CBCS SCHEME

USN □□□□□□□□□□ 15EC64

Sixth Semester B.E. Degree Examination, Dec.2019/Jan.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. Mention the layers of TCP/IP protocol suite and explain briefly about layers and protocols in each layer. (10 Marks)

b. Define bit stuffing. Perform bit stuffing for given data 0001111111001111101000 assume flag as 01111110. (06 Marks)

OR

2 a. Explain stop and wait protocol. (08 Marks)

b. (i) Define byte stuffing. (02 Marks)

(ii) Perform byte stuffing for frame payload in which E is the Escape byte, F is the Flag byte, and D is the data byte other than an Escape or Flag Character.

D	E	D	D	E	D	D	E	F	D	F	D

(06 Marks)

Module-2

3 a. Explain 1-persisent, non-persistent and p-persistent methods of (CSMA) Carrier Sense Multiple Access. (06 Marks)

b. Explain the Ethernet frame format of standard Ethernet. (06 Marks)

c. In a standard Ethernet with the transmission rate of 10 Mbps, length of the medium is 2500 meters and size of the frame is 512 bits. The propagation speed of the signal in the cable is normally 2×10^8 mts/sec. Find:

(i) Propagation delay
(ii) Transmission delay
(iii) Number of frames that can fit in the medium
(iv) Efficiency (04 Marks)

OR

4 a. Explain working of (CSMA/CD) carrier sense multiple access/collision detection. (08 Marks)

b. Discuss polling and controlled access technique. (04 Marks)

c. A slotted ALOHA network transmits 200 bit frames using a shared channel with a 200 Kbps bandwidth. Find the throughput if the system (all stations together) produce.

(i) 1000 frames/sec
(ii) 500 frames/sec
(iii) 250 frames/sec (04 Marks)

Module-3

5 a. What are the characteristics of wireless LAN? (05 Marks)

b. Write a note on Piconet and Scatternet in Bluetooth. (05 Marks)

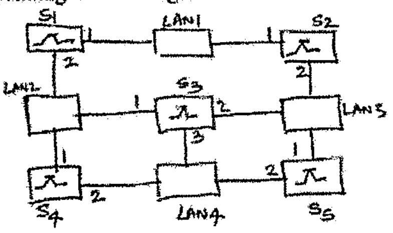
c. Explain the characteristics of Virtual Local Area Network (VLAN) used to group stations. (06 Marks)

OR

6 a. Explain the following interconnecting devices:
   (i) Hub
   (ii) Link layer switch
   (iii) Router (06 Marks)

b. What is NAT? Explain how NAT helps in Address depletion (Network Address Translation). (05 Marks)

c. Find the spanning tree and logical connection between the switch.



$S_1, S_2, S_3, \ldots S_5$ are switches

Fig.Q6(c) (05 Marks)

Module-4

7 a. Explain IPV4 datagram format. (08 Marks)

b. Explain three phases of remote host and mobile host communication. (08 Marks)

OR

8 a. Explain least cost tree using shared link state data base with suitable example. (10 Marks)

b. With a neat diagram, explain general format of ICMP messages. (06 Marks)

Module-5

9 a. With a neat diagram, explain connection establishment, data transfer and connection termination in Transmission Control Protocol (TCP). (10 Marks)

b. The following is the content of UDP (User Datagram Protocol) header in hexadecimal format CB84000D001C001C. Find:
   i) What is the source port number?
   ii) What is the Destination port number?
   iii) What is the total length of the user datagram?
   iv) What is the length of the data?
   v) Is the packet directed from a client to a server or vice versa? (06 Marks)

OR

10 a. Briefly explain TCP segment format. (10 Marks)

b. Explain different field in user datagram packet format with a neat diagram. (06 Marks)

* * * * *

Scheme & Solution

VTU Question Paper - January 2020

Subject : Computer Communication Networks (15EC64)

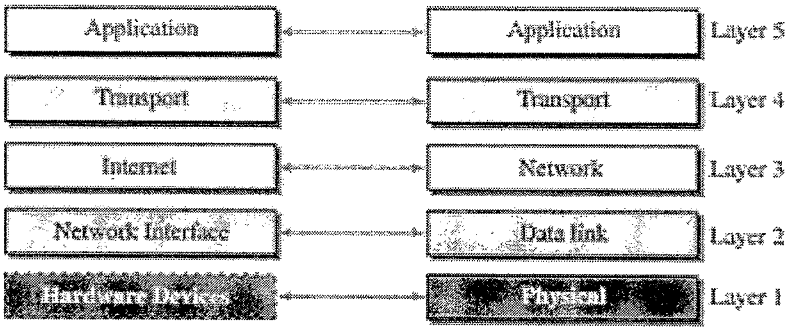
Prepared by: Dr. Arun Kakhandki, Professor, ECE Dept, KLS VDIT, Haliyal.

Module - 1

Q.1(a):

Mention the layers of TCP/IP protocol suite and explain briefly about layers and protocols in each layer --- (10 marks)

Soln:



— (2½ m)

Fig. 1 (a)

Description of each layer - — 1½ m x 5 = 7½ m

1. Physical Layer -

Physical Layer is the lowest level in TCP/IP protocol suite. The communication between two devices at the physical layer is still a logical communication because there is another layer, the transmission media, under the physical layer which is hidden.

2. Data-link layer -

Data-link layer is responsible for taking the datagram and moving across the link. The link can be a wired LAN with a link-layer switch, a wireless LAN, a wired LAN, or a wireless WAN.

TCP/IP does not define any specific protocol for data-link layer. The data-link layer takes a datagram and encapsulates it in a packet called a "frame".

Examples of data-link protocols are Ethernet, point-to-point (PPP), HDLC and MAC.

3. Network Layer -

Network layer is responsible for creating a connection between the source computer & distination. The communication at the network layer is host-to-host. and packet takes the possible route out of many available 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. The other auxiliary protocols of the network layer are ICMP, IGMP, DHCP and ARP.

4. Transport Layer -

The logical connection at the transport layer is end-to-end. The transport layer at the source host gets the message from the application layer, encapsulate it in a tansport layer packet (called a segment or user datagram) and sends it thro' the logical (imaginary) connection, to the transport layer at the destination host. In other words, transport layer is responsible for giving services to the application layer.

The various protocols of transport layer are TCP, UDP, SCTP.

5. Application Layer -

In application layer communication is process-to-process. To communicate, a process sends a request to the other processes and receive a response.

Various protocols of application layer are: HTTP, SMTP, FTP, TELNET, ~~SHELL~~ (SSH), SNMP

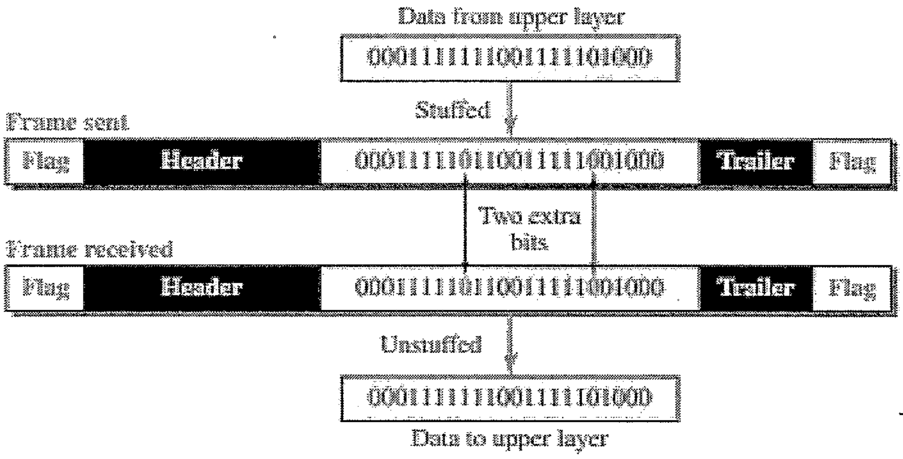
Q.1(b):

Define bit stuffing. Perform bit stuffing for a given data 0001111111001111101000. Assume flag as 01111110. --- (6 marks)

Soln:

Bit stuffing -

Bit stuffing is the process of adding one extra zero (0) whenever fire consecutive one's (1's) follow a zero (0) in the data, so that receiver does not mistake the pattern 0111110 for a flag. —— (2M)



—— (4M)

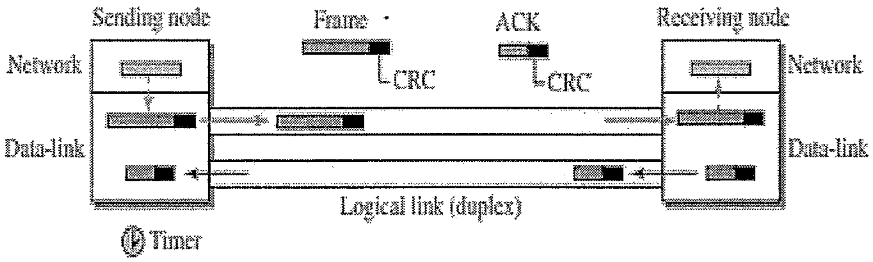
Fig. 1(b)

Q.2(a):

Explain stop and wait protocol --- (8 marks)

Soln:

Stop and Wait Protocol -



—(3m)

Fig. 2(a)

Stop and wait protocol uses both flow and error control mechanism. In this protocol, Sender sends one frame at a time and wait for an acknowledgement before sending the next one. To detect corrupted frames, CRC needs to be added to each data frame. When a frame arrives at a receiver site, it is checked. If its CRC is incorrect, the frame is corrupted and silently discarded. The silence of the receiver is the signal for the sender that a frame was either corrupted or lost. Everytime a sender sends a frame, it starts a timer. If ~~the~~ an acknowledgement arrives before the timer expires, the timer is stopped and the sender sends the next frame (if it has one to send). If timer expires, sender resends the previous frame, assuming that the frame was either lost or corrupted. This means that the sender needs to keep the copy of the frame until its acknowledgement arrives. When the corresponding acknow-ledgement arrives, the sender discards the copy and sends the next frame it is ready. In stop and wait protocol, only one frame and one acknowledgement can be in the channels at any time.

The outline from stop and wait protocol is as shown in above figure 2(a). —— (5m)

Q.2(b):

(i) Define byte stuffing --- (2 marks)

(ii) Perform byte stuffing for the payload in which E is the escape byte, F is the flag byte, and D is a data byte other than an escape or a flag character --- (6 marks)

D	E	D	D	E	D	D	E	F	D	F	D

Soln:

(i) Byte stuffing -

Byte stuffing is the process of adding one extra byte whenever there is a flag or escape character in the text. —(2M)

ii) Consider the given data:

E = Escape byte; Flag byte = F; Data byte = D.

Byte stuffing process:

(a) The byte stuffing process adds a new byte to the frame. The new byte refers as flag byte. If a character is present with the same pattern as flag, the byte stuffing process adds a new byte to the data.

(b) The byte stuffing process begins with the flag byte followed by a header (H) and ends with a trailer (T) byte and flag (F) byte.

(c) If a flag byte encounters in the middle, then add one extra escape (E) byte before flag (F) byte.

(d) If an escape byte occurs, then add one escape byte before escape bit. —(3m)

∴ Give frame payload is

D	E	D	D	E	D	D	E	F	D	F	D

Final payload using byte stuffing is given by

F	H	D	E	E	D	D	E	E	D	D	E	E	E	F	D	E	F	D	T	F

—(3m)

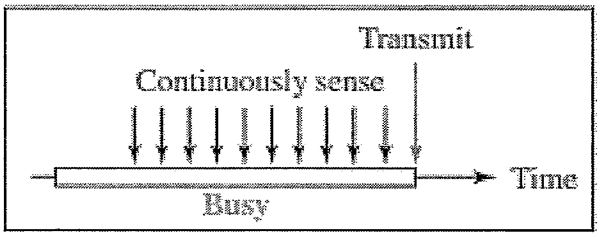
Module - 2

Q.3(a):

Explain 1-persistent, non-persistent and P-persistent methods of CSMA --- (6 marks)

Soln:

(i) 1 - persistent method -

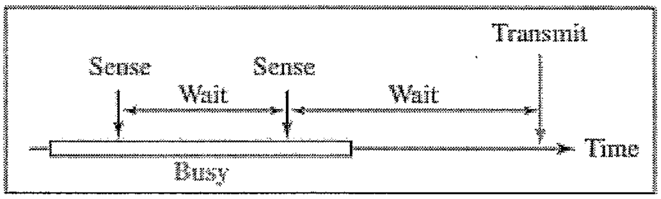


— (1M)

Fig. 3(a)-1

The 1 - persistent method is simple & straightforward. In this method, after the station finds the line idle, it sends its frame immediately (with probability 1). This method has the highest chance of collision, because two or more stations may find the line idle and send their frames immediately. — (1M)

(ii) Non - persistent method -

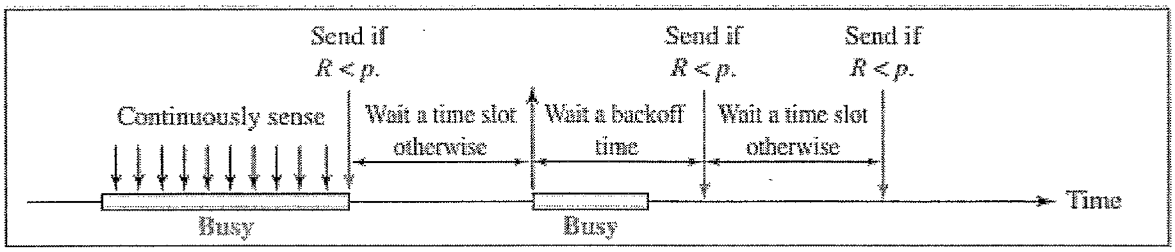


— (1M)

Fig. 3(a) - 2

In the non-persistent method, a station that has a frame to send senses the line. If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again. The non-persistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously. — (1M)

(iii) p-persistent method -



(1m)

The p-persistent method is used if the channel has time slots with a slot duration equal to greater than the maximum propagation time. The p-persistent approach combines the advantages of other two strategies. It reduces the chance of collision and improves efficiency. In this method, after the station finds the line idle it follows these steps :

1) with probability p, the station sends its frame.

2) with probability q = 1-p, the station waits for the beginning of the next time slot and checks the line again.

(a) if the line is idle, it goes to step 1

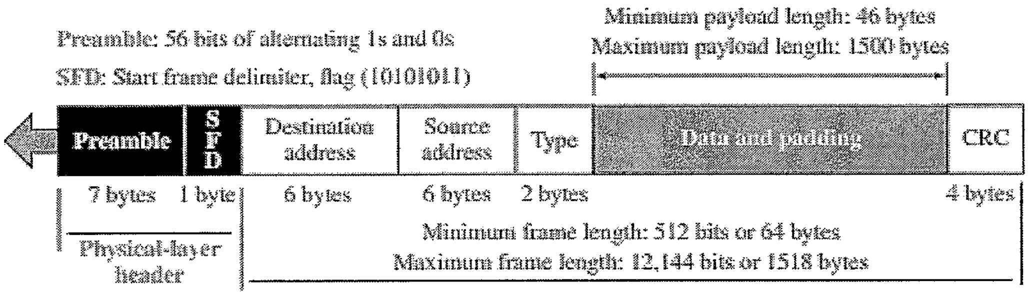
(b) if the line is busy, it acts as though a collision has occured and uses the back-off procedure.

(1m)

Q.3(b):

Explain the Ethernet frame format of standard Ethernet --- (6 marks)

Soln: The Ethernet frame format of standard Ethernet contains seven fields as shown in figure below.


Preamble: 56 bits of alternating 1s and 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 and padding
CRC
7 bytes
1 byte
6 bytes
6 bytes
2 bytes
4 bytes
Physical-layer header
Minimum frame length: 512 bits or 64 bytes
Maximum frame length: 12,144 bits or 1518 bytes

—(2m)

Fig. 3(b)

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

(ii) Start Frame Delimiter (SFD): This field (1byte: 10101011) signals the beginning of the frame. The SFD warns the station or stations that this is the last chance for synchronization. The last two 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. Ethernet frame is a variable-length frame and it needs a flag to define the beginning of the frame. The SFD is also added at the physical layer.

(iii) Destination address (DA): This field is 6 bytes or 48 bits and contains the link-layer address of the destination station or stations to receive the packet. 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 broad-cast address, it decapsulates the data from the frame and passes the data to upper-layer protocol. defined by the value of the type field.

(iv) Source address (SA) : This field is also six bytes and contains the link-layer address of the sender of the packet.

(v) Type : This field defines the upper-layer protocol whose packet is encapsulated in the frame. This protocol can be IP, ARP, OSPF etc. It serves the same purpose as the protocol field in a datagram and the port number in a segment or user datagram. It is used for multiplexing and demultiplexing.

(vi) Data : This field carries data encapsulated from the upperlayer protocols. It is a minimum of 46 and a maximum of 1500 bytes. If the data coming from upper layer is more than 1500 bytes, it should be fragmented and encapsulated in more than one frame. If it is less than 46 bytes, it needs to be padded with extra zero's (0's). A padded data frame is delivered to the upper-layer protocol as it is, which means that it is the responsibility of the upper layer to remove or in case of the sender, to add the padding. The upper layer protocol needs to know the length of the data.

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

—— (4m)

Q.3(c):

In the Standard Ethernet with the transmission rate of 10 Mbps, length of the medium is 2500 m and the size of the frame is 512 bits. The propagation speed of a signal in a cable is normally 2 × 10^8 m/s.
Find (i) Propagation delay (ii) transmission delay (iii) number of frames that can fit in the medium (iv) Efficiency --- (6 marks)

Soln:

(a) Propagation delay $= \dfrac{\text{Length of the medium}}{\text{Propagation speed of a signal}}$

$$= \frac{2500}{2 \times 10^8} = \underline{\underline{12.5\ \mu\text{sec}}}$$

(b) Transmission delay $= \dfrac{\text{Size of the frame}}{\text{Transmission rate}}$

$$= \frac{512\ \text{bits}}{10 \times 10^6} = \underline{\underline{51.2\ \mu\text{sec}}}$$

(c) No of frames that can fit in the medium,

$$a = \frac{\text{propagation delay}}{\text{Transmission delay}} = \frac{12.5\ \mu\text{sec}}{51.2\ \mu\text{sec}} = \underline{\underline{0.24}}$$

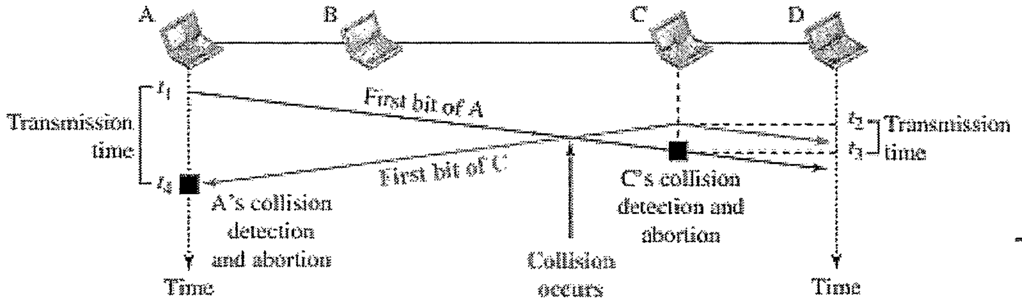
which means only 0.24 of a frame occupies the whole medium.

(d) Efficiency $= \dfrac{1}{1 + 6.4 \times a} = \dfrac{1}{1 + (6.4 \times 0.24)}$

$$= \underline{\underline{39.4\ \%}}$$

Q.4(a):
Explain CSMA/CD --- (8 marks)

Soln: CSMA/CD



(3m)

Fig. 4(a)

- CSMA/CD augments the algorithm to handle collision. In CSMA/CD, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however there is a collision, the frame is sent again.

- To understand CSMA/CD method, refer the Fig. 4(a) where stations 'A' and 'C' are involved in the collision.

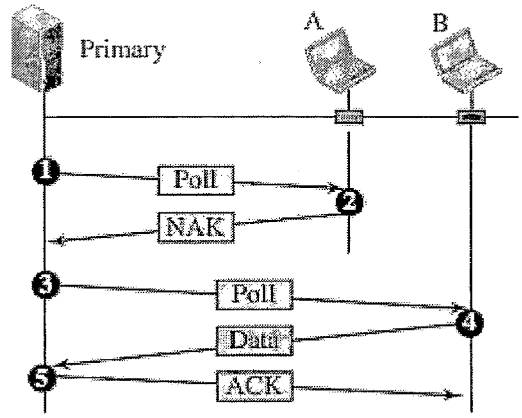
At time t_1, station 'A' has executed its persistence procedure and starts sending the bits of its frame. At time t_2, station 'C' has not yet sensed the first bit sent by 'A'. Station 'C' executes its persistence procedure and starts sending the bits in its frame, which propagates both to the left and to the right. The collision occur sometime after time t_2. Station 'C' detects a collision at time t_3 when it receives ~~the~~ first bit of 'A's frame. Station 'C' immediately aborts transmission. Station 'A' detects collision at time t_4 when it receives the first bit of C's frame; it also immediately aborts transmission.

From figure it is very clear that 'A' transmits for the duration $t_4 - t_1$ and 'C' transmits for the duration $t_3 - t_2$.

For CSMA/CD to work, restriction on the frame size is needed. Before sending the last bit of the transmission, the sending station must detect a collision if any, and abort the transmission. (5m)

Q.4(b):
Discuss polling as controlled access technique --- (4 marks)

Soln: Polling :



—— (2m)

Fig. 4(b)

Polling works with topologies in which one device is designated as a "primary station" and other devices are "secondary stations". All data exchanges must be made thro' the primary device even when the ultimate destination is a secondary device. The primary device controls the link; the secondary devices follow its instructions. It is up to the primary device to determine which device is allowed to use the channel at a given time. The primary device, therefore, is always the initiator of a session.

The drawback of the polling is, if the primary station fails, the system goes down. —— (2m)

Q.4(c):

A slotted ALOHA network transmits 200-bit frames using a shared channel with a 200-kbps bandwidth. Find the throughput if the system (all stations together) produces

a. 1000 frames per second.

b. 500 frames per second.

c. 250 frames per second. --- (4 marks)

Soln:

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

(a) If the system creates 1000 frames/sec or 1 frame/msec, then $G = 1$.

In this case $S = G \times e^{-2G} = 0.135$ (13.5%)

∴ Throughput = 1000 × 0.135 = 135 frames.

∴ only 135 frames out of 1000 will probably survive. — (1m)

(b) If the system creates 500 frames/sec or $\frac{1}{2}$ frames/sec, then $G = \frac{1}{2}$.

In this case $S = G \times e^{-2G} = 0.184 = 18.4\%$.

∴ Throughput = 500 × 0.184 = 92

∴ Only 92 frames out of 500 will probably survive. — (1m)

(c) If the system creates 250 frames/sec or $\frac{1}{4}$ frames/sec, then $G = \frac{1}{4}$

In this case $S = G \times e^{-2G} = 0.152 = 15.2\%$

∴ Throughput = 250 × 0.152 = 38

∴ Only 38 frames out of 250 will probably survive. — (1m)

Module - 3

Q.5(a):
What are the characteristics of wireless LAN? --- (5 marks)

Soln: Several characteristics of wireless LAN are;
Attenuation, interference, multipath propagation & error.

(i) Attenuation : The strength of electromagnetic signals decreasing rapidly because the signal disperses in all directions; only a small portion of it reaches the receiver. The situation becomes worse with mobile senders that operate on batteries and normally have small power supplies.

(ii) Interference : Another issue is that a receiver may receive signals not only from the intended sender, but also from other senders if they are using the same frequency band.

(iii) Multipath propagation : A receiver may receive more than one signal from the same sender because electromagnetic waves can be reflected back from obstacles such as walls, the ground, or any objects. ~~The~~ As a result, the receiver may receives some signals at different phases (because they travel different paths). This makes the signal less recognizable.

(iv) Error :- with the characteristics likee attenuation, interference, and multipath propagation, errors and error detection are expected and may be more serious issues in a wireless network than in a wired network. If error level becomes the measurement of SNR, then it becomes why error detection and error correction and retransmission are more important in a wireless network. SNR measures the ~~good~~ ratio of good stuff to bad stuff (signal to noise). If SNR is high, then the signal is stronger than the noise, so it may be possible to convert the signal to actual data. If SNR is low, then the signal is corrupted by the noise and the data cannot be recovered.

—— (5m)

Q.5(b):

Write a note on Piconet and Scatternet in Bluetooth --- (5 marks)

Soln:

Piconet -

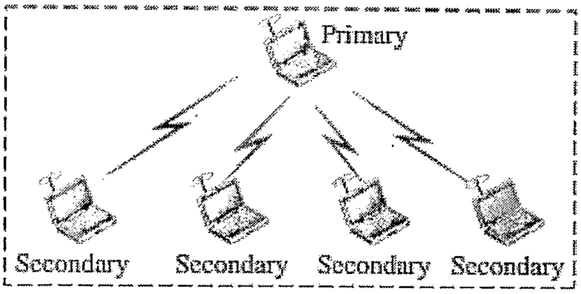


Fig. 5(b)1

A bluetooth network is called a piconet, or a small net. A piconet can have stations up to eight, one of which is called the primary; the rest are called secondaries. All secondary stations synchronize their clocks & hopping sequence with the primary. The communication between primary & secondary stations can be one-to-one or one-to-many and a piconet can have only one primary. Any secondary station more than seven can be in parked state. A secondary in parked state can be synchronized with primary, but can not take part in communication until is moved from parked state to active state. —— (2 1/2 M)

Scatternet -

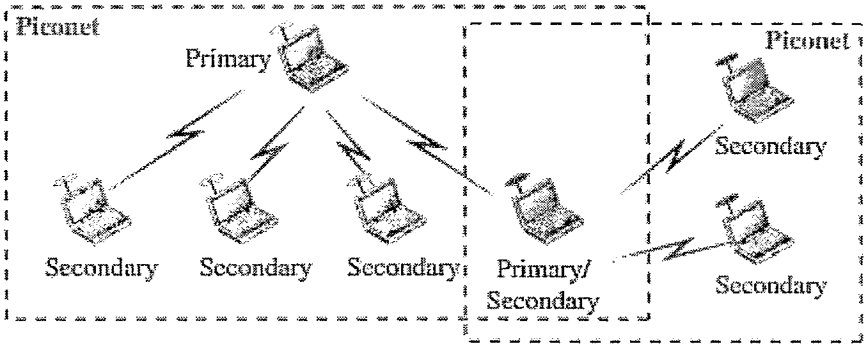


Fig. 5(b)2

Piconets can be combined to form a scatternet. A secondary station in one piconet can be the primary in another piconet. This station can receive messages from primary in the first piconet (as a secondary) and, acting as primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets. ——(2 1/2 M)

Q.6(a):
Explain the following interconnecting devices:
(i) Hub (ii) Link layer switch (iii) Router --- (6 marks)

Soln: (i) Hub :

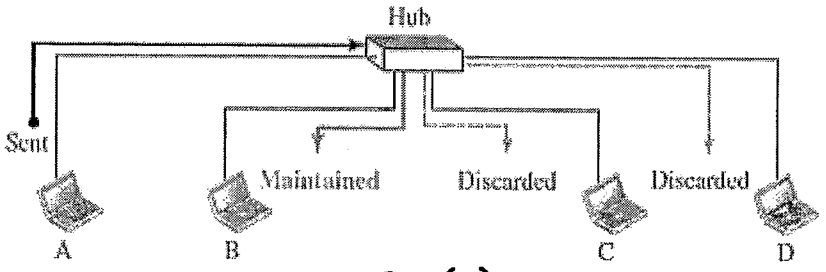
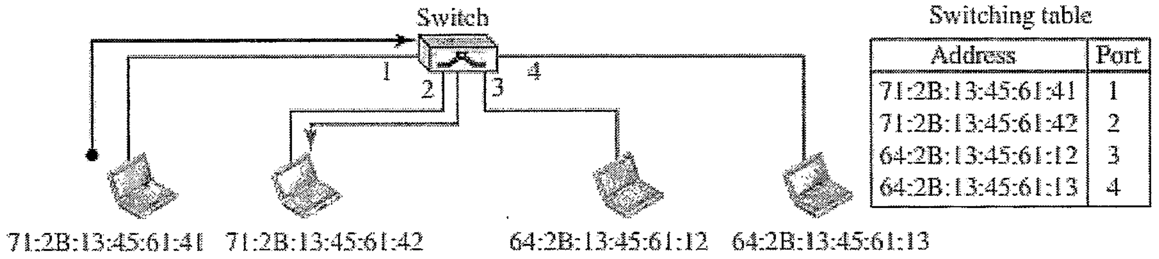


Fig. 6(a)1 —(2m)

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 the data. A hub or a repeater receives the signal and, before it becomes too weak or corrupted, regenerates & retimes the original bit pattern. The repeater then sends the refreshed signal.

Being a physical layer device, a hub or a repeater do not have a link-layer address and they donot check the link layer address of the received frame. They just regenerate the corrupted bits and send them out from every port.

(ii) Link-Layer switch :



Switching table

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

Fig. 6(a)2 —(2m)

A link-layer switch operates in both physical and data-link layer. As a physical layer device, it regenerates the signal it receives. As a data-link layer device, the link-layer switch can check the MAC addresses (source & destination) contained in the frame.

Unlike hub, a link-layer switch has filtering capability. It can check the destination address of a frame and can decide from which outgoing port the frame should be sent. A link-layer switch has a table used in filtering decisions.

(iii) Router :

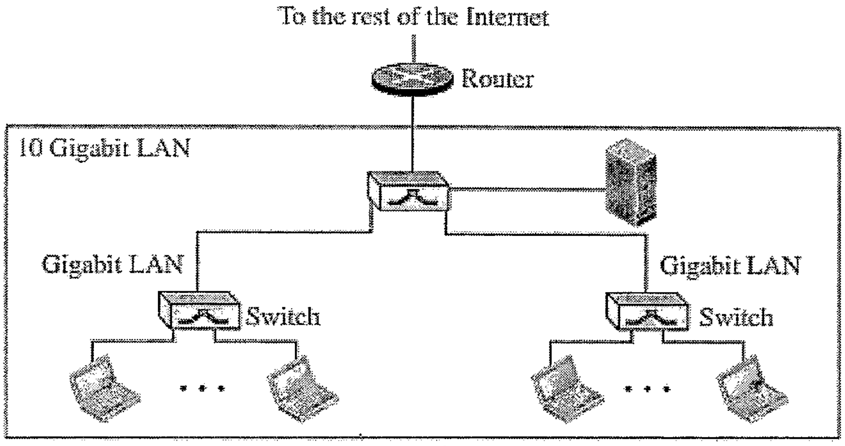


Fig. 3(a) 3

——(2m)

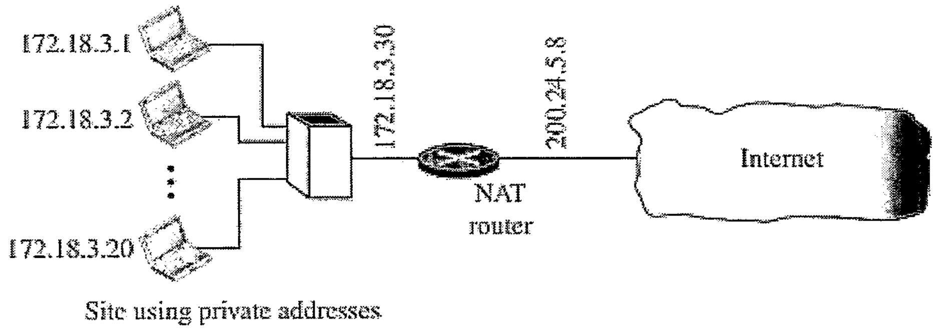
A router is a three-layer device which operates in physical, data-link, and network layers. As a physical layer device, it regenerates the signal it receives. As a link-layer device, the router checks the physical addresses (source & destination) contained in the packet. As a network layer device, a router checks the network layer addresses.

A router can connect networks i.e., a router is an internet-working device; it connects independent networks to form an internetwork. Two networks connected by a router become an internetwork or internet.

Q.6(b):

What is NAT? Explain how NAT helps in address depletion (Network Address Translation) --- (5 marks)

Soln: NAT :



— (1m)

Fig. 6(b)

A technology that can provide the mapping between the private and universal addresses, and at the same time support virtual private networks is called Network Address Translation. (NAT).

NAT allows a site to use a set of poivate addresses for internal communication and a set of global internet addresses (at least one) for communication with the rest of the world. The site must have only one connection to the global internet thro' a NAT capable router that runs NAT software. — (2m)

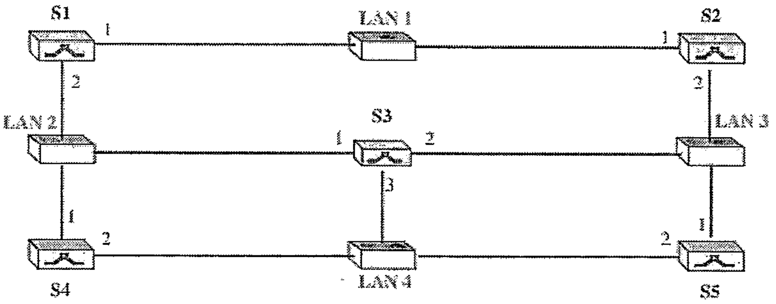
Address Translation :

All of the outgoing packets go thro' the NAT router, which replaces the source address in the packet with the global NAT address. All incoming packets also pass thro' the NAT router, which replaces the destination address in the packet (NAT router global address) with the appro-priate private address.

NAT router has a tanslation table to tanslate the destination address for a packet coming from the internet. — (2m)

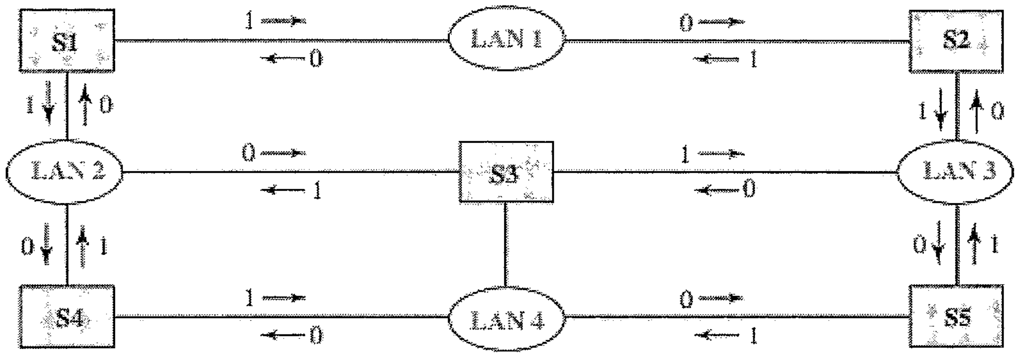
Q.6(c):

Find the spanning tree and logical connection between the switch --- (5 marks)



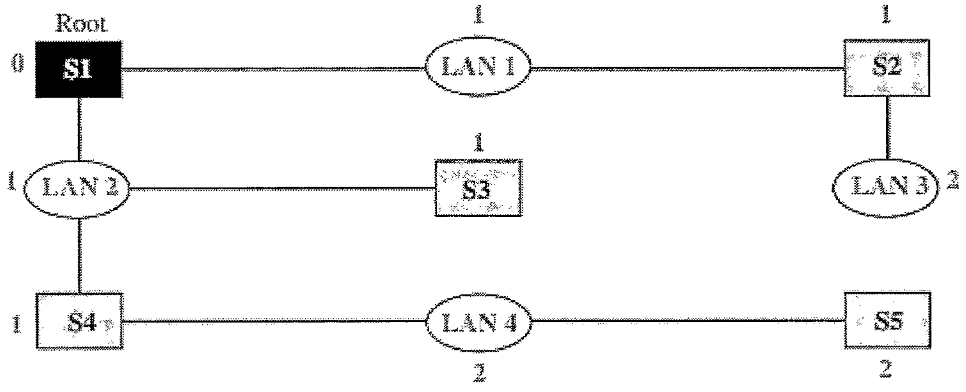
S1, S2, S3, S4 S5 are switches.

Soln:



Graph representation with cost assigned to each arc

—(2m)



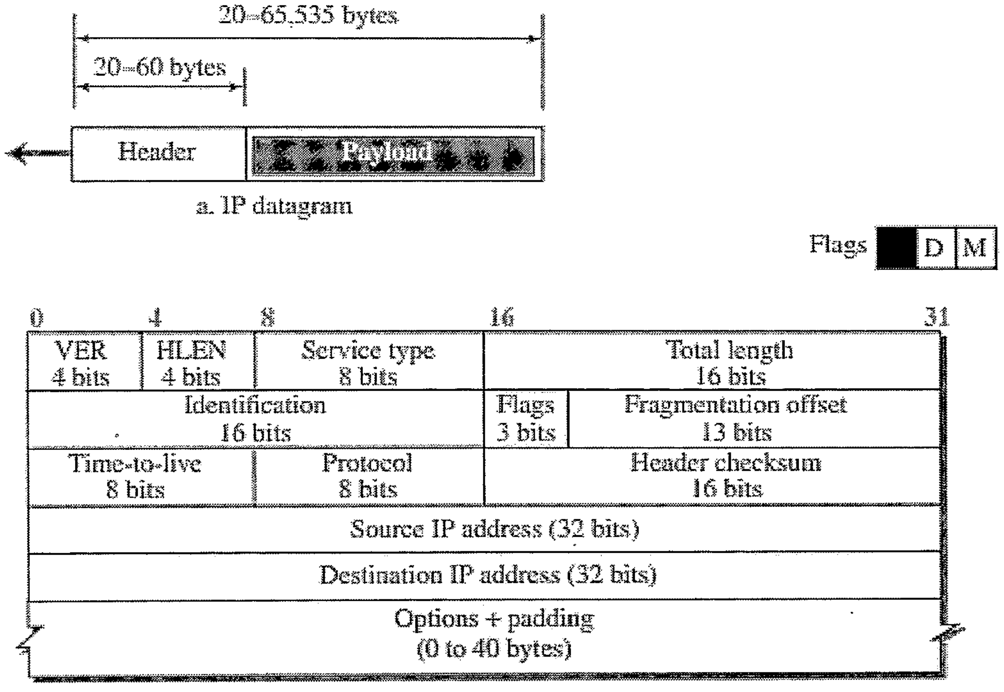
Finding the shortest paths and the spanning tree in a system of switches

— (3m)

Module - 4

Q.7(a):
Explain IPv4 datagram format --- (8 marks)

Soln: IPv4 datagram format -



a. IP datagram

b. Header

— (2m)

Fig. 7(a)

IPv4 datagram is a variable-length packet consisting of two parts: header and payload (data). The header is 20-60 bytes in length and contains information essential to routing and delivery.

Description of each field in IPv4 datagram: — (6m)

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

(ii) Header length: The 4-bit header length (HLEN) field 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 and 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 and the value is inserted in the field. The receiver needs to multiply the value of this field by 4 to find the total length.

(iii) Service Type : IETF redefined this field to provide differential services (DiffServ) from type of service (TOS). 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.

(iv) Total Length : This 16 bit field defines the total length (header + data) of the IP datagram in bytes. A 16-bit number can define a total length of up to 65,535 (when all bits are 1) However, the size of the datagram is normally much less than this. This field helps the receiving device to know when the packet has completely arrived. To find the length of 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.

$\therefore$ Length of data = Total length − (HLEN × 4).

(v) Identification, Flags, and Fragmentation offset : These three fields are related to the fragmentation of the IP datagram when the size of the datagram is larger than the underlying network can carry.

(vi) Time-to-Live : Due to some malfunctioning of routing protocols a datagram may be circulating in the internet, visiting some networks over and over without reaching the destination. This may create extra traffic in the internet. The time-to-live (TTL) field is used to control the maximum number of hops (routers) visited by the datagram. When a source host sends the datagram, it stores a number in this field. This value is approximately two times the maximum number of routers between any two hosts. Each router that processes the datagram decrements this number by 1. If this value, after being decremented, is zero, the router discards the datagram.

(vii) Protocol : Protocol is a 8-bit field which provides multiplexing at the source and demultiplexing at the destination. Protocol fields at the network layer ~~plat~~ the same role as the port numbers at the transport layer. However two port numbers are needed in a transport layer packet because the port numbers at the source and destination are different, but only

One protocol field is required because this value is same for each protocol no matter whether it is located at the source or the destination.

In TCP/IP, the data section of a packet, called the payload, carries the whole packet from another protocol. A datagram 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 or some auxiliary protocols. The internet authority has given any protocol that uses the service 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 protcol number is inserted in this field; when the datagram arrives at the destination, the value of this field helps to define to which protcol the payload should be delivered.

(viii) Header Checksum : IP is not a reliable protocol; it does not check whether the payload carried by a datagram is corrupted during the transmission. IP puts the burden of error checking of the payload on the protocol that owns the payload, such as UDP or TCP. The datagram header, however, is added by IP, and its error checking is the responsibility of IP. Errors in the IP header can be a disaster. For example: if the destination IP address is corrupted the packet can be delivered to the wrong host. If the protcol field is corrupted the payload may be delivered to the wrong protocol. If the fields related to fragmentation are corrupted, the datagram cannot be reassembled at the destination, and so on. For these reasons, IP adds a header checksum field to check the header, but not the payload. Since, the value of some fields, such as TTL, which are related to fragmentation and options, may change from router to router, the checksum needs to be recalculated at each router. Checksum in the internet normally uses a 16-bit field, which is the complement of the sum of other fields calculated using 1's complement arithmetic.

(ix) Source and Destination address : This 32-bit field define the IP address of the source and destination respectively. The source host should know its IP address. The destination IP address is ~~known by~~ either known by the protocol that uses the service of IP or is provided by the DNS. The value of these fields must remain unchanged during the time the IP datagram travels from the ~~host~~ source host to destination host.

(x) Options : A datagram header can have up to 40 bytes of options. Options can be used for network testing and debugging. Although options are not a required part of the IP header, options processing is required of the IP software. This means that all implementions must be able to handle options if they are present in the header.

The existence of options in a header creates some burden on the datagram handling; some options can be changed by routers, which force each router to recalculate the header checksum. There are one-byte and multi-byte options.

(xi) Payload : Payload, or data, is the main reason for creating a datagram. Payload is the packet coming from other protocols that use the service of IP. comparing a datagram to a postal package, payload is the content of the package; the header is only the information written on the package.

Q.7(b):

Explain three phases of remote host and mobile host communication --- (8 marks)

Soln: To communicate with a remote host, a mobile host goes thro' three phases : (i) agent discovery (ii) registration (iii) data transfer.

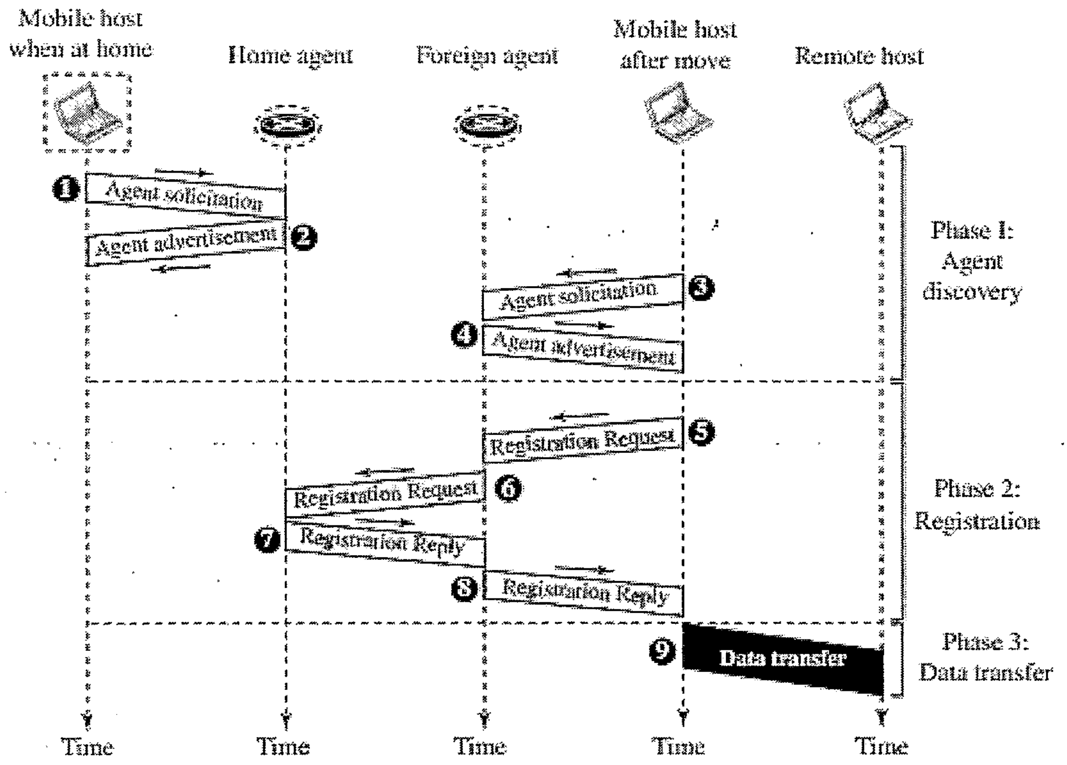


Fig. 7(b) —— (2m)

(i) Agent Discovery : It's the first phase in mobile communication which involves the mobile host the foreign agent and the home agent. Agent discovery consists of two subphases. 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 two types of messages: (a) advertisement and (b) solicitation.

(a) Agent advertisement : When a router advertises its presence on a network using an ICMP router advertisement, it can append an agent advertisement to the packet if it acts as an agent. Mobile IP does not use a new packet type for agent advertisement.

(b) Agent solicitation : Mobile IP does not use a new packet type for agent solicitation; it uses the router solicitation packet of ICMP. —— (2m)

(ii) Registration : Registration is the second phase, also involves the mobile host and the two agents. After a mobile host has moved to a foreign network and discovered the foreign agent, it must register.

There are four 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 its registration, if it has expired
4) The mobile host must cancel its registration (deregistration) when it returns home.

Registration phase consists of two sub phases :
~~(i)~~ Request & reply → ~~and~~ (a) registration request. (b) registration reply

~~(ii)~~ Request & reply : To register with the foreign agent and the home agent, the mobile host uses a registration request and a registration reply.

(a) Registration request : A registration request is sent from the mobile host to the foreign agent to register its care-of address. and also to announce its home address and home agent address. The foreign agent, after receiving and registering the request, relays the message to home agent. Now, the home agent knows the address of the foreign agent because the IP packet that is used for relaying has the IP address of the foreign agent as the source address.

(b) Registration reply : A registration reply is sent from the home agent to the foreign agent and then relayed to the mobile host. The reply confirms or denies the registration request.

A registration request or reply is sent by UDP using the well-known port 434. ——— (2m)

(iii) Data transfer : In data transfer phase all the four, mobile host, remote host, foreign agent and home agent are involved. After agent discovery and registration, a mobile host can communicate with a remote host.
Data transfer involves ~~four~~ stages :

(a) From remote host to home agent : When a remote host wants to send a packet to the mobile host, it uses its address as the source address and the home address of the mobile host as the destination address. The packet, however, is intercepted by the home agent, which ~~(b) From~~ pretends it is the mobile host.

(b) From home agent to foreign agent: After receiving the packet, the home agent sends the packet to the foreign agent, using the tunneling concept. The home agent encapsulates the whole IP packet inside another IP packet using its address as the source and the foreign agent's address as the destination.

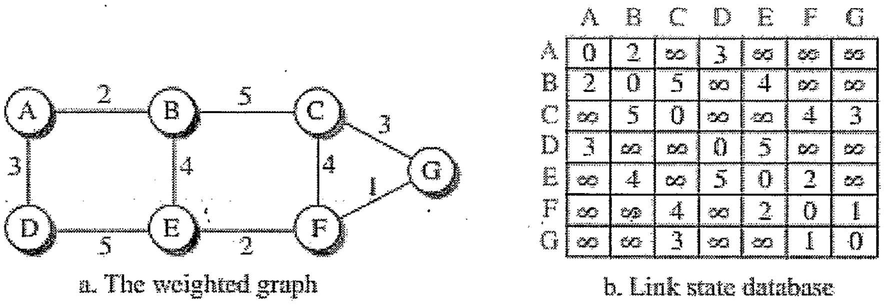
(c) From foreign agent to mobile host: When the foreign agent receives the packet, it removes the original packet. However, since the destination address is the home address of the mobile host, the foreign agent consults a registry table to find the care-of address of the mobile host.

(d) From mobile host to remote host: When a mobile host wants to send a packet to a remote host, it sends as it does normally. The mobile host prepares a packet with its home address as the source, and the address of the remote host as the destination. Although the packet comes from the foreign network, it has the home address of the mobile host.

——— (2 m)

Q.8(a):
Explain least cost using shared link state data base with suitable example --- (10 marks)

Soln: When an internet is modeled as a weighted graph, one of the ways to interpret the best route from the source router to the destination router in suen a way that the total cost for the route is the least cost among all possible routes. A Link-State (LS) routing algorithm is used for creating least-cost trees and forwarding the tables. In LS Routing algorithm the cost associated with an edge defines the state of the link. Links with lower costs are ~~defined~~ preferred over the links with higher costs. If the cost of the link is infinity, it means that the link does not exist or has been broken.



a. The weighted graph

b. Link state database

	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

— (2M)

Fig. 8(a) 1. - Example of LSDB.

LSDB :- Link-State Database - —— (2M)

To create a least-cost tree with LS roting algorithm, 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 Link-State Database (LSDB). There is only one LSDB for entire internet; each node needs to have a duplicate of it to be able to create the least-cost tree. The LSDB can be represented as a two-dimensional arry (matrix) in which the value of each cell defines the cost of the corresponding link.

Each node will update its LSDB by a process called "flooding". Each node can send some greeting messages to all its immediate neighbors to collect two pieces of information for each neighboring node: the identity of the node and the cost of the link. The combination of these two pieces of information is called the LS packet (LSP); the LSP is sent out of each interface, as shown in Fig. 8(a) 2, for Fig. 8(a) 1. 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 node discards the old LSP and 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 that flooding stops somewhere in the network. After receiving all new LSP's, each node creates the comprehensive LSDB

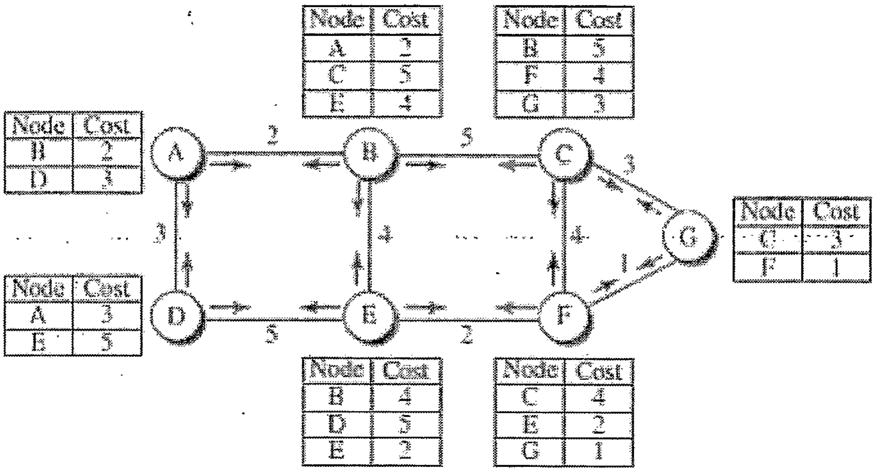


Fig. 8 (a) 2. —— (5m)

as shown in Fig. 8(a)2. This LSDB is same for each node and shows the entire map of the internet. In other words, a node can make the whole map if it needs to, using this LSDB.

To create a least-cost tree for itself, using the shared LSDB, each node needs to run the popular Dijkstra Algorithm. Dijkstra algorithm is an iterative method and uses the following three steps:

1.) The node chooses itself as the root of the tree, creating a tree with a single node, and sets the total cost of each node based on the information in the LSDB.

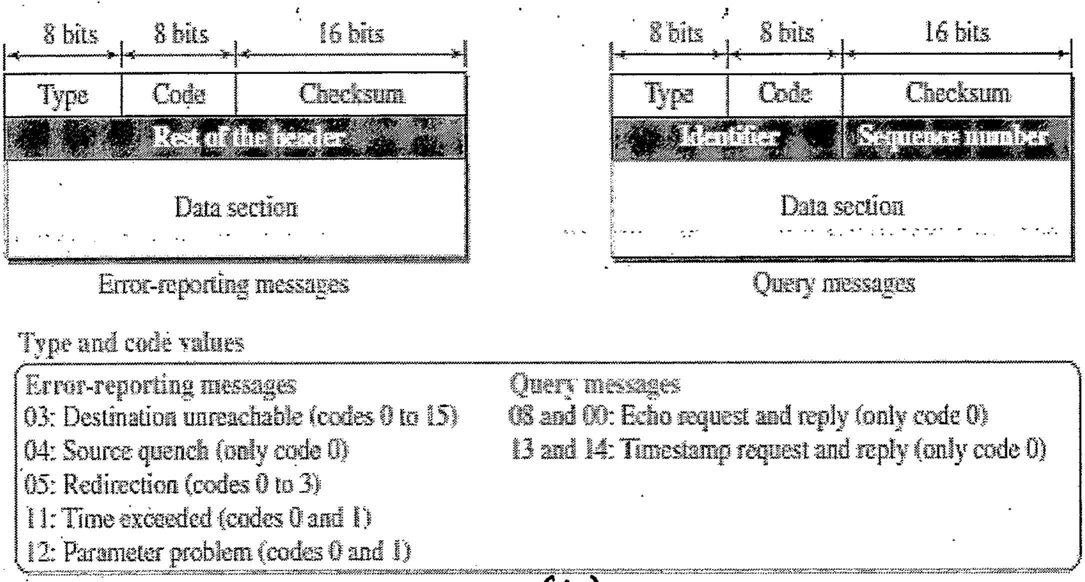
2.) The node selects one node, among all nodes not in the tree, which is closest to the root, and adds this to the tree. After this node is added to the tree, the cost of all other nodes not in the tree needs to be updated because the paths may have been changed.

3.) The node repeats step-2 until all nodes are added to the tree.

—— (3m)

Q.8(b):
With a neat diagram, explain general format of ICMP messages --- (6 marks)

Soln: ICMP messages are divided into two broad categories: (i) Error-reporting messages and (ii) Query messages.



Type and code values

Error-reporting messages
03: Destination unreachable (codes 0 to 15)
04: Source quench (only code 0)
05: Redirection (codes 0 to 3)
11: Time exceeded (codes 0 and 1)
12: Parameter problem (codes 0 and 1)

Query messages
08 and 00: Echo request and reply (only code 0)
13 and 14: Timestamp request and reply (only code 0)

Fig. 8 (b) —— (3m)

The error-reporting messages report problems that a router or a destination host may encounter when it processes an IP packet. The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host. For example, nodes can discover their neighbors. Also, hosts can discover and learn about routers on their network and routers can help a node redirect its messages.

An ICMP message has an 8-byte header and a variable size data section. Although the general format of the header is different for each message type, the first 4 bytes are common to all.

The first field ICMP type, defines the type of the message. The code field specifies the reason for the particular message type. The last common field is the checksum field. The rest of the header is specific for each message type. The data section in error messages carries information for finding the original packet that had the error.

In query messages, the data section carries extra information based on the type of query.

—— (3m)

Module - 5

Q.9(a):
With a neat diagram explain connection establishment, data transfer, and connection termination in TCP --- (10 marks)

Soln: (i) Connection establishment in TCP - — (4m)

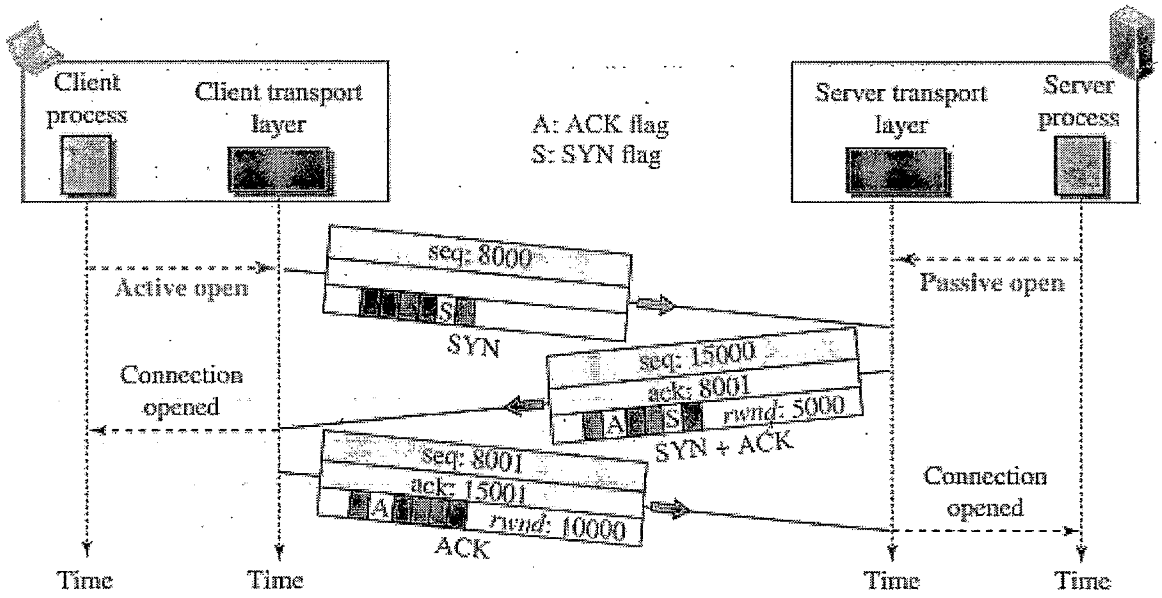


Fig. 9(a) 1.

TCP transmits data in full-duplex mode. When two TCP's in two machines are connected, they are able to send segments to each other simultaneously. This implies that each party must initialize communication and get approval from the other party before any data are transferred.

The connection establishment in TCP is called three-way handshaking, and it consists of three steps:
Let us consider the example of client - server communication as shown in Fig. 9(a) 1.

1) The client send a first segment, a SYN segment, in which only the SYN flag is set. This segment is synchronization of sequence numbers. SYN segment is a control segment which can not carry any data, but it consumes one sequence number, and needs to be acknowledged.

2) The sends the second segment, a SYN + Ack segment with two flag bits set as SYN and ACK. This segment has a dual purpose. First, it is a SYN segment for communication in the other direction. Secondly the Server has to acknowledge the receipt of the SYN segment from the client by setting the Ack flag and displaying the next sequence number it expects to receive from the client. A SYN + Ack segment can not carry data, but it does consume one sequence number.

3) The client sends the third segment, ACK. An ACK segment, if carrying no data, consumes no sequence number.

(ii) Data Transfer: —— (3m)

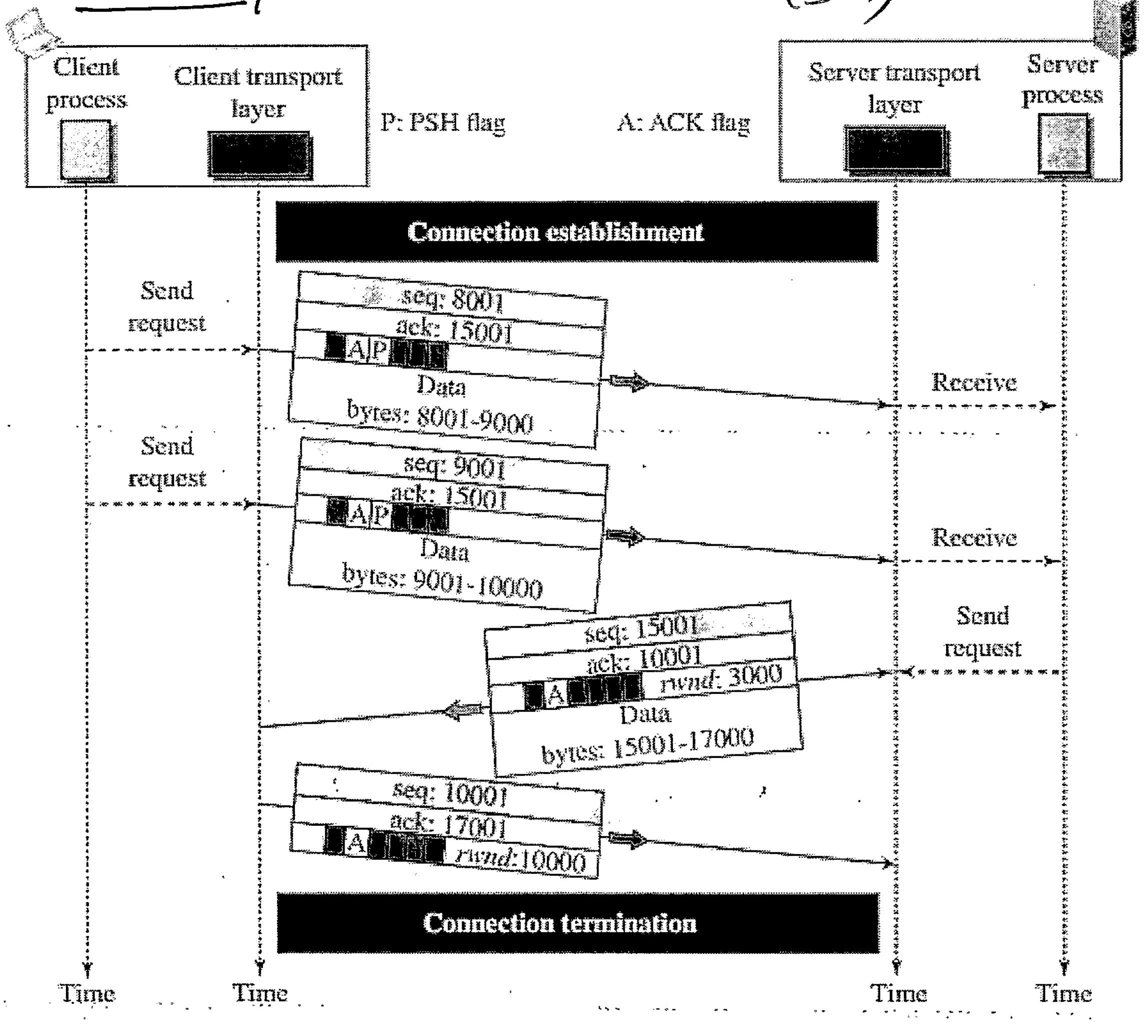


Fig. 9(a) 2.

After connection is established, bidirectional data transfer can take place. The client and server can send data and acknowledgements in both directions. Data traveling in the same direction ~~are~~ as an acknowledgement are carried on the same segment. The acknowledgement is piggybacked with the data.

(iii) Connection Termination: —— (3m)

Either of the two parties involved in exchanging data (client or server) can close the connection although it is initiated by the client. Most implementations today allow two options for connection termination; three way or four-way handshaking with a half-close option.

Connection termination by three-way handshaking -

1) The client TCP, after receiving a close command from the client process, sends the first segment, a FIN segment in which the FIN flag is set.

~~3) The client sends the third segment, ACK. An ACK segment, if carrying no data, consumes no sequence numbers~~

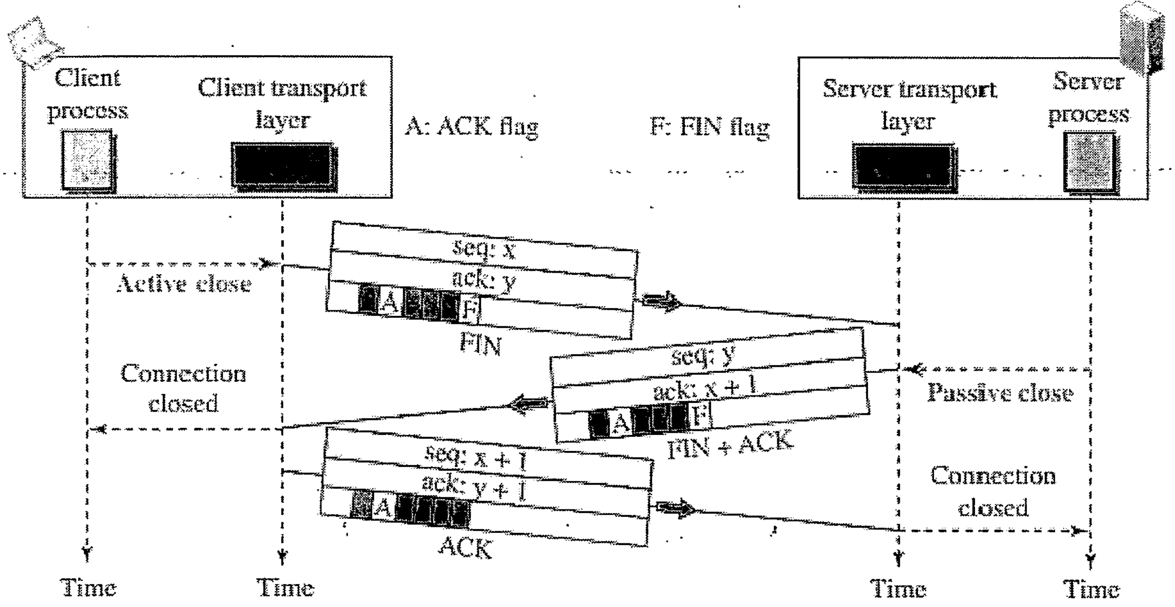


Fig. 9(a) 3.

FIN segment can include a last chunk of data sent by the client or it can be just control segment as shown in Fig. 9(a)3. The FIN segment consumes one sequence number if it does not carry data.

2.) The server TCP, after receiving the FIN segment, informs its process of the situation and sends the second segment, a FIN + ACK segment, to confirm the receipt of the FIN segment from the client & at the same time to announce the closing of the connection in other direction. This segment can also contain the last chunk of data from the server. If it does not carry data, it consumes only one sequence number because it needs to be acknowledged.

3.) The client TCP sends the last segment an ACK segment, to confirm the receipt of the FIN segment from the TCP server. This segment contains the acknowledgement number, which is one plus the sequence number received in the FIN segment from the server. This segment cannot carry data and consumes no sequence numbers.

Q.9(b):

The following is the content of a UDP header in hexadecimal format.

CB84000D001C001C

a. What is the source port number?

b. What is the destination port number?

c. What is the total length of the user datagram?

d. What is the length of the data?

e. Is the packet directed from a client to a server or vice versa? --- (6 marks)

Soln:

(a) The source port number is the first four hexadecimal digits $(CB84)_{16}$, which means that the source port number is 52100.

(b) The destination port number is the second four hexadecimal digits $(000D)_{16}$, which means that the destination port number is 13.

(c) The third four hexadecimal digits $(001c)_{16}$ define the length of the whole UDP packet as 28 bytes

(d) The length of the data is the length of the whole packet minus the length of the header, ie.,

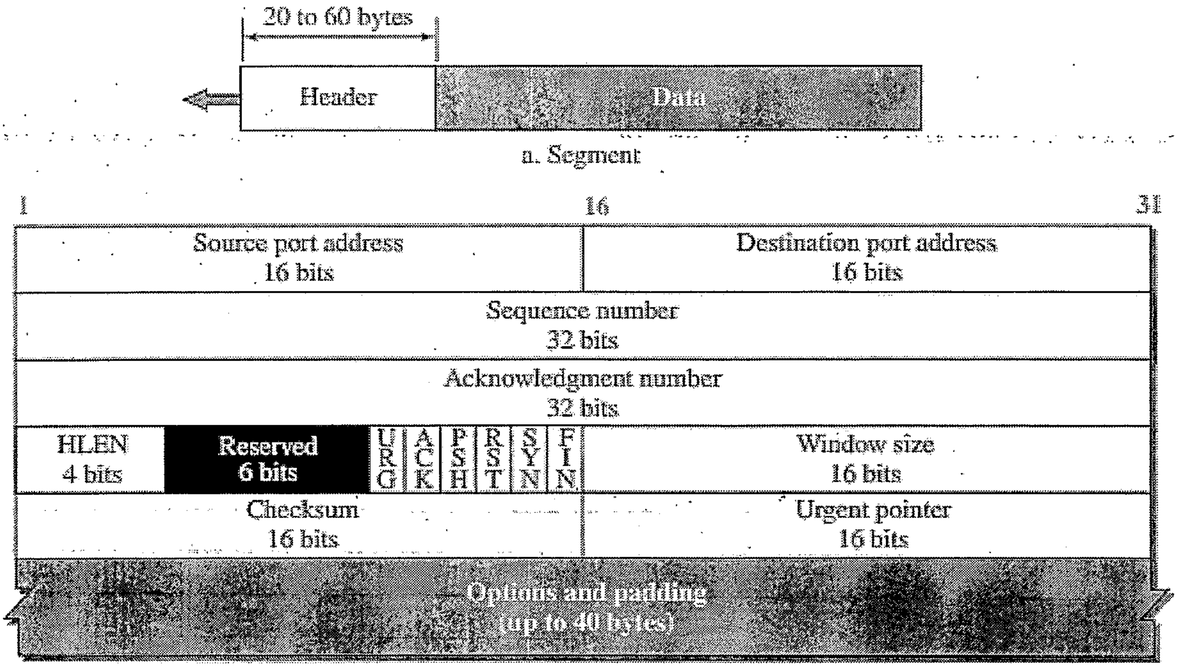
$28 - 8 = 20$ bytes

(e) Since the destination port number is 13 (well known port), the packet is from the client to the server.

Q.10(a):

Briefly explain TCP segment format --- (10 marks)

Soln: **TCP segment format**



a. Segment

b. Header

Fig. 10 (a)

A packet in TCP is called a segment. The segment consists of 20 to 60 bytes, followed by a data from the application program. The header is 20 bytes for no-options and up to 60 bytes if it contains options.

Description of header fields -

1) Source port address - This is a 16-bit field that defines the port number of the application program in the host that is sending the segment.

2) Destination port address - This is a 16-bit field that defines the port number of the application program in the host that is receiving the segment.

3) Sequence number - This 32-bit field defines the number assigned to the first byte of data contained in this segment. Since TCP is a stream ~~bit~~ transport protocol, to ensure connectivity, each byte to be transmitted is numbered. The sequence number tells the destination which byte in this sequence is the first byte in the segment. During connection establishment each party uses a random number generator to create an ISN, which is usually different in each direction.

4.) Acknowledgement number - This 32-bit field defines the byte number that the receiver of the segment is expecting to receive from the other party. If the receiver of the segment has received byte number x from the other party, it returns x+1 as the acknowledgement number. Acknowledgement and data can be piggybacked together.

5.) Header length - This 4-bit field indicates the number of 4-byte words in the TCP header. The length of the header can be between 20 and 60 bytes. Therefore the value of this field is always between 5 (5×4=20) and 15 (15×4=60).

6.) Control - This field defines 6 different control bits or flags as shown below.

URG	ACK	PSH	RST	SYN	FIN

one or more of these bits can be set at a time. These bits enable flow control, connection establishment and termination, connection abortion, and the mode of data transfer in TCP. A brief description of each bit is ~~sho~~ as shown above.

7.) Window size - This field defines the window size of the sending TCP in bytes. The length of this field is 16 ~~bytes~~ bits, which means that the max. size of the window is 65,535 bytes. This value is normally referred to as the receiving window (rwnd) and is determined by the receiver. The sender must obey the dictation of the receiver in this case.

8.) Checksum - This 16-bit field contains the checksum. The calculation of the checksum for TCP is same as that of UDP. But the use of checksum for UDP is optional, whereas for TCP it is mandatory. The same pseudo-header serving the same purpose, is added to the segment. For the TCP pseudoheader, the value for the protocol field is 6.

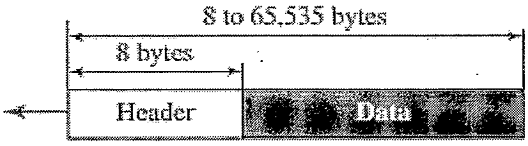
9.) Urgent pointer - This 16-bit field, which is valid only if the urgent flag is set, is used when the segment contains urgent data. It defines a value that must be added to the sequence number to obtain the number of the last urgent byte in the data section of the segment.

10.) Options - There can be up to 40 bytes of optional information in the TCP header.

Q.10(b):

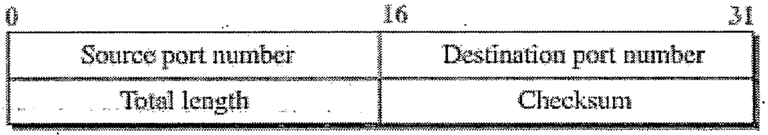
Explain different fields in user datagram packet format with a neat diagram --- (10 marks)

Soln: User datagram packet format -



a. UDP user datagram

—— (2m)



0	16	31
Source port number	Destination port number	
Total length	Checksum	

b. Header format.

—— (2m)

Fig. 10(b).

- The user datagram protocol (UDP) is a connectionless, unreliable protocol.
- UDP packets, called user datagrams, have a fixed size header of 8 bytes made of four fields, each of 2 bytes (16 bits).
- The first two fields define the source and destination port numbers.
- The third field defines the total length of the user datagram, header plus data.
- The 16 bits can define a total length of 0 to 65,535 bytes. However, the total length needs to be less because a UDP user datagram is stored in an IP datagram with the total length of 65,535 bytes.
- The last field can carry the optional checksum.

—— (6m)