CBCS SCHEME

USN | | | | | | | | | | 15EC64

Sixth Semester B.E. Degree Examination, Aug./Sept. 2020
Computer Communication Networks

Time: 3 hrs. Max. Marks: 80

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

Module-1

1 a. Outline the functions of various layers in TCP/IP with necessary diagram to show logical connection between layers. (08 Marks)

b. Explain the various services of datalink layer. (08 Marks)

OR

2 a. Explain stop and wait protocol. Also explain with necessary diagrams how sequence and acknowledge numbers prevent duplication of frames. (10 Marks)

b. Compare various physical topologies in a computer network. (06 Marks)

Module-2

3 a. List the controlled access methods. Also explain reservation access method. (06 Marks)

b. Summarize standard Ethernet implementations. (04 Marks)

c. A pure ALOHA network transmits 200 bit frames on a shared channel of 200 kbps. What is the throughput if the system produces :
i) 1000 frames per second
ii) 500 frames per second
iii) 250 frames per second. (06 Marks)

OR

4 a. Explain CSMA/CA protocol with a flow diagram. (08 Marks)

b. Explain Ethernet frame. (04 Marks)

c. A network using CSMA/CD has a bandwidth of 10Mbps. If the maximum propagation time is 25.6μs, what is the minimum size of the frame? (04 Marks)

Module-3

5 a. Compare two types of Bluetooth networks and also explain various layers of Bluetooth. (08 Marks)

b. Explain in brief DHCP. (04 Marks)

c. An organization is granted a block of addresses with the beginning address 14·24·74·0/24. The organization needs to have 3 subblocks of addresses to use in its three subnets : one subblock of 10 addresses, one subblock of 60 addresses and one subblock of 120 addresses. Design the subblock. (04 Marks)

OR

6 a. Explain in brief various categories of connecting devices. (06 Marks)

b. Explain the following :
i) QoS
ii) Congestion control. (04 Marks)

c. Explain with a neat diagram virtual circuit packet switched network. (06 Marks)

Submitted By
Dg. ALK.

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

Module-4

7 a. Explain with a neat diagram IP datagram format. (08 Marks)
b. Illustrate with an example, Linkstate routing. (08 Marks)

OR

8 a. What is distance vector routing? Explain the various drawbacks of distance vector routing and a few solutions to overcome the same. (08 Marks)
b. Explain with a diagram three phases of mobile IP. (08 Marks)

Module-5

9 a. Explain with a neat diagram, Goback-n protocol. (08 Marks)
b. Explain TCP segment format. (08 Marks)

OR

10 a. Explain various services of UDP. (05 Marks)
b. Compare connection oriented and connectionless services. (08 Marks)
c. Suppose a TCP connection is transferring a file of 5000 bytes. The first byte is numbered 10001. What are the sequence numbers for each segment if data are sent in five segments, each carrying 1000 bytes? (03 Marks)

* * * * *

1a. Outline the functions of various layers in TCP/IP with necessary diagram to show logical connection between layers — (8M)

Soln: Logical connections between layers of the TCP/IP protocol suite

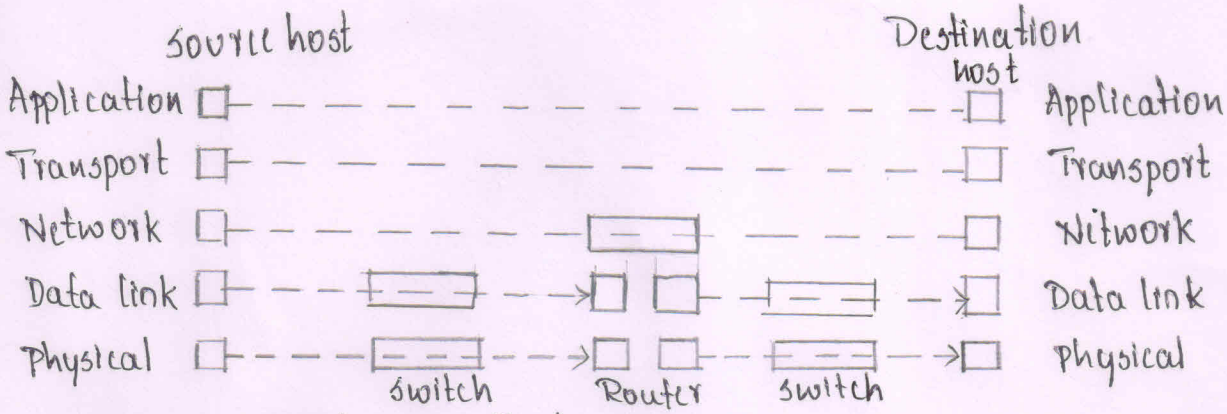


Fig 1(a)

— 1.5M

Explaination
1.5M x 5 = 7.5M

In the figure shown above, the duty of the application, transport and network layers is end to end. However, the duty of the data-link and physical layers is hop-to-hop, in which a hop is a host or router. In other words, the domain of duty of the top three layers is the internet, and the domain of duty of the two lower layers is the link.

Another way of thinking of the logical connections is to think about the data unit created from each other layer. In top three layers the data unit should not be changed by any router or link layer switch. In the bottom two layers, the packet created by the host is changed only by the routers, not by the link layer switches.

Description of each layer.

1. Physical Layer: Physical layer is responsible for carrying individual bits in a frame across the link. Although the physical layer is the lowest layer is still a logical communication because there is another hidden layer, the transmission media, under the physical layer. Two devices are connected by a transmission medium. Transmission medium does not carry bits, It carries electrical or optical signals. so the bits

received in a frame from data-link layer are transformed and sent through the transmission media. There are several protocols that transform a bit to a signal.

2. Data-link layer: Internet is made up of several (LANS and WANS) connected by routers. There may be several overlapping sets of links that a diagram can travel from host to the destination. The routers are responsible for choosing the best links. However, when the next link to travel is determined by the router, the data link layer is responsible for taking the datagram and moving it across the link. The link can be wired LAN with a link-layer switch, a wireless LAN, a wired WAN or a wireless WAN. There are different protocols used with any link type. In each case, the data link layer is responsible for moving the packet through the link. TCP/IP does not define any specific protocol for the data link layer. It supports all the standard and proprietary protocols. Any protocols that can take the diagram and encapsulates it in a packet called a frame. Each link layer protocol may provide a different service. Some link layer protocols provide complete error detection and correction, some provide only error correction.

3. Network layer: The network layer is responsible for creating a connection between the source computer and the destination computer the communication at the network layer is host-to-host. However since there can be several routers. from source to destination, the routers in the paths are responsible for choosing the best route for each packet Network layer is responsible for host to host communication and routing the packet through possible routes.

The network layer in the Internet includes the main protocol, Internet Protocol (IP) that defines the format of the packet called a datagram at the network layer. Ip also defines the format and structure of addresses used in this layer. Ip is also responsible for host-host routing a packet from its source to its destination, which is achieved by each router forwarding the datagram to the next router in its path.

IP is a connectionless protocol that provides no flow control, no error

error control, and no congestion control services. The network layer also includes unicast and multicast routing protocols. A routing protocols. does not take part in routing, but it creates forwarding tables for router to help them in the routing process. The network layer also (includes) has some auxiliary protocols that help IP in its delivery and routing tasks. The Internet Group Message protocol (ICMP) helps IP to report some problems when routing a packet. The Internet Group Management protocol (IGMP) is another protocol that helps IP in multitasking. The dynamic host configuration protocol (DHCP) helps IP to get the network layer address for a host. The Address Resolution Protocol (ARP) is a protocol that helps IP to find the link-layer address of a host or a router when its network-layer address is given.

4. Transport Layer: The logical connection at the transport layer is also end to end. The transport layer at the source host gets the message from the application layer, encapsulates it in a transport layer packet connection to the transport layer at the destination host.

There are a few transport-layer protocols in the Internet. each designed for some specific task. The main protocol, Transmission Control Protocol (TCP), is a connection-oriented protocol that first establishes a logical connection between transport layers at two hosts before transferring data. It creates a logical pipe between two TCPs for transferring a stream of bytes. TCP provides flow control, error control, and congestion control to reduce the loss of segments due to congestion in the network. The other common protocol, user datagram protocol (UDP) is a connectionless protocol that transmits user datagrams without being related to the previous or the next one. UDP is a simple protocol that does not provide flow, error or congestion control. Its simplicity, which means small overhead, is attractive to an application program that needs to send short messages and cannot afford the retransmission of the packets involved in TCP, when a packet is corrupted or lost. A new protocol, stream control Transmission Protocol (SCTP) is designed to respond to new applications that are emerging in the multimedia.

5. Application Layer: As shown in the figure, the logical connection between the two application layers is end to end. The two application layers exchange messages between each other as through there is a bridge between the two layers. However we should know that the communication is done through all the layers.

Communication at the application layer is between two process. To communicate, a process sends a request to the other process and receives a a application layer in the internet includes many predefined protocols, but a user can also create a pair of process to be run at the two hosts.

The hypertext transfer protocol (HTTP) is a vehicle for accessing the world wide web (www). The simple Mail Transfer Protocol (SMTP) is the main protocol used in electronic mail (e-Mail) service. The File Transfer Protocol (FTP) is used for transferring files from one host to another. The Terminal Network (TELNET) and secure shell (SSH) are used for accessing a site remotely. The simple Network Management Protocol (SNMP) is used by an administrator to manage the internet at global and local levels. The domain name system (DNS) is used by other protocols to find the network layer address of a computer. The internet group management protocol (IGMP) is used to collect membership in a group.

1b. Explain the various services of data link layer —— (8m)

soln: Various services of data link layer are —— 2m x 4 = 8m

1. Framing: It's the first servile provided by the data-link layer is framing The data-link layer at each node needs to encapsulate the datagram in a frame before sending it to the next node. The node also needs to decapsulate the datagram from the frame received on the logical channel. A frame may have both a header and a trailer. Different data-link layers have different formats for framing.

2. Flow Control: The sending data link layer at the end of a link is a producer of frames, the receiving data link layer at the other end of a link of a consumer. If the rate of produced frames is higher than the rate of consumed frames, frames at the receiving end need to be buffered while waiting to be consumed. And there is no unlimited buffer size at the receiving side. There are two choices. The first choice is to let the receiving data link layer drop the frames if its buffer is full. The second choice is to let the receiving data link send a feedback to the sending data link layer is to let the receiving data-link layer send a feedback to the sending data link layer) for flow control. Since flow control also occurs at the transport layer, with a higher degree of importance.

3. Error Control: At the sending node, a frame in data link layer needs to be changed to bits, transformed to electromagnetic signals and transmitted through the transmission media. At the receiving node, electromagnetic signals are received, transformed to bits and put together to create a frame. Since electromagnetic signals are susceptible to error, a frame is susceptible to error. The error needs first to be detected. After detection it needs to be either corrected at the receiver node or discarded and retransmitted by the sending node.

4. Congestion Control: Although a link may be congested with frames, which may result in frame loss, most data link layer protocols do not directly use a congestion control to alleviate congestion, although some wide-area networks do. In general, congestion control is considered an issue in the network layer or the transport layer because of its end to end nature.

2a. Explain stop and wait protocol. Also explain with necessary diagram how sequence and acknowledge numbers prevent duplication of frames. -(10m)

Soln

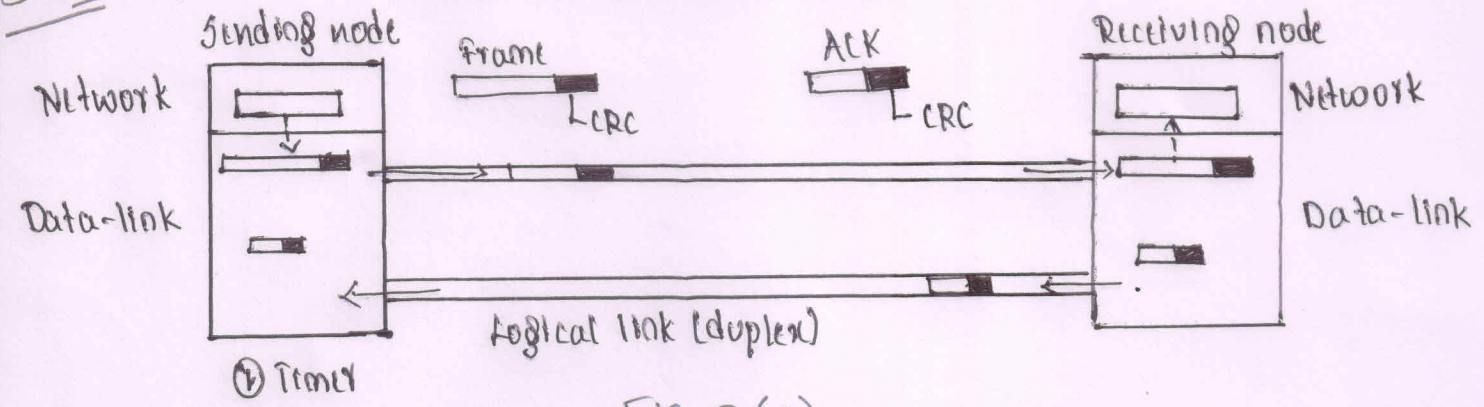


Fig. 2(a)

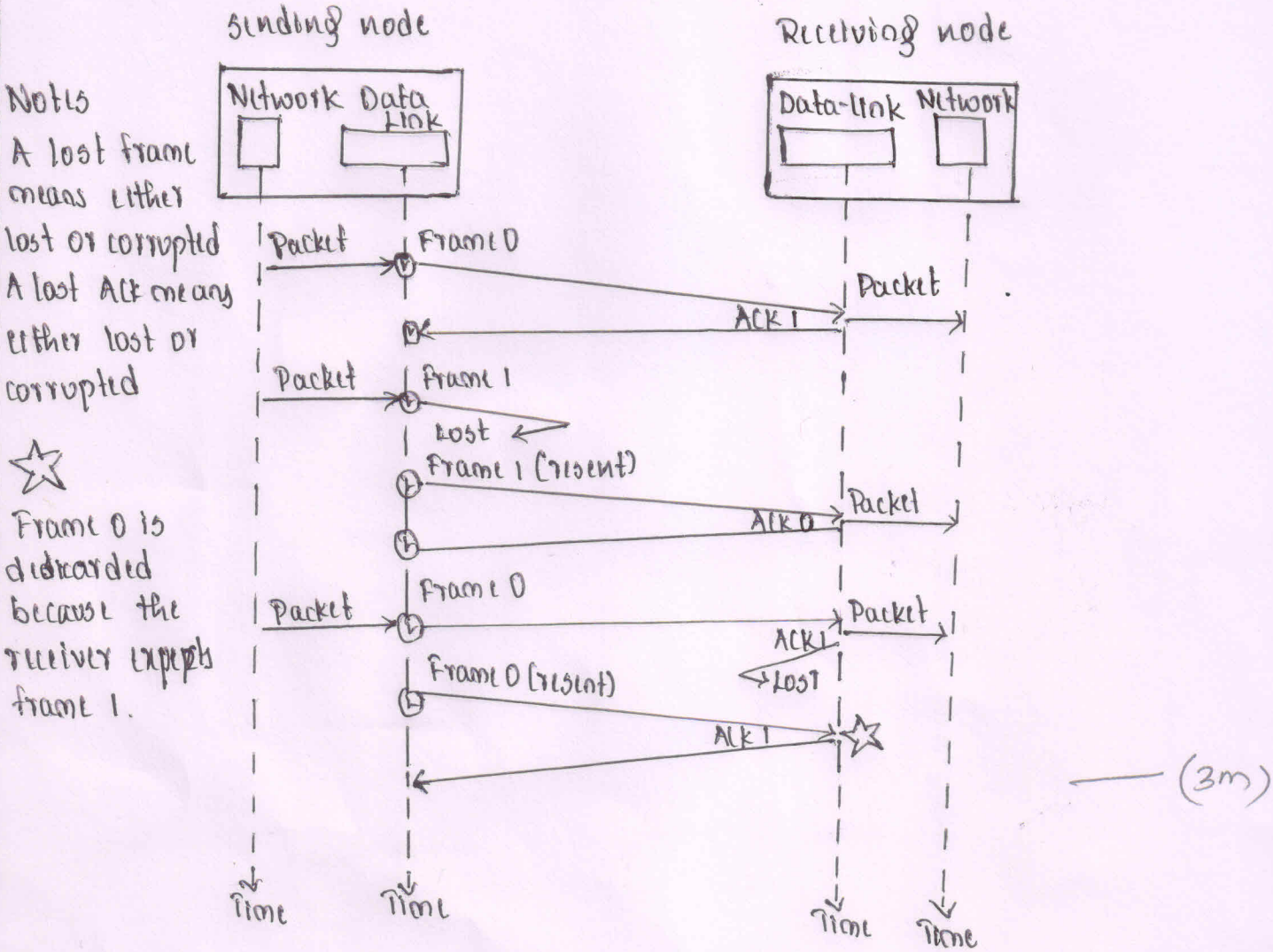
stop and wait protocol uses both flow and error control. In this protocol the sender sends one frame at a time and waits for an acknowledgement before sending the next one. To detect corrupted frames, we need to add a CRC to each data frame. When a frame arrives at the receiver site, it is checked. If its CRC is incorrect, the frame is corrupted and silently discarded. The silence of the receiver is a signal for the sender that a frame was either corrupted or lost. Every time the sender sends a frame, it starts a timer. If an acknowledgement arrives before the time expires, the timer is stopped and the the sender sends the next frame. If the timer expires, the sender resends the previous frame, assuming that the frame was either lost or corrupted. This means that the sender needs to keep a copy of the frame until its acknowledgment arrives. When the corresponding acknowledgement arrives, the sender discards the copy and sends the next frame if it is ready. In stop and wait protocol only one frame & one acknowledgement can be in the channels at any time.

Duplicate packets as much as corrupted packets need to be avoided. It's needed to add sequence numbers to the data frames and acknowledgement numbers to the ACK frames. However numbering in this case is very simple, sequence numbers are 0, 1, 0, 1, 0, 1....; the acknowledgement numbers can also be 1, 0, 1, 0, 1, 0... In other words, the sequence numbers start with 0, the acknowledgement numbers start with 1. An acknowledgement number always defines the sequence number of the next frame to receive.

The below figure shows how adding sequence numbers and acknowledgement numbers can prevent duplicates. The first frame is sent & acknowledgement. The

acknowledgment is lost. The frame is resent.

Sequence and acknowledge numbers prevent duplication of frames



Notes

A lost frame means either lost or corrupted

A lost Ack may either lost or corrupted

☆ Frame 0 is discarded because the receiver expects frame 1.

— (3m)

Legend

① starts the timer

② stop the timer

③ Restart a time-out timer

Fig. 2(a1)

Explanation — 5(m)

9.b. Compare various physical topologies in computer networks. —(6m)

Soln: The term physical topology refers to the way in which a network is laid out physically. Two or more devices connect to a link; 2 or more links form a topology. The topology of a network is the geometric representations of the relationship of all the links & linking devices to one another. There are 4 basic topologies: mesh, star, bus and ring

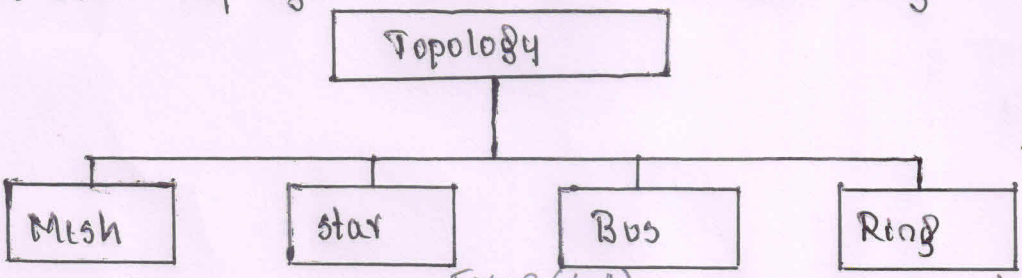


Fig. 2(b1)

1. Mesh Topology: In a mesh topology every device has a dedicated point to point link to every other device. The term dedicated means that the link carries traffic only between the 2 device it connects. To find the number of physical links in a fully connected mesh network with n nodes we first consider that each node must be connected to every other node. Node 1 must be connected to n-1 nodes, node 2 must be connected to n-1 nodes & finally node n must be connected to n-1 nodes we need n(n-1) physical links. However, if each physical link allows communication in both directions, we can divide the number of links by 2. In other words we can say that in a mesh topology we need. n(n-1)/2

n=5
10 links

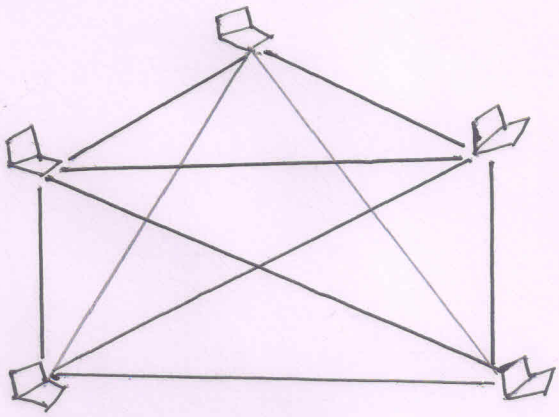


Fig. 2(b2)

A mesh offers several advantages over other network topologies.

1. The use of dedicated links guarantees that each connection carries it own data load, thus eliminating the traffic problems that occur when link must be shared by multiple devices.
2. A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.

3. There is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. physical boundaries prevent other users from gaining access to messages.

4. Point to point links make fault identification & fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault & aids the its finding its cause & solution.

The main disadvantages of each mesh are related to the amount of cabling & the number of I/O ports required.

1. Because every device must be connected to every other device, installation & reconnection are difficult.
2. The sheer bulk of the wiring can be greater than the available space can accomodate.
3. The hardware required to connect each link can be prohibitively expensive.

For these reason a mesh topology is usually implemented in a limited fashion for eg: as a backbone connecting the main computers of a hybrid network that can include several other topologies.

2. Star Topology : In a star topology, each topology has a dedicated point to point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.

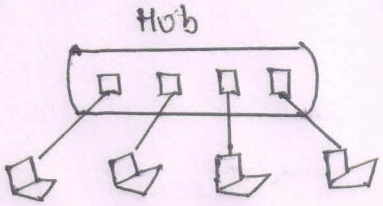


Fig (2b3)

Advantage: 1) star topology is less expensive than a mesh topology. In a star each device needs only one link & one I/O ports to connect it to any number of others. This factor also makes it easy to install & reconfigure. Far less cabling needs to be hosted, & additions, moves & deletions involve only one connection between that device & the hub.

2. Other advantage of include robostness. If one link fails, only that link is affected. All other link remains active. This factor also lends itself to easy fault isolation. As long as the hub is working, it can be used to monitor link problems & bypass defective links.

Disadvantages: i) One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.

ii). Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in star than in some other topologies.

3. Bus Topology: A bus topology is a multipoint connection. One long cable acts a balance to link all the devices in a network.

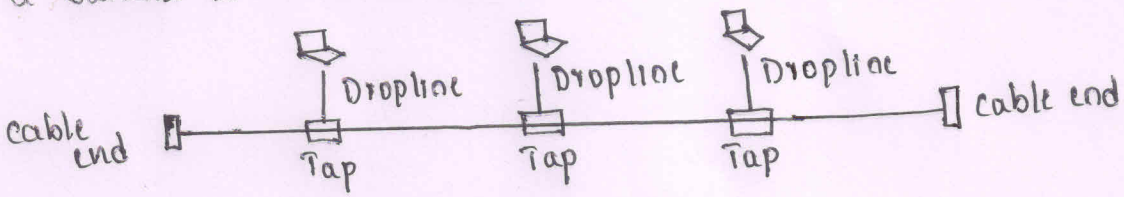


Fig. 2(b4)

Advantages: i) Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies.

2. In a bus, redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.

Disadvantages: i) It include difficult reconnection & fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices.

2. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number & spacing of devices connected to a given length of cable. Adding new devices may therefore require modification or replacement of the backbone.

A fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

4. Ring Topology: In a ring topology each device has a dedicated point-to-point connection with only 2 devices on either side of it. A signal is passed is along the ring in one direction, from device to device, until it reaches its

destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits & passes them along.

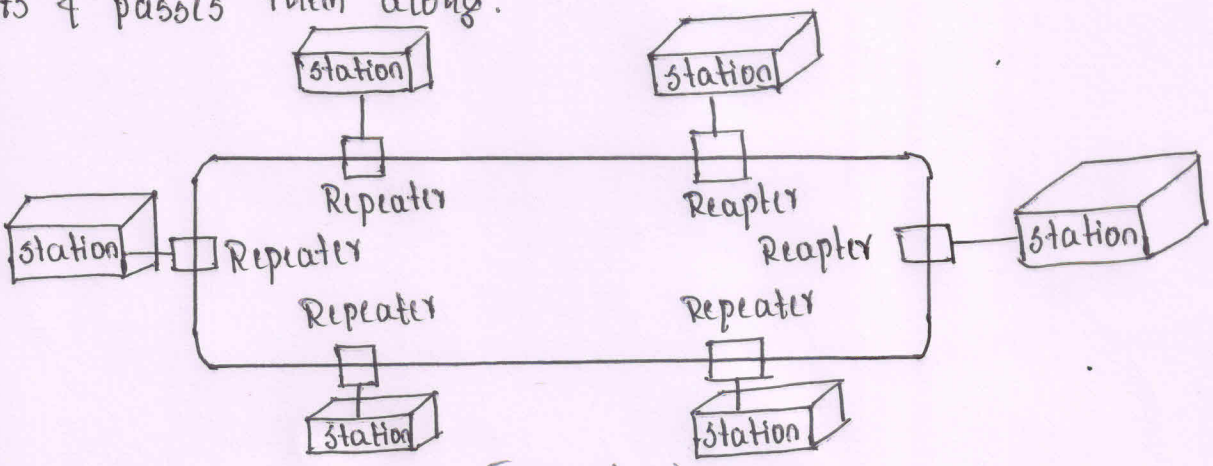


Fig 2(b5)

Advantages: 1. A ring is relatively easy to install & reconfigure. Each device is linked to only its immediate neighbors.

2. To add or delete a device requires changing only 2 connections. The only constraints are media & traffic considerations.

3. In addition, fault isolation is simplified. Generally in a ring a signal is circulating at all times. If one device does not receive a signal within a specified period. it can issue an alarm. the alarm alerts the network operator to the problem & its location.

Disadvantages: 1. Unidirectional traffic can be disadvantage. In a simple ring, a break in the ring can be disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

Explaination → 1.5 m x 4 = 6m

3a. List the controlled access methods. Also explain reservation access method (6m)

Soln: There are 3 controlled access methods: 1) Reservation, 2) Polling 3) Token Passing. —— (1m)

Reservation access method

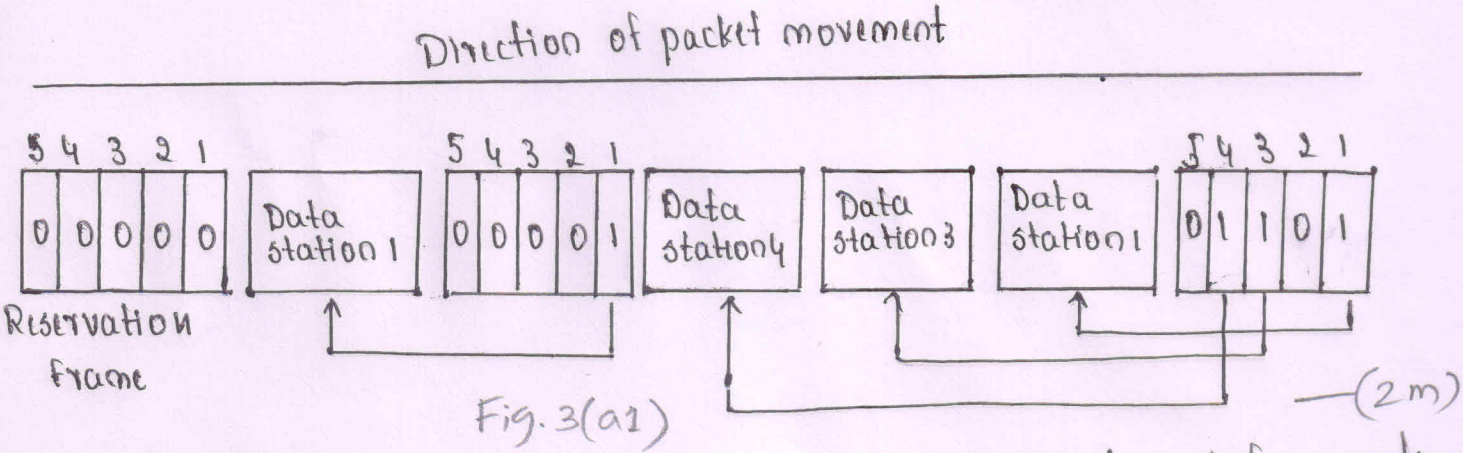


Fig. 3(a1) —— (2m)

In reservation method, a station needs to make a reservation before sending data. Time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval. If there are N-stations in the system, there are exactly N reservation mini-slots in the reservation frame. Each mini-slot belongs to a station. When a station needs to send a data frame, it makes a reservation in its own mini-slot. The stations that have made reservations can send their data frames after the reservation frame. Above figure shows a situation with five stations and a five-minislot reservation frame. In the first interval, only stations 1, 3 & 4 have made reservations. In the second interval, only station 1 has made a reservation.

—— (3m)

3.b. Summarize standard Ethernet implementations —— (4m)

Soln : The standard Ethernet defined several implementations, but only 4 of them became popular during the 1980s. Table below shows a summary of standard Ethernet implementations.

Summary of standard Ethernet implementation

Implementation	Medium	Medium Length	Encoding
10Base5	Thick coax	500m	Manchester
10Base2	Thin coax	185m	Manchester
10Base-T	2 UTP	100m	Manchester
10Base-F	2 fiber	2000m	Manchester

—(2m)

Table-3(b)

In the nomenclature 10BaseX, the number defines the data rate, the term Base means baseband signal, and x approximately defines either the maximum size of the cable in 100 meters or the type of cable, T for unshield twisted pair cable (UTP) and F for fiber-optic. The standard Ethernet uses a baseband signal, which means that the bits are changed to a digital signal & directly sent on the line.

—— (2m)

3c. A pure ALOHA network transmits 200 bit frames on a shared channel of 200-kbps. What is the throughput if the system produces (a) 1000 frames per second (b) 500 frames per second (c) 250 frames per second. —— (6m)

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

Soln : a) If the system creates 1000 frames per second, or 1 frame per millisecond, then $G=1$. In this case $S=G\times e^{-2G}=0.135$. This means that the throughput is $1000\times 0.135 = 135$ frames. Only 135 frames out of 1000 will probably survive.

b) If the system creates 500 frames per second, or 1/2 frames per millisecond, then $G=1/2$. In this case $S=G\times e^{-2G}=0.184$. This means that the throughout is $500\times 0.184=92$ and that only 92 frames out of 500 will probably survive. Note that this is the maximum throughput case, percentagewise.

c) If the system creates 250 frames per second, or 1/4 frames per millisecond, then $G=1/4$. In this case $S=G\times e^{-2G}=0.152$. This means that the throughput is $250\times 0.152=38$. Only 38 frames out of 250 will probably survive.

—— 2m x 3 = 6m

4a. Explain CSMA/CA protocol with a flow diagram. ——— (8m)

Soln: Carrier Sense multiple access with collision avoidance was invented for wireless network. Collisions are avoided through the use of CSMA/CA's three strategies: the interface space, the contention window, & acknowledgments, as shown in figure below. (Flow diagram)

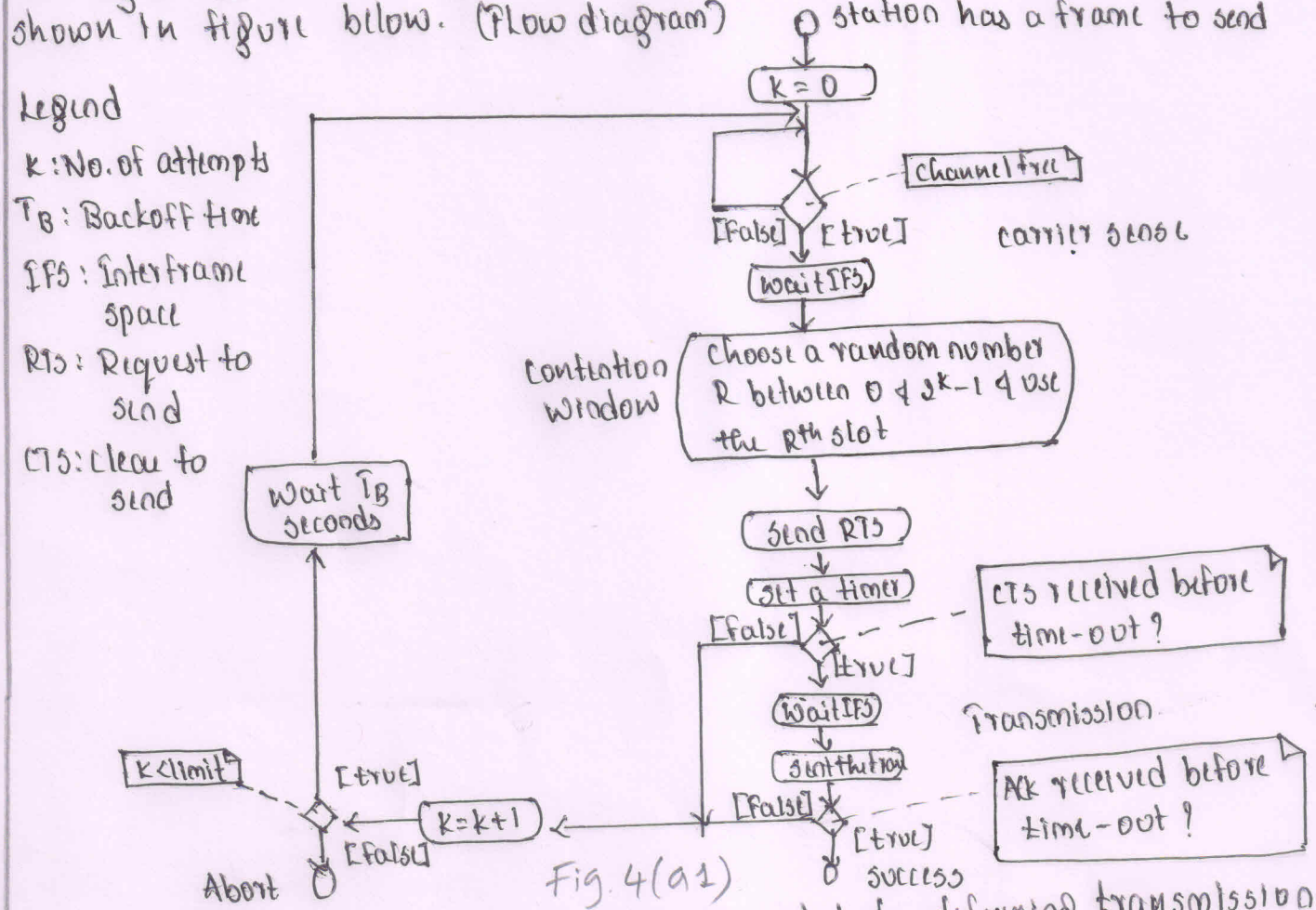


Fig. 4(a1)

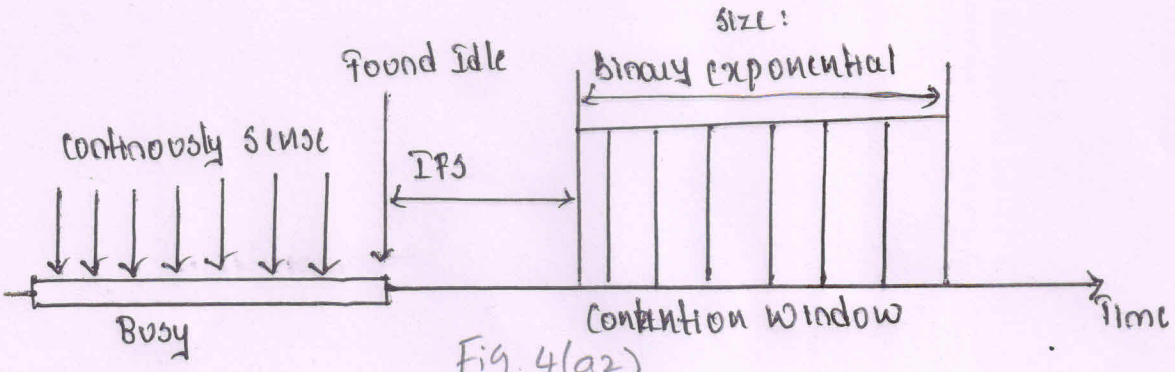
(3m)

(1m)

Interframe space: First 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 the interframe space or IFS. Even though the channel may appear idle when it is sensed, a distant station may have already started transmitting. The distant station's signal has not yet reached this station. The IFS time allows the front of the transmitted signal. If the channel is still idle, the station can send, but it still needs to wait a time equal to the contention window. The IFS variable can also be used to prioritize stations or frame types. Eg: a station that is assigned a shorter IFS has a higher priority.

Contention Window: It is an amount of time divided into slots. A station that is ready to send chooses a random number of slots as its wait time. The number of slots in the window changes according to the binary exponential backoff strategy. This means that it is set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time. This is very similar to the p-presistent method except that a random outcome defines the number of slots taken by the waiting station. One interesting point about the contention window is that station needs to sense the channel after each time slot. However, if the station finds the channel busy, it does not restart the process; it

just stops the timer & restarts it when the channel is sensed as idle. This gives priority to the station with the longest waiting time as shown in figure below.



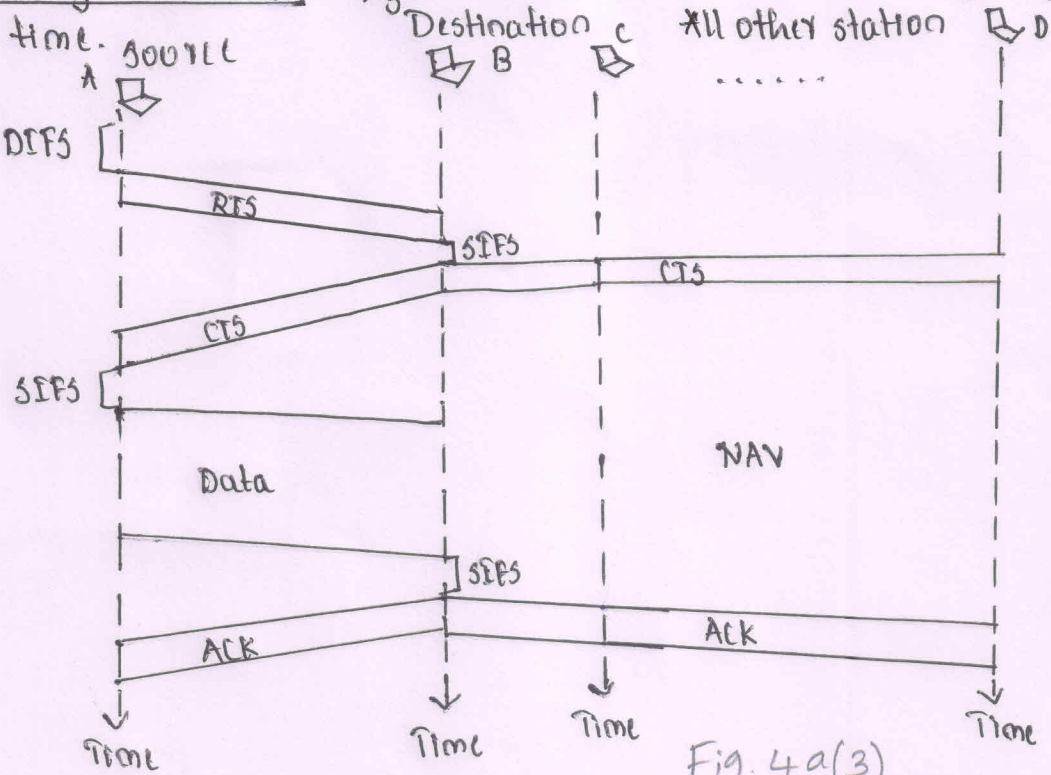
(1m)

Fig. 4(a2)

Acknowledgment: With all these precautions, there still may be a collision resulting in destroyed data. In addition the data may be corrupted during the transmission. The positive acknowledgment & the time-out timer can help guarantee that the receiver has received the frame.

(1m)

Frame Exchange Time Line: Figure below shows the exchange of data & control frames in time.



(1m)

Fig. 4a(3)

1. Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.
   a. The channel uses a persistance strategy with backoff until the channel is idle.
   b. After the destation is found to be idle, the station waits for a period of time called the DCF interframe space; then the station sends a control frame called the request to send (RTS)
2. After receiving the RTS & waiting a period of time called the short interframe space (SIFS). the destination station sends a control frame, called the clear to send (CTS) to the source station. This control frame indicates that the

the distination station is ready to receive data.

3. The source station sends data after waiting an amount of time equal to SIFS.

4. The distination station, after waiting an amount of time equal to SIFS, sends an acknowledgment. to show that the frame has been received. Acknowledgment is needed in this protocol because the station does not have any means to check for the successful arrival of its data at the distination. on the other hand, the lack of collision in CSMA/CD is a kind of indication to the source that data have arrived.

4b. Explain Ethernet frame. ——————— (4m)

soln : The Ethernet frame contains 7 fields, as shown in figure below.

Ethernet Frame

Preamble: 56 bits of alternating 1s & 0s
SFD: Start frame delimiter, flag (10101011)

Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes

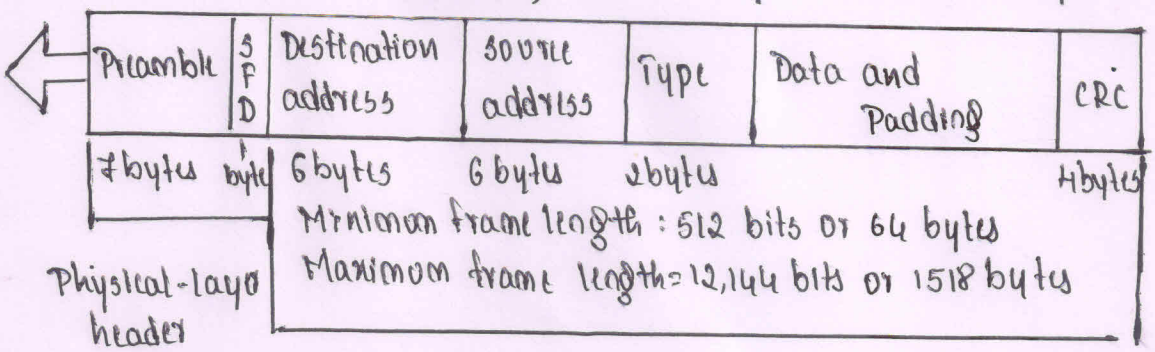


Fig. 4(b)

——— (2m)

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

Start frame delimiter (SFD): This field signals the beginning of the frame. The SFD warns the station or stations that this is the last chance for synchronization. The last 2 bits are (11)2 and alert the receiver that the next field is the destination address. This field is actually a flag that defines the beginning of the frame. We need to remember that an Ethernet frame is a variable-length frame. It needs a flag to define the beginning of the frame. The SFD field is also added at the physical layer.

Destination Address (DA). : This field is six bytes & contains the link layer address of the destination station or stations to receive the packet. We will discuss addressing shortly. When the receiver sees its own link-layer address, or a multicast address for a group that the receiver is a member of, or a broadcast address, it decapsulates the data from the frame & passes the data to the upper layer protocol defined by the value of type field.

Data : this field carries data encapsulated from the upper layer protocols. It is a maximum of 46 & a maximum of 1500 bytes. We discuss the reason for these minimum & maximum values shortly. If the data coming from the upper layer is more than 1500 bytes, it should be fragmented & encapsulated in more

than one frame. If it is less than 46 bytes, it needs to be padded with extra 0s. A padded data frame is delivered to the upper-layer protocol as it is which means that is responsibility of the upper layer to remove or, in the case of the sender, to add the padding. The upper layer protocol needs to know the length of its data. eg, a datagram has a field that defines the length of the data.

Type : This field defines the upper-layer protocol whose packet is encapsulated in the frame. this protocol can be IP, ARP, OSPF, & so on. In other words, it serves the same purpose as the protocol field in a datagram & the port-number in a segment or user datagram. It is used for multiplexing & demultiplexing.

Source Address (SA) : This field is also six bytes & contains the link-layer address of the packet. We will discuss addressing shortly.

CRC : The last field contains error detection information in this case a CRC-32. The CRC is calculated over the addresses, types & data field. If the receiver calculates the CRC & finds that it is not zero, it discards the frame.

——(2m)

4.c. A network using CSMA/CD has a bandwidth of 10Mbps. If the maximum propogation time is 25.6 μs what is the minimum size of the frame?

(4m)

Soln: The minimum frame transmission time is $T_{fr} = 2 \times T_p = 51.2\ \mu s$

This means, in the worst case, a station needs to transmit for a period of 51.2 μs to detect the collision.

The minimum size of the frame is 10Mbps x 51.2 μs = 512 bits or 64 bytes

This is actually the minimum size of the frame for standard Ethernet.

(4m)

5a. Compare 2 types of Bluetooth networks and also explain various layers of Bluetooth. ——— (8m)

Soln: Bluetooth defines 2 types of networks: piconet and scatternet.

Piconets

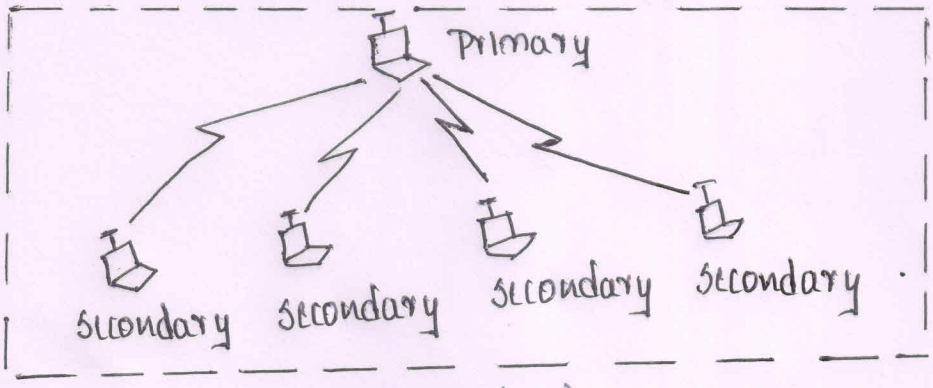


Fig. 5(a1)

A Bluetooth network is called a piconet, or a small net. A piconet can have up to eight stations, one of which is called the primary; the rest are called secondaries. All the secondary stations synchronize their clocks and hopping sequence with the primary. Note that a piconet can have only one primary station. The communication between the primary & secondary stations can be one to one or one-to many. Although a piconet can have a maximum of seven secondaries, additional secondaries can be in the parked state. A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state to the active state. Because only eight stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state. ——— (4m)

Scatternet

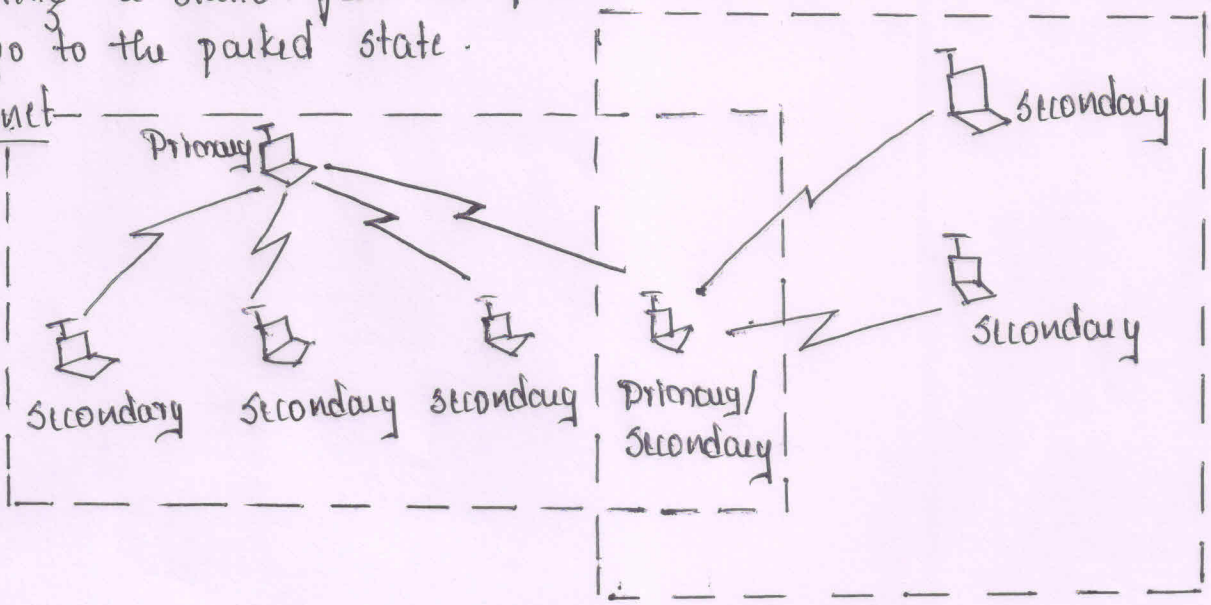


Fig. 5(a2)

Piconets can be combined to form what is called a scatternet. A secondary station in one piconet can be primary in another piconet This station can receive messages from the primary in the first piconet and acting as a primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets.

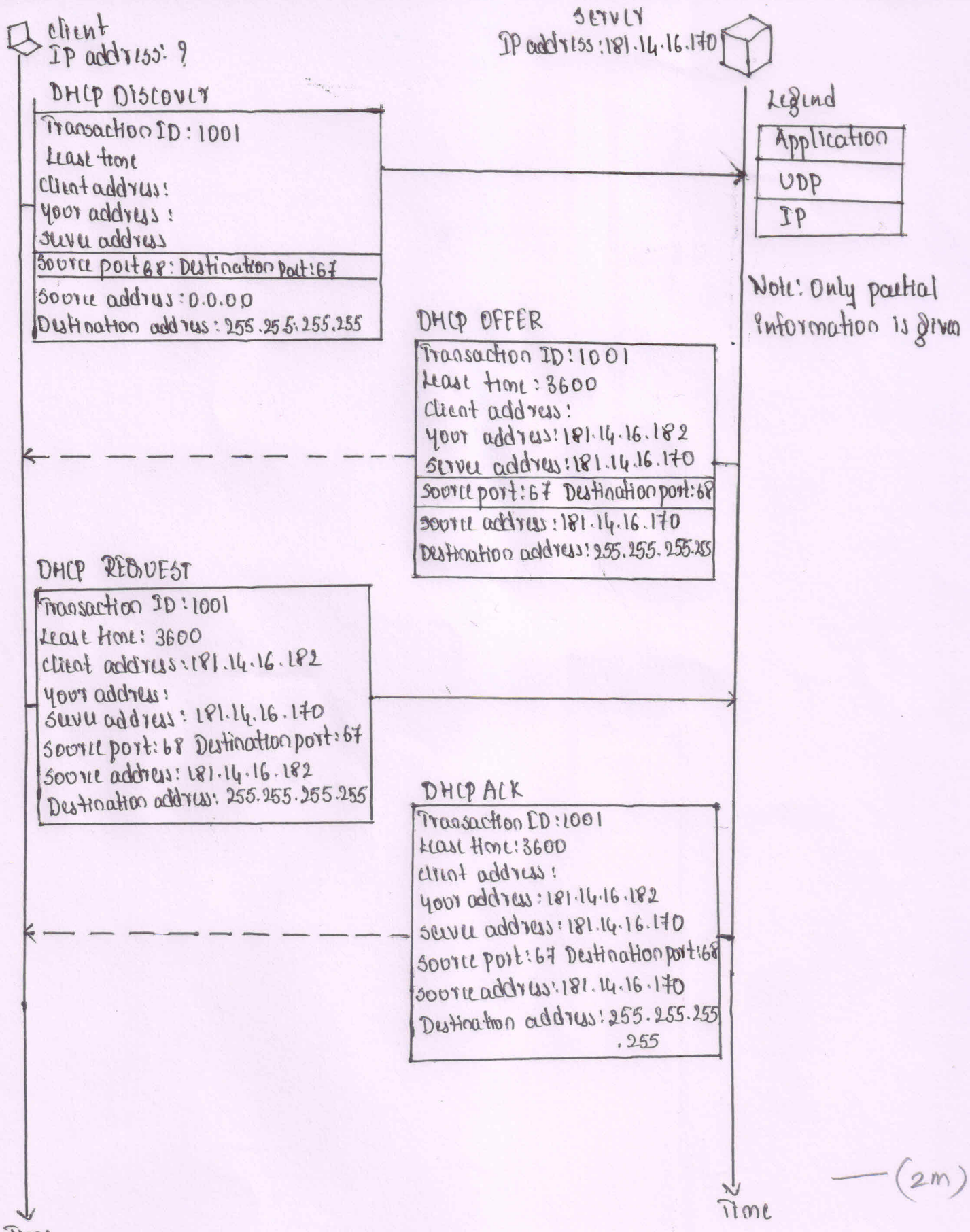
——— (4m)

5.b. Explain in brief DHCP ——— (4m)

Soln: We have seen that a large organization or an ISP can receive a block of address directly from Internet corporation for assigned names & Numbers (ICANN) & a small organisation can receive a block of address from an ISP After a block of address are assigned to an organization, the network administration can manually assign address to the individual hosts or routers. However, address assignment can manually assign automatically using the Dynamic Host configuration Protocol (DHCP). DHCP is an application layer program, using the client-server paradigm, that actually helps TCP/IP at the network layer.

DHCP has found such widespread use in the Internet that it is often called a plug and play protocol. It can be used in many situations. A network manager can configure DHCP to assign permanent IP address to the host and routers. DHCP can also be configured to provide temporary, on demand IP address to hosts. The second capability can provide a tempory IP address to a traveller to connect her laptop to the Internet while she is staying in the hotel. It also allows an ISP with 1000 granted address to provide services to 4000 households, assuming not more than one-fourth of customers use the internet at the same time. In addition to its IP address, a computer also needs to know the network prefix. Most computers also need two other pieces of information such as the address of a default router to be able to communicate with other networks & the address of a name server to be able to use names instead of address In other words, 4 pieces of information are normally needed. the computer address, the prefix the address of a router & the IP address of a name server. DHCP can be used to provide these pieces of information to the host.

——— (2m)


client
IP address: ?
server
IP address: 181.14.16.170
DHCP DISCOVER
Transaction ID: 1001
Least time
Client address:
Your address:
Server address
Source port 68: Destination Port: 67
Source address: 0.0.0.0
Destination address: 255.255.255.255
Legend
Application
UDP
IP
Note: Only partial information is given
DHCP OFFER
Transaction ID: 1001
Least time: 3600
Client address:
Your address: 181.14.16.182
Server address: 181.14.16.170
Source port: 67 Destination port: 68
Source address: 181.14.16.170
Destination address: 255.255.255.255
DHCP REQUEST
Transaction ID: 1001
Least time: 3600
Client address: 181.14.16.182
Your address:
Server address: 181.14.16.170
Source port: 68 Destination port: 67
Source address: 181.14.16.182
Destination address: 255.255.255.255
DHCP ACK
Transaction ID: 1001
Least time: 3600
Client address:
Your address: 181.14.16.182
Server address: 181.14.16.170
Source port: 67 Destination port: 68
Source address: 181.14.16.170
Destination address: 255.255.255.255
Time
Time

(2m)

Fig 5(b)

5.c. An organization is granted a block of address with the beginning address 14.24.74.0/24. The organization needs to have 3 subblocks of address to use in its 3 subnets: one subblock of 10 address, one sub block, one subblock of 60 address, & one subblock of 120 addresses. Design the subblocks. ——— (4m)

Soln: There are $2^{32-24} = 256$ addresses in this block.
The first address is 14.24.74.0/24; and the last address is 14.24.74.255/24.
To satisfy the third requirement, we assign address to subblocks, starting with the largest and ending with the smallest one.

a. The number of addresses in the largest subblock, which requires 120 addresses, is not a power of 2. We allocate 128 addresses. The subnet mask for this subnet can be found as

$$n_1 = 32 - \log_2 128 = 25.$$

The first address in this block is 14.24.74.0/25; & the last address is 14.24.74.127/25.

b. The number of addresses in the second subblock, which requires 60 addresses, is not a power of 2 either. We allocate 64 addresses. The subnet mask for this subnet can be found as $n_2 = 32 - \log_2 64 = 26$
The first address in this block is 14.24.74.128/26; The last address is 14.24.74.191/26.

c. The number of addresses in the smallest subblocks, which requires 10 addresses, is not a power of 2 either. We allocate 16 addresses. The subnet mask for this subnet can be found as $n_3 = 32 - \log_2 16 = 28$.
The first address in this block is 14.24.74.192/28; the last address is 14.24.74.207/28.

If we add all the addresses in the previous subblocks, the result is 208 addresses, which means 48 addresses are left in reserve. The first address in this range is 14.24.74.208. The last address is 14.24.74.255.

——— (4m)

6a. Explain in brief various categories of connecting devices. — (6m)

Soln: Hosts & networks do not normally operate in isolation. Connecting devices will be used to connect hosts together to make a network or to connect networks together to make an internet. Connecting devices can operate in different layers of the Internet model.

There are 3 kinds of connecting device: hubs, link-layer switches, and routers. Hubs, today operate in the first layer of the Internet model. Link-layer switches operate in the first two layers. Routers operate in the first 3 layers.

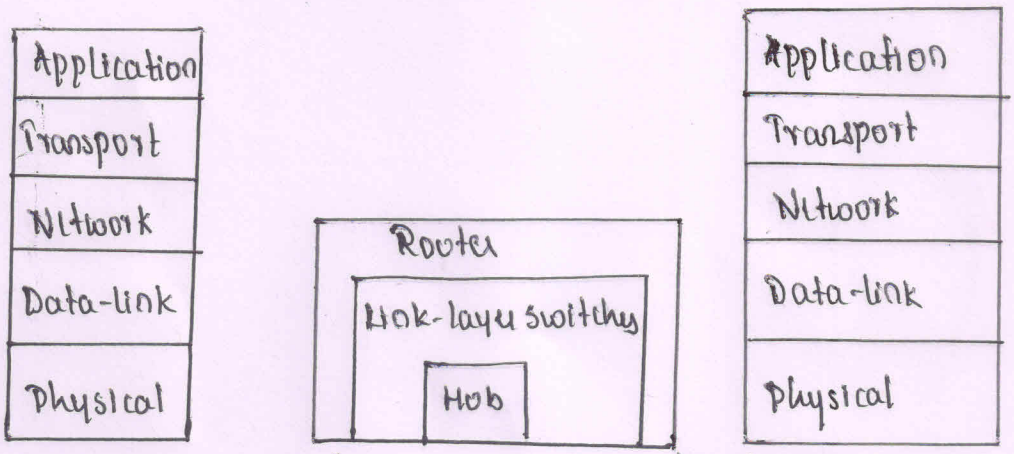
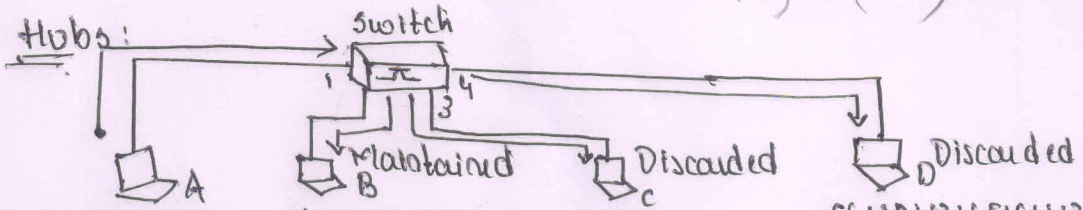


Fig. 6(a1)

1. Hubs:



— (3m)

Fig 6(a2)

Link layer switch

Switching table

Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	2
64:2B:13:65:64:12	3
64:2B:13:45:61:13	4

A hub is a device that operates only in the physical layer. Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of data. A repeater receives a signal & before it becomes too weak or corrupted, regenerates & retimes the original bit pattern. The repeater then sends the refreshed signal. In the past, when Ethernet LANs were using bus topology, a repeater was used the connect two segments of a LAN to overcome the length restriction of the coaxial cable. Today, however Ethernet LANs use star topology. In a star topology a repeater is a multiport device, often called a hub, which can be used to serve as the connecting point & at the same time function as a repeater.

2. Link-layer switches : —— (2m)

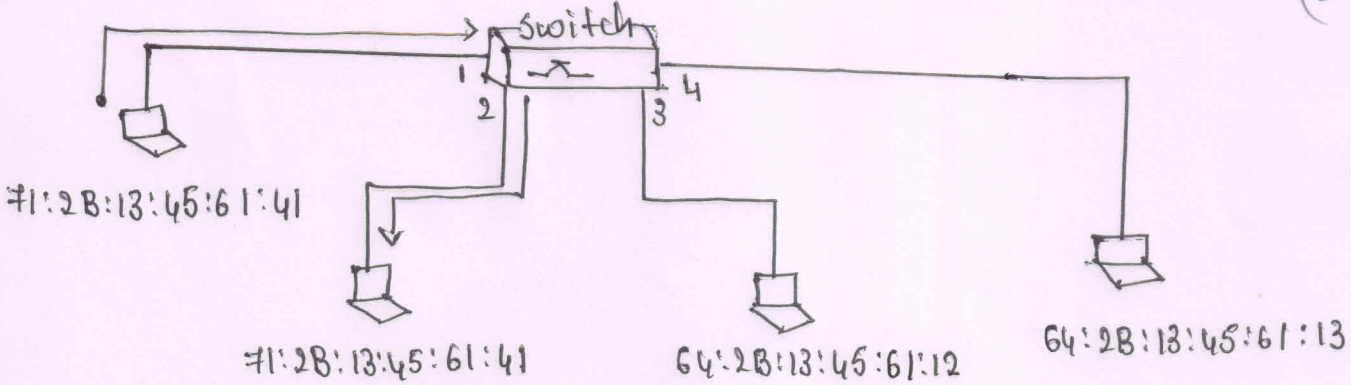


Fig. 6(a3)

A link-layer switch operates in both the physical & the data-link layers. As a physical layer device. it regenerates the signal it receives. As a link-layer switch can check the MAC addresses contained in the frame.

3. Routers : A router is a 3 layer device, it operates in the physical, data link & network layers. As a physical layer device. It regenerates the signal it receives. As a link layer device. the router checks the physical addresses contained in the packet As a network layer device, a router checks the network layer addresses. A router can connect networks. In other words, a router is an internet working device ; it connects independent networks to form an internetwork. According to this definition, 2 networks connected by a router become an internetwork or an internet.

—(2m)

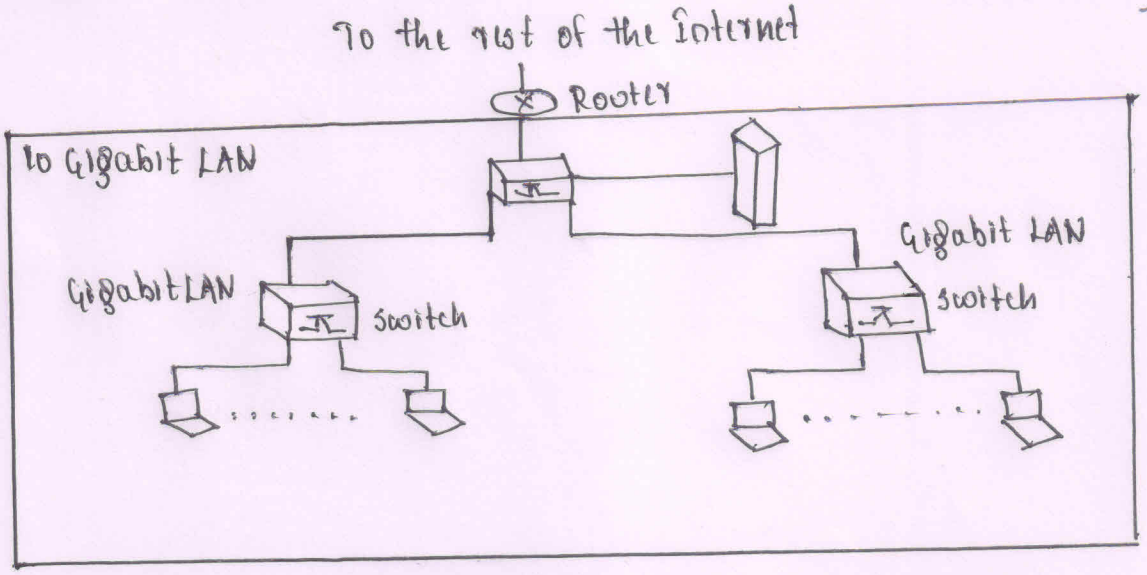


Fig. 6(a4)

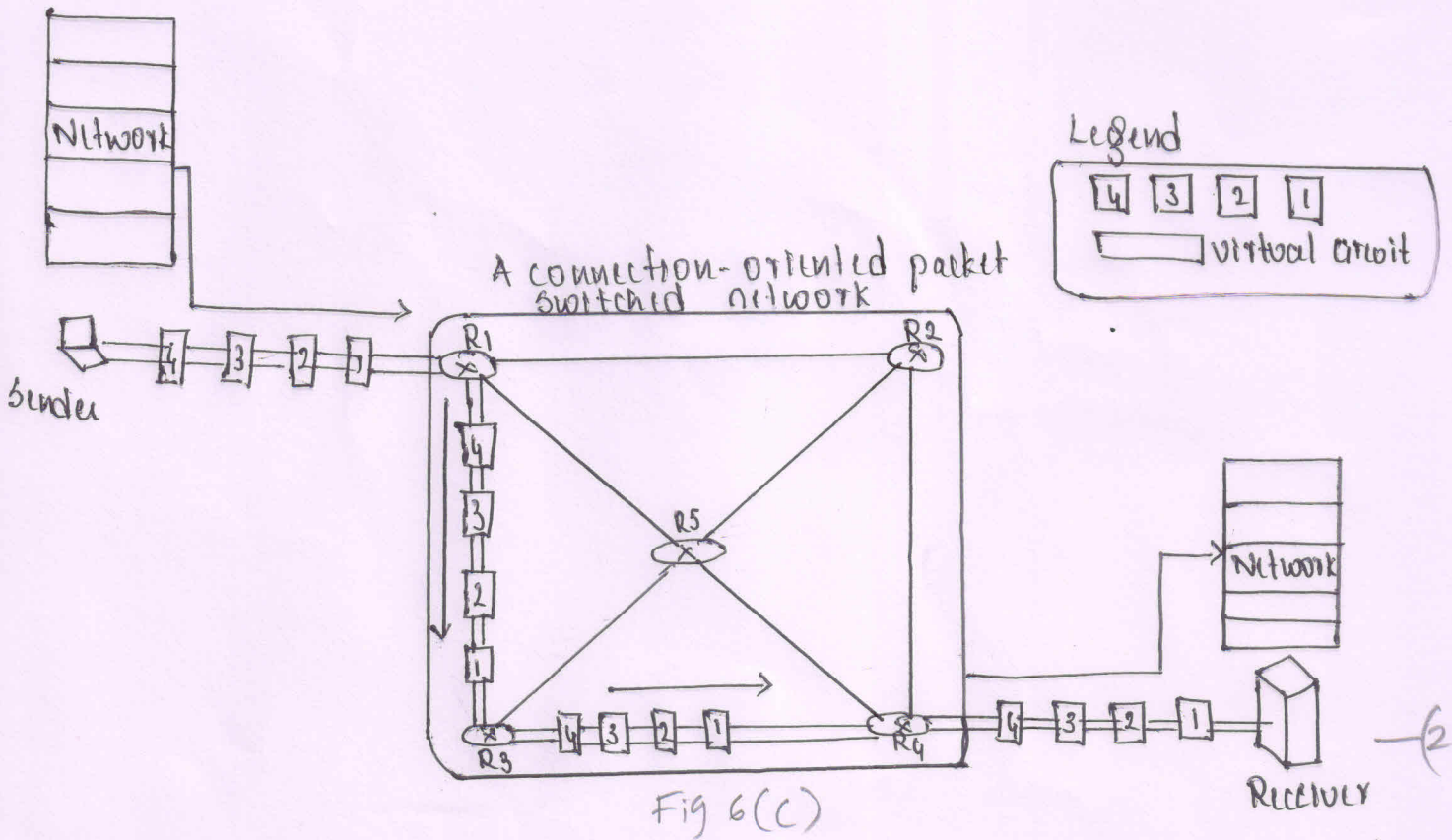
6.b. Explain the following ——— (4m)

(i) Quality of service (QoS): As the internet has allowed new applications such as multimedia communication has time communication of audio and video, the quality of service of the communication has become more and more important. The internet has thrived by providing better quality of services to support. these application however to keep the network layer untouched, these provisions are mostly implemented in the upper layer ——— (2m)

(ii) Congestion control: Congestion control is another issue in a network layer protocol. Congestion in the network layer is a situation in which too many datagrams are present in an area of internet. Congestion may occur if the number of datagrams sent by source computers is beyond the capacity of the network or routers. In this situation, some routers may drop some of the datagrams. However as more datagrams are dropped, the situation may become worse because, due to the error control mechanism at the upper layers, the sender may send duplicates of the lost packets. If the congestion continues, sometimes a situation may reach a point where the system collapses & no datagram are delivered We discuss congestion control at the network layer later in the chapter although it is not implemented in the internet. ——— (2m)

6c. Explain with a neat diagram virtual circuit packet switched network.

Soln: Virtual-Circuit Packet switched network. —(6m)



—(2m)

Fig 6(c)

In a virtual circuit approach there is a relationship between all packets belonging to a message. Before all datagrams in a message can be sent, a virtual connection should be set up to define the path for the datagrams. After connection setup, the datagrams can all follow the same path. In this type of service, not only the packet contains the source & destination addresses, it must also contain a flow label, a virtual circuit identifier that defines the virtual path the packet should follow. Although it looks as though the use of the label may make the source & destination addresses unnecessary during the data transfer phase, parts of the internet at the network layer still keep these addresses. One reason is that part of the packet path may still be using the connectionless service. Another reason is that part of packet path may still be using the connectionless service. Another reason is that the protocol at the network layer is designed with these addresses, & it may take a while before they can be changed.

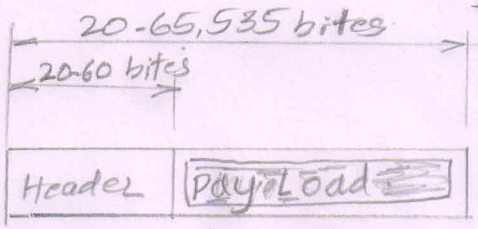
Each packet is forwarded based on the label in the packet. To follow the idea of connection-oriented design to be used in the Internet, we assume that the packet has a label when it reaches the router. In the figure shown above, the forwarding decision is based on the value of the label when it reaches the router. In the figure shown above, the forwarding

decision is based on the value of the label or virtual circuit identifier as it is sometimes called. To create a connection-oriented service, a 3-phase process is used : setup, data transfer and teardown. In the setup phase, the source & destination addresses of the sender & receiver are used to make table entries for the connection oriented service. In the teardown phase the source & dustination inform the router to delete the corresponding entries. Data transfer occurs between these two phases.

——— (4m)

7a. Explain with a neat diagram IP datagram format — (8m)

Soln IP datagram format: A datagram is a variable-length packet consisting of 2 parts: header and payload. The header is 20 to 60 bytes in length and contains information essential to routing & delivery. It is customary in TCP/IP to show the header in 4-byte sections.

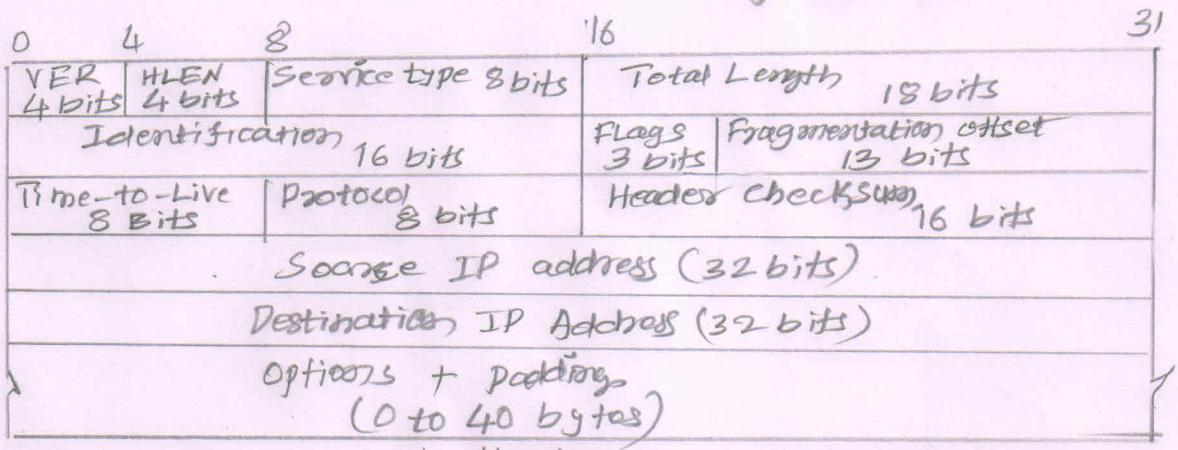


a. IP datagram.

Legend
VER: Version number
HLEN: Header Length
bite: 8 bites — (2m)

Fig. 7(a1)

Flags D M



b. Header — (2m)

Fig. 7(a2)

Brief description of each field:

Version Number: The 4-bit version number (VER) field define the version of the IPv4 protocol which obviously has the value of 4.

Header Length: The 4-bit header length that defines the total length of the datagram header in 4-byte words. The IPv4 datagram has a variable length header. When a device receives a datagram, it needs to know when the header stops & the data, which is encapsulated in the packet, starts. However, to make the value of the header length fit in a 4-bit header length the total length of the header is calculated as 4-byte words. The total length is divided by 4 & the value is inserted in the field. The receiver needs to multiply the value of this field by 4 to find the total length.

Service Type: In the original design of the IP header, this field was referred to as type of service (TOS), which defined how the datagram should be handled. In 1990s, IETF redefined the field to provide different services. When we discuss differentiated services

in field to provide better situation to define the bits in this field. The use of 4-byte words for the length header is also logical because the IP header always needs to be aligned in 4-byte boundaries.

Total length : This 16-bit field defines the total length of the IP datagram in bytes. A 16 bit number can define a total length up to 65,535. However the size of the datagram is normally much less than this. This field helps the receiving device to know when the packet is completely arrived. To find the length of the data coming from the upper layer, subtract the header length from the total length. The header length can be found by multiplying the value in the HLEN field by 4

Length of data = total length - (HLEN)×4

Protocol : In TCP/IP, the data section of a packet, called the payload, carries the whole packet from another protocol. A datagram, eg. can carry a packet belonging to any transport-layer protocol such as UDP or TCP. A datagram can also carry a packet from other protocols that directly use the service of the IP, such as some routing protocols. The internet authority has given any protocol that uses the services of IP a unique 8 bit number which is inserted in the protocol field. When the payload is encapsulated in a datagram at the source IP, the corresponding protocol number is inserted in this field; when the datagram arrives at the destination, the value of this field helps to define to which protocol the payload should be delivered. In other words, this field provides multiplexing at the source & demultiplexing at the destination.

(4m)

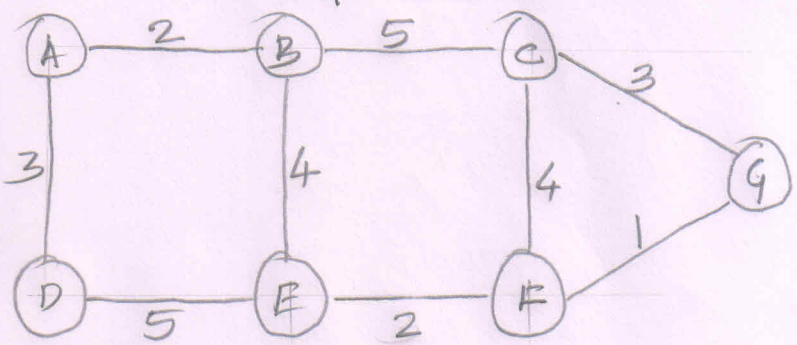
7.b. Illustrate with example, link state routing. —— (8m)

Soln: Link-State Routing: It uses the term link state to define the characteristic of a link that represents a network in the internet. In this algorithm the cost associated with an edge defines the state of the link. Links with lower costs are preferred to links with higher costs; if the cost of a link is infinity, it means that the link does not exist or has been broken.

Link-State Database (LSDB): 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 the LSDB. There is only one LSDB for the whole internet, each node needs to have a duplicate of it be able to create the least-cost tree.

Let us consider an example of an LSDB for the graph in figure shown below the LSDB can be represented as a 2D array in which the value of each cell defines the cost of the corresponding link.

Example of a link-state database



a. The weighted graph

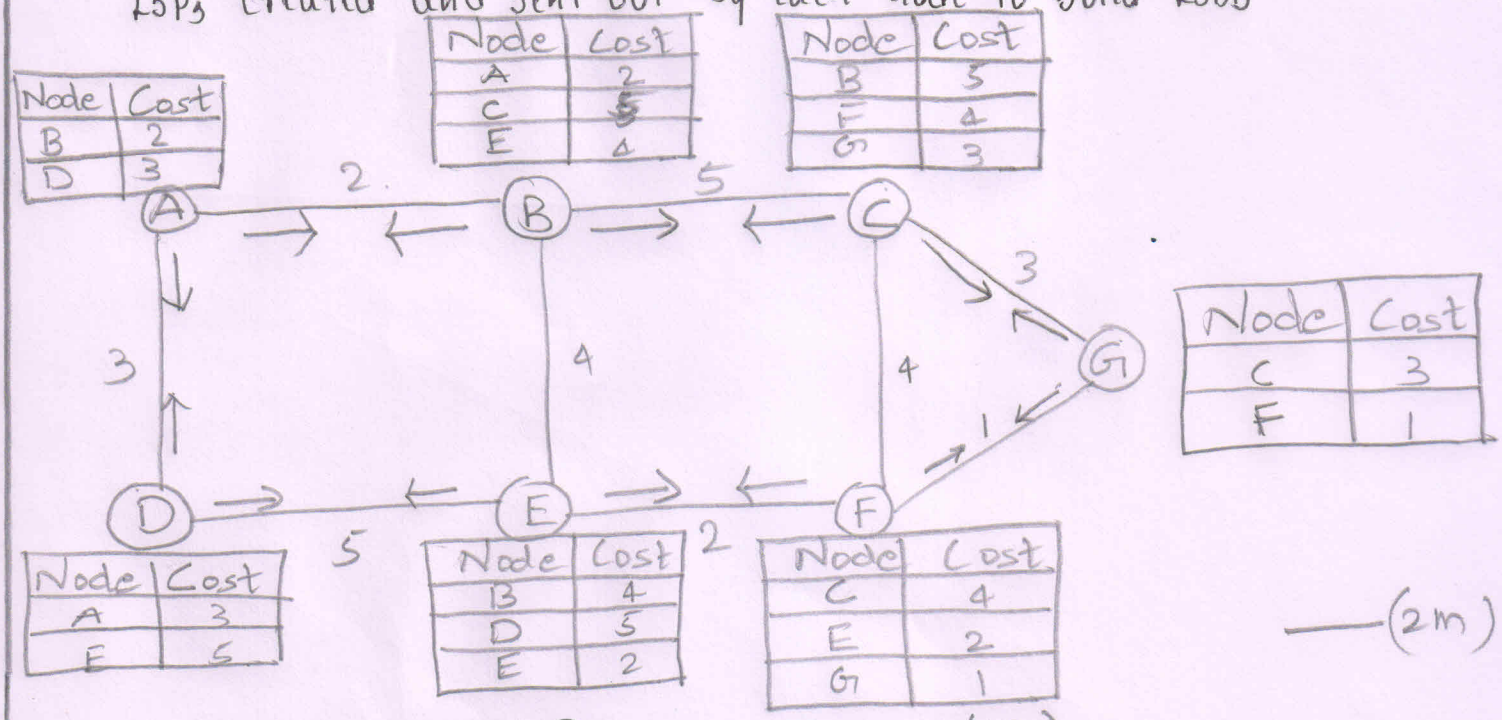
	A	B	C	D	E	F	G
A	0	2	∞	3	∞	∞	∞
B	2	0	5	∞	4	∞	∞
C	∞	5	0	∞	∞	4	3
D	3	∞	∞	0	5	∞	∞
E	∞	4	∞	5	0	2	∞
F	∞	∞	4	∞	2	0	1
G	∞	∞	3	∞	∞	1	0

Fig 7(b1) —(2m)

Each node can create this LSDB that contains information about the whole internet. And this can be done by a process called flooding. Each node can send some greeting messages to all its immediate neighbors to collect 2 pieces of information for each neighboring node: the identity of the node and the cost of the link. The combination of these 2 pieces of information is called the LS packet. the LSP is sent out of each interface. when a node receives an LSP from one of its interfaces; it compares the LSP with the copy it may already have. If the newly arrived LSP is older than the one it has. It discards the LSP. If it is newer or the first one received, the one node discards the old LSP & keeps the received one. It then sends a copy of it out of each interface except the one from which the packet arrived. This guarantees the flooding stops somewhere in the network. We need to continue

ourselves that, after receiving all new LSPs each node creates the comprehens-ive LSDB as shown in figure. This LSDB is the same for each node & shows the whole map of the internet. In other words, a node can make the whole map if it needs to, using this LSDB.

LSPs created and sent out by each node to build LSDB



(2m)

Formation of least-cost Trees Fig. 7(b2)

To create a least cost tree for itself, using the shared LSDB, each node needs to run the famous Dijkstra Algorithm. This iterative algorithm uses the following steps:

1. The node chooses itself as the root of the tree, creating a tree with a single node, & sets the total cost of each node based on the information in the LSDB.
2. The node selects one node, among all nodes not in the tree, which is closest to the root and 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 repeats step 2 until all nodes are added to the tree. We need to convince ourselves that the above 3 steps finally create the least cost tree.

Lines 4 to 13 implement step 1 in the algorithm. Lines 16 to 23 implement step 2 in the algorithm step 2 is repeated until all nodes are added to the tree. We need to go through an initialization step & six iterations to find the least cost tree.

Dijkstra's algorithm

```
1. Dijkstra's algorithm()
2. {
3. // Initialization
4. Tree = {root} // Tree is made only of the root
5. for(y=1 to N) // N is the number of nodes
6. {
7. if (y is the root)
8. D[y] = 0 // D[y] is shortest distance from root to node y
9. else if (y is a neighbor)
10. D[y] = c[root][y] // c[x][y] is cost between nodes x and y in LSDB
11. else
12. D[y] = ∞
13. }
14. // calculation
15. repeat
16. {
17. find a node w, with D[w] minimum among all nodes not in the Tree
18. Tree = Tree ∪ {w} // Add w to tree
19. // update distances for all neighbors of w
20. for (every node x, which is a neighbor of w & not in the Tree)
21. {
22. D[x] = min{D[x], (D[w] + c[w][x])}
23. }
24. } until (all nodes included in the Tree)
25. } // End of Dijkstra.
```

(4m)

8a. What is distance vector routing? Explain the various drawbacks of distance vector routing and a few solutions to overcome the same. ——— (8m)

Soln : Distance Vector Routing: In an internet, the goal of the network layer is to deliver a datagram from its source to its destination or destinations. The distance vector (DV) routing uses the goal to find the best route. —(2m)

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 between immediate neighbors to make the trees 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. Before how incomplete least cost trees can be combined to make complete ones, it is important to discuss 2 the Bellman-Ford equation & the concept of distance vectors.

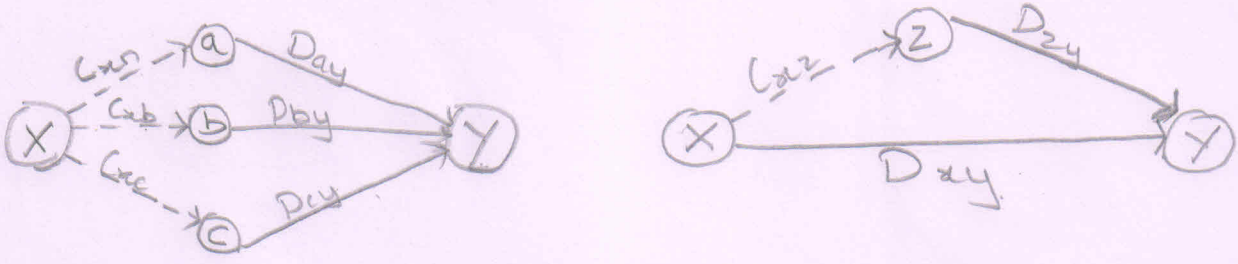
Bellman Ford Equation is the heart of distance vector routing. This equation is used to find the least cost between a source node, x & a destination node y, though some intermediary nodes (a, b, c ...) when the costs between the source & the intermediary nodes & the least costs between the intermediary nodes & the destinations are given. The following shows the general case in which D_y is the shortest distance & C_y is the cost between nodes 1 & 1

$$D_{xy} = \min\{[C_{xa} + D_{ay}), [C_{xb} + D_{by}), [C_{xc} + D_{cy}), \ldots\}$$

In distance-vector routing normally it is to update an existing least cost with a least cost through an intermediary node, such as z, if the latter is shorter. In this case, the equation becomes simple as shown below.

$$D_{xy} = \min\{D_{xy}, [C_{xz} + D_{zy})\}$$

Below figure shows how both equations can be implemented graphically.



a. General case with three intermidiate nodes

b. Updating a path with a new route

Fig. 8 (a)

Bellman Ford equation enables to build a new least cost path from previously established least-cost paths. In the figure shown below, it is $(a \to y)$, $(b \to y)$ and $(c \to y)$ as previously established least-cost paths & $(x \to y)$ as the new least-cost path. We can even think of this equation as the builder of a new least cost tree from previously least cost trees if we use the equation repeatedly. In other words the use of this equation in distance-vector routing is a witness that this method also uses least cost trees, but this use may be in the background.

(6m)

8b. Explain with diagram 3 phases of mobile IP ——— (8m)

Soln: 3 phases of mobile IP are: agent discovery, registration & data transfer

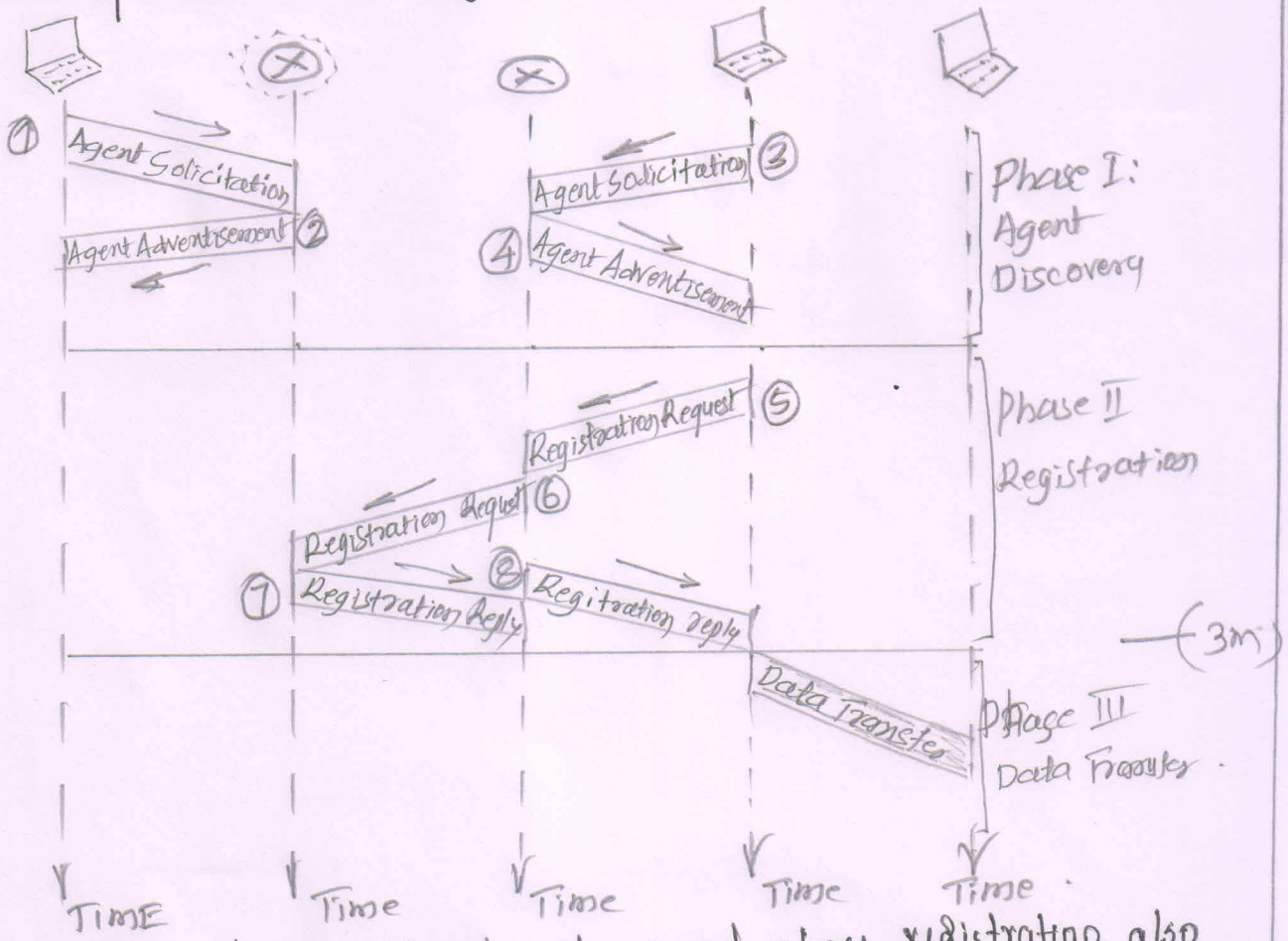


Fig. 8(b)

The first phase agent discovery involves the second phase, registration, also involves the mobile host & 2 agents. Finally in the third phase, the remote host is also involved. We discuss each phase separately.

1. Agent Discovery: The first phase in mobile communication, agent discovery, the mobile host, the foreign agent, and the home agent. It consists of 2 sub phases. A mobile host must discover a home agent before it leaves its home network. A mobile host must also discover a foreign agent after it has moved to a foreign network. This discovery consists of learning the care of address as well as the foreign agent's address. The discovery involves 2 types of messages: advertisement & solicitation.

2. Registration: The second phase in mobile communication is registration. After a mobile host has moved to a foreign network & discovered the foreign agent, it must register. There are 4 aspects of registration.

1. The mobile host must register itself with the foreign agent.
2. The mobile host must register itself with its home agent. This is normally done by the foreign agent on behalf of the mobile host.
3. The mobile host must renew registration if it has expired.

4. The mobile host must cancel its registration when it returns home

3. Data Transfer :

After agent discovery and registration, a mobile host can communicate with a remote host.

——— (5m)

9a. Explain with a neat diagram, Go-Back-N protocol. —— (8m)

Soln: Go-Back N protocol (GBN): To improve the efficiency of transmission multiple packets must be in transistion while the sender is waiting for acknowledgement. In other words, we need to let more than one packet be outstanding to keep the channel busy while the sender is waiting for acknowledgement. One protocol that can achieve this goal is called Go-Back-N The key to Go-Back-N is that we can send several packets before receiving acknowledgement arrive. Figure below shows the outline of the protocol. Note that several data packets & acknowledgement can be in the channel at the same time.

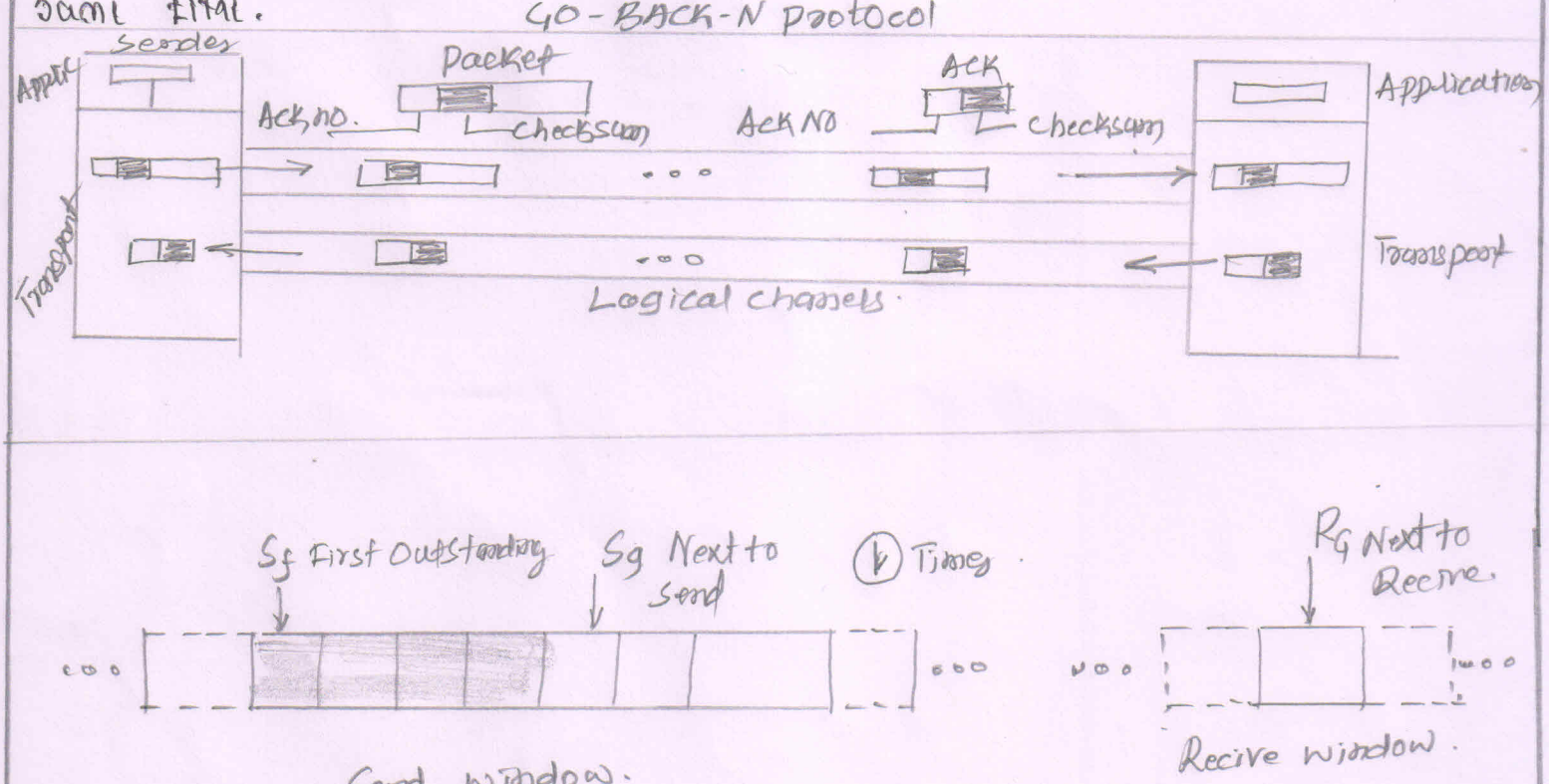
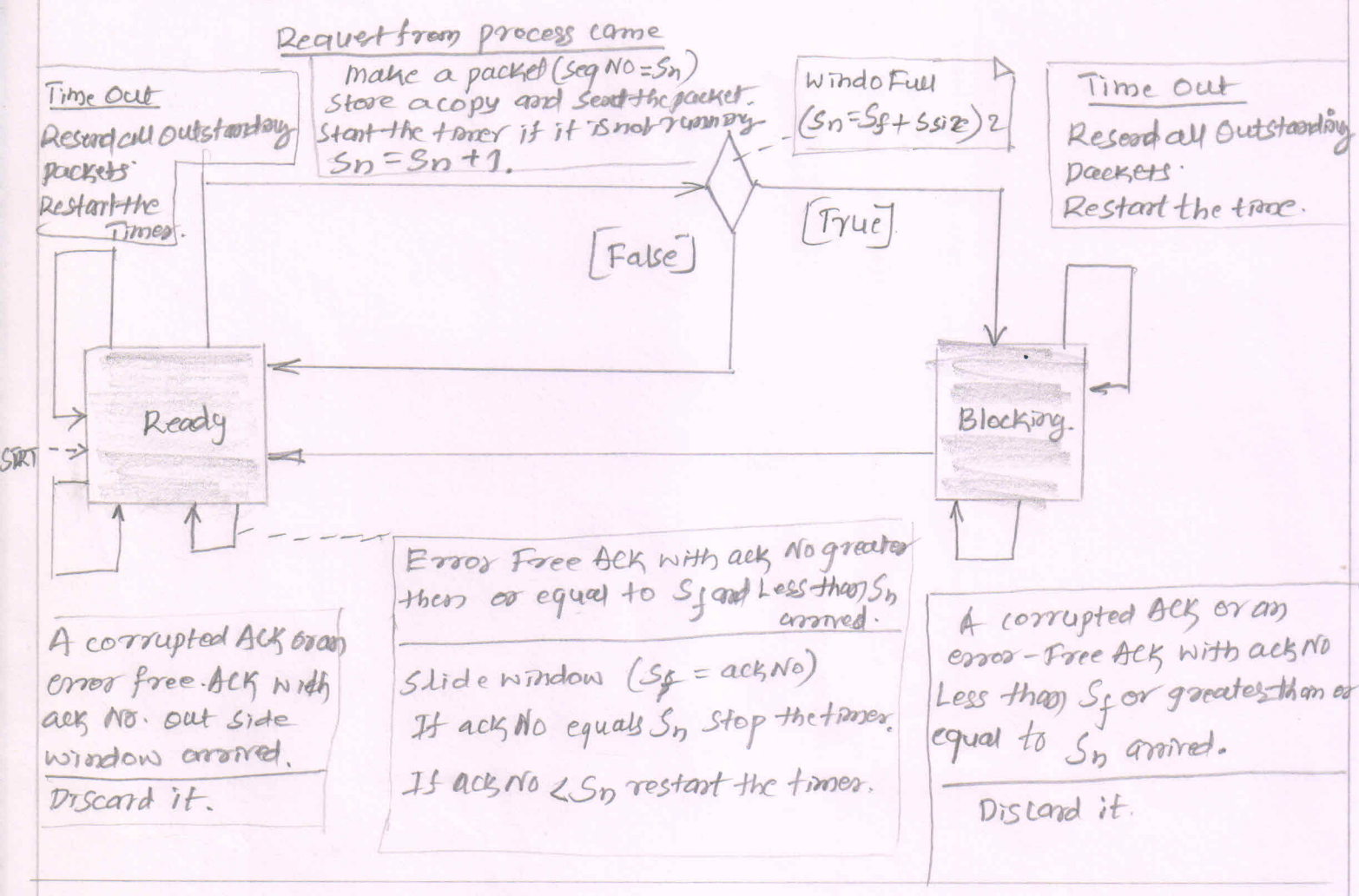


Fig 9(a1)

Note: All arithmetic equations are in modulo 2^m.



Reciver

Note
All arithmatic equations are in modulo 2^m.

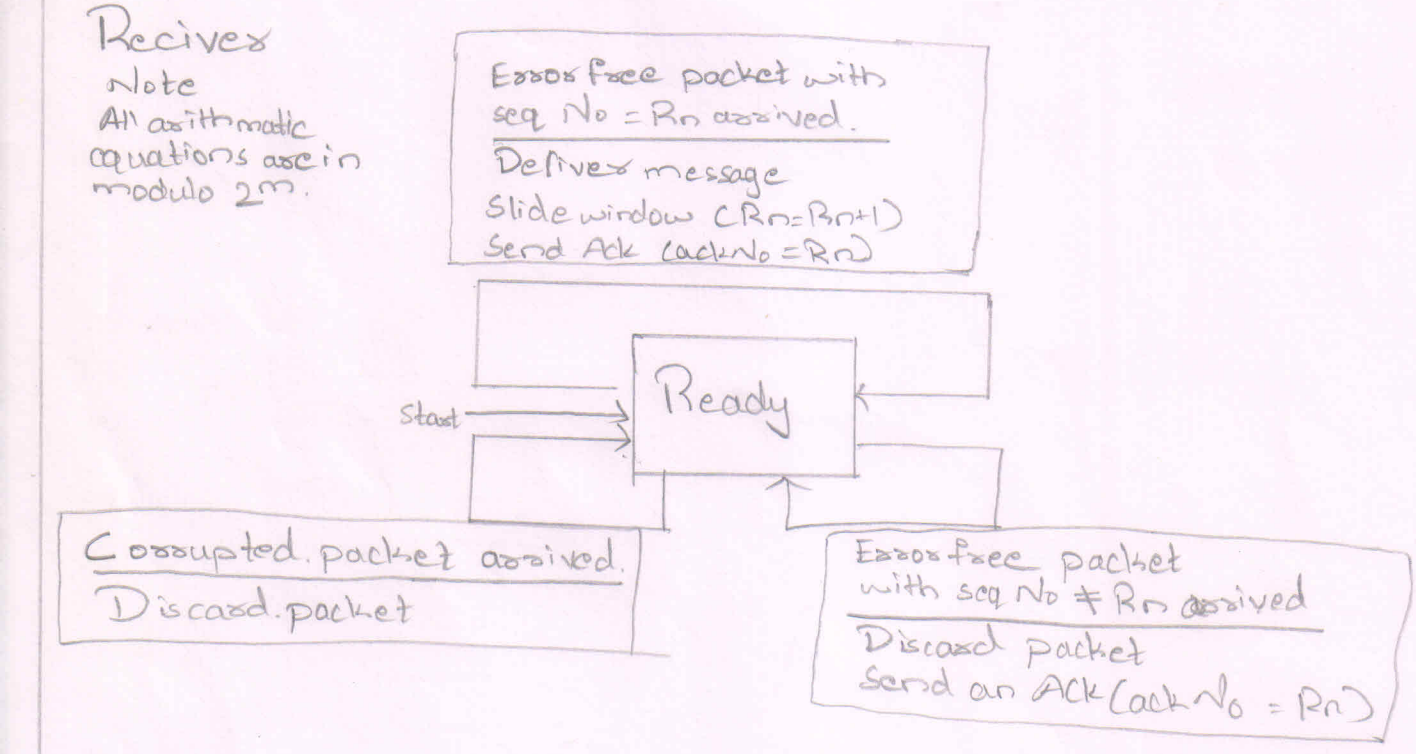


Fig. 9(a2)

(8m)

9b. Explain TCP segment format. ——— (8M)

Soln : TCP segment format: Although buffering handles the disparity between the speed of the producing & consuming process, one more step is needed before we can send data. The network layer, as a service provider for TCP, needs to send data in packets not as a stream of bytes. At the transport layer, TCP groups a number of bytes together into a packet called a segment. TCP adds a header to each segment & delivers the segment to the network layer for transmission. The segments are encapsulated in an IP datagram & transmitted This entire operation is transparent to the receiving encapsulated in an IP datagram & transmitted. This entire operation is transparent to the receiving process. Later we will see that segments may be received out of order, lost or corrupted & resent. All of these are handled by the TCP receiver with the receiving application process unaware of TCP's activities. Figure below shows how segments are created from the bytes in the buffers in TCP. ——— (4M)

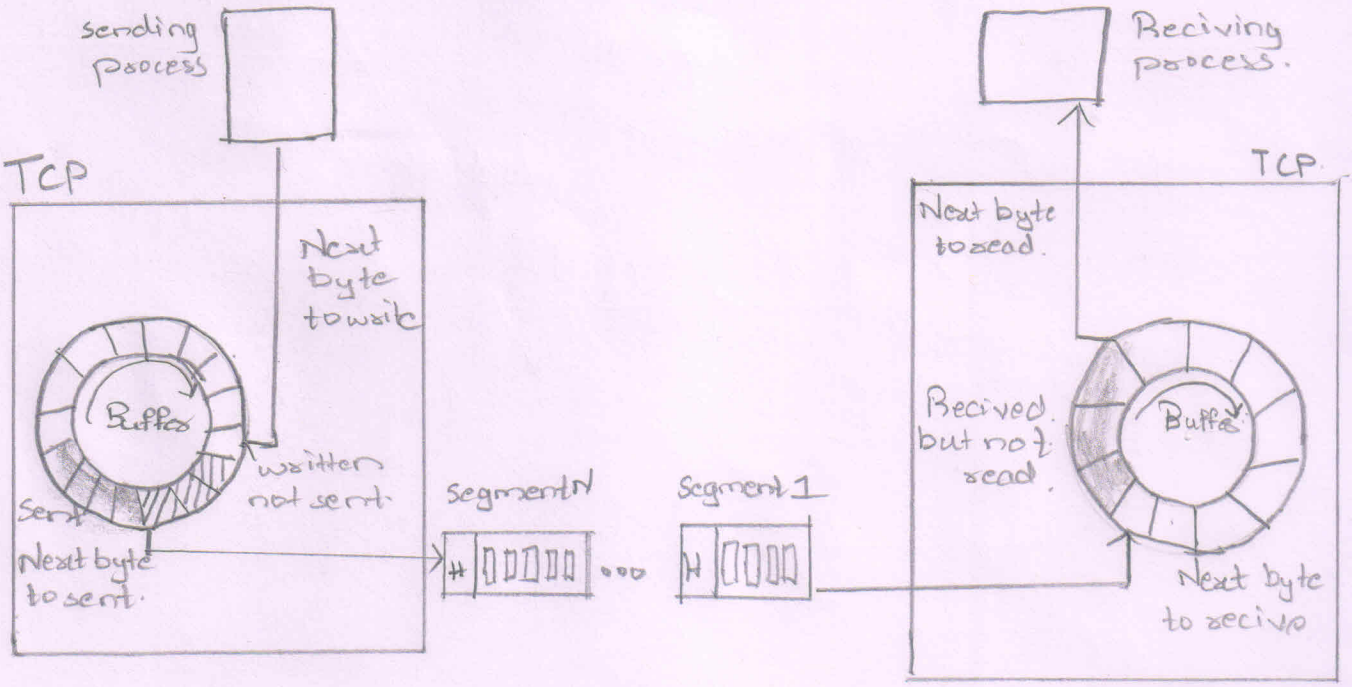


Fig. 9(b) ——— (4M)

10 a. Explain various services of UDP ——— (5m)

Soln : General services are provided by UDP are:

1. Process to Process communication : UDP provides process to process combinatio -n using socket addresses, a combination of IP addresses & port numbers.

2. Connection Services: UDP provides a connectionless service. this means that each user datagram sent by UDP is an independent datagram. There is no relationship between the different user datagrams even if they are coming from the same source process & going to the same destination program. The user datagrams are not numbered. Also, unlike TCP, there is no connection establishment and no connection termination. This means that each user datagram can travel on different path. One of the ramifications of being connectionless is that the process that uses UDP cannot send a stream of data to UDP & expect UDP to chop them into different, related user datagrams. Instead each request must be small enough to fit into one user datagram. Only those processes sending short messages, messages less than 65,507 bytes, can use UDP.

3. 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 the process using UDP should provide for this service, if needed.

4. Error Control : UDP is a very simple protocol. There is no flow co-) ×

There is no error control mechanism in UDP except for the checksum. This means that the sender does not know if a message has been lost or duplicated. When the receiver detects an error through the checksum, the user datagram is silently discarded. The lack of error control means that the process using UDP should provide for this service, if needed.

5. Checksum : UDP checksum calculation includes 3 sections: a pseudo header, the UDP header, & the data coming from the application layer. The pseudo header is the part of the header of the IP packet in which the user datagra -m is to be encapsulated with some fields filled with 0s. If the checksum does not include the pseudoheader, a user datagram may arrive safe & sound. However, if the IP header is corrupted, it may be delivered to the wrong host. The protocol field is added to ensure that the packet belongs to UDP & not to TCP the value of the protocol field for UDP is 17. If this value is changed during transmission, the checksum calculation at the receiver will detect it & UDP drops the packet. It is not delivered to the wrong protocol.

6. Congestion Control: Since UDP is a connectionless Protocol. it does not provide

Congestion control. UDP assumes that the packets sent are small & sporadic & cannot create congestion in the network. This assumption may or may not be true today, when UDP is used for interactive real-time transfer of audio and video.

7. Encapsulation And Decapsulation: To send a message from one process to another, the UDP protocol encapsulation & decapsulation messages.

8. Queuing: We have talked about ports without discussing the actual implementation of them. In UDP, queues are associated with ports. At the client site, when a process starts it requests a port number from the operating system. Some implementations create both an incoming & an outing queue associated with each process. other implementation create only an incoming queue associated with each process.

9. Multiplexing And Demultiplexing: In a host running a TCP/IP protocol suite there is only one UDP but possibly several process that may want to use the services of UDP. To handle this situation, UDP multiplexes & demultiplexes.

—(5m)

10.b. Compare connection-oriented & connectionless services. ——— (8m)

soln: Connectionless service: In a connectionless service, the source process needs to divide its message into chunks. when of data of the size acceptable by the transport layer & deliver them to the transport layer one by one. The transport layer treats each chunk as a single unit without any relation between the chunks. when a chunk arrives from the application layer, the transport layer encapsulates it in a packet & sends it. To show the independency of packets, assume that a client process has 3 chunks of messages to send to a server process. The chunks are handed over to the connectionless transport protocol in order. However since there is no dependancy between the packets at the transport layer, the packets may arrive out of order at the destination & will be delivered out of order to the server process. In figure shown below it is shown the movement of packets using a time line, but its assumed that the delivery of the process to the transport layer & vice versa are instantaneous. The figure shows that at the client site, the 3 chunks of messages are delivered to the client transport layer in order (0, 1 & 2) Because of the extra delay in transportation of the data belong to the same message, the server process may have received a strange message. The situation would be worse if one of the packets were lost. Since there is no numbering on the packets. the receiving transport layers do not coordinate with each other. the receiving transport layer does not know when the first packet will come nor when all of the packets have arrived. We can say that no flow control, error control or congestion control can be effectively implemented in a connectionless service.

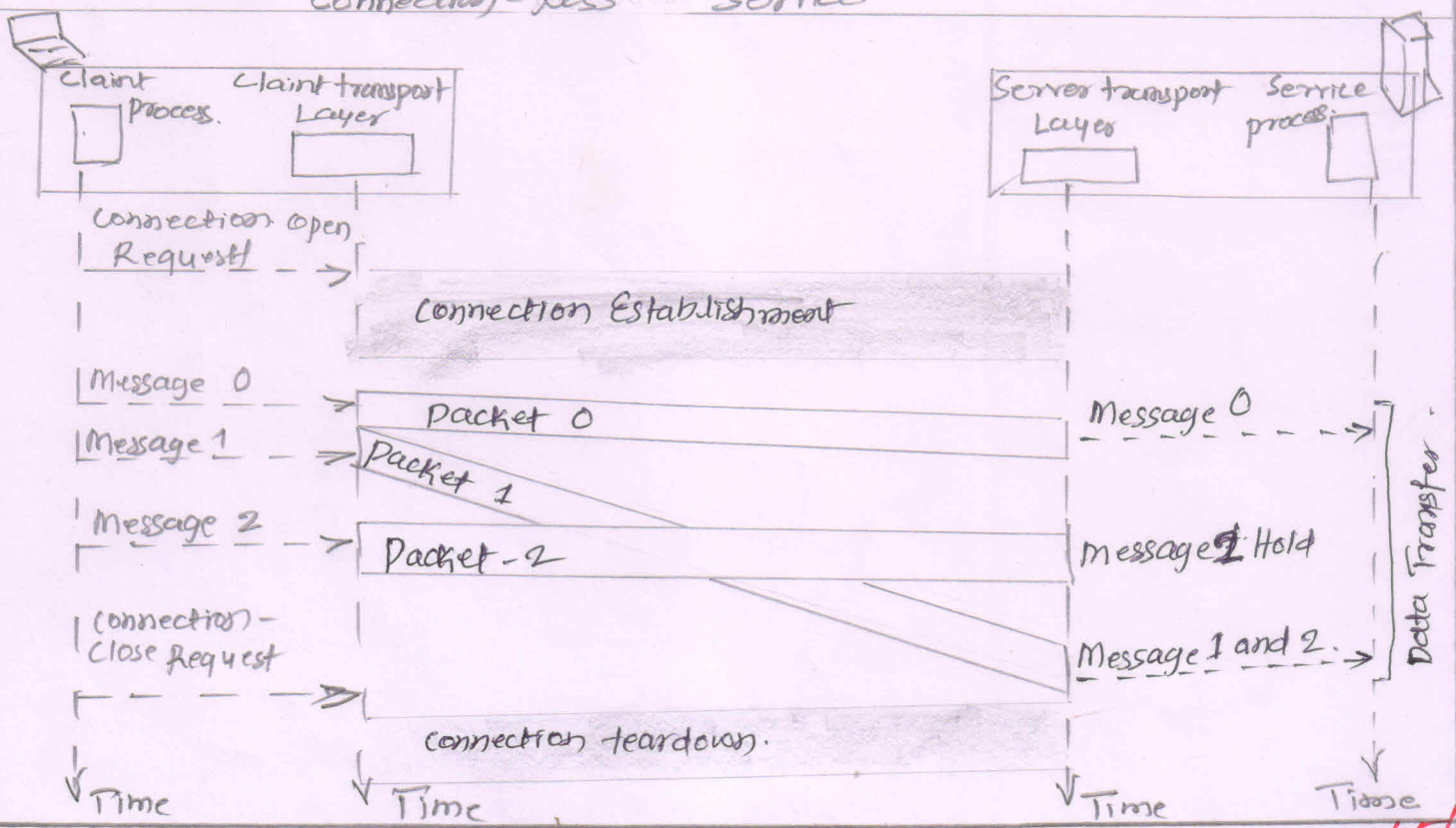


Fig 10(b1)

45/4

Connection-Oriented Service: In a connection-oriented service, the client & the server first need to establish a logical connection between themselves. The data exchange can only happen after the connection established. After data exchange, the connection needs to be torn down.

The connection-oriented service at the transport layer is different from the same service at the network layer. In the network layer, connection oriented service means a coordination between the 2 end hosts & all the routers in between. At the transport layer over either a connectionless or connection oriented protocol at the network layer. Figure below shows the connection established, data-transfer & tear down phases in a connection-oriented service at the transport layer. We can implement flow control, error control & congestion control in a connection oriented protocol.

connection Oriented service

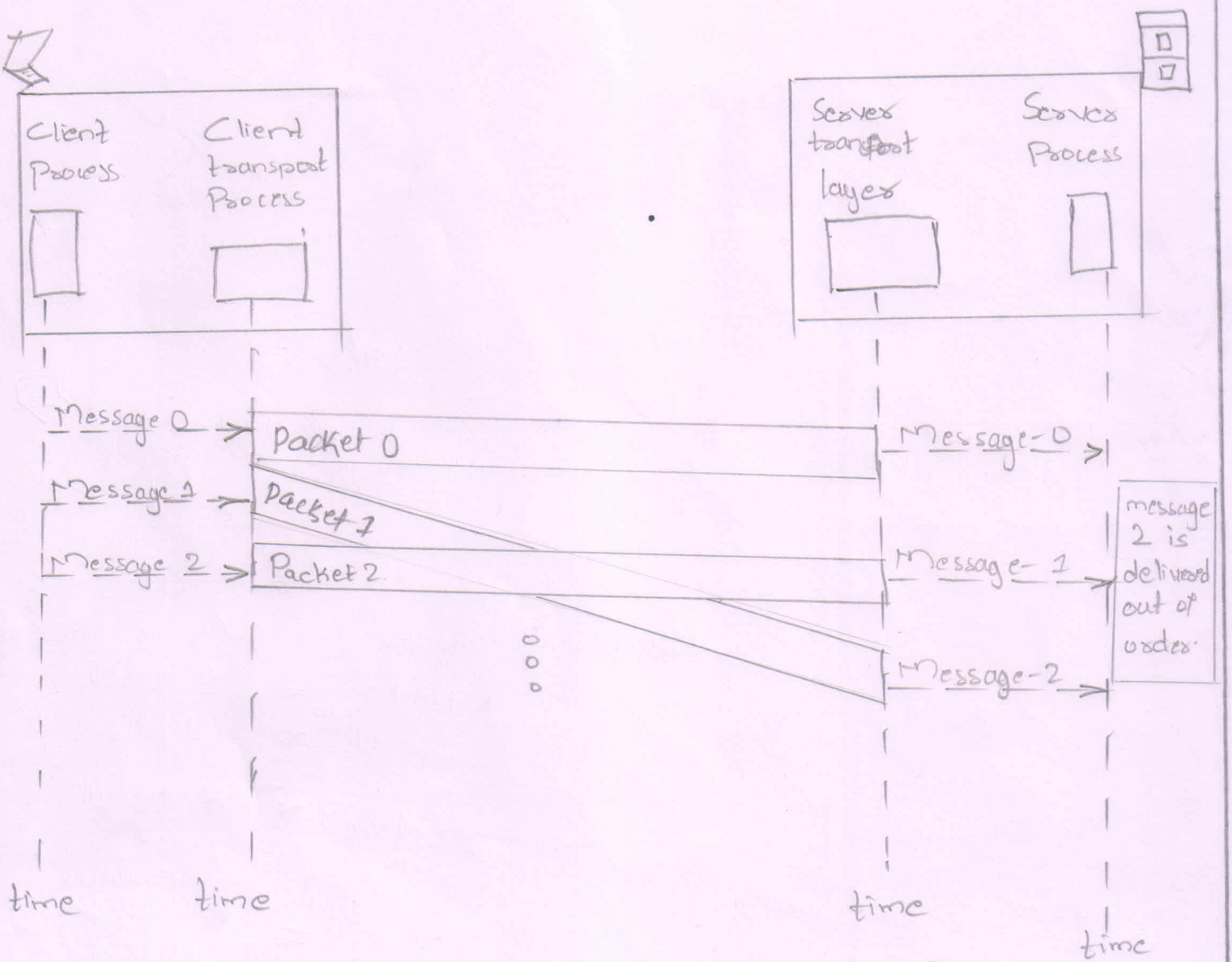


Fig. 10(b2) —(8m)

10.c. Suppose a TCP connection is transferring a file of 5000 bytes. The first byte is numbered 10001. What are the sequence numbers for each segment if data are sent in five segments, each carrying 1000 bytes? ——(3m)

Soln : The following shows the sequence number for each segment.

Segment 1 → Sequence Number: 10001 Range: 10001 to 11000
Segment 2 → Sequence Number: 11001 Range: 11001 to 12000
Segment 3 → Sequence Number: 12001 Range: 12001 to 13000
Segment 4 → Sequence Number: 13001 Range: 13001 to 14000
Segment 5 → Sequence Number: 14001 Range: 14001 to 15000

——————(3m)