

Data Communication & Networking

M	T	W	T	F	S	S
Page No.:						
Date:						YOUVA

- * Data communication refers to the transmission of digital data b/w two or more computers or a computer network or data network.
- The physical connection b/w networked computing devices is established using either cable media or wireless media.

* Why to Learn Data Communication & Computer Network?

⇒ Network Basic Understanding

- A system of interconnected computers and computerized devices such as printers is called computer network.
- This interconnection among computers allows information sharing among them.
- Computers may connect to each other by either wired or wireless media.

⇒ Network Engineering

- This is a complicated task, which involves software, firmware, chip level engineering, hardware and electric pulses.
- To ease network engineering, the whole networking concept is divided into multiple layers.
- Each layer is involved in some particular task and is independent of all other layers.
- But as a whole, almost all networking tasks depend on all of these layers.
- Layers share data b/w them and they depend on each other only to take input and send output.

	M	T	W	T	F	S	S
Page No.:							
Date:							YOUVA

* Internet

- A network of networks is called internet.
- It is the largest network in existence on this planet.
- The internet hugely connects all WANs and it can have connection to LANs and Home networks.
- Internet uses TCP/IP protocol suite and uses IP as its addressing protocol.
- Internet enables its users to share and access huge amount of information worldwide.
- It uses WWW, FTP, email services, audio and video streaming etc.

* Applications of DCN

- Resource sharing such as printers and storage devices.
- Exchange of info. by means of e-mails.
- Information sharing by using Web or Internet.
- Interactions with other users using dynamic web pages.
- Ip phones.
- Video Conferences.
- Parallel computing.
- Instant messaging.

* What is computer Network?

- A computer network is a set of devices connected through links. A node can be computer, printer or any other device capable of sending or receiving the data.
- The links connecting the nodes are known as communication channels.

- DCN uses distributed processing in which task is divided among several computers.
- Instead, a single computer handles an entire task, each separate computer handles a subset of the task.

M	T	W	T	F	S	S
Page No:	Computer	YOGA	Date:			

* Advantages of Distributed processing.

- (1) Security - It provides limited interaction that a user can have with the entire system.
For eg:- a bank allows the users to access their own accounts through an ATM without allowing them to access the bank's entire database.
- (2) Faster problem solving - Multiple computers can solve the problem faster than a single machine working alone. A team of multiple computers running the same program at the same time can provide the security through redundancy.
- (3) Security through redundancy - Multiple computers running the same program and if any computer has a failure, the other computers can override it.

* Basic Networking Commands.

- (1) ARP has been minimized to help you know the Address Resolution Protocol.
- This is a protocol that is used to resolve IP addresses to their MAC address.
- If you have an IP add, but you don't know the MAC add, then you are using the ARP command to know the MAC add.
- To find something on the network, type the command ping.

Application AL

Transport TL

Network NL

IA | TB

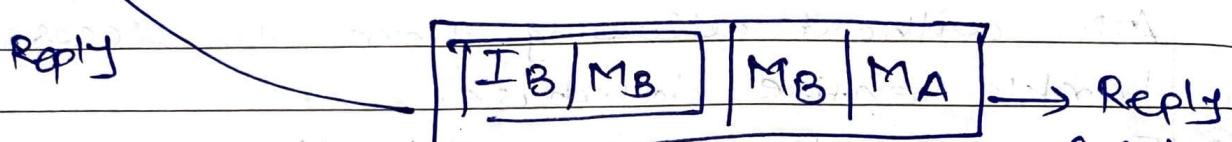
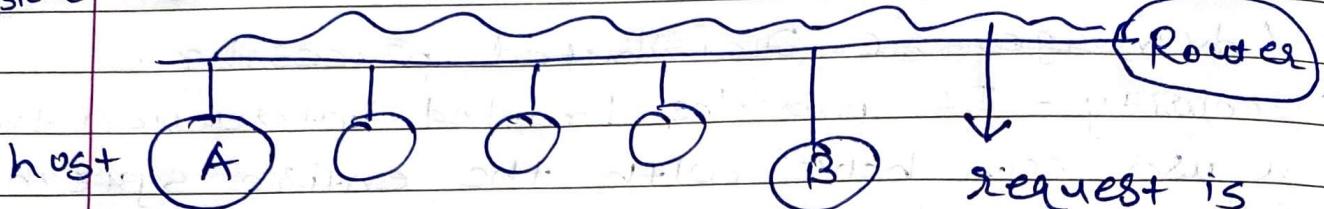
Data Link DLL

[IBT?]

MA | FF!FF!FF!FF!FF!FF

Request + Broadcast

Physical PL



→ Here, Host A knows the IP address of destination host, but A wants to know the MAC address of host B.

→ So, based on the destination IP add, A send the request, which includes, IP add of destination host, MAC address of source host and broadcast add.

→ After receiving the request, correct destination host will send reply to the host, which includes, IP address of destination host, MAC add. of destination host and MAC add of source host.

Note

ARP request → Broadcast

ARP reply → Unicast

→ Then we can use these MAC addresses for communicating by sending and receiving data and stuff in Data-Link layer.

- ② Ifconfig
- Ifconfig stands for interface
 - It is one of the most basic command used in network inspection.
 - Basic information displayed upon using ifconfig include:
 - (1) IP address
 - (2) MAC address
 - (3) MTU (Maximum Transmission Unit)

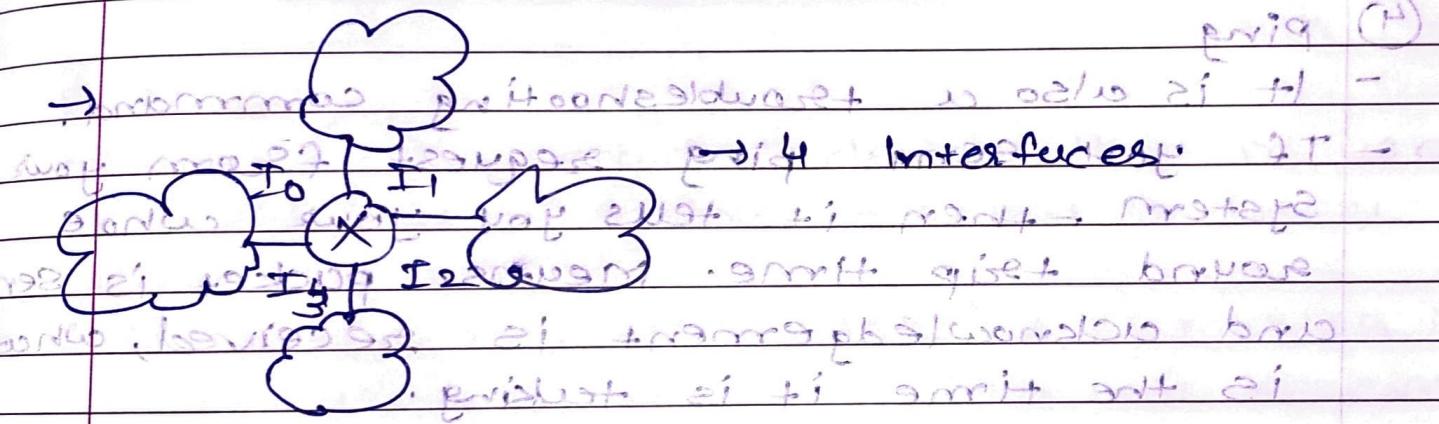
M	T	W	T	F	S	S
Page No.:	1	2	3	4	5	6

YOUVA
Date:

What is Interface?

A diagram showing a computer monitor and keyboard connected to a single point on a horizontal line labeled "Interface". This line extends to the right, with a cloud-like shape at the end labeled "when your Network adapter connects to a network card or PC is connecting to a network, that is called an interface".

When your Network adapter connects to a network card or PC is connecting to a network, that is called an interface.



- We want to know, what is the IP add of the PC, MAC add of PC, MTU, that time we use if config.
- MTU = how much bytes/data can be sent maximum in one go.

③ Trace Route.

- This one is one of the most useful commands in networking. It is used to troubleshoot the network.
- It detects the delays and determines the pathway to your target.

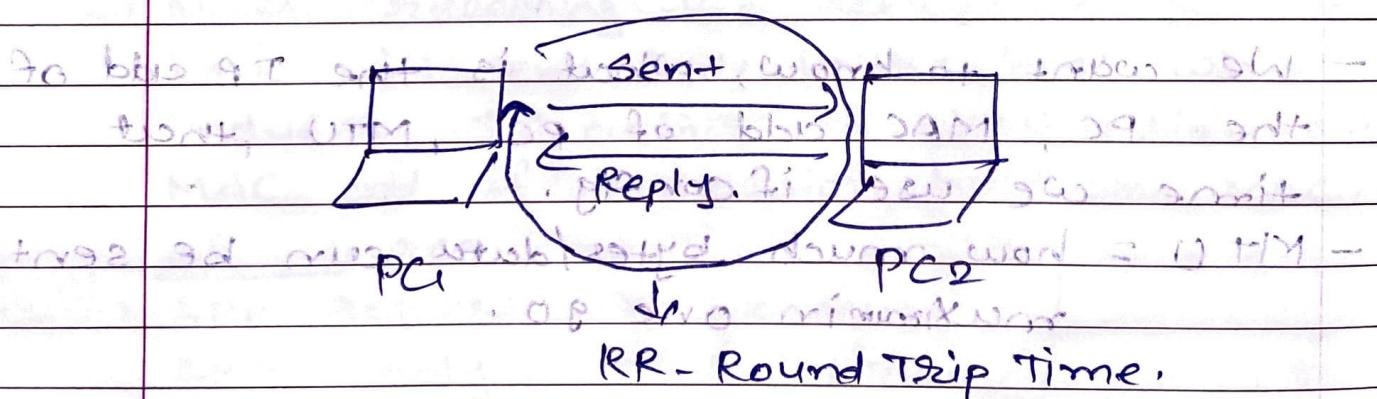
→ Source → Destination

→ ~~route~~ ~~path~~ ~~location~~ mi hau
 prior major b~~o~~ to ~~the~~ ~~route~~ ~~lines~~. the ~~the~~ ~~reason~~
 of latency, delay means the
 route → we are tracing the
 (line) ~~meanings~~ using either traceroute command.

- It provides the names and identification, identifies relay device on the path.
- It follows the route to the destination
- It determines where the network latency comes from and reports it.

(4) ping

- It is also a troubleshooting command.
- If you send ping request from your system - then it tells you your whole round trip time. Means, packet is sent and acknowledgement is received, what is the time it is taking.



- You can write ping with Google.com, if you write ping with any particular site, then that request goes to server and comes back and it uses ICMP.
- Internet Control Message protocol
- PING - Packet Internet Groups.

(5) netstat

Network statistics.

- All the important points related to network interface, that how many open connections are there, what is the routing table, all these information is given by netstat.

(6) NSlookup

- this is a use for DNS related queries, but it is the older version of DIGI.

* Various networking and Internetworking Devices.

(1) HUB

- HUB is a network device that is used to connect multiple computers in a network.
- All the information send to the HUB is automatically send to each port to every device:- eg: Watsgroup. - Broadcasting
- A HUB is less expensive, less intelligence & less complicated.
- this is not private, used for broadcasting.
- HUB generally used to connect computers in a LAN

5 transmission mode of HUB is half duplex.

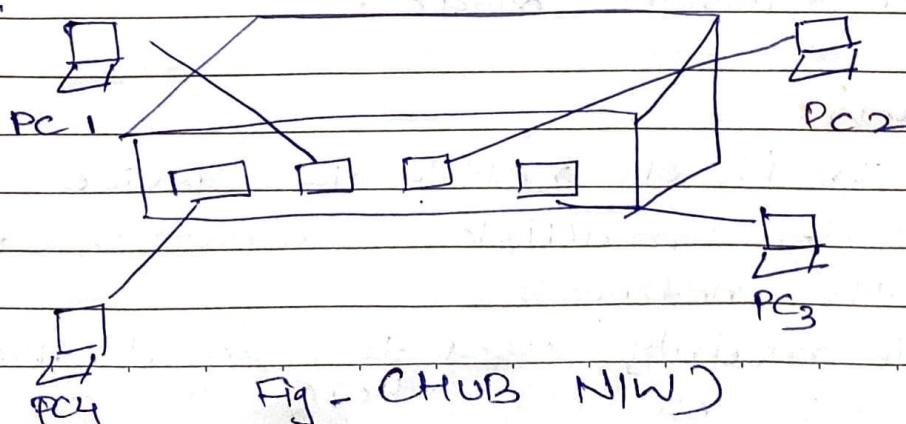


Fig - (HUB NW)

- Half Duplex + One way communication
- At a certain time either can only send or receive.

- In fig, there are 4 ports, each PC is connected to each port, if PC-2 wants to send the msg to PC1, if PC-2 is not able to send private message to PC1, msg goes to every PC and relevant PC keep that msg and others discard that msg.

→ Advantage :- HUB can broadcast the message.

- It is less expensive that anyone can use it.
- Easy installation
- Robust - one computer down → other can handle that task.

→ Disadvantage:- If the HUB is failed, the entire network will be failed.

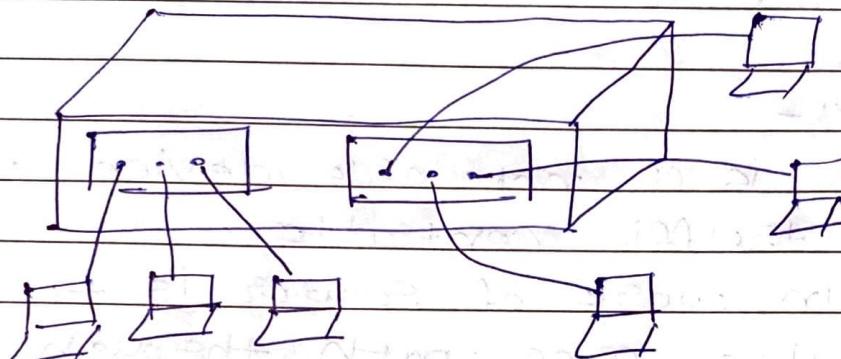
- We can't send private/personal data through hub.
- HUB doesn't provide any security.
- HUB can't support full duplex transmission mode.

(2) Switch:

- Switch is a network device that connects multiple computers together in the network.
- It is mainly used to send the private msg as well as there is no cascading of

Date:-

- Switch can easily identify that which device is connected with which port by using MAC address; thus why it delivered msg on particular destination machine.



switch.

- It has 2 plugs → Each plug with 3 pcs.
- Each pc has different MAC add, Using MAC add, it can send the packet to the particular PC.
- At the time of data transmission, switch will create one table, where source and destination MAC address will store.

Note:- Switch is more intelligent than HUB.

Advantages :- (1) It generally used to unicast the msg.

- (2) It provides more security than HUB.
- (3) Switch supports full duplex data transmission mode.
- (4) It is used to send the data packet based on MAC Address.

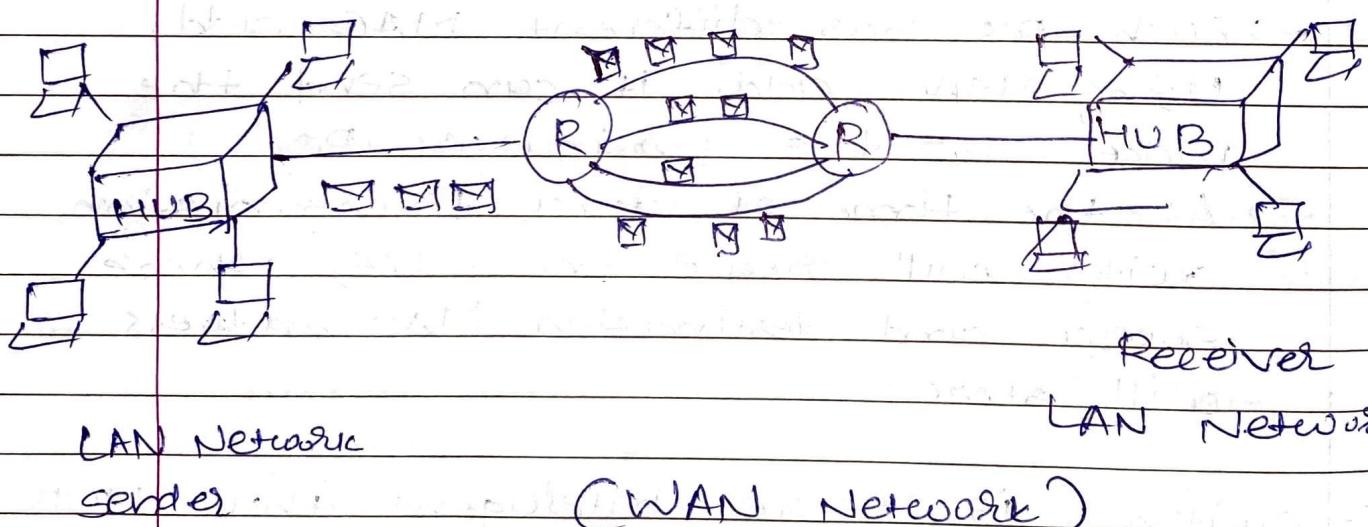
- ⑤ If a node fails, there will be no effect in the entire network.

Dis-advantage:- ① If switch is failed then entire network will be failed.

- ② It is more expensive.
③ Difficult to setup.

④ Router:-

- Router is a network device which works as a traffic controller.
- A main task of router is to choose a congestion free path through which the data will travel.
- Router receive data packet from the sender, analyze and forward those data packet, then send it to the receiver.



- Sender is sending 3 packets.
- Router checks the add on each packet.
- Router check the free path, then send packet accordingly.
- Receiver side router receive the packet, check the ip, then send it to the destination.

Note:- Router uses both LAN & WAN networks.

(eg: pizza delivery)

Advantages:- ① It provides connection b/w two dis-similar type of network.

- ② Transmission rate is very high.
- ③ It internally uses some algo to find out congestion free path.
- ④ It provides both wired or wireless facility.

Disadvantages:- ① Router is more expensive compare to other devices.

- ② Routers are complex to maintain.
- ③ Security issues.
- ④ It only works with TCP/IP protocol.

⑤ Repeater.

- Repeater is a Network device through which we can "boostup the weak signals".
- When the signal travels in the network, after traveling some distance, the intensity of the signal becomes low, In order to regenerate the weak signal, we should use repeater device.

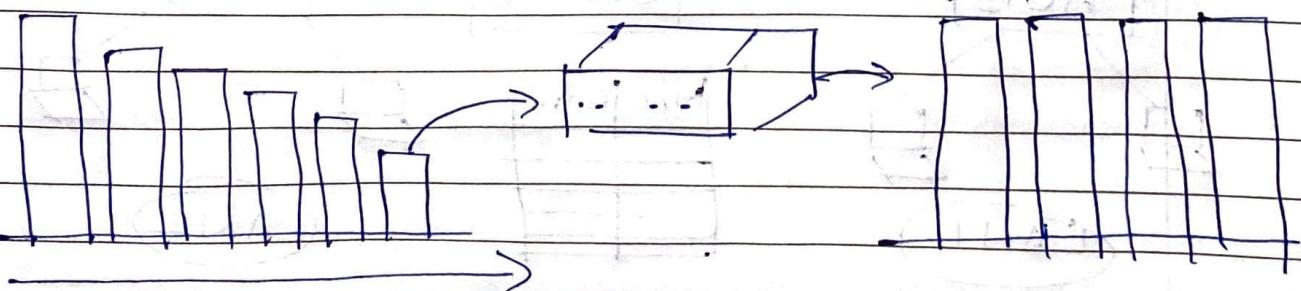


fig:- Repeater.

Note:- It is used in wired and wireless.

→ Real Time eg:- Cable TV. (Black Box) Repeater to maintain the quality.

Advantage:- It is used to regenerate the weak signal.

- (2) It is cheaper than other n/w device.
- (3) Repeater has the ability to extend the length of signal.
- (4) Increase / maintain the signal performance.

Disadvantage:- It required no. of repeater after some distance.

- (2) Repeaters also unable to connect dissimilar type of n/w.

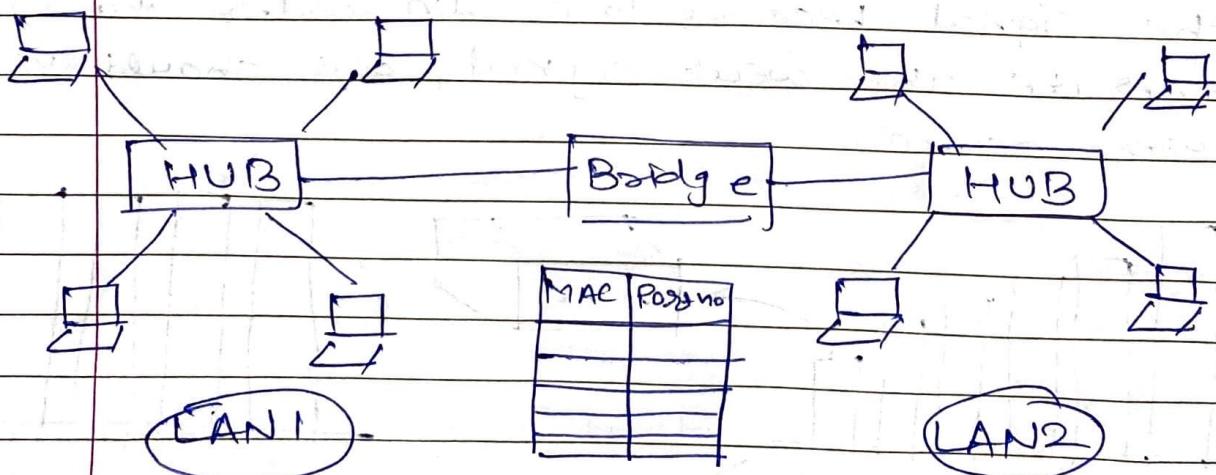
Digital \leftrightarrow Digital = ✓

Digital \leftrightarrow Analog = X

- (3) They can't reduce n/w traffic.

5) Bridge.

- Bridge is a network device that is used to separate LAN into no. of section.



- Bridge

Note! - It operates both physical as well as Data link layer of OSI model.

Advantages! - By using bridge device we can extends network.

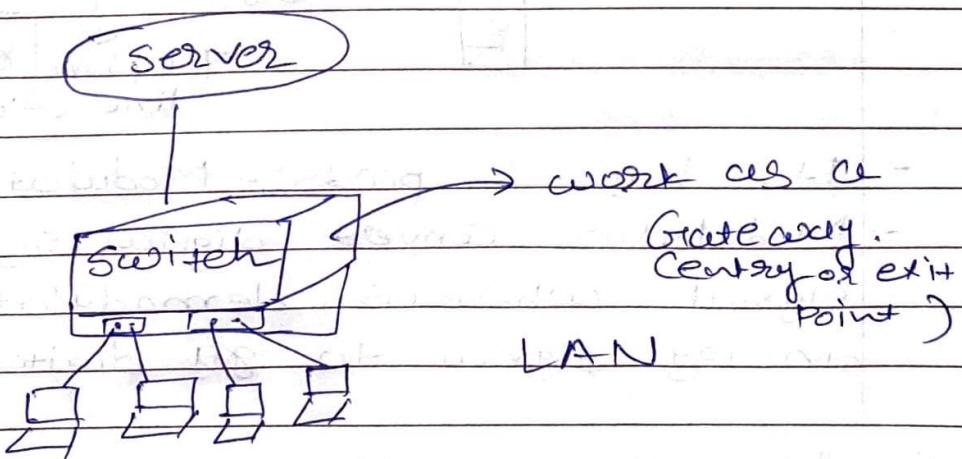
- (2) It broadcast the data to each node like HUB & Repeaters.
- (3) Collision can be reduced easily.
- (4) It is more intelligent.

Disadvantages! - It doesn't establish connection b/w 2 diff' network.

- (2) Once it broadcast the msg then it is incapable to stop the msg.
- (3) It is more expensive.
- (4) The transmission speed of data is slower than repeater.

(6) Gateway.

- Gateway is a h/w device that is used to connect two dissimilar type of network.
- It allows us to send and receive data through the internet even it is LAN network.



- Note! - It operates with all layers of OSI model.

Advantages:- (1) It connects two network which has different protocol.

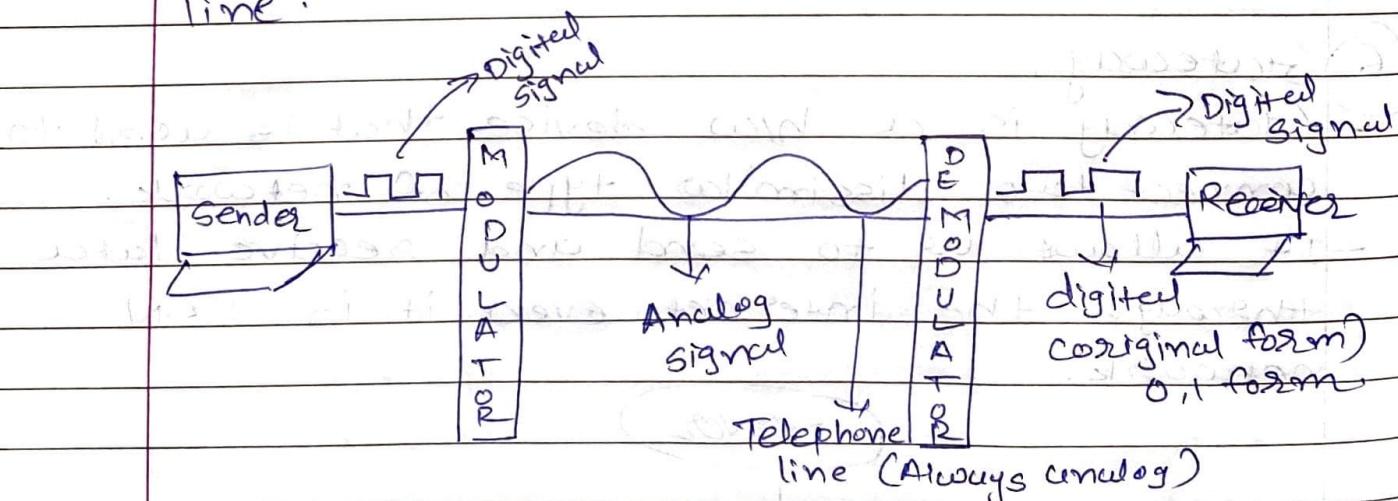
- (2) It operates with all 7 layers of OSI model.
- (3) We can not access the internet without a gateway.
- (4) It provides the security.

Disadvantages:- (1) It is more expensive.

- (2) Data transmission rate is slower.
- (3) Difficult to maintain as well as very complex.
- (4) It is less intelligent.

7) Modem

- Modem stands for modulator & demodulator. It is a network device that is placed below the computer system and telephone line.



- It has 2 parts:- Modulator & Demodulator.
- Modulator converts digital signal to analog signal whereas, demodulator converts the analog signal to digital signal.

Note:- It allows us to connect computer to connect with internet.

(8) NIC

- NIC stands for network interface card.
- It is h/w device without which we can not connect computer to the network/internet.

Types:- (1) Internal Network Card
 (2) External Network Card.

⇒ (1) Internal Network Card.

- In this cards, the motherboard has a slot for h/w card, where it can be inserted.
- It requires a network cable (RJ45) to provide h/w access.

⇒ (2) External Network Card.

- In desktop & laptop, that doesn't have an internal NIC, external NIC's are used.
- It has two types:- (1) Wireless
 (2) USB cable.

Connected through IP add or LAN.

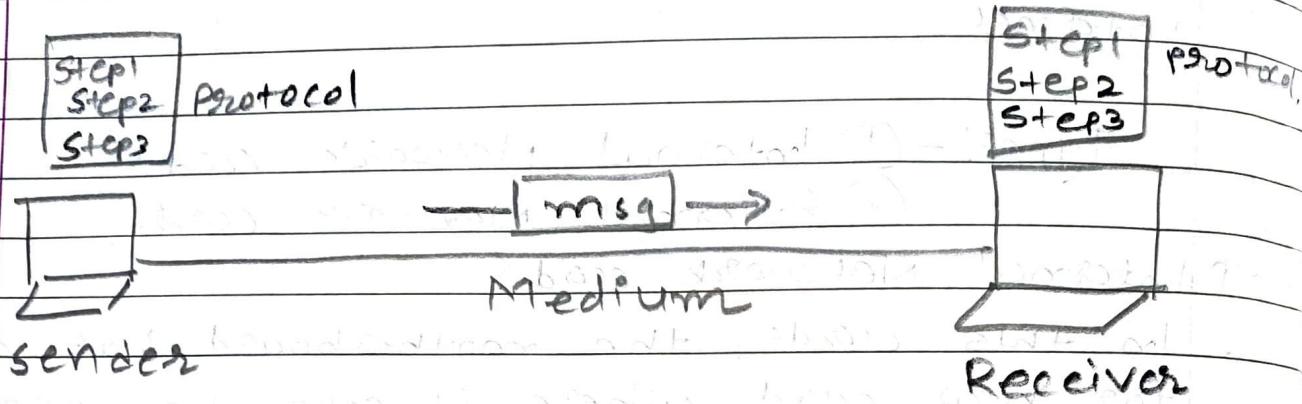
⇒ NIC add = 48 Bit.

* Data Communication.

- Data Communication is the process of sending or receiving digital data b/w two or more computer via transmission medium such as wire, cable.

* Components of data communication.

→ msg -



→ Msg - Data / Info (Text, number, pictures, sound, or video or any combination of these.)

- Sender - Computer, workstation, telephone handset, video camera or anything.

- Receiver - same devices as sender.

- Medium - Physical path (Twisted pair wire, coaxial cable, fiber-optic cable, laser, radio waves)

- Protocol - Set of rules (Agreement b/w the communicating devices.)

(eg:- without protocol 2 devices may be connected but not communicating)

(eg:- Just as a person speaking French cannot be understood by a person we speaks only Japanese.)

* Protocols.

- Protocol is a "set of rules" which are used in digital communication to connect network devices and exchanging information b/w them.
- Eg: - Internet - IPX - TCP/IP
- WiFi or LAN - IEEE 802.11



Sender

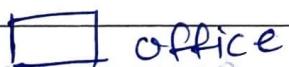
Receiver

"In communication if both want to communicate first, sender and receiver need some kind of protocol for communication.

- Without protocol data exchange can not be done.
- Without protocol we can not even access the internet.

Rules from the pedestrian

Eg:-



"If you walk towards left side road -
if you want to walk towards right side road, if you want to walk towards right side road, you need to take left side."

"So, in the case of hi only. That is the rule."

"So, if you go towards left side road -"

"Left Side Right → If signal is red, you



Home

can not cross the road. That is another rule."

* Types of Protocol.

- ① TCP - IP
- ② HTTP - Hyper Text Transfer Protocol.
- ③ SMTP - Simple Mail Transfer Protocol.
- ④ POP - Post Office Protocol.
- ⑤ IMAP - Internet Message Access Protocol.
- ⑥ UDP - User Datagram Protocol.
- ⑦ PPP - Point to Point Protocol.
- ⑧ FTP - File Transfer Protocol.

* Elements of Protocol.

- ① Syntax = "What is communicated"
 - Structure or format of the data.
 - Indicates how to read the bits.

eg:

Sender Add.	Dest. Add.	-----
8 bits	8 bits	original Data

format of one protocol.

- ② Semantics = "How it is communicated"
 - Interprets the meaning of the bits
 - knows which fields define what action.
 - Router will be define by semantic.

- ③ Timing = "When it is communicated".
 - When data should be sent and what speed at which data should be sent
 - Speed at which it is being received.

* Standards

- Standards provide guidelines to manufacturers, vendors, government agencies and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications.

- You been not a manufacturer, you can not produce whatever you want. There should be certain guidelines in you need to follow.

⇒ Data communication standards falls into 2 categories:

(1) De facto = meaning "by fact" or "by convention".

- It is not approved by any law, It is just the fact

(2) De jure = meaning "by law" or "by regulation"

- It has been approved by law.

→ De facto = Standards that have not been approved by organized body but have been adopted as standards through widespread use are de facto standards.

→ De jure = Those standards by law or by regulation. These are the standards recognized officially by an organization.

* Standard organizations

- Standards are developed through the cooperation of standards creation committees, forums and government regulatory agencies.

- * Standards creation committees
 - ISO = International organization for standardization.
 - ITU-T = International Telecommunication standards sector (ITU-T)
 - ANSI - American National Standard Institute.
 - IEEE - Institute of Electrical and Electronics Engineers of America.
 - EIA - Electronic Industries Association.

Want "Ed" equivalent = want "Ed" (1)
Want "Circumlocution Ed"

Want "Ed" because have to do it
with only one of it

Want "Ed" because is part of (2)
Want "Ed"

Want "Ed" because want part of it

Want "Ed" because alternative word. so

Want "Ed" because not to do it
Want "Ed" because (3) alternative

Want "Ed" because not to do it
Want "Ed" because (4) alternative

Want "Ed" because (5) alternative
Want "Ed" because (6) alternative

Want "Ed" because (7) alternative
Want "Ed" because (8) alternative

Want "Ed" because (9) alternative
Want "Ed" because (10) alternative

Want "Ed" because (11) alternative
Want "Ed" because (12) alternative

Want "Ed" because (13) alternative
Want "Ed" because (14) alternative

* Networks

⇒ Distributed processing

- Most networks use distributed processing, which our task is divided among multiple computers.
- Instead of one single large machine, separate tasks (amongst the computers.)
"part (Separated) computer handle a subset".

* Network criteria.

Networks must be able to meet a certain number of criteria. The most important of these are performance, reliability and security.

⇒ Performance → It can be measured in many ways, including transit time and response time.

- Transit Time = It is the amount of time required for a msg to travel from one device to another.

- Response Time = It is the elapsed time b/w an inquiry and a response.
- Performance of a network depends on number of users, the type of transmission medium, the ^{capacity} ~~size~~ of connected w/c and efficiency of s/w.

⇒ Reliability → In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

⇒ Security → Network security issues include protecting data from unauthorized access, protecting data from damage and development.

* Networks

⇒ Distributed processing

- Most networks use distributed processing, in which our task is divided among multiple computers.
- Instead of one single large machine, separate tasks among the computers.
("Separate" computer handle a subset).

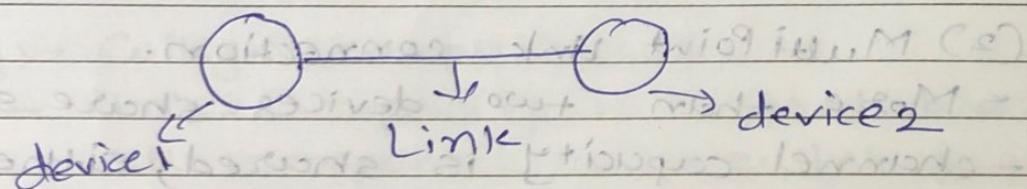
* Network criteria.

- Networks must be able to meet a certain number of criteria. The most important of these are performance, Reliability and Security.

⇒ Performance → It can be measured in many ways, including transit time and response time.

- Transit Time = It is the amount of time required for a msg to travel from one device to another.

- Response Time = It is the elapsed time b/w an inquiry and a response.
 - Performance of a network depends on number of users, the type of transmission medium, the ^{capability} of connected WC and efficiency of SW.
- ⇒ Reliability → In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.
- ⇒ Security → Network security issues include protecting data from unauthorized access, protecting data from damage and development.
- * Types of connection.
- Network is a two or more devices connected through links.
 - Link is communication pathway transferring data from 1 device to another.
 - Link can be imagined as a line drawn between 2 points.



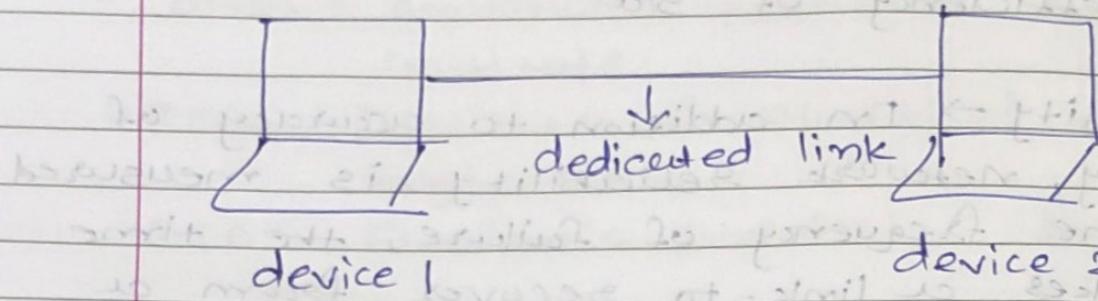
- During communication, 2 devices must be connected to same link at same time.

→ There are two types of link connections.

(1) Point-to-Point.

- Dedicated link b/w 2 devices.

- Entire link capacity is reserved for transmission b/w 2 devices.



→ This link is reserved for these 2 devices only.

→ No other device can use this link even if this link is free. No other device can join to this link.

- Mostly we actual length of wire to connect 2 ends.

(full length of wire is used to connect two devices.)

- LAN wire is used to connect the devices.

e.g)- Changing television channels by infrared remote control.

(2) Multi Point link connection.

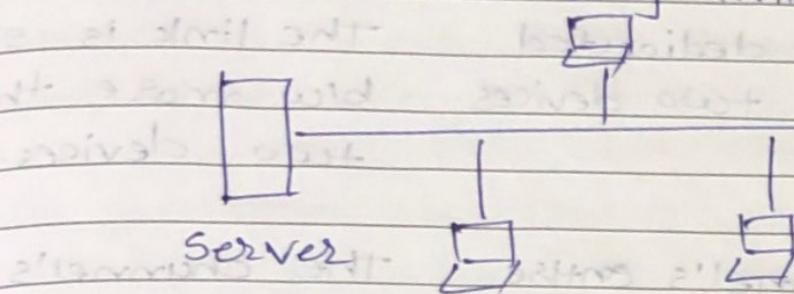
- More than two devices share single link.

- channel capacity is shared, either spatially or temporally.

→ Spatially shared connection = several devices using link simultaneously.

- All the devices are using same link at a same time.

→ Timeshared connection = If users take turns while using link.



- 3 computers and a server are connected to single link.

- total devices = 4

- In timeshared connection, once the first device is done with the data sharing then second device will use the same link, after second device shares the data, third device will use the link, they use the link turn by turn, not simultaneously.

- So when they use the link turn by turn, it is called as time shared connection.

→ - And when all the three systems are using the link at the same time, that time we call it a specially shared connection.

→ eg:- College computer labs.

- link's capacity is shared b/w the all computa. So one link is used by all the computers. So this is called as multi-point link.

connection.

Comparison chart

Point To Point

Multi Point

Link

- There is dedicated link b/w two devices.

The link is shared b/w more than two devices.

Channel - The channel's entire

capacity capacity is reserved for the two connected devices.

The channel's

capacity is shared temporarily among the devices connected to the link.

Transmitter - There is a single transmitter and receiver transmitter and receiver, single receiver. multiple receivers.

Example - Television-Remote Computer Labs.

Key Differences

* When there is a single dedicated link only b/w two devices, it is a point-to-point connection whereas, if a single link is shared by more than two devices then it is said to be a multipoint connection.

② In multipoint connections, the channel capacity is shared temporarily by the devices in connection. On the other hand, in a point-to-point connection, the entire channel capacity is reserved only for the

two devices in the connection.

3) In point-to-point connection, there can only be a single transmitter and a single receiver. On the other hand, in multipoint connection, there is a single transmitter, and there can be multiple receivers.

→ If you want to send your data to the multiple receivers, using point to point, connection will create more overhead, instead multipoint connection will be more helpful.

* Physical Topology.

- Types of transmission medium.

- The host can communicate one of three different ways.

- 1) Unicast - one-to-one

- 2) Broadcast - one-to-many all

- 3) Multicast - one-to-many

⇒ Unicast Transmission

- One-to-One

- In unicast, unicast is used when data is transmitted from one point to another point.

- It is a one-to-one communication, that is one sender and one receiver.

- When one device transmits the data to another device then it is called unicast transmission.

- Generally, we use one-to-one communication on our daily basis like - sending a message,

browsing a website, downloading a file

→ eg:-1) A device having an IP address 20.1.3.0 in a network wants to transmit the data to the device with IP address 30.10.5.0 in another network, then this transmission is called unicast transmission.

→ eg:-2) There are 4 computers connected to the switch device, so if PC1 wants to communicate with PC2, then they can directly communicate with each other so this is unicast communication because it is one-to-one communication.

→ eg:-3) Browsing a website is also unicast communication, where the web server acts as a sender and our computer acts as a receiver.

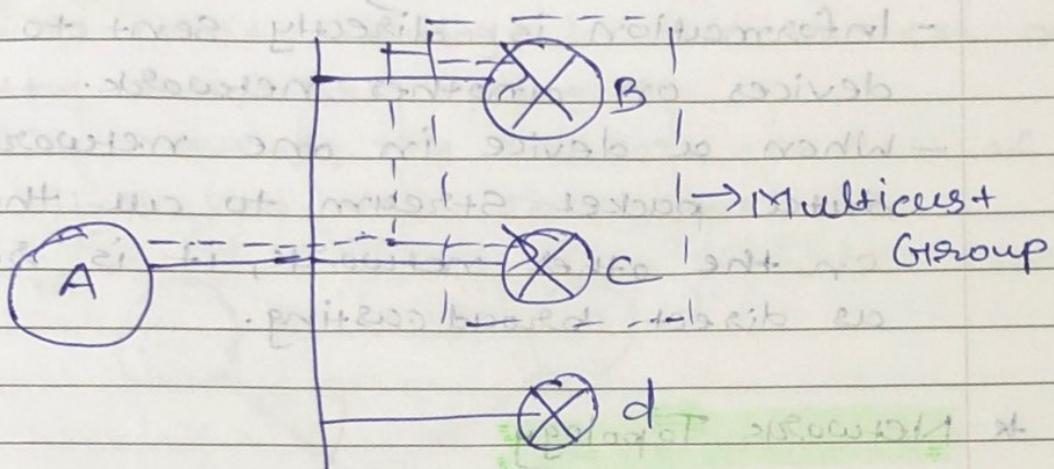
→ eg:-4) Downloading a file from an FTP server is another example of unicast transmission, where the FTP server acts as a sender and our computer acts as a receiver.

⇒ Multicast Transmission

- Multicast is a term, that is used when data is transmitted to multiple devices.
- This type of multicast transmission is used, when data is sent to a group.
- This type of transmission goes beyond the boundaries of unicast one-to-one and

broadcast (one-to-all).

- It can be one-to-many or many-to-many transmission means, data send efficiently from one source (or many sources) to many destinations simultaneously, generally within a local network.
- In unicast, multicast, when a device sends one copy of data, then it is delivered to many devices (not delivered to all devices like in broadcast).



⇒ Broadcast Transmission.

- Broadcast is a term, that is used when data is transmitted to all the devices.
- It is one-to-all transmission means; there is one sender, but the information is delivered to all the connected receivers.
- In broadcast transmission, when a device sends one copy of data, then that data will be delivered to all the devices.
- This term "broadcast", mostly used in cable TV transmission. TV signals are sent from one source (one point) to all the possible destinations (all points).

⇒ We can classify broadcasting techniques into two types:-

(1) Limited Broadcasting

- Information sent to all the devices on the same network.
- When a device transfers data to all devices on the same network, it is referred to as limited broadcasting.

(2) Direct Broadcasting

- Information is directly sent to all the devices on another network.
- When a device in one network transfers data packet stream to all the devices on the other network, it is referred to as direct broadcasting.

* Network Topology

- A network topology describes how computer, printers and other devices (i.e. nodes) are connected to the network.

- Two main types of network topologies in computer network are (1) Physical Topology (2) Logical Topology

(1) Physical Topology

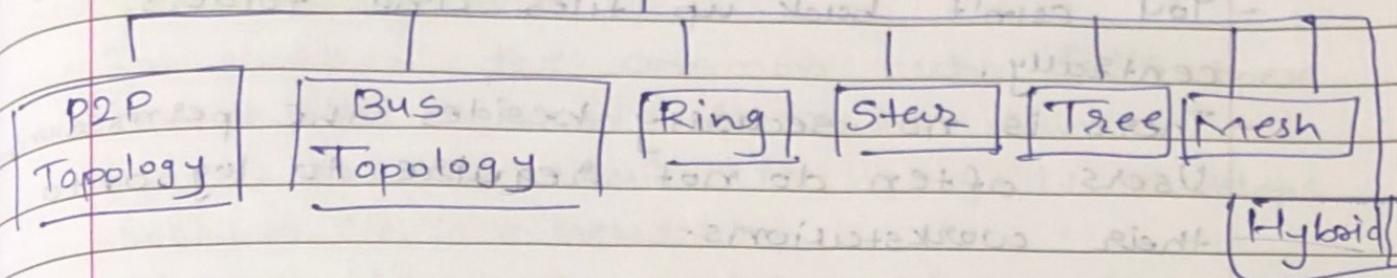
- This type of network is a physical layout of the computer cables and other network devices.

(2) Logical Topology

- Logical topology gives insights about network's physical design.

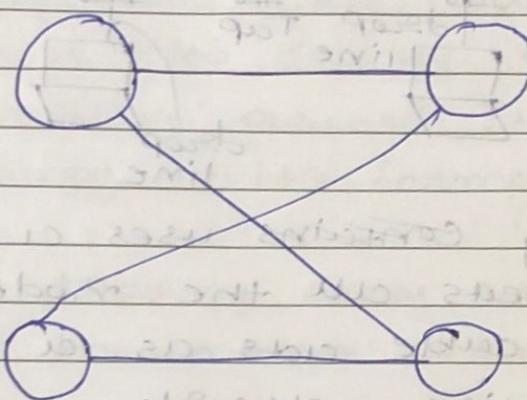
→ Different types of physical Topologies are -

Topology



① Point to Point (P2P)

- Point-to-point topology is the easiest of all the network topologies.
- In this method, the network consists of a direct link b/w two computers.

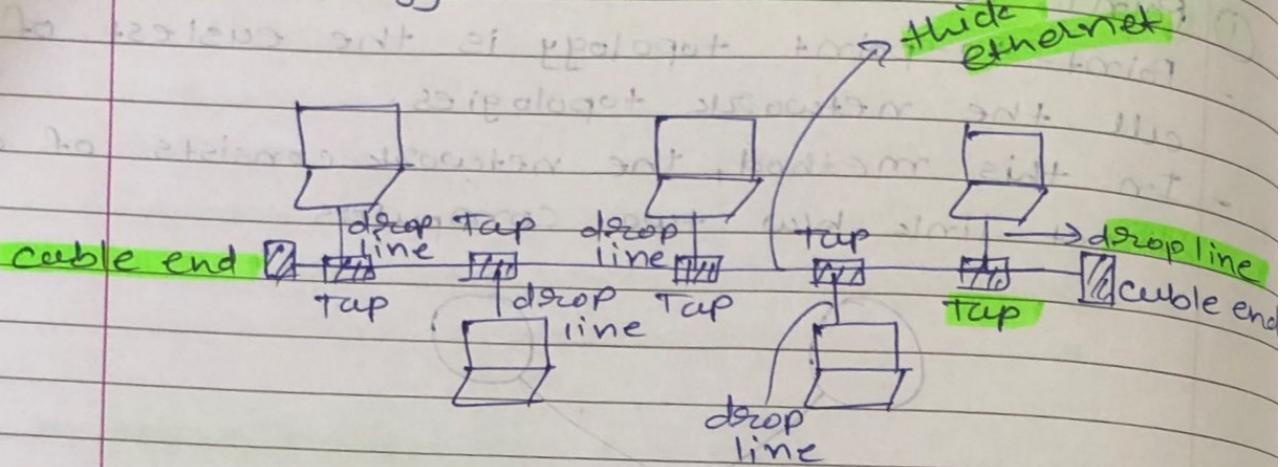


→ **Advantages:-** This is faster and highly reliable than other types of connections since there is a direct connection.

- No need for a network operating system.
- Does not need an expensive server as individual workstations are used to access the files.
- No need for any dedicated network technicians because each user sets their permissions.

- ⇒ **Disadvantages!** - The biggest disadvantage is that it only be used for small areas where computers are in close proximity.
- You can't back up files and folders centrally.
 - There is no security besides the permission. Users often do not require to log onto their workstations.

② Bus Topology



- Bus topology contains uses a single cable which connects all the nodes.
- the main cable acts as a spine / backbone for the entire network.
- One of the computers in the network acts as the computer server.
- It has two endpoints; it is known as a linear bus topology.

⇒ Advantages! -

- Cost of the cable is very less as compared to other topology, so it is widely used to build small networks.
- Famous for LAN network because they are inexpensive and easy to install.

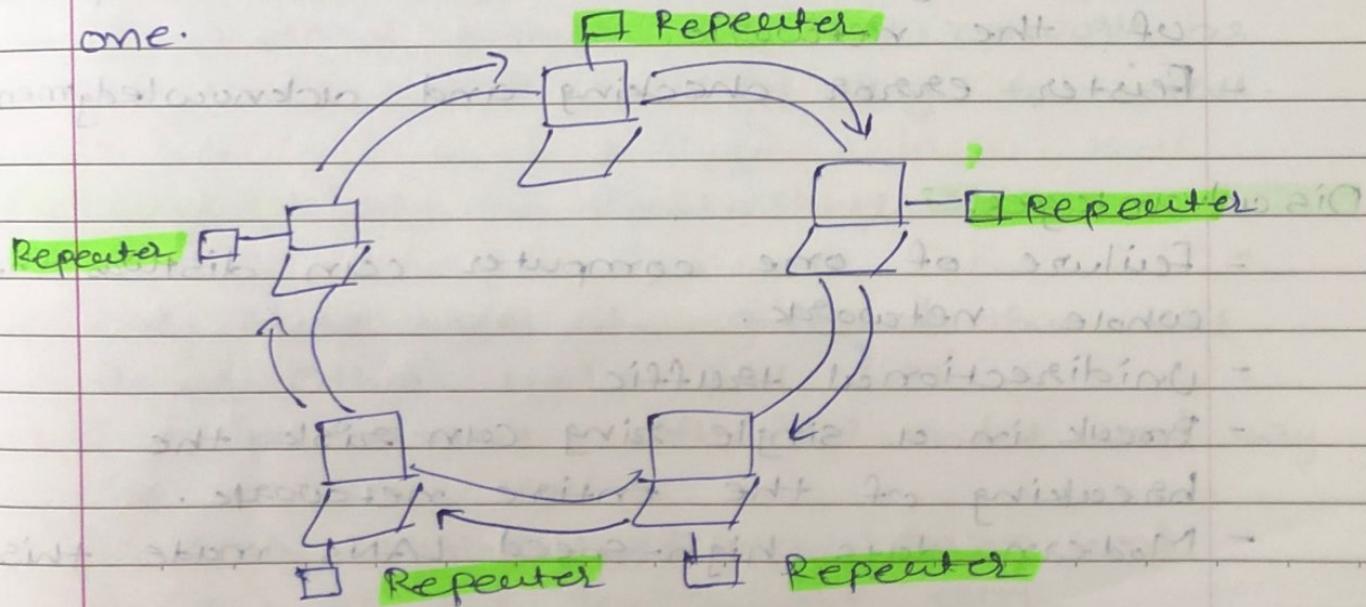
- It is widely used when a network installation is small, simple or temporary.

→ Disadvantages:-

- In case if the common cable fails, then the entire system will crash down.
- When network traffic is heavy, it develops collision in the network.
- Whenever network traffic is heavy, or nodes are too many, the performance time of the network significantly decreases.
- Cables are always of a limited length.

③ Ring Topology

- It is used for LAN & WAN in which every device has exactly 2 neighbours for communication purpose. It is called a ring topology as its formation is like a ring.
- In this topology, every computer is connected to another computer in a circular manner.
- The last node is combined with the first one.



- Here, the data travels around the ring in only one direction.

- eg:- If node 1 wants to send the data to Node 3,
- Node 1 sends the data to Node 2
 - Node 2 checks the odd, then transmits
 - Node 2 sends the data to Node 3
 - Node 3 checks the odd, and matches with its own odd. If matches then keep it.
 - If we wants to insert a PC in already formed network, we can easily add/remove a PC in the network. the administrator needs only one ^{more} port & extra cable.

- Advantages:-**
- Easy to install and reconfigure.
 - Adding or deleting a device in ring topology needs **you** to move only two connections.
 - The troubleshooting process is difficult in ring topology.
 - Offers equal access to all the computers of the network.
 - Faster error checking and acknowledgment.

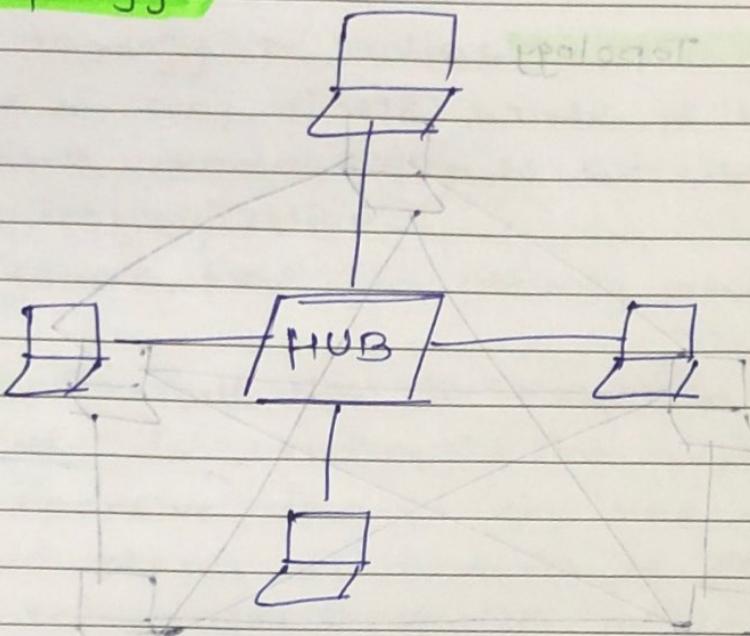
Disadvantages:-

- Failure of one computer can disturb the whole network.
- Unidirectional traffic
- Break in a single ring can risk the breaking of the entire network.
- Modern days high-speed LANs made this

topology less popular.

- In the ring, topology signals are circulating at all times, which develops unwanted power consumption.
- It is very difficult to troubleshoot the ring network.

(4) Star Topology.



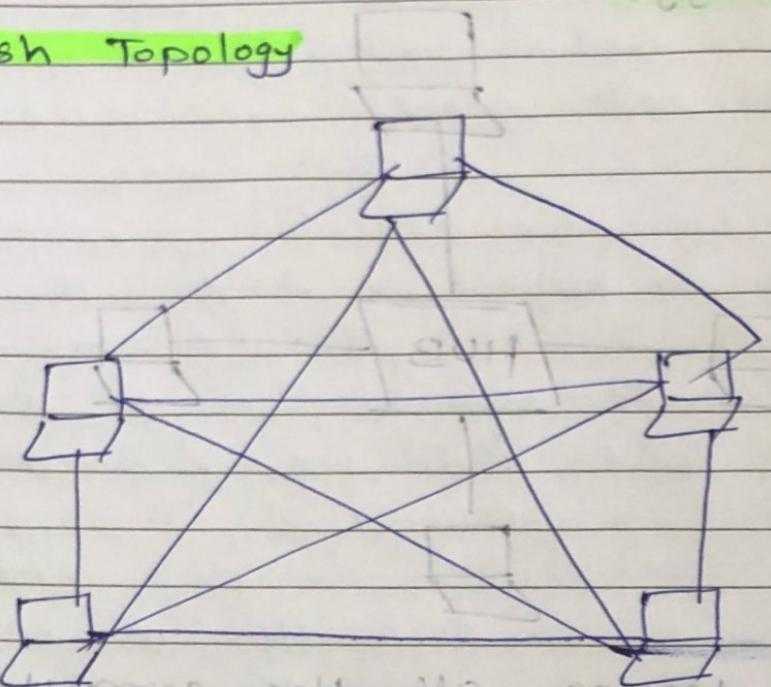
- In star topology, all the computers connect with the help of hub. This is called a central node, and all other nodes are connected using this central node.
- It is most popular on LAN networks as they are inexpensive and easy to install.

Advantages: - Easy to troubleshoot, set up and modify.

- Only those nodes are affected that has failed. Others nodes still work.
- Fast performance with few nodes and very low network traffic.
- In star topology, addition, deletion, and moving of the devices are easy.

- Disadvantages:-** If the hub or controller fails, attached nodes are disabled.
- Performance depends on the hub's capacity.
 - A damaged cable or lack of proper termination may bring the network down.
 - A dependency of the whole topology is on the one single point (the hub).

⑤ Mesh Topology



- In this topology, every nodes or device are directly connected with each other.
- Every device has dedicated point-to-point link to each other.
- The term dedicated means that, the link carries traffic only b/w the two devices only.
- The total number of cable required having n devices = $n(n-1)$ ($\because \frac{n(n-1)}{2} = \frac{5(4)}{2} = 10$)
- Each and every device is connected to $(n-1)$ devices.
- Total $(n+1)$ input/output (IO) ports required.

- All devices are connected to each other using multipoint connection.

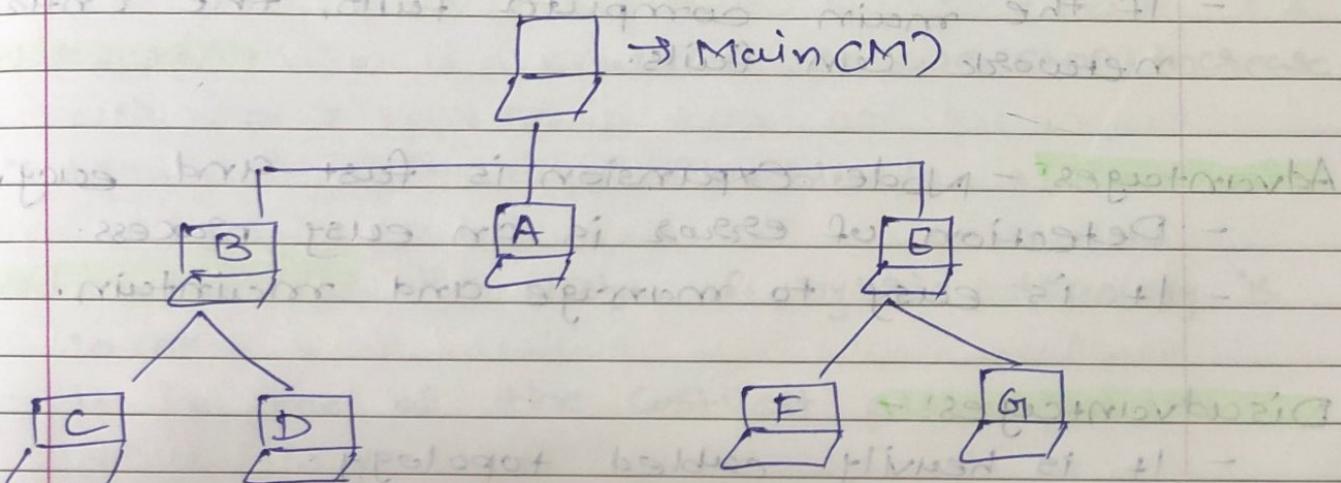
Advantages: - The use of dedicated links guarantees that each connection can carry its own data load.

- No traffic problem as nodes has dedicated links.
- A mesh topology is robust! - It has multiple links, so if any single route is blocked, then other routes should be used for data communication.
- Every system has its privacy and security.

Disadvantages: - Installation is complex because every node is connected to every node.

- It is expensive due to the use of more cables. No proper utilization of systems.
- Complicated implementation.
- It requires more space for dedicated links.

(6) Tree Topology



- A tree network topology is a sort of structure in which each node is related to others in a hierarchy.
- All elements are arranged as in this topology - like the branches of a tree.
- Tree topologies are commonly used to arrange data in databases and workstations in corporate networks.
- In given fig, the main computer M, initiates the traffic flow b/w various components.
- It uses a distributed approach, and every computer is managed by its upper-level computer.
- In fig C and D, the system is controlled by B, similarly, F and G are controlled by E, and further A, B and E are controlled by M. So, no doubt the controlling of children system by its parent reduce the workload of main computers.
- Indirectly, all the computers are controlled by the main computer M.
- ✓ - Still, no doubt the controlling of children system by its parent reduce the workload of main computers.
- If the main computer fails, the entire network fails.

Advantages: - Node expansion is fast and easy.

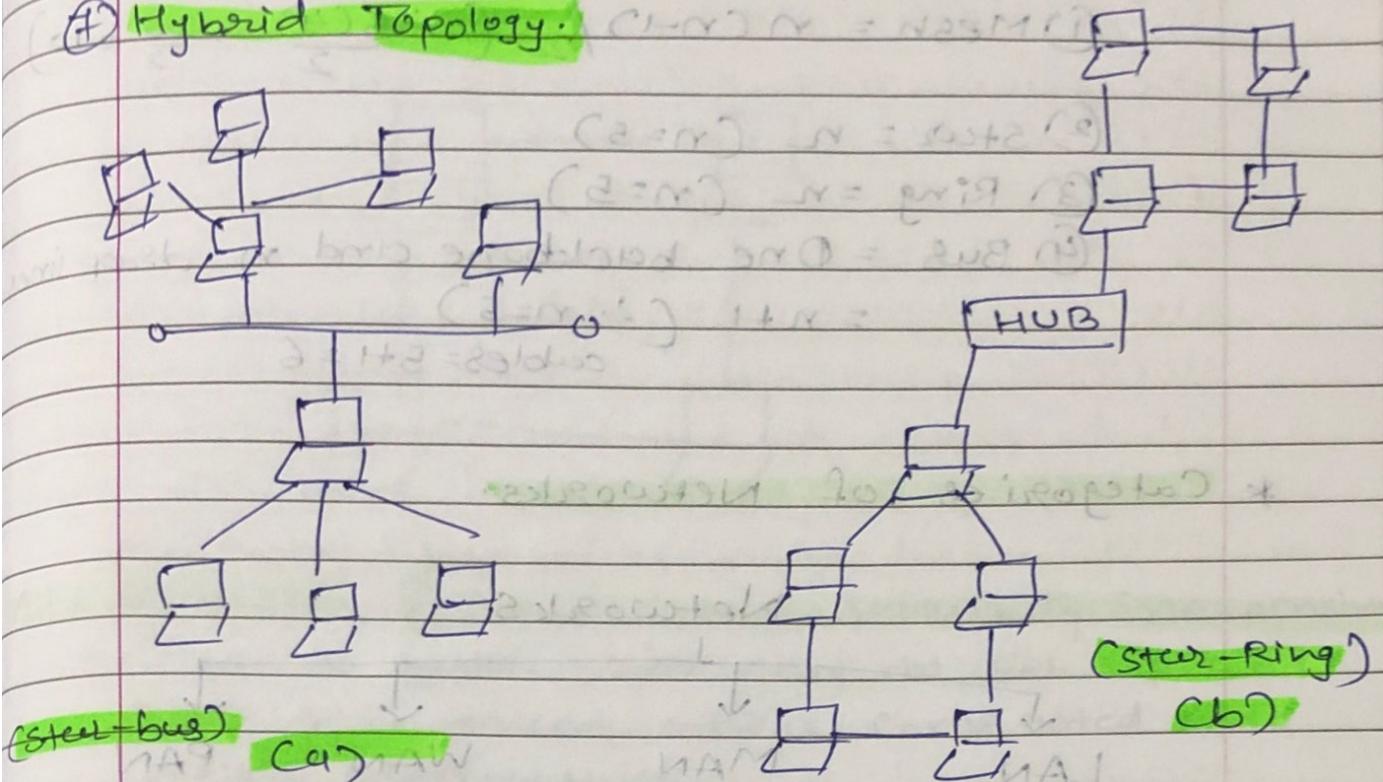
- Detection of error is an easy process.
- It is easy to manage and maintain.

Disadvantages: -

- It is heavily cabled topology.
- If more nodes are added, then its maintenance is difficult.

- If the hub or controller fails, attached nodes are also disabled.

(7) Hybrid Topology:



- Hybrid topology combines two or more topologies.
- If there is a ring in one office department while a bus in another department, connecting these two will result in Hybrid topology.

Advantages: - It is scalable, so we can increase our network size.

- Highly effective and flexible.

Disadvantages: - The design of hybrid topology is complex.

- It is one of the costliest processes.

* Number of cable required for cell topologies.

$$n=5$$

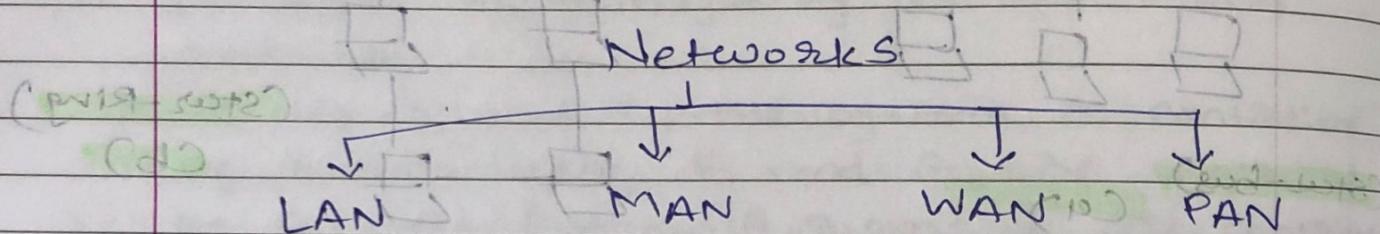
$$(1) \text{ Mesh} = n(n-1)/2 \quad (\because \frac{5(4)}{2} = \frac{20}{2} = 10)$$

$$(2) \text{ Star} = n \quad (n=5)$$

$$(3) \text{ Ring} = n \quad (n=5)$$

$$(4) \text{ Bus} = \text{One backbone and } n \text{ drop lines.} \\ = n+1 \quad (\because n=5) \\ \text{cables} = 5+1 = 6$$

* Categories of Networks.



LAN = Local Area Network

PAN = Personal Area Network

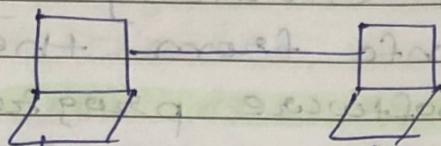
MAN = Metropolitan Area Network

WAN = Wide Area Network

* (1) Local Area Network (LAN)

- LAN is a group of computers connected to each other in a small area such as building, office, etc.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hw, such as, hubs, network adaptors and ethernet cables.

- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.



LAN

Advantages:- ① Simple and relatively inexpensive

This is quick and easy to set up and reasonably priced when compared to other alternatives.

If an organization intends to build a network at a minimal price and with flexibility, a local area network is the ultimate answer.

② Collaboration of Resources!:-

Expensive components such as printers and scanners cannot be linked to every device since it will indeed be very burdensome for the company, but thanks to LAN, a corporation only clearly need one printer and scanner, and anyone can link to that printer and scanner and sends instructions from their machines, leading in meaningful cost savings for the corporation.

(3) The association involving client and server:- All information from connected PCs may be maintained on a single server. If machine (client) demands information, the client may effortlessly log in and retrieve the info from the system.

(4) Accessing of software programs:-

- On the LAN, software programs may also be shared. All devices can use single licensed program.
- It is pricey to buy a license for each device on a network, ∵ sharing SW is simple and straightforward and cost-effective.

(5) Data Protection:- It is more safe and secure to keep information on the server. And if we wish to update or eliminate any file, we can do so

rapidly on a single server computer, and other devices will be able to obtain the new information.

- Only approved users have accessibility to the network's data.

(6) Fast Communication:- LAN connected systems or devices communicate directly at very high rates of speed.

Disadvantages:- (1) the information security issue that arises:- Unapproved users can retrieve data if the server equipment is not programmed correctly and there is a technical glitch.

(2) Long-distance major limitation:- LAN are often devised within a building or

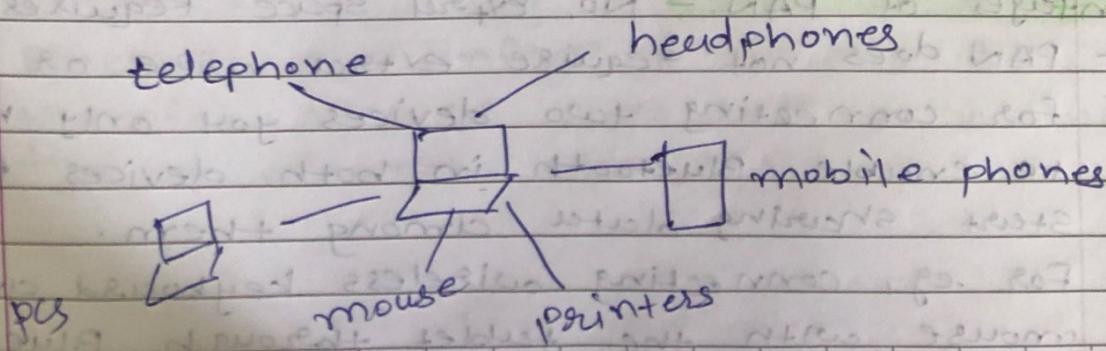
apartment complex and cannot be stretched to a bigger area.

(3) All devices may be disproportionately affected if the server fails:- If a file on the server gets heavily damaged or a hard disc crashes, all of the linked PCs will have extreme difficulty operating correctly.

(4) Data sharing via outside sources:- Another drawback of LAN that it is difficult and time-consuming to send files from outside the network since transportable media such as pen drives and CDs cannot be conveniently performed on all devices on the network.

*2) Personal Area Network (PAN)

- PAN is a network arranged within an individual person, typically within a range of 10 meters.
- PAN is used for connecting the computer devices of personal user is known as PAN.
- PAN covers an area of 30 feet.
- Personal computer devices that are used to develop the PAN are laptop, mobile phones, media player and play stations.



Types of PAN

Wired PAN

- Wired PAN is created by using the USB.

Wireless PAN

- Wireless PAN is developed by simply using wireless technologies such as WiFi, Bluetooth.

⇒ Examples of PAN include -

→ **Body Area Network**: Body Area Network is a network that moves with a person. For eg:- a mobile network moves with a person. Suppose a person establishes a network connection and then creates a connection with another device to share the information.

→ **Offline Network**: An offline network can be created inside the home, so it is also known as a home network.

→ A home network is designed to integrate the devices such as printers, computer, television but they are not connected to the internet.

Advantages of PAN:- No extra space required.

- PAN does not require extra wire or space.
- For connecting two devices you only need to enable Bluetooth in both devices to start sharing data among them.
- For eg, connecting wireless keyboard and mouse with the tablet through Bluetooth.

⇒ Connect to many devices at a time:-

- Many devices can be connected to one device at the same time in a PAN.

- We can connect one mobile to many other mobiles or tablets to share files.

⇒ Cost effective:-

- No extra wires are needed in this type of network. Also, no extra data charges are involved so PAN is an inexpensive way of communication.

⇒ It is easy to use.

⇒ If you use this type of data connection within 10 meters then your network is stable and reliable.

⇒ Secured:-

- This network is secured because all the devices are authorized before data sharing.

⇒ A person can move devices as it is a wireless network and data exchange is not affected. That means PAN is portable as well.

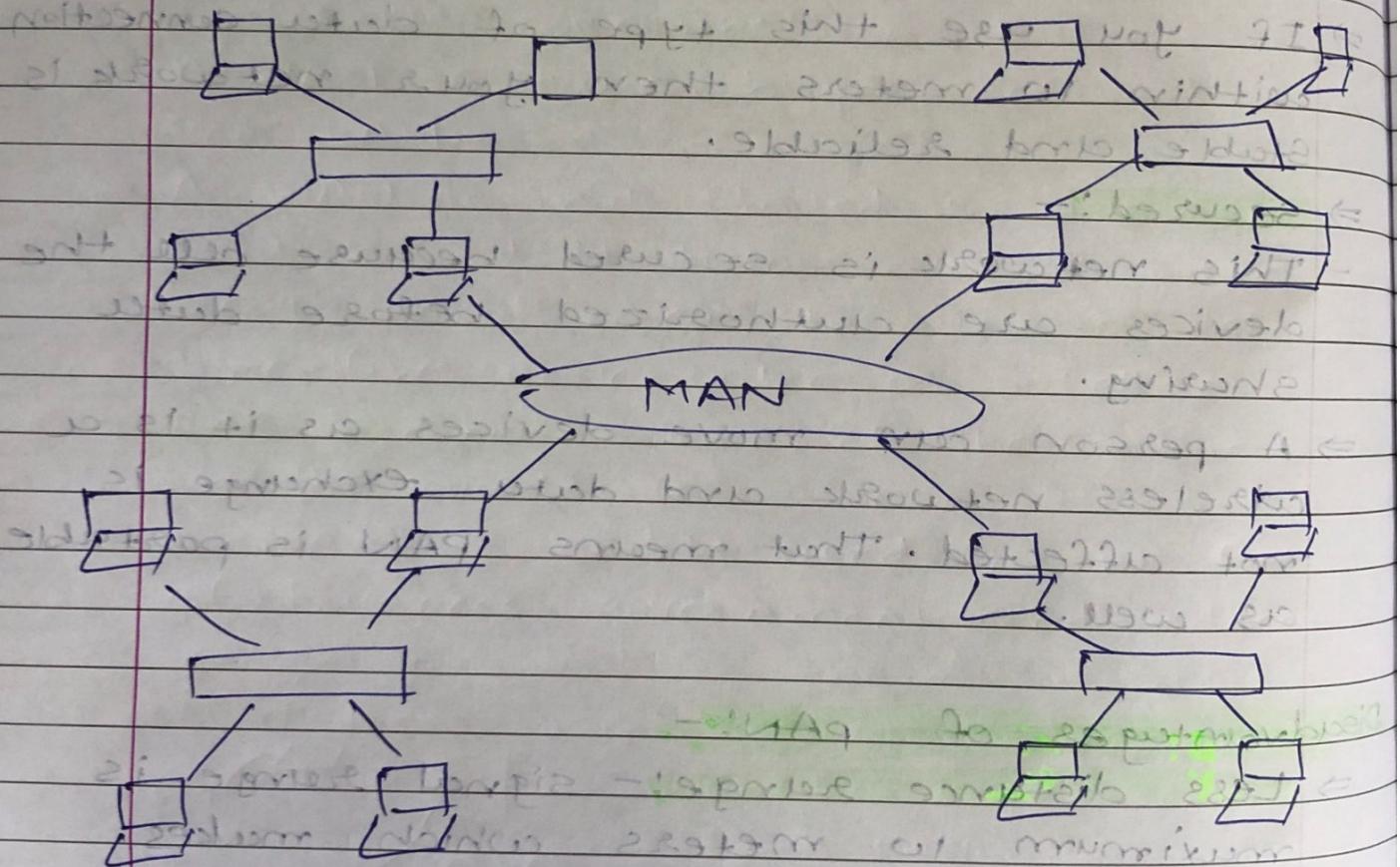
Disadvantages of PAN:-

⇒ Less distance range:- signal range is maximum 10 meters which makes limitation for long distance sharing.

⇒ Bluetooth and infrared have a slow data transfer rate as compared to another type of networks like LAN.

* 3) Metropolitan Area Network (MAN)

- A MAN is a network that covers a large geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through telephone exchange lines.
- It has a higher range than LAN.



- MAN is used in communication between the banks in a city.
- It can be used in an Airline Reservation.
- It can be used in a college within a city.
- It can also be used for communication in the military.

Advantages! - Less expensive

- It is less expensive to attach ~~with~~ MAN with MAN. MAN gives the good efficiency of data. In MAN, data is easily managed in a centralized way.
- ⇒ On MAN you can send local emails fast and free.
- ⇒ MAN uses fiber optics so the speed of data can easily reach upon 1000 mbps. Files and databases can be transferred fast.
- ⇒ In some installation of MANS, users can share their internet connection. So multiple users can get the same high-speed internet.
- ⇒ MAN has a high-security level than WAN.

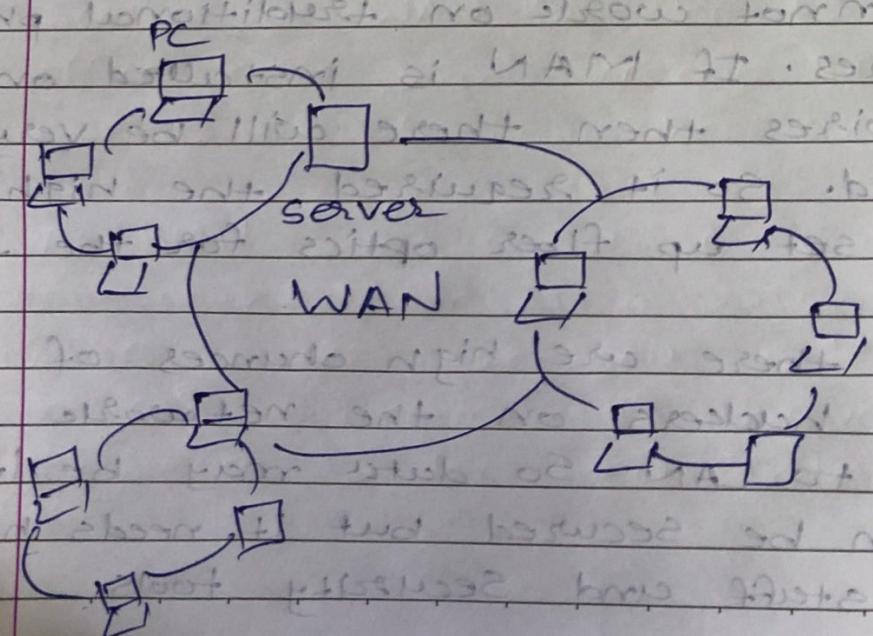
Disadvantages! -

- ⇒ If MAN becomes bigger then it becomes difficult to manage it. This is due to a security problem and other extra config.
- ⇒ MAN cannot work on traditional phone copper wires. If MAN is installed on copper wires then there will be very low speed. So it required the high cost to set up fiber optics for the first time.
- ⇒ In MAN there are high chances of attacking hackers on the network compared to LAN. So data may be leaked. Data can be secured but it needs high trained staff and security tools.

- ⇒ To setup MAN, it requires technical people that can correctly setup MAN. The technical people are network administrators and troubleshooters.
- ⇒ In MAN, additional cables are required to connect two LAN, which is another problem.

* (4) Wide Area Network (WAN)

- A WAN is a network that extends over a large geographical area such as states or countries.
- A WAN is quite bigger than the LAN.
- A WAN is not limited to a single location, but it spans over a large geographical area through a telephone line, fiber optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A WAN is widely used in the field of Business, government and education.



⇒ Examples of WAN

- Mobile Broadband : A 4G network is widely used across a region or country.
- One company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
- A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased lines provided by the telecom company.

Advantages:-

- ⇒ WAN covers a large geographical area of 1000 km or more if your office is in different cities or countries then you can connect your office branches through WAN.
- ⇒ Your company doesn't need to buy email, files and backup servers, they can all reside on head office. All office branches can share the data through the head office server. You can get back up, support, and other useful data from the head office and all data are synchronized with all other office branches.
- ⇒ Now companies work over the live server to exchange updated files. So all the coders and office staff get updated version of files within seconds.
- ⇒ Now everyone with computer skills can do business on the internet and expand his business globally. (shopping cart, sale & purchase)

⇒ Another benefit of WAN is that, you can distribute your work to other locations. For eg, you have an office in the U.S. then you can hire people from any other country and communicate with them easily over WAN. It also reduces your travel charges as you can monitor the activities of your team online.

Disadvantages:-

- ⇒ WAN has more security problems as compare to MAN and LAN. WAN has many technologies combined with each other which can create a security gap.
- ⇒ As data transferred on the internet can be accessed and changed by hackers so firewall needs to be enabled in their computer. Some people can also inject a virus into the computer so antivirus software needs to be installed. Other security SW also needs to be installed on different points in WAN.
- ⇒ Setting up WAN for the first time in office costs higher money. It may involves purchasing routers, switches and extra security SW.
- ⇒ As WAN covers a lot of areas so fixing the problem in it is difficult. Most of WAN wires go into the sea and wires get broken sometimes. It involves a lot of resources to fix lines under the sea.