Bangladesh University of Business & Technology (BUBT)

Name: MD Faysal Hasan

ID: 17181203063

program: B.Sc. in CSE, 28th intake section: 02

shift: Evening

Course Code: CSE 319

Course title: Computer networks

Ans to the question :- 1 (a)

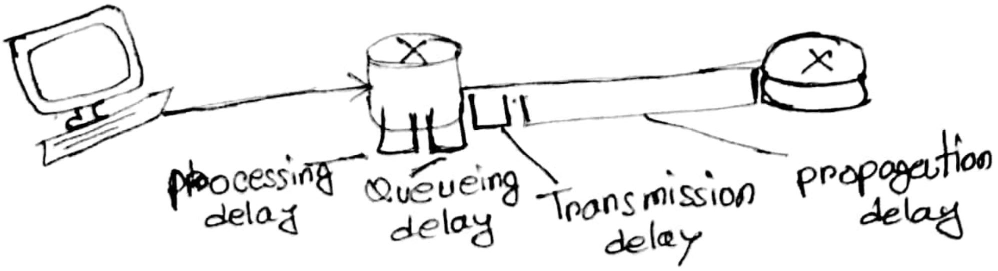
Ans: Packet switching is a connectionless network switching technique. Here, the message is divided and grouped into a number of units called packets that are individually routed from the source to the destination.

Most packet switches use store-and-forward transmission at the inputs to the link. Store-and-forward transmission means that the packet switch must receive the entire packet before it can begin to transmit the first bit of the packet onto the outbound link. So when the ~~packet~~ source send the packet through router. Router can not send to destination until all the bits it has received. Each packet switch has an output buffer, which stores packets that the router is about to sent into that link. If the links busy with the transmission of another packet the packet must wait in the output buffer. An arriving packet may find that the buffer is completely full with other packet. In this case, packet loss will occur.

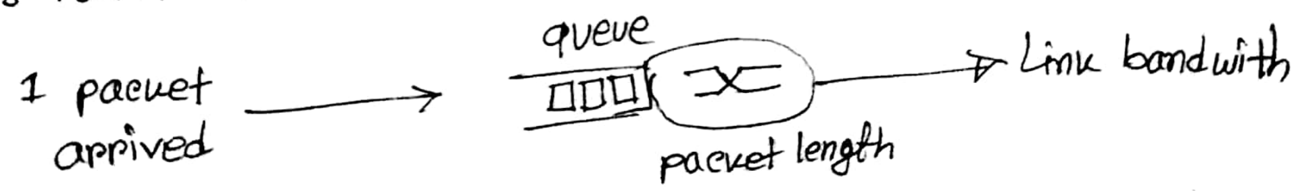
A packet travels from one node to the subsequence node along this path, the packet suffer from several types of delay. at each node along the path. The most important of these delay are:-

1. Processing delay :- processing delay is the time it takes routers to process the packet header. The processing delay can also include other factor, such as the time needed to check for bit level error in the packet that occured in transmitting the packet's bits from the upstrem node.

~~2. Queu~~



2. Queuing delay: Queuing delay is the time a job waits in a queue until it can be executed. It depends on congestion. It is the time difference between when the packet arrived destination and when the packet data processed or executed.



3. Transmission delay: Time taken to put a packet onto link. In other words, it is simply time required to put data bits on the wire/communication medium. It depends on length of packet and bandwidth of network

Transmission delay = Data size / bandwidth.

4. Propagation delay:- Time taken by the first bit to travel from sender to receiver end of the link. In other words, it is simply the time required for bits to reach the destination from the start point.

Propagation delay = distance / transmission

To get a hands-on fell for end-to-end delay in a computer network, we can make use of the tracerouter program. Tracerouter is a simple program that can run in any internet host, when the user specifies a destination hostname, the source sends multiple packet's toward that destination. When a router received one of these packet's, it sends back to the source a short message that contain the name and address of the router.

Ans to the question :- 01(b)

The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information system.

The client and server communicate for an extended period of time, with the client making a series of request and server responding to each of the request. In the formar approch the application is said to use non-persistent connection and in the letter approch persistent connection.

Non-Persistent connection :- ~~Each~~

* Each request/response pair be sent over a separate TCP connection.

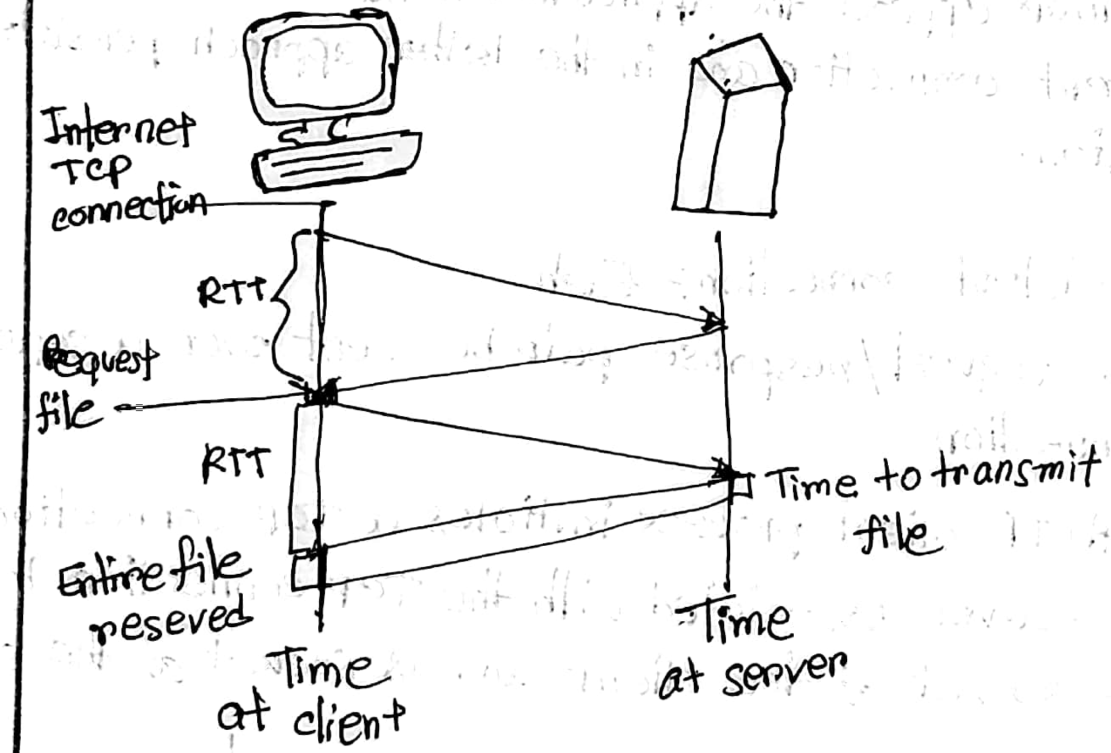
* The HTTP client process initiates a TCP connection to the server Associated with the TCP connection, there will be socket at the client and a socket at the server.

* The HTTP client sends an HTTP request message to the server via its socket.

* The HTTP server process receives the request message via its socket, retrieves the object, encapsulates the object in an HTTP pespones message, and sends the response message to the client via its socket.

* The HTTP server process tells TCP to close the TCP connection.

* The HTTP client receives the response message. The TCP connection terminates. The message indicates that the enclapsulated object is an HTML file



* All the parts of an http request message is Request line, Header lines, Blank line and Entity body

Request line: The request line has three field: The method field, the URL field, and the HTTP version field. The method field taues several different values including GET, POST, HEAD, PUD and DELETE.

Header line: The header line Host Specifies the host on which the object resides.

Connection: It wants the server to close the connection after sending the request object.

User-agent: header line specifies the user agent, that is, the browser type that is making the request to the server.

Example:-

GET/somedir/page.html
Host: www.someschool.edu
Connection: close
User-agent: Mozilla/5.0
Accept-language: En

Ans to the question 2(a)

Ans:- Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice versa.

⊞ Principal of Cryptography

* Cryptographic techniques allow a sender to disguise data so that an intruder can gain no information from the intercepted data.

* The receiver, of course, must be able to recover the original data from the disguised data.

* If a user wants to send a message to another user. then message in its original form is know as plaintext.

* User encryption his plaintext message using an encryption algorithm so that the encrypted message know as ciphertext.

* User provide a key, K_A a string of number as input to the encryption algorithm

* The encryption algorithm takes the key and the plaintext as input and produce ciphertext as output

* The notation $K_A(m)$ refers to the ciphertext from of the plaintext message, m.

* ~~Bob~~ receives an encrypted message $KA(m)$; he decrypts it by computing $K_B(K_A(m)) = m$

Polyalphabetic encryption

Given, pattern, C1C2C3C2C1C3C2

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
$C_1=9$	J	K	L	m	n	o	p	q	r	S	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
$C_2=5$	f	g	h	i	J	K	L	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
$C_3=12$	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	K	L

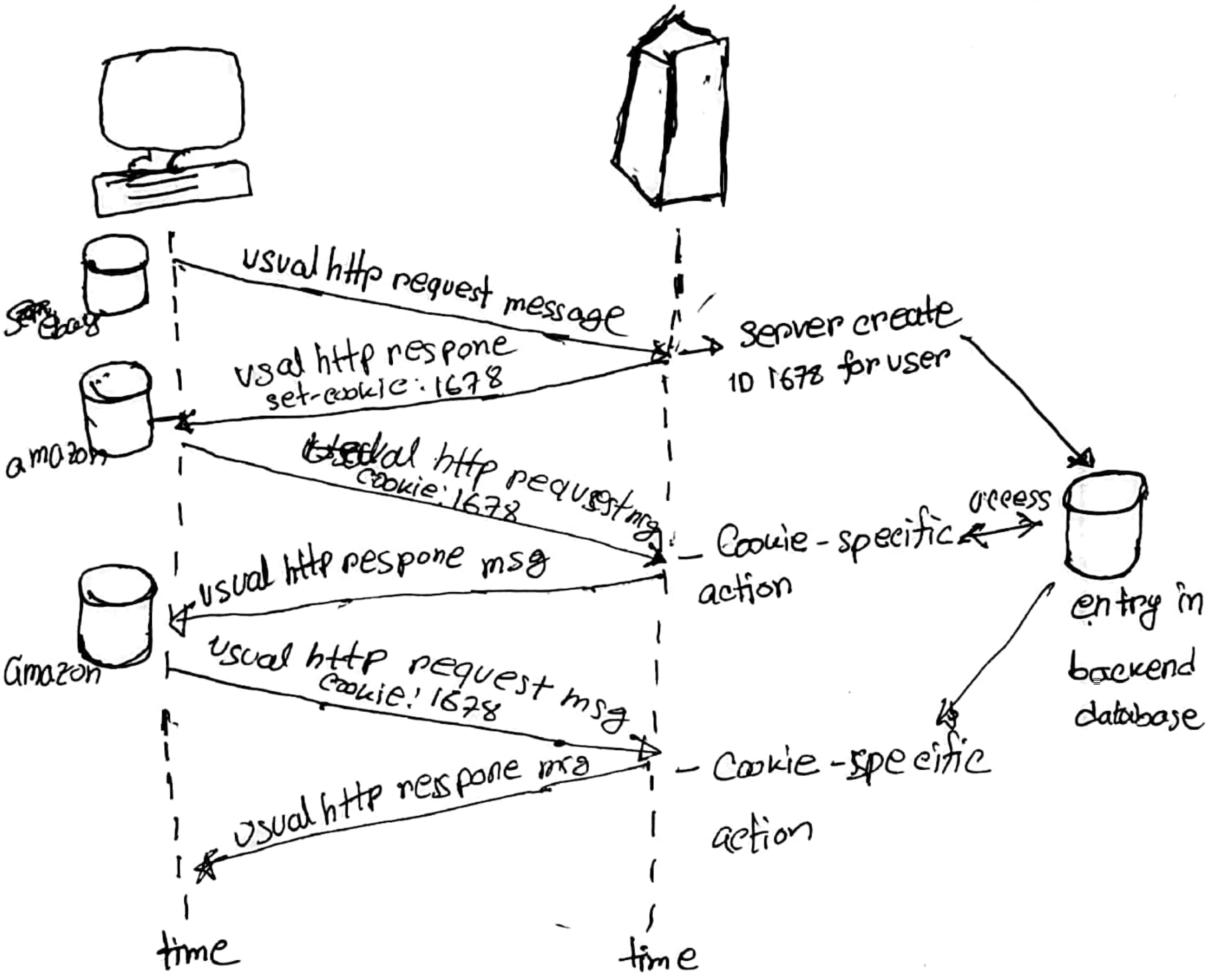
pattern: C1 C2 C3 C2 C1 C3 C2 C1 C2 C3 C2 C1 C3 C2 C1 C2 C3 C2 C1 C3C2 C1 C2 C3 C2 C1 C3 C2

Plaintext: Social or Physial Distancing
ciphertext: Btonjx ta Utdbufu Iuxcms lnze

Ans to the question :-02(b)

Ans :- In the Back-end database the server sensitive information be stored. web server that can handle thousend of simulaneous TCP connection, when a User try to browse a wbsit through a browser, when the request come into the web server the server create a unique identification number and create an entry in its backend database that is indexed by the identification number. The web server than responds to user's browser, including in th HTTP respon a Set-cookie: header, which contain the identification number.

* User state of cookies

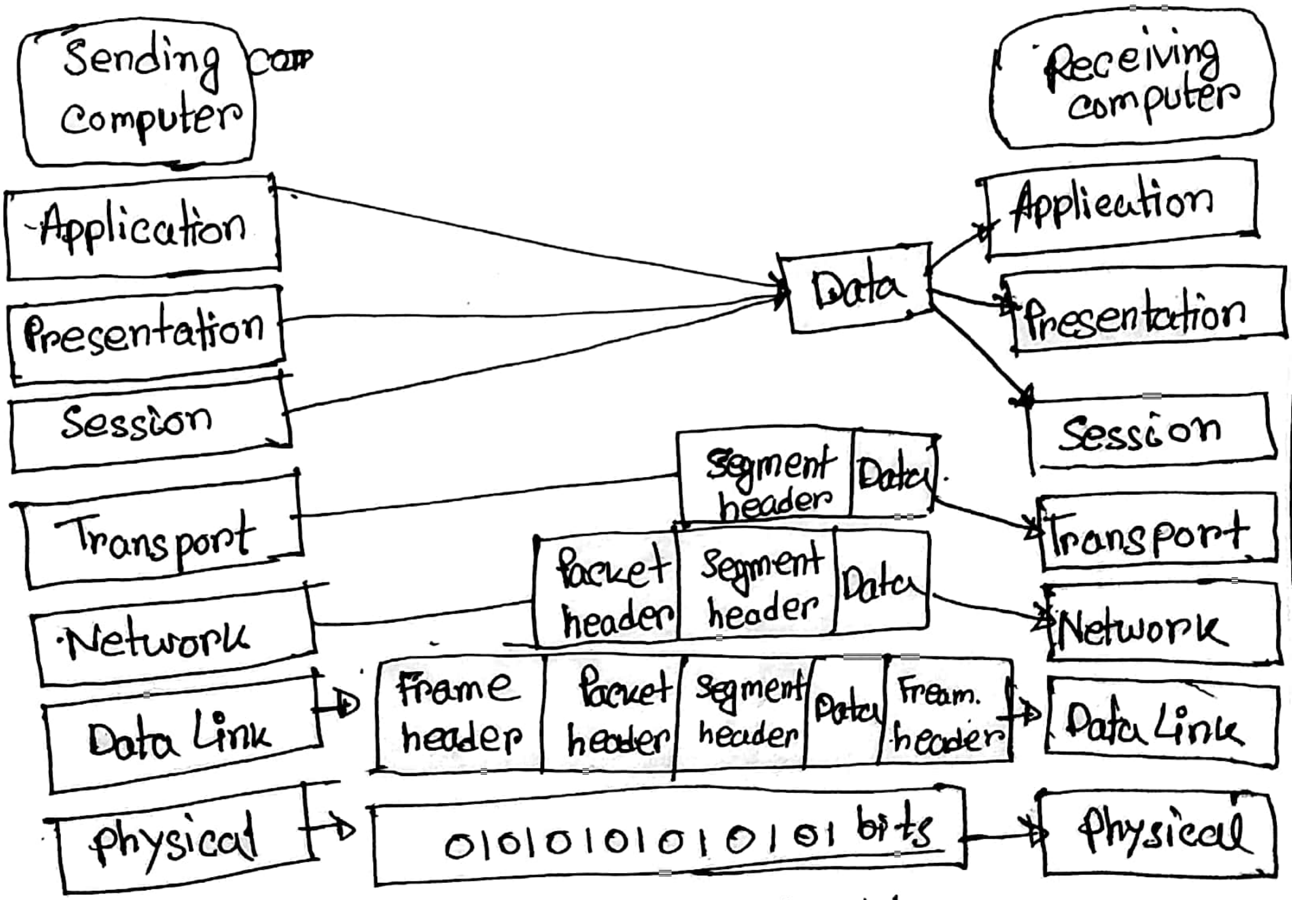

ebay
usual http request message
server create ID 1678 for user
usual http respone set-cookie: 1678
amazon
usual http request msg cookie: 1678
Cookie - specific action
access
entry in backend database
usual http respone msg
amazon
usual http request msg cookie: 1678
Cookie - specific action
usual http respone msg
time
time

Although cookies often simplify the internet shopping experience for the user, they ~~are~~ are controversial because they can alsobe considered as an invasion privacy. A website can learn a lot of cookie and user-supplied account information to a third party

Ans to the question 3(a)

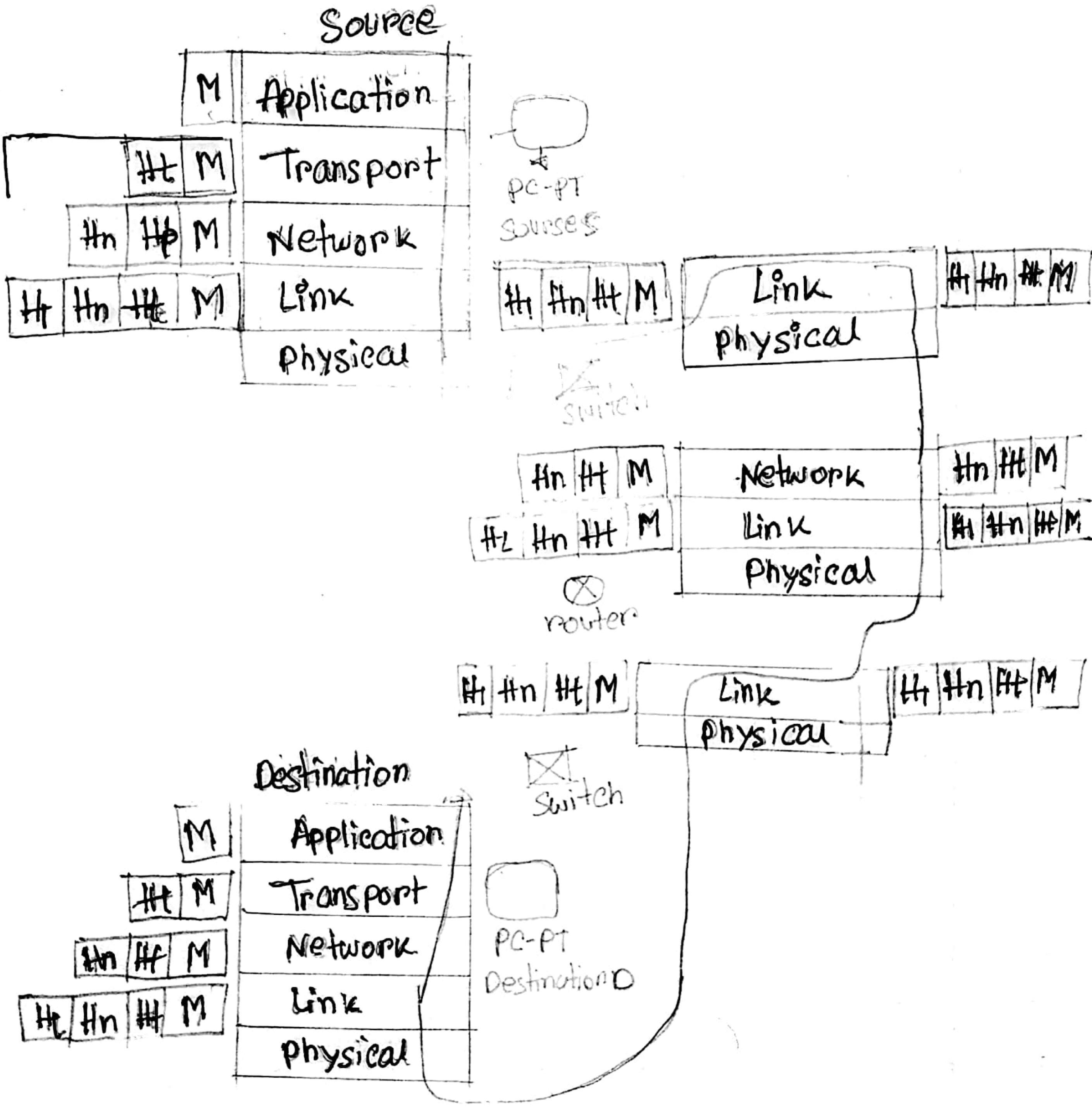
In networking model, the terms encapsulation and de-encapsulation refer to a process in which protocol information is added to the data and removed from the data when it passes through the layers.

Data Encapsulation and De-encapsulation work:- Protocol information can be added and after the data. If information is added before the data, it is known as header, If information added after the data, it is know as trailer.



encapsulation and de-encapsulation in TCP/model

* The step of the encapsulation and de-encapsulation process of a message M send from a sender S to a destination D on the internet



Ans to the question 3(b)

Ans: IP address is an address having information about how to reach a specific host, espically outside the LAN. An IP address is a 32 bit unique address having an address space of 2^{32};

IP address belonging to the class A are assigned ~~to~~ the network that contain a large number of hosts

- The network ID is 8 bit long
- The host ID is 24 bit long

Aclass A subnet has 24 bit worth of addressing which is enough for almost 17 million individual devices. Most entities have only small fraction of this number of devices, so most of the address are not used.

Given. The IP address = 205.16.37.39/28

The number of address in the block is = $2^{32-28} = 16$

The first address in this block :

The first address can be found by ANDing the given address wit the mask

dotted- do decimal : 205.16.37.39/28

dotted- binary : 11001101 00010000 00100101 00100111

Mask : 1111 1111 11111111 11111111 00100000

First Ads : 11001101 00010000 00100101 001.00000

or ; 205.16.37.32

. The last address in this block :

The last address can be found by ORing the given address

Address : 11001101 00010000 00100101 00100111

Mask complement : 00000000 00000000 00000000 00001111

last Address : 11001101 00010000 00100101 00101111

or : 205.16.37.47