each node is directly connected to every other nodes in the network.
* Fault tolerant and reliable

Advantages:

- Fault tolerant
- Reliable

Disadvantages

- Issues with broadcasting messages
- Expensive and impractical for large networks.

~~Upon b~~ - when broadcasting is being done by the sender, the receiver nodes also broadcast the same message to the sender back again.

Hybrid: Topology with one or more different topologies.

Q. Traffic problem can be minimized by :?

Ans: Mesh Topology (Each of the nodes is connected with each other through separate cable).

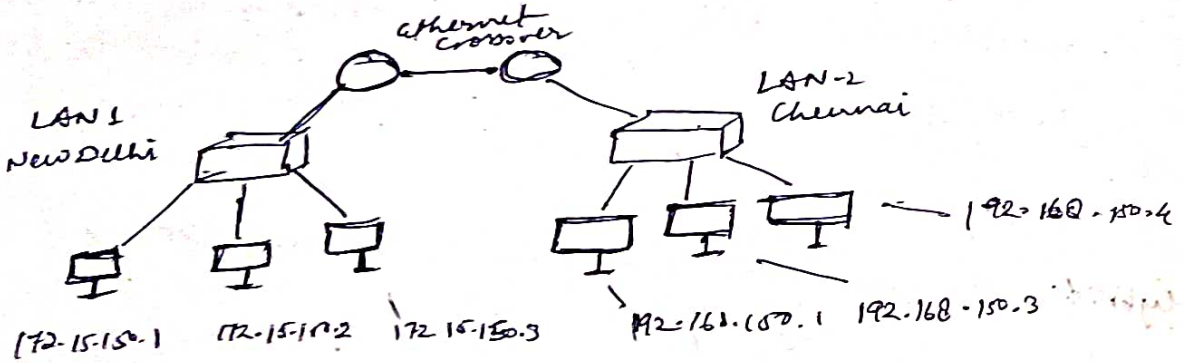
Q: How many ports are required if there are n number of nodes in a star topology?

Soln: $n \times 2$.

Basics of IP addressing:

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

- Every node in the computer network is identified with the help of IP address.



IP address (IPv4)

* Every node in the computer network is identified with the help of IP address.
* Logical address (depends upon location)
* Can change based on the location of the device.
* Assigned manually or dynamically
* Represented in decimal and it has 4 octets (x.x.x.x).
* 0.0.0.0 to 255.255.255.255 (32 bits).

0 → 255.

→ 16.28.45.67 is not a valid IPv4 address.

IPv6 addressing:- It is 128 bits in length and consists of 16-bit ~~field~~ fields, with each field bounded by a colon. Each field must contain in hexadecimal number, in contrast to the dotted-decimal notation of IPv4 addresses.

MAC address:-

* MAC address stands for Media Access control.
* ~~LAN~~ Every node in the LAN is identified with the help of MAC address.
* IP address = Location of a person (may change)
* MAC address = Name of the person. (does not change)

→ Routers need IP address
→ Switches need MAC address.

→ Every node in the LAN is identified with the help of MAC address.
→ Physical address or Hardware Address.
→ Unique.
→ Cannot be changed
→ ~~Assign~~ Assigned by the manufacturer.
→ Represented in hexadecimal.
→ Example :- 70-20-84-00-ED-FC (48 bits)
→ Separator: ~~hyp~~ hyphen (-), period (.), colon (:) depends on manufacturer

IP address	MAC address
· 32 bits · Represented in decimal · Router needs IP address to forward data eg:- 10.24.250.65	· 48 bits · Represented in hexadecimal · Switch needs MAC address to forward data · 70-20-84-00-ED-AC

Switching techniques in Computer Networks:-

It is basically finding the best route for transferring the data from sender to receiver and particularly in a large network.

Switching techniques

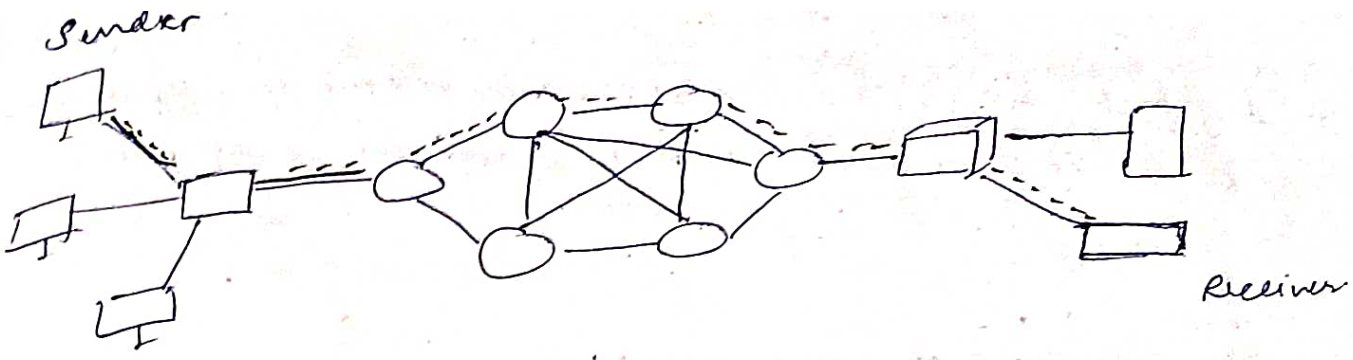
- Circuit switching
- Message switching
- Packet switching
  - Datagram approach
  - Virtual circuit approach.

Circuit switching:- · a dedicated path is established b/w the sender and receiver

· Before data transfer, connection will be established first

· Eg:- telephone network.

3 phases of circuit switching:- (i) Connection establishment
(ii) Data transfer
(iii) connection disconnection



--- path set-up.

Message switching:-

* Store and forward mechanism
* ~~Message~~ Large message is broken into parts and the parts are transferred to the intermediary nodes. Upon arrival of all the parts at intermediary nodes, the message is then ~~if forward~~ forwarded further.
* Not suited for real-time communication systems. like streaming live media content, ~~etc~~. calls, etc

((Draw diagram).

Packet switching:-

* The internet is a packet switched network.
* ~~Data~~ Message is broken into individual chunks called as packets
* Each packet is sent individually.
* Each packet will have source and destination IP address with sequence number
* Sequence numbers will help the receiver to
  (i) Reorder the packets.
  (ii) Detect missing packets
  (iii) send acknowledgements.

* Any packet may be received at the receiver's end in any order. So the sequence number helps to arrange the message packets correctly.

Two approaches to packet switching are:-

1) Datagram approach
2) Virtual circuit approach.

Datagram approach:-

* Datagram ~~packet~~ packet switching is also known as connectionless switching.
* Each independent entity is called as datagram.
* Datagrams contain destination info. and the intermediary device uses this info. to forward datagrams to right destination.
* In datagram packet sw., the path is not fixed. (Each datagram can take different route).
* ~~Intermediary nodes~~
* Intermediary nodes take the routing decisions to forward the packets.

Virtual circuit approach:-

* Virtual circuit switching is also known as connection-oriented switching.
* In case of virtual circuit switching, a preplanned route is established before the messages are sent.
* Call accept and call request packets are used to used to establish the connection b/w sender and receiver.

* In this approach, the path is fixed for the duration of a logical connection. (different path is allotted, the next time a connection is estb.).

Layering

Layering means decomposing the problem into more manageable components (layers).

Advantages:-
1. Provides more modular design
2. Easy to troubleshoot.

Role of protocols —
* Set of rules that governs data communication.
* The protocol in each layer governs the activities of the data communication.

Two types of layered architecture are :-
1) OSI reference model
2) TCP/IP model.

OSI model:

* OSI stands for Open System Interconnection.
* It is a model for understanding and designing a network architecture that is flexible, robust and interoperable (-meaning able to communicate with to systems having different OS installed. etc.)
* Developed by ISO
* It is not a protocol.
* It is only a guideline and hence referred to as OSI reference model.

- The purpose of OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.

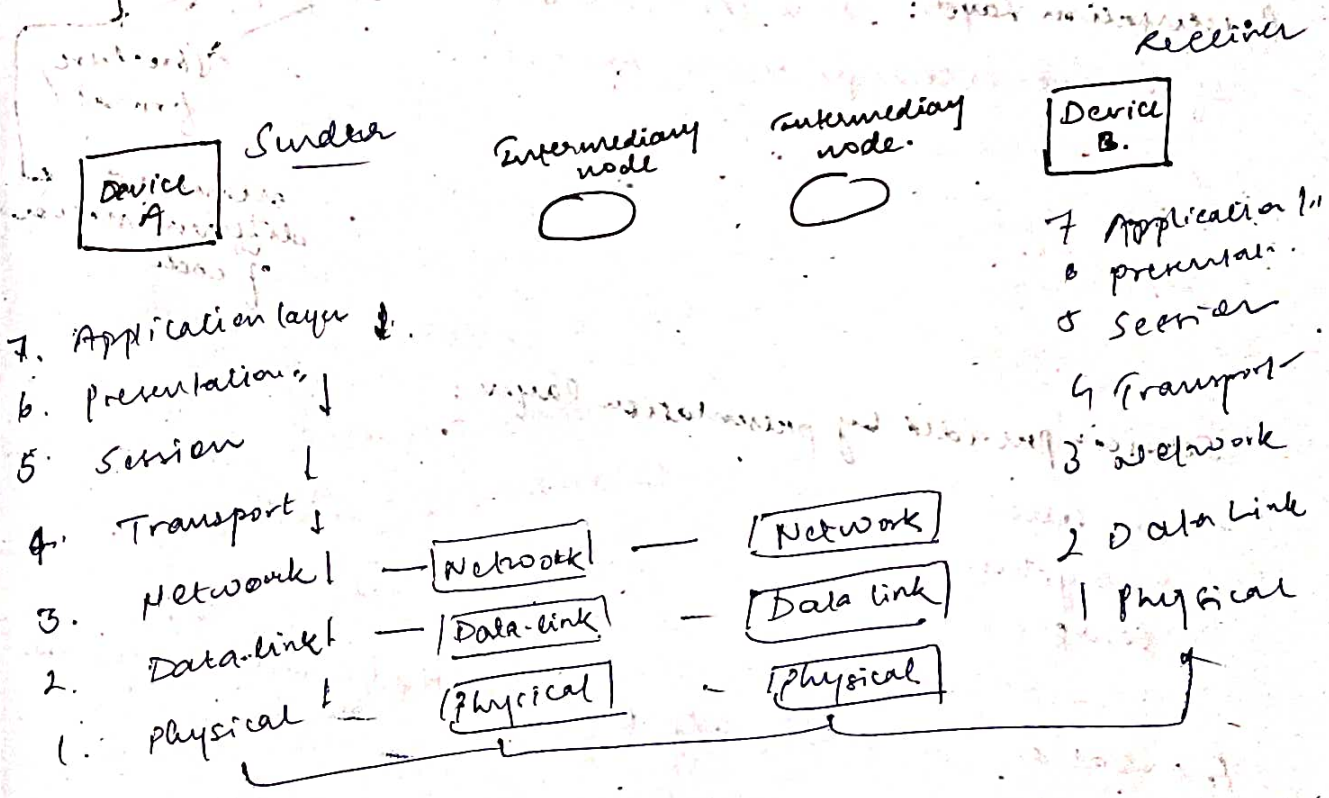
TCP/IP model:

- Transmission Control Protocol / Internet Protocol.
- The TCP/IP protocol suite was developed prior to the OSI model.
- Therefore the layers of the TCP/IP protocol suite do not exactly match to those in the OSI model.
- TCP/IP is a heirarchical prot. made up of interactive modules, each of which provides a specific functionality.

One layer will take care of IP addressing
other layer " " " MAC address.
other " " " Port addressing.

OSI reference model:

Application Layer
Presentation layer
Session layer
Transport layer
Network Layer
Data link layer
Physical layer.



* Intermediary nodes cannot access layers above network layer for safety

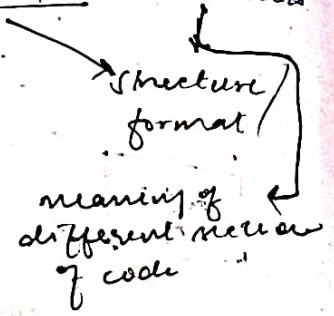
* The physical layer converts the data to be transmitted in form of 0s and 1s and on the basis of transmission media available, converts the code into appropriate signals.

Application Layer : It enables the user to access the network resources.

Services provided By application layer :

- File Transfer and Access management (FTAM)
- Mail services.
- Directory services.

Presentation Layer: It is concerned with the syntax and semantics of the info. exchanged b/w the systems.



Services provided by presentation layer :

- Translation
- Encryption
- compression.

Translation: converting into a format that is both acceptable by sender and receiver.

Encryption:- protection from disclosure (by converting into an unreadable format). Decryption happens on receive side.

Compression: Reduce the number of bits of data.

Session layer: It establishes, maintains, and synchronizes the interaction among communicating devices.

Services provided by session layer:- * Dialog control
* Synchronization

Dialog control:- ~~way of communication eg, simplex half~~ allows two ~~the~~ process to communicate either in half duplex mode or full duplex mode.

Synchronization:- Addition of checkpoints while sending large data. Crash failure eg:- sending book 100 pages. adding checkpoints at 100 pages allows the sender to receive acknowledgement that 100 pages have been received.

Transport layer: (handles port addressing) It is responsible for process to process delivery of the entire message

Services provided:- 1) Port addressing
2) Segmentation and reassembly
3) Connection control
4) End-to-end flow control
5) Error control

→ Port addressing helps the ~~process to know correct~~ operating system to handover the data to right process.

* Segmentation and reassembly: breaking down the message into smaller portions and give them sequence numbers. and upon reception, reassembling the portions to get the complete message.

* connection control:- → connection oriented
  → connectionless

* End to end flow control: accurate rate of data transfer

* Error control:

Network layer: (IP addressing)
It is responsible for delivery of data from the original source to the destn network.

Services provided:-

* Logical addressing
* Routing. — uses IP address

Data link layer: (Hardware MAC addressing)
Responsible for moving data (frames) from one node to other node.

Services provided by data-link layer :-

* Framing
* Physical addressing
* Flow control
* Error control
* Access control.

[Processes are identified by port numbers]

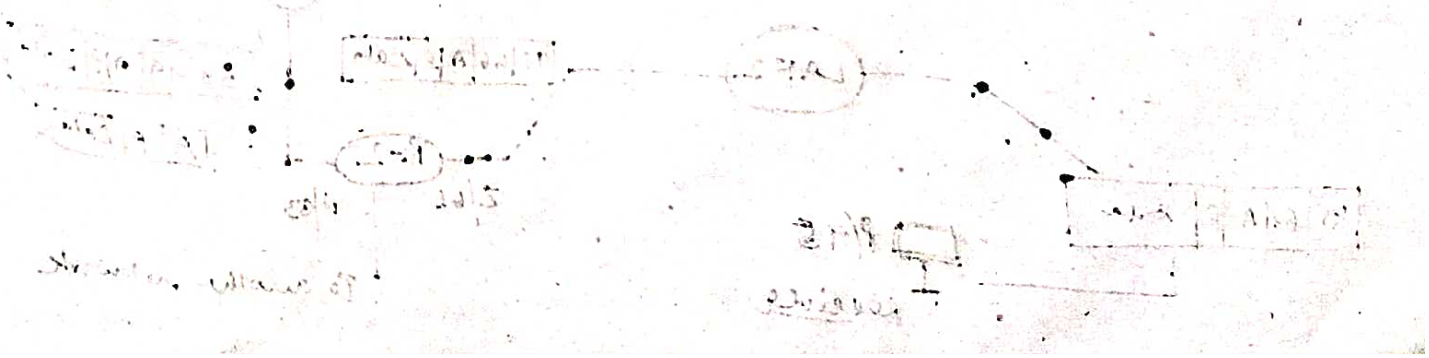
* Access control: If two or more systems share a common link, then it is the work of data link layer that which the system has the control over that link at that particular instant.

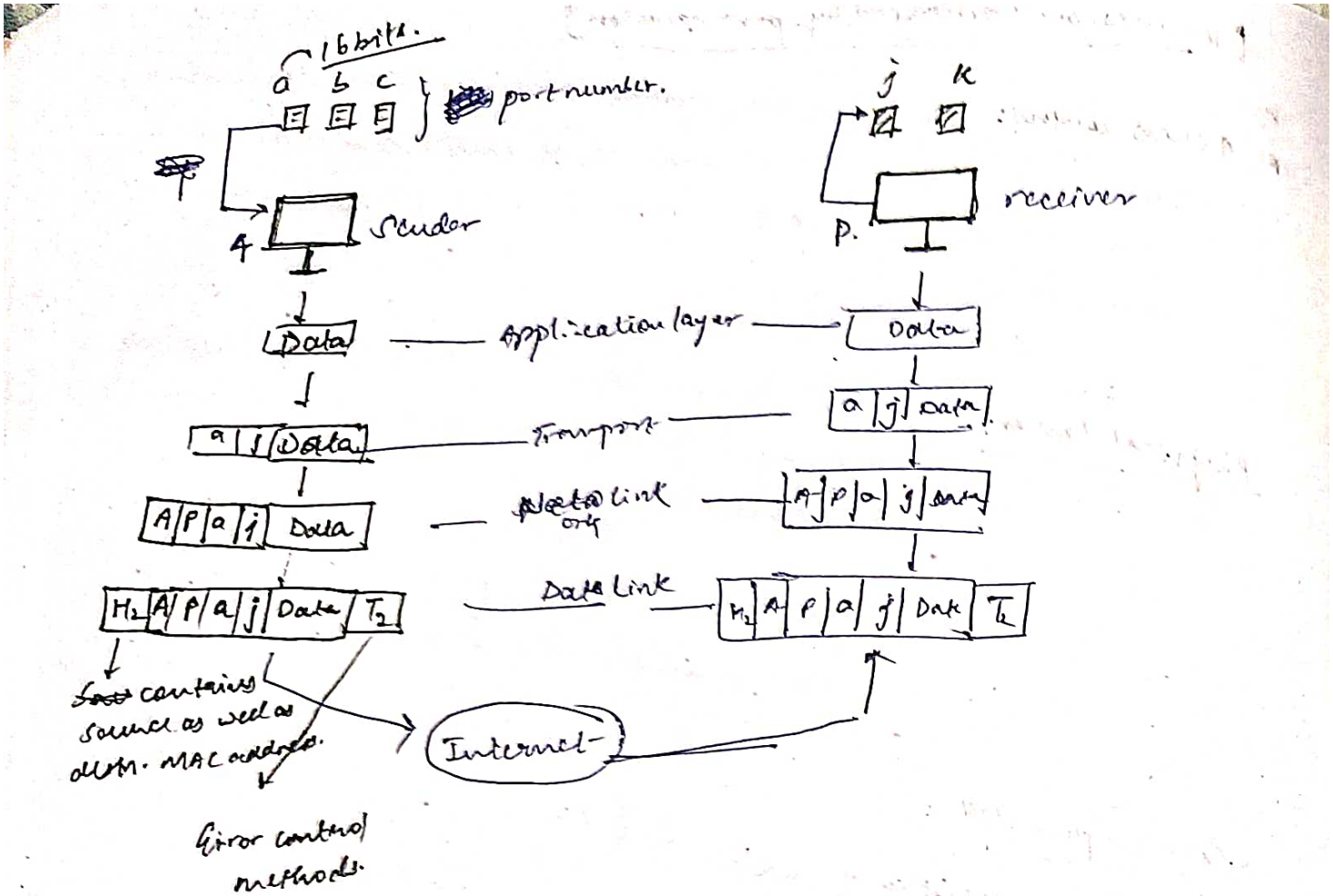
Physical layer: - responsible for transmitting bits over a medium.
- Also provides electrical and mechanical specifications.
- Sends the data in a format depending upon type of medium (W or W/L)

Services provided :-

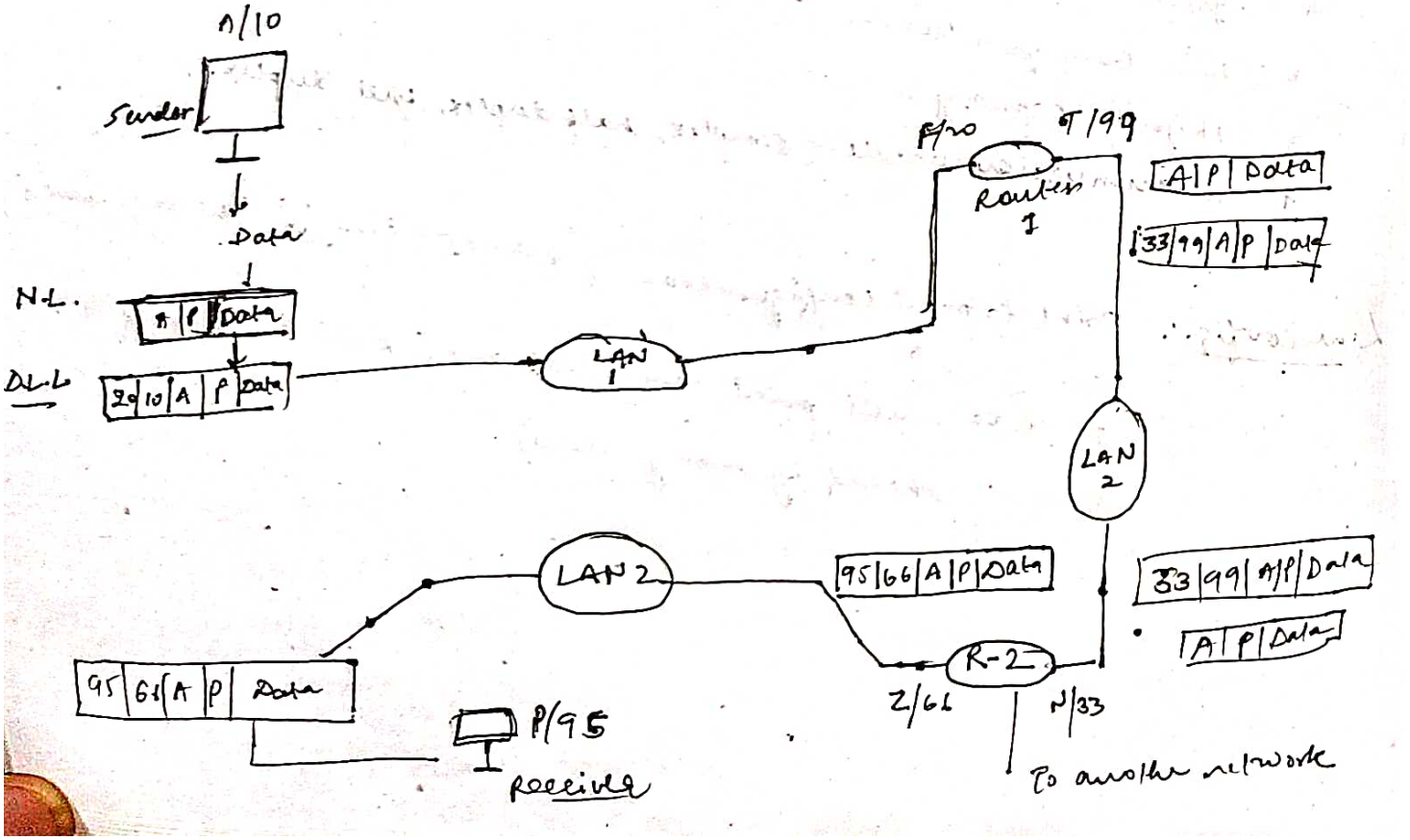
* Physical characteristics of media. — (W/ WL)
* Representation of bits.
* Data rate
* Synchronization of bits.
* Line configuration.
* Physical topology.
* Transmission mode - (simplex, half duplex, full duplex)

Line config.: point to point configuration (dedicated line for the two nodes)
or
point to multi-point configuration. (common channel is shared by many nodes).





Working of IP and MAC addressing



Error detection in computer networks :-

A cond" where the received info does not match with the sender's info. During transmission, digital signals suffer from noise that can introduce errors in binary bits. basically from sender to receiver (0 may change to 1 or 1 may change to 0).

Error detection codes (implemented either at data link layer or Transport layer of OSI model) are additional data added to a given digital message to help us detect if any error has occured during transmission of message.

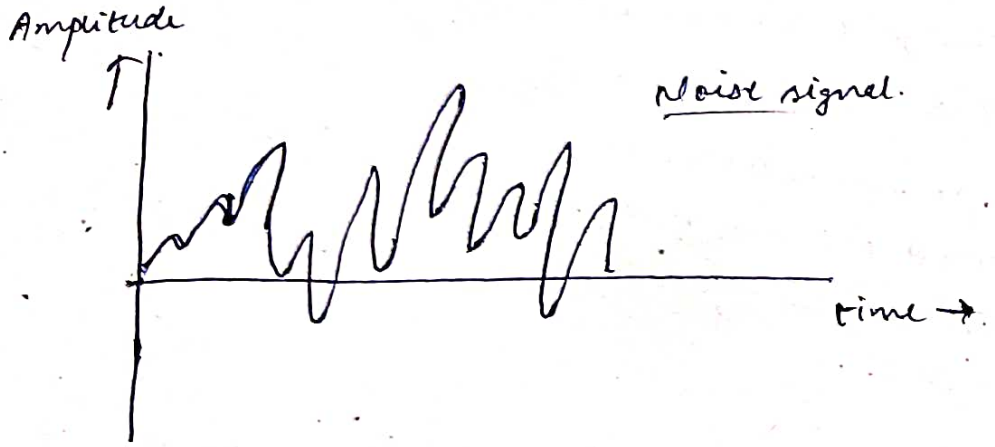
eg:- Simple parity check
Two dimensional parity check
Checksum
CRC.

Attenuation: It is the loss of signal strength in networking cables or connections. This typically is measured in decibels (dB) on voltage and can occur due to a variety of factors. It may cause signals to become distorted or indescernible. An example of this is wifi signal and strength getting noticably weaker the further that your device is from the router. To solve this, network administrators may need to adjust the cable or insert amplifiers or repeators in order to boost the signal strength.

Tutorials for

Noise: Noise is an unwanted signal that interferes with the original message signal and corrupts the parameters of the message signal. This alteration in the communication process, leads to the message getting altered. It may most likely enter the channel or at receiver end.

Noise is signal that has no pattern and no constant frequency or amplitude. It is quite random and unpredictable.



Examples of noise are :-

1. Hiss sound in radio receivers.
2. Buzz sound among b/w telephone comm.
3. Flicker in T.V. receivers.

effect of noise:

1. Noise limits the operating range of systems.
2. Noise affects the sensitivity of receivers.

Source: 1. **External source:** Atmospheric noise (due to irregularities in atmosphere.)

2. extra terrestrial noise, such as solar noise, cosmic noise.
3. Industrial noise.

Internal source:- This noise is produced by the receiver components while functioning.

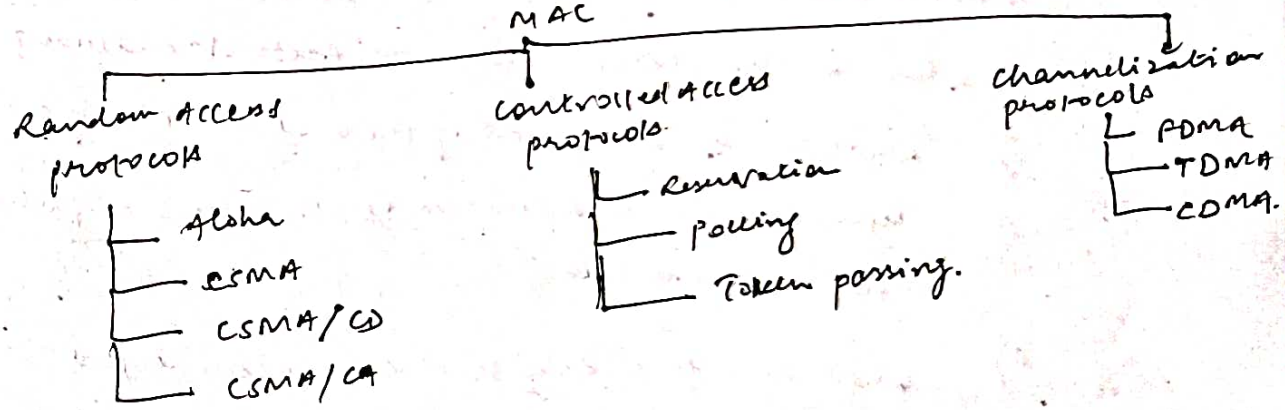
Eg:- Thermal agitation noise (Johnson noise or Electrical noise)

Shot noise

Transit-time noise (delay transmission)

(2)

Multiple Access protocols:



Aloha:- MAC: resolving problems related to multiple access points.
Eg: with a single medium.

- If there is a dedicated link b/w the sender and receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously.

Hence MAC protocols are required to decrease collision and avoid crosstalk.

Random access protocols

- In this, all stations have same priority. That is no station has more priority than another station. Any station can send data depending on medium's state (idle or busy).
- In random access method, each station has the right to the medium without being controlled by another station.
- If more than one st. tries to send, there's an access conflict (collision) and the frames will either be destroyed or modified.

To avoid access conflict, each station follows a procedure:-

1) When can the station access the medium?
2) What can the station do if the medium is busy?
3) How can the st. determine if the success or failure of the transmission?
4) What can the st. do if there is an access conflict?

Controlled access protocol:

* In controlled access, the st. consult one another to find which st. has right to send.

Screenshots:

Aloha:- Aloha is a random access protocol.

(Any station can send data at anytime)

- It was actually designed for WLAN. but it is also applicable for shared medium.
- In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.

collison - frames are either lost / corrupted.

Type of Aloha:

1) Pure Aloha
2) Slotted Aloha.

- Pure Aloha allows st. to transmit whenever they have data to be sent.
- when a station sends data, it waits for an acknowledgement.
- If the acknowledgement is not received within allotted time. then the station waits for a random amount of time called back-off time (TL) and resends the data.
- Since different stations wait for different amount of time, the prob of further collison decreases.
- The throughput of pure aloha is maximized when frames are of uniform length.

- whenever two frames try to occupy the channel at the same time there will be a collison and both will be garbled.
- If the 1st bit of new frame overlaps with just the last bit of previously transmitted frame, both the frames will be totally destroyed and both will have to retransmitted later.

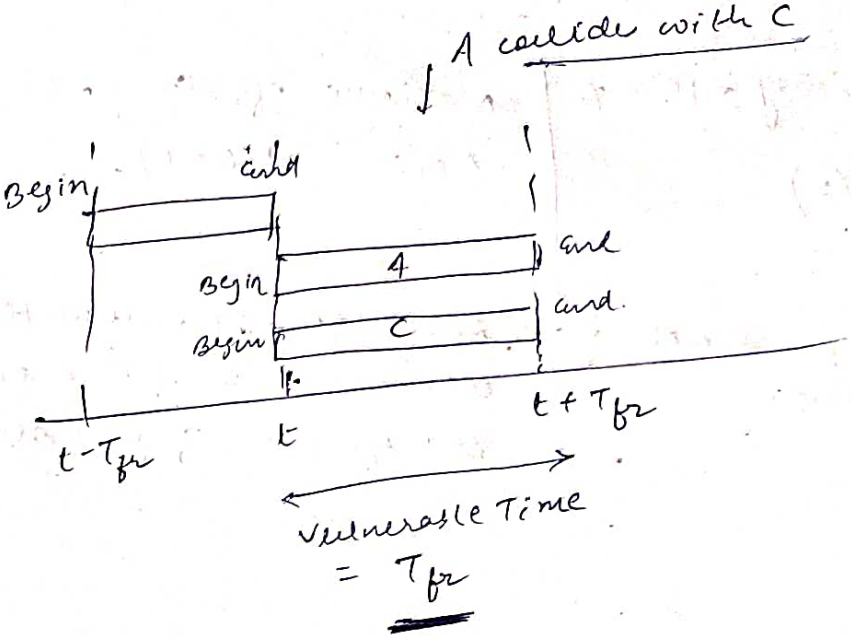
Vulnerable Time = $2 * T_{fr}$

- Throughput = $G \times e^{-2G}$; where G is the no. of stations wish to transmit in the same time

- max. throughput = 0.184 for ~~G = 0.5 (1/2)~~, G = 0.5.

Slotted Aloha

- Developed to improve efficiency of pure aloha as the chances for collison in pure Aloha is high
- The time of the shared channel is divided into discrete time intervals called slots.
- Sending a a data is allowed only at the beginning of these slots.
- If a station misses out the allowed time, it must wait for next slot. This reduces the prob. of collison.



Slotted Aloha.

Vulnerable time = Frame Transmission Time.

~~Throu~~ Throughput = $G \times e^{-G}$; where G = the number of Stations wish to transmit in ~~the~~ the same time.

Max. throughput = 0.368 for G = 1.

Pure Aloha	Slotted Aloha
• A station can transmit data anytime.	• Any station can transmit the data at the beginning of any time slot.
• The time is continuously and not globally synchronized.	• The time is discrete and globally synchronized.
• ~~Vulne~~ Vulnerable time in which collision may occur = $2 \times T_{fr}$	• Vulnerable time in which collision may occur = T_{fr}.
• Prob. of successful transmission of data packet = $G \times e^{-2G}$	• Prob. of successful data trans. = $G \times e^{-G}$

- Max efficiency = 18.4% (occurs at G = 1/2)
- Main advantage: Simplicity in implementation

- Maximum efficiency = 36.8% (occurs at G = 1).
- Advantage: It reduces the no of collision to half and doubles the efficiency of pure Aloha.

CSMA:

- Carrier sense multiple access
  - ↓
  - Channel/medium
- To minimize the chance of collision and therefore increase performance, the CSMA method was developed.
- Principle of CSMA: "Sense before transmit" or "listen before talk".
- Carrier busy = Transmission is taking place.
- Carrier idle = No transmission currently taking place.
- The possibility of collision still exists because of propagation delay. A station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received.

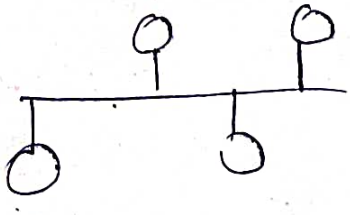
Types of CSMA:

1. 1- persistent CSMA
2. p- persistent CSMA
3. Non-persistant CSMA
4. 0- persistent CSMA

CSMA/CD (CSMA with collison Detection)
CSMA/CA (CSMA with collison Avoidance)

1. 1-persistant CSMA:

- Before sending the data, the station first senses the channel to see if anyone else is transmitting the data at that moments.
- If the channel is idle, the station transmit a frame.
- If busy then it senses the transmission medium continuously until it becomes idle.
- Since the station transmits the frame with the probability of 1 when the carrier or channel is idle, this scheme of CSMA is called as 1-persistant CSMA.
- The longer the propagation delay, the worse the performance of the protocol.



2. Non-persistant CSMA

- It also senses the channel before transmitting
- However, if the channel is already in use, the station does not sense it ~~for~~ continuously. Thus missing out the chance of seizing the opportunity to transmit data on the end of previous transmission.
- It waits for random period of time and then repeats the algo. The algo leads to better channel utilization but longer delays than 1 persistant CSMA.

3. p-persistant CSMA: