V V COLLEGE OF ENGINEERING
V V Nagar, Arasoor, Tisaiyanvilai

Department of Electronics And Communication Engineering
Academic Year: 2020-2024 (Even Semester)
Regulation 2017

EC8551 / COMMUNICATION NETWORK

III year ECE

Unit I

Date of submission	Signature of staff incharge	Verification by HOD	Verification by Principal
31/10/22			

Unit II

Date of submission	Signature of staff incharge	Verification by HOD	Verification by Principal
31/10/22			

Unit III

Date of submission	Signature of staff incharge	Verification by HOD	Verification by Principal
31/10/22			

Unit IV

Date of submission	Signature of staff incharge	Verification by HOD	Verification by Principal
31/10/22			

Unit V

Date of submission	Signature of staff incharge	Verification by HOD	Verification by Principal
31/10/22			

Principal

EC8551	COMMUNICATION NETWORKS	L	T	P	C
		3	0	0	3

OBJECTIVES:

The student should be made to:

- Understand the division of network functionalities into layers
- Be familiar with the components required to build different types of networks
- Be exposed to the required functionality at each layer
- Learn the flow control and congestion control algorithms

UNIT I FUNDAMENTALS & LINK LAYER 9

Overview of Data Communications- Networks – Building Network and its types– Overview of Internet - Protocol Layering - OSI Mode – Physical Layer – Overview of Data and Signals - introduction to Data Link Layer - Link layer Addressing- Error Detection and Correction

UNIT II MEDIA ACCESS & INTERNETWORKING 9

Overview of Data link Control and Media access control - Ethernet (802.3) - Wireless LANs – Available Protocols – Bluetooth – Bluetooth Low Energy – WiFi – 6LowPAN–Zigbee - Network layer services – Packet Switching – IPV4 Address – Network layer protocols (IP, ICMP, Mobile IP)

UNIT III ROUTING 9

Routing - Unicast Routing – Algorithms – Protocols – Multicast Routing and its basics – Overview of Intradomain and interdomain protocols – Overview of IPv6 Addressing – Transition from IPv4 to IPv6

UNIT IV TRANSPORT LAYER 9

Introduction to Transport layer –Protocols- User Datagram Protocols (UDP) and Transmission Control Protocols (TCP) –Services – Features – TCP Connection – State Transition Diagram – Flow, Error and Congestion Control - Congestion avoidance (DECbit, RED) – QoS – Application requirements

UNIT V APPLICATION LAYER 9

Application Layer Paradigms – Client Server Programming – World Wide Web and HTTP - DNS- - Electronic Mail (SMTP, POP3, IMAP, MIME) – Introduction to Peer to Peer Networks – Need for Cryptography and Network Security – Firewalls.

TOTAL:45 PERIODS

OUTCOMES:

At the end of the course, the student should be able to:

- Identify the components required to build different types of networks
- Choose the required functionality at each layer for given application
- Identify solution for each functionality at each layer
- Trace the flow of information from one node to another node in the network

TEXT BOOK:

1. Behrouz A. Forouzan, "Data communication and Networking", Fifth Edition, Tata McGraw – Hill, 2013 (UNIT I –V)

REFERENCES

1. James F. Kurose, Keith W. Ross, "Computer Networking - A Top-Down Approach Featuring the Internet", Seventh Edition, Pearson Education, 2016.
2. Nader. F. Mir," Computer and Communication Networks", Pearson Prentice Hall Publishers, 2nd Edition, 2014.
3. Ying-Dar Lin, Ren-Hung Hwang, Fred Baker, "Computer Networks: An Open Source Approach", Mc Graw Hill Publisher, 2011.
4. Larry L. Peterson, Bruce S. Davie, "Computer Networks: A Systems Approach", Fifth Edition, Morgan Kaufmann Publishers, 2011.

UNIT - 1

FUNDAMENTALS AND LINK LAYER

Networks:

A networks is a set of devices interconnected by a communication medium.

Types of connections

1. Point-to-point: link, there is dedicated link between two devices.

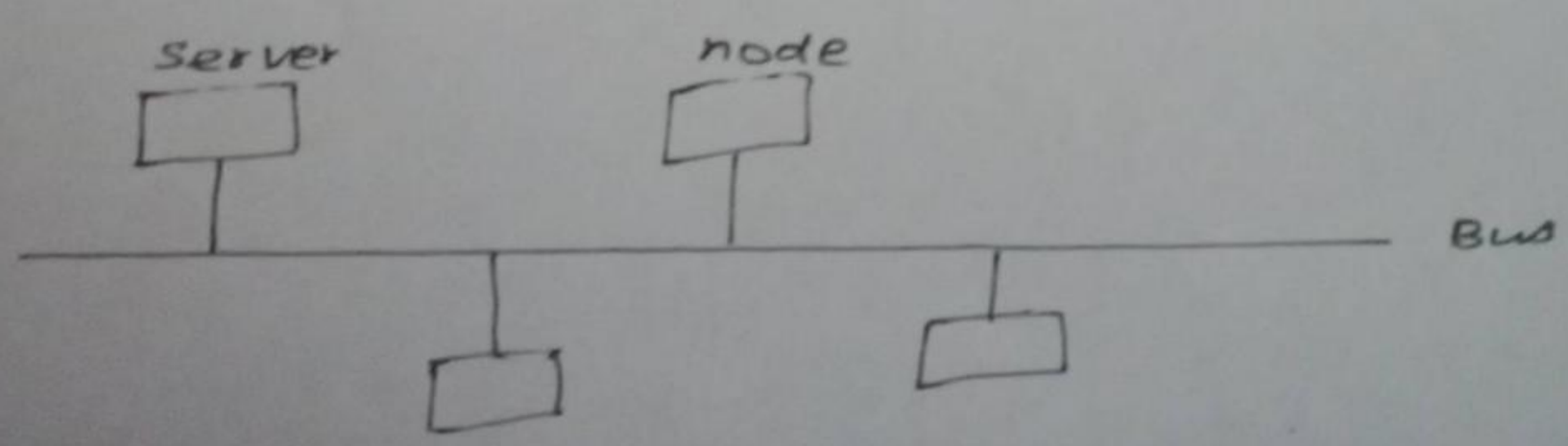
2. Multipoint - when 2 or more devices share a common link, it is called as multipoint connection.

Physical Topology:

The physical topology of LAN refers to the way in which the stations are physically interconnected.

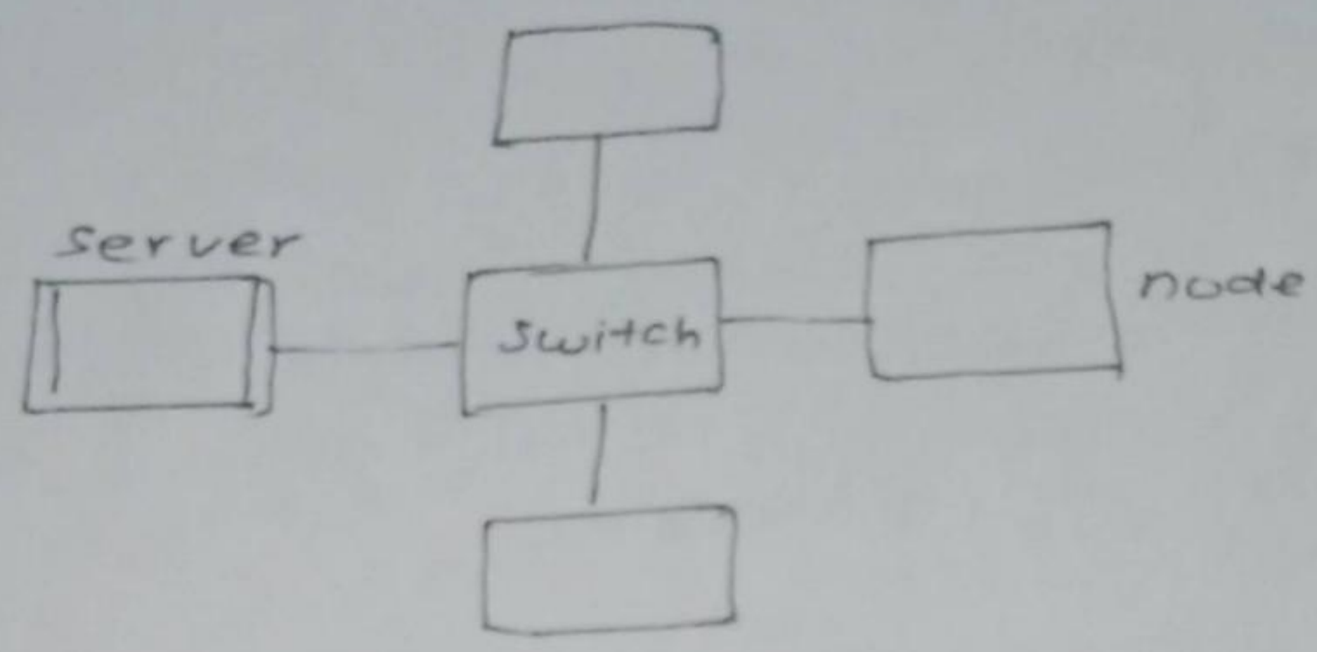
Bus Topology:

In bus topology, multiple devices are connected one by one, by means of drop cables.



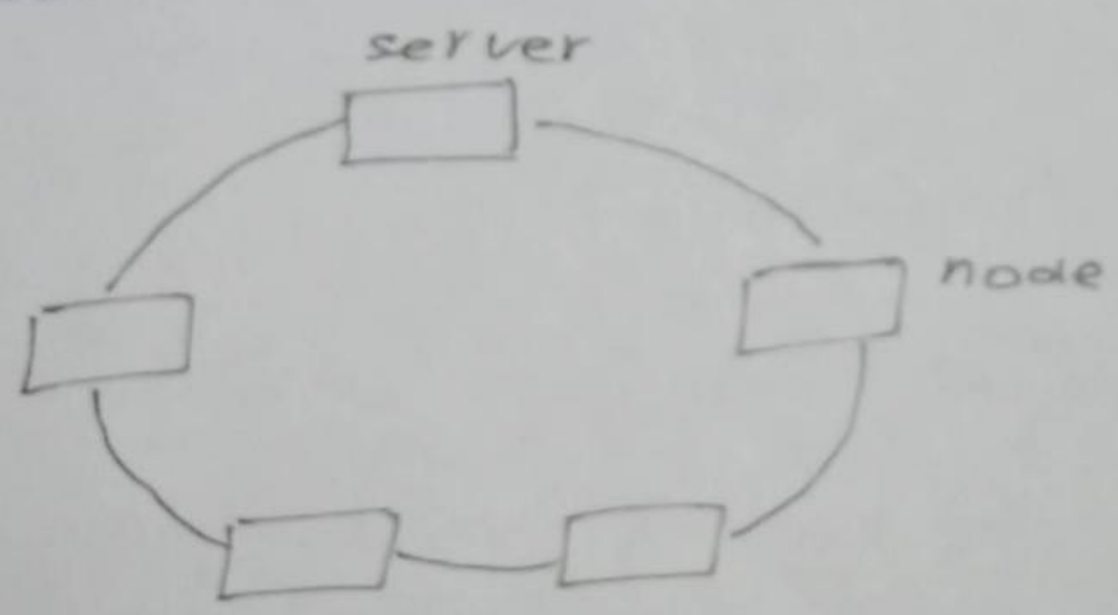
Star Topology:

A stare topology consists of a number of devices connected by point-to-point links to a central hub.



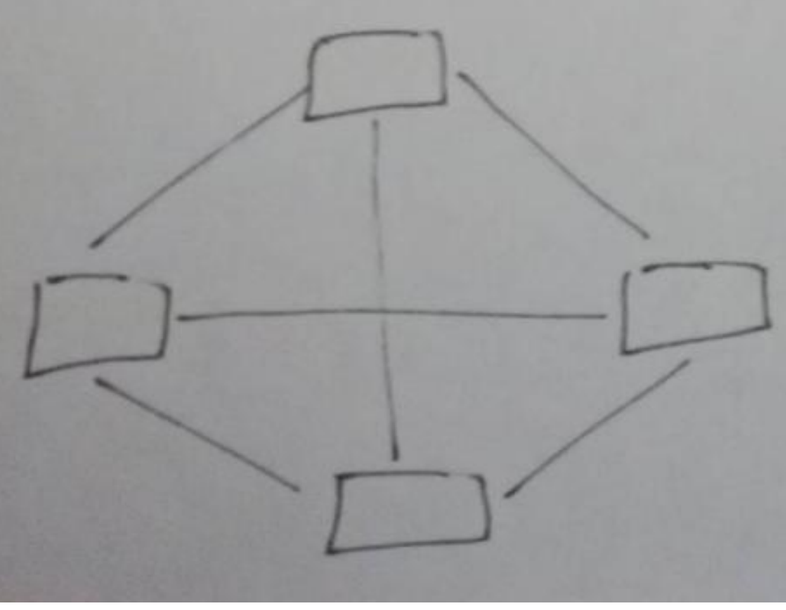
Ring Topology:

In ring topology, each computer is connected to the next computer, with the last one connected to the first.



Mesh Topology:

The mesh topology has a link b/w each devices in the network.



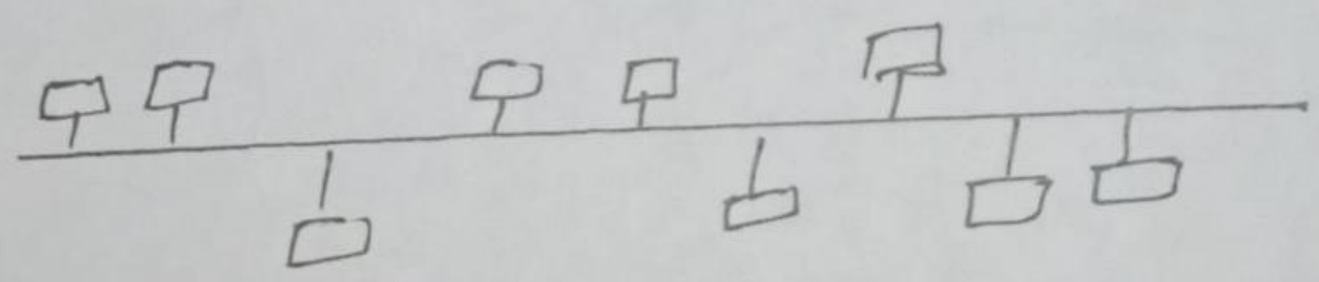
Network Tybes

Local Area Network (LAN):

The IEEE 802 LAN is a popularly used shared medium peer-to-peer communication network that broadcasts information for all stations to receive.

The LAN enables stations to communicate directly using a common physical medium on a point-to-point basis without any intermediate switching node being required.

A LAN is a system composed of computers hardware and transmission media and saftware.



Metropolitan Area Networks (MAN)

A MAN, white larger than LAN to city or group of nearby corporate offices. It uses similar technology of LAN.

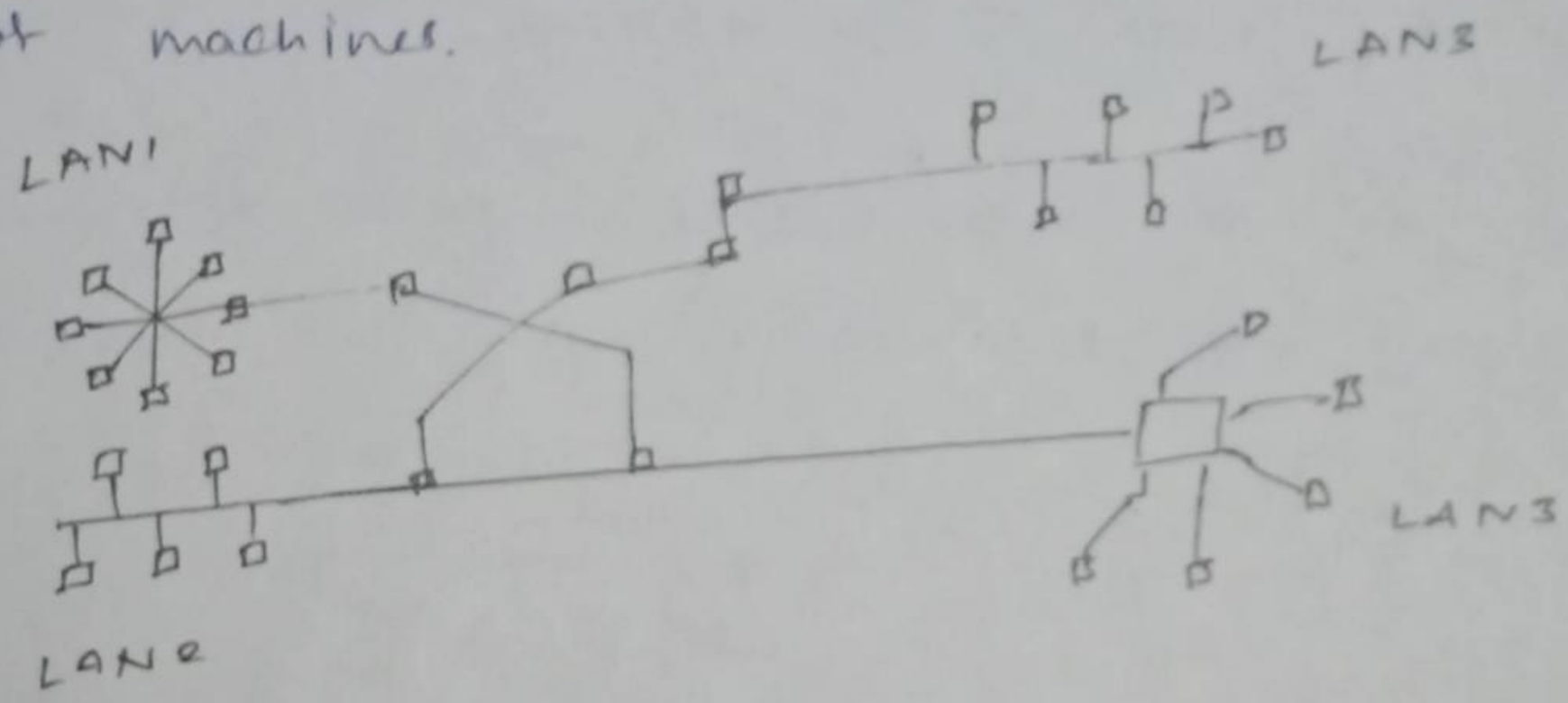
The Metropolitan Area Network stands are sponsored by the IEEE, ANSI and the Regional Bell operating companies.

Wide Area Network (WAN)

A WAN provides long distance transmission of data and voice.

A network that covers a larger area such as a city, state, country or the world is called wide area network.

The WAN contains host and collection of machines.



Wireless Networks :

A wireless LAN or WAN is a wireless local area network that uses radio waves as its carrier. The last link with the users is wireless, to give a network connection to all users in a building or campus. The backbone network usually uses cables.

protocols:

A protocol is a set of rules that governs data communication. protocol defines the method of communication, how to communicate, when to communicate etc.

Important elements of protocols are,

1. syntax
2. semantics
3. Timing

syntax:

syntax means format of data or the structure of data.

sematics:

sematics is the meaning of each section of bit eg - address.

Timing:

Timing means, at what time data can be sent and how fast data can be sent.

These all about the protocols and its elements.

protocal layering:

A computer network must provide general cost effective, fair and robust connectivity among a large number of computers. Designing a network to meet these requirements is no small task.

Layered Architecture:

Computer network is designed around the concep of layered protocols or functions. For exchange of data between computers, terminals or other data processing devices, there is data path between two computers, either directly or via a communication network.

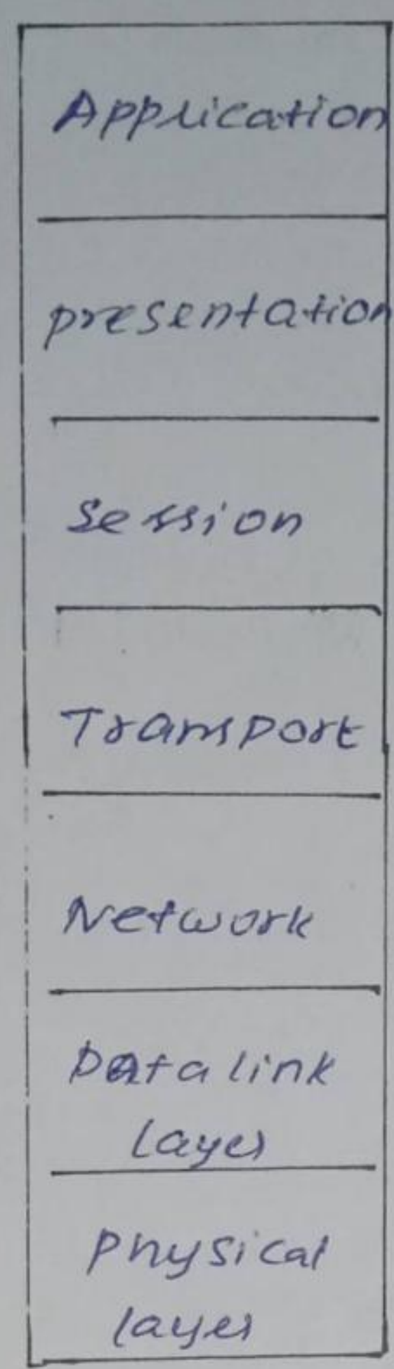
OSI MODEL

The ISO was one of the first organisation that introduce and develop the open System Interconnection reffers to OSI MODEL.

OSI model is a seven layer standared.

OSI model does not specify the communication standared or protocol to be used.

OSI MODEL Structure

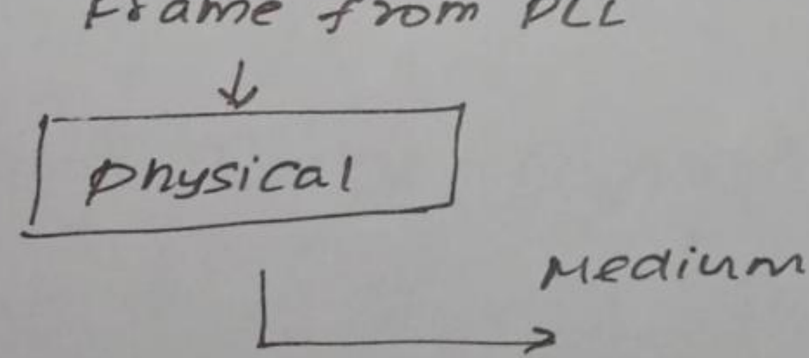


Layers in OSI Model

Physical Layer:

physical layer is the lowest layer of the OSI Model.

physical layer co-ordinates the functions.

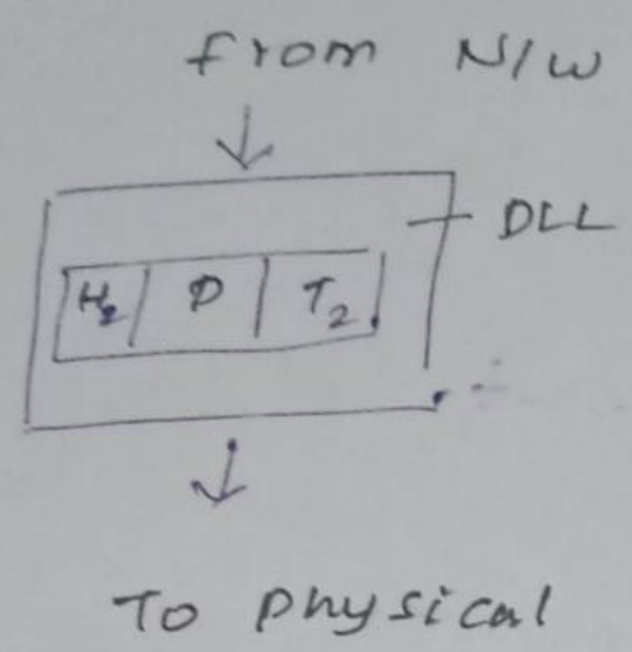


Functions:

1. physical characteristics
2. Representation of bits
3. Data rate
4. Synchronization of bits

2. Data link layer:

The DLL is responsible for transmitting frames from one node to the next.

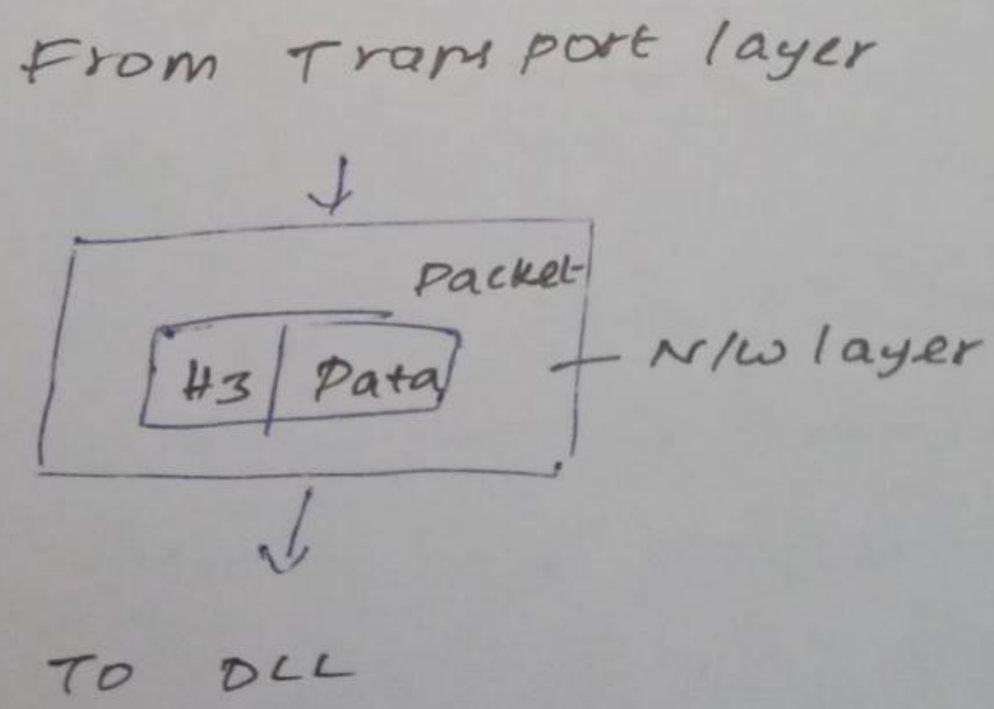


Functions:

1. Framing
2. physical addressing
3. Flow control
4. Error control
5. Access control.

3. Network Layer:

The network layer is responsible for the the delivery of packets from source to destination.

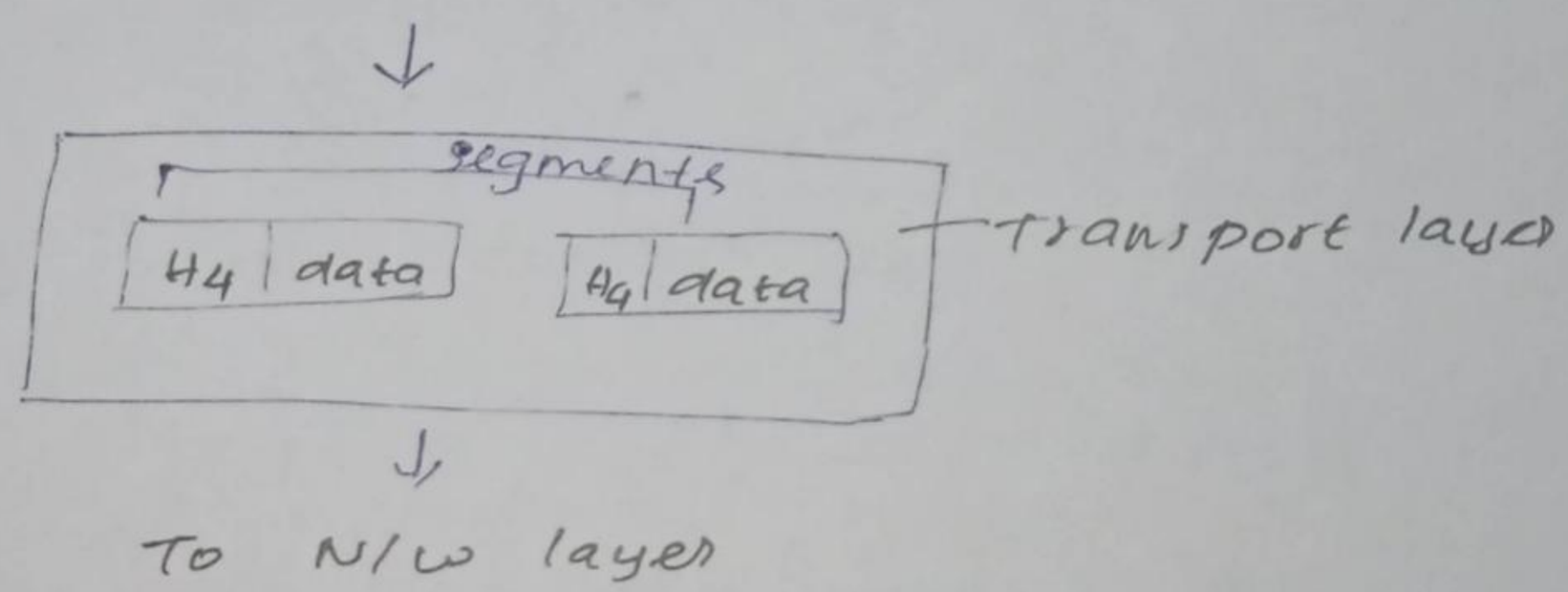


Functions:

1. Logical Addressing
2. Routing
3. Access Control

4. Transport layer:

The transport layer is responsible for delivery of message from one process to another.

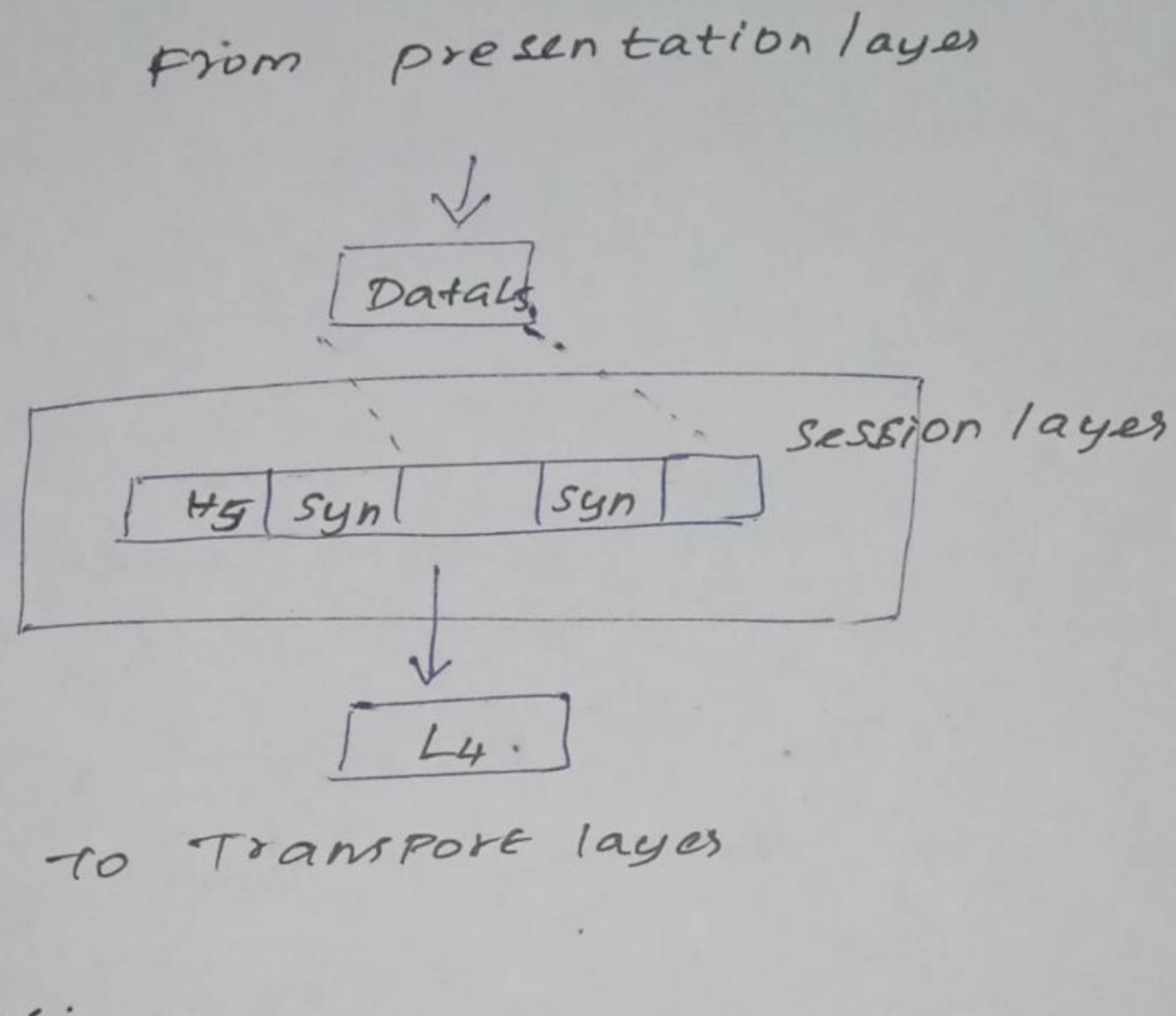


Functions:

1. Port addressing
2. Segmentation & reassembly
3. Connection control
4. Flow control
5. Error control.

5. Session layer:

The session layer is network dialog controller. It estabilishes and synchrony between Communication System.

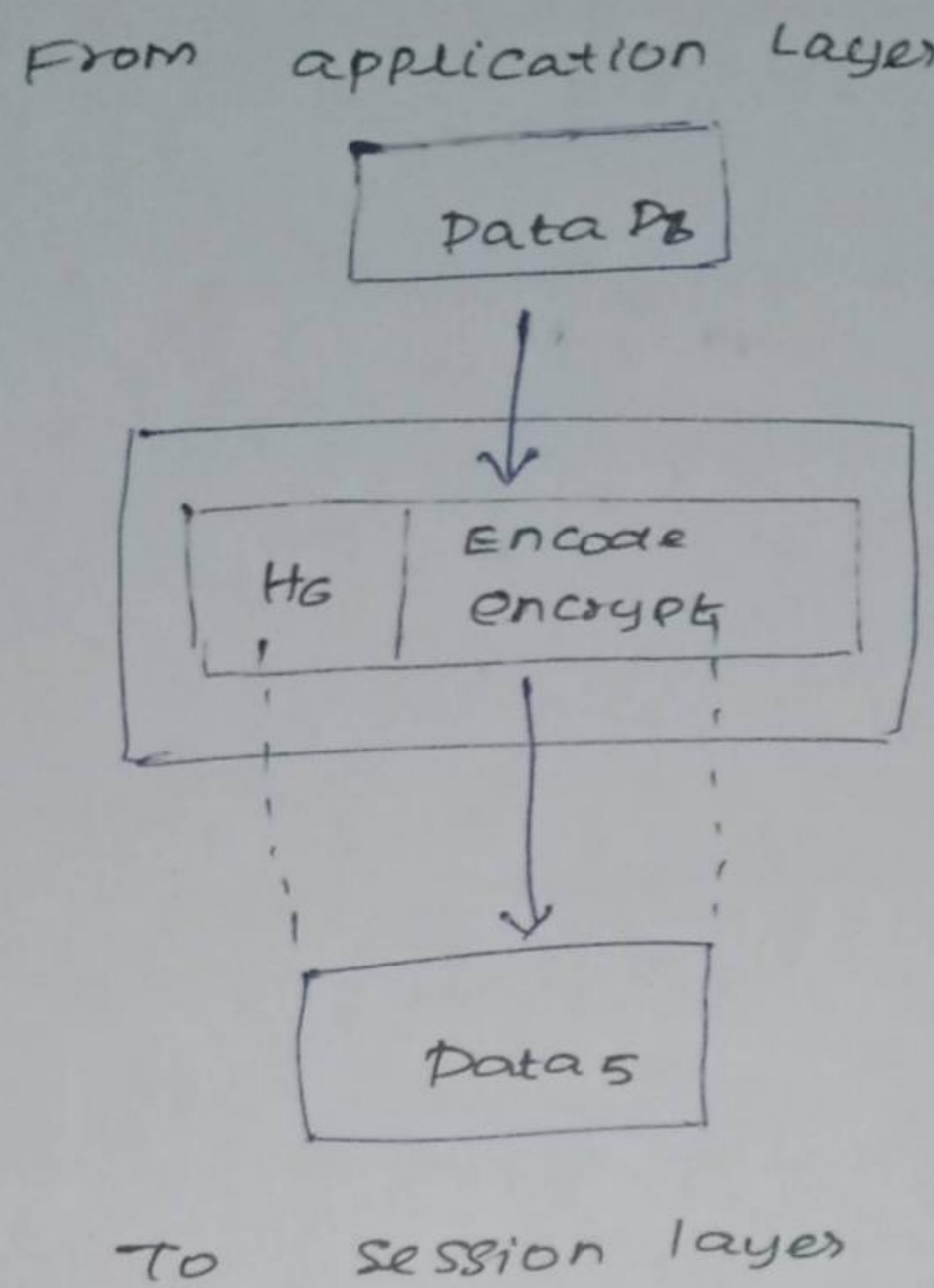


Functions:

1. Dialog control
2. Synchronization
3. Dialog Seperation

6. Presentation Layer

The presentation layer deals with syntax and semantics of the information being exchanged.



Functions:

1. Translation
2. Encryption, decryption
3. Encoded, Decoded
4. Compression, Decompression

7. Application Layer:

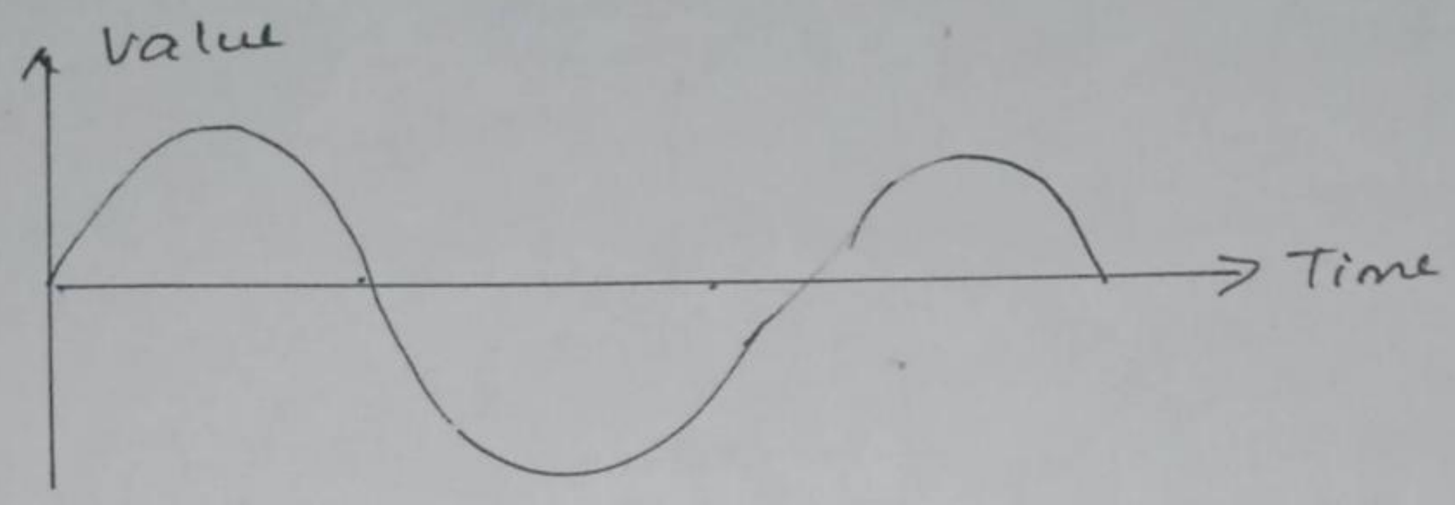
Application layer is responsible for accessing the network by user.

Functions:

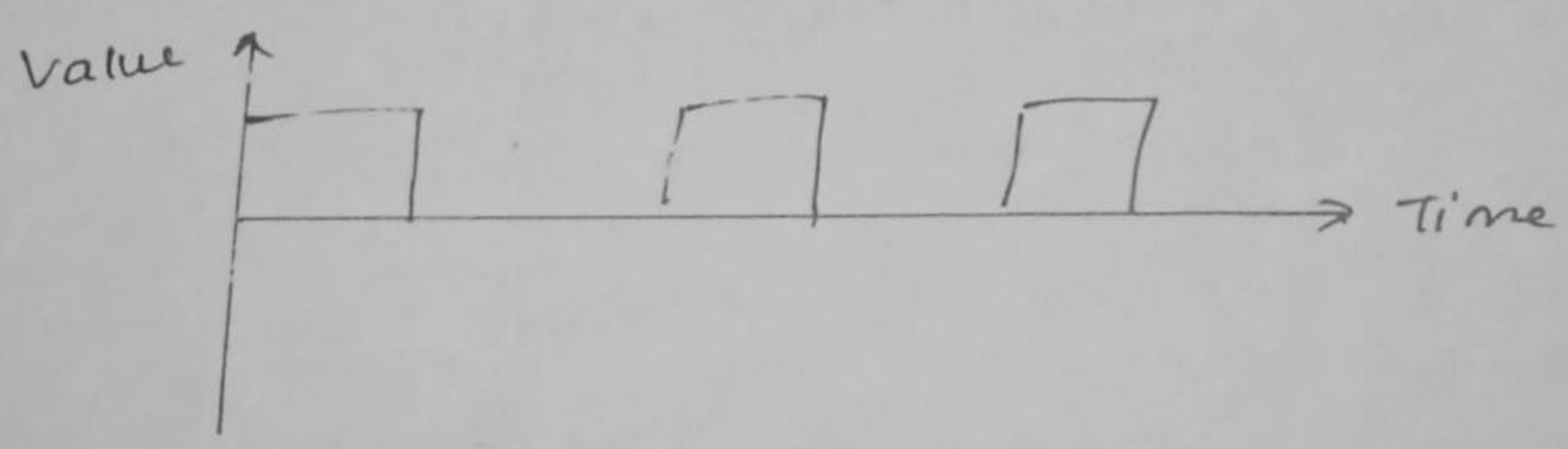
1. Network virtual terminal
2. File transfer, Accessing
3. Mail services
4. Directory services.

Analog and Digital Signals

Both data and signals that represent them can be either analog or digital in form.



Digital data take on discrete values. All binary signals are digital, but digital signal are not nessacerily binary.



Introduction to Data Link layer

Some important functions of data link layer includes well defined services interface to the network layer, framing, flow control, error detection and error control, frame following and sequencing. These all are very important functions for reliable communication.

Unacknoledgement Connectionless service:

As the name suggests it is unacknoledge form of transmission.

Here the source machine senas the data to the destinationmachine without any acknowledgement.

Acknowledgement connectionless service:

In acknoledged connections service each data frame is acknowlegded by the destination machine.

Acknowledgement connections services:

Acknowledgement connection service establilishes prior to data transmission.

Services provides to Network layer:

the primary responsibility of data link layer is to provide services to the network layer.

The principle service is transmitting data from the network layer on the source machine to the network layer on the destination machine.

Framing :

Framing in the data link layer separates a message from one source to a destination or from other message to other destinations by adding a sender address and a destination address.

To service the network layer, data link layer uses the service provided to it by the physical layer.

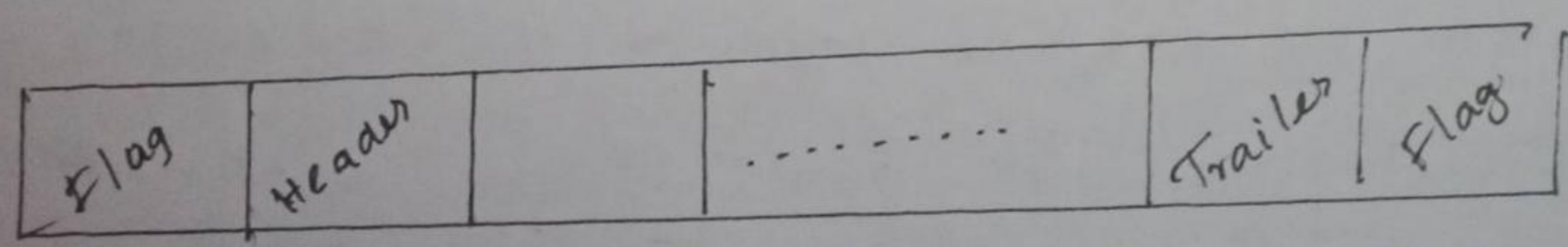
physical layer accepts the raw bit stream and delivers it to the destination.

Variable size framing:

1. Character oriented
2. Bit oriented.

Character oriented protocol:

In this type data to be carried are 8 bit characters from a coding system such as ASCII.



Bit Oriented protocol:

In this protocol, the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio and video.

Most protocol use a special 8 bit pattern flag 01111110 as delimeter

Error control:

To ensure the proper sequencing and safe delivery of frames at the destination, an acknowledgement should be sent by the destination network.

If the sender received a positive acknowledgement it means the frame has arrived safely.

If the sender receives a negative acknolege it means that frame is to be re gone wrong and retransmitted

A timer at sender's end is introduced. Also sequence numbers to the outgoing frames are maintained

Flow control:

When the sender is running on fast machine or highly loaded machine and receiver is on slow or heavily loaded machine.

Then the transmitter will transmit frames faster than the receiver can accept them.

Even if the transmission is error free at a certain point the receiver will simply not be able to handle the frames as they arrive and will start to lose some.

Link Layer Addressing

Data link layer uses MAC address to choose one node among several nodes, if the connection is not point to point.

A link-layer address is also called a link address, or physical address, and sometimes a MAC address.

Types of link layer Addressing

1. unicast
2. Multicast
3. broadcast

unicast:

unicast refers to one-to-one communication. Each host or each interference of a router is assigned a unicast address.

A frame with a unicast address destination is destinated only for one entity in the link.

Multicast:

Multicasting refers to one-to-many communication.

Most link-layer protocols define multicast address.

Broadcast:

Broadcasting refers to one-to-all communication. A frame with a destination broadcast address is sent to all entities in the link.

Most link-layer protocols define a broadcast

Error detection and Correction

Data transmission from one device to another device with complete accuracy is possible through the network. An unavoidable noise and interference is added to the communication channel.

Reasons for error:

1. If the power supply in the system is not exactly at the specified voltage component may not operate perfectly.

2. System may be operating at its low or high temperature limit.

3. Cross talk from adjacent signals can corrupt the signal.

Types of Error.

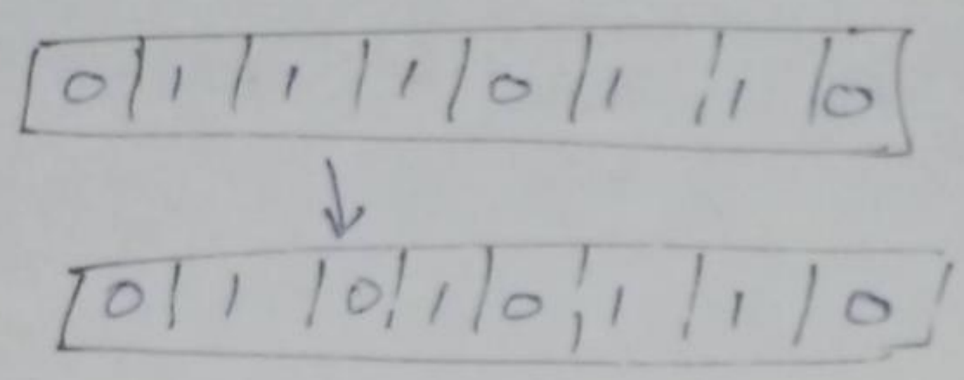
1. Single bit error

2. Burst error

Single bit error:

It means that only 1 bit of a given data unit is changed from 1 to 0 or from 0 to 1

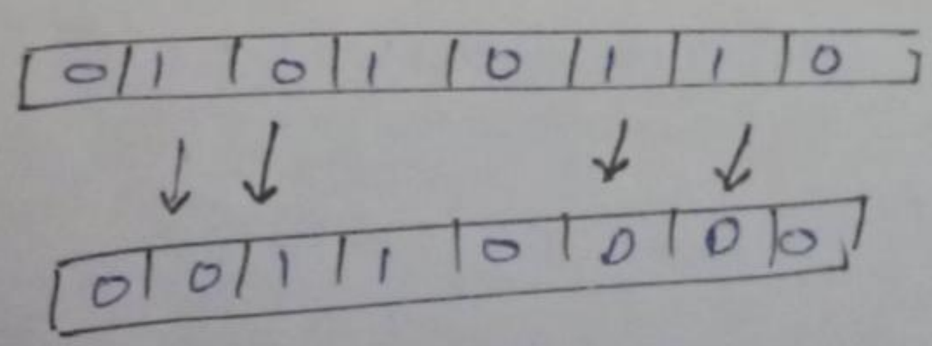
A single bit error is an isolated error condition that alters one bit but does not affect nearby bits.



Multibit error:

The term burst error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.

Burst errors are more common and more difficult to deal with errors. Burst errors can be caused by impulse noise. Note that the effects of Burst errors are greater at higher data rates.



Error detection:

The simplest form of error detection is to append a single bit, called a parity check, to a string of data bits.

The parity check bits has the value 1 if the number of 1s in the bit string is called odd and has the value 0 otherwise.

Redundancy:

Redundancy is a form of error detection where each data unit sent multiple times. i.e., twice.

At the receiver side, the two units are compared and if they are same, it is assumed that no transmission errors have occured.

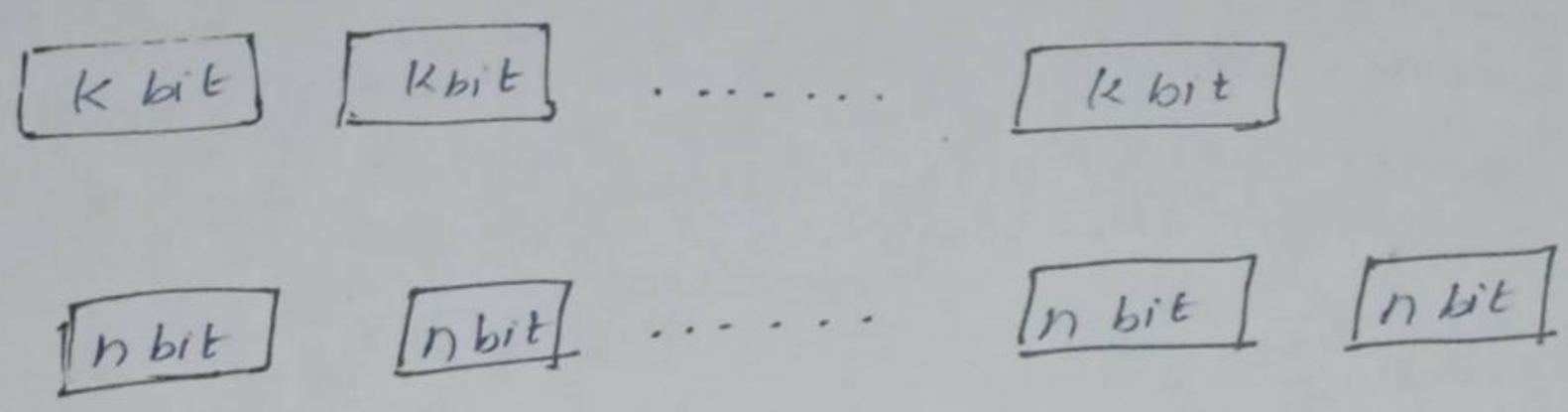
When the data unit is a single character, it is called character redundancy.

whereas if the data unit is the entire message, it is called message redundancy.

Block Coding

In block coding, message is divided into blocks.

Each block size is k bits and called as data words.



Error detection:

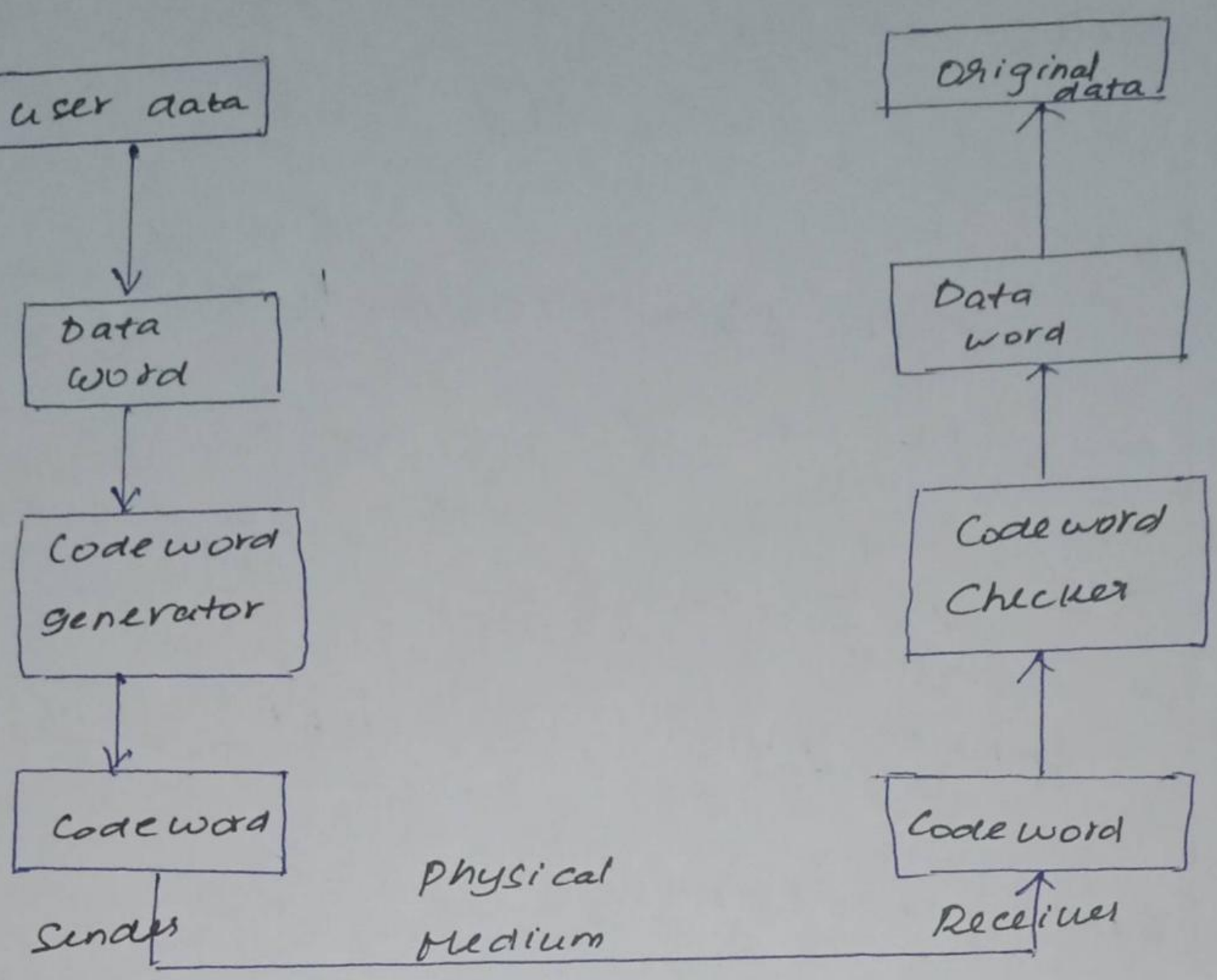
Following step are used for detecting errors in the block coding.

1) The receiver has a list of valid codewords.

2) The original codeword has changed to an invalid one.

The sender creates codewords out of datawords by using a generator that applies the rules and produces of encoding. Each codeword send to the receiver may change during transmission.

If the received codeword is the same as one of valid codewords, the word is accepted.



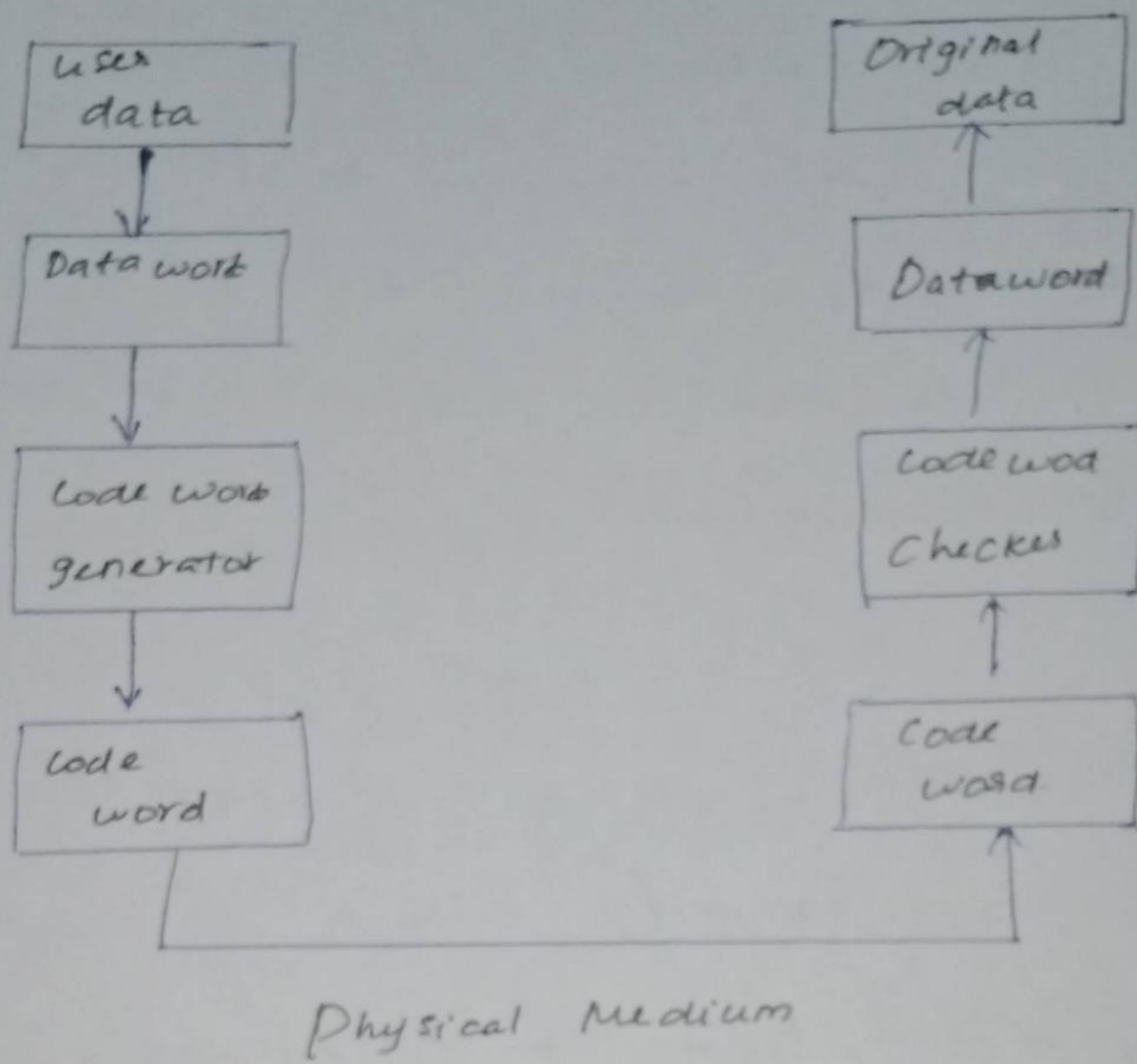
Error detection process.

Error correction:

The following figure shows the error correction process.

Error correction is much more difficult that error detection.

In error correction, the receiver needs to find the original cordeword sent. More numbers of redundant bits are required for error correction than for error detection.



Error Correction in block coding

Hamming Distance:

Hamming bits are inserted into the message at the random locations.

Hamming code is a single error Correcting code. It is most complex from the stand point of creating and interpreting the error bits.

The number of bits in the message are counted and used to determine the number of hamming bits to be used.

The equation is used to count the number of hamming bits.

$$2^H \geq M + H + 1$$

$M \rightarrow$ no. of bits in message

$H \rightarrow$ hamming bits

Minimum hamming distance:

The minimum hamming distance is the smallest hamming distance between all possible pairs in the set of words.

To find the value of dmin, we find the hamming distance between all words and select the smallest one.

Linear Block Coding:

In a linear block code, the exclusive OR (X OR) of any two valid codewords creates another valid codeword. Almost all block codes used today belong to a subset called linear linear block codes.

Cyclic Redundancy check:

parity method detects only odd number of errors. To overcome this weakness polynomial codes error detection method is used.

Working of CRC:

Suppose we want to send the bit sting 1101011 and generator polynomial

ie $G(x) = x^4 + x^3 + 1$

Step 1: Append 0's to the end of the string.

The number of 0s is the same the degree of the generator polynomial.

Step 2: Devide B(x) by G(x). We can write this algebraically as

$$\frac{B(x)}{G(x)} = Q(x) + \frac{B(x)}{G(x)}$$

$G(x) = x^4 + x^3 + 1 = 11001$

String - 11001011 = After appending 11010110000

```
            1 0 0 1 0 1 0
11001) 1 1 0 1 0 1 1 0 0 0 0
       1 1 0 0 1
       ---------
         0 0 1 1 1
         0 0 0 0 0
         ---------
           0 1 1 1 1
           0 0 0 0 0
           ---------
             1 1 1 1 0
             1 1 0 0 1
             ---------
               0 1 1 1 0
               0 0 0 0 0
               ---------
                 1 1 1 0 0
                 1 1 0 0 1
                 ---------
                   0 1 0 1 0
                   0 0 0 0 0
                   ---------
                     1 0 1 0 - Remainder
```

Step 3:

Define $T(x) = B(x) - R(x)$. In this case

$B(x) = 1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 0$

$R(x) = 1\ 0\ 1\ 0$

$T(x) = 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 1\ 0$

Note that the string T is actually the same as string B with appended 0s replaced by R. The sender transmit the string T.

Cyclic codes Analysis:

Let us define the followings

$f(x)$ - polynomial with binary coefficients

$d(x)$ - Data words

$c(x)$ - Code word

$g(x)$ - Generator

$e(x)$ - error

$S(x)$ - Syndrome

if $S(x)$ is not syn zero, then one or more bits is corrupted.

$$\frac{\text{Received codeword}}{g(x)} = \frac{C(x)}{g(x)} + \frac{e(x)}{g(x)}$$

A single bit error is $e(x) = x^i$, where

$i \rightarrow$ position of bit.

If the single bit is caught, then x^i is not divisible.

Advandages of Cyclic codes:

1. Easily implemented in hardware.
2. CRC are faster when implemented in hardware.
3. It give good performance in detecting single bit errors, double errors, an odd number of errors and burst error.

x ——— x

UNIT - 2

MEDIA ACCESS AND INTERNETWORKING

Overview of Media Access & control.

One feature of LAN is that its backbone is a shared channel or transmission link, which provides all user to access to the transmission facilities. It may be possible that two or more stations transmitting simultaneously, causing their signals to interfere and becomes garbled.

Random access technique are,

i) ALOHA

ii) carrier sense multiple Access (CSMA)

iii) CSMA with collision detection (CSMA/CD)

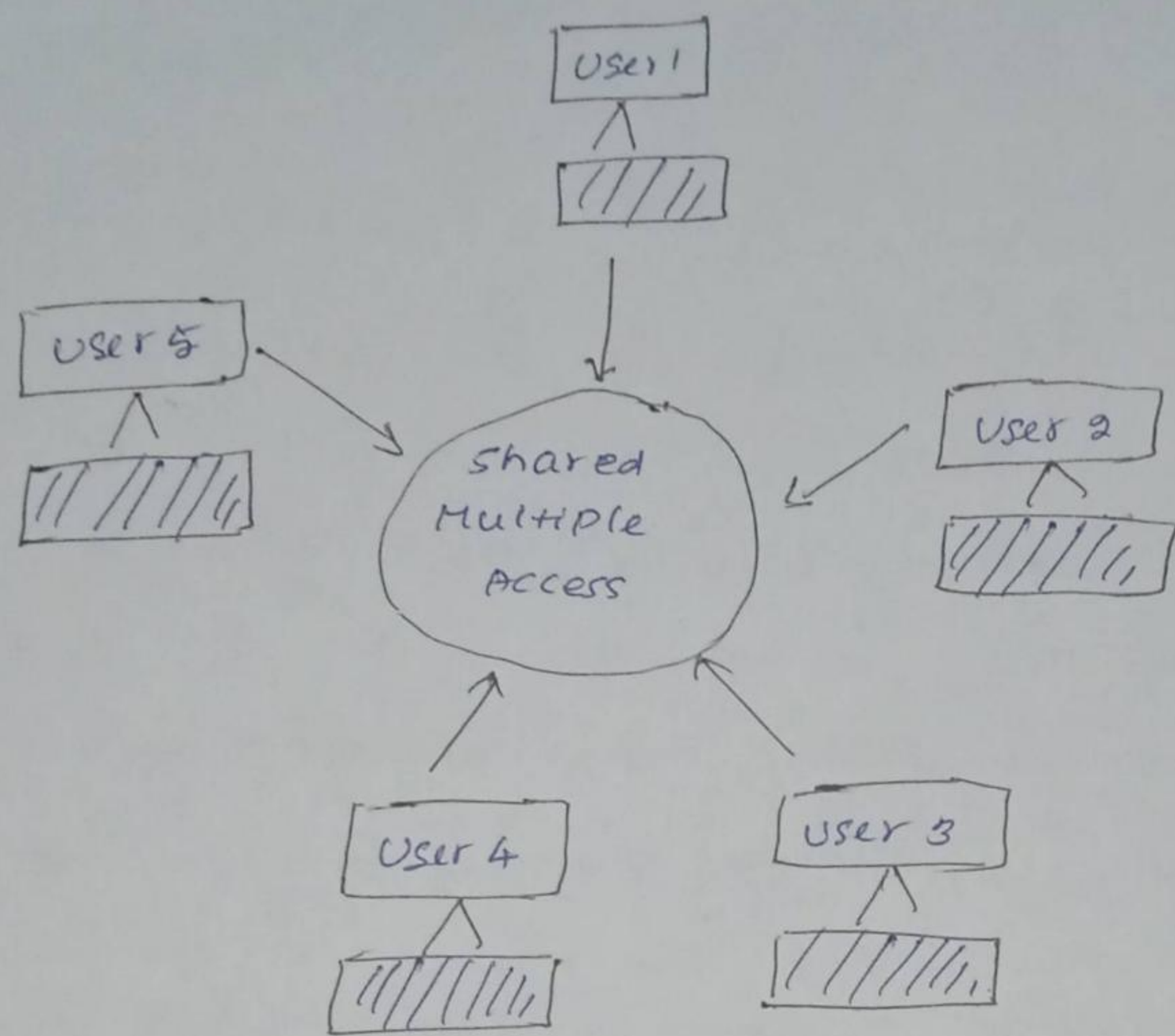
iv) Register insertion

Controlled access to LAN can be performed in to 2 types:

1. centralized technique
2. Distributed technique.

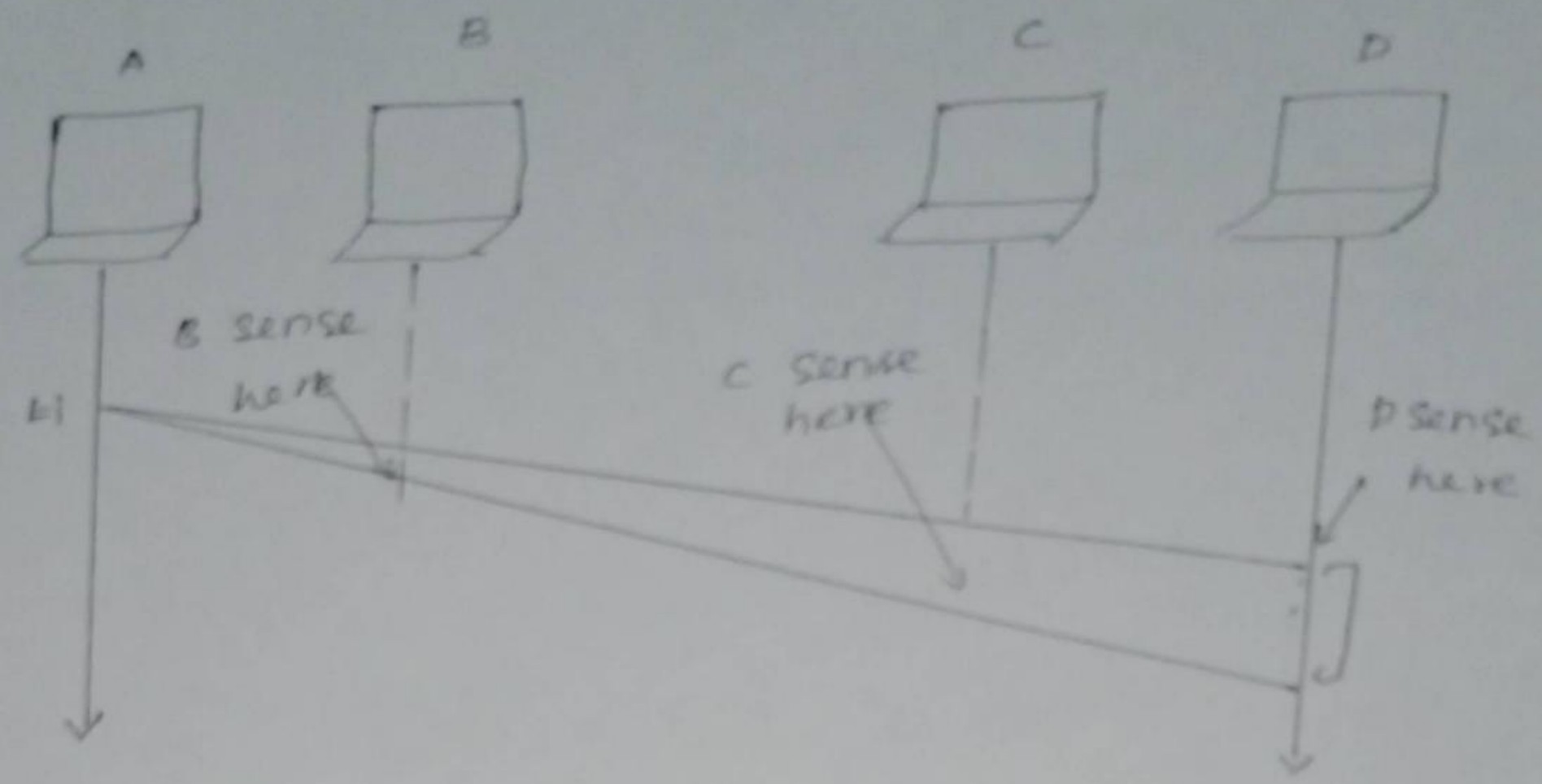
This sharing techniques are used in wired communications, and networks based on radio communication.

Multiple Access Communication:



Carrier sense Multiple Access protocol:

The low maximum throughput of the ALOHA schemes is due to the wastage of transmission bandwidth because of the frame collisions. This wastage can be reduced by avoiding transmissions that are certain to cause collision. By sensing the medium for the presense of a carrier signal from other stations a stations can determine whether there is an on going transmission.



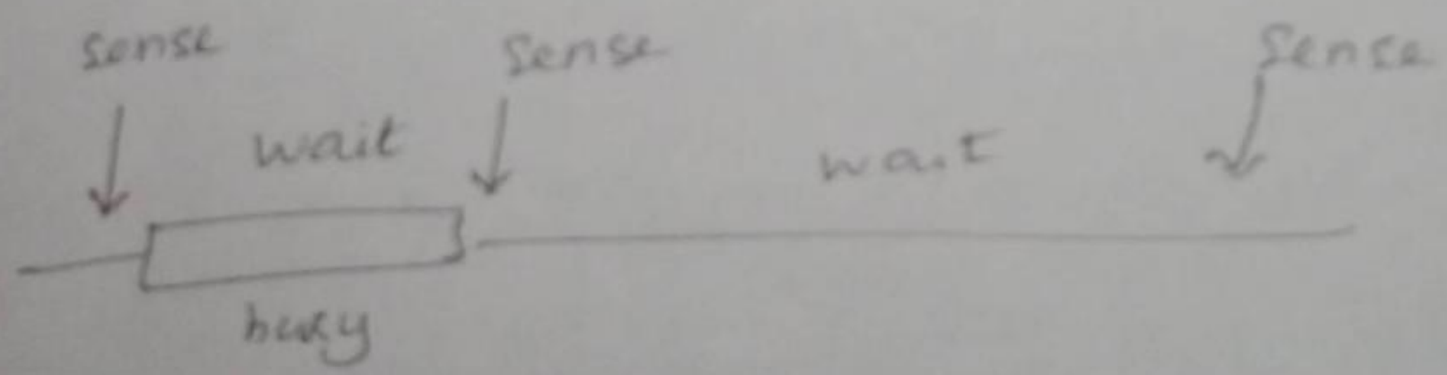
variable periode in CSMA

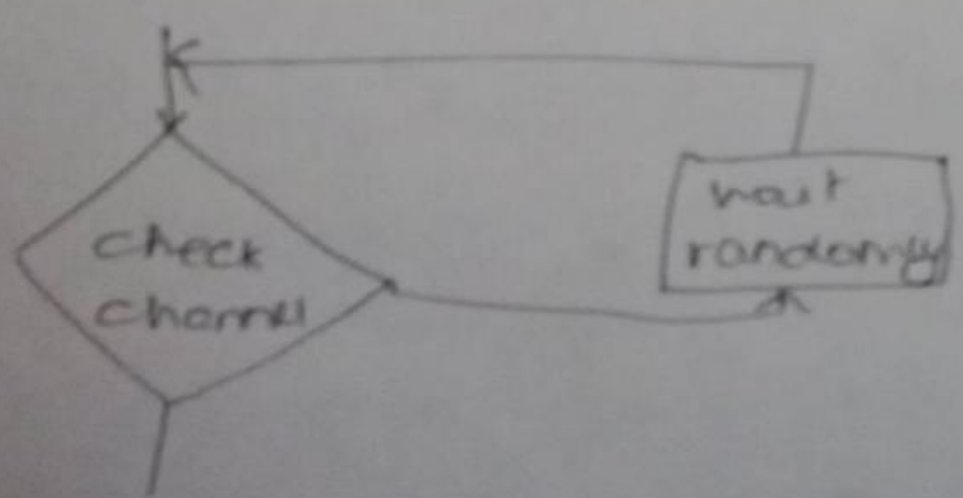
Persistence Methode:

These - three protocoll are,

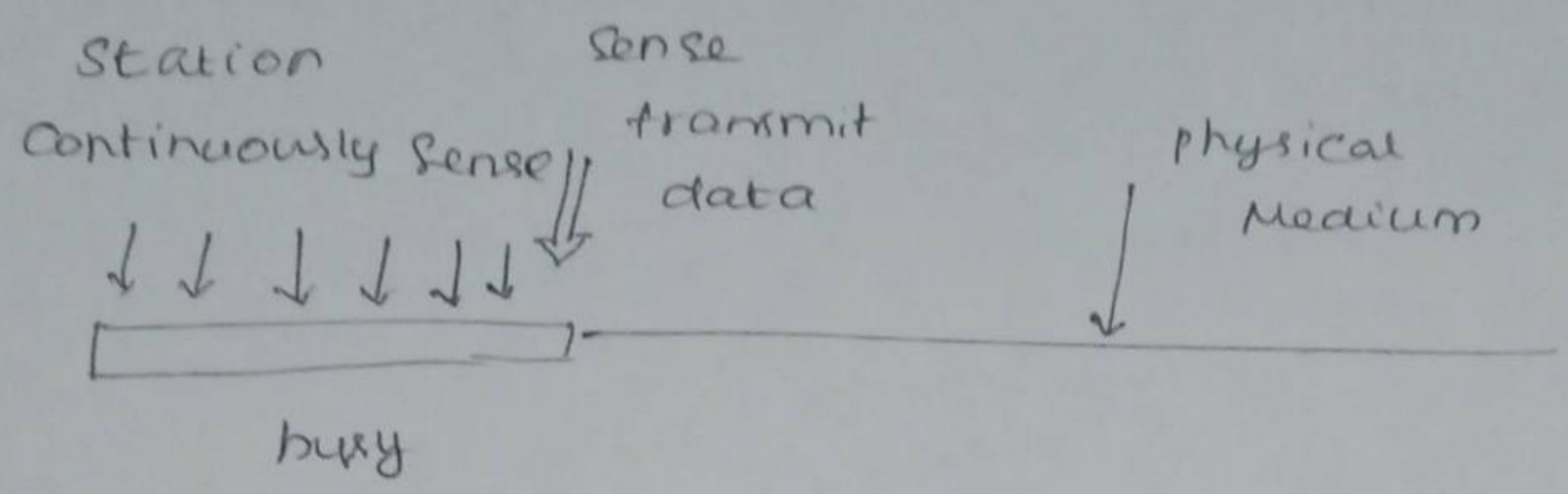
1. Non - presistent CSMA
2. 1 - persistent CSMA
3. p - persistent CSMA

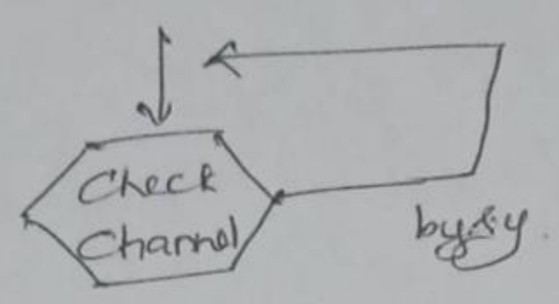
Non - persistent CSMA:



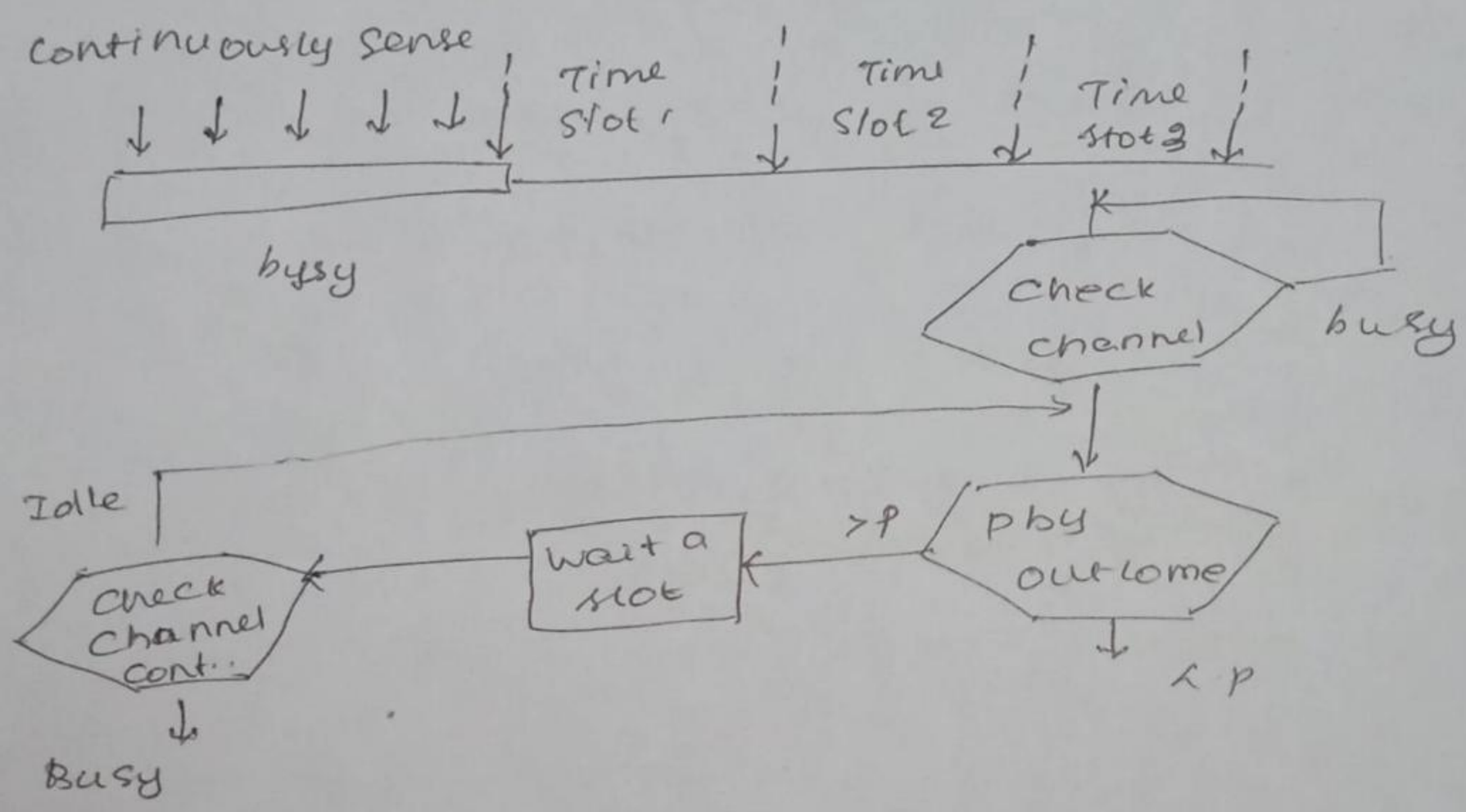


2) 1 - persistent CSMA:





3. N - persistent CSMA:



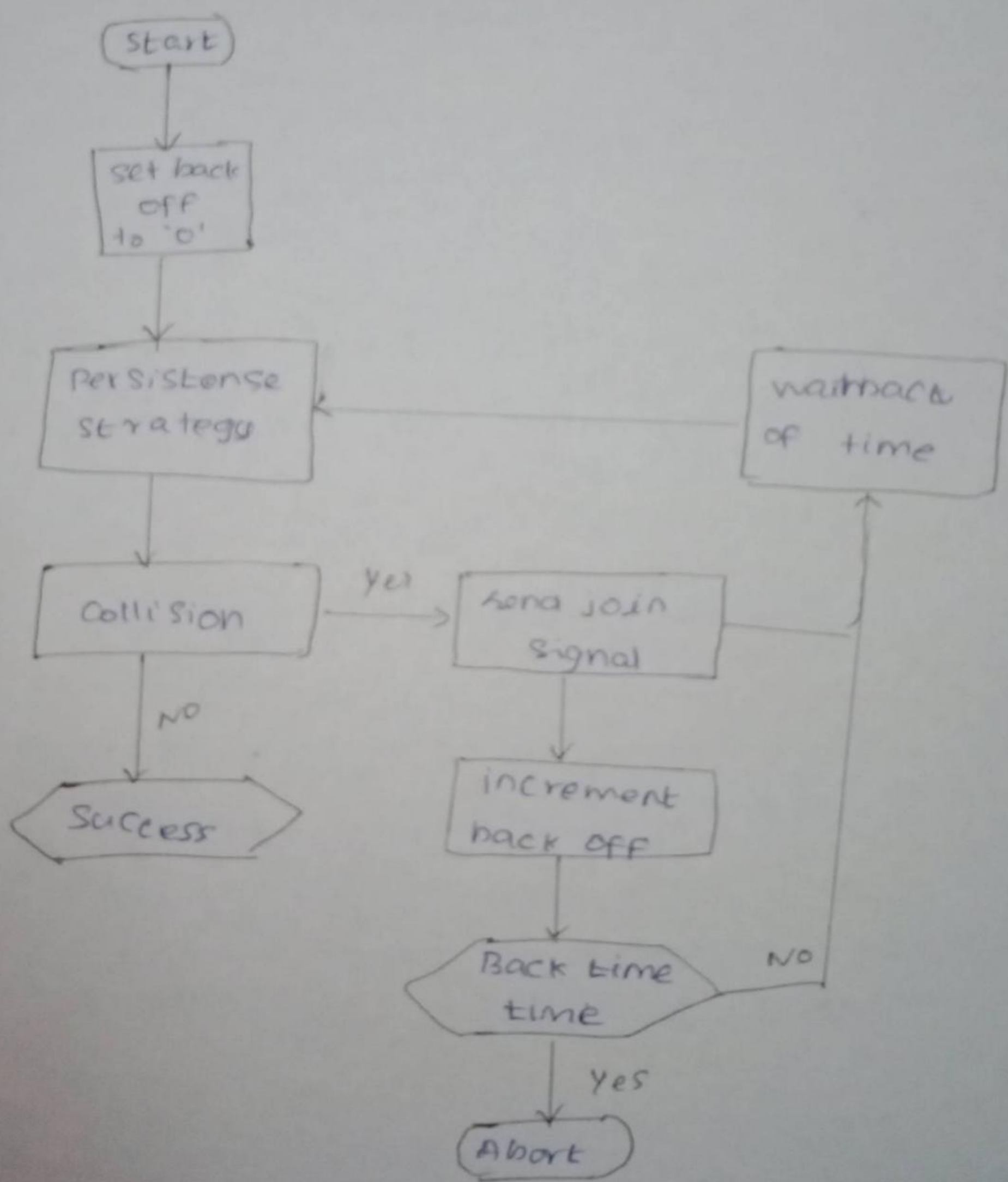
Carrier sence Multiple Access with Collision Detection.

CSMA/CD is the most commonly used protocol for LANS. CSMA/CD specifications where developed jointly by digital equipment corportion, Inter and xerox. This network is called Ethernet.

CSMA / CD Throughput:

The trough put of CSMA/CD is greater than that of pure of slotted ALOHA.

For 1 - persistant method maximum throughput is arround 50% when G=1.



Flowchart for CSMA/CD

Standared Ethernet IEEE 802.3

The original ethernet was created in 1976 at Xerox Palo Alto Reasearch Center.

a) Standared Ethernet (10 Mbps)

b) Fast Ethernet (100 Mbps)

c) Gigabit Ethernet (1 Gbps)

d) Ten-Gigabit Ethernet (10 Gbps)

MAC - Sub layer:

MAC sublayer frames data received from the upper layer and passes them to the physical layer.

Frame Format:

preamble	SFD	Destination address	source address	Length or type	Data and padding	CRC
7 byte	1 b	6 b	6 b	2 b		4 b

physical layer header

IEEE 802.3 Frame Format

preamble:

A 7 byte pattern of alternating 0s and 1s used by the receiver to establish by bit synchronization.

Start Frame Delimeter (SFD):

This indicate the actual start.

Destination Address (DA):

The DA field is also 6 byte and container the physical Address of the sender of the packet or group of address.

Source Address (SA):

The SA field also containes 6 bytes and contains the physical Address of the sender of the packet.

Length or Tybe:

Length of LLC data field in octets or Ethernet type field.

Data:

Data unit supplied by LLC.

CRC:

This field contains error detection information.

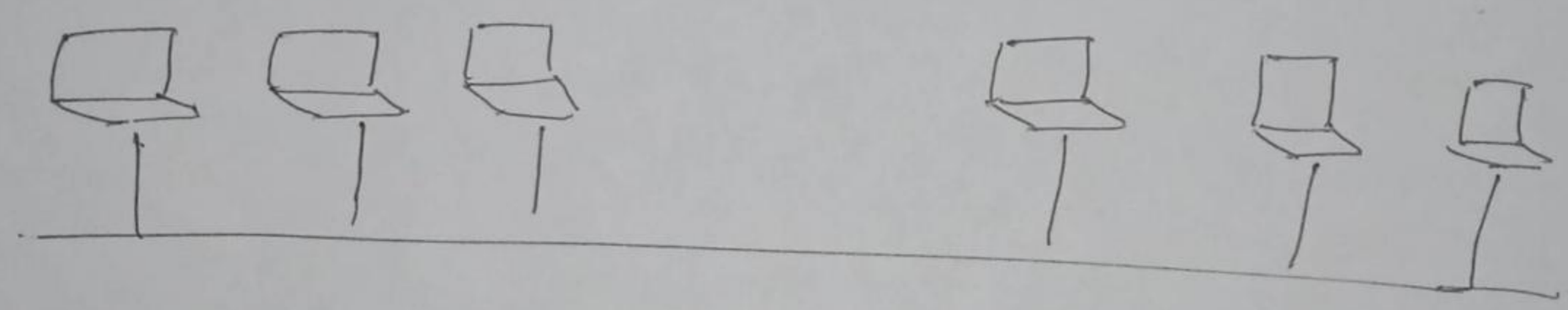
Bridged Ethernet:

Bridges have two effects on the Ethernet LAN.

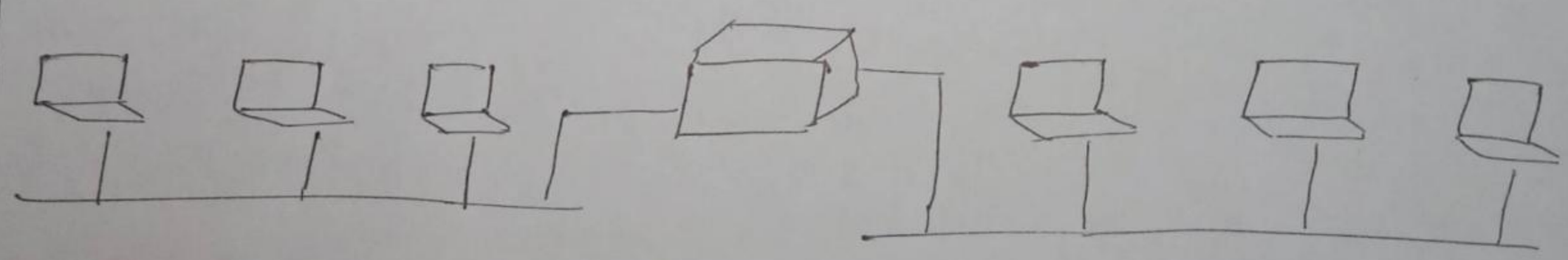
1. Raising the Bandwidth:

If only one station has frames to send, it benifits from the total capacity.

But if more than one station needs to use the network, the capacity is shared.



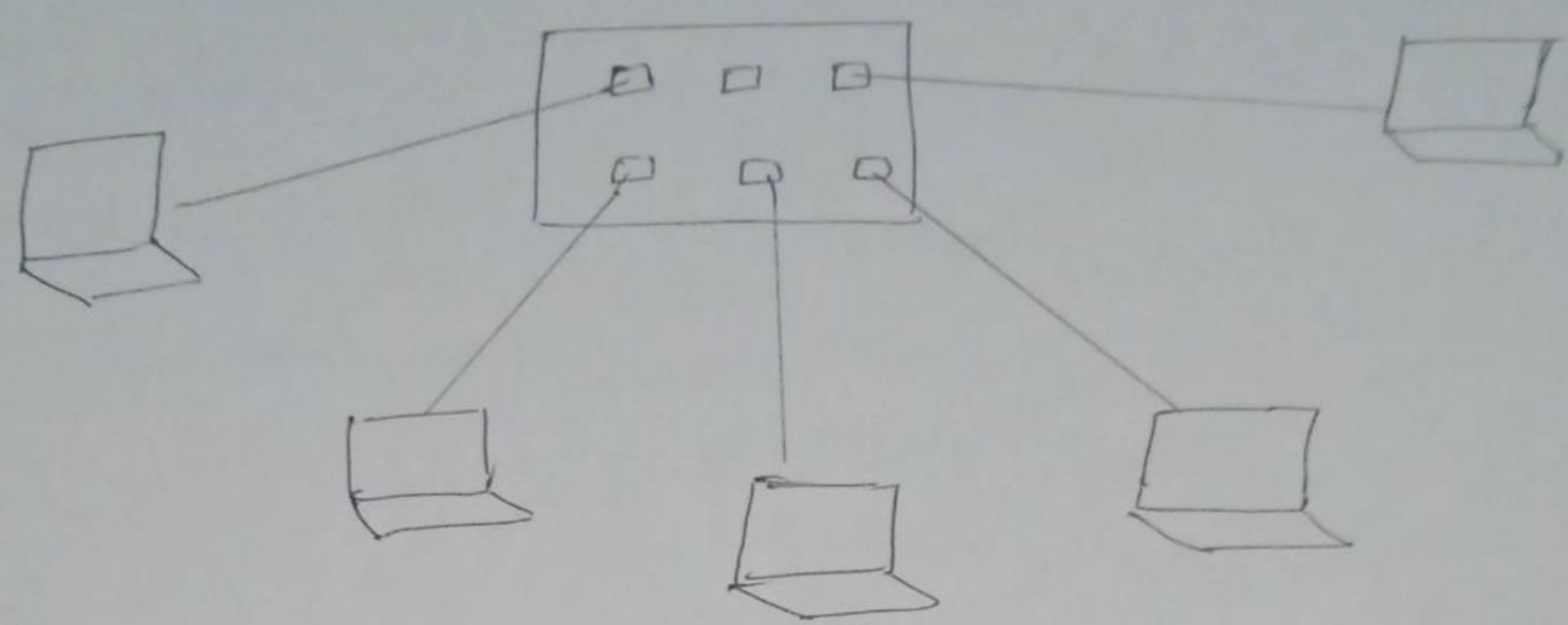
without bridge



with bridge

A bridge divides the network into two or more networks. Bandwidth-wise, each network is independent.

Switched Ethernet:



A layer-2 switch is an N-port bridge with additional sophistication that allows faster handling of the packets.

Fast Ethernet:

Fast ethernet is backword compatible with standared ethernet.

Fast ethernet refers to a set of specification developed by IEEE 802.3 committee to provide a low cost, ethernet compatible LAN operating at 100 Mbps.

A traditional ethernet is half duplex. A station can either transmit or receive a frame, but it cannot do both simultaneously.

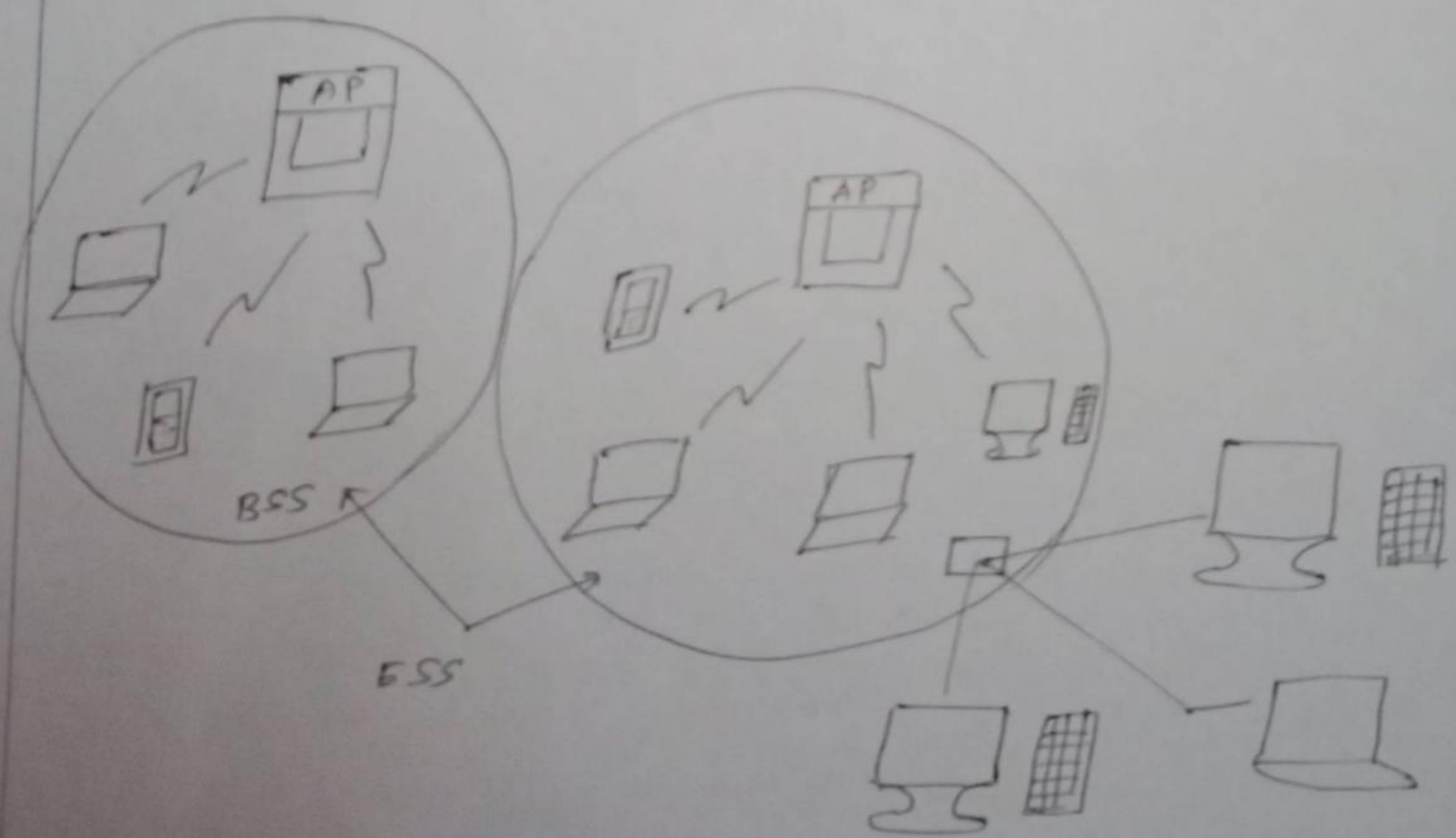
Wireless LAN

Wireless Networks have many applications. For, ex: user on the road often want to use their Laptop to send and read remote files, login on remote machines and so on.

IEEE 802.11 X:

802.11 refers to a family of specification developed by the IEEE for wireless LAN technology.

All three of the specification use carrie sense Multiple Access with Collision Detection, as the path sharing protocol.



802.11 LAN

Wireless LAN protocol:

Wireless LANs typically are not totally wireless, but instead use either radio or infrared technology to connect a node or group of nodes into the main body of the network.

Wireless networks are always an extension of cabled networks, not a replacement of them.

Requirement of wireless LAN:

1. No. of nodes
2. Throughput
3. connection to backbone LAN
4. service area

Application of WLAN:

1. LAN extension
2. cross building
3. Nomadic acces

Advantages:

1. It is a reliable type of communication
2. WLAN reduces physical wires.

Disadvantages:

1. It has limited area to cover
2. WLAN requires license

Blue tooth

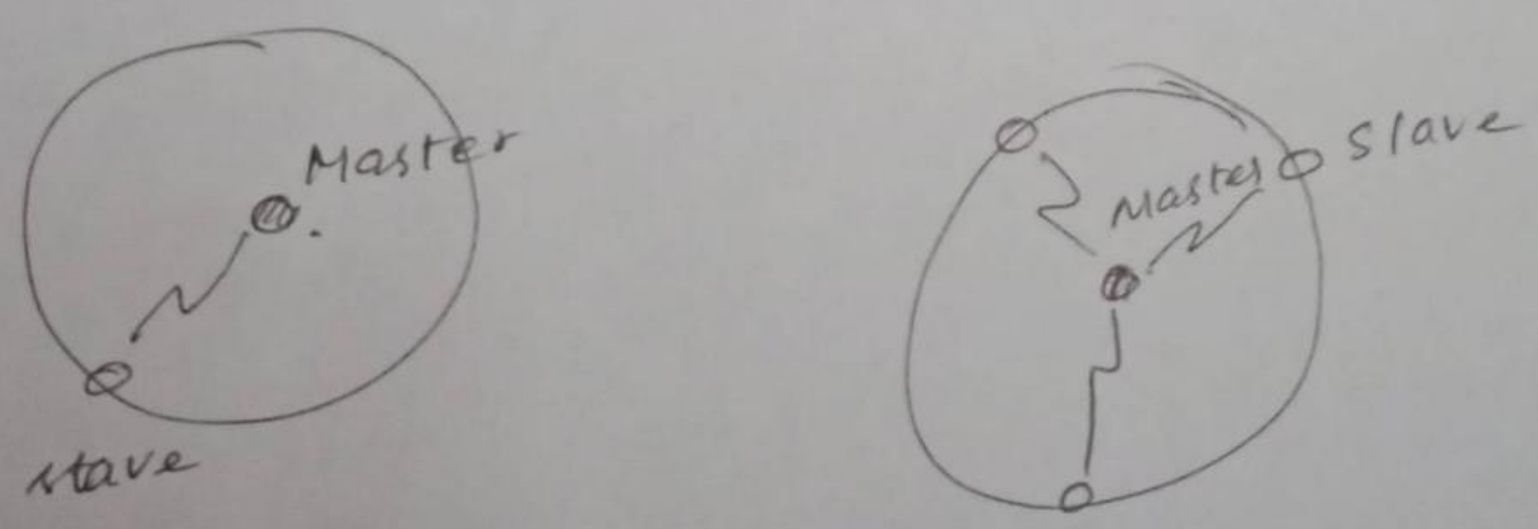
Bluetooth is a low cost, low power, shortrange wireless communication technology used in networking, mobile phones and other portable device.

Although the range of each bluetooth device is approximately 10 meters.

Different devices can be automatically link-up with each other as soon as they come into range. i.e., it creates a temporary network or personal Area Network (PAN).

Bluetooth Architechture:

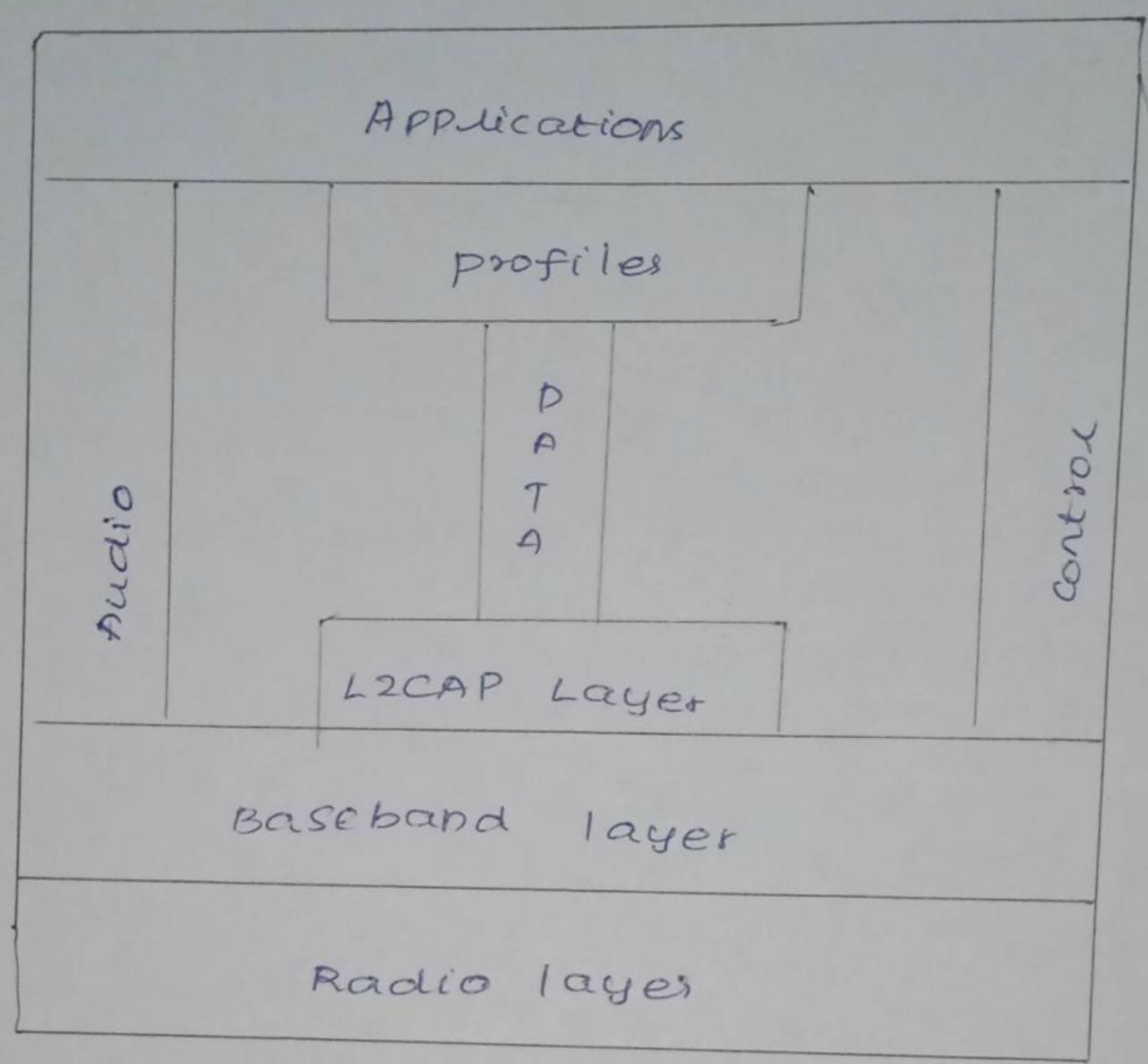
The basic element of a Bluetooth is piconet.



piconet types.

Several piconet can be estabilished and linked together is a topollogy called Scatternet

LAYER Architechture of Bluetooth



Radio layer:

Radio layer is roughly equivalent to the physical layer.

Blue tooth devices are lowe power and have a range of 10m.

Band:

Blue tooth use 2.4 GHz, ISM band.

FHSS:

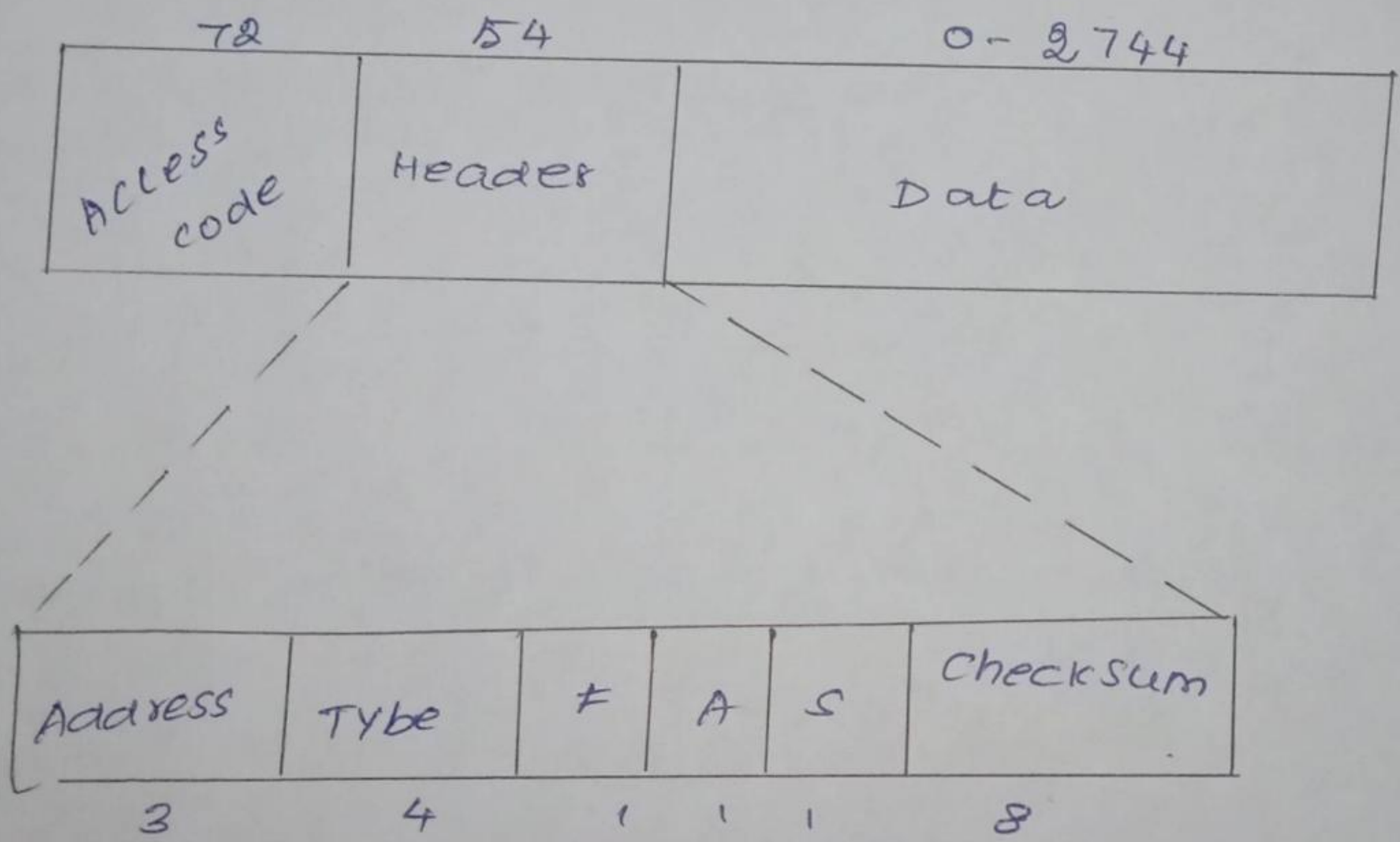
Frequency hopping spread spectrume method in the physical layer to avoid interference from other devices.

Baseband layer:

This layer is equivalent to MAC Layer in LAN. The access method is TDMA. The primary and method communicate with each other using time slots.

1. Single secondary communications.
2. Multiple secondary communications.

Frame format:



L2CAP:

L2CAP is logical control and Adaption protocol. This provides segmendation and re-assemby services to alloco large pades to pass.

Zigbee:

The IEEE 802.15.4 Standard does not standardise the higher communication protocol layers, including the network and application layers. To assure interporability between devices.

Characteristics of Zigbee:

1. Data rates of 250 kbps, 20kbps, and 40 kbps.
2. Star or peer to peer operations.
3. support for low latency devices.
4. CSMA-CA Channel access.
5. Dynamic devices addressing.
6. Fully handshaked protocol.

Device Addressing:

Two or more devices with a PSO communicating on the same physical channel constitute a WAN which includes at least one FFD independent PAN will be selected a unique PAN identifies.

Functions of physical layer:

1. Activation and deactivation of radio transiver.
2. Energy detection within the current channel.
3. Link quality indication for received packets.
4. clear channel assessment for CSMA-CA.
5. channel frequency selection.
6. Data transmission & reception.

Network Layer services:

Main Task of the Network Layer is to move packets from the source host to the destination host.

It transport from sending to receiving hosts via internet. Network Layer protocols exist in every host and route. In order to provide this service, the transport layer relies on the services of the network layer, which provides a communication services between hosts. In particular, the network layer moves to another.

x ⟶

UNIT-3

ROUTING

Routing:

A host or a router has a routing table with an entry for easy destination, or a combination of destination to route IP packets.

A static routing table contains information entered manually. The administation enters the route for each destination into the table.

Properties of routing:

1. Correctness & simplicity
2. Robustees
3. stability
4. fairness

Routing algorithm classification:

1. Static routing Algorithm
2. Dynamic routing algorithm.

Static Routing Algorithm:

In static routing the network topology determines the initial paths. The precalculated paths are then loaded to the routing table.

2 Dynamic Routing Algorithm:

Dynamic routing algorithm change their routing decision if there is change in topology traffic. each routes continuously checks the network status by communicating with neighbours.

Routing Table:

once the routing decision is made, this information is to be stored in routing table so that the routes knows how to forward a packet.

Design Goals:

1. optimality
2. simplicity & low overhead
3. Robustness & stability
4. Rapid convergence
5. Flexibility.

Routing algorithm can be programmed to adapt to changes in network bandwidth, routes queue size, network delay and other visible device

Unicast routing:

Routing table can be static or dynamic

Manual entires are done in static table.

Dynamic table is updated automatically when there is a change somewhere in the internet.

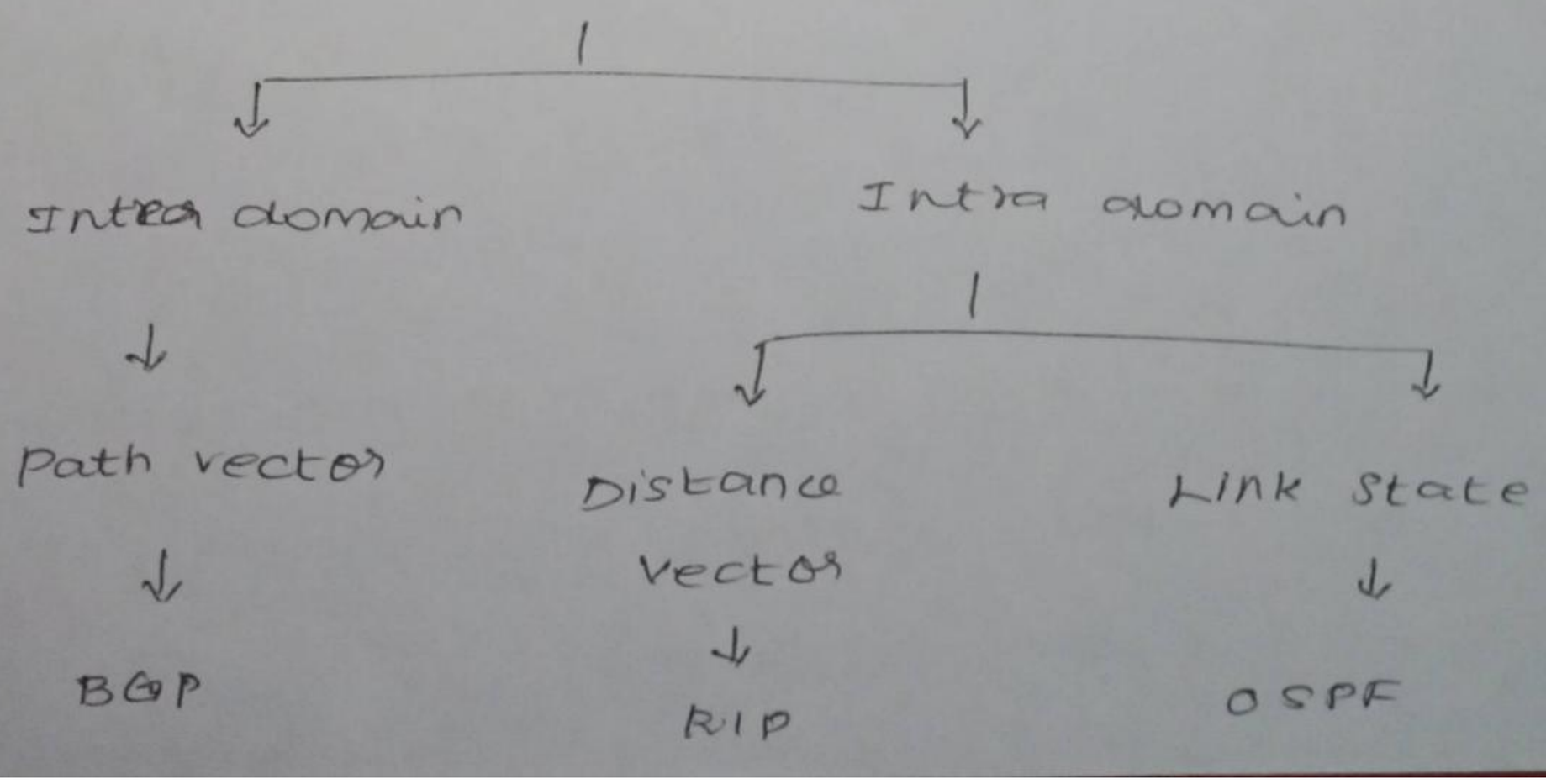
Now a day, dynamic table is used because of sudden changes in the internet.

Inter and Intra domain Routing:

An internet is divided in autonomous systems

An autonomous system is a group of networks and router under the autority of a sigle admistration.

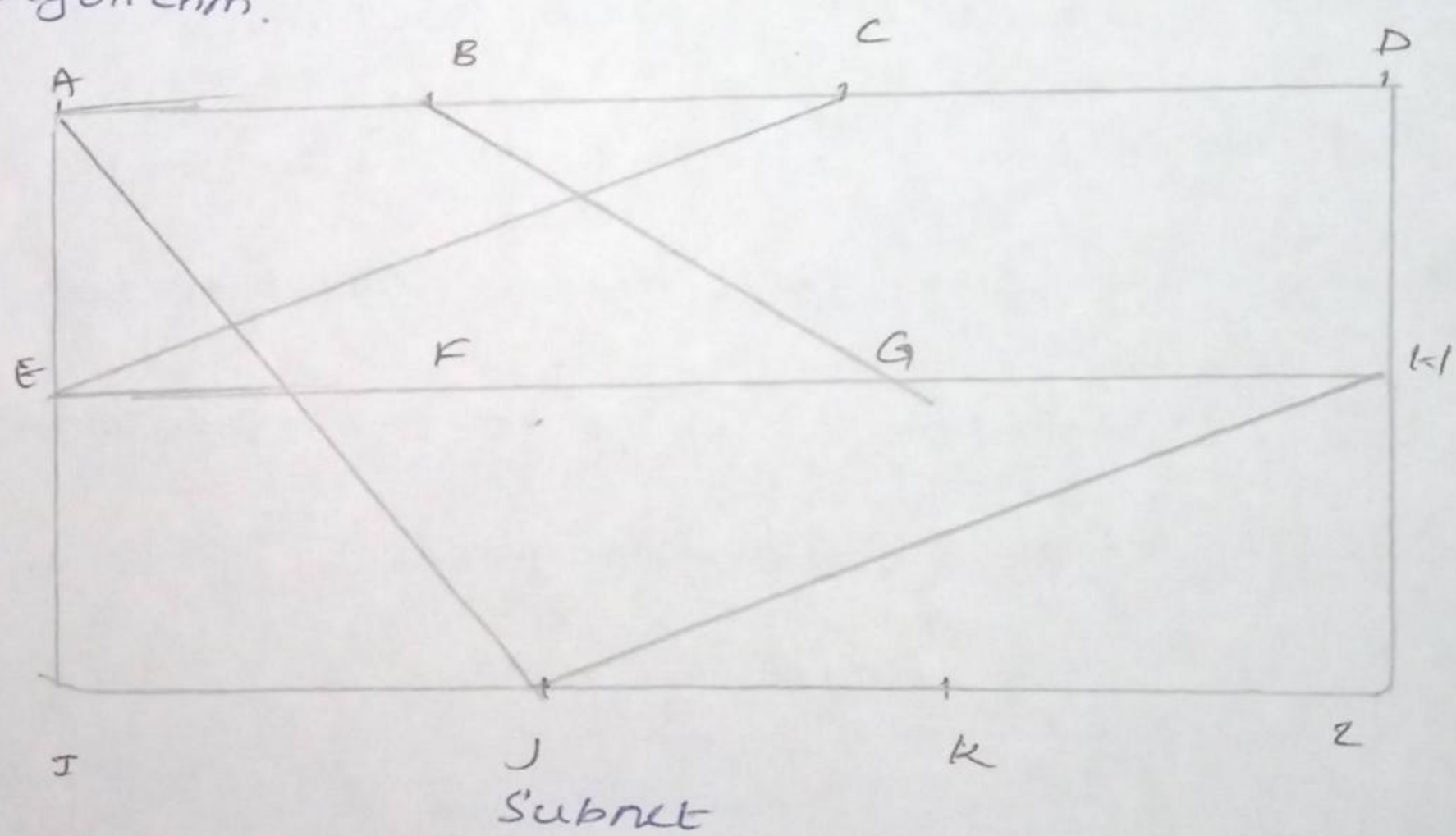
Classification of routing protocols:



Routing Algorithms

Distance vector Routing:

Distance vector routing algorithm is the dynamic routing algorithm. It was designed mainly for small network topologies. Distance vector routing algorithm is sometimes called by other names, most commonly the distributed Bellman-Ford routing algorithm & the ford-fulkerson algorithm.



Count-to-infinity problem:

An imagenetwork and denotes the distance from other routes A to every other routes. until now everything works free

Issues with the distance vector Routing:

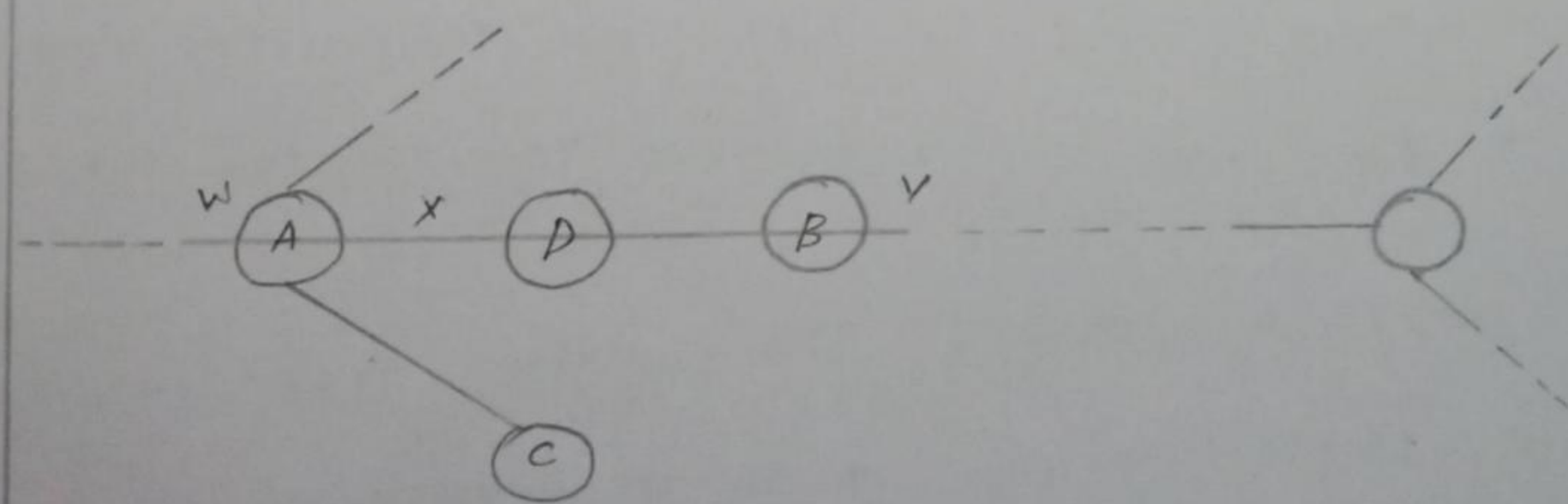
1. The primary drawback of thes algorithm is this vulnerability to the count-to-Infinity problem

2. Another drawback of this scheme is that does not take into account Link Bankwidth.

3. yet another problem with this algorithm is that it takes appreciably long time for convergence as the network-size grows.

Routing Information protocol (RIP)

In RIP, routing updates are exchanged between neighbours approximately every 30 seconds using a so called RIP response message. The response message sent by a routes or host contains a list of upto 25 destination networks within a autonomous systems (AS). Response messages are also known as RIP advertisments.



Portion of AS

RIP Message Format :

The following figure shows the RIP message format.

Command	version	Reversed
Family		All 0s
Network address		
All 0s		
All 0s		
Distance		

RPI Message Format

1. Command: This is 8 bits field specifies the type of message. 1 for request and 2 for response.

2. version: This is 8 bits field define the version.

3. Family: This 16 bits field defines the family of the protocol used. For TCP/IP the value is 2.

4. Network address: The address field defines the address of the destination network.

5. Distance: This 32 bit field defines the hop count from the advertising routes.

2. Measuring line cost:

To determine the cost for a line, a router sends a special ECHO packet over the line that the other side is required to send back immediately.

problems with the basic algorithm:

1. The sequence numbers may wrap arround, causing confusion.

2. If a router ever crashes, it will lose track of its own sequence number.

3. If a sequence number is ever corrupted and 65,540 is received instead of 4.

Some refinements to the basic algorithm make it more robust:

When a state packet comes in to a routes for flooding. It is put it is put in a holding area to wait a short while first.

If another state packet from the same source comes in before it is transferred.

If they equal, the duplicant is discarded.

If they are different, the older one is known one is thrown out.

Multipurpose Internet Mail Extensions :

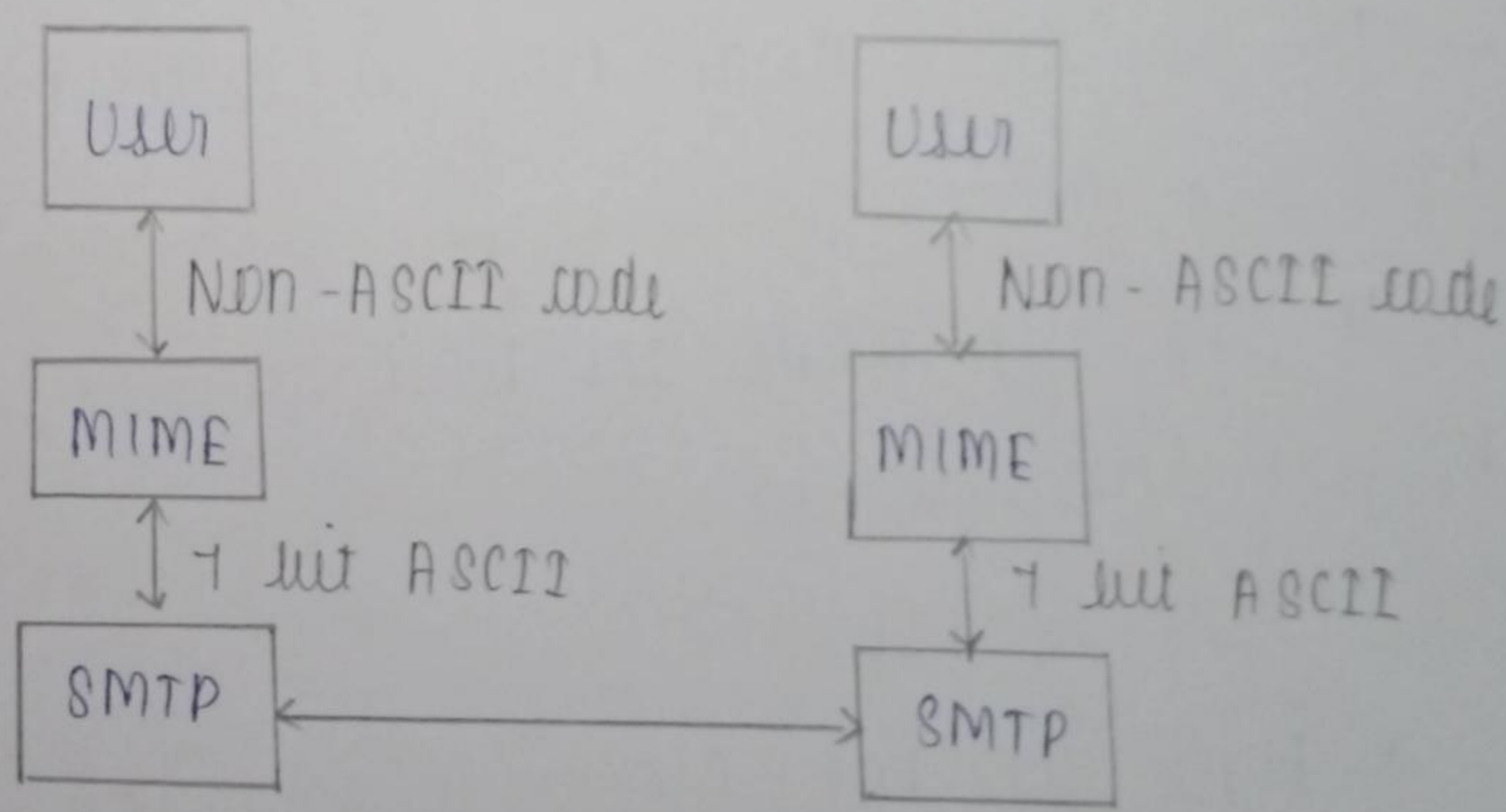
→ MIME is a supplementary protocol that allows non-ASCII data to be sent through SMTP

→ MIME defined by IETF to allow transmission of non-ASCII data via e-mail.

→ It allows arbitrary data to be enclosed in ASCII for normal transmission.

→ All media types are sent or received over the WWW are encoded using different MME.

→ Messages sent using MIME encoding include information that describes the type of data and the encoding that was used.



MIME

Post Office Protocol (POP) :-

→ POP 3 is used to transfer e-mail messages from a mail server to mail client software.

→ POP 3 begins when the user agent opens a TCP connection to the mail server on port 110.

→ POP3 progresses three parts: authorization, Transaction, update.

→ In authorization phase, user agent retrieves messages.

→ In update phase, it occurs after the client has issued the quit command, ending POP3 session.

→ POP 3 has two modes : Delete mode, keep mode.

→ In the delete mode, mail is deleted from mail box after each retrieval.

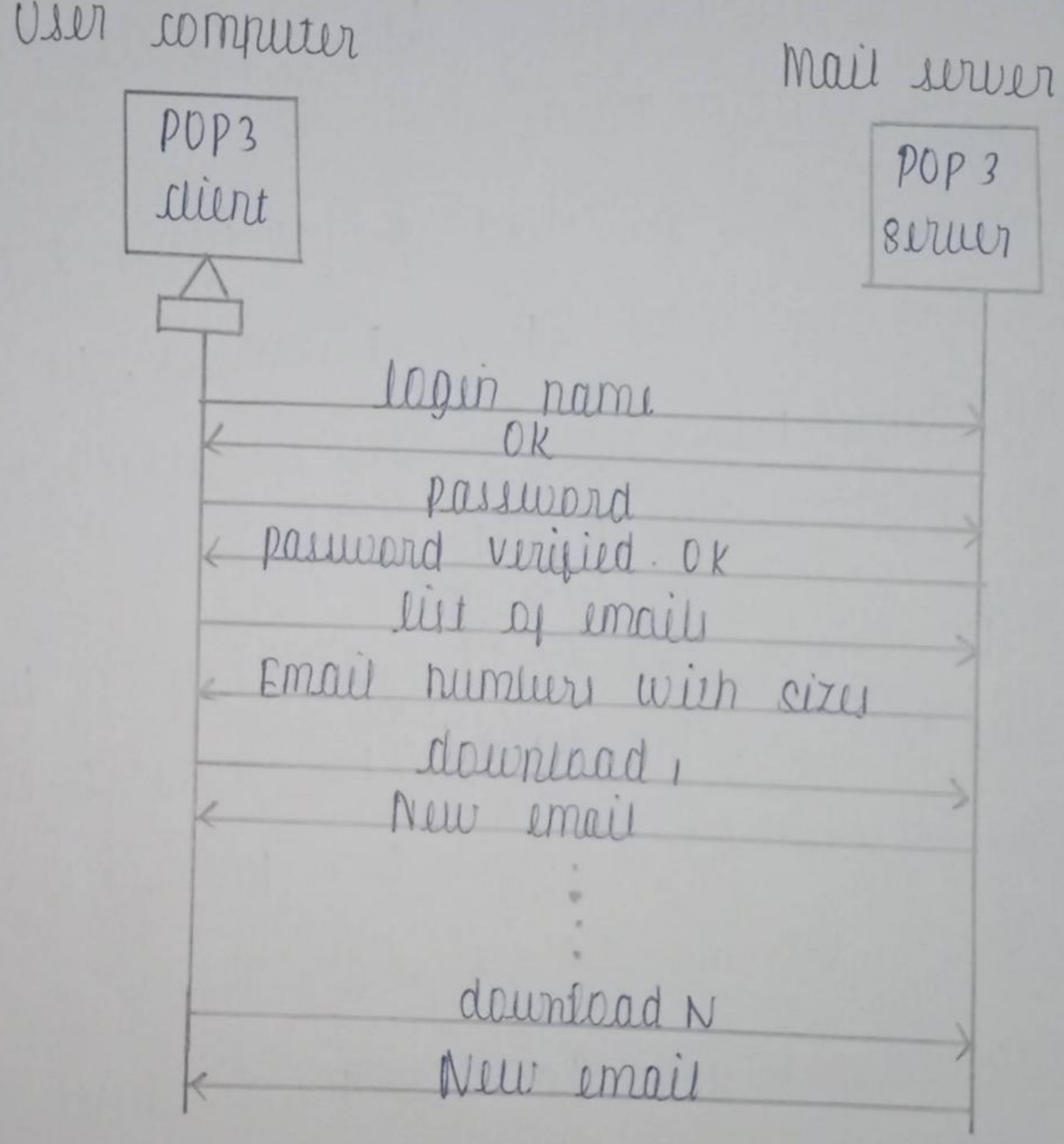
→ In the keep mode, the mail remains in the mailbox after retrieval.

Limitations of POP3 :-

* POP3 does not allow the user to organise mail on the server, the user cannot have

different folders on the server.

→ POP3 does not allow user to partially check the contents of e-mail before downloading.



IMAP :-

→ IMAP is the Internet Mail Access Protocol. IMAP4 is more powerful and more complex. IMAP is similar to SMTP.

→ It does not copy email to the user's

personal machine because user may have several.

→ An IMAP client connects to a server by TCP.

→ IMAP supports the following modes for accessing email messages : Offline mode, online mode, disconnected mode.

→ Offline mode : A client periodically connects to server to download email messages. After downloading, messages are deleted from the server. POP 3 support this mode.

→ Online mode : client process e-mail messages on the server. The e-mail messages are stored on the server itself but are processed by an application on the client's end.

→ Disconnected mode : In this mode both offline and online modes are supported.

IMAP4 provides following extra functions :-

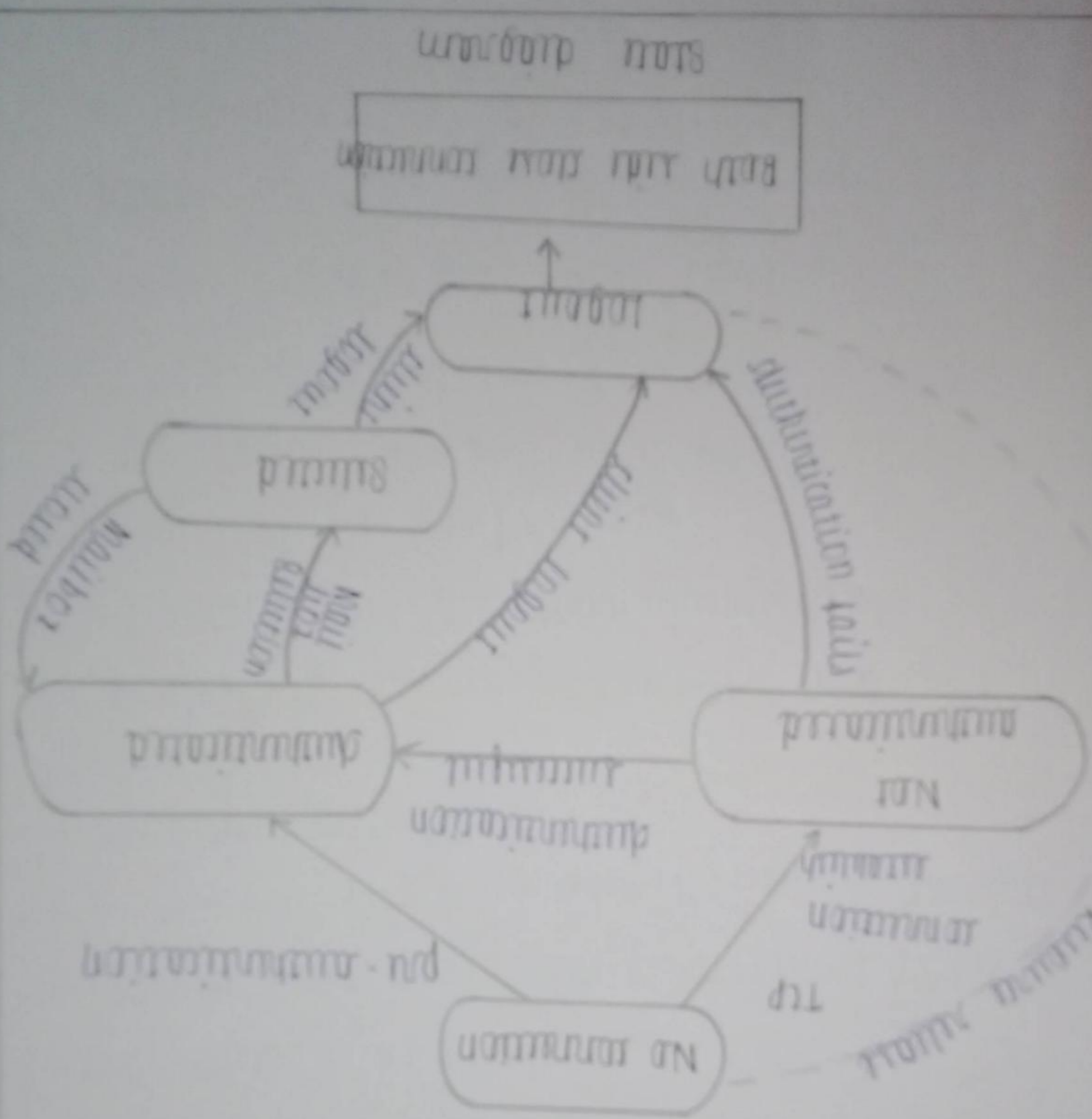
→ User can check the e-mail header prior to downloading.

→ User can partially download e-mail.

→ A user can create, delete or rename mail boxes on the mail server

→ A user can create a hierarchy of mailboxes in a folder for e-mail storage

→ User can search the contents of the email for a specific string of characters.



State diagram

Man in the middle attack :-

→ MITM attack is an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised.

→ Eavesdropping, including traffic analysis and a known - plaintext attack.

→ chosen ciphertext attack, depending on what the receiver does with message decrypts.

→ Substitution attacks

→ Replay attacks.

→ Denial of service attack. The attacker may for instance jam all communications before attacking one of the parties.

→ The defence is for both parties to periodically send authenticated status messages and to treat their disappearance with paranoia.

→ MITM is typically used to refer to active manipulation of the messages, rather than passively eavesdropping.

Cryptography and Network security :-

(i) confidentiality :-

→ confidentiality refers to limiting information access and disclosure to authorized users and preventing access by or disclosure to unauthorized.

→ Sensitive information should be kept secret from individuals who are not authorized.

→ Underpinning the goal of confidentiality are authentication methods like user IDs and passwords that uniquely identify a data system's users and supporting control methods that limit each identified user's access to the data system's resources.

→ confidentiality is not only applied to storage of data but also applies to the transmission of information.

→ confidentiality means that people cannot read sensitive information, either when it is on a computer or while it is travelling across a network.

Integrity :-

→ Integrity refers to trustworthiness of information

→ Integrity should not be altered duration.

→ It includes the concept of data integrity namely that data have not been changed inappropriately, whether by accident or deliberately malign activity.

→ It also includes origin or source integrity that is, the data actually came from the person or entity you think it did, rather than impostor.

→ Integrity ensures that information is not changed or altered in transit. Under certain attack models, an adversary may not have to power to impersonate an authentication party or understand a confidential communication, but may have the ability to change the information being transmitted.

→ On a more restrictive view, however integrity of an information system includes

only preservation without corruption of whatever was transmitted or entered into the system, right or wrong.

Availability :-

→ Availability refers to the availability of information resources. An information system that is not available when you need it is almost as bad as none at all.

→ Availability means that people who are authorized to use information are not prevented from doing so. It may be much worse, depending on how reliant the organization has become on a functioning computer and communication infrastructure.

→ Almost all modern organizations are highly dependent on functioning information systems. Many literally could not operate without them.

→ Availability, like other aspects of security

may be affected by purely technical issues.
Eg: a malfunctioning part of a computer or communication device, natural phenomena or human causes.

Security attacks :-

→ computer based systems have three valuable components : Hardware, software and data.
→ Securities of these components are evaluated in terms of vulnerability, threats, attacks.
→ An assault on system security that drives from an intelligent threat, an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system.

Asset :-

→ Asset means people, property and information.
→ People may include employees and customers along with invited persons such as guests.

maintaining ongoing security, allowing the people responsible for security of one's resources.

Threat :-

→ Anything can exploit vulnerability, intentionally or accidentally and obtain damage or destroy an asset.

→ Threat refers to the source and means of a particular type of attack

→ A threat assessment is performed to determine the best approaches to securing a system against a particular threat or class of threat.

→ A potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm.

→ Threats come in many forms, depending on their mode of attack. From viruses to trojans, spyware and bots, threats have evolved into sophisticated programs intended to computers.

Firewalls :-

→ Information systems in an organization have changed very rapidly over the years from centralized data processing, LANs, WANs.

→ A firewall is inserted between the internet and LAN for security purpose. The firewall protects the LAN from internet based attacks and also provides security and audits.

→ A firewalls may be a hardware or a software program running on a server host computer. A firewall is placed at junction or gateway between the two networks.

→ A firewall must have atleast two network interfaces one for the network it is intended to protect and one for the network it is exposed.

→ The term firewall comes from the fact that by segmenting a network into different physical subnetwork.

capabilities of firewall:-

→ A firewall examines all traffic routed between the two networks to see if it meets the certain criteria.

→ A firewall filters both inbound and out bound traffic. It can also manage public access to private networked resources

→ Firewalls can filter packets based on their source and destination addresses and port numbers. This is known as address filtering.

→ Firewalls can also filter specific types of network called protocol filtering because the decision to forward or reject traffic is dependent upon the protocol used.

Example: HTTP, FTP, Telnet.

→ Firewalls can also filter traffic by packet attributes or state.

Unit - IV

Transport layer.

Overview of Transport layer:

→ Transport layer protocol provides for logical communication between application processes running on different hosts.

→ logical communication : communicating processes are not physically connected to each other from the applications view point

→ Application processes use the logical communication provided by the Transport layer to send messages to each other.

→ Transport layer is the 4th layer in OSI.

→ It is responsible for reliable data delivery

→ The upper layer protocol depends heavily on the Transport layer protocol.

Functions of Transport layer:

→ This layer breaks message into packet

→ It performs error recovery, if the lower layer are not adequately error free.

→ function of flow control if not done adequately at the network layer.

→ function of multiplexing and Demultiplexing sessions together

Parameters used for communication.

1. local host
2. local process
3. Remote host
4. Remote process.

communication mechanism through the Internet:

Data Delivery systems collect, manage & electronically distribute the information that keeps everyone in your network informed and aware.

Delivery of Data is done in 3 ways.

1. node to node delivery.
2. host to host "
3. process to process delivery

Node to Node delivery:

At the data link level, delivery of frames take place btwn two nodes connected by a point-point link

2. Host to Host delivery :-

At the network level, datagram delivery can take place between two hosts by using IP address from user's point of view.

3. Process to process delivery:

At the Transport level, communication can takes place btwn processes or application programs by using port addresses.

Addressing method :-

→ address need to deliver something to one specific destination among may. All the layer. uses different addressing methods.

→ DLL uses a MAC address.

→ Network layer uses a IP address.

→ Transport layer uses port number.

→ port number from 0 to 65535 is used in the internet. It is 16 bits integer. so the range is 0 to 65535.

→ The client program defines itself with a port number, chosen randomly by the Transport layer software running on the client host.

IANA Ranges:

The internet Assigned Number Authority has divided the port number into three ranges.

a) well-known parts
b) Registered parts
c) Dynamic parts.

Well-known port

→ Range : 0 to 1023.
→ Assigned & controlled by IANA

Registered port

→ Range : 1024 to 49151
→ Not assigned and controlled by IANA
→ only registered to prevent duplication.

Dynamic :

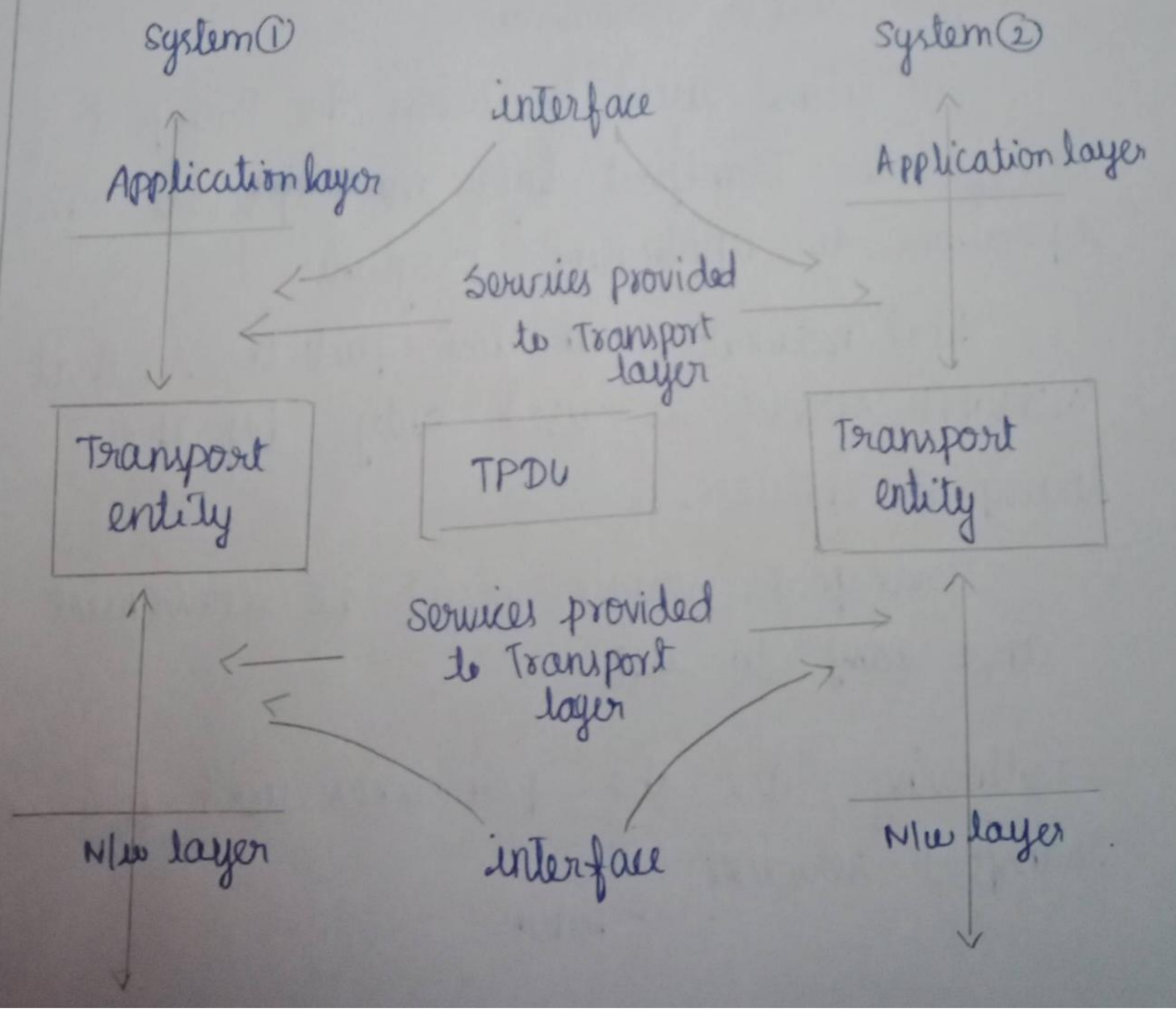
→ Range : 49152 to 65535
→ Neither controlled and nor registered.
→ Used by any process.
→ There are ephermeral ports.

THE TRANSPORT SERVICES:-

The transport protocol should provide to higher level protocols. The transport entity provides services to transport service users.

The hardware and software within the transport layer that does work is called Transport entity.

It can be in the OS Kernel, in a seperate user process or on the network interface card.



The following categories of service are useful for describing the transport service

1. Type of service
2. Quality of service
3. Data Transfer.
4. User interface.
5. Connection management
6. Expedited delivery
7. status reporting
8. security

Transport service primitives :-

To allow users to access the Transport service, the Transport layer must provide some operations to application programs.

Real networks can lose packets, so that network service is used only by the transport entities.

Transport service must be convenient and easy to use.

Following are the primitives used for simple transport service.

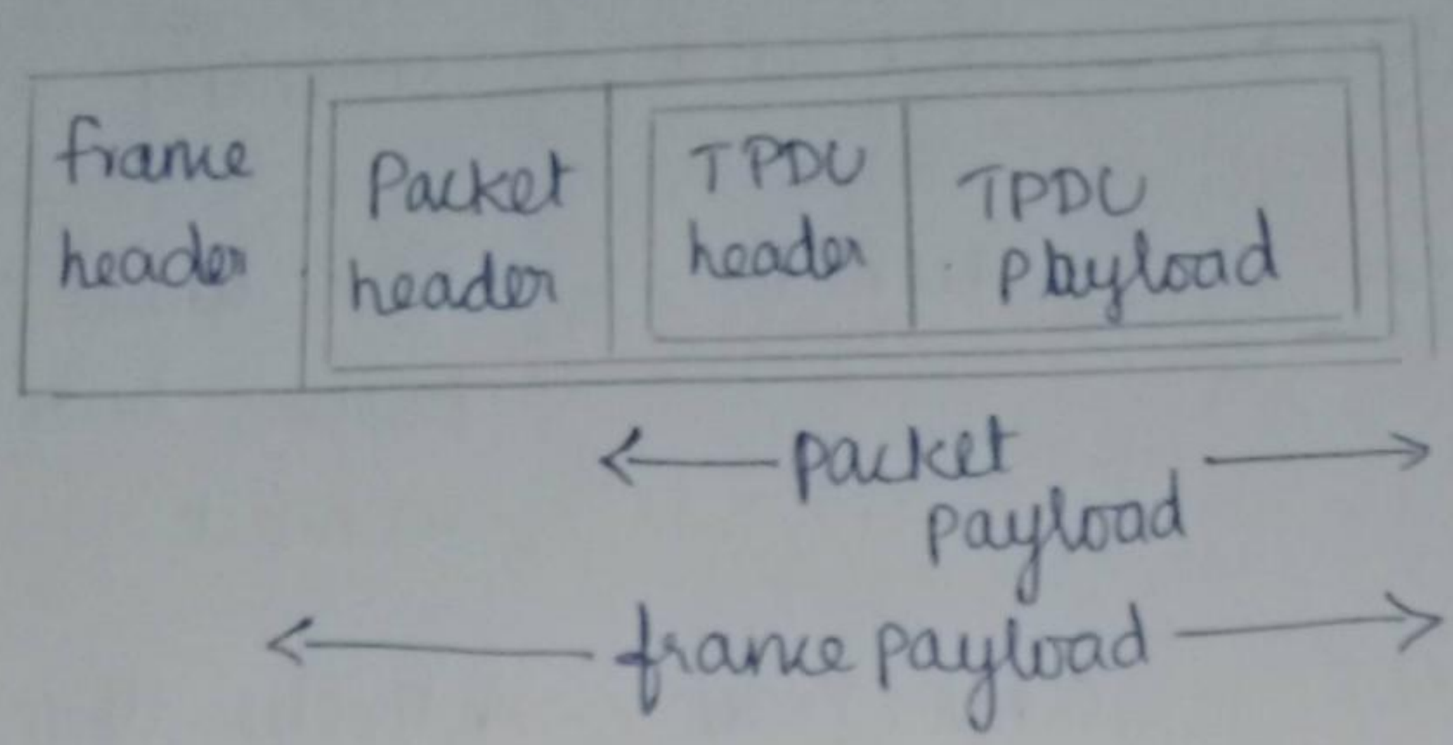
Primitive	Packet send	Meaning:
LISTEN	(None)	Block untill some process tries to connect
CONNECT	CONNECTION REQ.	Actively attempt to establish a connection
SEND	DATA	send information
RECEIVE	(None)	Block untill a data packet arrives
DISCONNECT	Disconnection REQ.	The side wants to release the connection

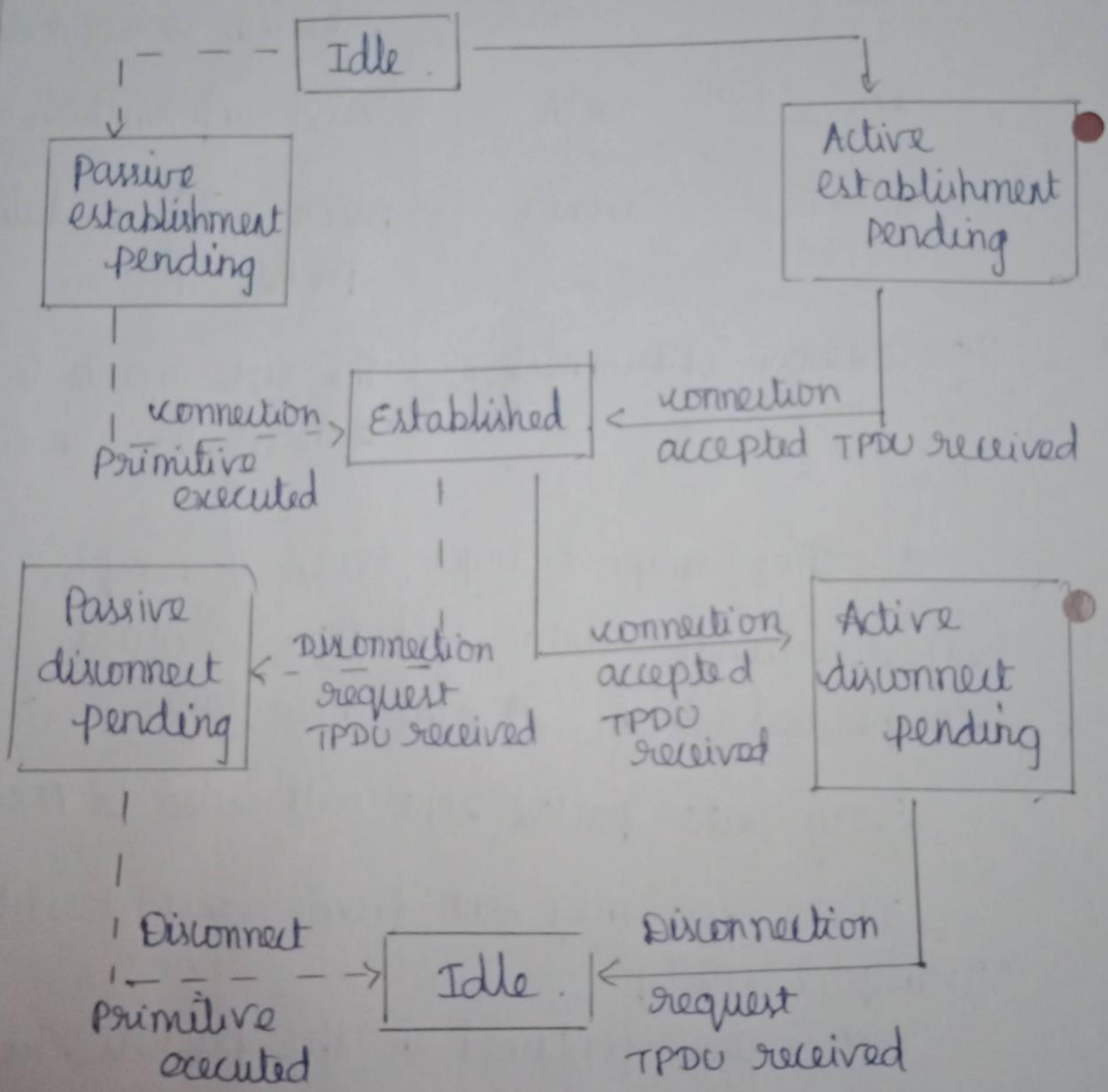
· At the Transport layer, even a simple unidirectional data exchange is more complicated than at the n/w layer.

Every data packet sent will also be ACK.

TPDU for msg sent from Transport entity to Transport entity.

TPDU are contained in the packets. Packets are contained in frames.





it shows the state diagram for a simple

connection management scheme.

when the connection is no longer needed, it must be realised to free up table space within the two transport entities

Disconnection has two types

1. Assymetric
2. Symmetric.

Socket :

Sockets are the end ports of internet communication.

connection are communication links that are created over the internet using TCP

→ Before an application program can transfer any data, it must first create an end point for communication by calling socket.

Its prototype is :

```
int socket(int family, int type, int protocol);
```

→ After creation, the bling s/m call can be used to assign an address to the socket.

```
int bind (int sd, struct sockaddr*name,
                                int namelen);
```

→ A client establishes a connection on a socket by calling connect

```
int connect(int sd, structure sock addr* name,
                                int namelen);
```

→ for connection-oriented, connect attempts to establish virtual ckt between client & server

```
int listen(int sd, int backlog);
```

→ server can accept the connection request.

```
int accept(int sd, struct sock addr* addr,
                                int* addrlen);
```

→ socket is closed by using close system call

```
int close(int sd);
```

TRANSPORT LAYER PROTOCOLS.

1. Transmission control protocol (TDP)
2. User Datagram Protocol (UDP)
3. Stream Control Transmission Protocol (SCTP)

1. TDP

→ it is a reliable connection oriented protocol that allows segment on one machine to be delivered without error

on any other machine in the internet

② UDP :-

UDP is an unreliable connectionless protocols. for applications that do war TCP's sequencing or flow control and wish to provide their own.

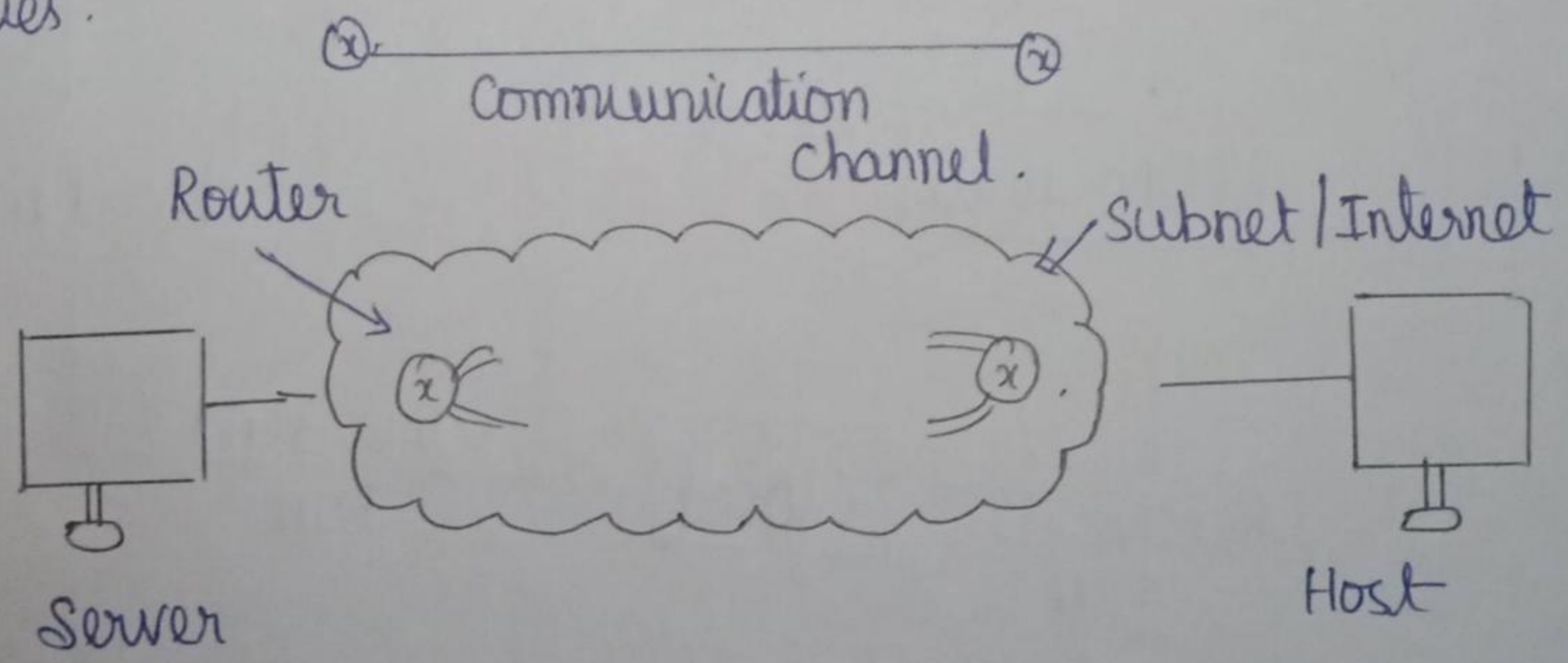
③ SCTP

SCTP provides for newer application such as voice over the internet.

It combines the best features of UDP & TDP

ELEMENTS OF TRANSPORT PROTOCOLS :-

The Transport service is implemented by a transport protocol used btwn two transport entities.



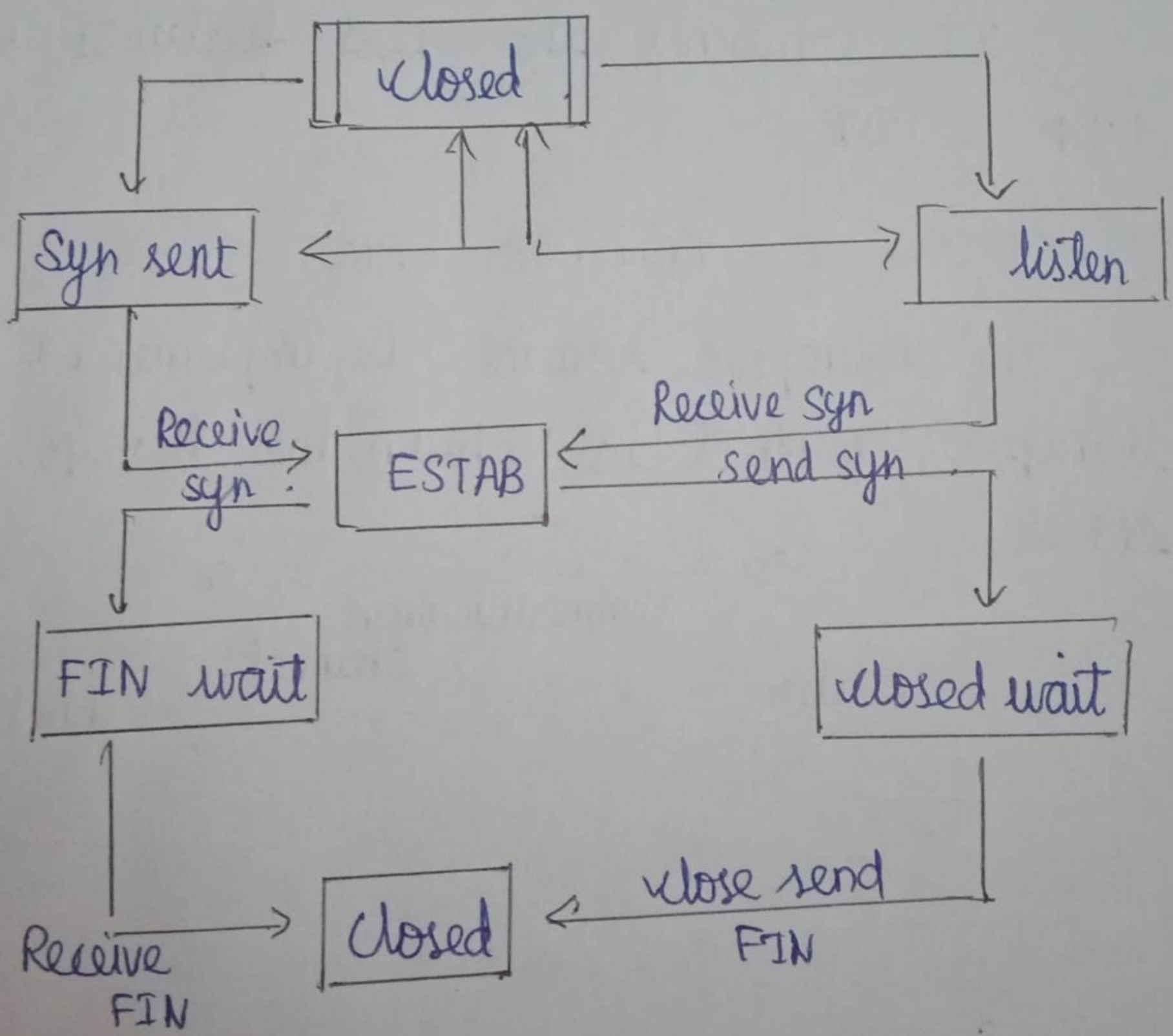
connection establishment :-

it requires 3 main purposes.

① it allows each end to assure that the other exists

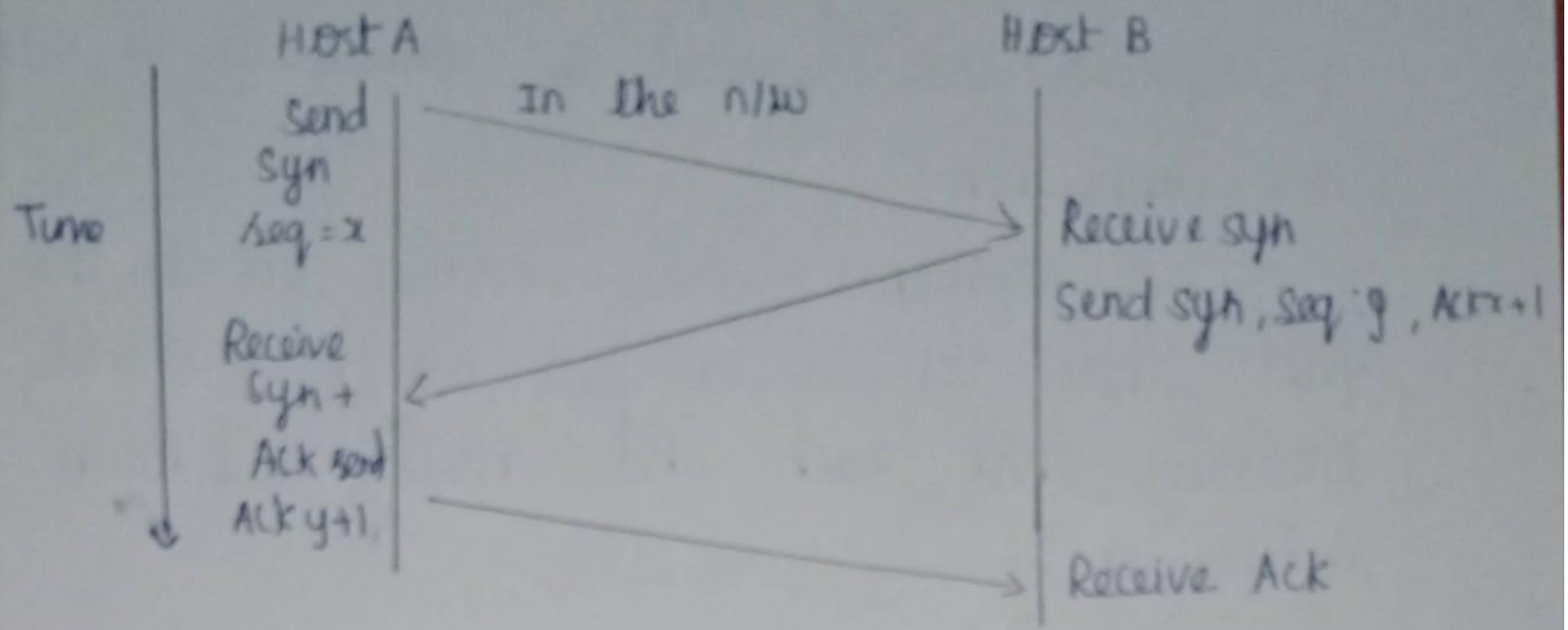
② it allows negotiation of optimal parameter like maximum segment size, max window size & OS

③ it triggers allocation of transport entity resources like buffer space.

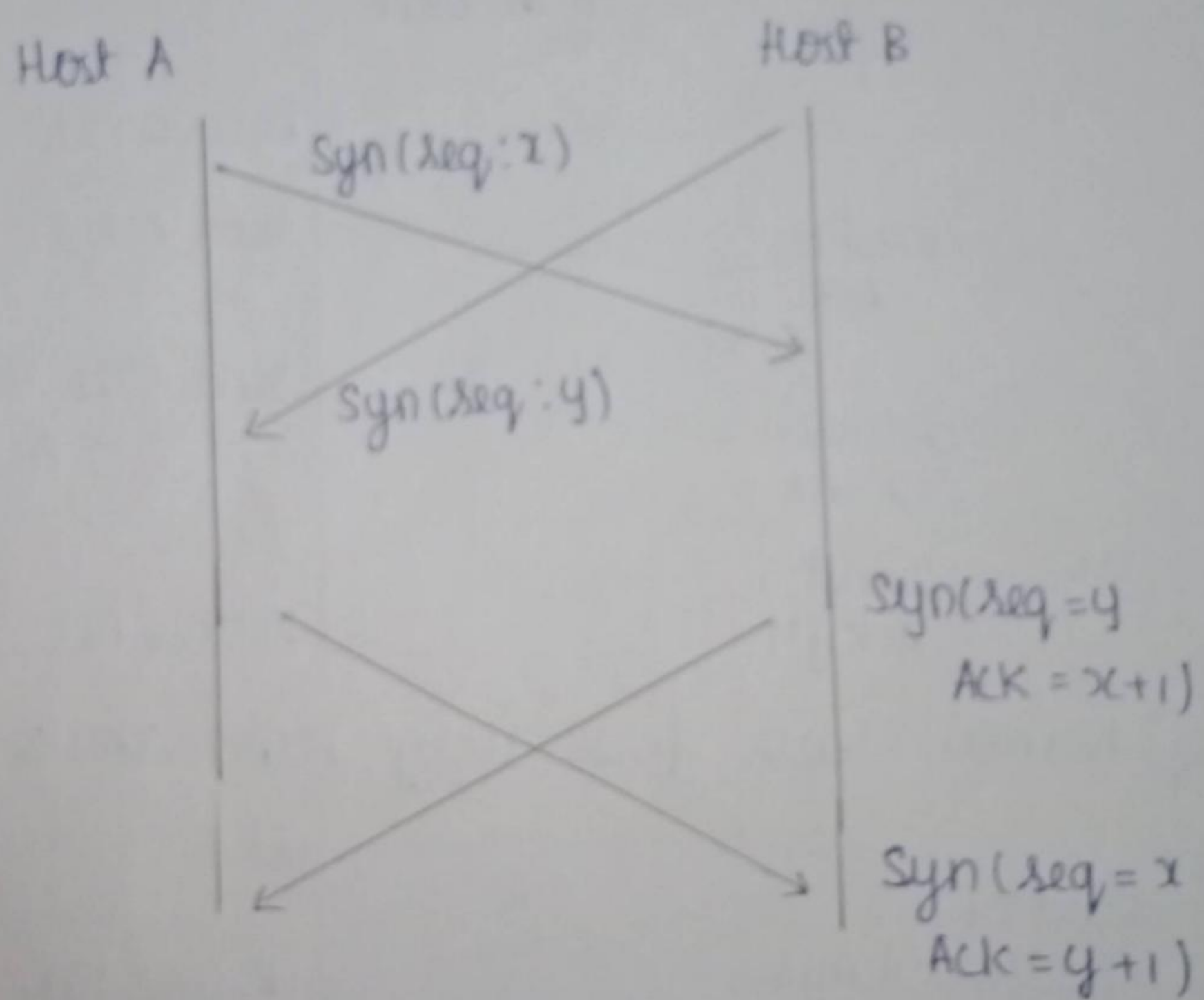


state diagram for simple connection

TCP connection establishment



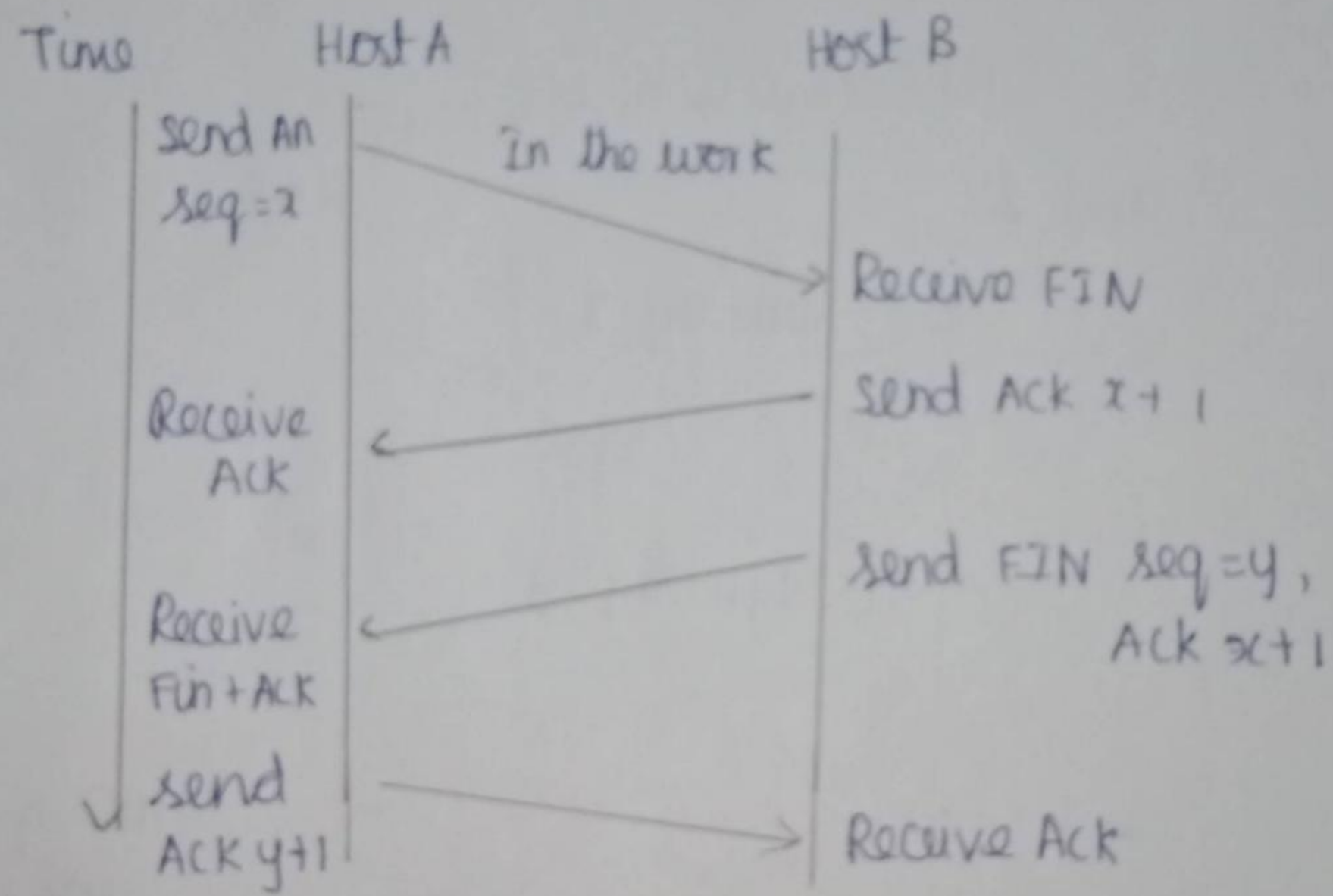
Call collision



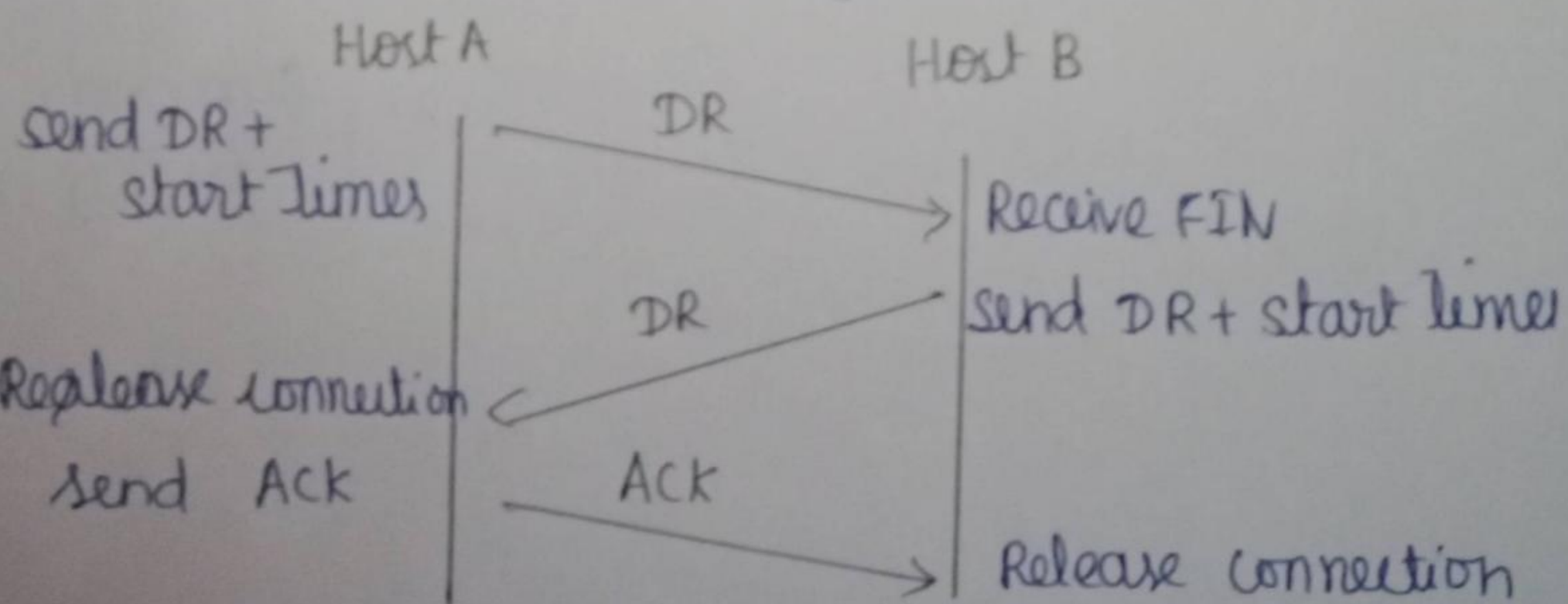
Connection Termination (14)

In order for a connection to be released, 4 segments are required to completely a close a connection.

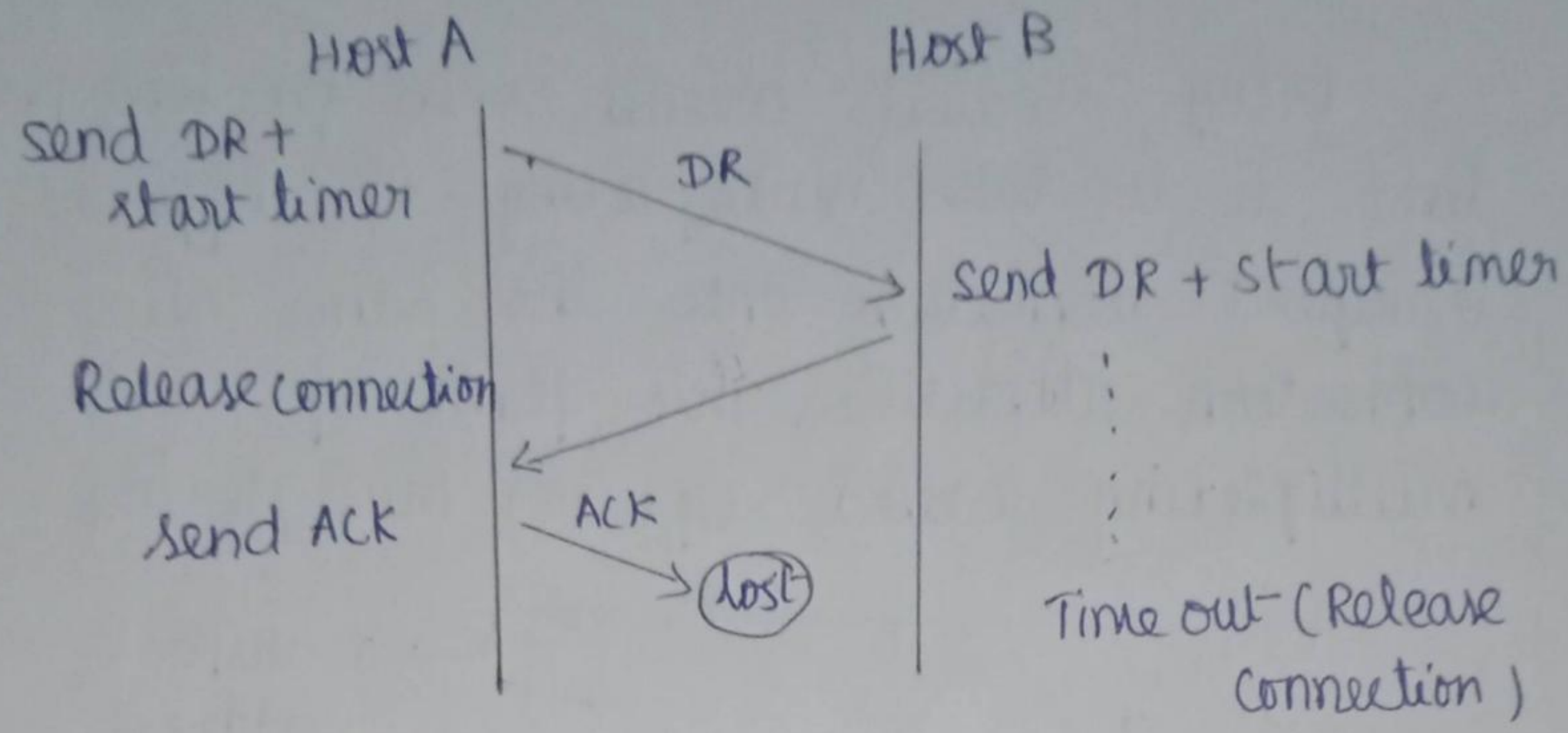
4 segments are necessary due to the fact that TCP is a full duplex protocol meaning that each and must shutdown independently.



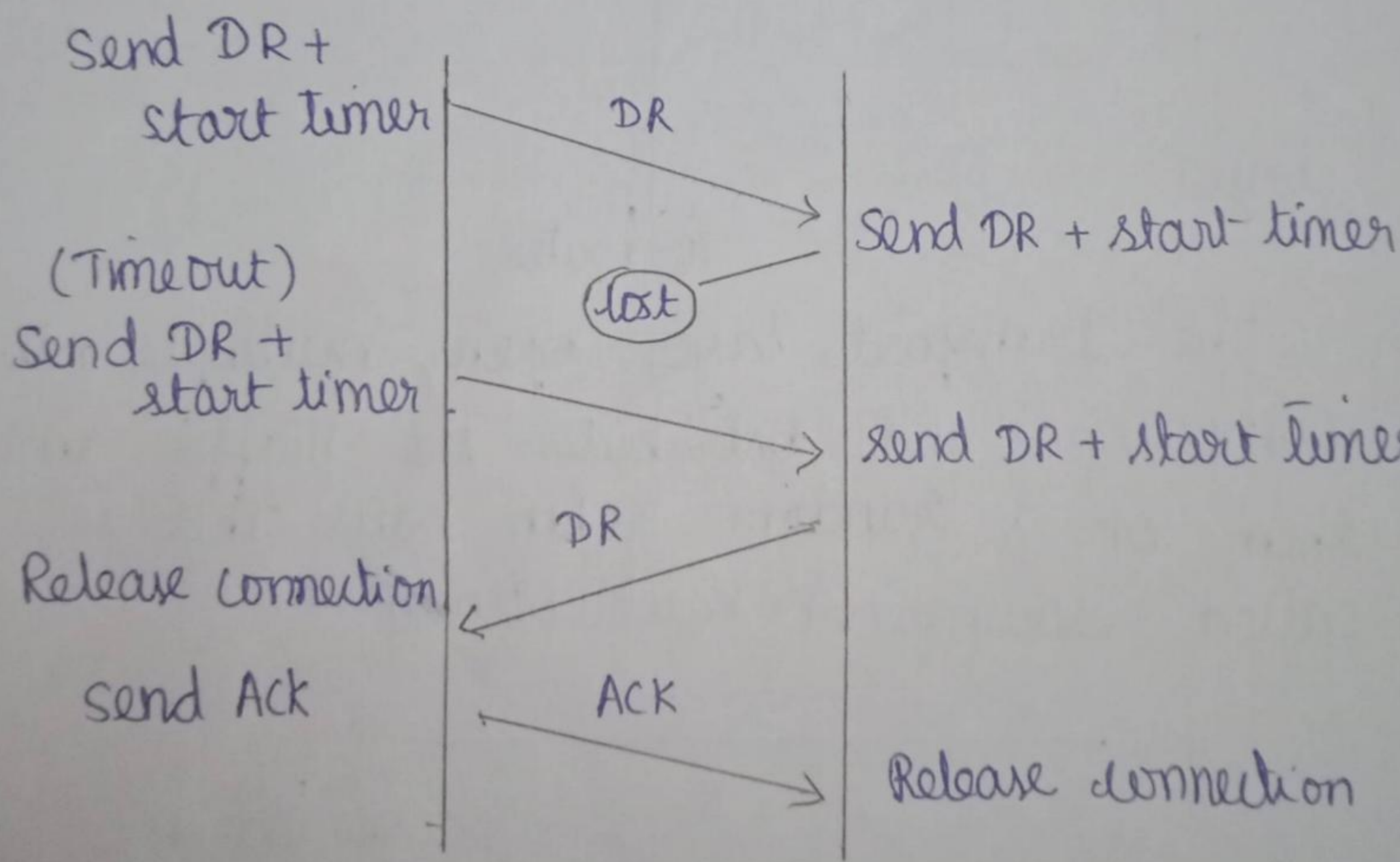
① Normal case three way band shake



② find ACK lost

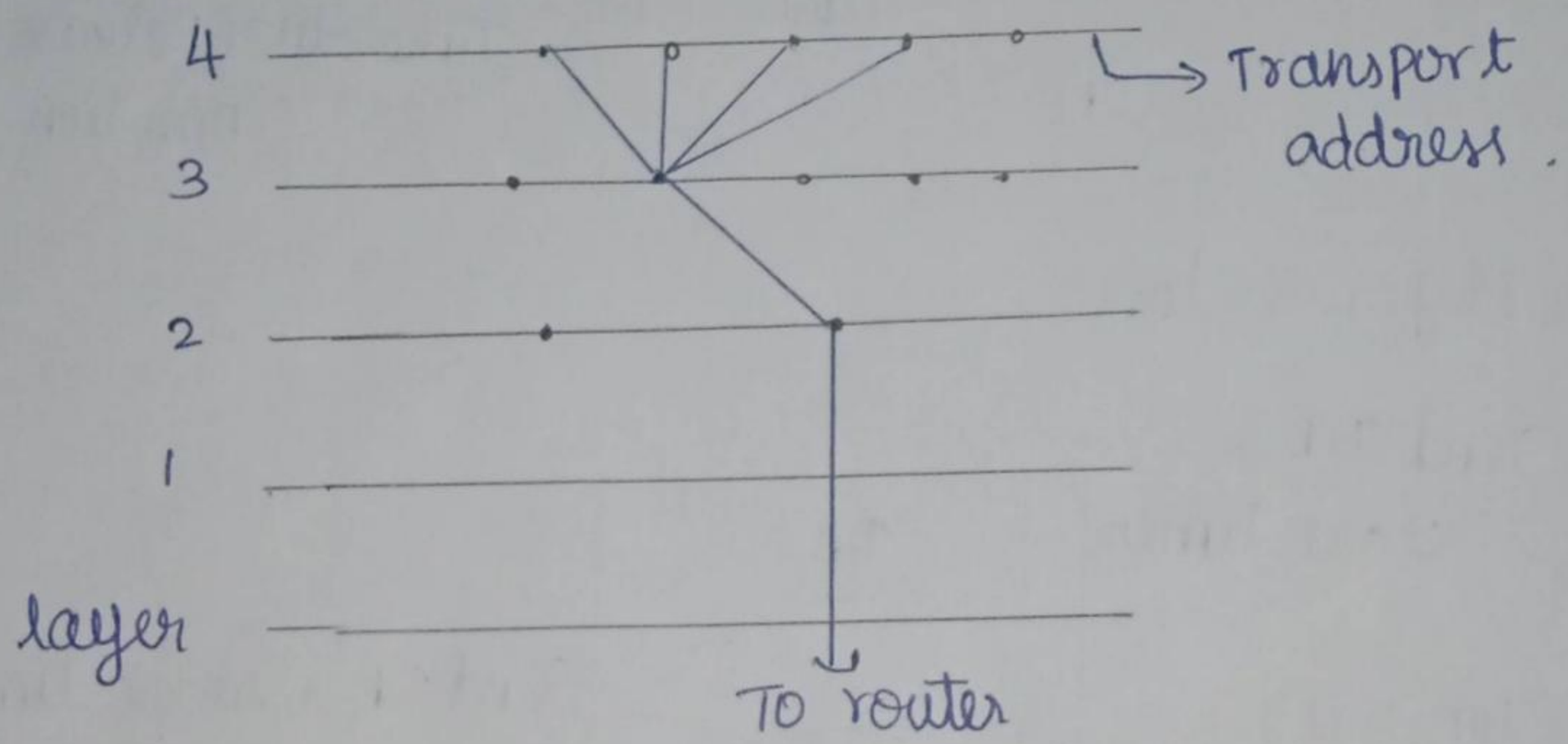


③ Response loss.

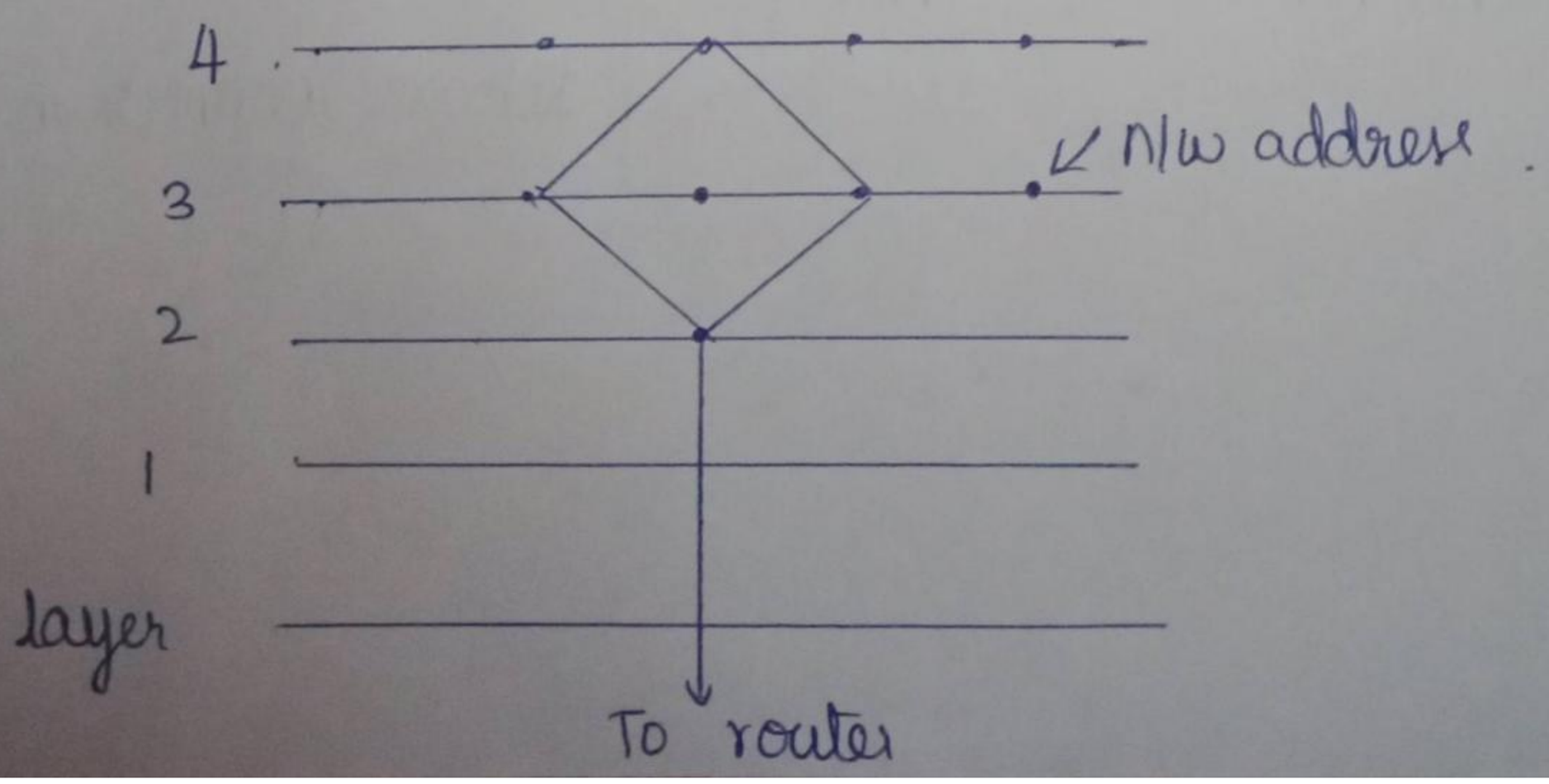


Multiplexing :-

Many virtual circuits open for long periods of time is to take multiplexing of different transport connection onto the same n/w connection attractive. This form of multiplexing called Upward multiplexing



The transport layer opens multiple n/w connection and distributes the traffic among them on a random - robin basis. This is called downward multiplexing



USER DATAGRAM PROTOCOL:

→ UDP is a simple, data-gram oriented, transport layer protocol.

→ This protocol is used in place of TCP.

→ UDP is connectionless protocol.

→ it provides no realiability or flow control mechanisms.

→ it has no error recovery procedures.

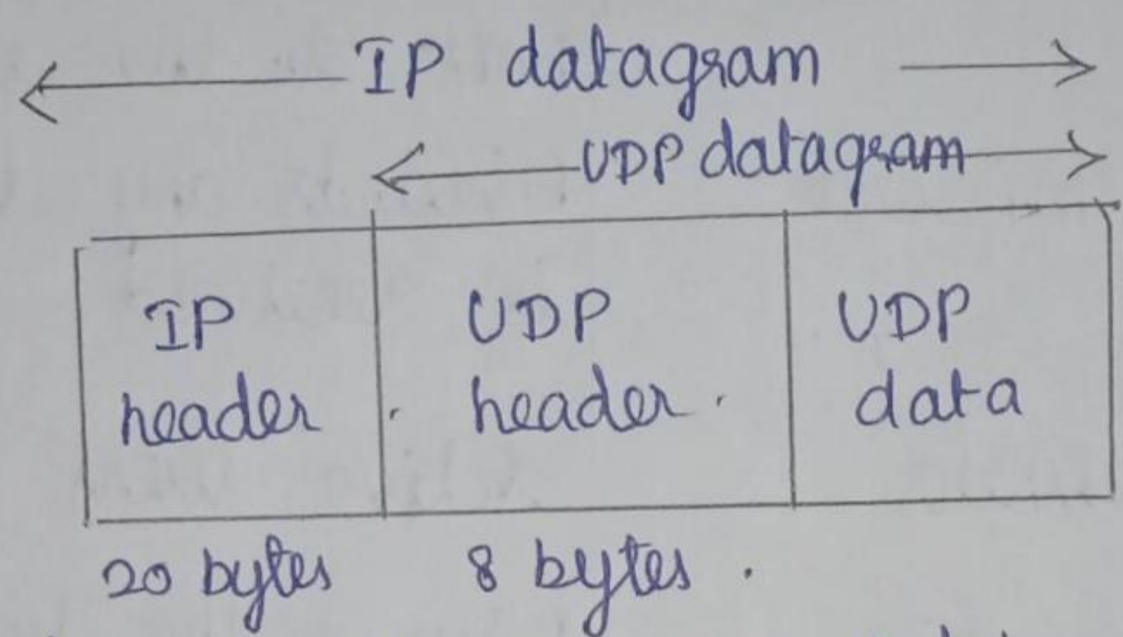
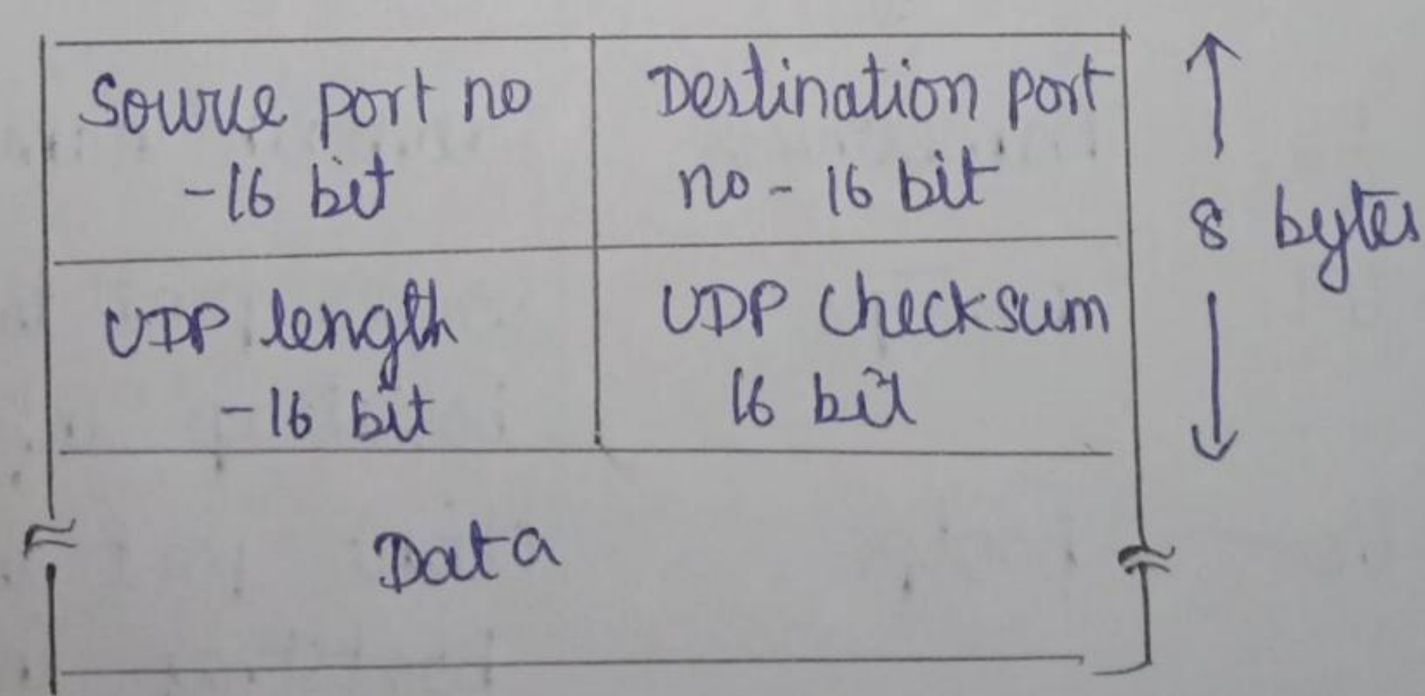


fig shows the encapsulation of UDP datagrams as an IP datagram.



port number :-

UDP uses port number as the addressing mechanism in the transport layer.

following is the list of well known port number used by UDP

Port no.	Protocol	Description.
7	Echo.	Echos a received datagram back to the sender.
9	Discard	Discards any datagram that is received
11	users	Active users
13	Daytime	Returns the data & the time
17	Quote	Returns the quote of the day
19	charger.	Returns a string of characters
53.	Nameserver	domain name service
67	Bootps	server port to download bootstrap information
68	Bootpc.	client port to download bootstrap information
69	TFTP	Trimal File Transfer Protocol
111	RPC	Remote Procedure call.
123.	NTP	N/w Time Protocol.

~~SNMP~~

TCP Services:

→ TCP provides connection-oriented, reliable, byte stream service.

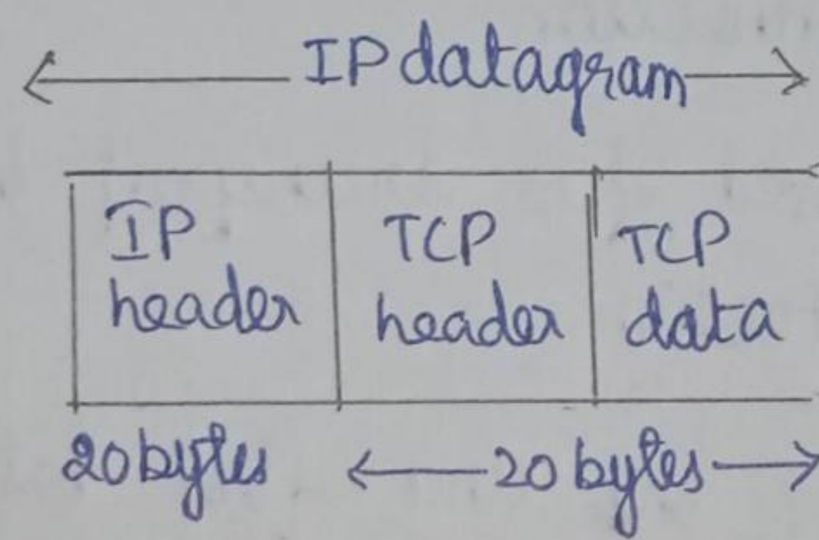
→ TCP does not support multicasting & broadcasting.

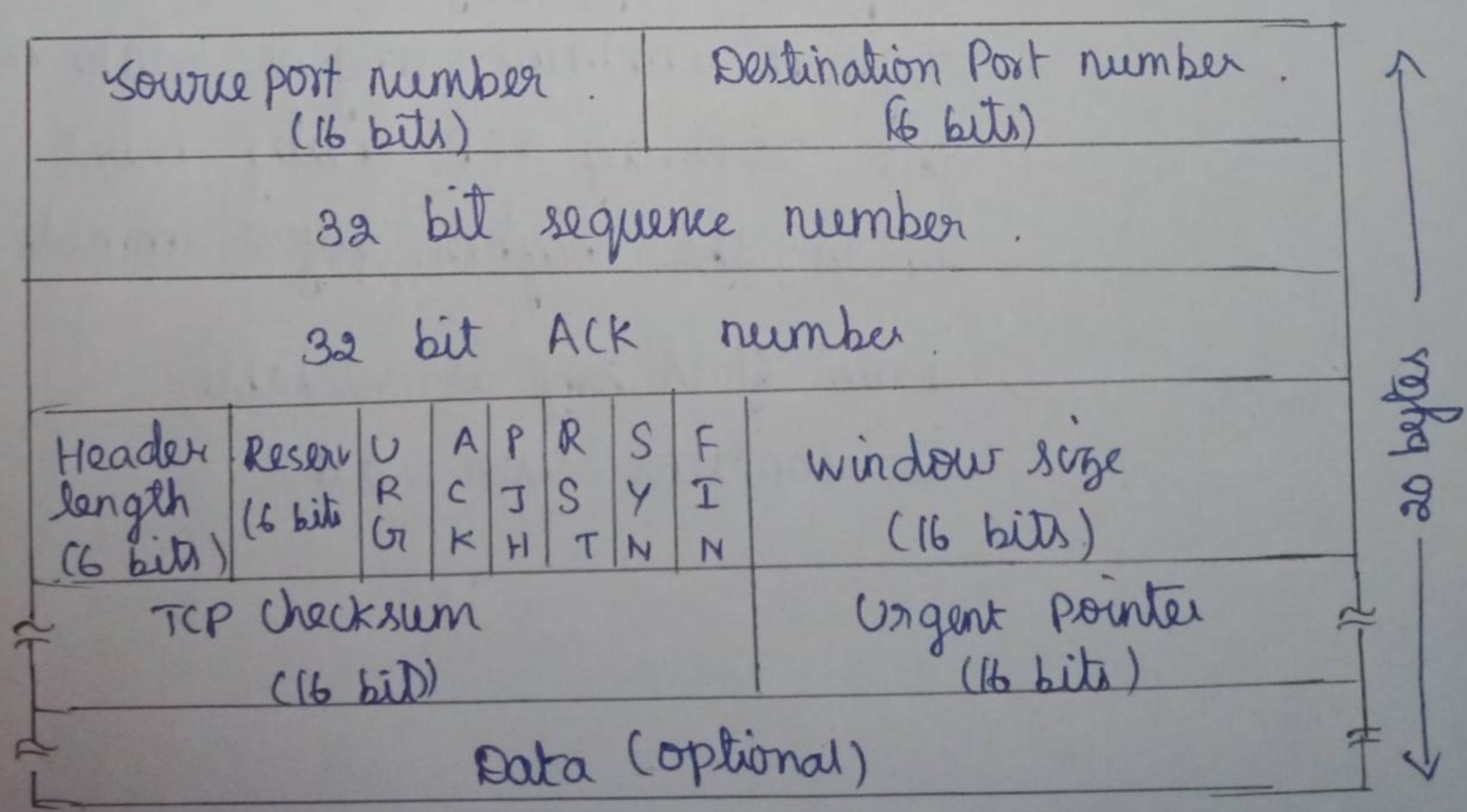
→ The application of data into what TCP considers the best sized chunks to send.

→ The units of information passed by TCP to IP is called a segment.

TCP segment format:

TCP data is encapsulated in an IP datagram





URG → urgent pointer is valid if it is set to 1.

ACK → ACK bit is set to 1 to indicate that the ack no is valid

PSH → The receiver should pass this data to the application as soon as possible

RST → it is used to reset the connection

SYN → Synchronize sequence number to indicate a connection

FIN → fin bit is used to release a connection.

Checksum → used for transport layer error detection

urgent pointer → if the urg flag bit is set, the segment contains urgent data meaning the receiving TCP entity must deliver it to the higher layers immediately.

Data → Data field size is variable. it contains user data

connection:

TCP is a connection-oriented protocol

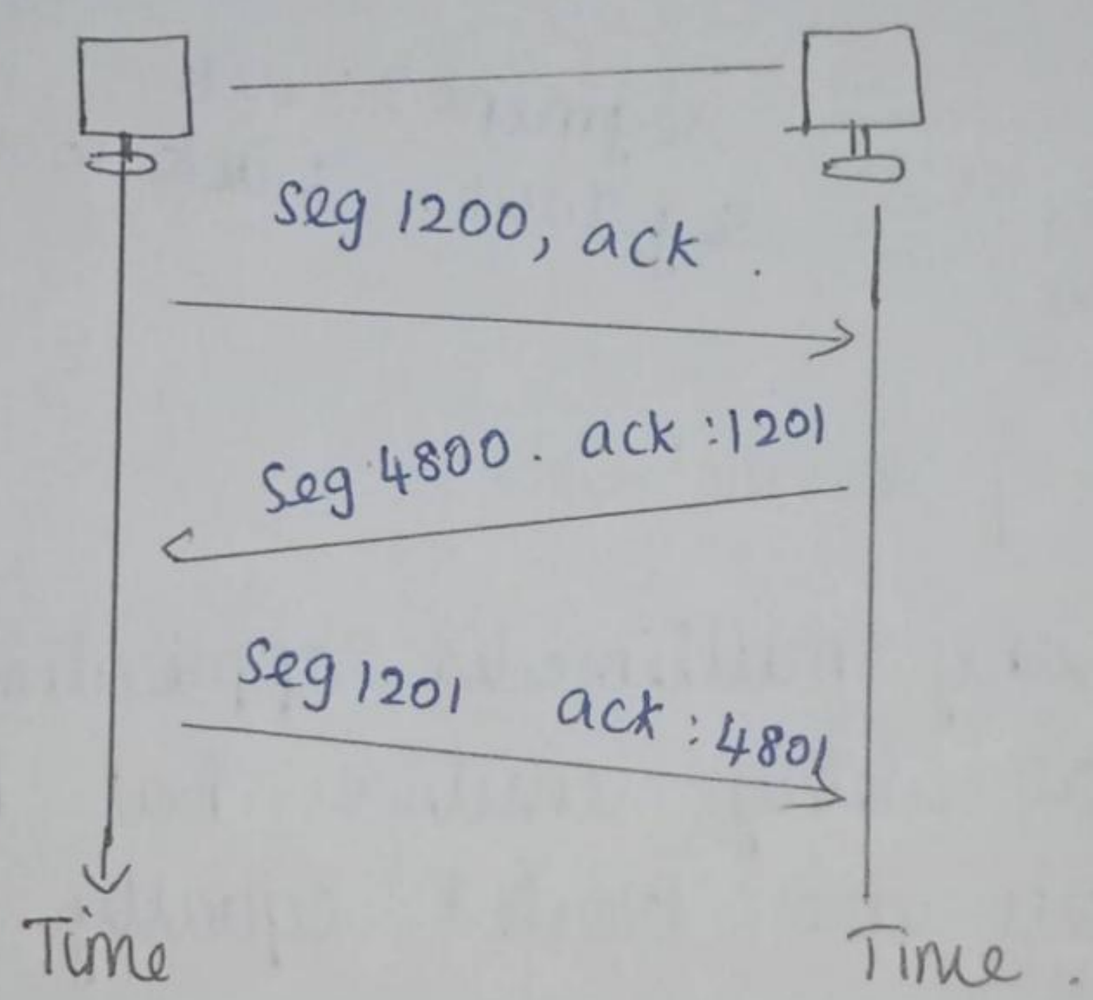
1. connection establishment
2. connection termination

connection establishment.

→ TCP transmits data in full duplex mode.

→ 4 steps are needed to establish a connection

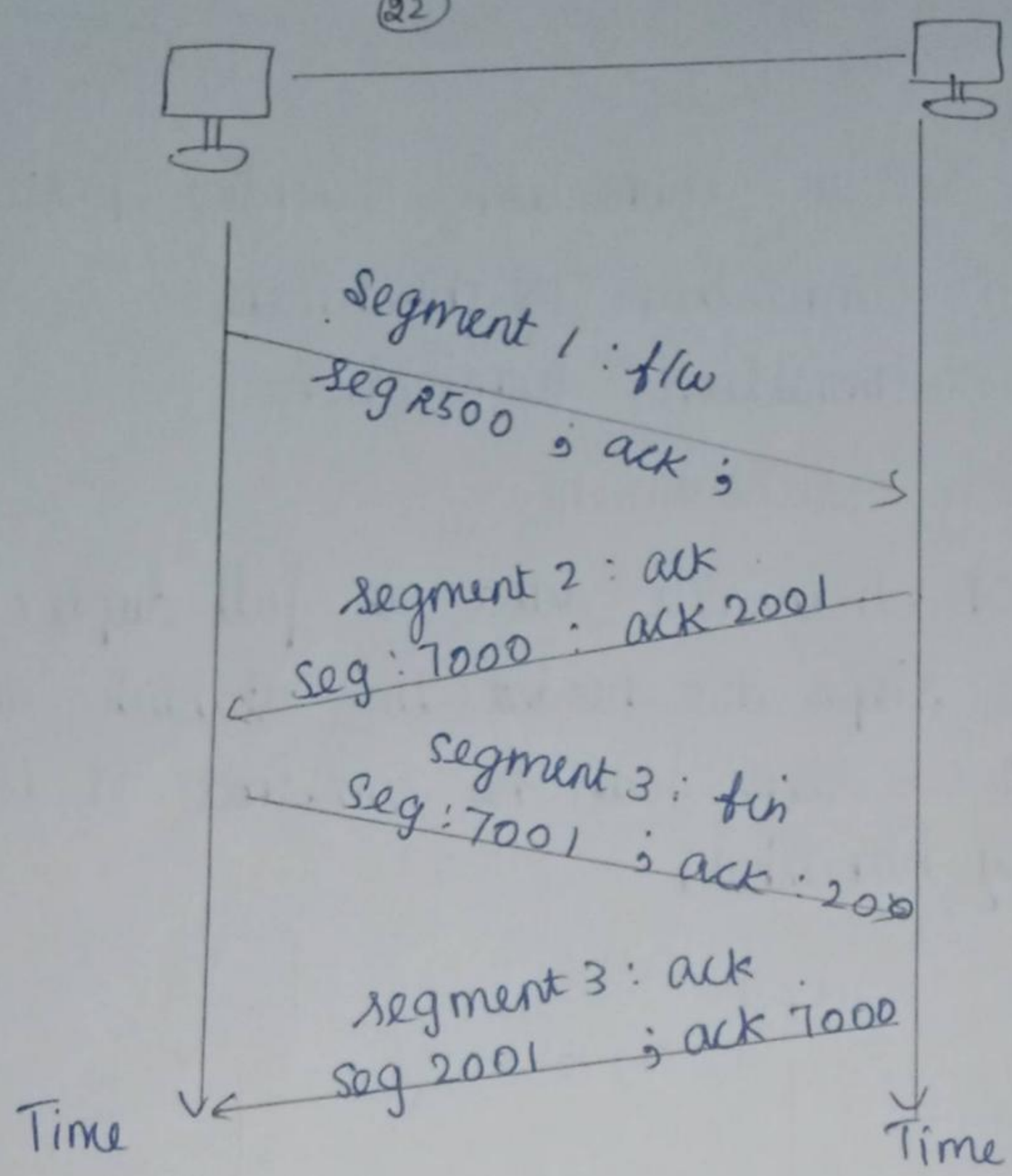
→ 2 & 3 steps can be combined. It is called three way handshake.



connection termination

Any of the two parties involved in exchanging ~~xchng~~ data can close the connection

When connection in one direction is terminated, the other party can continue sending data in other direction.



Quality of service :-

In any multimedia application audio/video packets are delay sensitive but by internet all packets are treated equally.

This causes congestion in traffic followed by delay & loss of packets.

Principle 1 :

packet making allows a router to distinguish among packets belonging to different classes of traffic.

Modified principle 1:

packet classification allows a router to distinguish among packets belonging to different classes of traffic.

Principle 2:

A degree of isolation is desirable among traffic flows, so that one flow is not adversely affected by another misbehaving flow.

Principle 3:

for isolating flows, its is desired to use resources like BW and suffers as efficiently as possible.

Principle 4:-

A call admission process is needed where flows declare their QOS requirement.

Decbit scheme:

Decbit means destination experiencing congestion control.

Queue length is counted over last busy period + idle - 1 current busy period.

RED :-

RED → Random early Detection.

The main idea is to provide congestion control at the router for TCP flows.

RED is based on Decbit

it was designed to work well with TCP

RED notifies sender by dropping packets.

Packets dropping pby is increased as the ave queue length increases.

Policing :-

Policing is the regulation of the rate at which packet flow is injected into the network.

Criteria for policing

Three important policing criteria are identified

1. Avg rate
2. Peak rate
3. Burst size.

Differential service / QoS

The differentiated services (Diffserv) group has developed an architecture for providing scalable & flexible service differentiation. This architecture has the ability to handle different classes of traffic in different way within the internet.

Functional elements of differentiated services

it consists of two sets of functional elements

1. Edge function
2. Core function

Application requirements:

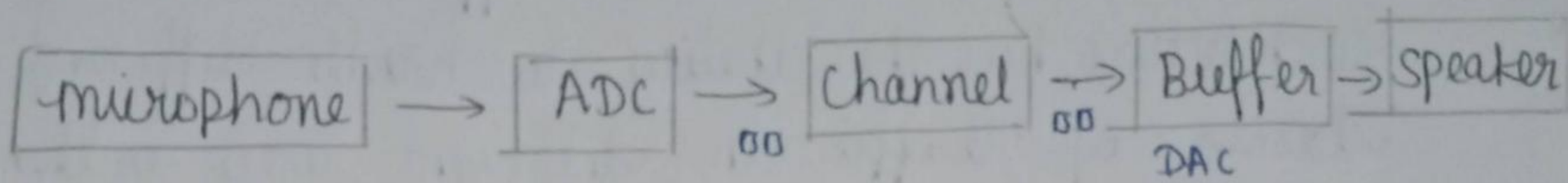
We can divide application into two types

1) Real time
2) Non Real time

Another term for non real time class of application is elastic, since they are able to stretch gracefully in the face of increased delay.

Real time audio example :

consider audio application illustrated in fig.



Data is generated by collecting samples from a microphone.

it is digitalized using ADC.

The digital samples are placed in packets.

The packets are transmitted across the network

They are received at other end.

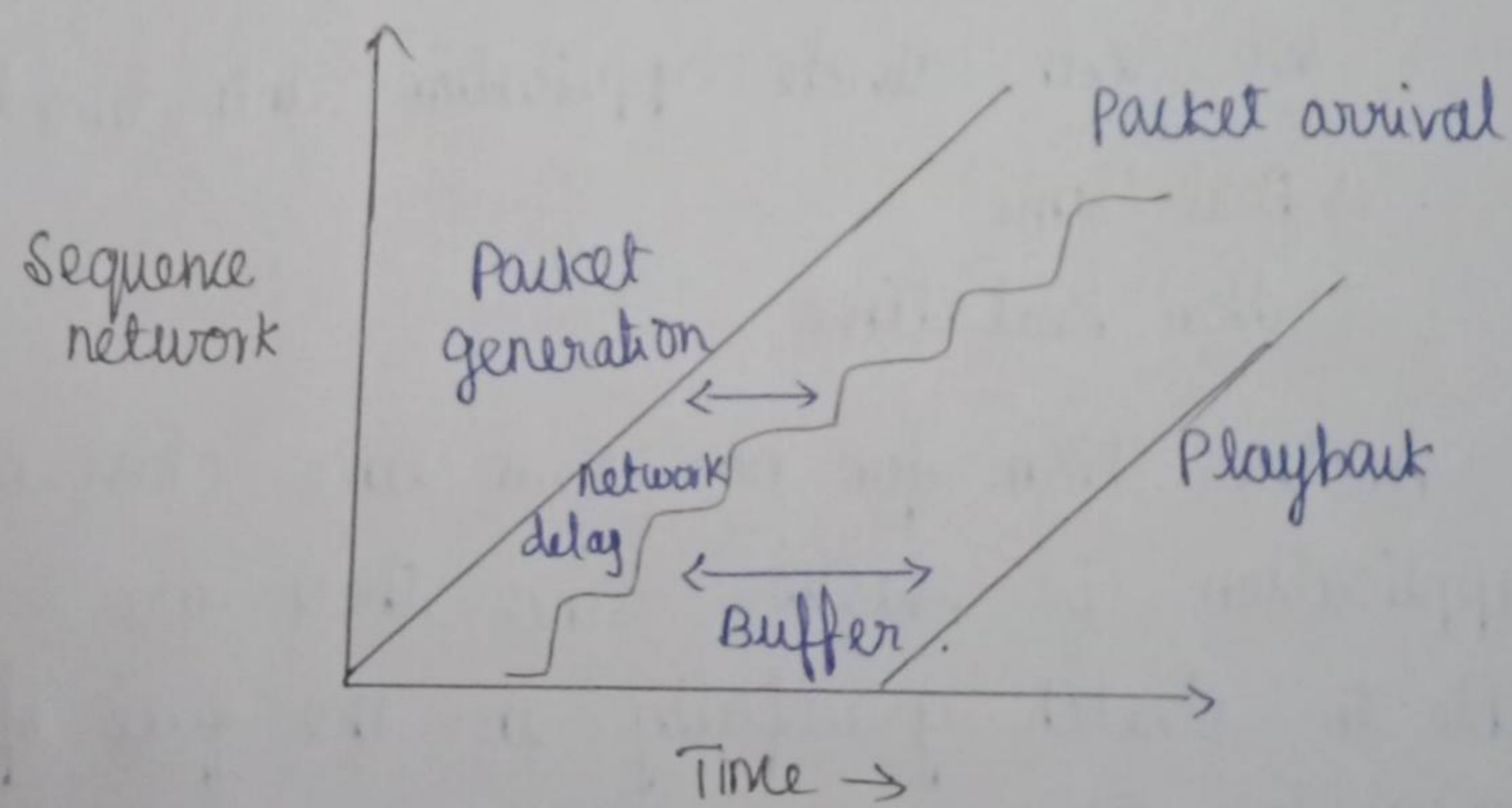


fig: playback buffer

unit V	Application layer.

Syllabus:

Application Layer paradigms - client server programming - world wide web and HTTP - DNS - Electronic Mail (SMTP, POP3, IMAP, MIME) - Introduction to peer to peer Networks - Need for cryptography and Network security - Firewalls.

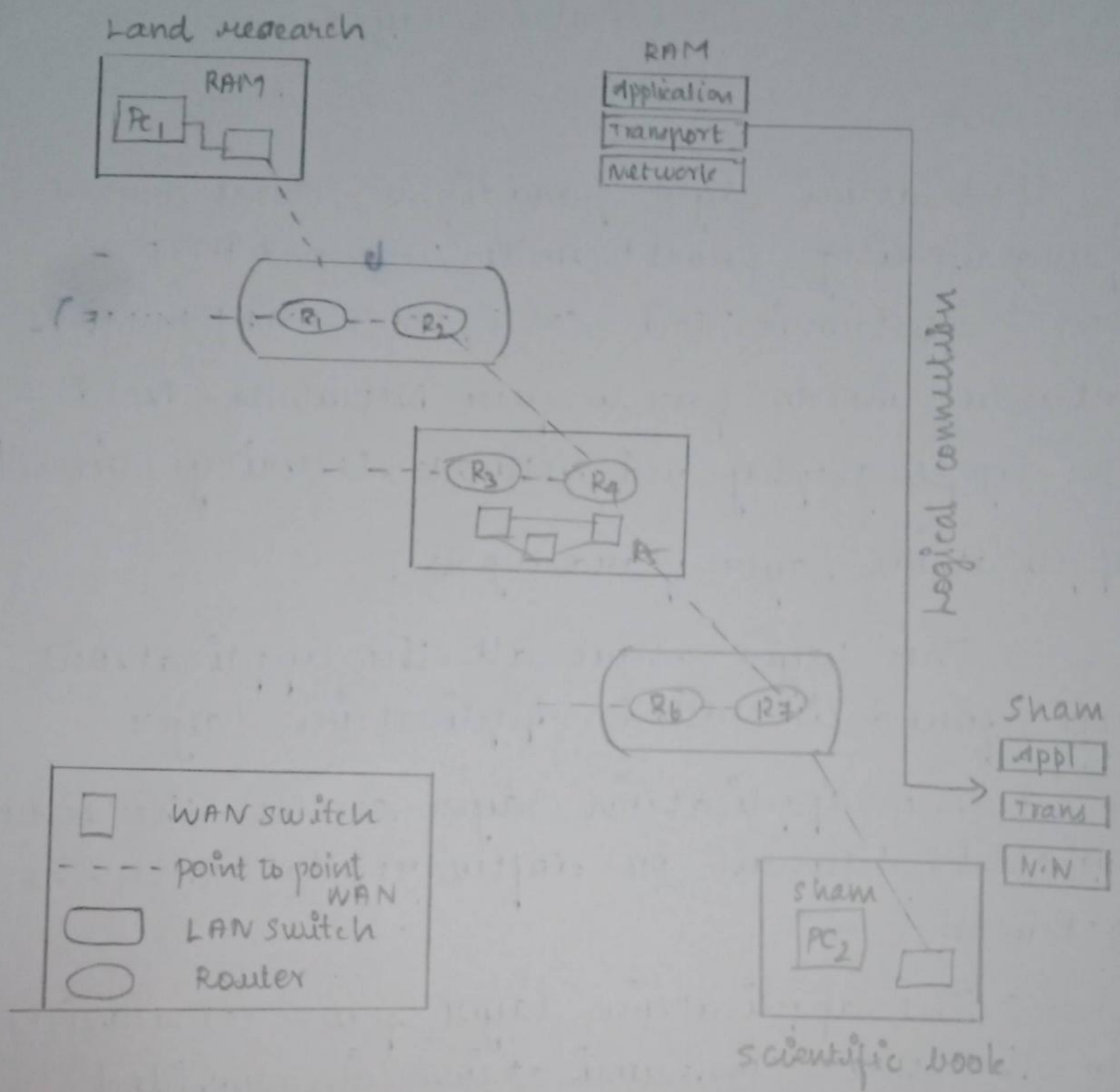
Application Layer paradigms:

→ The layer where all the applications are found is called Application layer.

→ The application layer enables the user, whether human or software, to access the network.

→ The application layer provides services to the user. communication is provided using a logical connection, which means that the two application layers assume that there is an imaginary direct connection through which they can send & receive messages.

→ Application layer needs support protocols, to allow the applications to function.



Logical connection at the application layer.

→ A scientist working in a research company Land research, needs to order a book related to his research from online bookseller, named scientific books.

→ Logical connection takes place between the application layer of a computer at Land research and the application layer of a server at scientific books.

→ several traditional services are still using this paradigm, eg., WWW, HTTP, FTP, SSH, E-mail, and so on.

Problems:

→ The server should be a powerful computer.

→ There should be a service provider willing to acept the cost and create a powerful server for a specific service.

Client - server programming:

→ In the client - server model, the requesting device is called a client and the device responding to the request is called a server.

→ These are considered to be in the application layer. Data transfer from a client to server - upload, data from server to client - download

→ The server runs a service, or

Process → daemon → typically run in the back ground - not under an end user's direct control.

→ when a 'daemon' means a request from a client, it exchanges appropriate messages with the client, required by its protocol & proceed to send the data in a proper format.

Application programming Interface (API).

→ set of instructions to talk with the lowest four layer (in OS)

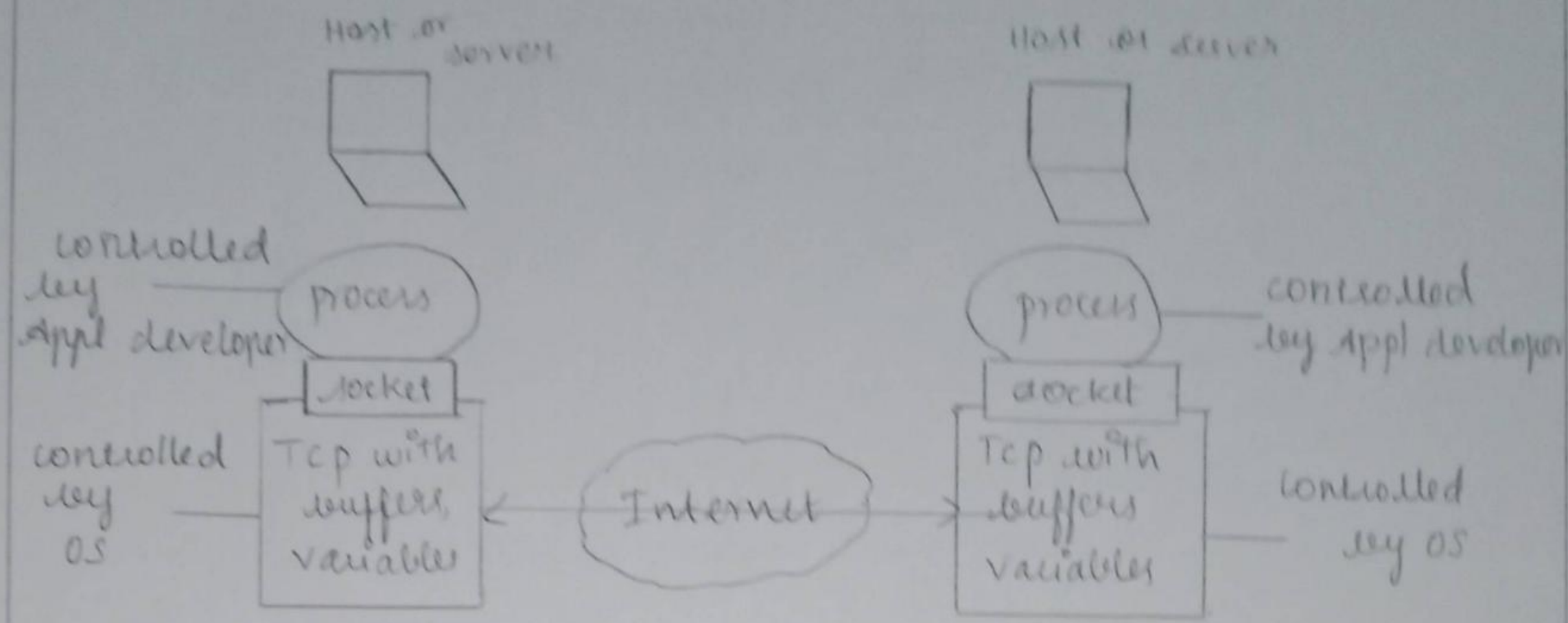
→ Instructs to open a connection, send and receive data; close the connection.

Interface between a process & Network:

Types → three most common APIS.

* Socket Interface.
* Transport Layer interface.
* STREAM.

• A process sends messages info, & receives messages from, network through a software interface — socket.



Application process, sockets and underlying transport protocol

Socket interface:

→ started in the early 1980 at UC Berkeley as part of a UNIX environment.

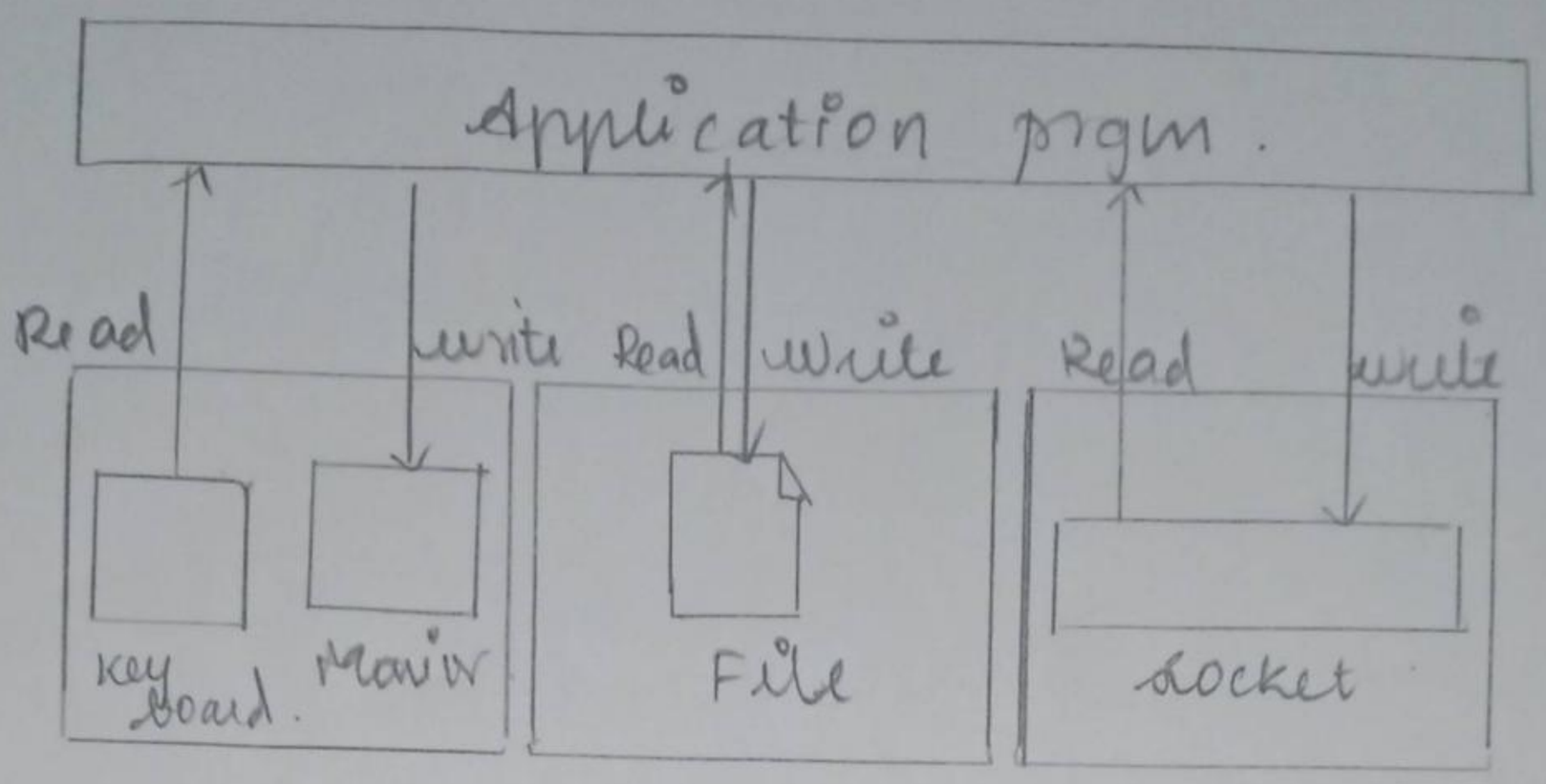
→ set of instructions that provide communication between the application layer and the OS.

→ allow us to use the set of instructions already designed in a PL for other source & sink.

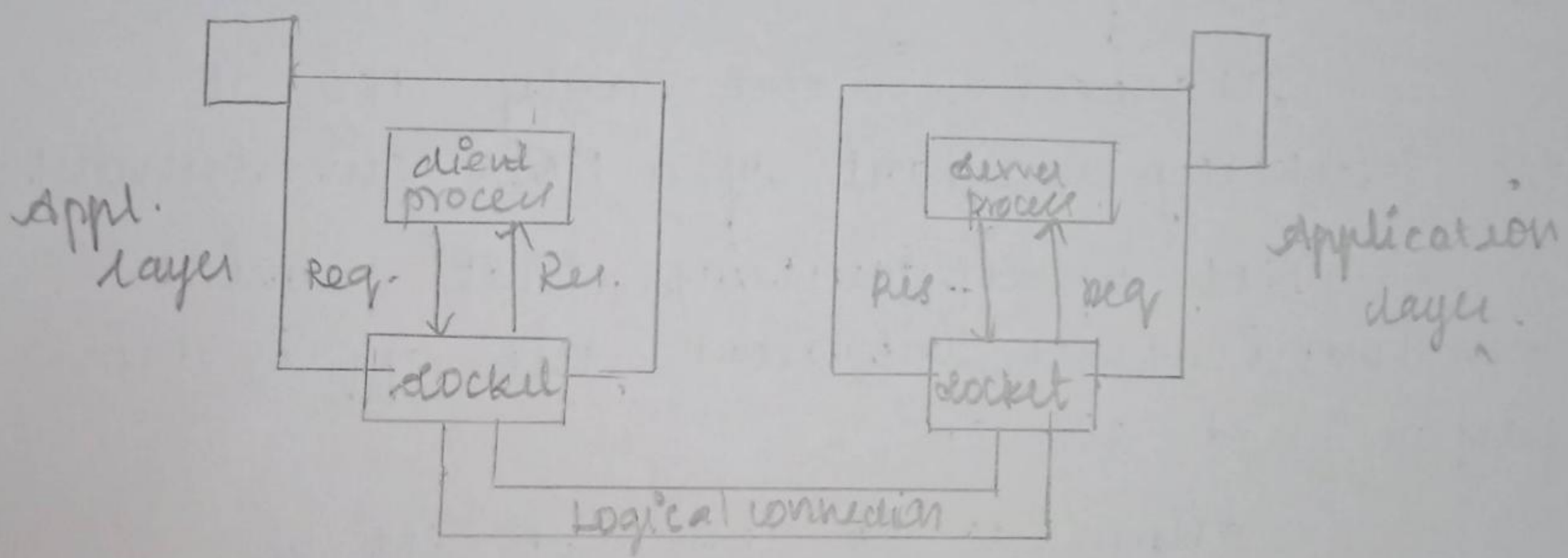
→ socket — not a physical entity

→ It is an abstraction.

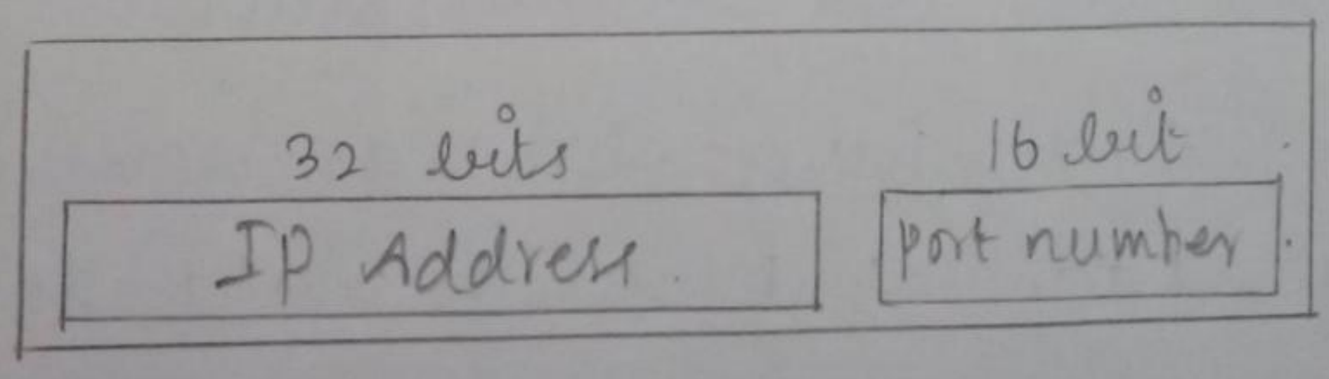
Eg: in C, C++, java → has several instructions that can read and write data to sources & sinks

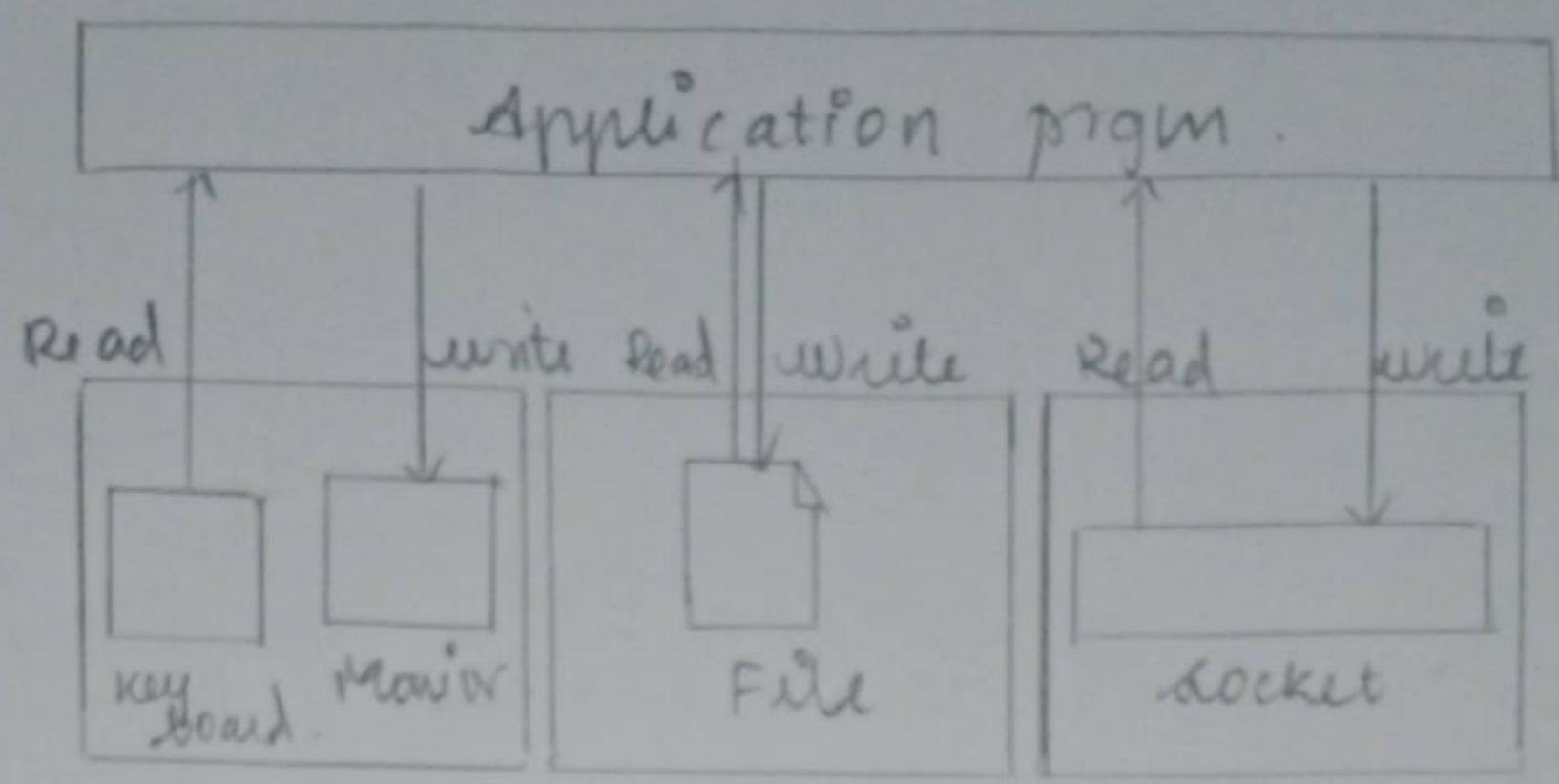


communication between a client process & a server process is nothing but communication between two sockets.

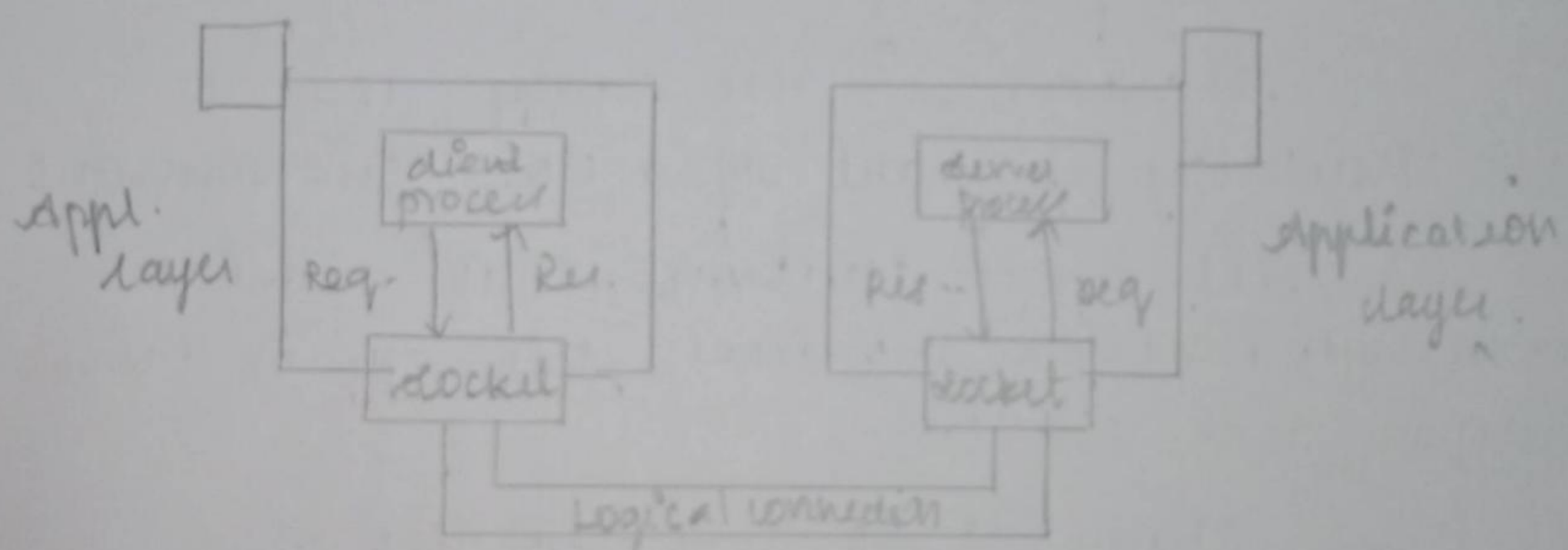


→ process to process communication need a pair of socket address for communication. local socket address & remote socket address.

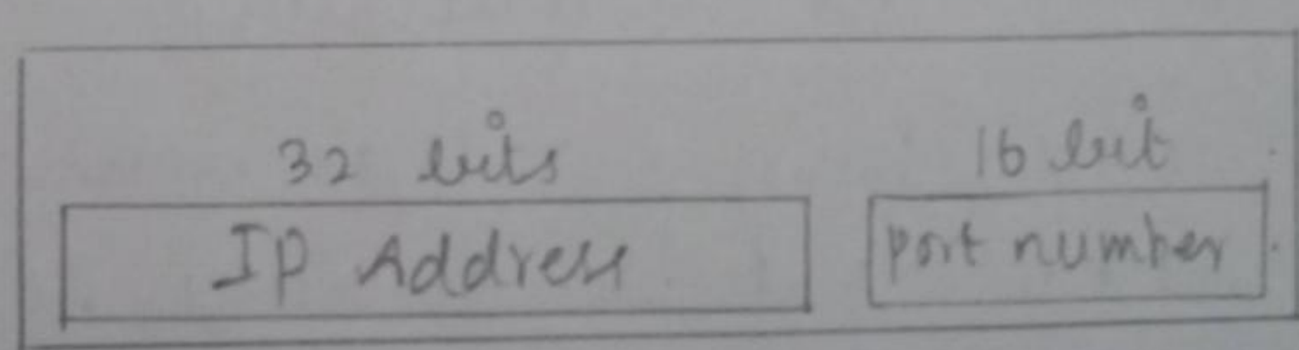




communication between a client process & a server process is nothing but communication between two sockets.



→ process to process communication need a pair of socket address for communication. local socket address & remote socket address.



Using services of the transport layer;

Broadly classify the possible transport layer services along four dimensions.

1) Reliable data transfer 2) Throughput.

3) Timing 4) security.

Use UDP: → For sending small messages.

→ simplicity & speed is more important for application more than reliability.

Use TCP → For sending long messages and requires reliability.

→ providing security it use SSL (secure socket layer).

World wide Web (WWW);

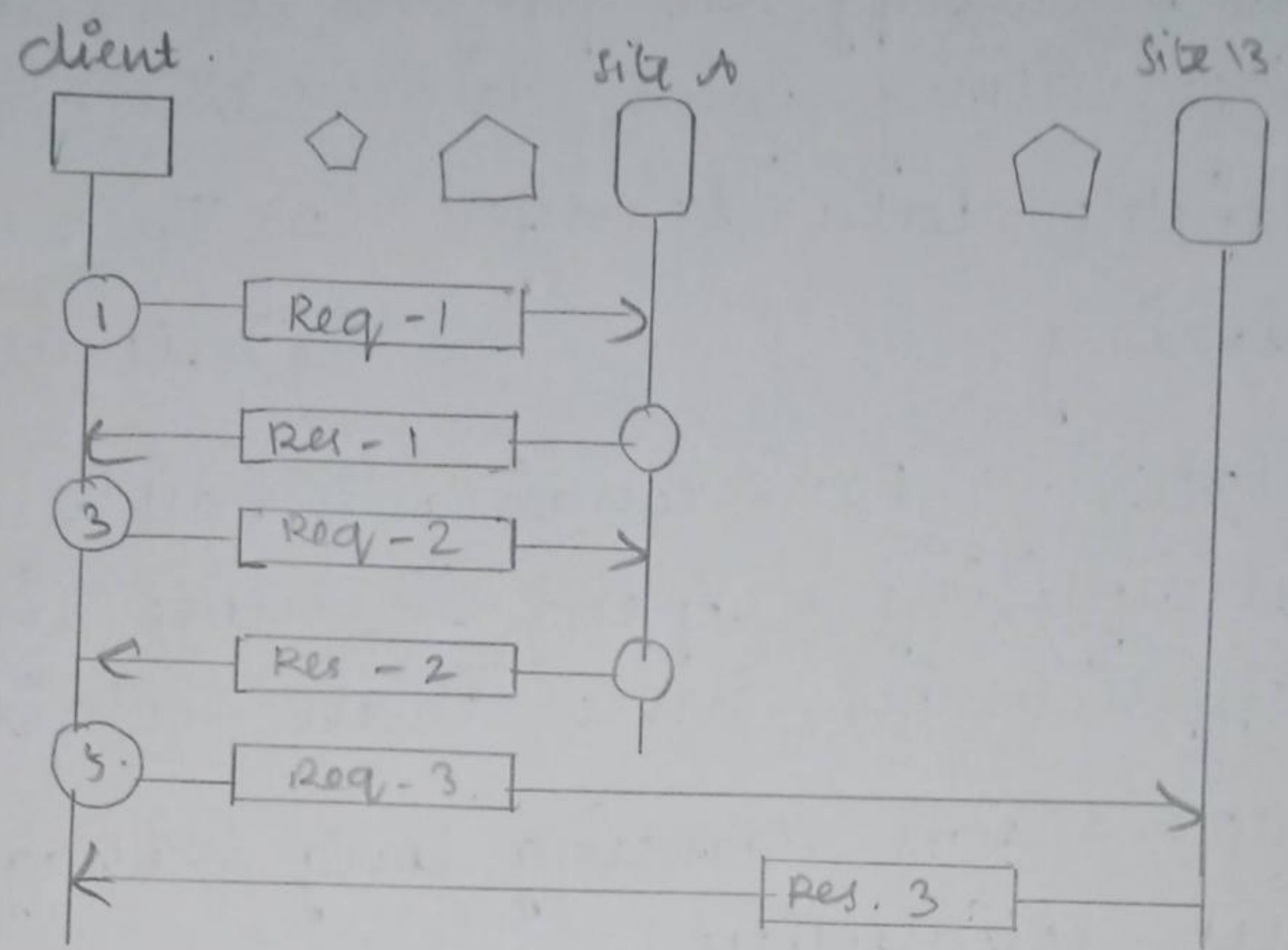
→ repository of information linked together from points all over the world.

→ has a unique combination of flexibility, portability and user-friendly features that distinguish over many location provided by the internet.

→ distributed client server service, which a client using a browser can

access a service using a server.

Architecture:



Architecture of WWW.

→ The reference has the URL for the new site. The user is also interested in seeing this document. The client sends another request to the new site, and the new page is retrieved.

Client side:

→ Each browser usually consists of three parts: a controller, client protocol, interpreters. The controller receives I/p from the keyboard or the mouse & uses the client programs to access the

document.

→ After the document has been accessed, the controller use one of the interpreters to display the document on the screen.

→ The client protocol → FTP or HTTP.

→ The interpreter - HTML, Java or Java script, depending on the type of document

Server side;

→ webpage is stored at the server.

→ Each time a client request arrives, the corresponding document is sent to the client.

→ To improve efficiency - servers stores requested files in a cache in memory. memory is faster access than disk.

Uniform Resource Locator (URL);

→ A client that wants to access a webpage needs the address. To facilitate the access of documents distributed throughout the world, HTTP uses locators.

→ The Uniform Resource Locator is a standard for specifying any kind of information on the internet. It defines four things: protocol, host computer, port and path.

→ protocol: 1) client / server program used to retrieve the document. Many protocols can retrieve the document like FTP or HTTP. Most common - HTTP.

→ Host: the computer on which the info is located, although the name can be an alias.

→ Webpages usually stored in computers, they are given alias name begin with "www".

→ Not Mandatory.

→ can optionally contain the port number of the server.

→ path: pathname of the file where the information is located.

Cookies:

A cookie is a piece of data from a website that is stored within a web browser that the website can be retrieve at a later time. cookies are used to tell the server that the client have returned to a particular website. When client returns to a website, a cookie provides information and allows the site to display selected settings and targeted content.

Creation of cookies;

They are generated by the websites that are different from the web pages users are currently surfing. usually because they are linked to ads on the pages. Visiting a site with 10 ads may generate 10 cookies even if users never click on those ads.

→ It contains two bits of data: a unique ID for each user & a site name.

web documents;

The documents in the WWW can be grouped into three categories static documents, dynamic documents & active documents.

1) Static documents;

→ contain fixed content.

→ created and stored on the server.

→ client can get a copy of the document only.

→ Static document users cannot change the content, but the content in the server can be changed.

→ when the client access a doc, a copy of the doc is sent, user can use a browsing program to display it.

Static documents are prepared using one of the languages.

1) HTML (Hypertext Markup language)
2) XML (Extensible Markup Language).
3) XHTML (Extended Hypertext M.L).
4) XSL (Extensible Style Language).

HTML:

→ language for creating web pages.

→ Markup language comes from the book publishing industry.

→ Before a book is typeset & printed, a copy editor reads the manuscript of the book and puts a mark on it.

2) Dynamic documents:

→ created by a webserver when the browser requests the document.

→ when a request arrives, it runs an application program or script which creates the dynamic document.

→ The server returns the O/p of the program as a response to the browsers requested the documents.

→ A fresh document is created for each request, the content for dynamic document may vary from one request to another.

Common gateway Interface (CGI):

→ CGI is a technology used to create & handle dynamic documents.

→ set of standards that defines, how the dynamic document is written, how the Data I/p into the program & how it is shown.

→ The problem with CGI technology is the inefficiency that results if parts of the dynamic document that is to be created is fixed & not changing from request to request.

Hypertext Transfer protocol (HTTP):

→ standard web transfer protocol.

→ consists of two fairly distinct items: The set of requests from browsers to servers & the set of response from servers to browsers.

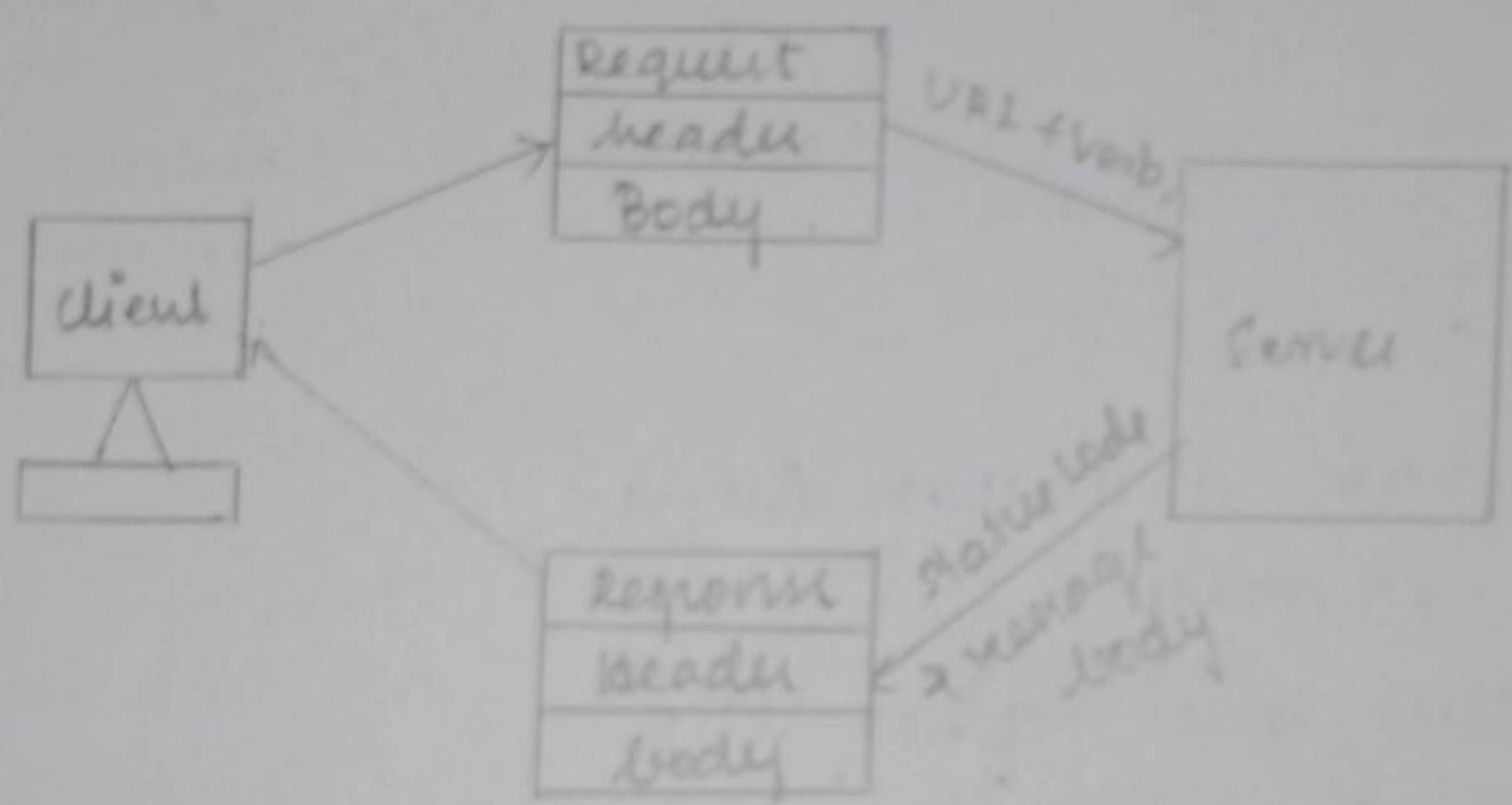
→ Newer version of HTTP supports two kinds of requests:

* simple requests → Single GET name naming the page without protocol
* full request → indicated by presence of protocol version on the GET request line.

HTTP transaction:

→ uses the services of TCP. HTTP is a stateless protocol.

→ The client initiates the transaction by sending a request message. The server replies by sending a response.

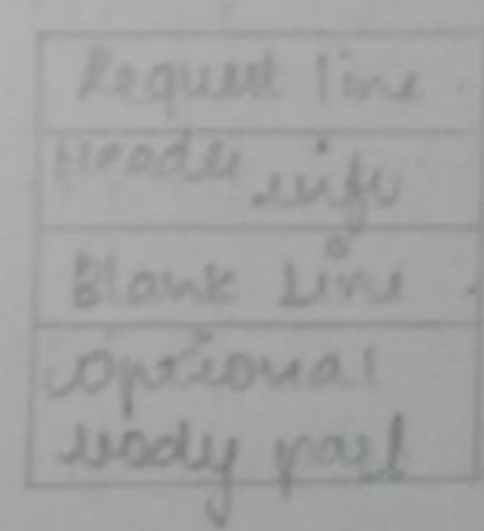


HTTP Messages:

→ Types : 1) Request 2) Response.

→ Same format

→ Request message consists of a request line, headers & a body.



Request line:

→ It defines the

1) Request type.

2) Resource.

3) HTTP version.

→ Request type categorizes the request message into several method for HTTP.

GET / home.htm	HTTP

Request line

method://host port/path

URL Example

Eg: http://www.technicalpublication.org/home.html

↑ protocol ↑ sub domain ↑ Domain name ↑ top-level domain ↑ File path.

Response Message:

→ contains a status line, a header & body.

→ status line defines the status of the response message.

Status line
Header info
a blank line
Body (optional)

→ It consists of the

a) HTTP version b) space c) status code.

d) space e) space phrase.

HTTP headers:

→ made of a header name, a colon, a space & header value.

Header name	:	header value

header format

→ exchanges additional information between the client and the server.

→ header line belongs to one of four categories general header, request header, response header & entity header.

→ General header - general information about the message. Request & response both contains general header.

→ Response header: present only in a response message. specifies the server configuration & special information about the server.

→ Request header: present only in a request message. specifies the client configuration & special information about the client.

→ Entity header: information about the body of the document. Mostly present in response messages, some request message such as POST & PUT methods.

Message body	<html>
	<head>
	<title>
	<head>
	<body>

Persistent & Non persistent connection:

1) persistent HTTP.

2) Non-persistent HTTP.

Non-persistent connections;

→ one TCP connection is made for each request / response.

Round Trip Time (RTT):

→ RTT is the time it takes for a small packet to travel from client to server & send back to the client.

→ RTT includes packet propagation delays, packet queuing delays in intermediate routers & switches and packet processing delays.

Disadvantages of non-persistent:

→ TCP processing and memory resource wasted in the server & the client.

→ requires delay of 2RTT associated with the transfer of each object.

→ Each TCP connection setup involves the exchanges of three segments between client and server machines.

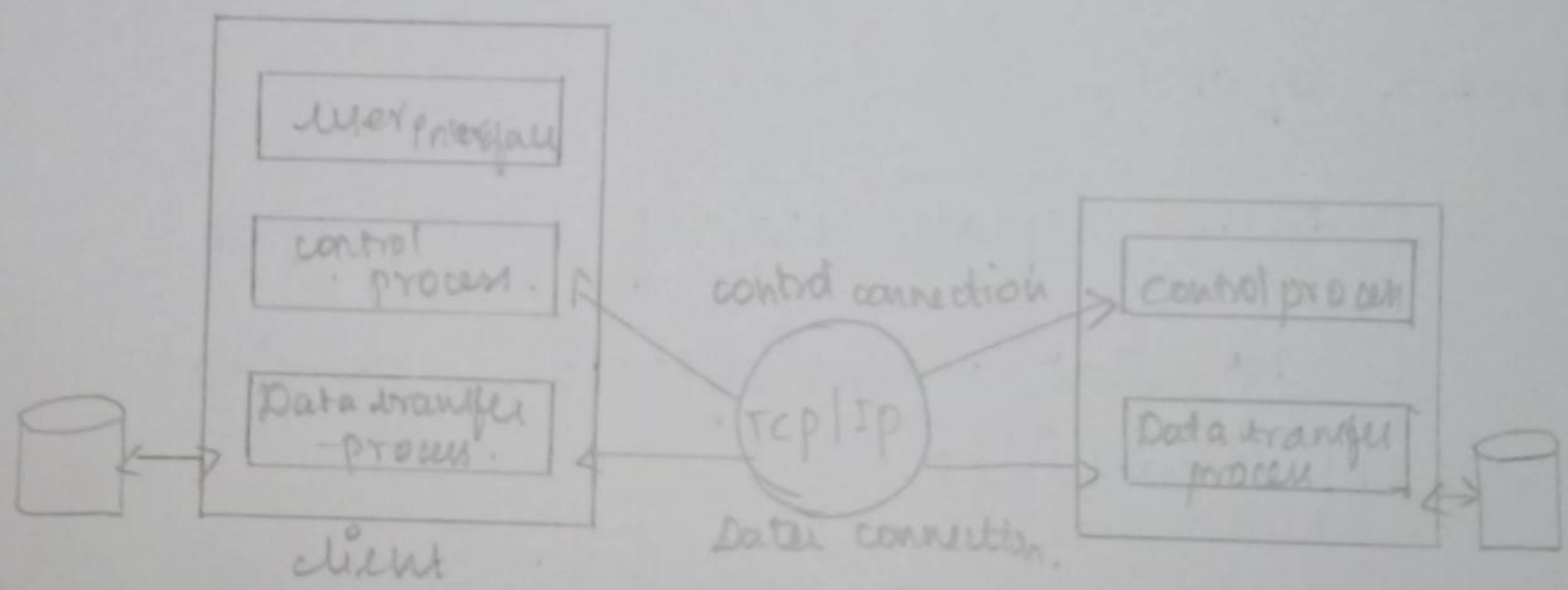
Persistent connection;

→ The server now keeps the TCP connection open for a certain period of time after sending a response.

→ This enables the client to make multiple requests over the same TCP connection & hence avoid the inefficiency & delay of the non-persistent mode.

File transfer protocol (FTP).

→ FTP is designed for distributing files to a numbers of user. FTP uses a client server system, in which files are stored at a central computer & transfered between that computer and others, widely distributed computers.



Domain Name System (DNS):

→ The DNS is a distributed database that resides on multiple machines on the internet and used to convert between names & address and to provide e-mail routing information.

Components of DNS:

→ DNS includes following components

1) Domain — com is domain.

2) Domain name - sequences of names.

3) Name server — mapping.

4) Name Resolver — software.

5) Name cache — storage used by name

6) zone — contiguous part

Name spaces:

→ Name space are of two types.

* flat name spaces — original set of machines.

*. Hierachical names →. provide a simple yet flexible naming structure.

Components of DNS:

→ DNS includes following components

1) Domain — com is domain.

2) Domain name - sequences of names.

3) Name server — mapping.

4) Name resolver — software.

5) Name cache — storage used by name

6) zone — contiguous part

Name spaces:

→ Name space are of two types.

* flat name spaces — original set of machines.

*. Hierachical name → provide a simple yet flexible naming structure.

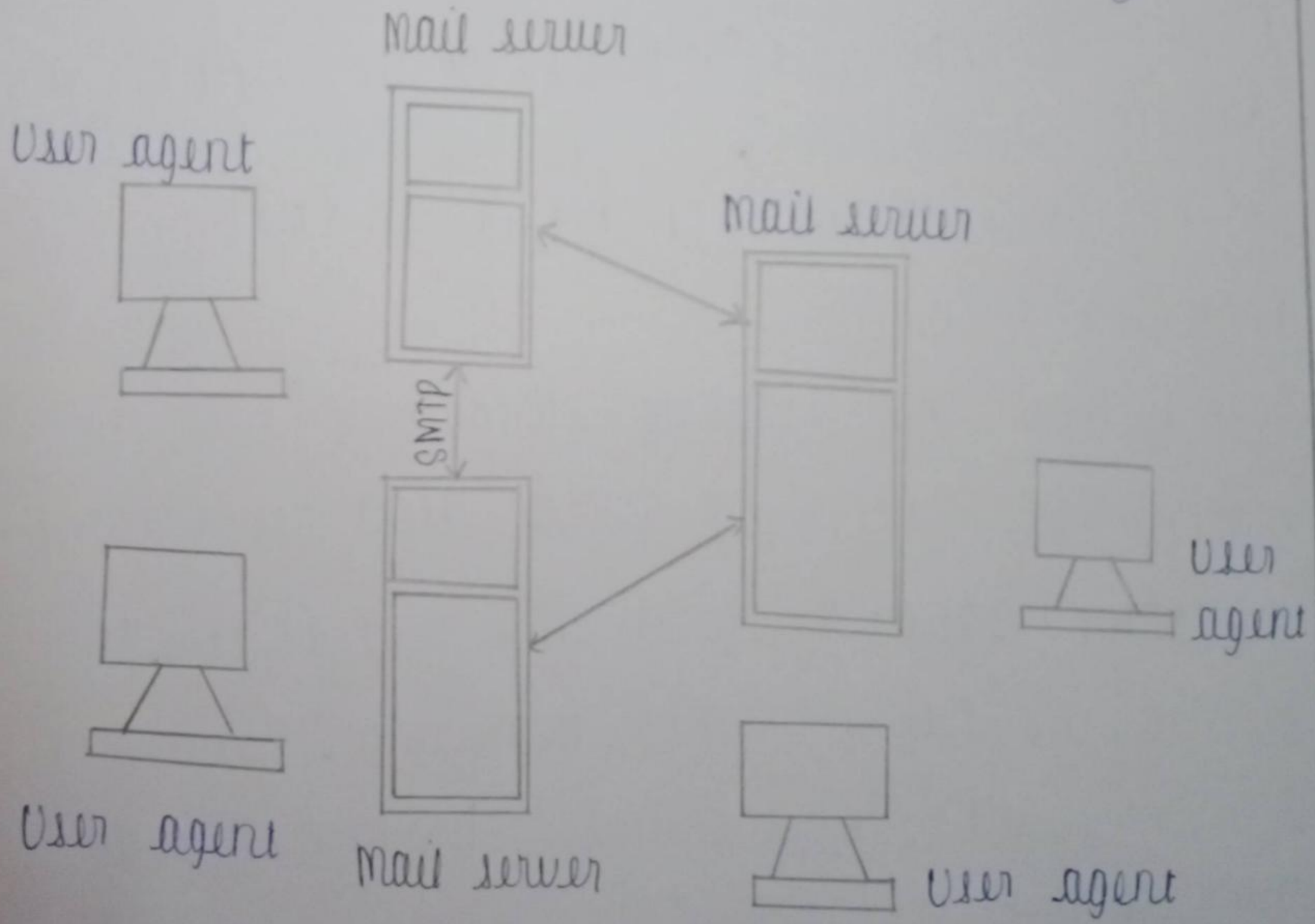
Electronic Mail :-

→ E-mail is an asynchronous communication medium. E-mail is used for sending a single message that includes text, voice, video or graphics.

→ It is fast, easy to distribute and inexpensive.

→ E-mail is not a real time service in that fairly large delays can be tolerated.

→ It is also not connection oriented in that a network connection does not need to be set up expressly for each individual message.



→ POP servers store incoming mail while SMTP servers relay outgoing mails.

→ ISP probably runs both an SMTP server and POP server for its customers.

components :-

1. User agents 2. Mail servers 3. SMTP

Message headers :-

Includes the address of receiver and sender. Each header consists of the type of header, a colon and content of the header.

From : " SachinMaradik " < kanohar@del2.vsnl.net.in>
Subject : admission
Date : Wed, 19 Jul 2021 12:43:31 +530

Formatted E-mail :-

→ E-mail that supports formatting such as boldface and underlining is a recent development.

→ HTML tags are just like web pages. It can include text formatting, numbering, bullets, horizontal lines, backgrounds, hyperlinks and HTML styles.

→ Rich text can be read by most word processing applications. MIME formatting are created just for e-mail.

→ Include text formatting, pictures, videos, sound and other information.

→ The MIME version declares that the message was composed using version 1.0 of the protocol.

→ To view the image, a receiver mail system must convert from base 64 encoding to binary.

→ A content type declaration must contain two identifiers, a content type and a sub type, separated by a slash.

Functions of E-mail:-

→ Composition: process of creating messages and answers. When answering a message, the e-mail system can extract originator's address from incoming e-mail.

→ Transfer: moving messages from the originator to the receiver.

→ Reporting: It inform the originator what happened to the message.

→ Displaying : Display is required for reading the email.

→ Disposition : It is the last step and related what the receiver does with message receiving.

Simple Mail Transfer protocol :-

→ SMTP is application layer protocol of TCP/IP model. SMTP transfers message from sender's mail servers to the recipients mail servers.

→ SMTP interacts with local mail system and it uses a TCP socket on port 25 to transfer e-mail reliably from client to server.

→ Email is temporarily stored on the local and eventually transfered directly to sender.

→ Mail client application interacts with a local SMTP server to initiate delivery of an e-mail message.

→ There is an input queue and an output queue at the interface between the local mail system and the client and the server parts of the SMTP.