KLS Vishwanathrao Deshpande Institute of Technology

(Accredited by NAAC with "A" Grade)

(Approved by AICTE, New Delhi, Affiliated to VTU, Belagavi)

(Recognized Under Section 2(f) by UGC, New Delhi)

Udyog Vidya Nagar, Haliyal - 581 329, Dist.: Uttara Kannada

www.klsvdit.edu.in | principal@klsvdit.edu.in | hodece@klsvdit.edu.in

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

University / Model Question Paper

Scheme & Solution

Faculty Name	:	Ms. Pavitra M. Badiger
Course Name	:	computer Networks and protocole
Course Code	:	BEC702
Year of Question Paper	:	2025
Date of Submission	:	17-07-2025

PBadiger
Faculty Member

HoD
17-07-2025

Dean (Acad.)

Head of the Department
Dept. of Electronic & Communication Engg.
KLS V.D.I.T., HALIYAL (U.K.)

Model Question Paper BEC702

Seventh semester B.E. Degree Examination 2025-26

Computer Networks and Protocols

Time: 3hrs. **Max. Marks: 100**

Note: 1. Answer any FIVE full questions, choosing ONE full question from each module.

		Module - 1	M	L	C
Q1	a.	What is Data Communication? Explain Components of data communication.	10	1,2	1
	b.	With a neat diagram, Explain the significance of layers in TCP/IP Protocol suite.	10	2	1
		OR			
Q2	a.	Explain different data flow techniques for communication between two devices.	10	2	1
	b.	With the neat diagram illustrate the concept of encapsulation and decapsulation in internet.	10	2	1
		Module – 2			
Q3	a.	Explain how collisions are avoided through the use of CSMA/CA's three strategies with flow diagram.	10	2	2
	b.	A Slotted ALOHA network transmits 200-bit frames on a shared channel of 200kbps. What is the throughput if the system (all station together) produces. a. 1000 frames per second b. 500 frames per second c. 250 frames per second	06	2	2
	c.	Explain the Ethernet frame format of Standard Ethernet.	04	2	2
		OR			
Q4	a.	Explain CSMA/CD working with help of Flow chart.	10	1	2
	b.	Explain the Architectural Comparison of Wireless LANs and list the characteristics of Wireless LANs.	10	2	2
		Module – 3			
Q5	a.	Write a note on Security of IPV4 datagram.	10	2	3
	b.	With suitable diagram explain distance vector routing.	10	1	3
		OR			
Q6	a.	Explain with an Examples, Link state routing and also apply Djkstra algorithm to find least cost path free.	10	2	3
	b.	Explain working of DHCP (Dynamic Host Configuration Protocol).	10	2	3
		Module – 4			
Q7	a.	Describe the connectionless and connection-oriented services provided by transport layer.	10	2	4
	b.	With a neat diagram, Explain state transition diagram in TCP.	10	1	4
		OR			
Q8	a.	Explain Go-Back-N protocol along with sliding window diagram.	10	2	4
	b.	Describe General services provided by UDP.	10	1	4

Head of the Department
Dept. of Electronic & Communication Engg.
KLS V.D.I.T., HALIYAL (U.K.)

<table>
<tr><td colspan="6"><b>Module – 5</b></td></tr>
<tr><td>Q9</td><td>a.</td><td>Explain the following i) HTTP ii) FTP.</td><td><b>10</b></td><td><b>2</b></td><td><b>5</b></td></tr>
<tr><td></td><td>b.</td><td>Explain DNS Name space, DNS in internet and resolution.</td><td><b>10</b></td><td><b>2</b></td><td><b>5</b></td></tr>
<tr><td colspan="6"><b>OR</b></td></tr>
<tr><td>Q10</td><td>a.</td><td>Explain the architecture of Electronic-mail with neat diagram.</td><td><b>10</b></td><td><b>1</b></td><td><b>5</b></td></tr>
<tr><td></td><td>b.</td><td>Explain with an examples, the working of HTTP (Hyper Text Transfer Protocol).</td><td><b>10</b></td><td><b>2</b></td><td><b>5</b></td></tr>
</table>

Head of the Department
Dept. of Electronic & Communication Engg.
KLS V.D.I.T., HALIYAL (U.K.)

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGG. * KLS VDIT HALIYAL

1a) What is Data Communication? Explain (10M
Component of Data communication.

Ans) Data communications are the exchange of data between two devices via some form of transmission medium such as wire cable. Effectiveness of data communication system depends on four fundamental characteristics :-

1) delivery : The system must deliver data to the correct destination.

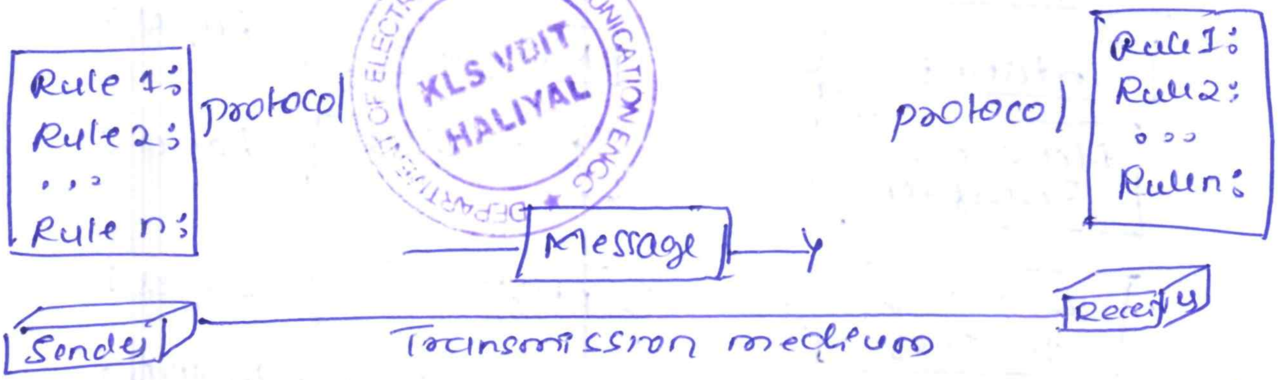
2) Accuracy : The system must deliver the data accurately. Data that have been altred in transmission and left uncorrected are unusable.

3) Timeliness : The system must deliver data in timely manner. Data delivered Late are useless.

4) Jitter : Jitter refers to variation in the packets arrival time.

Components of Data Communication :

→ a data communication system has five components.



1. message : The message is the information (data) to be communicated.
* popular forms of information include Text, numbers, pictures, audio and so-on.

2. Sender :
* The sender is the device that sends the data message.
* It can be computer, workstation, telephone handset, video camera & so on

3. Receiver : The receiver is the device that receives the message.

* It can be computer, workstation, telephone handset, television, and so on.

4. Transmission medium :

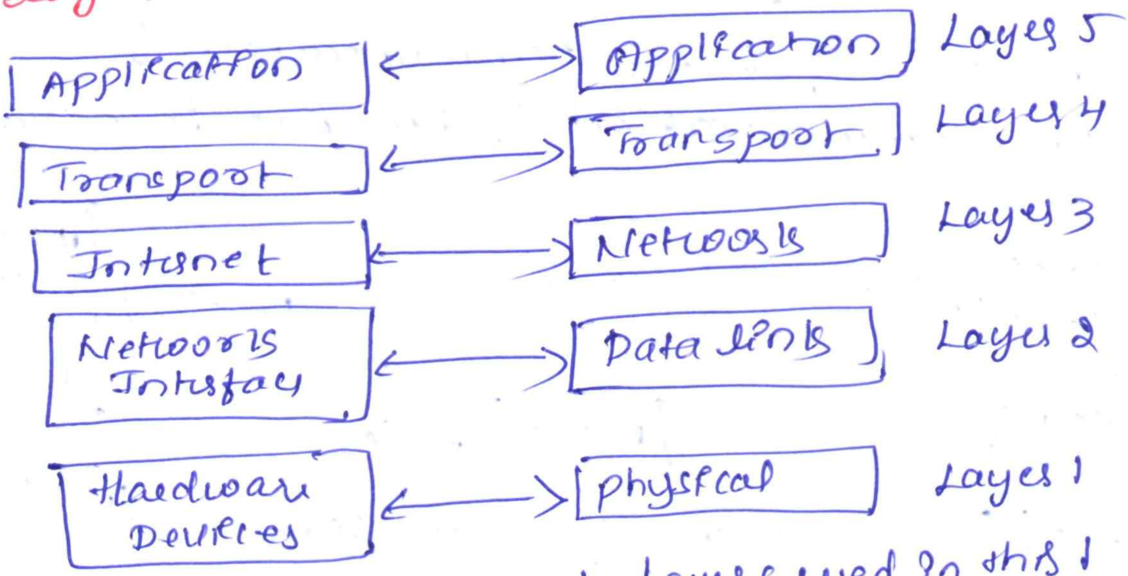
* The transmission medium is the physical path by which message travels from sender to receiver.
* Ex : twisted-pair wire, co-axial cable, fiber-optic cable, & radio waves.

5. Protocol :

* A set of rules that govern data communication.
* It represents an agreement b/w the communication devices.
* without a protocol two device can be connected but not communicating.

1b) with a neat diagram, explain the significance of layers in TCP/IP protocol suite (10M)

Ans >



a. original layers.

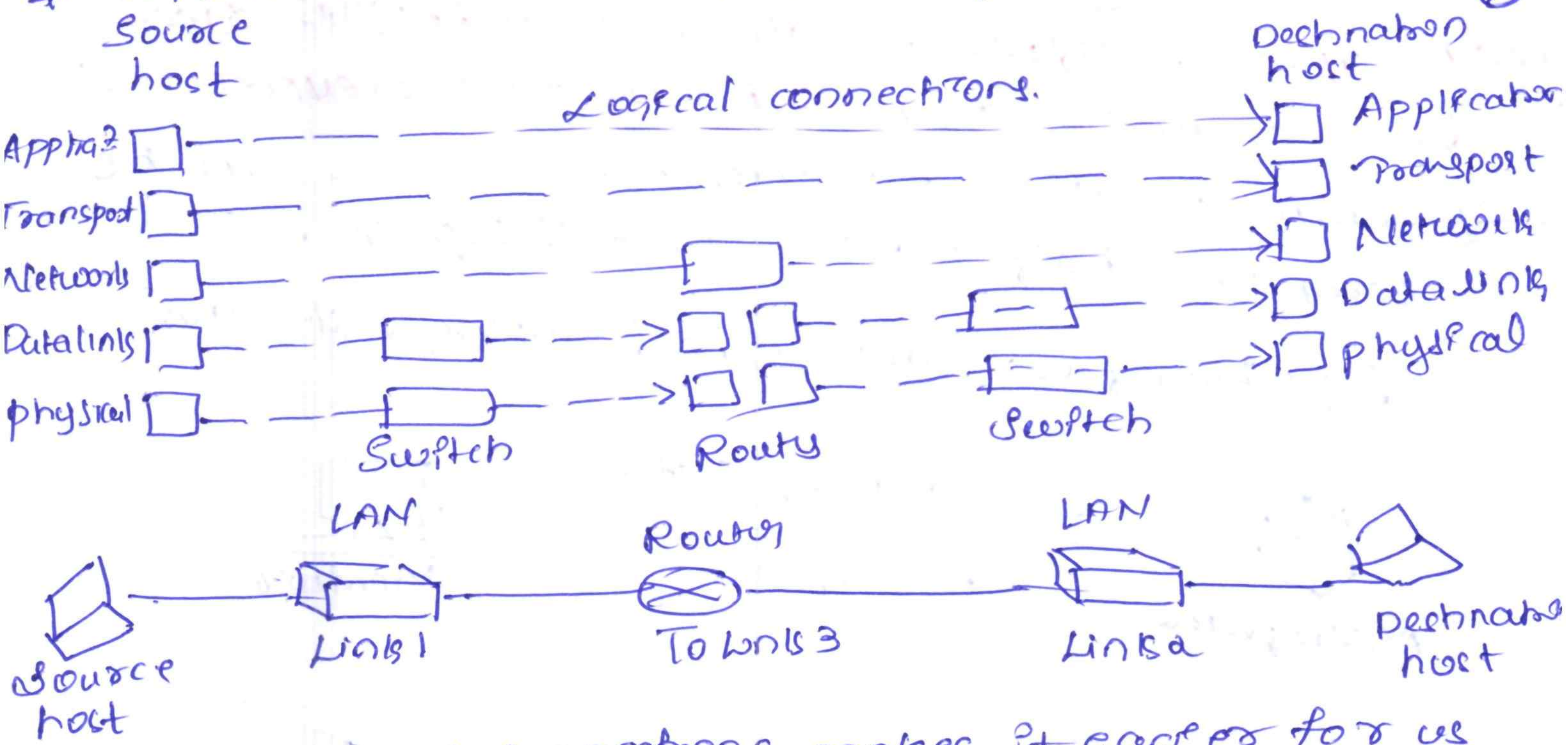
b. Layers used in this.

fig : Layers in TCP/IP protocol suite :

* The original TCP/IP protocol suite was defined as four software layers built upon the hardware.
* However, TCP/IP thought of as a five layer model

*

* Fig 2: Logical connection b/w layers in TCP/IP protocol



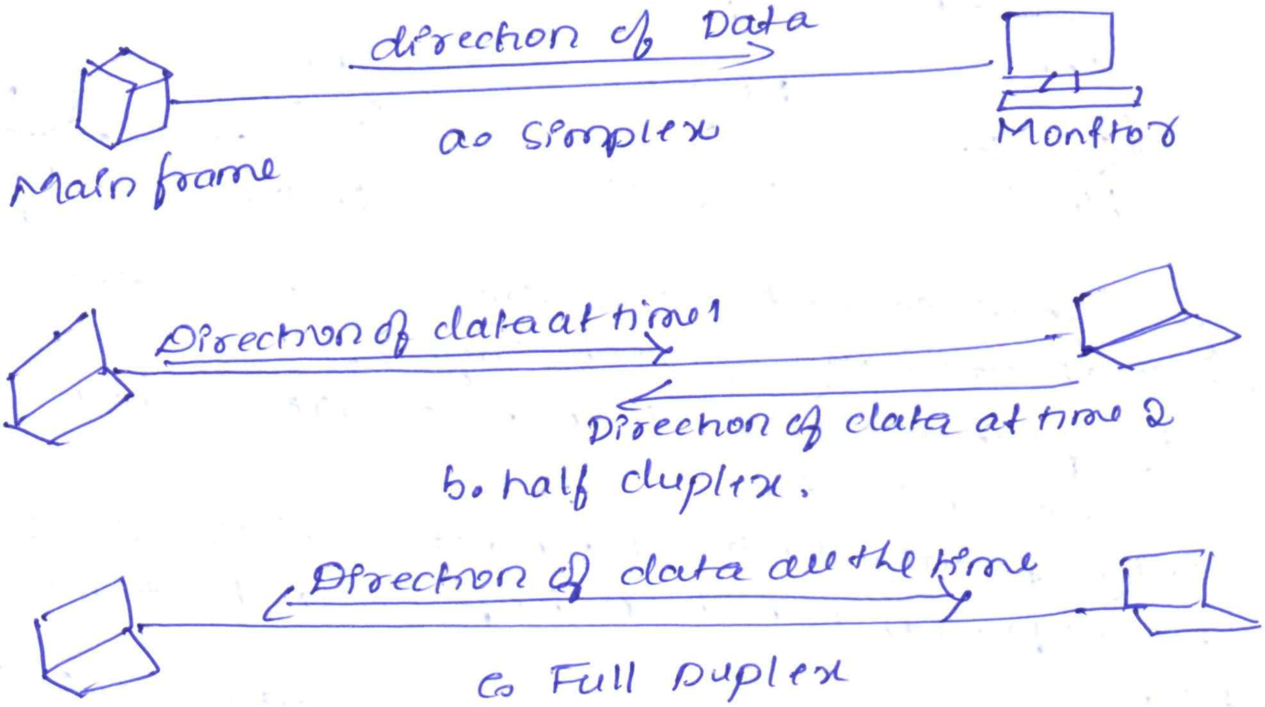
* using logical connections makes it easier for us to think about duty of each layers.
* The duty of application, transport, and network layers are end-to-end.
* The duty of data-link & physical layer is hop-to-hop, in which a hop is a host or router.
* In other words, the domain of duty of top 3 layers is internet, & domain of duty of two lower layer is link.
* In the top 3 layers, the data unit (packet) should not be changed by any router or link-layer switch.
* In the bottom two layers, the packet created by host is changed only by the routers, no by the link-layer switches.
* To better understand the duties or significance of Each layer, It is good using logical connection between two devices. as shown in fig 2

00

2a) Explain different data flow techniques used for communication between two devices (10m)

→ communication between two devices can be simplex, half Duplex, or full-Duplex.

fig: Data flow (simplex, half-duplex, Full-duplex)


direction of Data
Mainframe
Monitor
Direction of data at time 1
Direction of data at time 2
Direction of data all the time

a. simplex

b. half duplex.

c. Full Duplex

→ a. simplex mode :

* The communication is unidirectional, as on a one-way street.
* only one of the two devices on a link can transmit ; the other can only receive.

Ex: keyboard, monitors.

keyboard can only introduce i/p ; monitor can only accept o/p.

* The simplex mode can use entire capacity of channel to send data in one direction.

b. Half duplex :

* In this each stations can both transmit & receive, but not at the same time.
* while one device is sending, the other can only receive

* The half duplex mode is like one-lane road with traffic allowed in both direction.
Ex: walkie-talkies, & CB (citizens band) radios
* The half duplex mode is used in cases where there is no need for communication in both directions at the same time.
* Entire capacity of the channel can be utilized for each direction.

Full-Duplex:

* In full-duplex mode, both stations can transmit and receive simultaneously.
* The full-duplex mode is like two-way street with traffic flowing in both directions at the same time.
* signals going in one direction share the capacity of link with signal going in the other direction.
* This sharing can occurs in two ways:
Either the link must contains two physically separate transmission paths, one for sending & other for receiving.
Ex: telephone network.

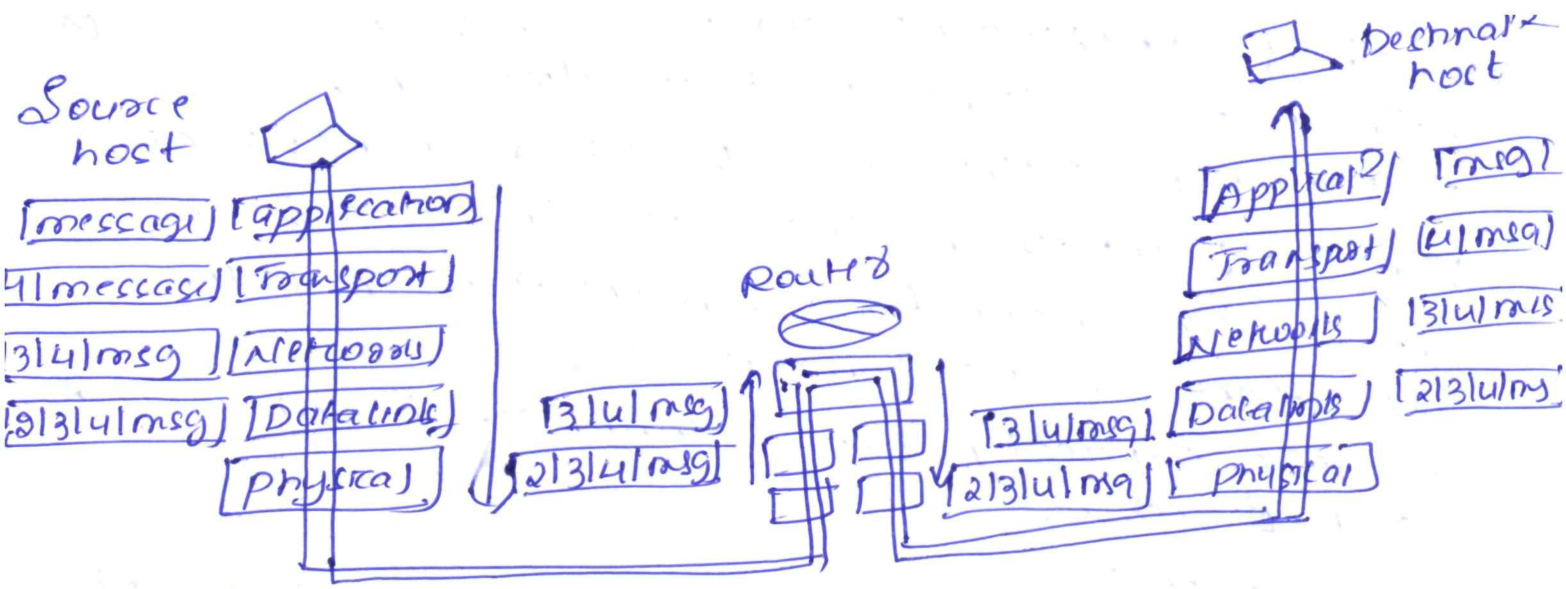
2b) with the neat diagram. illustrate the concept of encapsulation and decapsulation in Internet (10M)

Ans→ One of the important concept in protocol layering in the Internet is encapsulation / decapsulation.

Legend

[4] header at transport layer
[3] Header at nw layer
[2] Header at data-link layer
[1]

↓ Encapsulate
↑ Decapsulate.



Encapsulation ~~at~~ the source Host

1. at the source, we have only encapsulation.

1. At the application layer, the data to be exchanged is referred to as a message.

* a message normally doesnot given contain any header or trailer, but if does, we refers to the whole as the message. The message is passed to the transport layer.

2. The transport layer takes the message as the payload, the load that the transport layer should take care of.

* It adds the transport layer header to the payload, which contains the identifiers of the source and destination application programs that want to communicate plus some more information that is needed for the end-to-end delivery of message.

3. The network layer takes the transport-layer packet as data or payload & adds its own header to the payload.

4. The data-link link layer takes the nlw layer packet as data or payload & add its own header, which contains link-layer addresses of the host or the next hop.

Decapsulation & Encapsulation at the Router

At router we have both encapsulation & decapsulation because the router is connected to two or more links.

1. After the set of bits are delivered to the data-link layer, this decapsulation the datagram from the frame & passes it to the n/w layer.

2. The network layer only inspects the source & Destination addresses in the datagram header & consults its forwarding table to find next hop to which datagram is to be delivered.

3. The data-link layer of the next link encapsulates the datagram in a frame & passes it to the physical layer for transmission.

Decapsulation at the Destination host :

- At the destination host, each layer only decapsulates the packet received, removes the payload, & delivers the payload to the next-higher layer protocol until the message reaches the application layer.

MODULE — 02

3a) Explain how the collisions are avoided through the use of CSMA/CA's three strategies with flow diagram. (10M)

Ans:- Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for wireless networks.

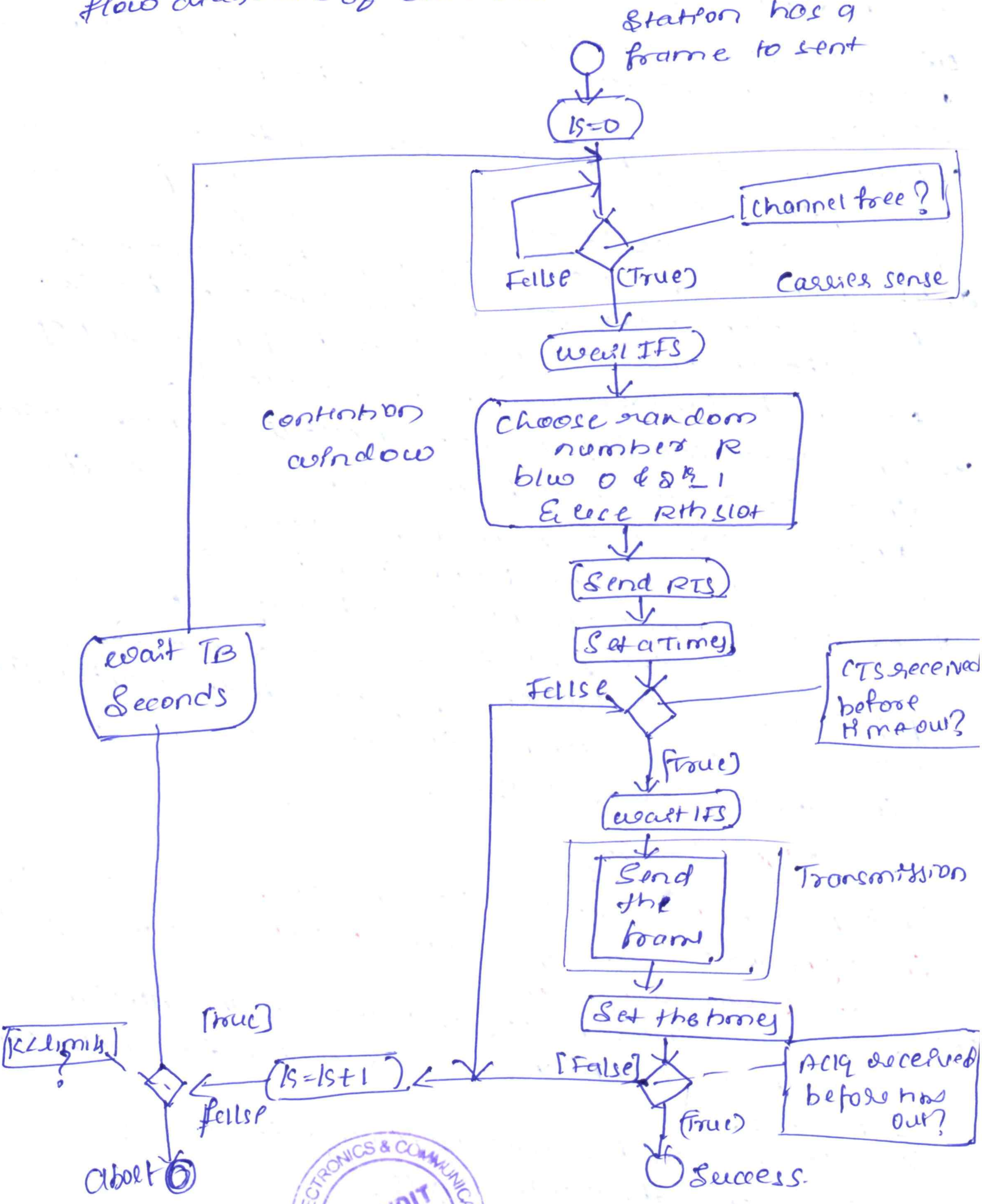
- Collisions can be avoided through the use of CSMA/CA's three strategies.

(i) the interframe space,

(ii) Contention window

(iii) acknowledgements.

flow diagram of CSMA/CA

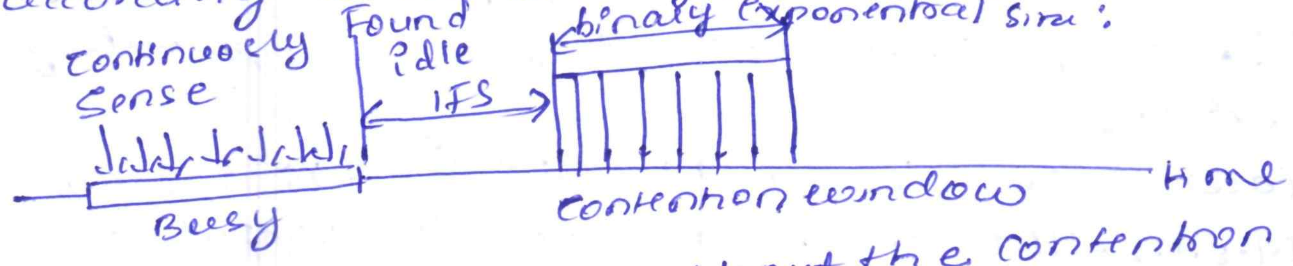


(i) Interframe space (IFS) :

- collisions are avoided by deferring transmission even if the channel is found idle.
- when an idle channel is found, the station does not send immediately.
- It waits for a period of time called interframe space. or (IFS)
- Eventhough channel may appear idle when it is sensed, a distinct station may have already started transmitting. distant station has not yet reached.
- The IFS time allows the front of the transmitted signal by distant station to reach this station.
- after awaiting an IFS time, if the channel is still idle, the station can send, but it still need to wait a time equal to contention window.

(ii) Contention window :

- Contention window is an amount of time divided into slots.
- A station that is ready to send chooses a random number of slot in the window changes according to the binary exponential backoff strategy



- One interesting point about the contention window is that the station needs to sense the channel after each time slot.
- This gives priority to the station with longest waiting time.

(iii) Acknowledgement : With All these precautions, there still may be collision resulting is destroyed data.

- the data may be corrupted during the transmission.
- The positive acknowledgement and the time out timer can help guarantee that the receiver has received the frame.

3b) A Slotted Aloha n/w. transmits 200 - bit frames on a shared channel of 200kbps. what is the throughput of the system (all station together) produces : (06M)

a. 1000 frames per seconds?

b. 500 frames per seconds?

c. 250 frames per seconds?

Ans The situation is similar to the previous exercise except that the n/w is using slotted ALOHA instead of pure ALOHA.

The frame transmission time is 200/200 kbps in 1ms.

a. In this case G is 1. So S = $G \times e^{-G} = 0.368$ (36.8 percent) This means that the throughput is 1000 × 0.0368 = 368 frames. only 368 out of 1000 frames will probably survive. Note that this is the maximum throughput case, percentagewise.

b. Here G is 1/2. In this case S = $G \times e^{-G} = 0.303$ (30.3 %). this means throughput is 500 × 0.0303 = 151. only 151 frames out of 500 will probably survive.

c. Now G is 1/4, In this case S = $G \times e^{-G} = 0.195$ (19.5 %). This means that the throughput is 250 × 0.195 = 49. only 49 frames out of 250 will probably survive.

3c) Explain Ethernet frame format of Standard Ethernet (4M)

→ Preamble: 56 bits of alternating 1s & 0s

SFD: start frame delimiter, flag (10101011)

minimum payload length: 46 bytes

maximum payload length: 1500 bytes

Preamble	SFD	Destination address	Source address	Type	Data & padding	CRC
7 bytes	1 byte	6 byte	6 byte	2 byte		4 byte

Physical-layer header

Minimum frame length: 512 bits or 64 bytes

maximum frame length: 12,144 bits or 1518 bytes.

preamble :

* This field contains 7 byte (56 bits) of alternating 0s & 1s that alert the receiving system to the coming frame & enable it to synchronize its clock if its out of synchronization.
* The pattern provides only an alert and a timing pulse
* The 56 bit pattern allows the stations to miss some bits at the beginning of the frame.
* The preamble is actually ~~at the~~ added at the physical layer and is not part of the frame.

Start of delimiter (SFD):

* This field (1 byte : 10101011) signals the beginning of the frame.
* The SFD warns the station or station that this is the last chance for synchronization.
* The last bit (2 bits are (11)₂ and alert the receiver that next field is destination address.
* This field is actually a flag that defines the beginning of the frame.

Destination address (DA)

* The field is six bytes (48 bits) & contains the link layer address of destination station or stations receive the packet.

Source address (SA)

* This field is also six bytes and contains the link-layer address of the sender of the packet.

Type : This field defines the upper-layer protocol whose packets is encapsulated in the frame.
* The protocol can be IP, ARP, OSPF, & so on.

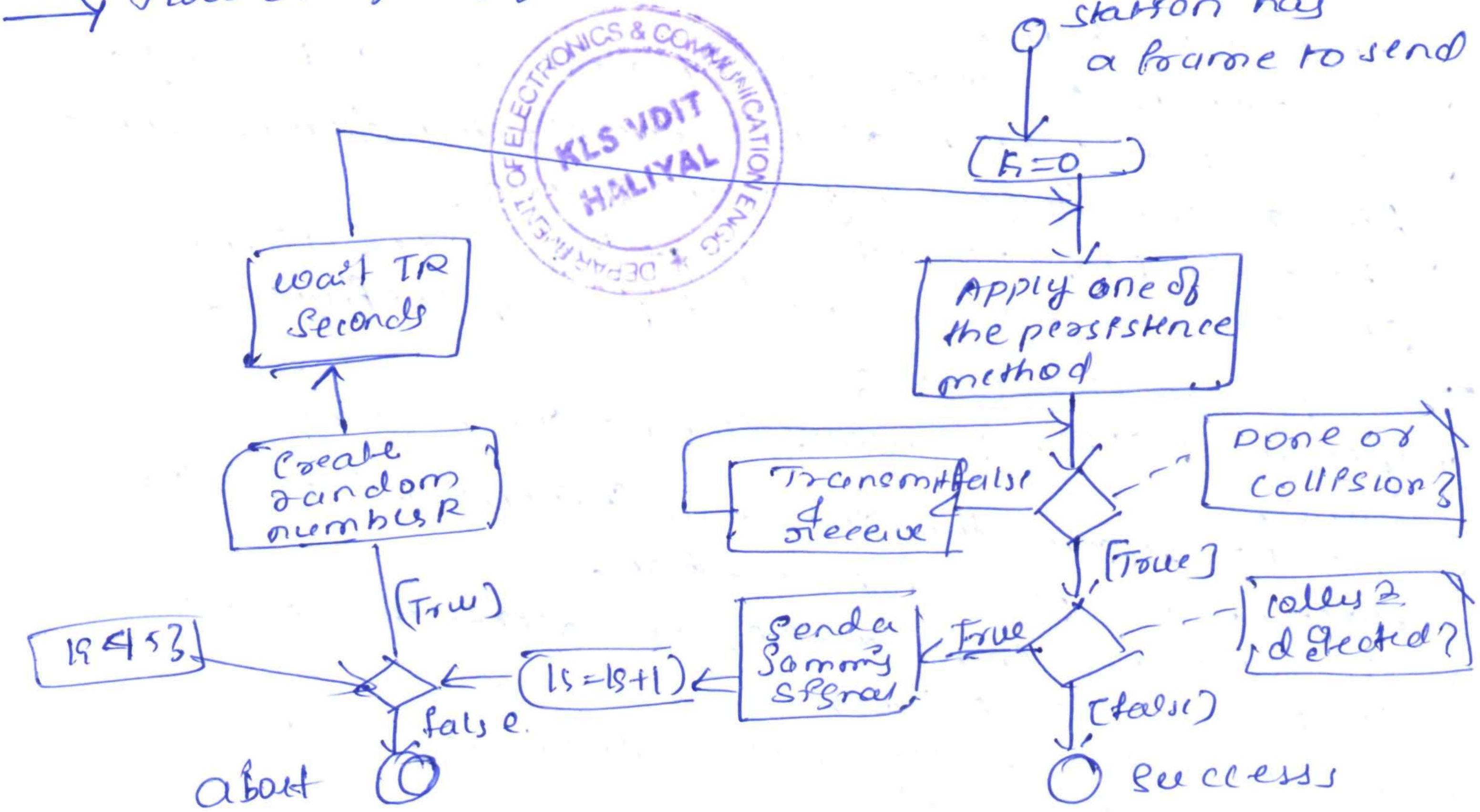
Data : This field carries data encapsulated from the upper-layer protocols.
* If the data coming from upper layer is more than 1500 bytes, it needs to be padded with extra 0s.

CRC: * The last field contains error detection information.
* In CRC-32. The CRC is calculated over address, type & data field.

OR

4a) Explain CSMA/CD working with help of flow Chart (10m)

→ Flow diagram of CSMA/CD



* It is similar to the one for the aloha protocol but there is differences.

* The first difference is the addition of the persistence process. we need to sense the channel before we start sending the frame by using one of the persistence process

* The corresponding box can be replaced by one of the persistence process.

* The second difference is the frame transmission.

* In ALOHA, we first transmission entire frame & then wait for an acknowledgment.

* In CSMA/CD, transmission & collision detection are continuous processes.

* we do not send the entire frame & then look for a collision.

* The transmits & receives continuously & simultane

* we use loop to show transmission lagges is continuous process.

* we constantly monitor in order to detect one of (+) two condition : either transmission is finished or collision is detected, either event stops transmissio

45) Explain the architectural comparision of Wireless LANs and List the characteristics of wireless LANs (10M)

Ans) Medium :

* The first difference we can see b/w wired & wireless LAN is the medium.
* In wired LAN, we use wires to connect hosts.
* In wireless LAN, the medium is air, the signal is generally broadcast.
* when the host in the a wireless LAN communicate with each other, they are sharing the same medium
* In a very rare situation, we may not be able to create point-to-point communication b/w two wireless hosts by using a very limited bandwidth & two-directional antennas.

Hosts :

* In a wired LAN, a host is always connected to its n/w at a point with a fixed link-layer address related to its n/w interface card (NIC).
* a host can move from one point in the internet to another point.
* In this case, its link-layer address remains the same, but its n/w layer address will change.
* In wireless LAN, a host is not physically connected to the network; it can move freely & can use the services of the Internet, it needs to the network;
* it can move freely & can use the services provided by the n/w.
* mobility in a wired n/w & wireless n/w are totally different issues.

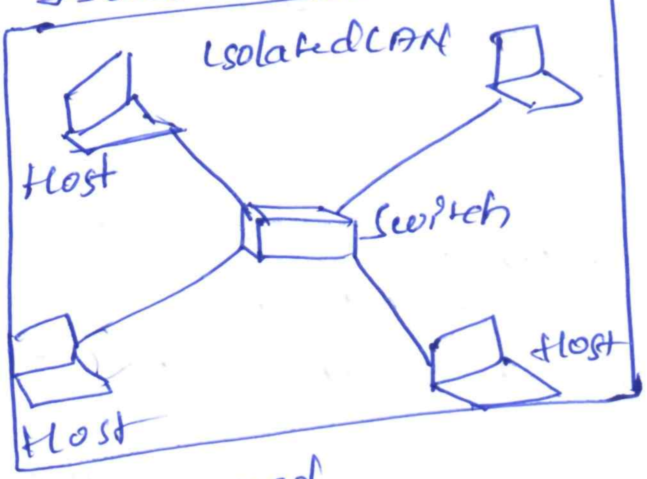
Isolated LAN

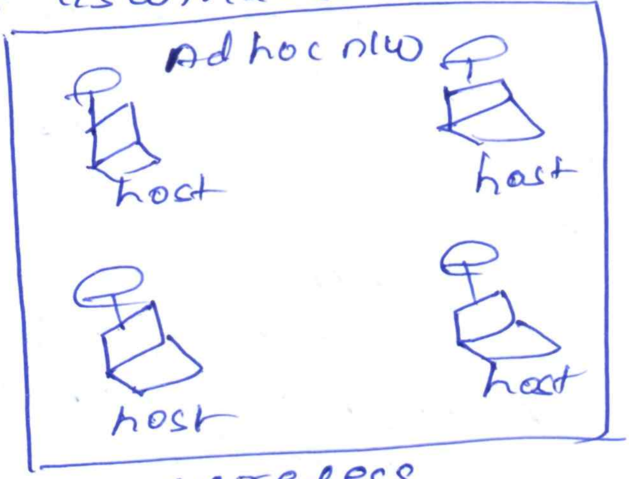
- The wired isolated LAN is a set of hosts connected via - link - layer switch.
- A wireless isolated LAN, called an ad hoc network in wireless LAN terminolgy, is set of hosts that communicate freely with each other.
- The concept of link - layer switch doesnot exist in wireless LANs.

Connection to other networks:

- a wired LAN can be connected to another network such as the internet using or an internetwork a router
- A wireless LAN may be connected to a wired infrastructure n/w, to a wireless n/w, or to another wireless LAN.

Isolated LANs: wired vs wireless

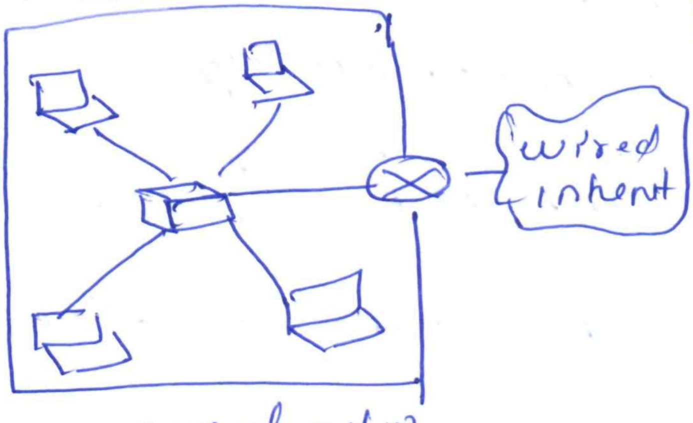


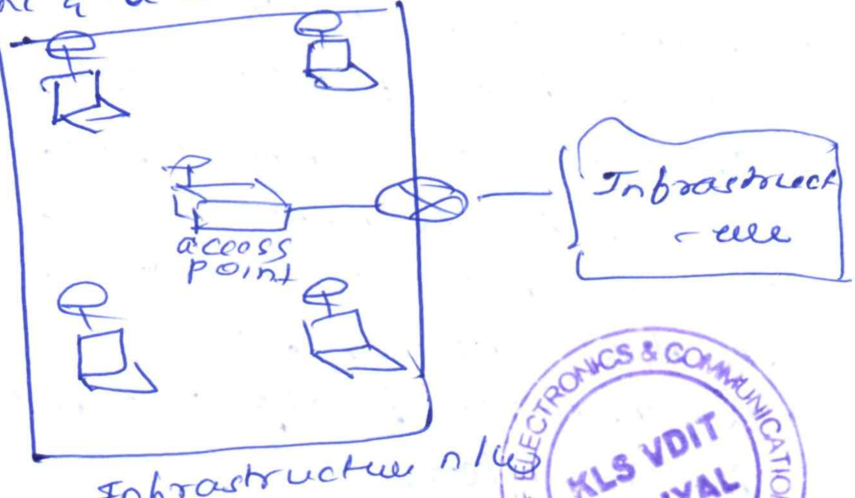


wireless.

wired

Connection of wired LAN & a wireless LAN to other n/w





wired n/w.

Infrastructure n/w

MODULE - 03

5a) write a note on security of IPV4 datagrams. (10M)

ans> There are 3 security issues that are particularly applicable to the IP protocol:
*packet sniffing, packet modification, & IP spoofing

→ Packet sniffing:

* An intruder may intercept an IP packet & make a copy of it. Packet sniffing is a passive attack, in which the attacker does not change the content of the packet.
* This type of attack has been very difficult to detect because the sender & the receiver may never know that the packet has been copied.
* Allathough packet sniffing cannot be stopped.
* Encryption of the packet can make the attacker's may still sniff the packet, but the content is not detectable.

→ Packet Modification:

* The second type of attack is to modify the packet.
* The attacker intercepts the packet, changes its contents, & sends the new packet to the receiver.
* This type of attack can be detected using a data integrity mechanism.
* The receiver, before opening and using contents of message, can use this mechanism to make sure the packet has not been changed during the transmission

→ IP Spoofing:

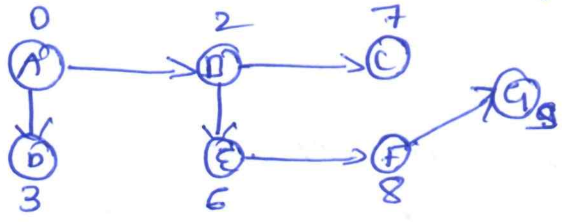
* an attacker can masquerable as somebody else & create an IP packet that carries the Source address of another computer.
* an attacker can send an IP packet to a bank pretending that it is coming from one of the customers.
* This type of attack can be authenticated or prevented using an origin authentication mechanism.

5b) with suitable diagram expeain distance vector routing. (10M)

ans → Distance-vector Rouring :

- The distance-vector (DV) routing uses the goal ~~w~~ to find the best route.
- In distance-vector routing, the first thing each node creates is its own least-cost tree with the rudimentary information it has about its immediate neighbors.
- The incomplete trees are exchanged b/w immediate neighbors to make the tree more & more complete & to represent the whole internet.
- We can say that in distance-vector-routing, a router continuously tells all of its neighbors what it knows about the whole internet.

'distance vectors corresponding to a tree



a. Tree for node A

	A
A	0
B	2
C	7
D	3
E	6
F	8
G	9

b. distance vector for node A

- The concept of distance vector is rationale for the name distance-vector routing.
- The least-cost tree is a combination of least-cost paths from the root of the tree to all destination
- These path are graphically glued together to form the tree.
- Distance-vector routing unglues these paths & creates a distance vectors a one-dimensional array to represent the tree.
- The name of the distance vector defines the root, the ~~de~~ indexes defines the destinations, and the value each cell defines the least cost from the root to the destination

* A distance vector doesnot give the path to the destination as the least-cost trees does ; it gives only the least cost to the destinations.

* Each node in an internet, when it boosted, creates a very rudimentary distance vector with the minimum information the node can obtain from its neighborhood

* It then makes a simple distances vector by inserting the discovered distances in the corresponding cells & leaves the value of other cell as infinity.

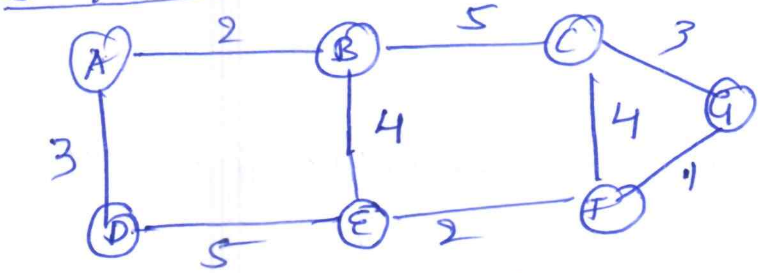
or

5a) Explain with an Example, Link State Routing and also Dijkstra algorithm to find least cost path tree (10m)

→ A routing algorithm that directly follows our discussion for creating least-cost trees and forwarding tables is link-state (LS) routing.

→ This method uses the term link-state to define the characteristics of a link (on edge) that represents a node in the internet.

Link-State DataBase (LSDB)



a. The weigh graph

A	0	2	∞	3	∞	∞	∞
B	2	0	5	∞	4	∞	∞
C	∞	5	0	∞	∞	4	3
D	3	∞	∞	0	5	∞	∞
E	∞	4	∞	5	0	2	∞
F	∞	∞	4	∞	2	0	1
G	∞	∞	3	∞	∞	1	0

b. linkg state database.

* To create a least-cost tree with this method, each node needs to have a complete map of the network, which means it needs to know the state of each link.

* The collection of states for all links is called link-state Database (LSDB).

* There is only one LSDB for the whole internet: each node needs to have duplicate of its to be able to create the least-cost tree.

* The LSDB can be represented as the two-dimensional array (matrix) in which the value of each cell define the cost of the corresponding link.

* Each node can send can send some greeting message to all its immediate neighbors to collect two piece of information for each neighbours node: the identity of the node & the cost of link.

* The combination of these two piece of information is called LS packets (LSP) & the LSP is sent out of each interface.

→ Dijkstra algorithm to find least cost trees.

1. The node choose itself as the root of the tree, creating a tree with single node, & set the total costs of each node based on the information in LSDB.
2. The node selects one node, among all nodes not in the tree, which is closest to the root, & adds this to the tree. after this node is added to the tree, the cost of all other nodes not in the tree needs to be updated because the paths may have been changed.
3. The node repeat step 2 until all nodes are added to the tree.

```
Dijkstra's Algorithm()
{
    Tree = {root}                  // Tree is made only ~~root~~ the root
    for (y=1 to N)
    { if (y is the root)
          D[y]=0
      else if (y is neighbour)
          D[y] = c[root][y]
      else
          D[y] = ∞
    }.

    // calculation
    repeat
    {
      find a node w, with D[w]
      Tree = Tree ∪ {w}
      for (every node x, which is a
      neighbour of w & not in Tree)
      {
        D[x] = min {D[x], (D[w], + c[w][x]}
      }
    } until (all nodes included in the Tree)
} // end of Dijkstra
```

6B) Explain working of DHCP (Dynamic host configuration protocol. (10m)

Ans ⇒ * DHCP is an application-layer program, using the client - server paradigm, that actually helps TCP/IP at network layer.

* DHCP has found such ~~app~~ widespread use in the Internet that it is often called a plug - and-play protocol.

* It can be used in many situations. A n/w manager configure DHCP to assign permanent IP addresses to the host & routers.

* DHCP can also be configured to provide temporary,

* The second capability can provide a temporary IP address to a traveller to connect her laptop to the Internet while she is staying in hotel.

* It also allows an ISP with 1000 granted addresses to provide services to 4000 households, assuming not more than one forth of customer use the Internet at the time.

* A computer also needs to know the network prefix.

* Most of the computer also need two pieces of information, such as the address of default router to be able to communicate with other networks and all the address of a name server to be able to use name instead of addresses.

* DHCP can be used to provide these piece of information to the host.

* address assignment in a organization can be done automatically using Dynamic Host configuration protocol (DHCP).

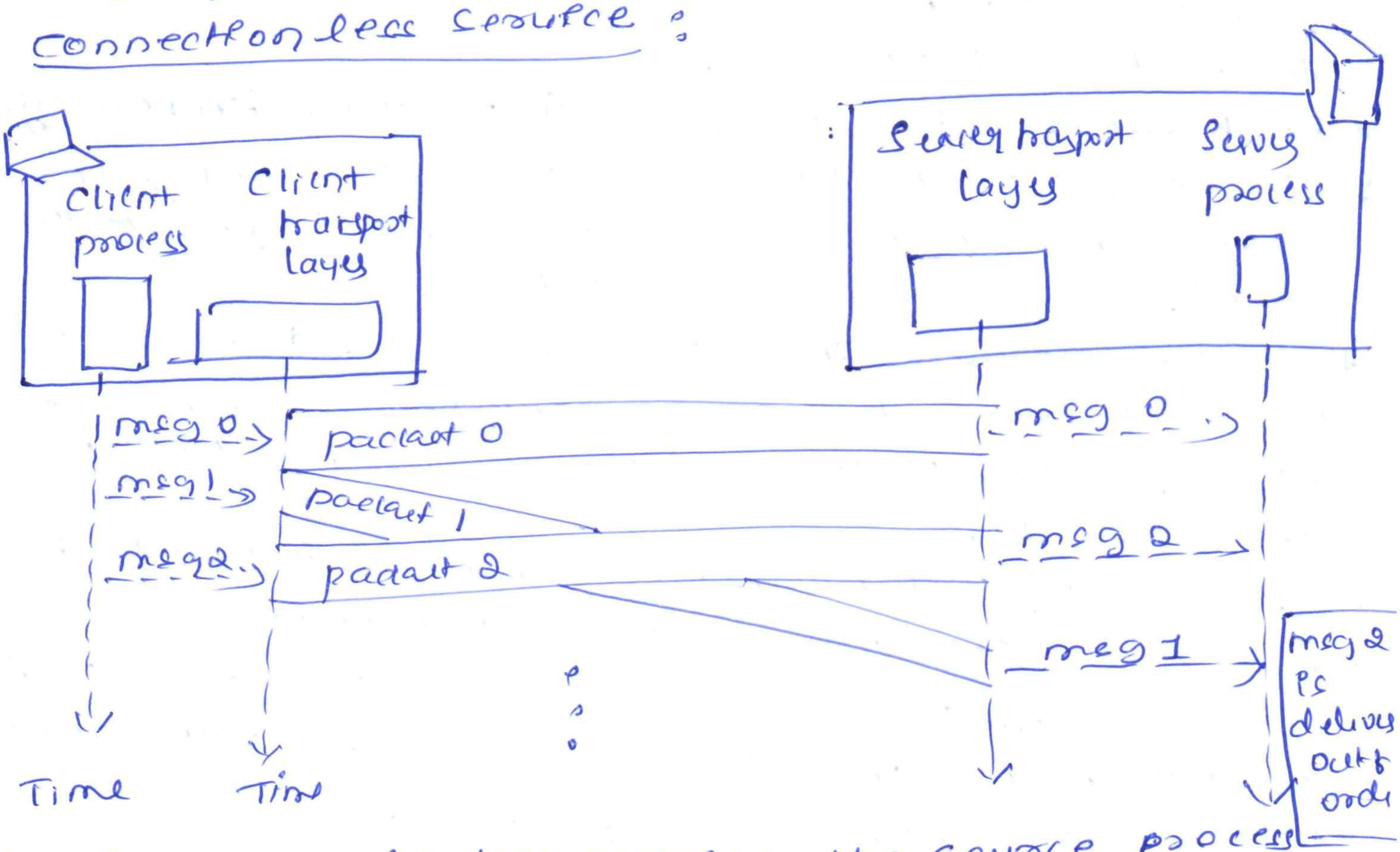
MODULE - 04

7a) Describe the connectionless & connection-oriented services provided by transport layer

ans ⇒ A transport-layer protocol, like a n/w layer protocol, can provide two type of services: connectionless & connection-oriented.

* The nature of these services at the transport layer, however, is different from one at the n/w layer.

Connectionless service :



→* In a connectionless service, the source process needs to divide its message into chunks of data of size acceptable by the transport layer & deliver them to the transport layer one by one.

* when chunk arrives from the application layer, the transport layer encapsulates it in a packet & send it.

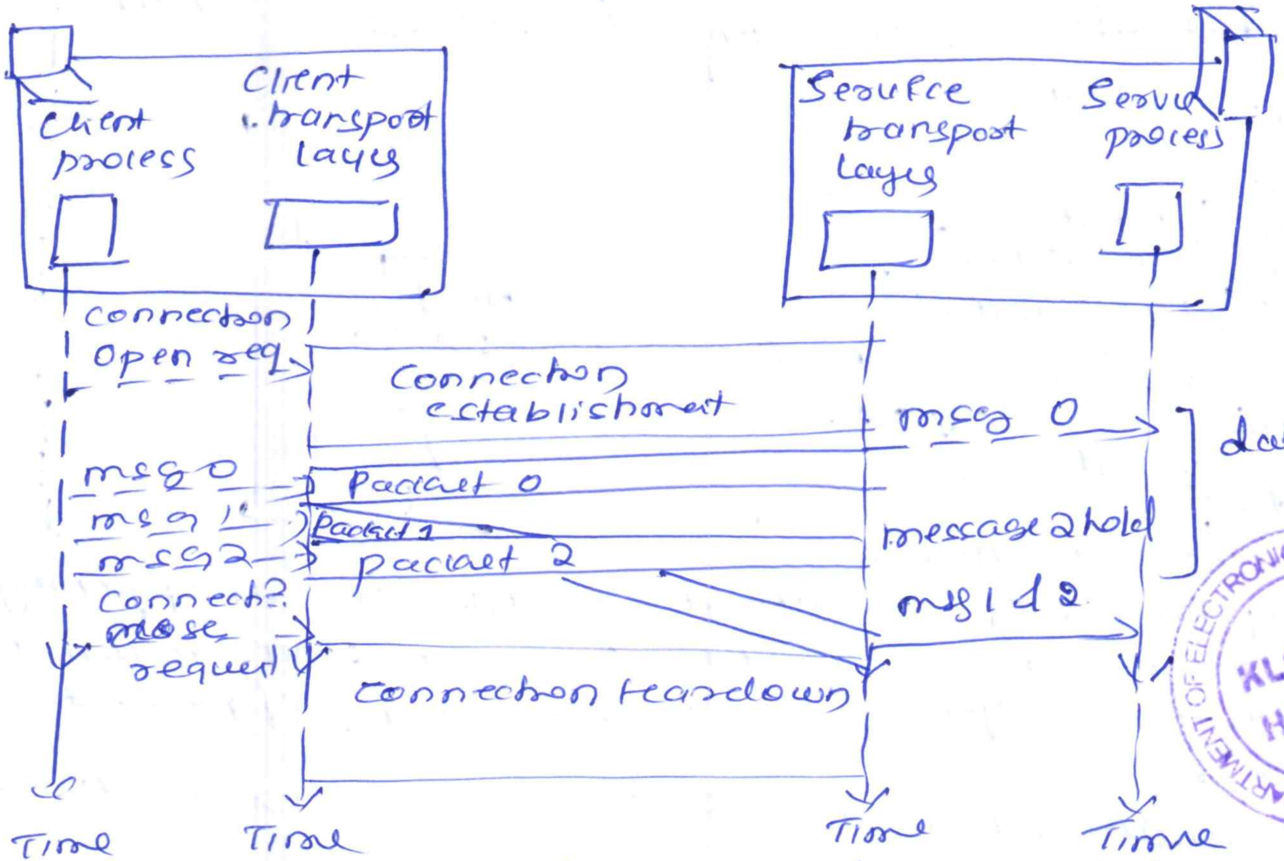
* To show the independency of packets.

* movement of packet using a time line, but we have assumed that the delivery of process to transport layer & vice versa are instantaneous.

order (0, 2, 1). If these three chunks of data belonge to the same message, the server process may have received a strange message.

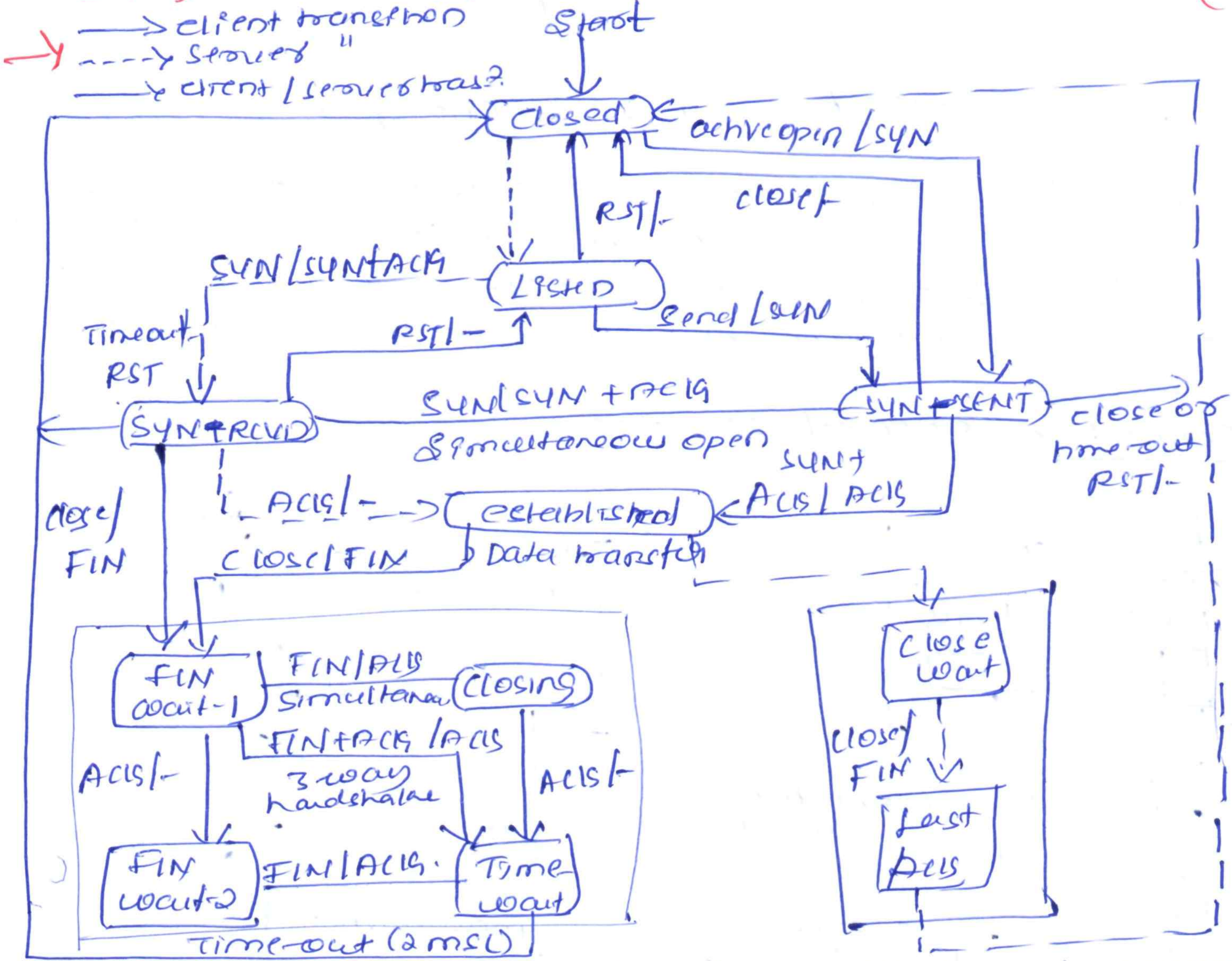
- Situation would be worse if one of the packets were lost.
- The above two problems arise from the fact that the two transport layers donot coordinate with each other.
- we can say no flow control, error control, or congestion control can be effectively implemented in connectionless service.

Connection-oriented service



- In this the client & server first need to established a logical connection b/w themselves.
- is different from same device at the n/w layer.
- In n/w layer connection oriented means coordination b/w two end hosts and all the routers in b/w.
- At the transport layer, connection-oriented service involve only the host; the service is end to end.
- This means that we should be able to make a connection-oriented protocol at the n/w layer.
- Connection-establishment, data-transfer, & teardown phase in connection oriented service at transport layer.

7b) with neat diagram, expalin state transition diagram in TCP. (10M)

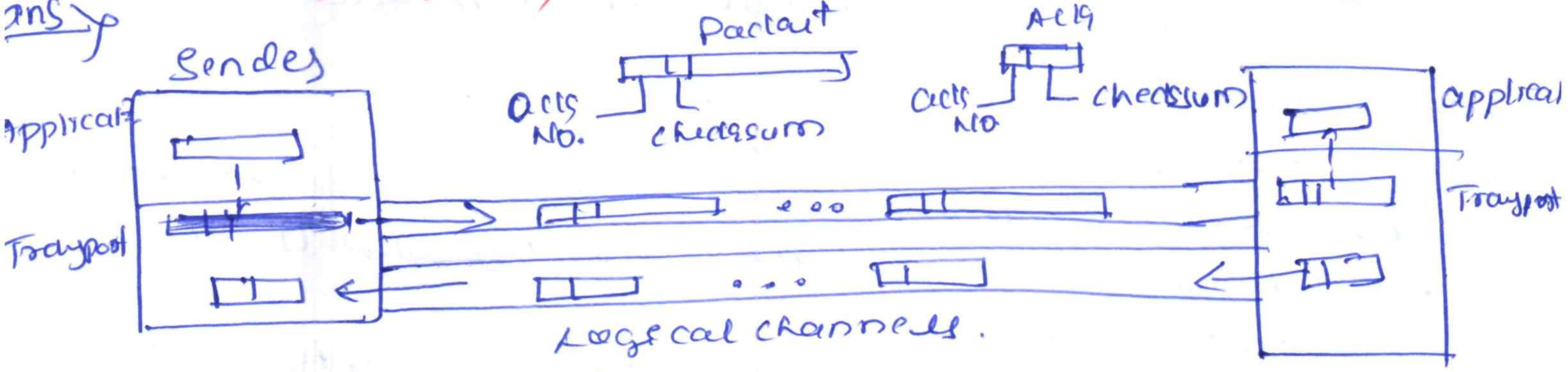


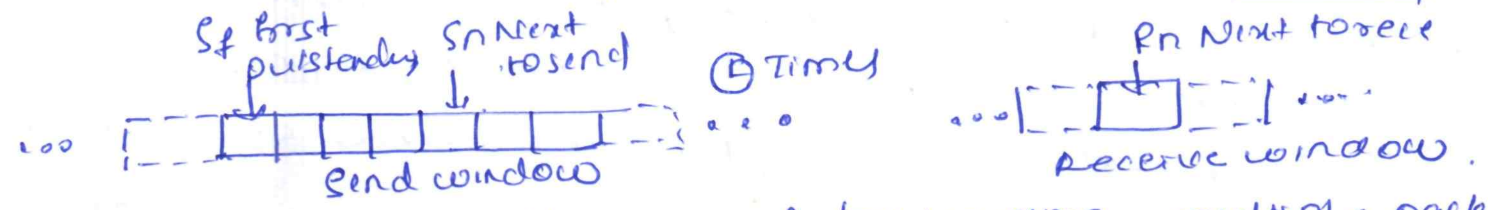
- To keep track of all different events happening during connection establishment, connection termination, & data transfer, TCP is specified as FSM (finite state machine).
- The transition from one state to another is shown using directed lines.
- Each line has two strings separated by a slash.
- the first string is input, what TCP receives.
- The second is o/p, what TCP sends.
- The dotted ~~black~~ line represent the transition that client normally go through.
- Coloured line show special situations.
- Rounded-corner rectangle marked ESTABLISHED in fact two sets of states, set for client & set for server, that are used for flow & error control.

or

8a) Explain Go-Back-N protocol along with Sliding window diagram (10M)

Ans →



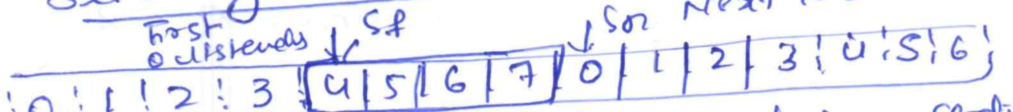


* To improve the efficiency of transmission, multiple packets must be in transition while sender is waiting for acknowledgement.

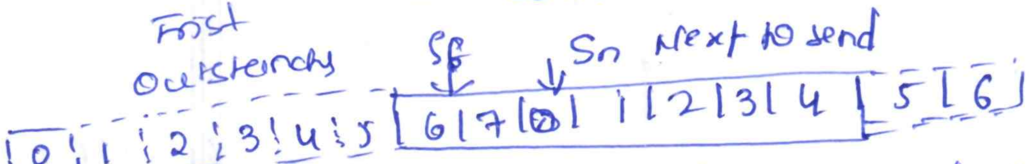
* we need to let more than one packet be outstanding to keep channel busy while the sender is waiting for acknowledgment.

* The key to Go-Back-N is the we can send several packets before receving acknowledgments, but receiver can only buffer one packet. we keep the copy of sent packets until acknowledgement arrives.

Sliding the send window



a. window before sliding



b. window after sliding (n=6 has arrived)

→ fig shows how a send window can slide one or more slots to the right when a acknowledgment arrives from the other end.

→ an acknowledgement with ackNo = 6 has arrived.

→ This means that the receiver is waiting for packet with sequence number 6.

8b) Describe General services provided by UDP (10m)

ANS -> i) process to-process communication:

* UDP provide process-to-process communication using socket addresses, a combination of IP addresses & port numbers.

ii) Connection less service:

* UDP provides a connectionless services, This means that each user datagram sent by UDP is an independent datagram.

* There is no relationship b/w the different user datagrams even if they are coming from same source process & going to the same destination program.

* One of ramifications of being connectionless is that the process that uses UDP cannot send a stream of data to UDP and expect UDP to chop them into different, related user datagram.

* Instead each request must be small enough to fit into one userdatagram.

Flow control: UDP is a very simple protocol.

* There is no flow control, & hence no window mechanism.

* The receiver may overflow with incoming messages.

* The lack of flow control means that process using UDP should provide for this service, if needed.

Error control:

* There is no error control mechanism in UDP except for the checksum.

* This means that the sender doesnot know if a message has been lost or duplicated.

* When the receiver detects an error through the checksum.

* user datagram is silently discarded.

* The lack of error control means that the processing

using UDP should provide for this resource, if needed.

Checksum:

* UDP checksum calculation includes three section. The pseudoheader is the part of header of the IP packet in which user datagram is to be encapsulated with some fields filled with 0's.

MODULE-05:

9a) Explain the following (i) HTTP
(ii) FTP.

ans → (HTTP) — * Hyper Text Transfer protocol is used to define how the client-server programs can be written to retrive webpages from the web.

* A HTTP client sends a request; an HTTP server returns a responses.

* The server uses the port number 80; the client uses a temporary port number.

* HTTP uses services of TCP, & is connection-oriented & reliable protocol. means before any transaction b/w client & server can take place, a connection needs to be established b/w them. after the transaction, the connection should be terminated.

* The client & server, however donot need to worry about errors in messages exchanged or loss of any message, because the TCP is reliable & will take care of the matter.

Non-persistent connections:

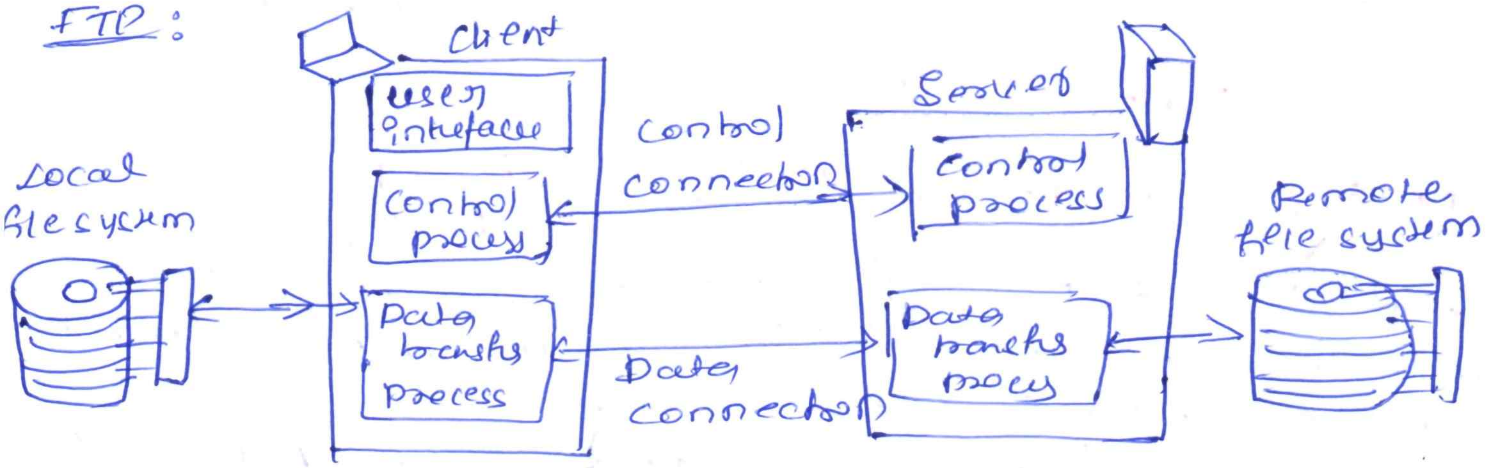
* In a nonpersistent connection, one TCP connection is made for each request / responce.

1. The client opens a TCP connection & sends a request
2. The server sends the response & closes the connection.
3. The client reads the data until it encounters an end-of file marker; it then closes the connection.

ii) FTP : File transfer protocol : is the standard protocol provided by TCP/IP for copying a file from one host to another.

* although transferring files from one system to another seems simple & straightforward, some problem must be dealt with first.

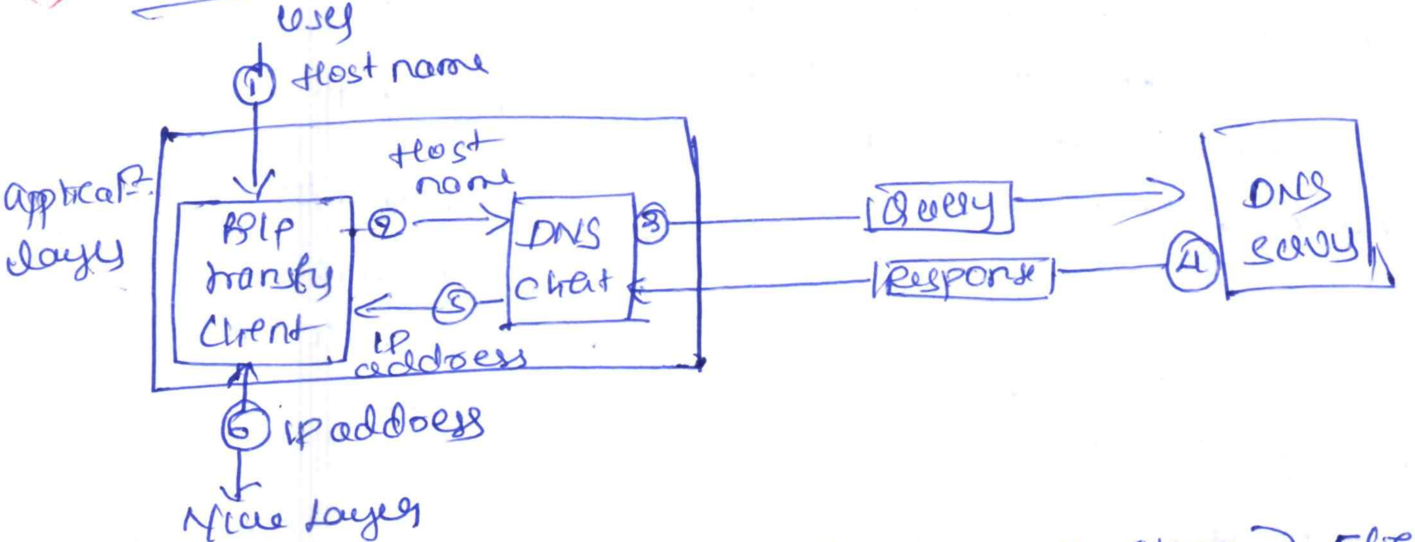
FTP :



* Two systems may have different ways to represent data,
* Two system may have different directory structure
* all ~~of~~ these problems have been different directory structure.
* all ~~of~~ these problems have been solved by FTP in a very simple & elegant approach.
* Although we can transfer files using HTTP, FTP is better choice to transfer large files or to transfer files using different formats.
* The client has 3 components : the user interface, the client ~~prot~~ control process, & client data transfer process.
* The server has 2 components : server control process & server data transfer process.
* The control connection is made b/w control process.
* The data connection is made b/w data transfer process.
* Separation of commands & data transfer makes FTP more efficient.
* The control connection uses very simple rules of communication.

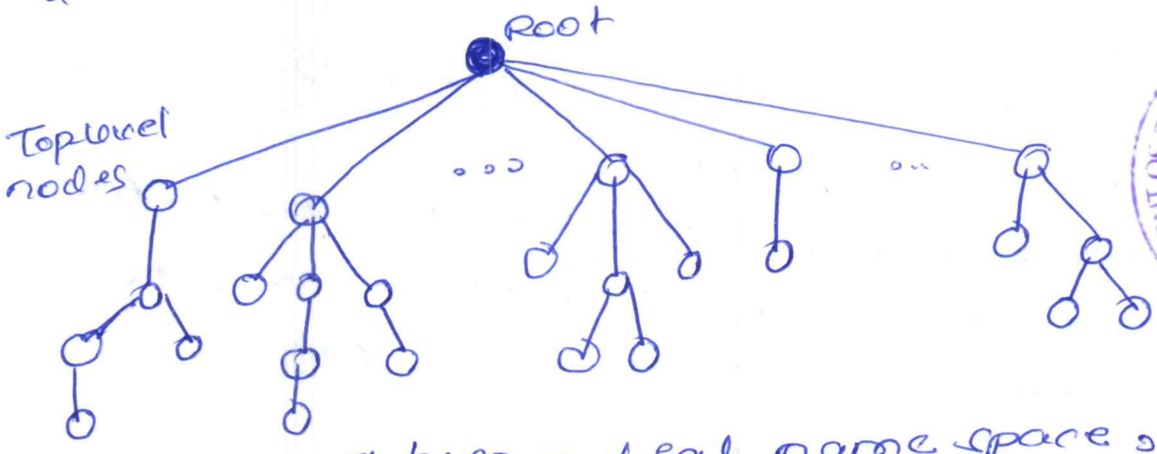
9b) Explain DNS Name space, DNS in Internet and Resolution (10M)

Ans) DNS Name Space :



* TCP/IP uses a DNS (Domain Name system) client & DNS server to map a name to an address.

* A user wants to use a file transfer client to access the corresponding file transfer server running on a remote host.



* To have a hierarchical name space, a domain name space was designed.

* In this design the name are defined in an inverted-tree structure with root at the top. The tree can have only 128 Levels : Level 0 (root) to level 127 ;

Label : Each node in the tree has a label, which is string with maximum of 63 characters.

* The root label is null string (empty string).

* DNS requires that children of a node have diffrent labels

DNS in the Internet

- DNS is a protocol that can be used for different platforms.
- In the Internet, the DNS was originally divided into three different section.
  ① Generic domains ② country domains & inverse domains, ~~country~~
- However due to rapid growth of the Internet.
- It became extremely difficult to keep track of the inverse domain, which could be used to find the name of host when given the IP address.

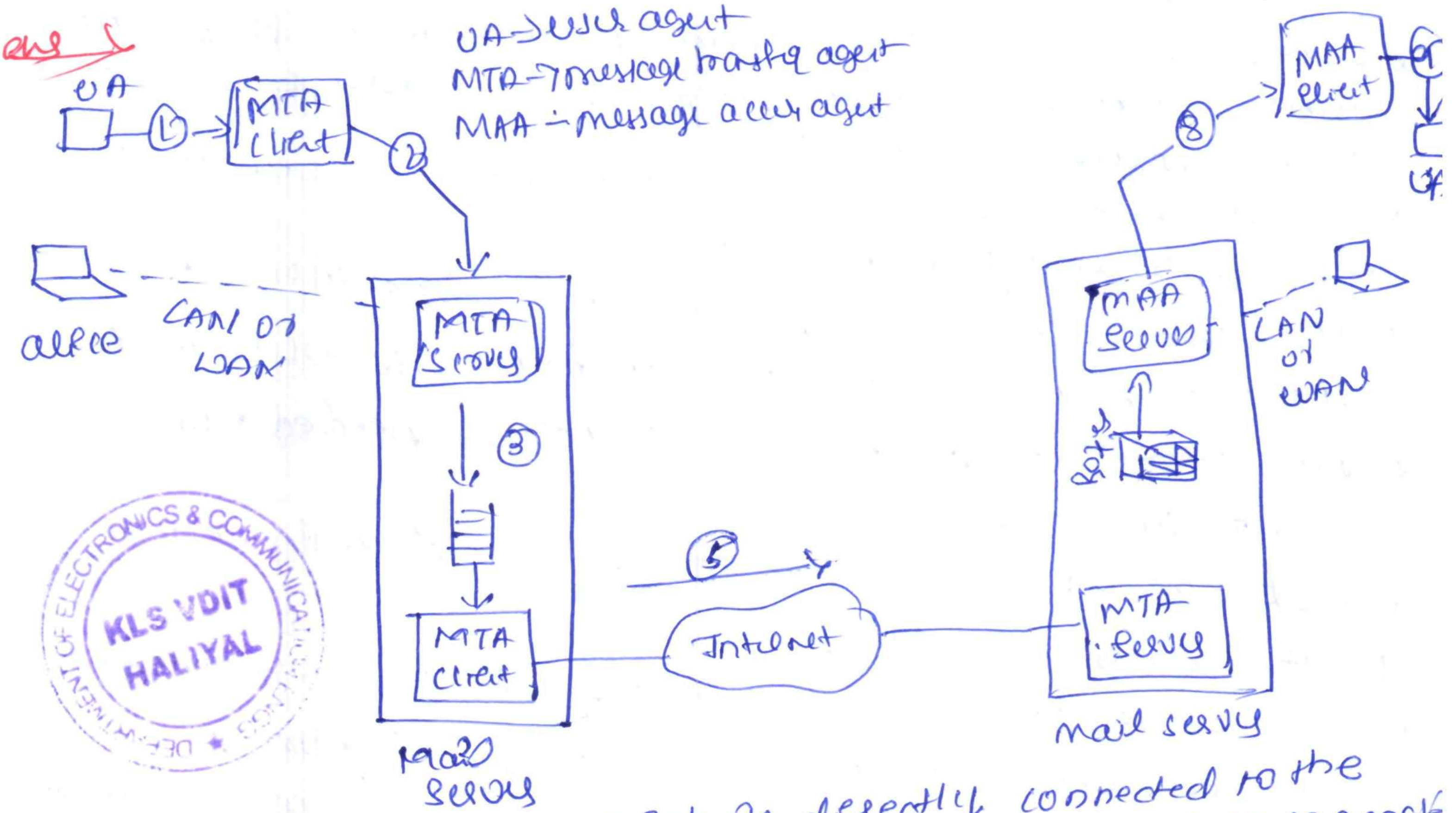
Resolution

- mapping a name to an address is called name-address resolution.
- DNS is designed as a client-server application.
- A host that needs to map an address to a name or name to an address calls a DNS client called resolver.
- The resolver access the closest DNS server with a mapping request.
- If the server has the information, it satisfies the resolve otherwise, it either refers the resolver to other servers or asks other servers to provide information.
- After the resolver receives ~~the~~ the mapping, it interprets the response to see if it is real resolution or an error, & finally delivers the result to the process the request

Or

10a) Explain the architecture of electronic- mail with neat diagram. (10M)

ans :-



* Case in which Alice or Bob is directly connected to the corresponding mail server, in which LAN or WAN connects is not required, but this variation in the scenario doesnt affect our discussion.

* In a common scenario, the sender and the receivers of the e-mail, Alice & Bob respectively, are connected via LAN WAN to two mail servers.

* The administration has created one mailbox has acce for each users where the received messages are stored.

* A mail box is part of server hard drive, a special file with permission restrictions.

* Only the owner of the mailbox has access to it.

* The administrator also created a queue to store message waiting to be sent.

* A simple email from Alice to Bob takes nine different steps.

- Alice or Bob uses three different agent: UA, message transfer agent (MTA), & MAA (message access agent.
- When Alice needs to send a message to Bob she runs a UA program to prepare the message & send it to her mail server.
- The mail server at her her site uses a queue to store message waiting to be sent.
- The message, however needs to be sent through the Internet from Alice's site to Bob's site using MTA
- Here two message transfer agents are needed: one client and one server.
- Bob cannot bypass the mail server and use the MTA server directly.
- To use MTA server directly, Bob would need to run the MTA server all the time because he does not know when message will arrive.

* Bob needs another pair of client-server program message access program. This is because an MTA client-server program is a push program: the client pushes the message to server.

- Bob needs pull program.
- The client needs to pull the message from the server.

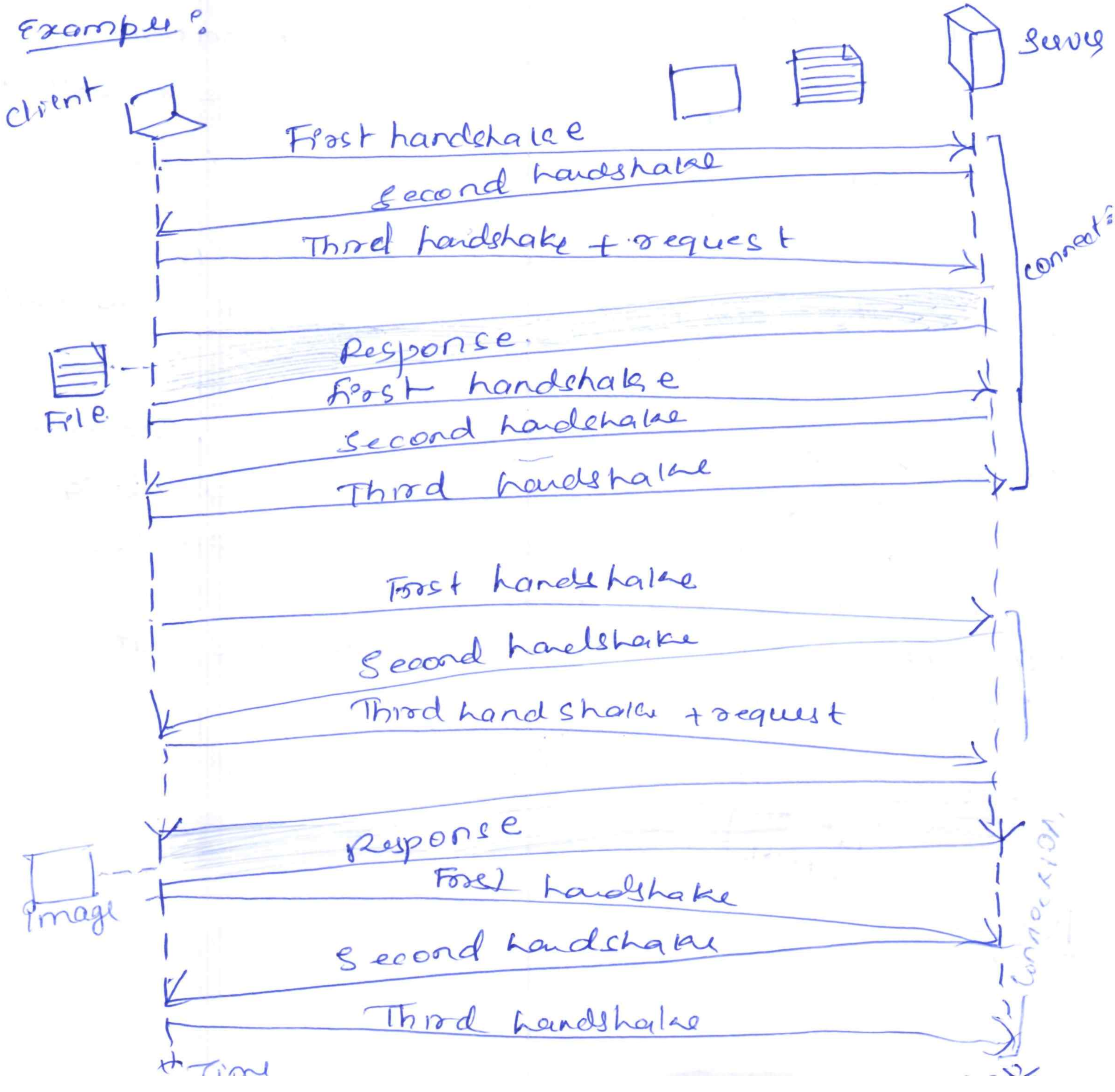
10b) Explain with an example, working of HTTP [Hyper Text Transfer protocol] (10M)

Ans> HTTP is used to define how the client server programs can be written to retrive web pages from web.

* An HTTP client sends a request ; an HTTP server- client request ; an HTTP server returns a responce.

* The server uses the port number, 80 ; the client uses a temporary port number.

Example:



* The client needs to access a file that contains one link to an image.

* The ~~imag~~ text file and image are located on the same server.

* Here we need two connections, TCP requests at least three handshake message to establish the connection, but the request can be sent with the third one.

* After the connection is established, the object can be transferred.

* after receiving an object, another three handshake messages are needed. to terminate the connection.

* This means that client and server are involved in two connection establishments & two connection terminations.

* If the transaction involves retrieving 10 or 20 objects, the round trip time spent for these hand-shake add up to big overhead.

* when we describe the client-server programming at the end of chapter, we will show that for each connection the client & server need to allocate extra resources such as buffers and variables.

* This is another burden on both sites, but especially on the server site.