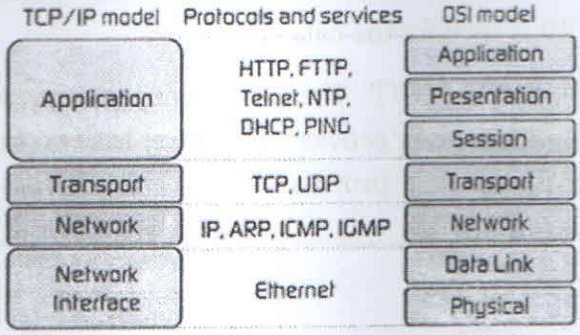
Synoptic - TE - IT - V - Computer Netwo

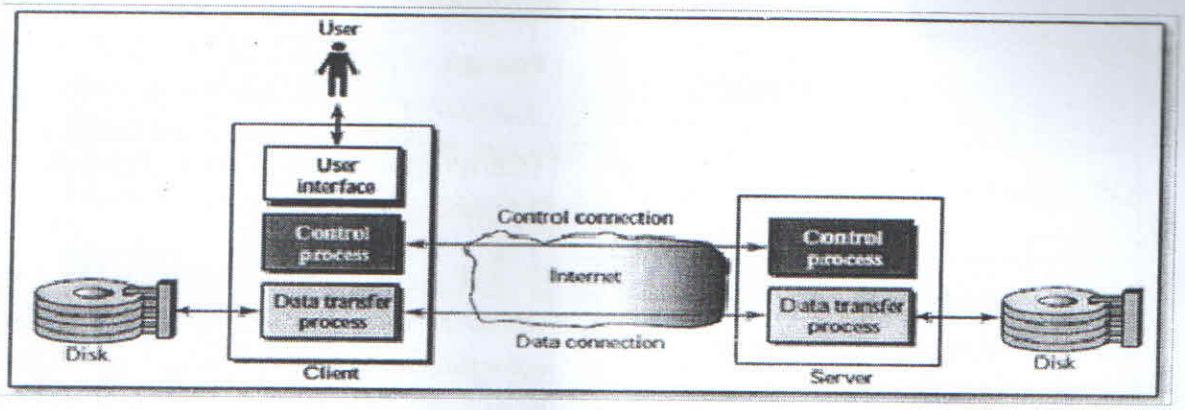
Q1a) Draw OSI and TCP/IP model .Compare and contrast these with respect to the functionality of each layer (Marks 6)



OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
In OSI model the transport layer guarantees the delivery of packets.	In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
OSI model has a separate Presentation layer and Session layer.	TCP/IP does not have a separate Presentation layer or Session layer.
OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	TCP/IP model is, in a way implementation of the OSI model.
Network layer of OSI model provides both connection oriented and connectionless service.	The Network layer in TCP/IP model provides connectionless service.
Protocols are hidden in OSI model and are easily replaced as the technology changes.	In TCP/IP replacing protocol is not easy.
OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
It has 7 layers	It has 4 layers

Q1b)(i)File Transfer Protocol (FTP) is the standard mechanism provided by TCP/IP for copying a file from one host to another.FTP uses two well-known TCP ports: Port 21 is used for the control connection, and port 20 is used for the data connection.

Figure shows the basic model of FTP. The client has three components: user interface, client control process, and the client data transfer process. The server has two components: the server control process and the server data transfer process.



The control connection is made between the control processes. The data connection is made between the data transfer processes.

The control connection remains connected during the entire interactive FTP session.The data connection is opened and then closed for each file transferred. It openseach time commands that involve transferring files are used, and it closes when the fileis transferred.The two FTP connections, control and data, use different strategies and different port numbers.

Control Connection:

The control connection is created in the same way as other application programsdescribed so far. There are two steps:

1. The server issues a passive open on the well-known port 21 and waits for a client.
2. The client uses an ephemeral port and issues an active open.

Data Connection:

The data connection uses the well-known port 20 at the server site.The followingshows how FTP creates a data connection:

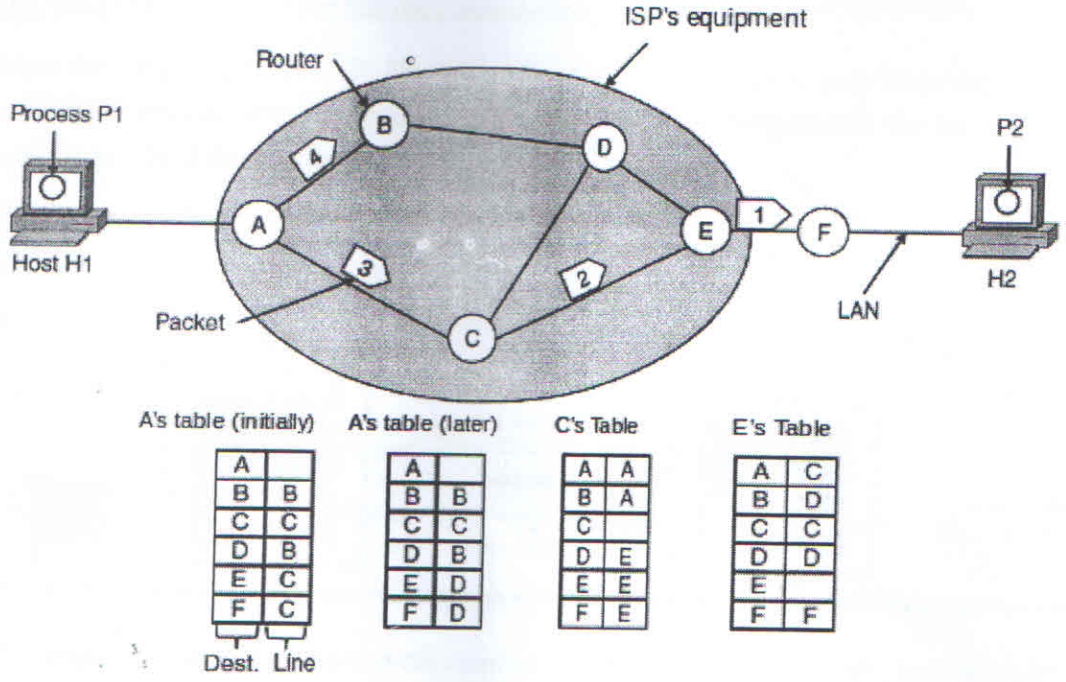
1. The client, not the server, issues a passive open using an ephemeral port. This must bedone by the client because it is the client that issues the commands for transferring files.
2. The client sends this port number to the server using the PORT command.
3. The server receives the port number and issues an active open using the wellknownport 20 and the received ephemeral port number.

Limitations of FTP:

Transferring files with FTP is not secure.

All data is sent in clear text, including usernames and passwords.

Implementation of Connectionless Service



Routing within a datagram network

Q1b) (ii)

-No set up is needed

-Each packet contains information which allows the packet to be individually routed hop-by-hop through the network .

- packet may arrive at destination out of order.

Q 1b)(iii) Optical Fibers - basics

• a very thin glass rod (cylindrical dielectric waveguide made of SiO 2)

•Operate at optical frequency about 10 14 Hz

•Compose of a core, cladding and jacket (a plastic sheathing for mechanical protection)

•Light injected into the core of a glass fiber will follow the physical path of the fiber due to the internal reflection of the light between the core and the cladding

•Fibers are classified by the way in which the light travels in them and is closely related to the diameter of the core and cladding

Optical Fibers – Single Mode step-index

•Optical Fibers types– Single Mode step-index ,multi mode step-index .

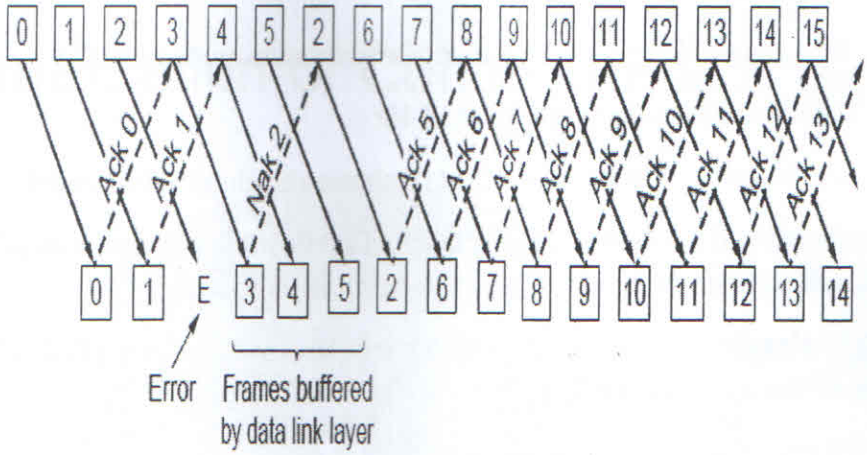
• single-mode fiber has small core for light coupling

- In multi mode step-index multiple beams from a light source move through the core in different paths.

Advantages :

- Secure transmission.
- Very high transmission capacity,High bandwidth
- Small size, light weight, flexible, easy installation
- immunity to interference: not effected by electrical magnetic interference (EMI) or radio frequency (RFI)
- Free of cross talk between fibers
- Insulation & Hazardous environment resistant: optical fiber is an insulator, provide total electrical isolation for many applications. It eliminates inference caused by ground loop and electrical discharge
- Security: signals cannot be tapped easily
- Stress and heat resistant & reliability and maintenance: constant medium, not subject to fading, adverse temperature, moisture and can be used for underwater cable, long service life span, not affected by short circuit, power surges or static electricity
- Versatility: available for most of data, voice and video communication formats
- Scalable: easily expanded. Only change electronics, no change on fibers
- Low cost, low loss and signal regen ration: optical fibers can travel over 70km before repeating the signals, save cost for repeater and maintenance

Q 2a) Selective repeat protocol



(b)

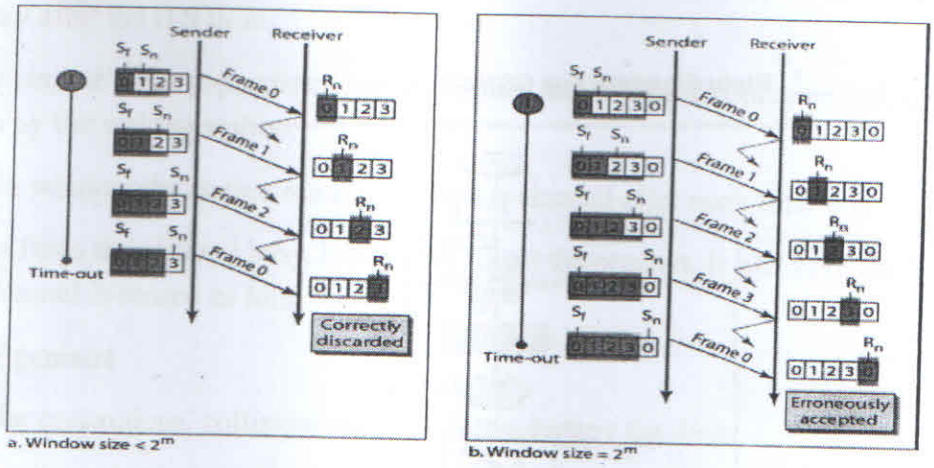
gh the system in
can not guarante
rrieh

less service

Ans: Divide (Mod-2) 001110110010000 by 10101 to get 4-bit code word: **1101.**
Details of the steps is given below

```
001110110010000
  10101
-----------
   10001
   10101
 ----------
    10000
    10101
   ----------
     10110
     10101
    ----------
       11000
       10101
      ----------
            1101
```

Q 2b)

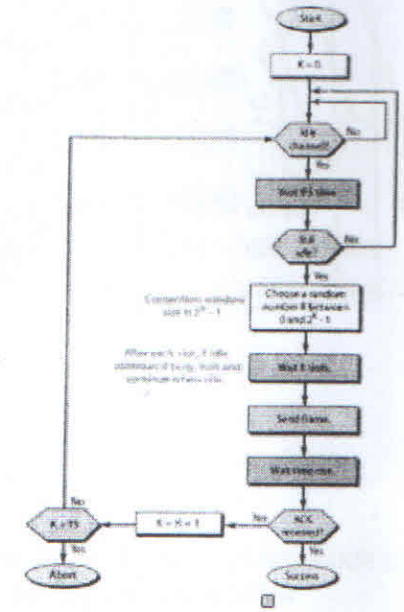


a. Window size < 2^m

b. Window size = 2^m

Q 3a)

Flow diagram for CSMA/CA



CSMA/CA avoids the collisions using three basic techniques.

(i) Interframe space

(ii) Contention window

(iii) Acknowledgements

1.Interframe space

Whenever the channel is found idle, the station does not transmit immediately. It waits for a period of time called interframe space (IFS).

• When channel is sensed to be idle, it may be possible that same distant station may have already started transmitting and the signal of that distant station has not yet reached other stations.

• Therefore the purpose of IFS time is to allow this transmitted signal to reach other stations.

• If after this IFS time, the channel is still idle, the station can send, but it still needs to wait a time equal to contention time.

• IFS variable can also be used to define the priority of a station or a frame.

2. Contention Window

• Contention window 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 back-off strategy. It means that it is set of 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-persistent method except that a random outcome defines the number of slots taken by the waiting station.

• In contention window the station needs to sense the channel after each time slot.

• 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.

3. Acknowledgement

• Despite all the precautions, collisions may occur and destroy the data.

• The positive acknowledgment and the time-out timer can help guarantee that receiver has received the frame.

This is the CSMA protocol with collision avoidance.

• The station ready to transmit, senses the line by using one of the persistent strategies.

• As soon as it find the line to be idle, the station waits for an IFG (Interframe gap) amount of time.

• If then waits for some random time and sends the frame.

• After sending the frame, it sets a timer and waits for the acknowledgement from the receiver.

• If the acknowledgement is received before expiry of the timer, then the transmission is successful.

• But if the transmitting station does not receive the expected acknowledgement before the timer expiry then it increments the back off parameter, waits for the back off time and resenses the line.

Q3b) **channelization protocols – FDMA,TDMA ,CDMA**

CDMA (Code Division Multiple Access)

exploits spread spectrum (DS or FH) encodingscheme

unique "code" assigned to each user; ie, code set partitioning

Used mostly in wireless broadcast channels (cellular,satellite,etc)

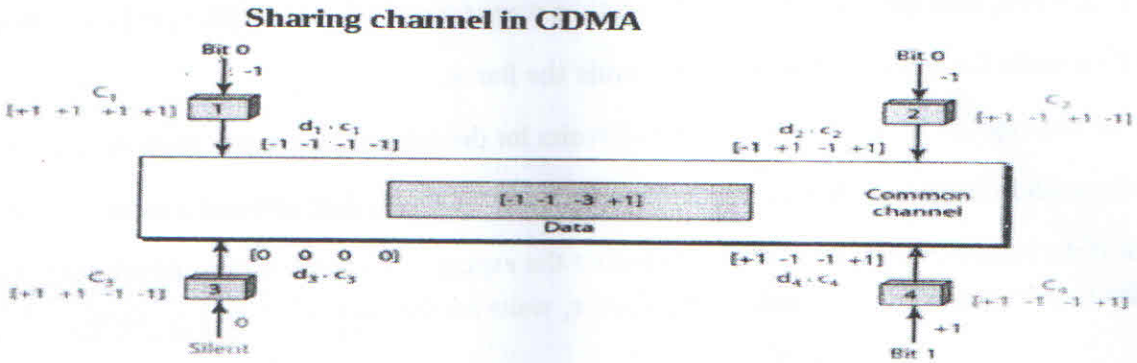
All users share the same frequency, but each user has own"chipping" sequence(ie, code)

Chipping sequence like a mask: used to encode the signal

encoded signal = (original signal) X (chipping sequence)

decoding : innerproduct of encoded signal and chippingsequence (note, the innerproduct is the sum of the component-by-component products)

To make CDMA work, chipping sequences must be chosen orthogonal to each other (i.e., innerproduct = 0)



In random access methods, there is no access control (as there is in controlled access methods) and there is no predefined channel (as in channelization). Each station can transmit when it desires. This liberty may create collision.

Q 4a) Each router must do the following:

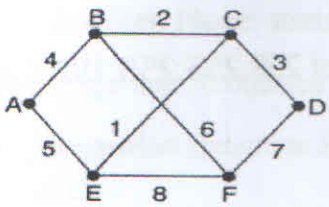
Discover its neighbors, learn their network address.

Measure the delay or cost to each of its neighbors.

Construct a packet telling all it has just learned.

Send this packet to all other routers.

Compute the shortest path to every other router.



(a)

Link State Packets

A		B		C		D		E		F	
Seq.		Seq.		Seq.		Seq.		Seq.		Seq.	
Age		Age		Age		Age		Age		Age	
B	4	A	4	B	2	C	3	A	5	B	6
E	5	C	2	D	3	F	7	C	1	D	7
		F	6	E	1			F	8	E	8

(b)

(a) A subnet. (b) The link state packets for this subnet.

Strengths

- Loop free as long as LS database's are consistent
  - Can have transient routing loops – shouldn't last long
- Messages are small
- Converges quickly
- Guaranteed to converge
-

Weaknesses

- Must flood data across entire network (scalability?)
- Must maintain state for entire topology (database)t and the corresponding

4b)

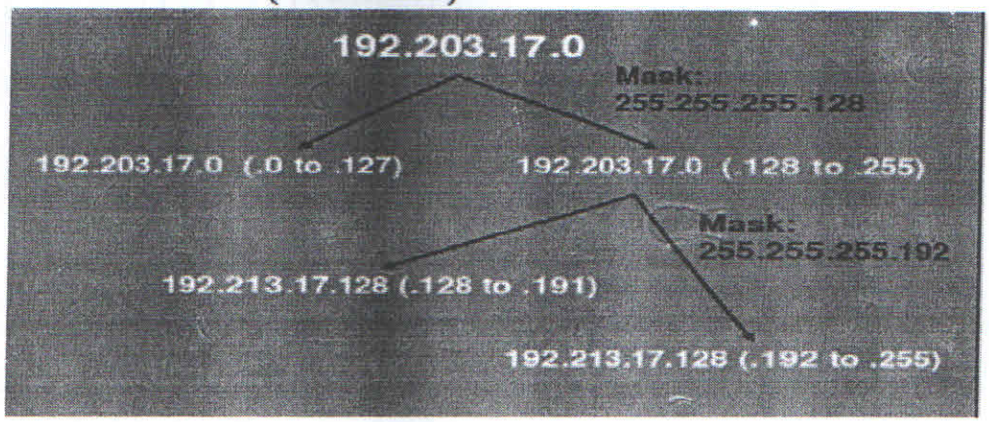
Basic concept:(Variable length subnet mask VLSM)

Use the mask 255.255.255.128 to divide the network address into two subnets with 128 hosts each.

- 192.203.17.0 (.0 to .127)
- 192.203.17.0 (.128 to .255)

Next subnet the second .128 subnet using a mask of 255.255.255.192. Creates two subnets, 64 hosts each

- 192.213.17.128 (.128 to .191)
- 192.213.17.128 (.192 to .255)



Q 5a)TCP uses a congestion window and a congestion policy that avoid congestion. If the network cannot deliver the data as fast as it is created by the sender, it must tell the sender to slow down. In other words, in addition to the receiver, the network is a second entity that determines the size of the sender's window.

Congestion policy in TCP –

1. Slow Start Phase: starts slowly increment is exponential to threshold
2. Congestion Avoidance Phase: After reaching the threshold increment is by 1
3. Congestion Detection Phase: Sender goes back to Slow start phase or Congestion avoidance phase.

Slow Start Phase : exponential increment – In this phase after every RTT the congestion window size increments exponentially.

Initially cwnd = 1 After 1 RTT, cwnd = 2^(1) = 2

2 RTT, cwnd = 2^(2) = 4

3 RTT, cwnd = 2^(3) = 8

Congestion Avoidance Phase : additive increment – This phase starts after the threshold value also denoted as *ssthresh*. The size of *cwnd*(congestion window) increases additive. After each RTT cwnd = cwnd + 1.

Initially cwnd = i After 1 RTT, cwnd = i+1

2 RTT, cwnd = i+2

3 RTT, cwnd = i+3

Congestion Detection Phase : multiplicative decrement – If congestion occurs, the congestion window size is decreased. The only way a sender can guess that congestion has occurred is the need to retransmit a segment. Retransmission is needed to recover a missing packet which is assumed to have been dropped by a router due to congestion. Retransmission can occur in one of two cases: when the RTO timer times out or when three duplicate ACKs are received.

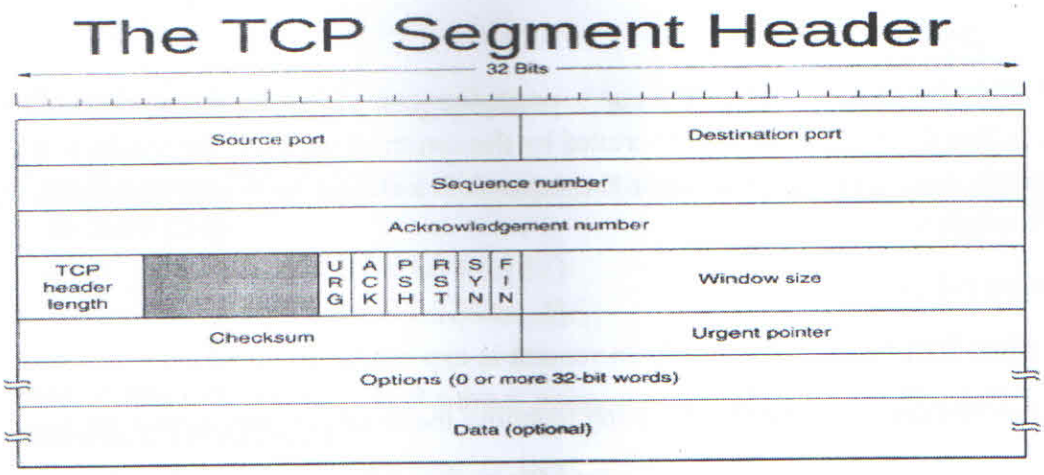
- **Case 1 : Retransmission due to Timeout** – In this case congestion possibility is high.

  (a) ssthresh is reduced to half of the current window size.
  (b) set cwnd = 1
  (c) start with slow start phase again.

- **Case 2 : Retransmission due to 3 Acknowledgement Duplicates** – In this case congestion possibility is less.

  (a) ssthresh value reduces to half of the current window size.
  (b) set cwnd= ssthresh
  (c) start with congestion avoidance phase

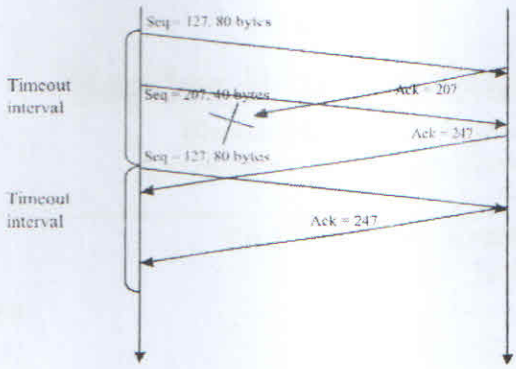
Q5a)



The following is a dump of a TCP header in hexadecimal format.
05320017 00000001 00000000 500207FF 00000000

source port is 2 bytes take 05 32 = 1330
next 2 bytes as destination address 00 17 == 23 (default TCP port)
next 4 bytes as sequence number 00 00 00 01 ==1
next 4 bytes as ack 00 00 00 00 == 0
next 4 bits as HLEN 5 ==5 -- this indicates number of sets of 4 bytes which makes the header lenght = 20bytes..
next 6 bits are reserved i.e.0 =0000and 2 bits from hex 0
next 6 bits are control bits = remaining 2 bits from hex 0 and 4 bits of 2
next 2 bytes indicate the window length 07 FF == 2047 bytes
Checksum 2 bytes 00 00 = 0
Urgent pointer 2bytes 00 00 =0

Q 5b)


Seq = 127, 80 bytes
Timeout interval
Seq = 207, 40 bytes
Ack = 207
Ack = 247
Seq = 127, 80 bytes
Timeout interval
Ack = 247