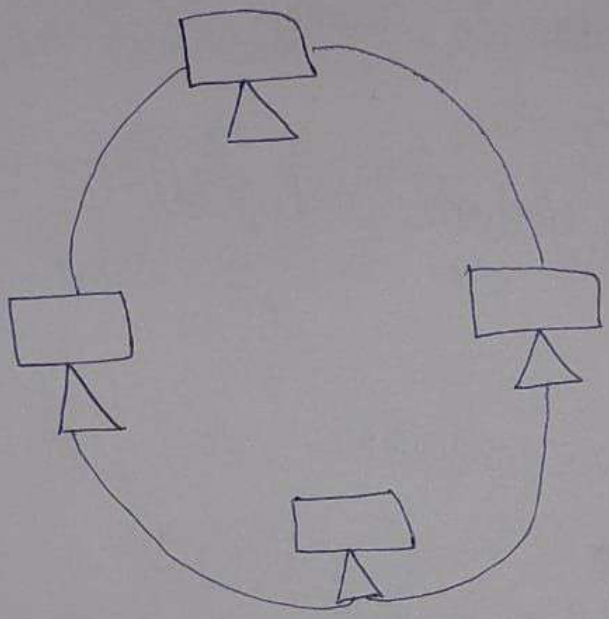
Chapter - 1

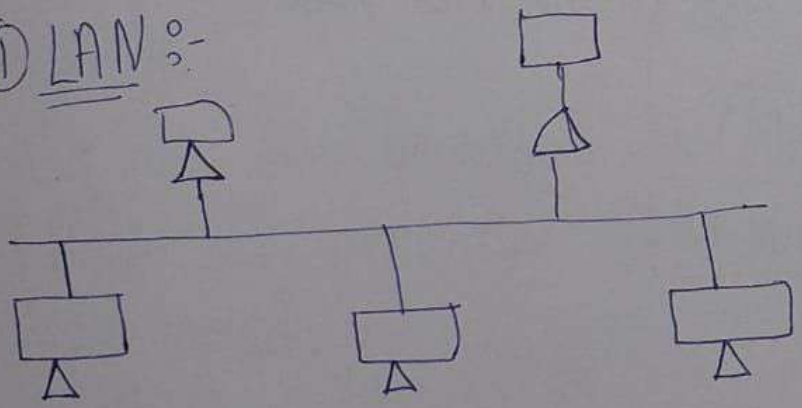
⇒ Computer Network :-

- A group of computers which are connected to each other fo the purpose of sharing their resources is called computer netw



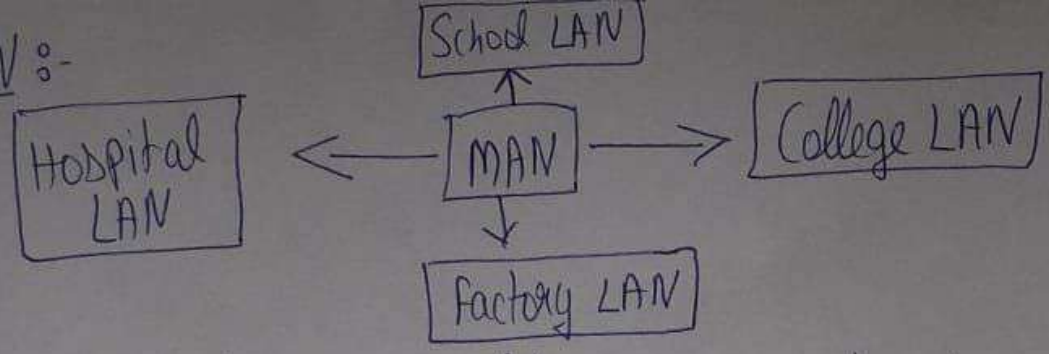
⇒ Classification of Computer network :-

① LAN :-



- LAN stands for local area network.
- It is used for building like offices.
- Transmission speed of data is high.
- LAN network range 0 to 150 m.
- LAN network ownership is private.

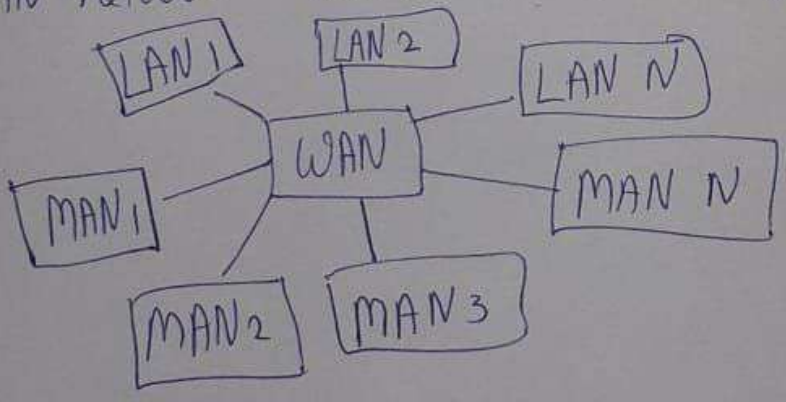
② MAN :-



- MAN stands for metropolitan area network.
- It is used for city like Kolkata.
- Transmission speed of data is average.
- MAN network range 5 to 50 km.
- MAN network ownership is private and public.

③ WAN :-

- WAN stands for wide area network.
- It is used for countries.
- Transmission speed of data is low.
- WAN network range is not fixed
- WAN network ownership is also private and public.

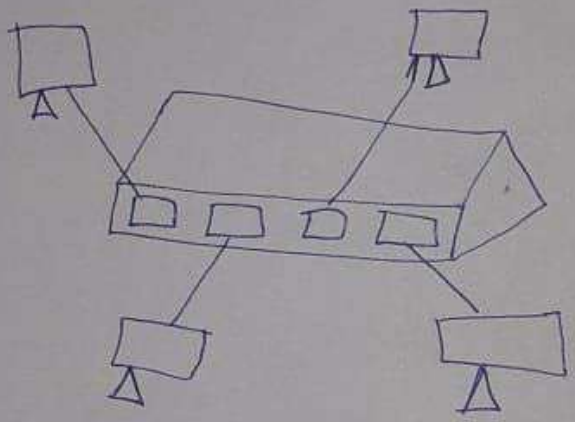


⇒ Network Hardware :-

- Network hardware is the physical equipments needed to perform the data processing and communication within the network.

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.
- A HUB is less expensive, less intelligence & less complicated.
- HUB generally used to connect computers in a LAN.
- Transmission mode of HUB is half duplex.



Advantages

- The HUB can broadcast the message.
- It is less expensive that anyone can use it.
- Easy installation.
- Robust

Disadvantages

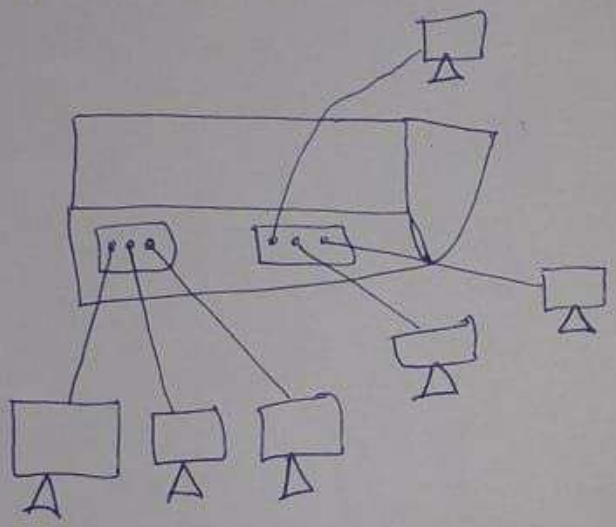
- If the HUB is failed the entire network will be failed.
- We can't send private / personal data through hub.
- HUB doesn't provide any security.
- HUB can't support full duplex transmission mode.

Switch :-

Switch is a network device that connects multiple computers together in the network.

It is mainly used to send the private message as well as their is no wasting of data.

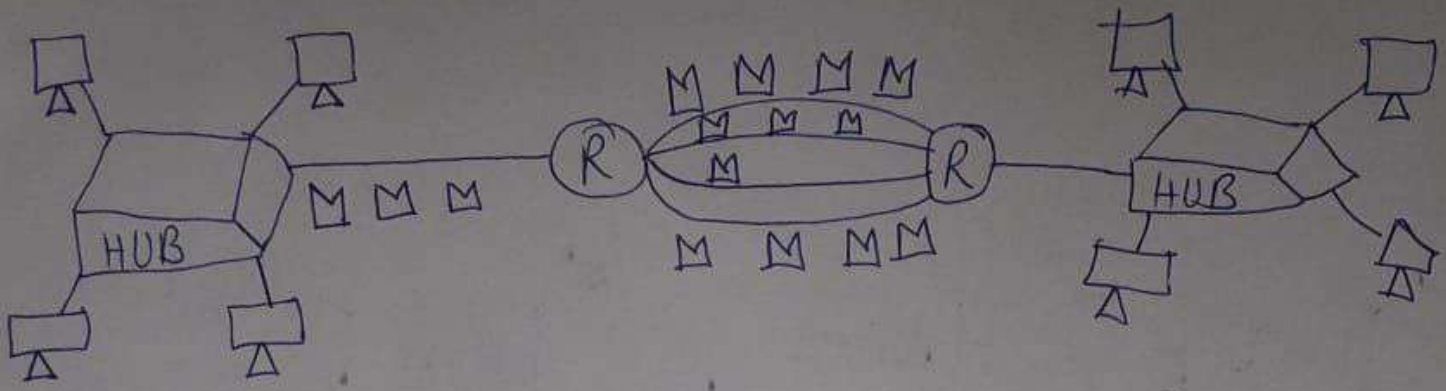
Switch can easily identify that which device is connected with which port by using MAC address thats why it delivered message on particular destination machine.



Note :- Switch is more intelligent than HUB.

3. Router :-

- Router is a network device which works as a traffic controller.
- A main work of router is to choose a congestion free path through which the data packet will travel.
- Router recieve data packets to the sender, analyze and forward those data packets then giving to reciever.



Sender

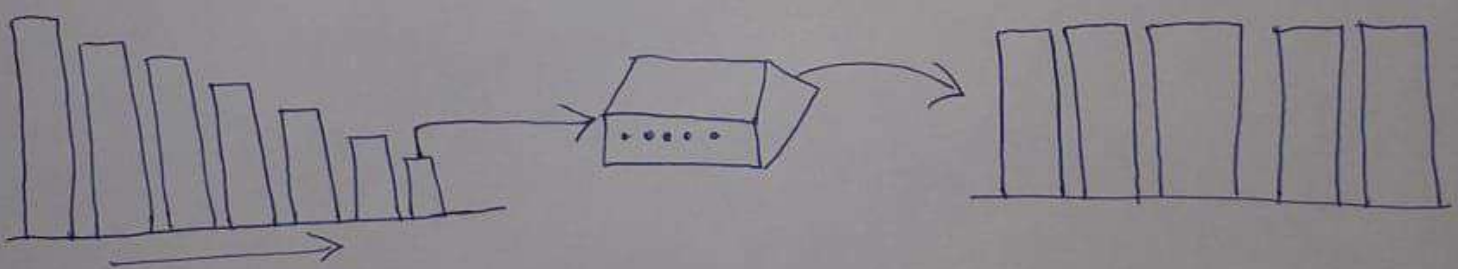
Reciever

Fig - Router Network device

Note :- Router uses both LAN & WAN Network.

4. Repeater :-

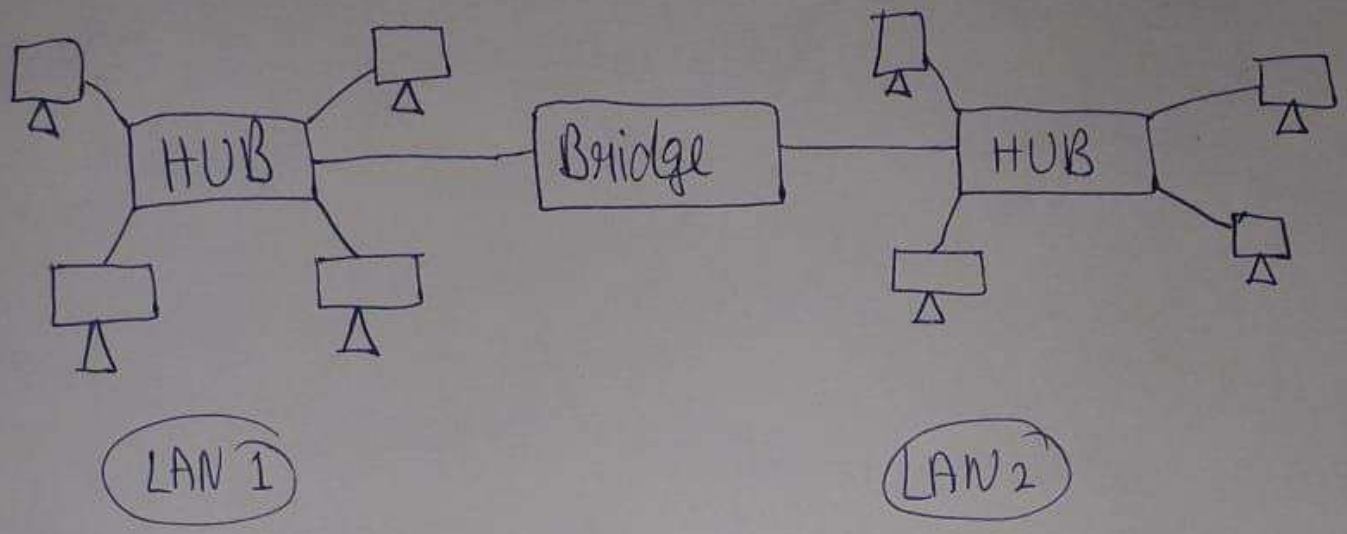
- Repeater is a network device through which we can boost up the weak signals.
- When the signal travels in the network, after travelling some distance the intensity of the signal becomes low.
- In order to regenerate the weak signal we should use repeater device.



Note :- It is used in Wired & Wireless.

5 Bridge :- Bridge is a network device that is used to

separate LAN into no. of section.

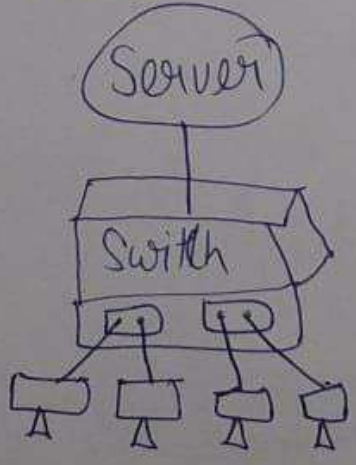


- It operates both physical as well as data link layers of OSI model.
- By using bridge device we can extends network. It broadcast the data to each node like HUB & Repeater.

6. Gateway :-

Gateway is hardware device that is used to connect two dissimilar type of network.

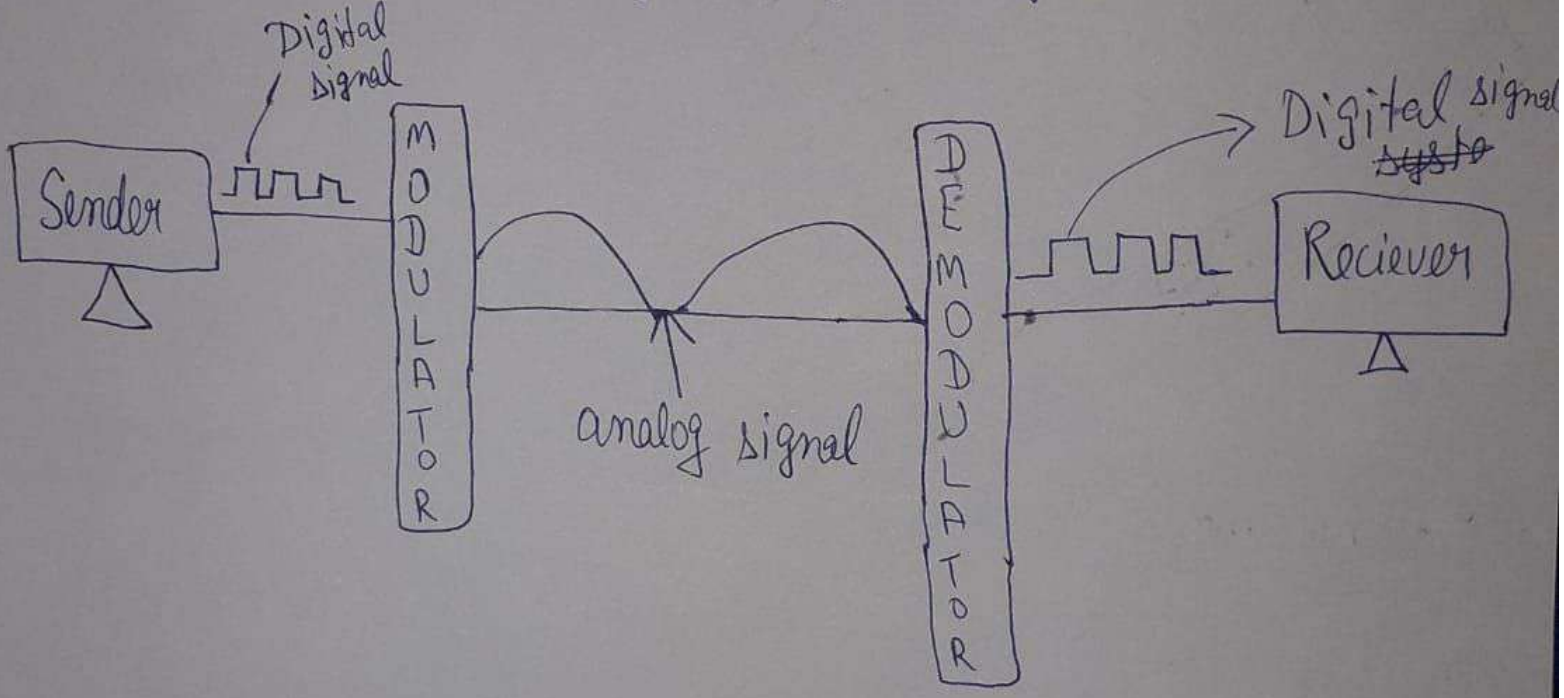
- It allow us to send & recieve data through the internet even it is LAN network.



- It operates all 7 layer of OSI model.

7. Modem device :-

- Modem stands for modulator & demodulator it is a network device that is placed between the computer system and telephone.
- It has two part modulator & demodulator.
- Modulator convert digital signal to analog signal where as demodulator convert analog to digital signal.



Note :- It allow us to computer to connect internet.

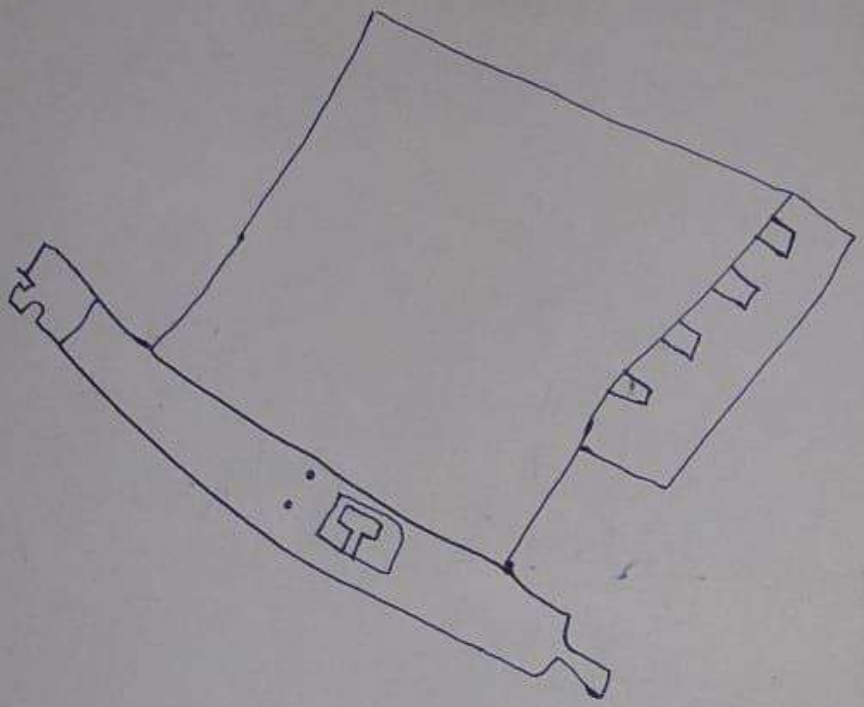
8. NIC :-

- NIC stands for network interface card, it is hardware device without which we can't 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 the network Card where it can be inserted.
- It requires a network cable (RJ45) to provide network access.



2. External network Card :-

- In desktop & laptop that don't have an internal NIC, external NIC's are used.
- It is of two types :- (i) Wireless
  (ii) USB Cable

⇒ Network Software :-

- Network Software is a broad category that includes network operating system, network protocols, and device drivers. These components work together to enable communication and management

twork device.

Network operating System :-

A network operating system is specialized software that manages network resources and enables devices to communicate within a network.

eatures of NOS :-

)User and Device Management :

ontrols user access and permissions

) File and printer sharing :

- Allows multiple devices to share files and peripherals.

3) Security & Authentication :-

- Provides firewalls, encryption and authentication.

4) Remote Access :-

Supports remote administration of network devices

Example :- Windows Server, Linux

2. Network protocol :-

- It is a set of rules and procedures for communication between devices in a network.

- Protocols for computer networking all generally uses packet switching technique to send and recieve messages in the form of packets.

- It provides the techniques to identify and make connection with each other, as well as formatting rules that specify how data is packed into messages sent and received.

3. Device deriver :-

- A device deriver is software that allows the operating system to communicate with network hardware such as network interface cards, routers, and switches.

Functions

(i) It enable the hardware functionality which allows the operating system to control network hardware.

(ii) It improves the performance that optimizes the data transmission and reception

(iii) It allows tuning of network settings for efficiency.

(iv) It ensures compatibility with security standards

⇒ Protocol Hierarchy :-

- A protocol hierarchy is a layered model where each layer in the communication system is responsible for specific tasks.
- The most common hierarchial models are OSI (7 layers) and TCP/IP (4 layers).

Each layer in this hierarchy :-

(i) Provides services to the layer above it.

(ii) Recieves services from the layer below it.
(iii) Communicates horizontally with its peer layer on another system (Peer to peer).

→ Hierarchial communication (Vertical communication)

- Hierarchial communication occurs within one computer or device, moving up and down the protocol stack.
- For example : Data travels downward from the application layer to the physical layer during transmission.
- On the receiver's side, data travels upward, from the physical layer to the application layer.
- It represents internal communication between different layers of the same system.
- Each layer adds or removes headers.

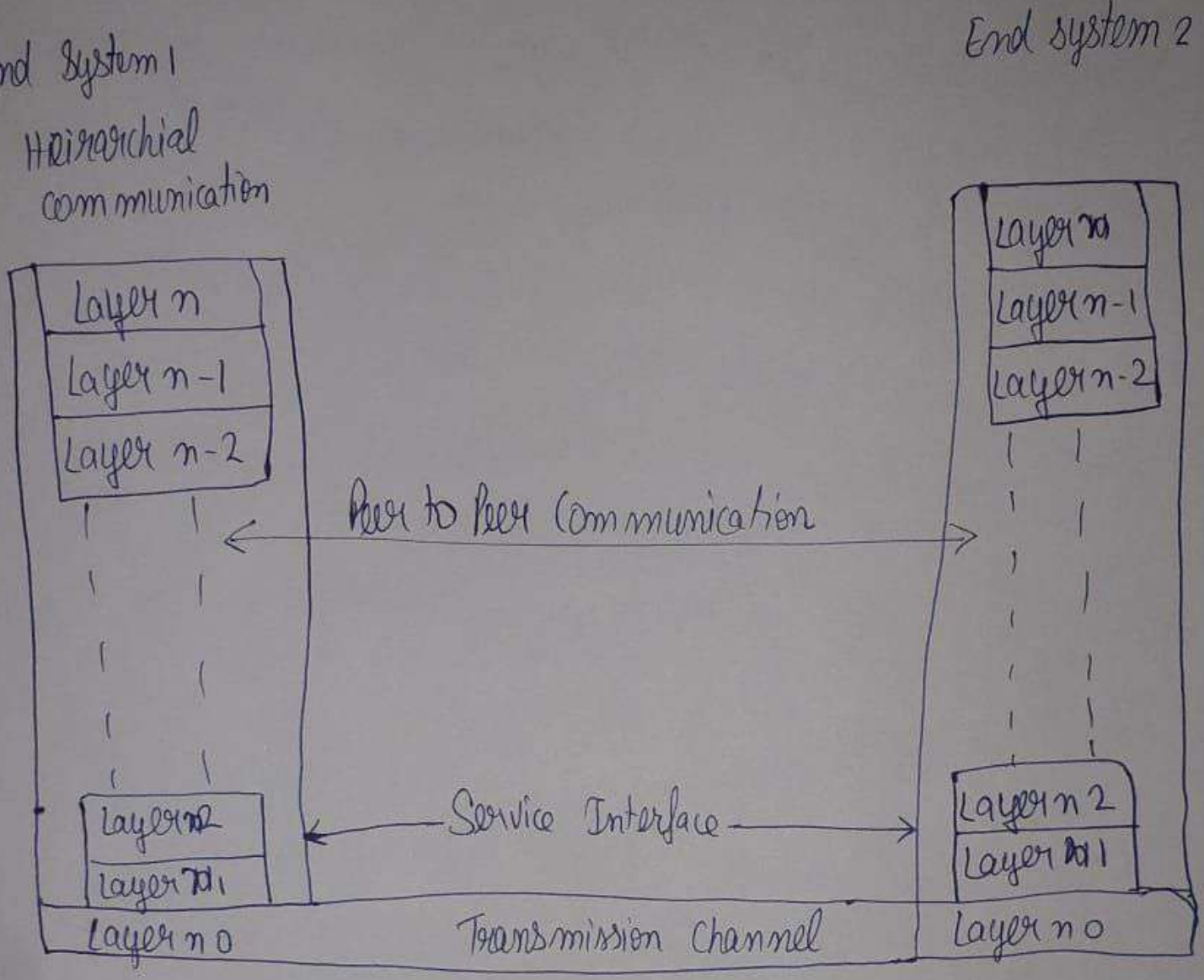
→ Peer to Peer Communication (Horizontal communication)

- Peer to peer communication happens between corresponding layers on different machines.
- For example :-

-HTTP (Application layer) on computer A talks to HTTP on computer B.
- TCP (Transport layer) on computer A talks to TCP on computer B.

- Each layer follows strict protocols to ensure both devices understand the data.

- Peer layers communicate across the network.
- They use protocols that define how communication happens (rules and formats).



⇒ Design issues of the layer :-

- There are some key design issues present in different layers of computer Network.

① Addressing :-

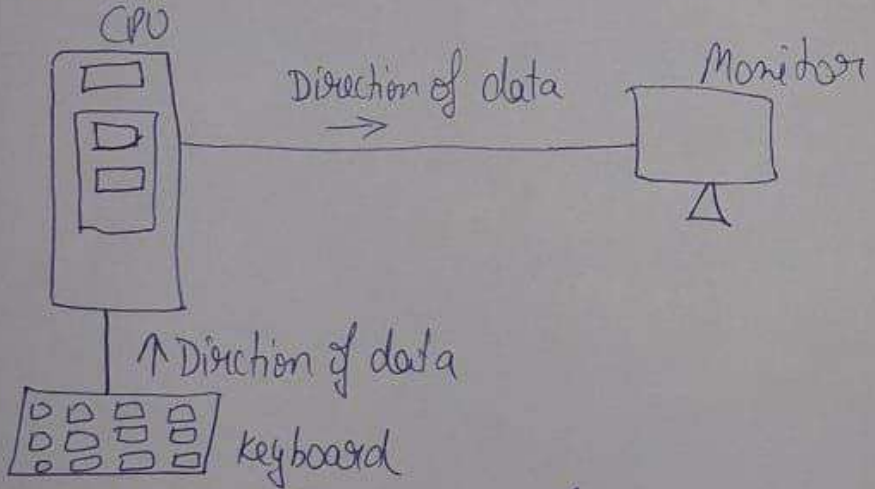
- Each layer needs to have some kind of machenism to identify sender and reciever.
- Network normally have multiple computers. Sender needs to

specify whom it want to talk.

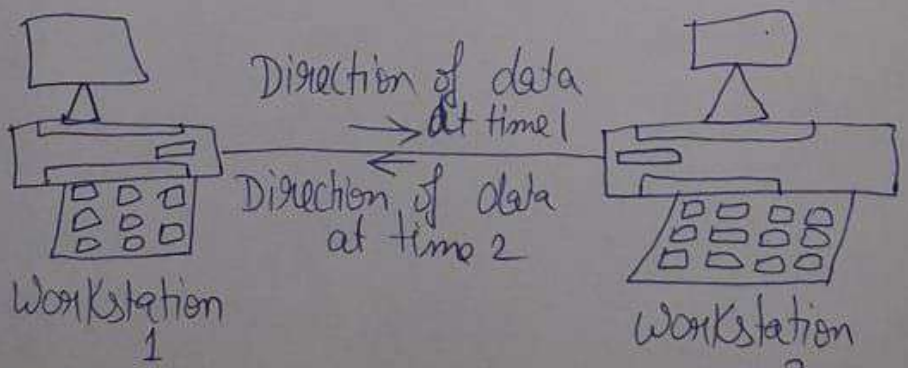
- So some kind of addressing is needed to specify destination. Each host machine connected in network has unique address.

(2) Unidirectional and bidirectional transmission :-

- Another design concern is to take decision on how the data is transmitted.
- In some systems data moves only in single direction (unidirectional data transfer).
- In some cases data can go in both the direction (bidirectional data transfer).
- Protocol should also decide how many logical channels are needed.



[Unidirectional data transfer)



[Bidirectional data transfer]

Error Control :-

All the layers needs to make sure that data sent by sender needs to arrive at in proper order and without any error.

Recievver should have some machenism to provide feedback (ACK) to the sender about whether data is recieved correctly or not.

- ACK and timer is used.

④ Flow control :-

- The another important design issue is "What if sender can send data faster then reciever can accept them".
- The situation can occur if the sender is running in a fast powerful computer and reciever is running on slow machine.
- In this case reciever can loose some data. Some flow control mechanism is needed at layers.

⑤ Assembling and Deassembling :-

- When the messages to send are very large in size. Sender divide the messages into smaller messages called deassembling and transmit smaller messages.
- Reciever Recieves smaller messages and combine them to form actual message called assembling.

⑥ Routing :-

- There might be multiple paths available between sender and reciever, layers needs to take decision on which path to choose. This process is called as Routing.

- The path which will take less time will be choosed.

⇒ Connection oriented and connectionless services :-

- Layers can offer two types of services to its upper layer : Connection oriented and connectionless.

1. Connection oriented service :-

- In connection oriented service
(i) Connection is first established
(ii) Connection is used
(iii) Connection is released

Example : Telephone System

1> User dails the number and waits for the answer (Connection is being established)

2> User communicates (connection is used)

3> User Hang UP (connection is released)

Connection acts like a tube, in which sender pushes the message from one end and reciever takes them out at other end i.e order of the messages are preserved.

When connection is established, the sender and reciever may conduct negociation on the parameter used i.e

1) Size of the message
2) Quality of Service

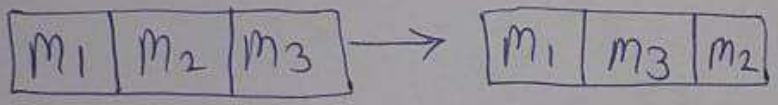
Typically one side makes the proposal other side can accept it, reject in make counter proposal.

2. Connectionless Service :

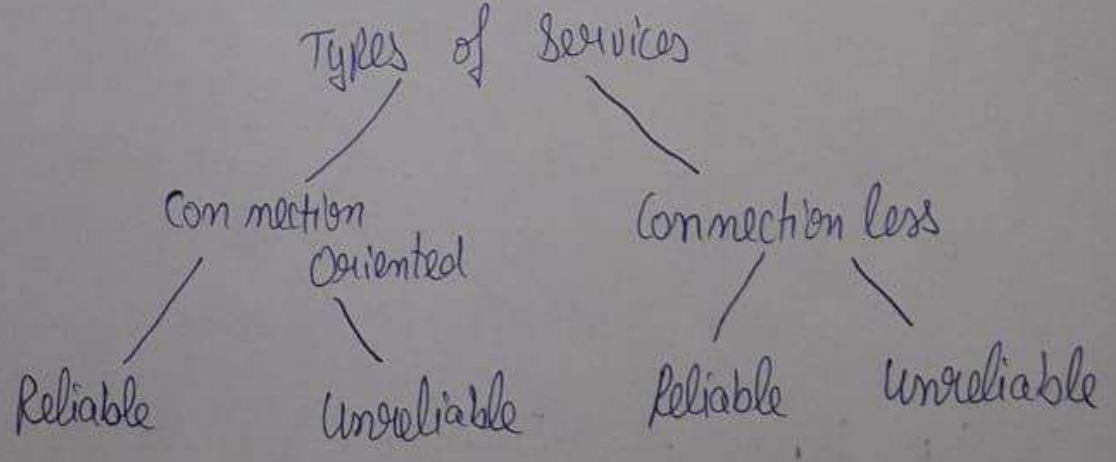
- In Connectionless Service no prior connection is established before sending a message.

eg: Postal system

- The order of the message may not be preserved.



- Each message will carry full destination address, each message will be routed through the path independent of each other.
- Both connection oriented and connectionless Service can be either Reliable or Unreliable.



- Reliable Service :-

- Reliable services will never loose data. Usually reliable services uses Acknowledgement to confirm whether messages are recieved or not.
- If the reciever recieves the message it sends the + ve ACK, otherwise it will send - ve ACK. When - ve ACK is recieved message is retransmitted
- The ACK process introduce overhead and delays.

- Unreliable Service :
- Unreliable service may loose data as it does not uses ACK machenism

⇒ Network Architecture :-

Network architecture means network layot that tells us how computers are arranged and how task are allocated to the computer.

Types of network architecture :-

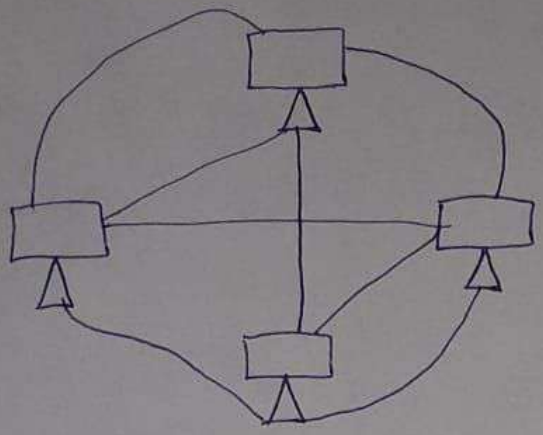
1. Peer to Peer architecture
2. Client Server architecture

1. Peer to peer architecture :-

- Peer to peer network also known as point to point network

in which all the computers are diversely linked together with equal privileges and responsibilities for sharing the data.

- There is no server in it.



Advantages :-

- It is a cheaper network as it has no server.
- If one computer stops working it will have no effect on other computer.
- Its setup and maintanance is also easy.

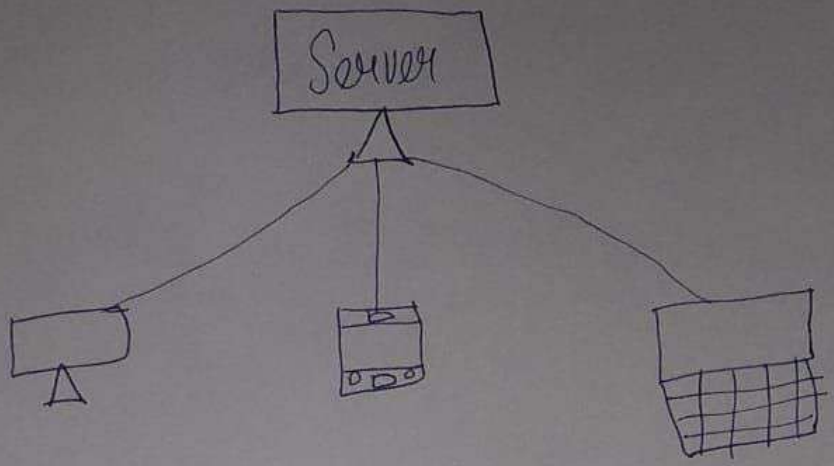
Disadvantages :-

(1) Security issues

(2) We can't backup the data because there is no server in this network.

2. Client server architecture :-

- Client server architecture also known as request response architecture.
- In this architecture client makes a request to the server, an server will fulfill the response.



Advantages :-

- It has a centralized system, from which data can be easily backed up.
- Security is better in this network.
- Entire system is maintained by the server.
- It has also increases the speed of resource sharing.

Disadvantages :-

- In case of server failure entire network will be failed.
- Server maintainance cost is high.

⇒ Network Structure :-

. It describes how the data on the network is organized and viewed.

1. Broadcast Network

. The communication channel that is shared by all the machines on the network.

. The message which consists of packets sent by any machine

are recieved by all other.
- The address field within the packet specifies the intended packet means where the packet is to be recieved.
- After recieving a packet, a machine checks the address field.

2. Multicast :-

- Basically concept of multicast evolves from the concept of broadcast.
- Some broadcast system supports transmission to a subset of mechanism which is known as multicasting.
- In the addressing one bit is reserved for multicasting.

3. Point to Point network :-

- It consist of many connections between individual pair of machines.
- To go from the source to destination, a packet on this type of network may have to visit one or more intermediate mechanism.
- Point to point transmission with one sender and one receiver is sometime called unicast.

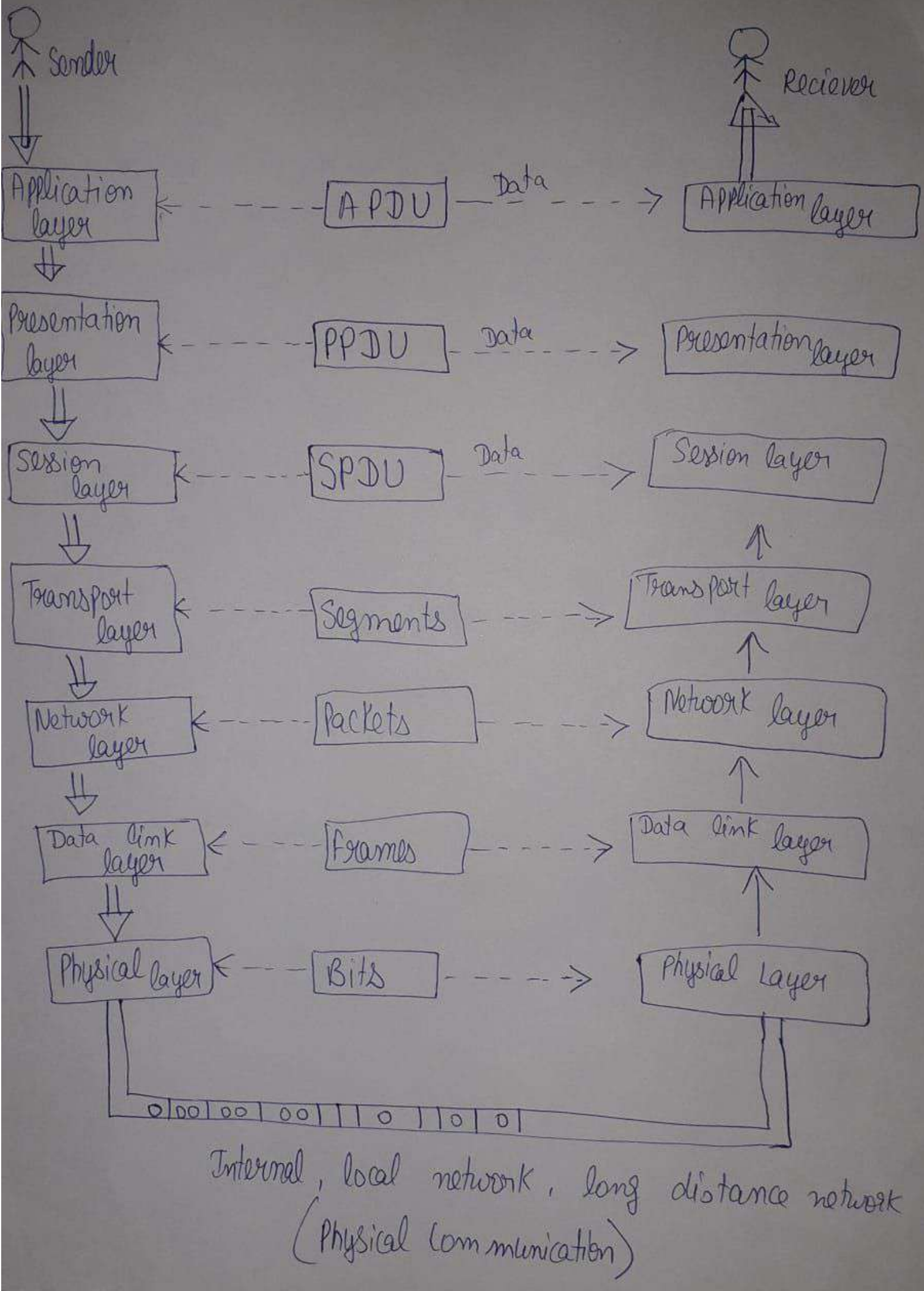
Chapter - 2

⇒ OSI Model :-

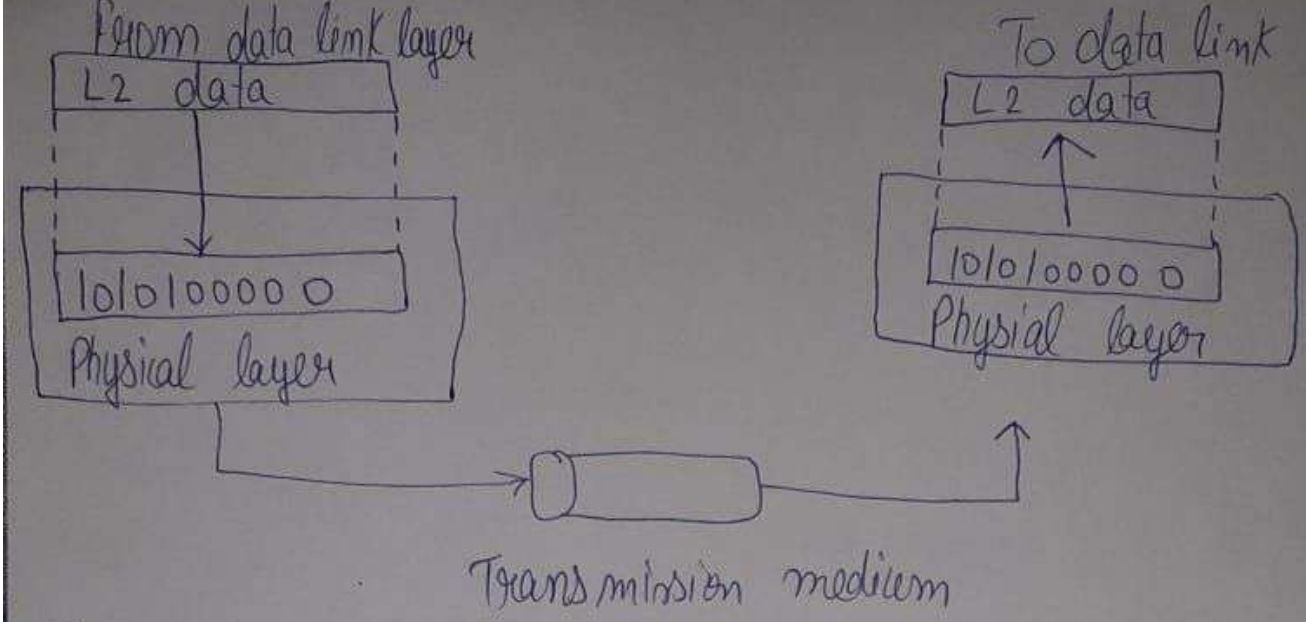
OSI stands for open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.

- OSI consists of seven layers, and each layer perform a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned to a particular task.
- Each layer is self contained, so that task assigned to each layer can be performed independently.
- OSI model 7 layers work collaboratively to transmit the data from one person to another across the globe..

OSI model layer diagram :-


Sender
Reciever
Application layer
APDU
Data
Application layer
Presentation layer
PPDU
Data
Presentation layer
Session layer
SPDU
Data
Session layer
Transport layer
Segments
Transport layer
Network layer
Packets
Network layer
Data Link layer
Frames
Data Link layer
Physical layer
Bits
Physical Layer
Internal, local network, long distance network
(Physical communication)

1 Physical layer :-



- The main function of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It established, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

Functions of physical layer :->

1. Line Configuration ->

- It defines the way how two or more devices can be connected physically.

2. Data transmission ->

- It defines the transmission mode whether it is simplex, half-duplex or full duplex mode between the two devices on the network.

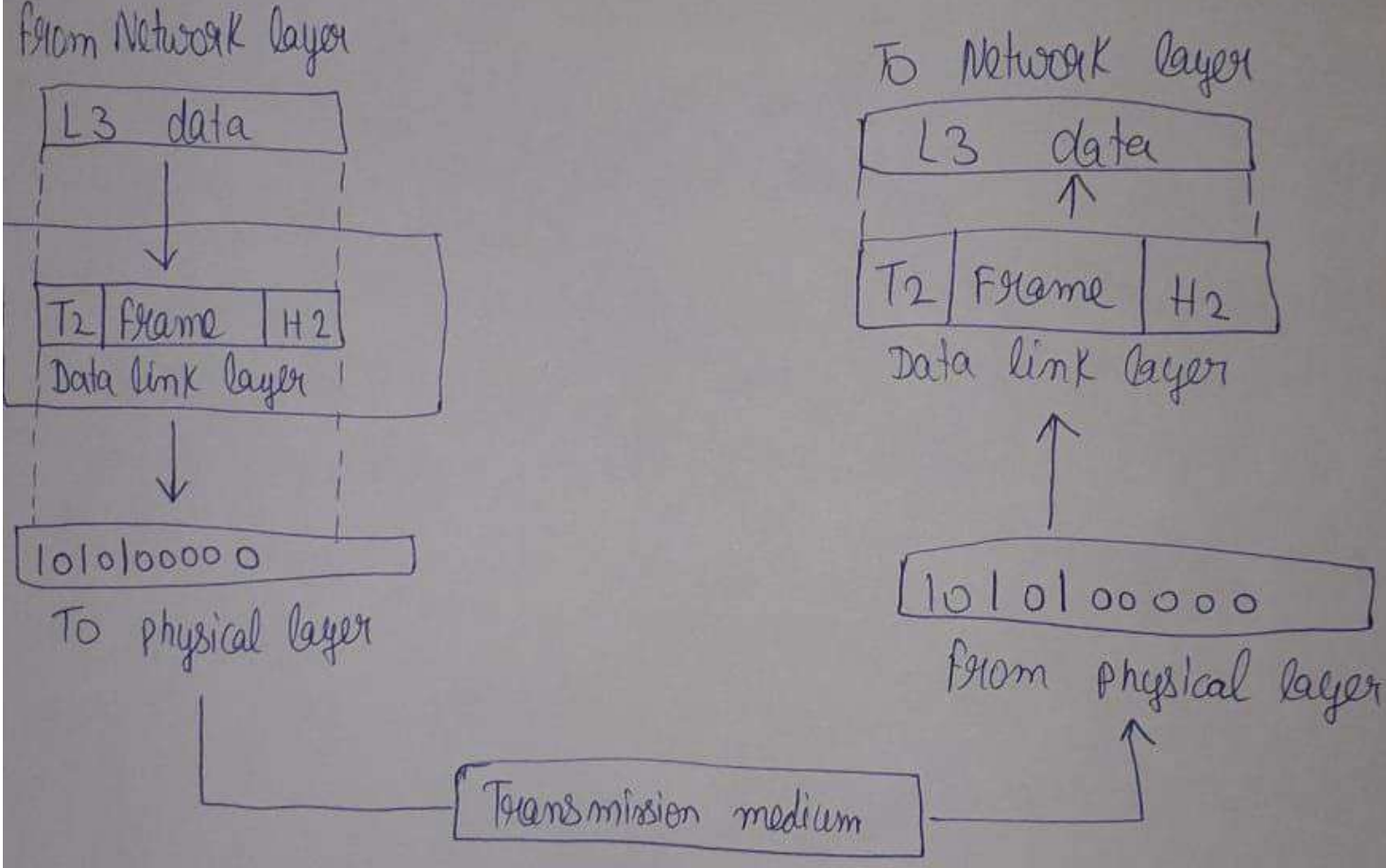
Topology →

It defines the way how network devices are arranged.

Signals →

It determines that type of the signal used for transmitting the formation.

Data link layer :-



This layer is responsible for the error-free transfer of data frames.

It defines the format of the data on the network.

It provides a reliable and efficient communication between two or more devices.

It is mainly responsible for the unique identification of each

Contains two sub layers :

Logical link control layer →

- is responsible for transferring the packets to the network layer the reciever that is recieving.

t identifies the address of the network layer protocol from the ader.

It provides flow control.

Media access control layer :→

A media access control layer is a link between the logical link ntrol layer and the networks physical layer.

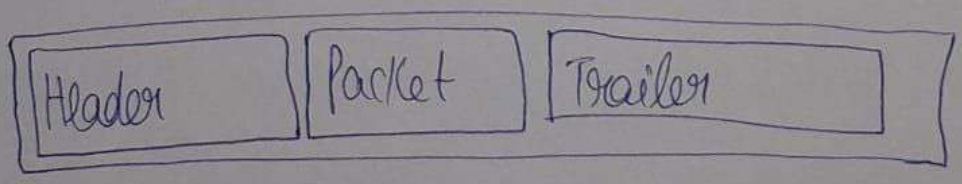
It is used for transferring the packets over the network.

unctions :-

> Framing →

The data link layer translates the physical's raw bit stream into packets known as frames.

The data link layer adds the header and trailer to the frame.

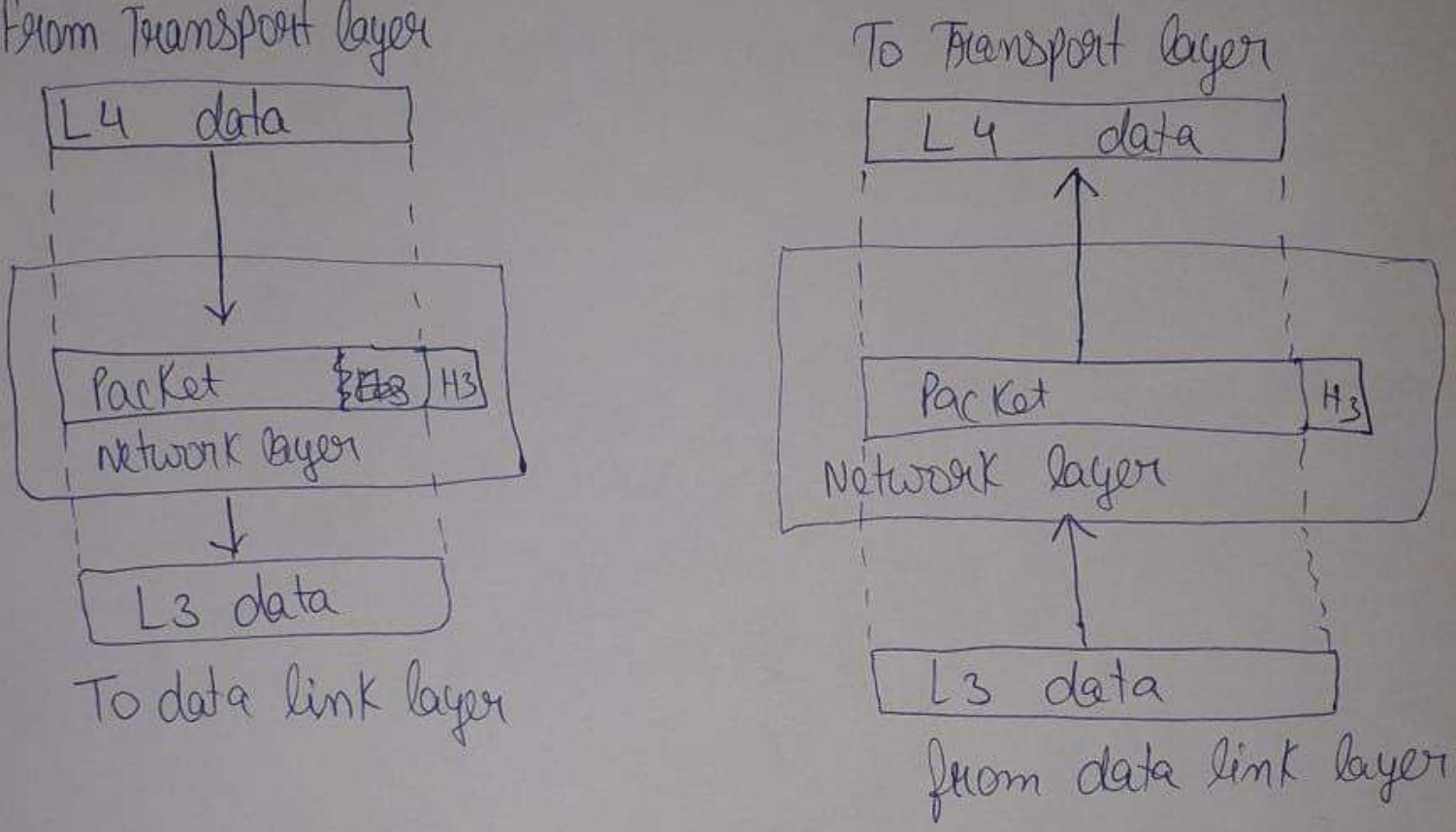


2> Physical Addressing :- The data link layer adds a header to the frame that contains a destination

address.

- The frame is transmitted to the destination address mentioned in the header.

3. Network layer :-



- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service and other factors.
- Data link layer is responsible for routing and forwarding the packets.
- Routers are the layers 3 device, they are specified in this

layer and used to provide the routing services within a internetwork.

- The protocols used to route the network traffic are known as network layer protocols.

Example of protocols are IP and IP v6.

⇒ Functions of network layer :

1. Internetworking :-

An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.

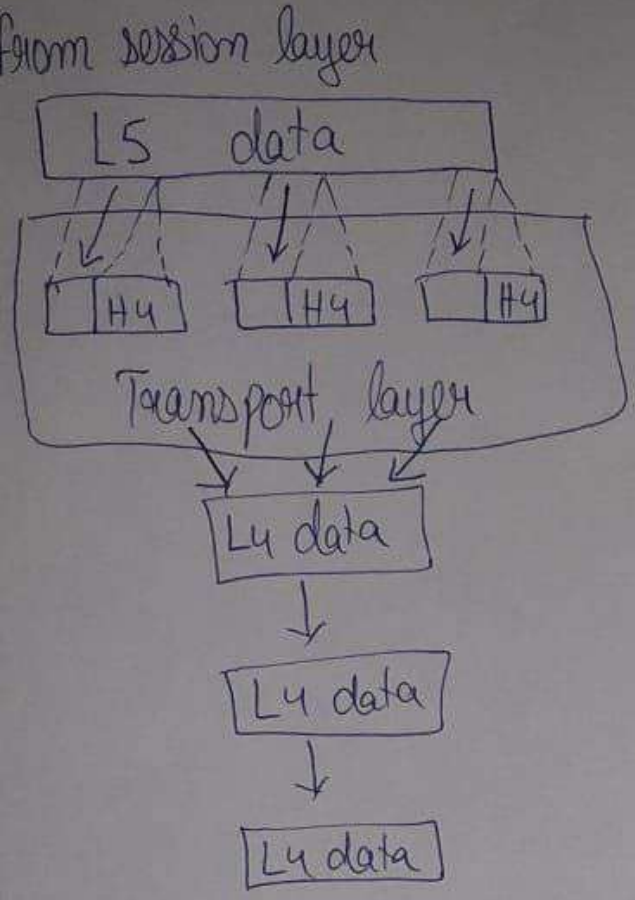
2. Addressing :-

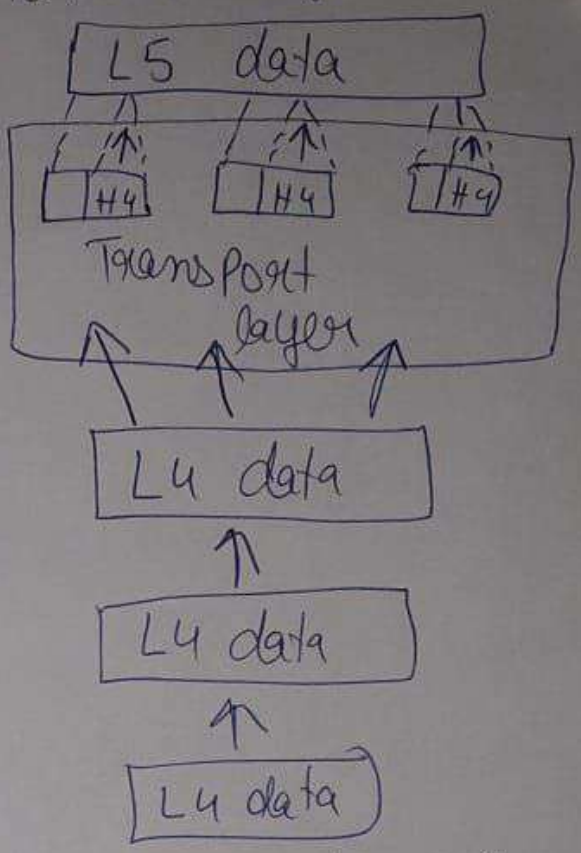
A network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.

3. Routing :-

Routing is the major component of the network layer and it determines the best optimal path out of the multiple path from source to destination.

4. Transport layer :-





- The transport layer is a layer 4 ensure that messages are transmitted in the order in which they are send and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It recieves the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end to end layer as it provides a point to point connection between source and destination to deliver the data reliably.

Functions

1. Segmentation and reassembly :-

When the transport layer recieves the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segments.

2. Connection Control :

Transport layer provides two services connection oriented services and connectionless service.

- A connectionless service treats each segments as an individual packet and they all travel in different routes to reach the destination.

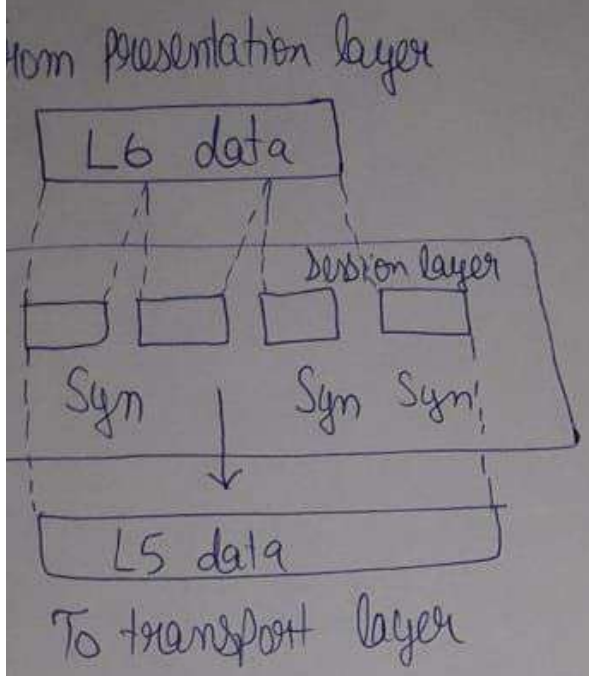
3. Flow Control :-

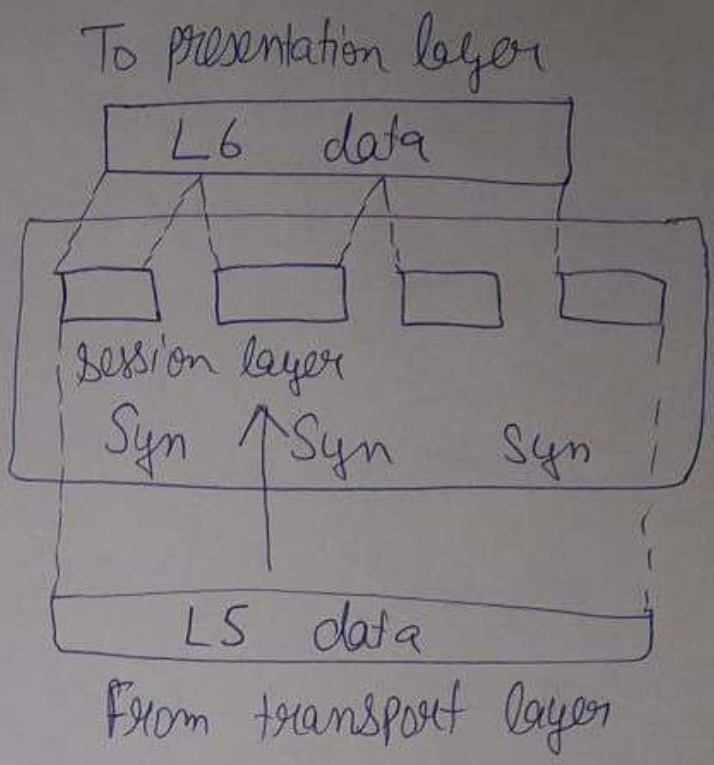
- The transport layer also responsible for flow control but it is performed end to end rather than across a single link.

4. Error Control :-

- The transport layer is also responsible for error control.
- Error control is ~~resp~~ performed end to end rather than across the single link.
- The sender transport layer ensure that message reach at the destination without any error.

Session layer :-





It is a layer 3 in the OSI model

The session layer is used to establish, maintain and synchronizes the interaction between community devices.

This layer is responsible for the establishment of connection, maintenance of sessions, authentication and is also ensures security.

Functions of session layer :

- Session establishment, maintenance and termination :-

This layer allows the two processes to establish, use the terminate a connection.

- Dialog control :

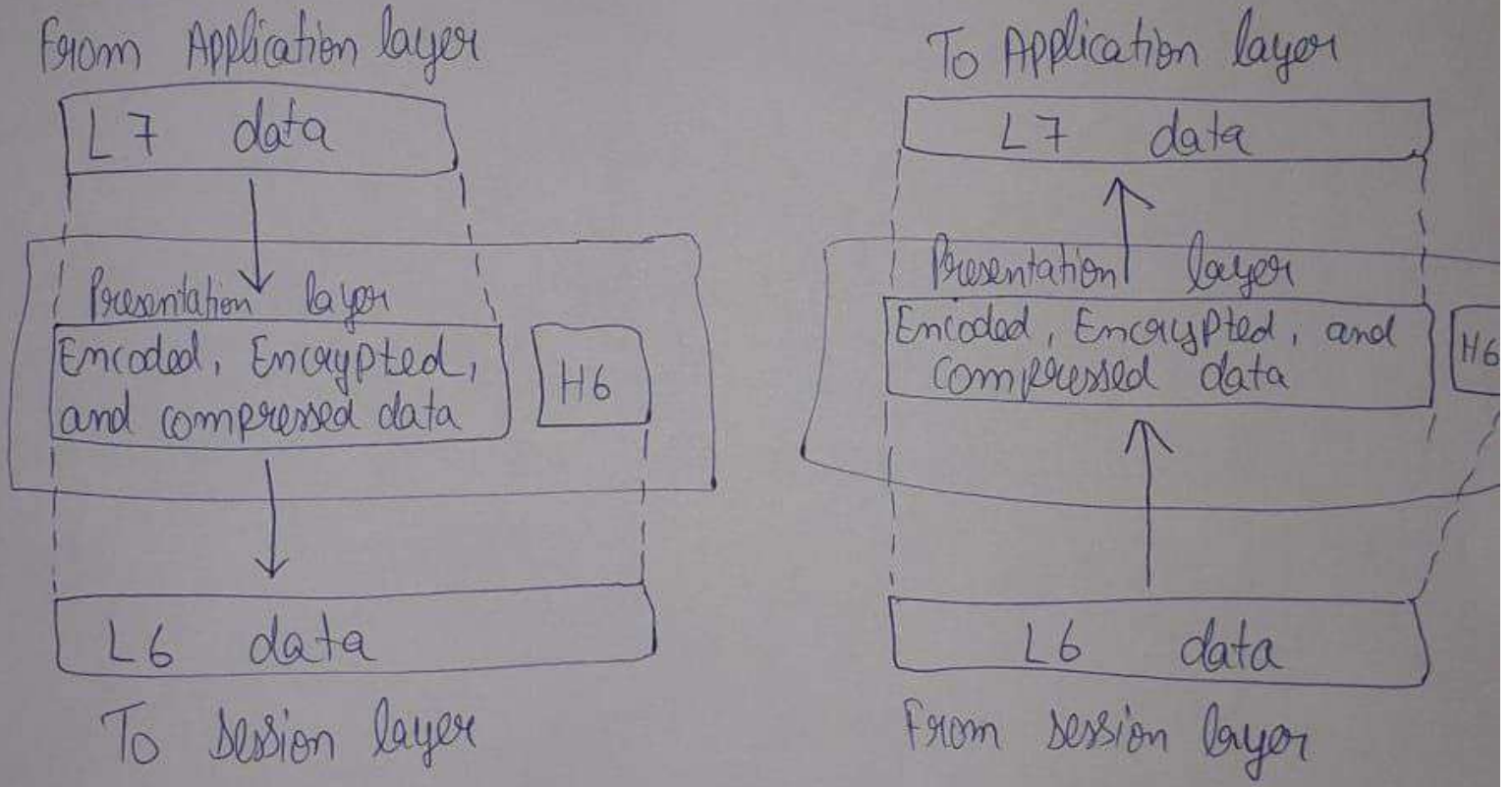
Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows

the communication between two processes which can be either half-duplex or full-duplex.

3. Synchronization :-

- Session layer adds some check points when transmitting the data in sequence if some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as synchronization and recovery

6. Presentation layer :-



- A presentation layer is mainly concerned with the syntax and semantics of the information exchange between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that convert

the data from one presentation format to another format.
- The presentation layer is also known as the Syntax layer.

Functions :-

1. Translating :-

- The processes in two systems exchange the information in the form of character string, number and so on.
- It converts the data from sender dependent format into a common format and changes the common format into receiver dependent format at the receiving end.

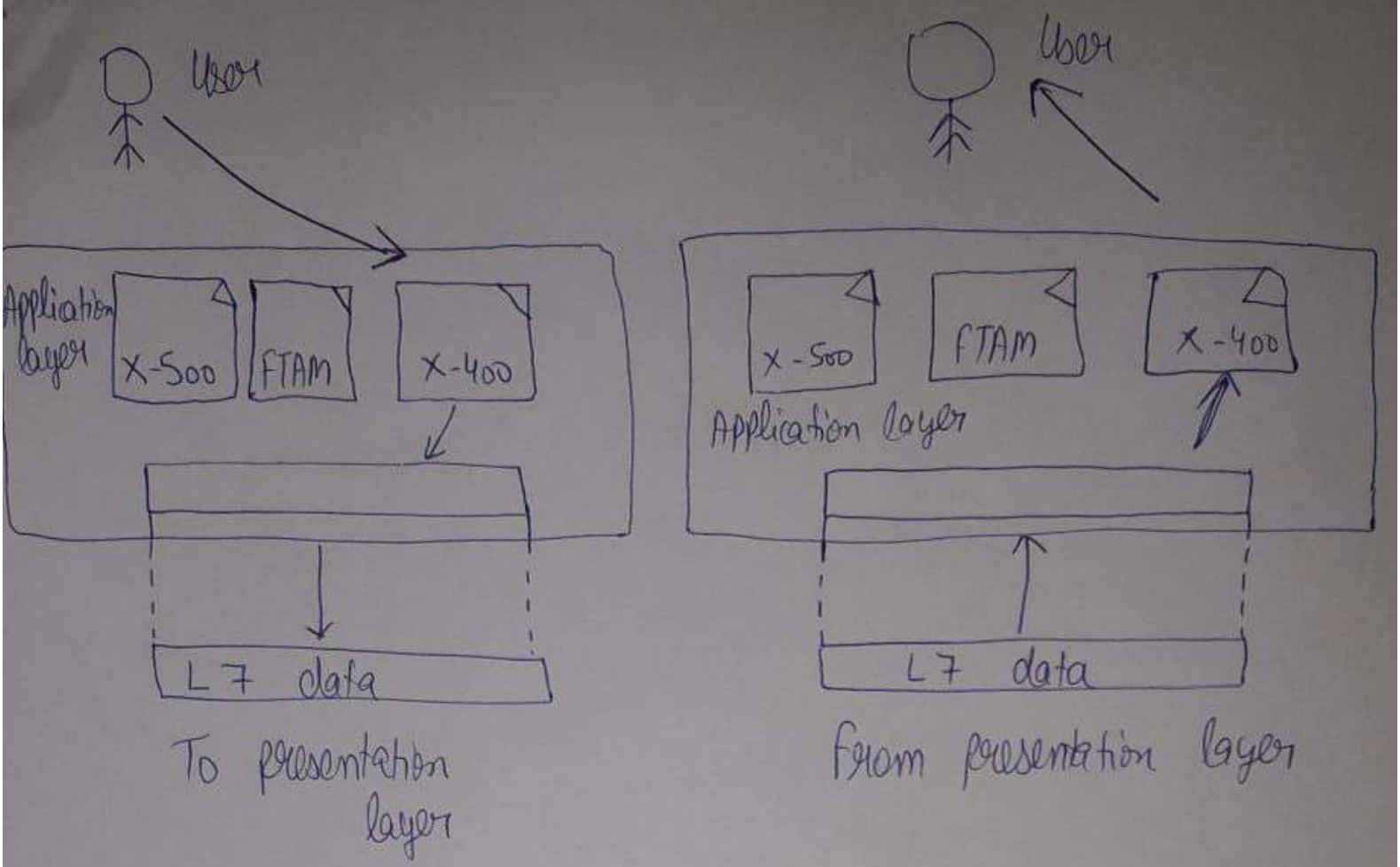
2. Encryption :-

- Encryption is needed to maintain privacy. Encryption is a process of converting the sender - transmitted information into another form and sends the resulting message over the networ

3. Compression :-

- Data compression is a process of compressing the data, such that it reduce the no. of bits to be transmitted.
- Data compression is very important in multimedia such as text, audio, video.

7. Application layer :-



- An application layer serves as a window for users and application process to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application layer is not an application but it performs the application layer function.
- This layer provides the network services to the end users.

Function :-

① File transfer, access and management (FTAM) :-

- An application layer allows a user to access the files in a remote computer to retrive the file from a computer

and to manage the files in a remote computer.

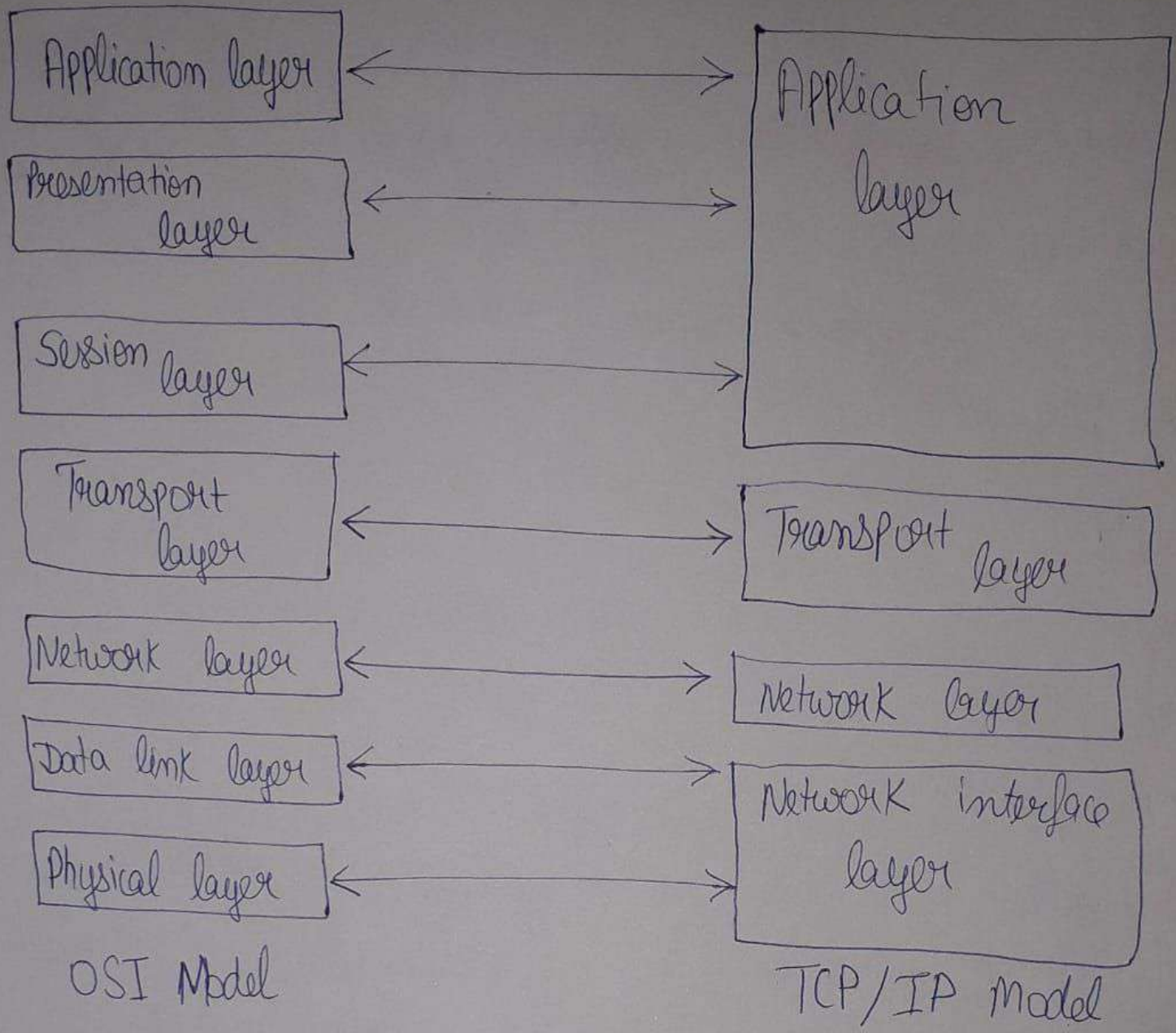
2. Mail services :-

- An application layer provides the facility for email forwarding and storage.

3. Directory Services :-

- An application layer provides the distributed database sources and is used to provide that global information about various objects.

Chapter - TCP/IP Protocol



- TCP/IP stands for transmission control Protocol / Internet Protocol and is a suite of communication protocols used to interconnect network devices on the internet.
- TCP/IP is also used as a communication protocol in a private computer network (an internet and extranet).
- TCP/IP specifies how data is exchanged over the internet by providing end to end communications that identify how

it should be broken into packets, addressed, transmitted routed and received at the destination.

⇒ Common TCP/IP protocols include the following:

1) Hyper text Transfer Protocol (HTTP) ⇒

- It handles the communication between a web server and a web browser.

2) HTTP Secure :⇒

- Handles secure communication between a web server and a web browser.

3) File Transfer Protocol ⇒

- It handles transmission of files between computers.
- The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

1) Application layer / Process &

2) Transport layer / Host to Host

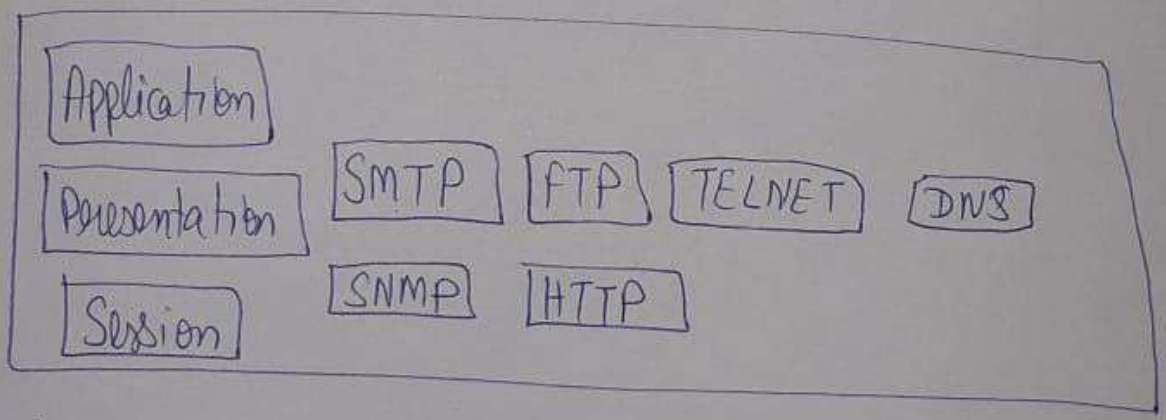
3) Internet layer / Network layer

4) Network layer / link layer

Application layer ⇒

- An application layer is the topmost layer in the TCP/IP model. It is responsible for handling high level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- Example of the application layer is an application such as file transfer, email, remote login etc.

Function and protocols of Application layer ⇒



- HTTP ⇒
- This protocol allows us to access the data over the world wide web.
- It transfer the data in the form of plain, text, audio, video.
- It is known as hypertext transfer protocol as it has

the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.

- SNMP ⇒

- SNMP stands for simple network management protocol.
- It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.

- SMTP ⇒

- SMTP stands for simple mail transfer protocol.
- The TCP/IP protocol that support the email is known as a simple mail transfer protocol.
- This protocol is used to send the data to another email address.

- DNS :-

- DNS stands for domain name system.
- An IP address is used to identify the connection of a host to the internet uniquely. But people prefer to use the names instead of addresses.

- TELNET ⇒

- It stands for Terminal network or teletype network protocol.

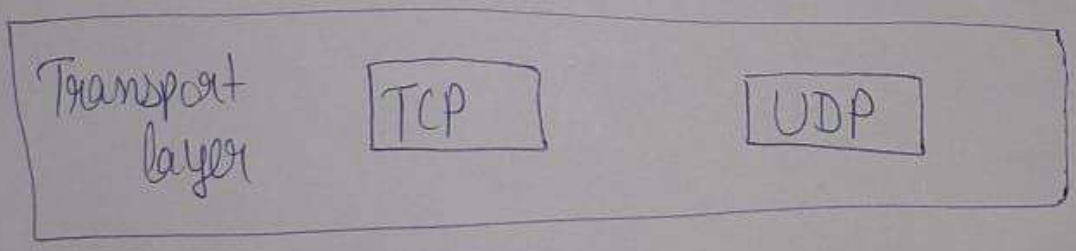
- It established the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.

- FTP :-

- FTP stands for file transfer Protocol.
- FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

2. Transport layer ⇒

- The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.



The two protocols used in the transport layer are user datagram protocol and transmission control protocol.

User datagram protocol (UDP) :-

- It provides connectionless service and end-to end delivery of transmission.
- It is an unreliable protocol as it discovers the error but

not specify the error.

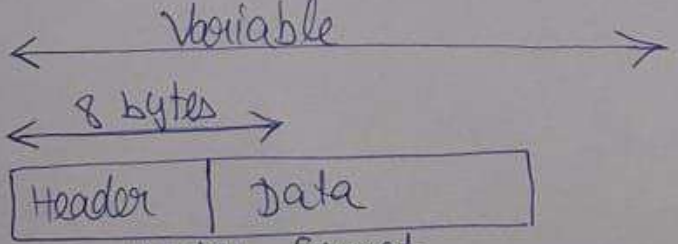
- User datagram protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged. ICMP (Internet control message protocol).

⇒ UDP consists of the following fields :

- Source port address ⇒ The source port address is the address of the application program that has created the message.
- Destination port address ⇒
- The destination port address is the address of the application program that recieves the message.

Total length ⇒ It defines the total no. of bytes of the user datagram in bytes.

Check sum ⇒ The check sum is a 16 bit field used in error detection.



Header Format

Source port address 16 bit	Destination Port address 16 bit
Total length 16 bits	Checksum 16 bits

Transmission control protocol (TCP) ⇒

- It provides a full transport layer services to applications.
- It creates a virtual circuit between the sender and reciever and it is active for the duration of the transmission.
- TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be recieved and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
- At the sending end, TCP divides the whole message into smaller units knowns as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
- At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

3. Internet layer ⇒

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Internet layer — ICMP | IGMP | IP | ARP | RARP

IP- Internet protocol
ARP- Address Resolution Protocol
ICMP → Internet Control message protocol
IGMP → Internet Group management protocol
RARP → Reverse Address resolution protocol

Following are the protocols used in this layer are : ⇒

1) IP Protocol ⇒

IP protocol is used in this layer, and it is the most significant part of the entire TCP / IP suite.

Responsibilities of this protocol :-

- IP addressing ⇒ This protocol implements logical host address known as IP address.

- Host to Host communication ⇒ It determines the path through which the data is to be transmitted.

- Data encapsulation and formatting ⇒ An IP protocol accepts the data from the transport layer protocol. An IP Protocol ensures that the data is sent and recieved securely. It encapsulates the data into messages known as IP datagram.

- ARP protocol ⇒

ARP stands for address resolution protocol.
ARP is a network layer protocol which is used to find the physical address from the IP address.

The two terms are mainly associated with the ARP protocols:

- ARP request ⇒

When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.

- ARP reply ⇒

Every device attached to the network will accept the ARP request and process the request but only recipient recognize the IP address and send back its physical address in the form of ARP reply.

The recipient adds the physical address both to its cache memory and to the datagram header.

3. ICMP protocol ⇒

- ICMP stands for internet control message protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router to router unit it reaches its destination.

An ICMP protocol mainly uses two terms:

ICMP test ⇒ ICMP test is used to test whether the destination is reachable or not.

ICMP reply ⇒ ICMP reply is used to check whether the destination device is responding or not.

The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.

1. Network interface (Access) layer :-

A Network layer is the lowest layer of the TCP/IP model.

A network layer is the combination of the physical layer and data link layer defined in the OSI reference model.

It defines how the data should be sent physically through the network.

This layer is mainly responsible for the transmission of the data between the devices on the same network.

The function carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP address into physical address.

The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

⇒ Difference between OSI and TCP/IP model :-

OSI model	TCP/IP model
1. OSI stands for open system Interconnection	1. TCP/IP implies Transmission Control Protocol / Internet protocol.
2. The OSI model was developed by ISO (International Standard organization) in 1984.	2. The TCP/IP model was developed by ARPANET (Advanced Research project agency network) in 1982
3. It consists of 7 layers : Starting from the bottom they are the physical, data link, Network, Transport, session, presentation and application layer.	3. It consists of 4 layers : Starting from the bottom they are the network interface, internet, transport and application layer.
4. The OSI model follows a vertical Approach.	4. The TCP/IP model follows a horizontal approach.
5. In the OSI model, the transport layer provides a guarantee for the delivery of the packets.	5. In TCP/IP transport layer does not provide the surety for the delivery of packets. But still, we can say that it is a reliable model.

Chapter - 5

Network layer

Network layer is the third layer of OSI model.
It is the lowest layer which deals with end to end transmission
It provides services to the transport layer.
This layer has a higher responsibility than data link layer because the data link layer is only supported to move the frame from one end to other.

⇒ **Network layer design issues :-**

The various issues for the network layer design are:
Services provided to the transport layer.
The services provided should be independent of the underlying technology.

With these goals is mind two different types of services emerged.
1. Connection oriented network services
2. Connectionless network services

Connection oriented services is one in which user is given a reliable end to end connection.

To communicate, the user requests a connection, then uses the connection to their contents and then closes the connection.
A telephone line is best example of connection oriented net.

2. In connectionless, the user simply bundles his information together, put an address on it and then send it off, in the hope that it will reach its destination.

- In this connection there is not guarantor that the message has been reached successfully.
- The best example is a letter sent through the post-office.

⇒ Services provided to the transport layer :-

- The service should be independent of the subnet Technology.
- Transport layer should be shielded from the number, type and topology of the subnet.
- The network service can be connectionless or connection oriented.
- The internet has connectionless network layer whereas ATM has connection oriented services.

⇒ Internal organisation of the network layer :-

1. To use connection oriented services.
2. To use connectionless services

- In the connection oriented service, a connection is called virtual circuit. It is similar to physical connection.
- In the connectionless organization, the independent packets are called as datagram.

1. Virtual circuit :-

- The principal behind the virtual circuit is to choose only one route from source to destination.
- When a connection is established, it is used for all traffic flowing over the connection.
- When the connection is released, the virtual circuit is terminated.

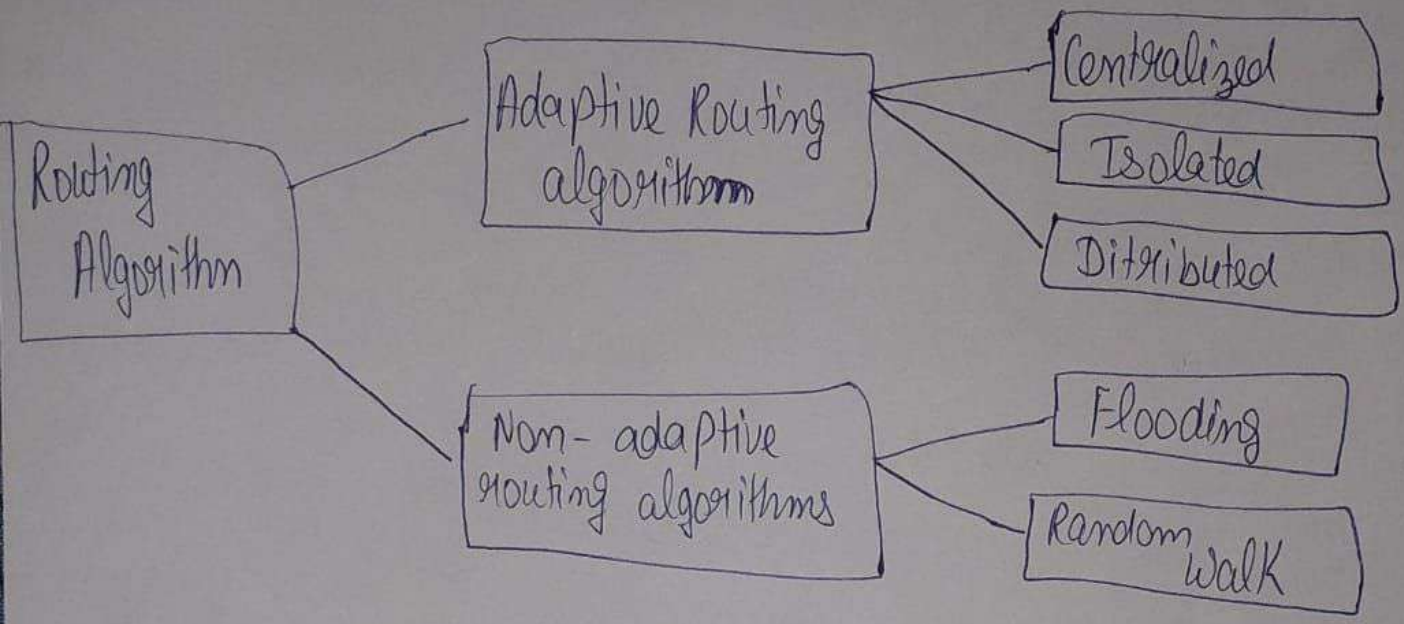
2. Datagram :-

- With a datagram, the routes from source to destination are not worked out in advance.
- Each packet sent is routed independently.
- Successive packet can follow different routes.
- The datagram subnet have to do more work but they are more robust and deals with failure and congestion more easily as compared to virtual circuit.

⇒ Routing Algorithm :-

- A routing algorithm is a procedure that lays down the route or path to transfer data packet from source to the destination.
- In order to transfer the packet from source to the destination, the network layer must determine the best route through which packets can be transmitted.
- The routing protocol is a routing algorithm that provides the best path from the source to the destination. The best path is the path that has the least cost path from source to destination.

- Routing is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm.



1. Adaptive Routing algorithm :-

- An adaptive routing algorithm is also known as dynamic routing algorithm.
- This algorithm makes the routing decision based on the topology and network traffic.
- The main parameters related to this algorithm are hop count, distance and estimated transit time.

The three popular types of adaptive routing algorithms are -

(i) Centralized algorithm :-

- It finds the least cost path between source and destination node by using global knowledge about the network. So it is also known as global routing algorithm.

i) Isolated algorithm :-

This algorithm procures the routing information by using local information instead of gathering information from other nodes.

ii) Distributed algorithm :-

- It is also known as decentralized algorithm as it computes the least cost path between source and destination in an iterative and distributed manner.

2. Non adaptive algorithm :-

- Non adaptive routing algorithm is also known as a static routing algorithm.
- When booting up the network, the routing information stores to the routers.
- Non-adaptive routing algorithm do not take the routing decisions based on the network topology or network traffic.

The two types of non-adaptive routing algorithms are -

1) Flooding :-

- In flooding when a data packet arrives at a router, it is sent to all the outgoing links except the one it has arrived on. Flooding may be uncontrolled controlled or selective flooding.

2) Random Walk :- This is a probabilistic algorithm where

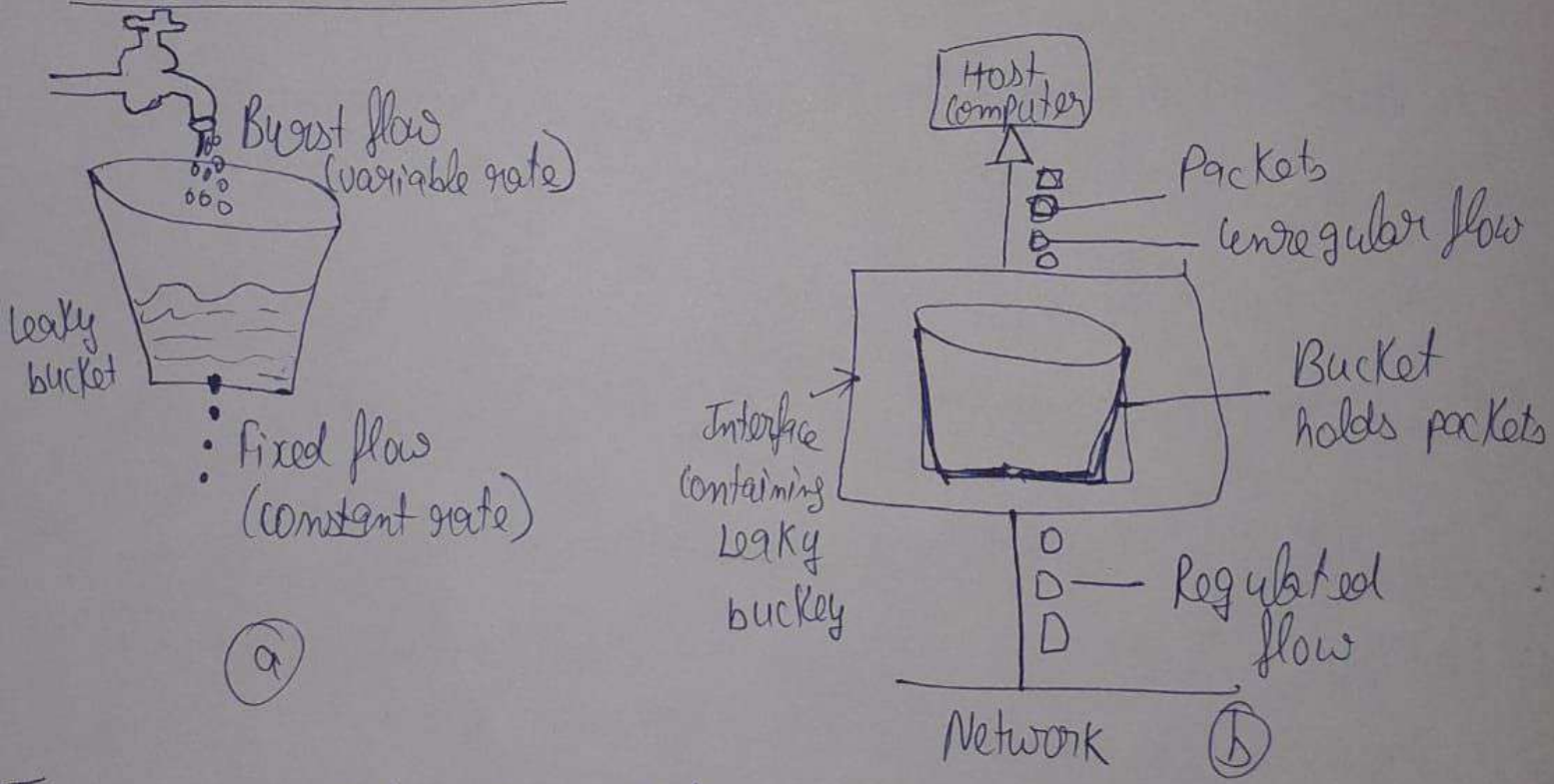
data packet is sent by the router to any one of its neighbours randomly.

⇒ Congestion Control Algorithm :-

Congestion is a network may occur if the load on the network is greater that capacity of network.

Congestion control refers to the mechanism & techniques that can either prevent congestion before it happens or remove congestion after it happened.

1. Leaky bucket Algorithm :-



Imagine a bucket with a hole at the bottom. ~~water~~ Water data packets enters the bucket at any rate but leaks out at a constant rate.

If more water enters than the bucket can hold the excess

overflows (packets are discarded).

The leaky bucket algorithm is a traffic shaping mechanism that controls the rate at which data packets are transmitted over a network.

- It smooths out bursty traffic by converting variable rate incoming traffic into a constant rate output.

Key features

- Rate control: Ensures data is transmitted at a fixed rate, regardless of how it arrives.
- Traffic smoothing: Prevents network congestion by averaging out bursts in data traffic.
- FIFO Queue: Uses a first in, first out structure to manage incoming packets.
- Packet Dropping: If the queue is full new incoming packets are discarded.

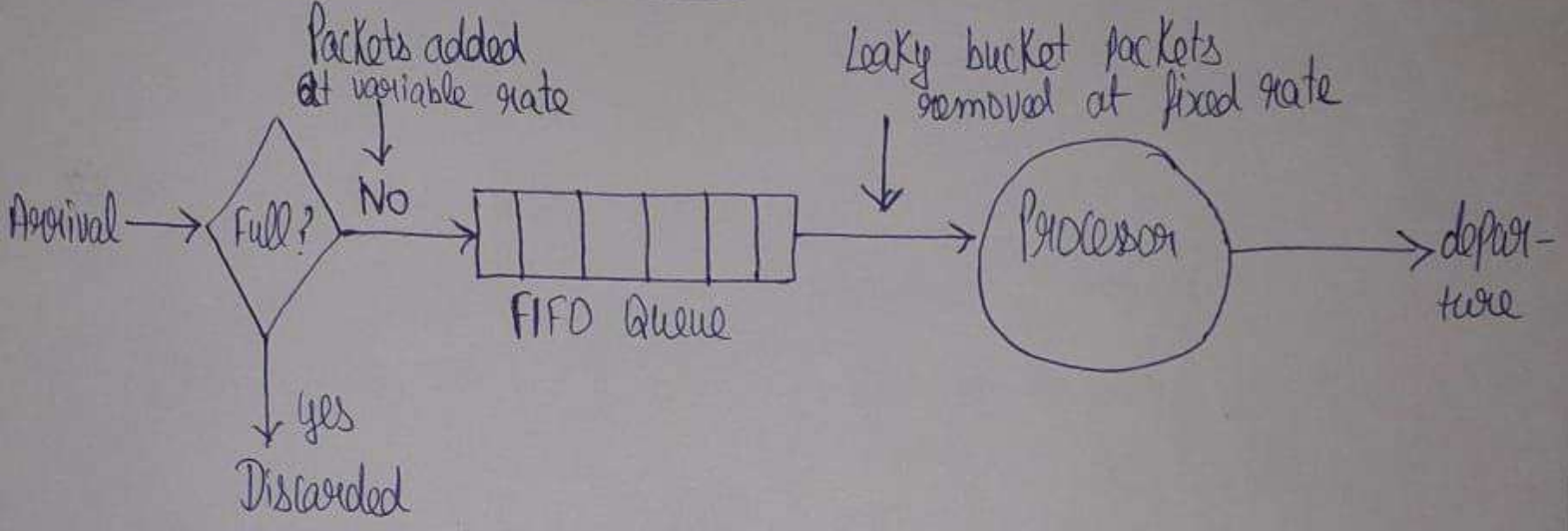
1. Figure (a)

- Shows a physical leaky bucket filled with water.
- Water leaks out at a fixed rate, regardless of the inflow rate.
- If too much water is added too quickly, it overflows (data packets are lost).

2. Figure (b):-

Represents a network version of the leaky bucket.
Unregulated packet flow enters the bucket.
The bucket holds packets temporarily.
Regulated flow exits at a fixed rate into the network.

⇒ Implementation of leaky bucket :-



1. Queue based Approach :

- Each host is connected to the network through an interface containing a leaky bucket.
- A FIFO queue holds packets until transmission.

2. Working Mechanism :

- Packets arrive at variable rates and enter the queue.
- The queue releases packets at a constant rate.
- A clock tick determines when packets are sent
- If the queue overflows, packets are discarded.

3. Handling different packet sizes :-

The algorithm checks each packet's size.
If it fits within the allocated transmission rate, it is sent.
If it exceeds capacity, it is dropped.

2. Token bucket Algorithm :-

- The token bucket algorithm is a traffic shaping and rate-limiting mechanism used in computer networks to control data flow.
- It allows data packets to be transmitted at an average rate while permitting bursts of data when sufficient tokens have accumulated.

How the Token bucket algorithm works :-

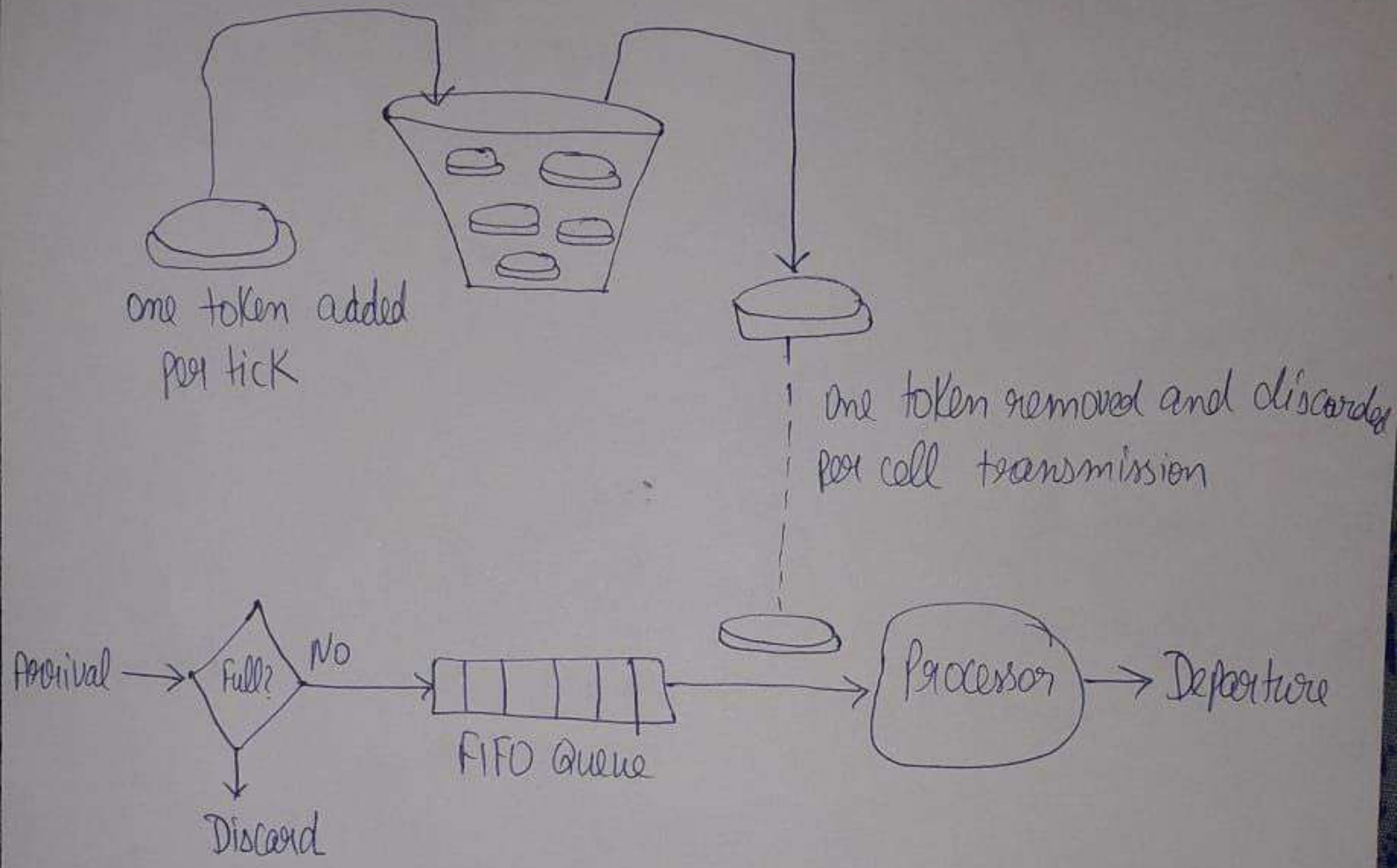
1. Token generation :-

- The system generates token at a constant rate (eg., 100 tokens per second).
- Each token represents permission to send a fixed amount of data (eg., 1 byte, 1 packet etc.)
- The bucket has a maximum capacity once full, extra tokens are discarded.

2. Data transmission :-

- When a packet arrives, the system checks if enough tokens are available.
- If enough tokens exists, the packet is sent immediately and the corresponding tokens are removed from the bucket.

- If there are not enough tokens, the packet must wait for new tokens to be generated.
- If tokens are available but the bucket is empty the packet is discarded



3. Handling burst traffic :-

- Unlike the leaky bucket, the token bucket accumulates unused tokens over time.
- If the system has been idle, it can send a large burst of data as soon as activity resumes, consuming all stored tokens at once.
- Once the bucket is empty, new packets must wait for tokens to be replenished.

Implementation :-

1. Components :

(i) Token bucket : A storage unit for tokens.
(ii) Tokens : Small units representing the right to send data.
(iii) Counter : A variable tracking the number of tokens.
(iv) FIFO Queue : Holds packets waiting for tokens.
(v) Processor : The system handling packet transmission.

2. Step by Step process :-

1. Initialize the counter to zero (indicating no tokens are available at the start).

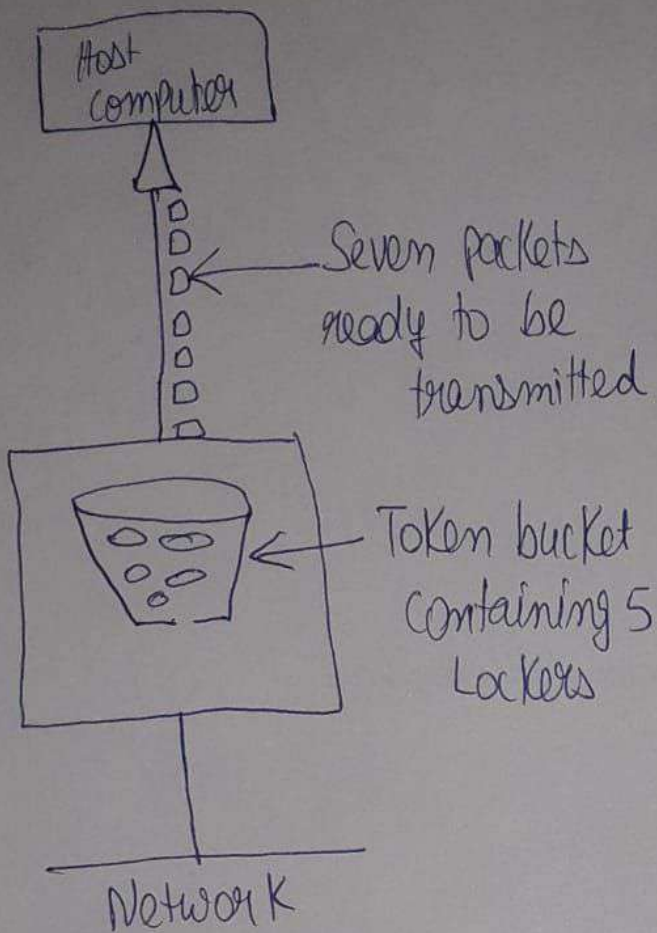
2. Generate tokens periodically and add them to the bucket (upto a maximum limit).

3. When a packet arrives, check the number of tokens:

- If tokens are available deduct the required number and send the packet.
- If no tokens are available, the packet waits in the FIFO queue.

4. If the bucket is empty, no packets the packet ~~waits in the FIFO queue~~ can be sent until new tokens are added.

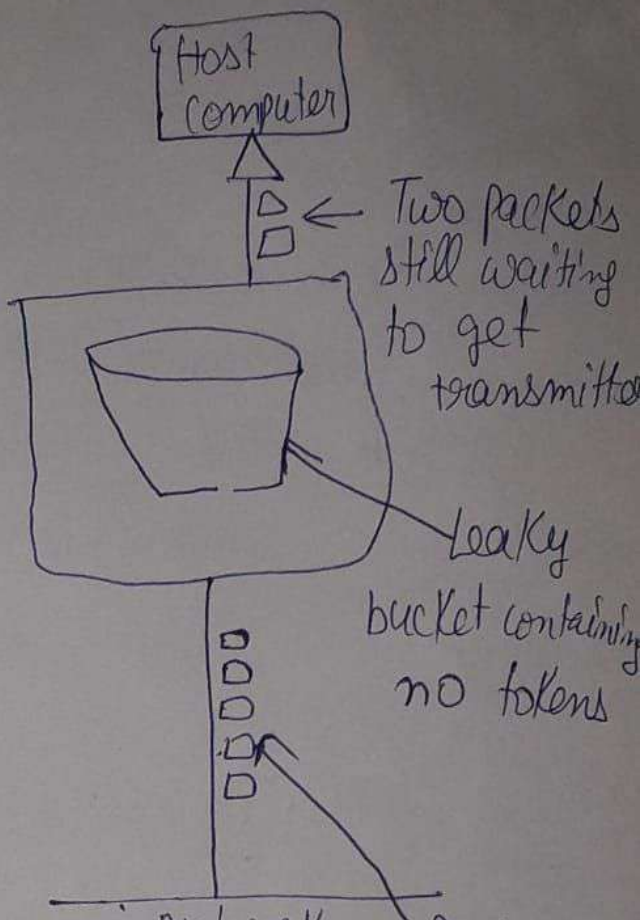
5. If tokens accumulate burst transmission is possible when needed.



(a)

Figure (a)

- Shows a token bucket with 5 tokens and 7 packets waiting. Only 5 packets can be transmitted, while 2 wait for more tokens



(b)

Figure (b)

- Shows a scenario where the bucket is empty, forcing packets to wait.

Chapter - 6
Transport layer

Transport layer :-

- Transport layer provides an end to end data transfer service that shields upper layer protocols.
- A transport layer / protocol can be either connection oriented, such as TCP, or connectionless, such as UDP.

Design issues :-

- Two basic types of transport services are possible : Connection oriented and connectionless or diagram service.
- A connection - oriented service provides for the establishment, maintenance and termination of logical connection between Transport service users.
- The connection - oriented service generally implies that the service is reliable.
- In Connectionless services the connections are not established in advance.
- All time they adopt the different route to reach at the distination.
- A network service that makes life easy for transport protocol

by guaranting the delivery of all transport data units in order and defining the required mechanisms.

⇒ Connection Management addressing :-

- Connection management refers to the process of establishing, maintaining and terminating connections between devices or systems in a network.
- It involves various protocols and techniques to ensure reliable and efficient communication between network entities.
- In transport layer end to end delivery can be done in either of two modes: Connection oriented and connectionless.
- The connection oriented modes is the more commonly used.
- A connection oriented protocol setup a virtual circuit or pathway between the sender and reciever.
- All of the packet belonging to a message are then sent over the same path.

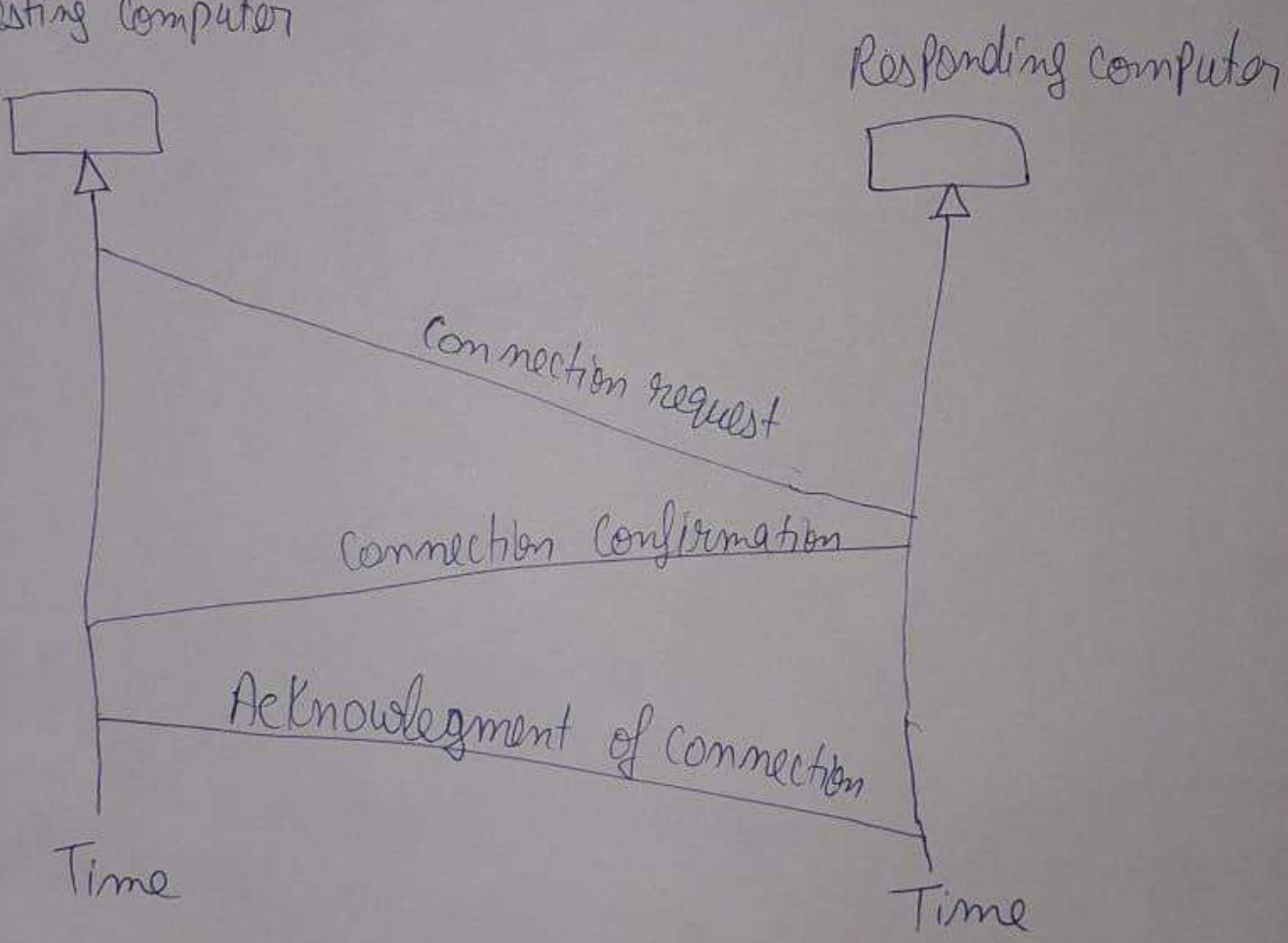
Connection - oriented transmission has three stages:

1. Connection Establishment
2. Data Transfer
3. Connection termination

1. Connection Establishment :-

- Before a communicating device can send data to the other, the initiating device must first determine the availability of the other to exchange data and pathway has to be found through the network by which the data can send. This is called connection Establishment.

- Connection establishment require three actions which is called a three way hand shake.



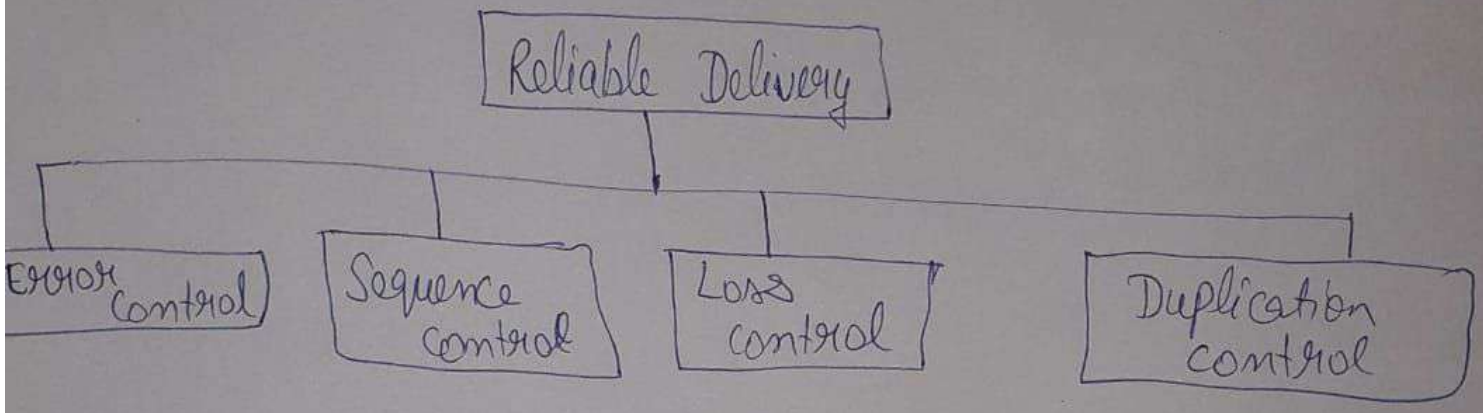
2. Data Transfer :-

- After the establishment of the connection between the system the data transferring starts b/w the systems.

· Connection Terminating / Realising :-

Once all of the data have been transferred, the connection has to be terminated.

i) The requesting computer sends disconnection request packet
ii) The responding computer confirms the disconnection request.
iii) The requesting computer acknowledges the confirmation.



⇒ Design issues of Transport layer :-

· Addressing ⇒

When a user wishes to set up a connection to a remote application process, it must specify which one to connect to.

The target user needs to be specified by all of the following:

- User identification
- Transport entity identification
- Host address Network Number.

The user address is specified as (Host, Port).

The Port variable represents particular TS users at the

specified host.

- In TCP, the combination of Port and Host is referred to as socket because routing is not concern with transport layer, it simply passes the Host portion of the address down to the network service.

- Port is included in a header, to be used at the destination by the destination transport protocol.

2. Segmentation and Reassembly =>

- In segmentation, a message is divided into transmitable segments, each segment containing a sequence number.
- This number enables this layer to reassemble the message.
- Upon arriving at its destination system message is reassembled correctly.

3. Connection control :-

- It can be of two types:

(i) Connectionless transport layer
(ii) Connection oriented layer

(i) Connectionless transport layer :-

This transport layer treats each packet individually and delivers

it to the destination machine.

- In this type of transmission, the reciever does not send an acknowledgment to the sender about the reciept of the packet.
- This is a faster communication techniques.

2. Connection Oriented transport layer :

- Here, a connection with the destination machine is created before transmitting the packets to the destination.

⇒ Transport layer protocol

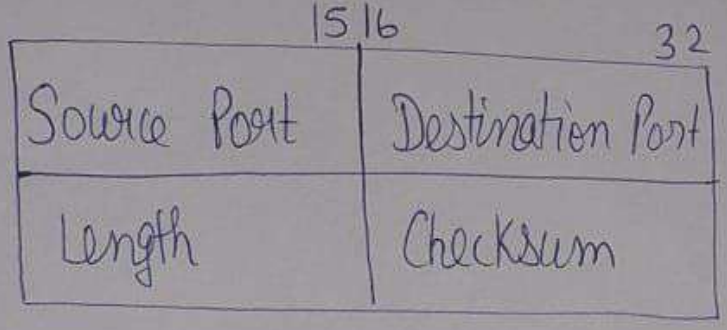
① UDP :-

- User datagram protocol is called a connectionless, unreliable protocol.
- It has very limited error checking capability.
- It is a very simple protocol and it can be used with minimum overhead.
- UDP can be used when process needs to send a small message without any issue of reliability.
- UDP takes less time as compared to TCP (transmission Protocol) or SCTP (Stream control protocol).

- It is a good protocol for data flowing in one direction
- It is simple and suitable for query based communication.

User datagram Header

- UDP packets are called as user datagrams, which contain the fixed size header of 8-bytes.
- UDP header contains four main parameters.



⇒ Source port :-

- This 16-bit information is used to identify the source port of the packet.

⇒ Destination port :-

- This 16 bit information is used to identify the application level service on destination machine.

⇒ Length :-

- Length field specifies the entire length of UDP packet (including header). It is a 16 bit field & min value is 8 byte i.e the size of UDP header itself.

⇒ Checksum :-

This field stores the checksum value generated by the sender before sending.

IPv4 has this field as optional. So when checksum field does not contain any value it is made 0 & all its bits are set to zero.

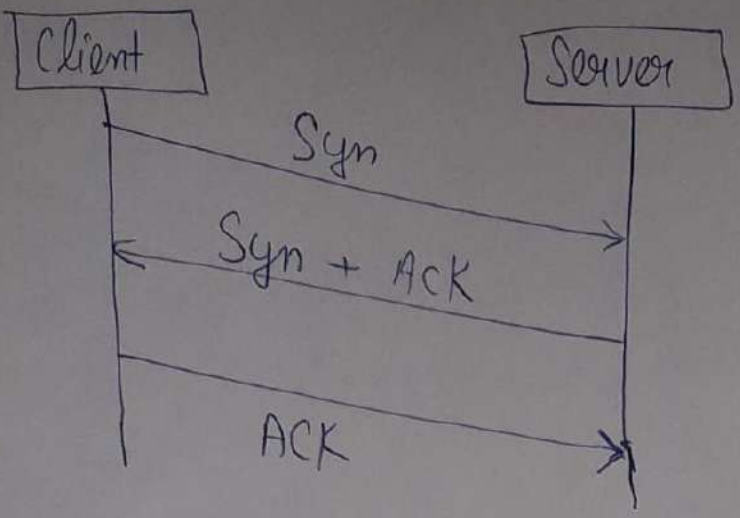
2. TCP (Transmission control protocol) :-

- TCP is connection oriented protocol.
- It uses flow & error control mechanism at transport layer, hence it is reliable transport protocol.
- TCP ensures that the data reaches intended destination in the same order it was sent.
- In TCP, a segment carries a data and control information.

⇒ Connection Establishment :-

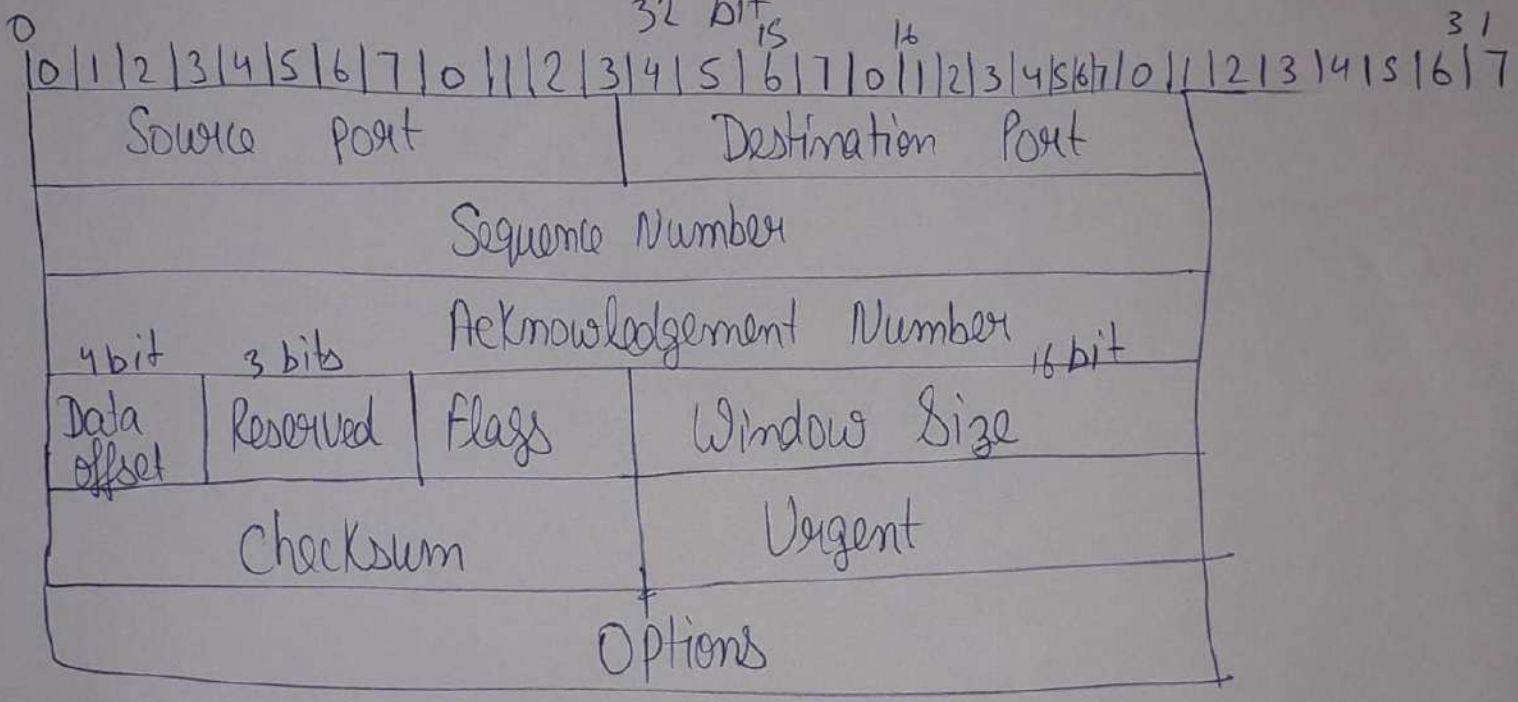
: TCP transmits data in both direction (full duplex mode).

- When two TCP's are connected to each other, each TCP is to initialize the communication (SYN) and approval (ACK) from each end to send the data.
- Three way hand shaking protocol is used to established connection b/w two TCP's.



Header

The length of TCP header is min 20 bytes long & max 60 bytes.



Chapter - 7
Application layer

⇒ Application layer

- Application layer is the TOP most layer of the OST and TCP/IO reference model.
- It allows the people to use the internet.
- It provides the services to the user directly.
- It recieves the services from the transport layer.
- In the Application layer we need the protocol to allow the real applications to functions these are

1. Network security
2. DNS
3. Network arrangement

⇒ DNS (Domain name system) :-

- DNS stands for domain name system. It is an automatic process that converts the domain name to its corresponding ip address (number).
- So, that web browser can understand which web page you want to access on the internet.

A domain name is user own personal internet address with his own domain name lits project a corporate identify.

- For the communication to take place successfully, the sender and reciever both should have address and they should known be to each other.

For example

An email address is like

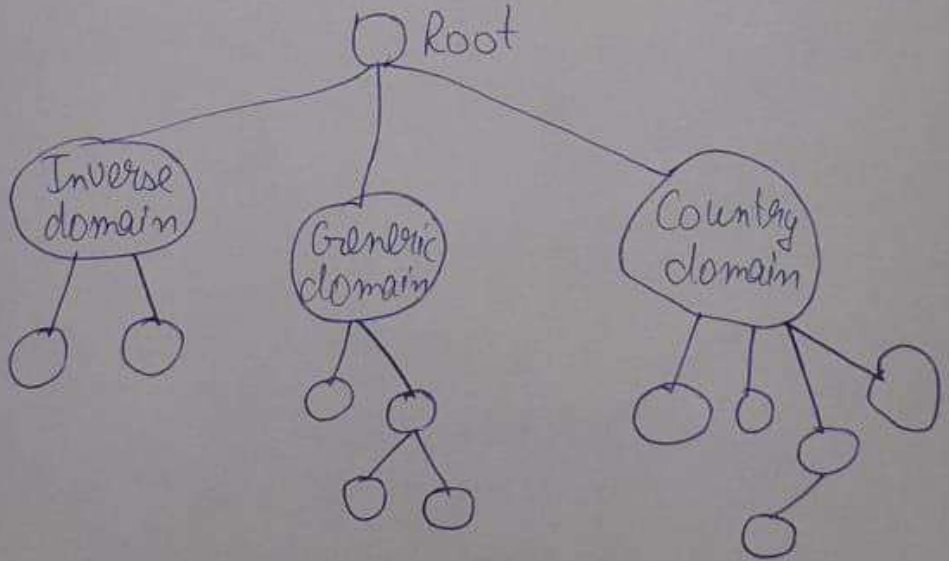
(balsimar @ rediffmail com)

Where as the address to access the web page is like

(Http: // www.google.com./)

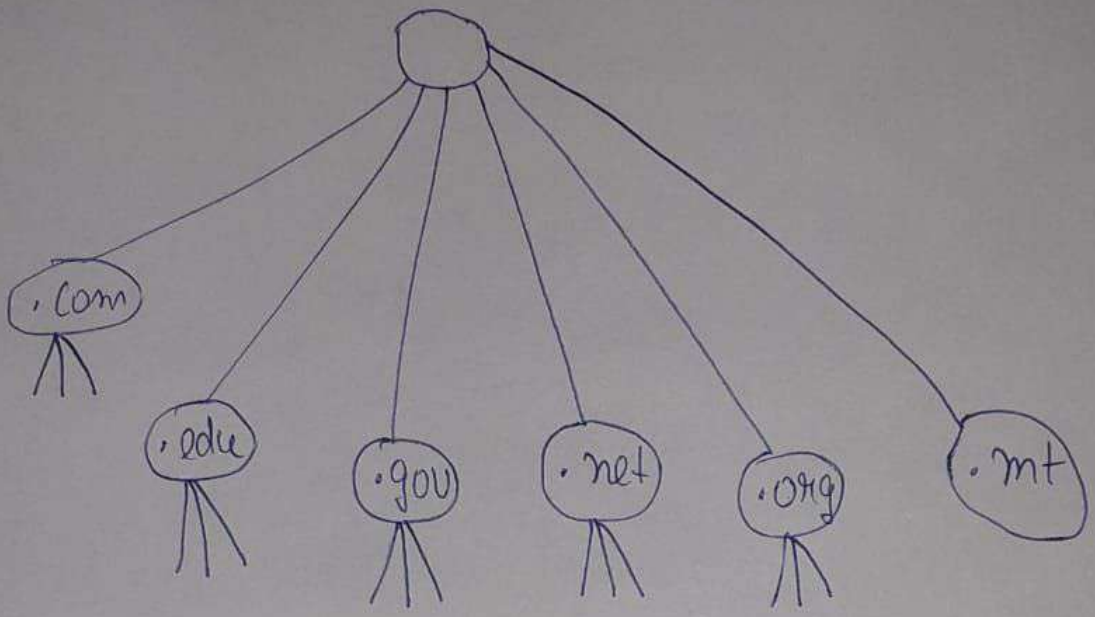
⇒ DNS in internet :-

- A domain name is used in the internet. It is an organizational level within the internet.
- Domain may be connected together to create a unique identifier.
- When connected together the domain name alway proceed left to right, from most specific to most general.
- The domain name is divided into three sections:



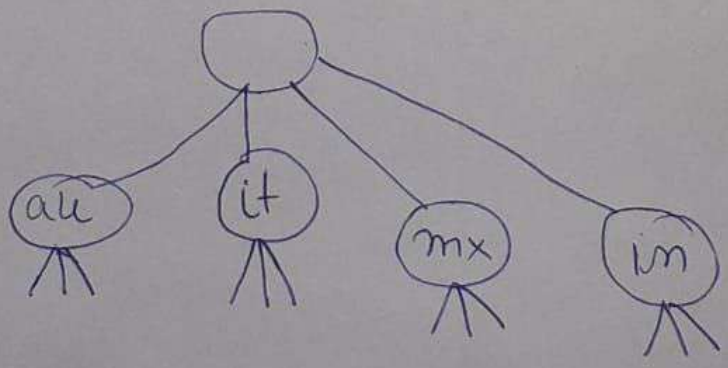
1. Generic domain :-

- The generic domain defines registered host according to their generic behaviour



2. Country / Geographic domain :-

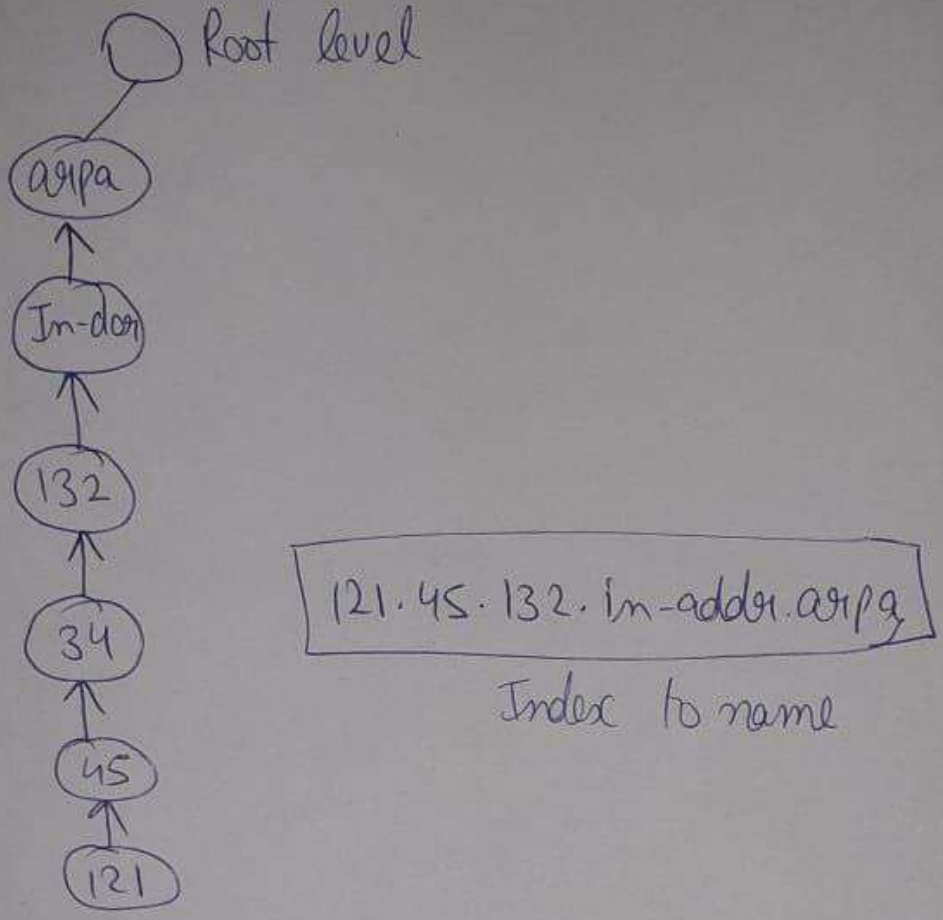
- In case of outside the United state, a code is included that indicates to which country it belongs.
- This code is consist of two characters which represents international country codes.



au - austorialia
in - India
mx - Mexico
jp - Japan
it - Itely

3. Inverse domain

- It is used to map an address to a name.



⇒ How does DNS work?

- To map a name into IP address, an application program calls a library procedure called the resolver. The name is passed on the resolver as a parameter
- The resolver sends the packet to the local DNS server which looks up the name and returns the corresponding IP address to the resolver.
- The resolver then sends this address to the caller. Then the program can establish a TCP connection with destination or sends the UDP packets.

⇒ World wide Web (WWW) :-

- The World wide web (WWW) is an architectural framework for accessing linked documents and serves as a global information repository.
- It is based on the hypertext system, where documents are linked together using pointers.
- The WWW uses the concept of hypertext.

(i) Client Side :-

- The client side refers to operations that occur in the user's browser when browsing the web.
- The web consists of numerous interlinked documents (pages) that users can access via browsers.

Characteristics :-

- The web is a collection of documents known as pages.
- Users navigate by clicking hyperlinks to related pages.
- Browsers fetch and display web pages.
- The browsers interprets text, formatting commands, and hyperlinks to present content properly.

Hyperlinks & Navigation :-

- Hyperlinks are text elements that link to other web pages.

- Browsers have navigation buttons for moving between pages.
- Web pages may contain icons, line drawings, maps and photos, which can also be linked.

(ii) Server Side in WWW :-

- The server side involves web servers processing and responding to client requests.
- Each website has a server process that listens for incoming connections.

Process of web page retrival :-

1. The browser determines the URL.
2. The browser asks DNS for IP address of the site.
3. DNS replies with IP address.
4. The browser establishes a TCP connection with the server.
5. The browser sends a GET request for the web page.
6. The server sends the main file.
7. The TCP connection is released.
8. The browser displays all the text of main page.

Features of server side processing :

- Uses HTTP protocol to handle requests and responses.
- Server performance can be affected by DNS resolution, network congestion, or server downtime.

(iii) Common gateway interface (CGI) :-

- The common gateway interface is a standard that enables web servers to execute external programs for generating dynamic content.

Meaning of CGI components:

1. Common - It defines rules applicable to all programming language.
2. Gateway - It acts as a bridge between the web server and external resources (databases, applications).
3. Interface - It provides a set of terms, calls, and variables for communication b/w the server and CGI programs

Functionality of CGI :-

- Creates dynamic web pages by processing user inputs.
- Defines how dynamic documents are structured and generated.
- Specifies how input data is supplied to programs and how output is returned.

⇒ Web browser :-

- A web browser is a software program used to access the world wide web (WWW).
- It allows a users to retrieve, display, and navigate web pages using the internet.

Functions of a Web browser

1. Accessing the WWW :-

- A web browser enables users to visit and explore web pages on the internet.

2. Displaying Web pages :-

- It renders HTML documents, including text, images, videos and links.

3. Following Hyperlinks :-

- Browsers helps users navigate from one resource to another using hyperlinks.

4. Fetching and processing data :-

- When a user enters a URL, the browser requests the web page from a web server using the HTTP (Hypertext transfer protocol).

5. Interpreting Web Technologies :-

- Modern browsers support HTML, CSS, Javascript and multimedia content.

Examples of Web browsers

- Netscape Navigator
- Internet Explorer
- Mosaic
- Lynx

Types of Web browser :-

1. Graphical Web browsers :

- Display both text and multimedia content (eg. chrom, Edge).

2. Non-Graphical Web browsers :-

- Only display text, useful for systems without graphical support (eg, Lynx).

How a Web browser works :-

1. The user enters a URL (uniform resource locator).
2. The browser sends a request to the web server.
3. The server locates the requested page and sends it back.
4. The browser interprets the HTML code and displays the page.

=> Surfing the Net :-

- Surfing the Net refers to browsing web pages by following hyperlinks in an almost random manner. This is how users explore different websites.

Key points about surfing the Net

1. Hyperlink Navigation : Users click links to move b/w web pages.
2. No fixed pattern : Internet surfing does not follow a fixed sequence.
3. Requires an internet connection : Users must connect to an

internet service provider (ISP) to access the web pages.

4. Starting page:

Most browsers open a predefined home page when launched.

5. Millions of websites:

Users can choose from an extensive range of websites for information or entertainment.

Steps to surf the Internet

1. Open a web browser.
2. Enter a URL or uses a search engine.
3. Click hyperlinks to visit different web pages.
4. Use bookmarks to save important sites.
5. Navigate back and forth using browser buttons.

⇒ E-mail :-

Email is a private communication between two parties who have account on the internet.

It is an electronic message sent from one computer to another.

You can send or receive personal and business related messages with attachment such as picture or formatted document etc.

Email passes from one computer known as a mail server to another as it travels over the internet.

To send the email you need a internet connection.

• Once email arrives at the destination mail server, it is stored in the electronic mail box until the recipient recieve it.

⇒ Structure of E mail message :-

1. Header 2. Body of Message

1. Header :-

- Header contains the name and address of the recipient, name and address of anyone who is being copied, subject of message.

2. Body :-

• Body contains the message itself.
• Just like with letters, you need the correct address, if you me the wrong address or mistype it, your message will get bounce back to you return back to sender.

⇒ Understanding E-mail address :-

• An email address is read from left to right for example.
• It should be written in small letter @ yahoo.com is read as "balsimar at rate yahoo dot.com."
• Here balsimar is the user name the person sending the email.
• In addition to username there is a domain. This is the ISP address.

Chapter - 8

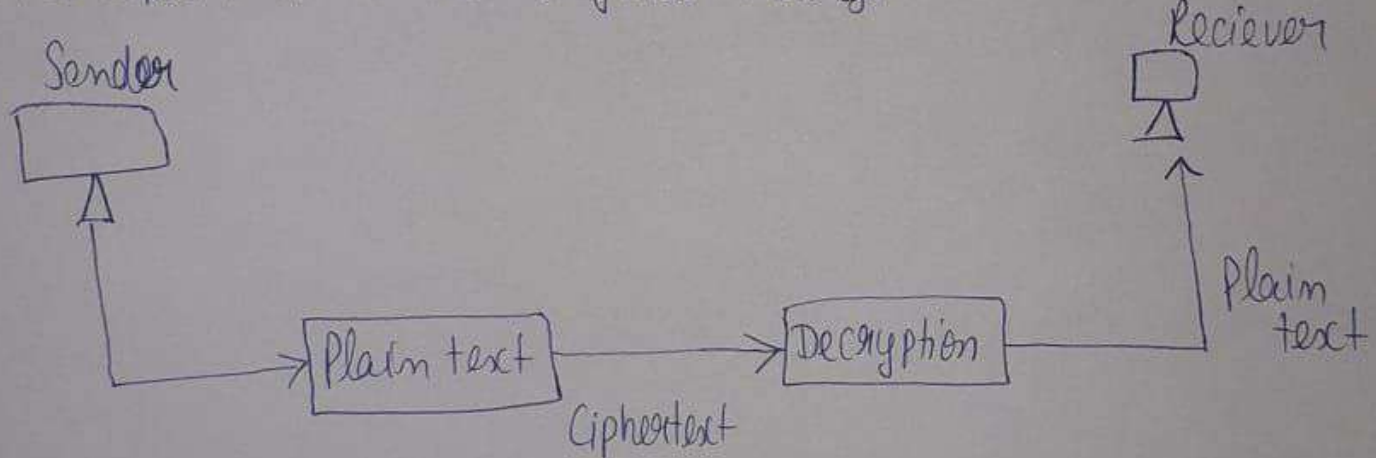
Network Security

Cryptography :-

Cryptography word with Greek origin means "secret writing". We use the term refer to the science and art of transforming message to make them secure and immune to attack.

Network security is mostly achieved through the use of cryptography: a science based on the abstract algebra.

Cryptography means writing secret code or Text. It refers to science and art of transforming the message to certain code and then retransform it to the original message.



Cryptography

Basic terminology used in Cryptography :-

i) Plain text : The original message, being transformed is called plain text

ii) Cipher text : The message is transformed into certain code is cipher text

i) Encryption algorithm :-

An encryption algorithm transform the plain text into cipher text.

ii) Decryption algorithm :-

It transform the cipher text back into the plain text. The sender uses an encryption algorithm but the reciever uses a decryption algorithm.

v) Cipher :-

Encryption and decryption refers to cipher.

The term cipher is also used to refer to different categories of algorithm in cryptography.

vi) Alice, Bob and Eve :

Alice is person who needs to send secure data.

Bob is the recipient data.

Eve is the person who want to distrub the communication b/w Alice and Bob.

vii) Key :

- A Key is number that the cipher an on algorithm operates on.

⇒ Substitution Cipher

- A substitution cipher substitute one symbol with other.
- If the symbol in the plain text are alphabetic character we replace one character with another.

- A substitution cipher replaces one symbol with another.

Example : We can replace S with A and K with B.

If symbols are digits (0 to 9) we can replace 3 with 7; and 2 with 6. Substitution cipher can be categorized into two parts.

1. Mono alphabetic cipher :-

- A symbol in the plain text is always changed to the same characters in the cipher text regardless of its position in the text.
- When one letter are grouped fillet is replace by another later called.

Example

Plain Text :- KHALSA (A → S)

Cipher Text :- KHSLSS

2. Polyalphabetic cipher :-

- The relationship between a character in the plain text to a character into the cipher text is one to many relationship.

Example :-

Plain text : HELLO

Cipher text : ABNZF

⇒ Transposition cipher :—

- The transposition cipher is related with the position or location changes.
- A character in the first position of the plain text may be may appear in the tenth position of the cipher text.
- In simple words a transposition cipher reorders the symbols in a block of symbols.

Example

Plain text	2	4	1	3
Cipher text	1	2	3	4

In Encryption we move the character at position.

$2 \rightarrow 1$

$4 \rightarrow 2$

$1 \rightarrow 3$

$3 \rightarrow 4$

This is the Rule (Key)

⇒ One time Pads (OTP):-

- The one time pad is a method for encryption messages that is theoretically unbreakable.
- It works by generating a random bit string and XORing it with the plain text message.

- Since the key is truly random and used only once, it ensures that every possible plaintext message of the same length is equally likely, making cryptanalysis impossible.

Example of one-time pad :-

- Consider the message I love you converted into binary (7 bit ASCII format).
- A random pad (key) of the same length is generated.
- The XOR operation b/w the messages and the pads produces cipher text.
- The cipher text appears completely random and has no patterns.

⇒ Two fundamental Cryptographic principles

1. Redundancy 2. Freshness

1. Redundancy :-

- Encrypted messages must include some redundant information that is not needed for understanding the message.
- Redundancy helps prevent active attacks where an intruder injects garbage data.
- However, too much redundancy can also aid passive attacks, making encryption easier to break.

2. Freshness :-

- Ensures that each message recieved can be verified as being fresh and not replayed.
- Protects against replay attacks, where an attacker resends previously captured valid message.
- Methods to ensure freshness include timestamps and cryptographic hashes.

⇒ Public Key :

- Public Key cryptography also known as asymmetric encryption was invented in 1976 by Whitfield Diffie and Martin Hellman.
- This encryption method differs from symmetric encryption, which uses a single key for both encryption and decryption. Instead asymmetric encryption uses a pair of keys:

1. Public Key - Known to everyone and used for encryption.
2. Private Key - Known only to the recipient and uses for decryption.

* How public key cryptography works ? :-

- If Simar wants to send a secure message to Aekam,
  (i) Simar encrypts the message using Aekam's public key.

(ii) AeKam then decrypts the message using their Private Key.

- This ensures that only AeKam can read the message, even if someone else intercepts it.

Key features :

- Highly Secure -

The private key cannot be guessed from the public key.

- Used in Online Security -

Used in email encryption, digital signatures, and secure websites.

- Requires Key sharing :-

The sender must know the recipient's Public Key before sending a message.

⇒ RSA Algorithm

- RSA algorithm is a public key cryptosystem widely used for secure data transmission, digital signatures, and authentication.

- Developed in 1977 by Rivest, Shamir, Adleman (RSA).
- Used in SSL/TLS, digital signature and secure email.
- Based on mathematical complexity of factoring large prime numbers.

Key generation steps :-

Step 1 : Select two large primes

- Choose two distinct large prime numbers:
  - (i) P and q
  - (ii) (Example: $P = 3, q = 11$, but real world uses 1024-bit primes)

Step 2 : Compute n and Euler's Totient $\phi(n)$

- $n = p \times q$

(Example: $n = 3 \times 11 = 33$)

- $\phi(n) = (p-1)(q-1)$

(Example: $\phi(33) = (3-1)(11-1) = 20$)

Step 3 : Choose a public key exponent e

- $1 < e < \phi(n)$
- $\gcd(e, \phi(n)) = 1$ (must be co prime)

(Example: $e = 3$, since $\gcd(3, 20) = 1$)

Step 4 : Compute private ~~key Exponent~~ key Exponent d

- d is the modular inverse of e mod $\phi(n)$

(Example: $d = 7$, because $3 \times 7 \equiv 1 \bmod 20$)

Final Keys

- Public Key $(n, e) = (33, 3)$
- Private Key $(n, d) = (33, 7)$

Encryption & Decryption :-

Encryption (Sender Side)

- Plaintext $M \rightarrow$ Ciphertext C

$$C = M^e \bmod n$$

(Example: If $M = 7$, then $C = 7^3 \bmod 33 = 343 \bmod 33 = 13$)

Decryption (Reciever Side)

- Ciphertext $C \rightarrow$ Plaintext M

$$M = C^d \bmod n$$

(Example $M = 13^7 \bmod 33 = 7$)

Why RSA is Secure? :-

- Security relies on difficulty of factoring large n (since $n = P \times q$)
- Brute-force attacks fail when primes are large (eg, 2048 bit)
- Private Key d cannot be easily derived from public key (n, e)

Practical Applications :

- Secure Web Browsing (HTTPs, SSL / TLS)
- Digital Signatures (Authentication)
- Secure Email (PGP Encryption

⇒ Digital Signature :-

- A digital signature is a cryptographic technique used to :

(i) Verify the authenticity of a sender.
(ii) Ensure integrity of a message / document.
(iii) Provide non-repudiation (sender cannot deny sending it).

How it works?

1. Sender signs the message using the private key.
2. Reciever verifies the signature using the sender's public key.
3. If verification succeeds, the message is authentic and unaltered.

Legal Status

- In many countries (including the USA & India), digital signatures are legally binding like handwritten signatures.

⇒ Symmetric Key Signatures (Message Authentication Code - MAC):-

Definition

- Uses a single shared secret key for both encryption and decryption.
- Provides sender authentication but non repudiation (since the key is shared).

Limitations

- No non-repudiation (both sender & reciever know the key).
- Not a true digital signature (only used for integrity checks)

Example:- HMAC (Hash-based MAC)

Combines a hash function (eg. SHA-256) with a secret key)
Used in banking, SSL / TLS and data verification.

⇒ Public Key Signatures (RSA, DSA, ECDSA) :-

- Uses asymmetric cryptography (Public & private keys).
- Provides non-repudiation (only the sender has the private key)

How it works? :-

1. Sender signs the message with their private key.
2. Reciever verifies using the sender's public key.
3. If verified, the message is authentic and untampered.

Example : RSA digital signature

1. Signing :
   - Compute hash of message $H(m)$.
   - Encrypt hash with private keys Signature = $H(m)^d \bmod n$.
2. Verification :
   - Decrypt signature with public key $H(m)' = \text{Signature}^e \bmod n$.
   - Compare $H(m)'$ with actual hash $H(m)$.

⇒ Message Digest :-

- A fixed size numeric fingerprint of a message (eg, SHA 256, MD5).
- Used to ensure data integrity.

Properties :-

- Deterministic (same input → same output)
- Fast computation
- Pre-image resistance (can not reverse engineer input from hash)
- Collision resistant (hard to find two different inputs with same hash).

Use Cases:

- Digital Signature (hash + encryption)
- Password storage (storing hashes instead of plain text)
- File integrity check (checksum).