CBCS SCHEME

USN | | | | | | | | | | |

18EC71

Seventh Semester B.E. Degree Examination, Feb./Mar. 2022
Computer Networks

Time: 3 hrs. Max. Marks: 100

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

Module-1

1 a. Describe significant services of all layers in TCP/IP protocol suite along with the encapsulation and decapsulation processes with necessary figures. **(16 Marks)**

b. List different performance criteria of a network. **(04 Marks)**

OR

2 a. Explain different physical structures and networks topologies with the help of diagrams. **(16 Marks)**

b. Distinguish TCP/IP model with OSI model. **(04 Marks)**

Module-2

3 a. Describe various fields in the format of an ARP packet and explain how ARP sends request and response messages. **(12 Marks)**

b. Write short notes on implementation of standard Ethernet topologies. **(08 Marks)**

OR

4 a. Describe the concept of bit stuffing and byte stuffing. **(10 Marks)**

b. Explain CSMA/CD working with the help of flowchart. **(06 Marks)**

c. List the characteristics of wireless LANs. **(04 Marks)**

Module-3

5 a. Explain working of DHCP [Dynamic Host Configuration Protocol]. **(08 Marks)**

b. Inspect the following MAC addresses and categories them as unicast, multicast and broadcast.

i) 4A : 30 : 10 : 21 : 10 : 1A
ii) 47 : 20 : 1B : 2E : 08 : EE
iii) EF : FF : 10 : 01 : 11 : 00
iv) FF : FF : FF : FF : FF: FF **(04 Marks)**

c. Explain IPV4 datagram format with a neat diagram. **(08 Marks)**

OR

6 a. Explain a simple implementation of Networks Address Translation (NAT). **(10 Marks)**

b. Explain distance vector routing algorithm using Bellman ford equations. **(10 Marks)**

Module-4

7 a. Describe connectionless and connection – oriented services provided by the transport layer. **(14 Marks)**

b. Describe the general services provided by UDP. **(06 Marks)**

OR

8 a. Explain working of Go-back-N protocol. **(10 Marks)**

b. Describe sending and receiving buffers in TCP, and explain how segments are created form the bytes in the buffers. **(10 Marks)**

Module-5

9 a. Explain the architecture and format of electronic mail. **(10 Marks)**

b. Distinguish Local Logging and Remote Logging. **(10 Marks)**

OR

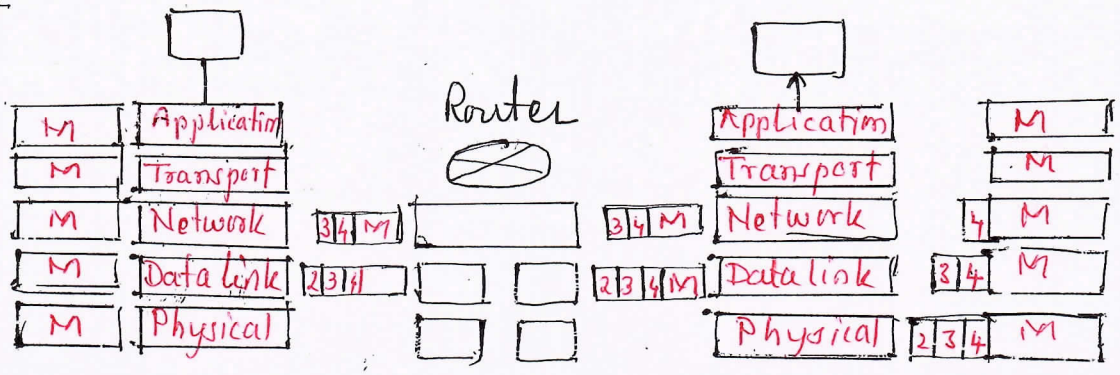
10 a. Explain persistent and non-persistent connections in HTTP. **(10 Marks)**

b. Write a short note on DNS recursive and iterative resolutions. **(10 Marks)**

* * * * *

MARK

1). a.) 16



Legend : [4] Header at transport layer ↓ Encapsulate.
[3] " " Network layer ↑ Decapsulate.
[2] " " Data-Link layer
M — Message.

Fig (1)

5

Above figure shows Encapsulation/Decapsulation concept for small internet

* Encapsulation at the Source Host
  * At the source we have only encapsulation
1. * At the application layer, the data to be exchanged as is referred to as a message
   * Message doesnot contain any header or trailer, but - if it does, we refer to the whole as the message.
   * The message is passed to transport layer.
2. * The transport layer takes the message as payload, the load that the transport layer should take - care of
   * It adds the transport layer header to the payload, which contains the identifiers of the source and - destination application programs that want to communicate plus some more information that is needed for the end-to-end delivery of the message.
   * The result is transport layer packet, which is called the segment (in TCP) and the user-datagram in (UDP)
   * The transport layer then passes the packet to the network layer.

5

3. * The network layer takes the transport-layer packet

as data or payload and adds its own header to the payload

* The header contains the addresses of the source and destination host and some more information is used for error checking of the header, fragmentation, and so on
* Result is network-layer packet called a datagram

4e. * The data link layer takes the network-layer packet as data or payload and adds its own header which contains the link-layer addresses of the host or the next hop.
* The result is link-layer packet which is called a frame. The frame is passed to the physical layer for transmission.

* Decapsulation and Encapsulation at the Router
* Router is connected to two or more links
* At router both decapsulation and encapsulation process is done.

1. After set of bits delivered to the data-link layer, this layer decapsulates the datagram from the frame and passes it to the network layer
2. * The network layer only inspects the source and destination addresses in the datagram header and consults its forwarding table to find the next hop
* The contents of the datagram should not be changed by the network layer unless there is need to fragment the datagram.
* The datagram is then passed to the data-link layer of the next link.
3. The data-link layer of the next link encapsulates the datagram in a frame and passes it to the physical layer for transmission.

Marks

* Decapsulation at the Destination Host
  * At destination host, each layer only decapsulates the packet received, removes the payload, and delivers the payload to the next-higher layer protocol until the message reaches the application layer. 2
  * Decapsulation is the last includes error checking.

1.6) Performance criteria of a network 04

* Performance can be measured in many ways, including transit time and response time.

Transit time is the amount of time required for a message to travel from one device to another. 1

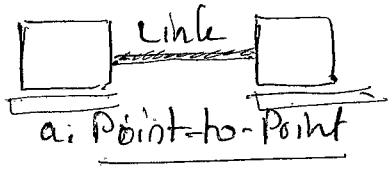
Response time is the elapsed time between an inquiry and a response

* Performance is often evaluated by two networking metrics: throughput and delay. We often need more throughput and delay 1
* Reliability: In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe. 1
* Security: Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses. 1

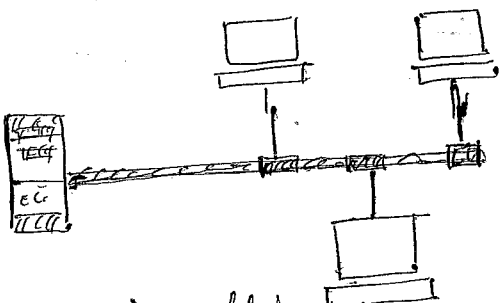
Marks 4

2.a) Physical Structures

* A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another.
* There are two possible types of connections point-to-point and multipoint
* Point-to-point: * Provides dedicated link between two devices
  * The entire capacity of the link is reserved for transmission between these two devices
  * Point-to-point connections use cable to connect the two ends.
  * Other options are microwave or satellite links
* Multipoint (multidrop) connection is one in which more than two specific devices share a single link



a. Point-to-Point



b. Multipoint

Fig (2)

* In a multipoint environment, the capacity of the channel is shared, either spatially or temporally.
  * If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a time shared connection

2 Physical Topologies (Network Topologies)

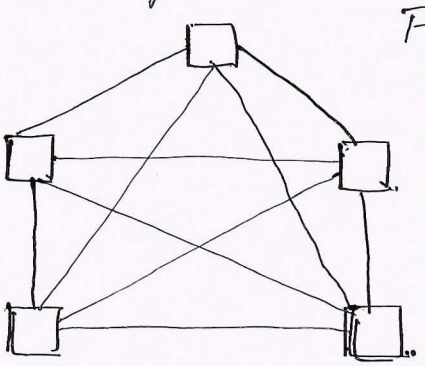
* The terms physical topology refers to the way in which a network is laid out physically.

Marks

* There are four basic topologies possible: mesh, star bus and ring.

* Mesh Topology 3

  * Every device has dedicated point-to-point link to every other device
  * The number of physical links in a fully connected mesh network with n nodes is equal to $n(n-1)$ Physical links.
  * In duplex mode the number physical links required are $n(n-1)/2$
  * Every device on the network must have $n-1$ input/output (I/O) ports.
  * Advantages: * Each connection can carry its own data load
    * Mesh topology is robust: If one link becomes unusable, it does not incapacitate the entire system
    * There is advantage of privacy or security.
    * Fault isolation and Fault identification is easy.
  * Disadvantages
    * Cabling and the number of I/O ports in mesh topology is more
    * Hardware required to connect each link can be expensive

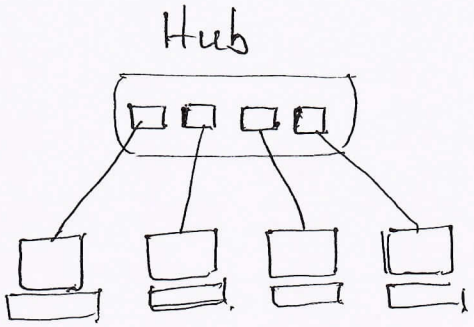


Fully connected mesh topology $n=5$
10 links

* Star Topology

3

* Each device has dedicated point-to-point link only to a central controller called a hub
* The controller acts as a 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.



A star topology connecting four stations.
Fig (3)

* Advantages: (i) Less expensive than a mesh topology
  (ii) Robustness: If one link fails, only that link is affected, All other links remain active.
  (iii) Easy fault identification and fault isolation

* Bus Topology

3

* A bus topology is a multipoint
* One cable acts as a backbone to link all the devices in a network.
* A drop line is a connection between the device and the main cable.
* A tap is a connector that either splices into the main cable or punctures the sheathing of a cable
* Signal travels along the backbone, some of its energy is transformed into heat. It becomes weaker and weaker as it travels further and further. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

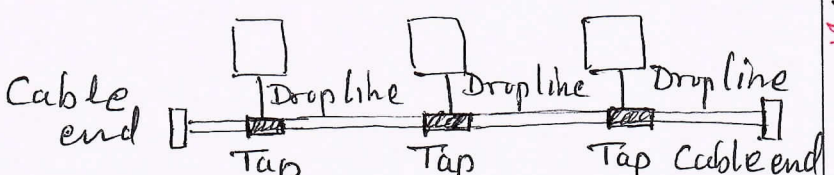
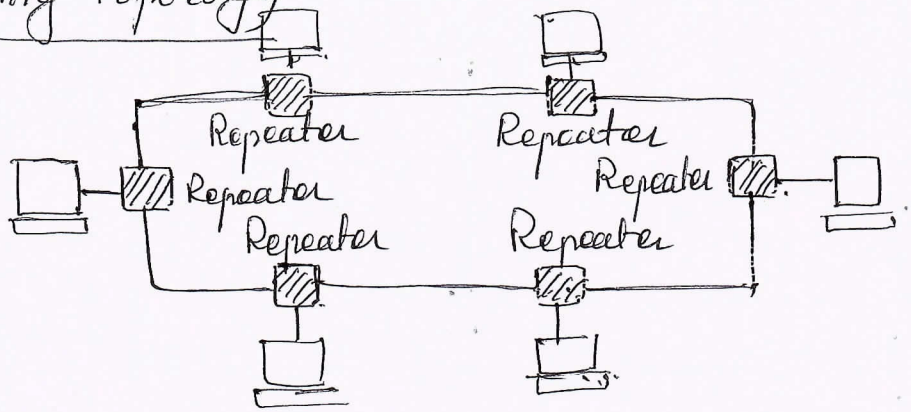


Fig (4) A bus topology connecting three stations

Advantage: Ease of installation
Disadvantage: Difficult Reconnection and fault isolation.

* Ring Topology



A ring topology connecting six stations

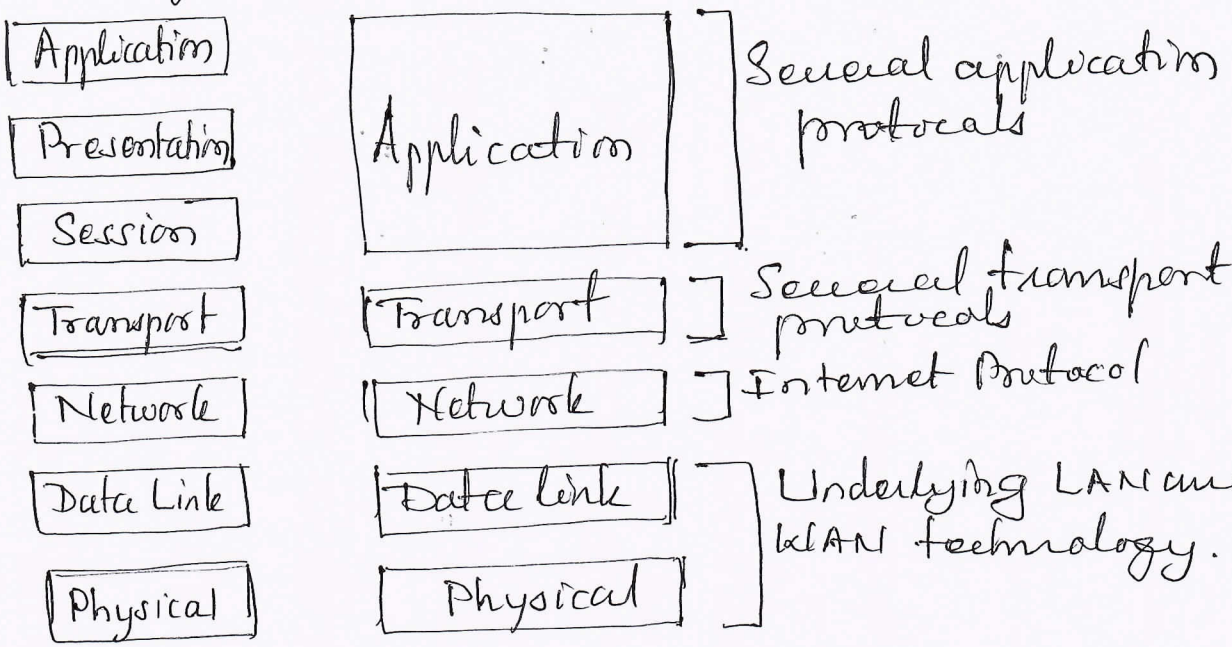
* Each device has a dedicated point-to-point connection with only the two devices on either side of it
* A signal is passed along the ring in one direction, from device to device until it reaches its destination
* Each device regenerates the bits and passes them along towards the destination

Advantages: * Easy to install and reconfigure
Each device is linked to only its immediate neighbors (either physically or logically).
* Fault isolation is simplified.

Disadvantage: Unidirectional traffic can be a disadvantage.

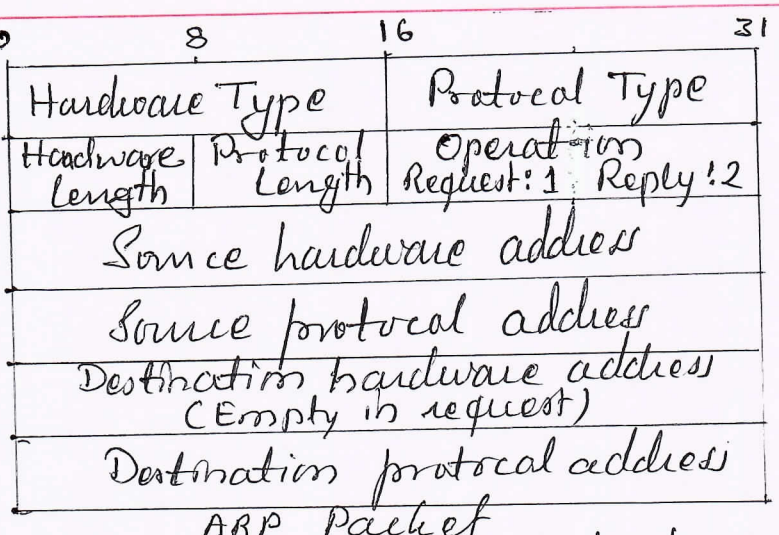
Marks

2.b) Distinguish TCP/IP model with OSI model 4



* Session and presentation layers are missing from the TCP/IP protocol suite
* The application layer in TCP/IP is considered to be the combination of upper three layers in OSI model

3.a) Describe various fields in the format of an ARP packet and explain how ARP sends request and response messages. 12



ARP Packet

3

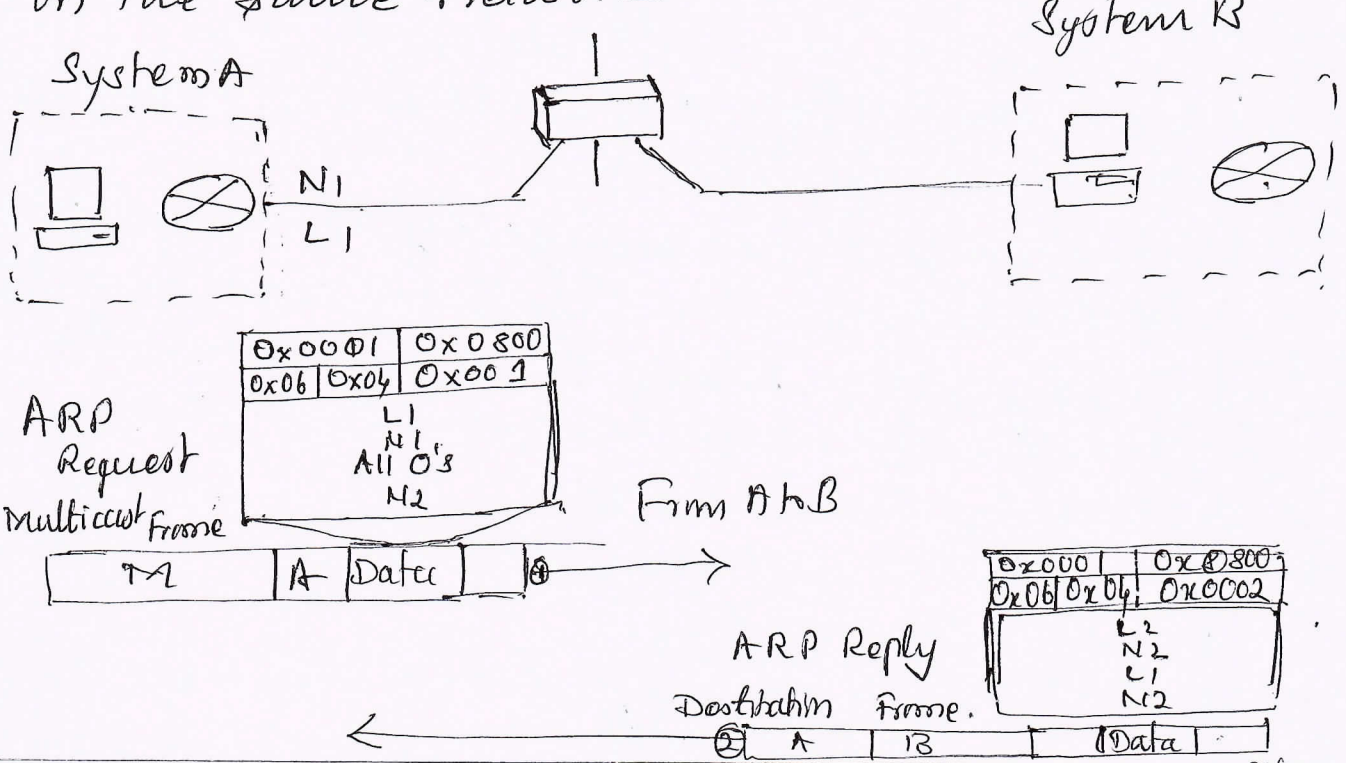
Hardware: LAN or WAN Protocol
Protocol: Network-Layer protocol.
Figure shows ARP packet.
* The hardware type field defines the type of the

lehle-layer protocol.

* Ethernet is given the type 1
* The protocol field defines the network-layer protocol
* IPv4 protocol is $(0800)_{16}$.
* The source hardware and source protocol addresses are variable-length fields defining the lehle layer and network-layer addresses of the sender
* The destination hardware address and destination protocol address fields define the receiver lehle-layer and network-layer addresses.
* An ARP packet is encapsulated directly into a data-lehle frame. The frame needs to have a field to show that the payload belongs to the ARP and not to the network datagram.

> ARP request and response messages

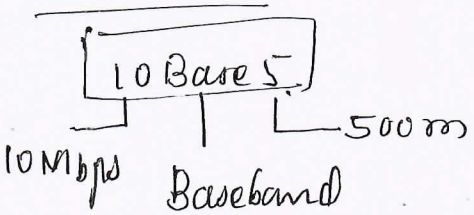
Figure shows host "A" with IP address N1 and MAC address L1 has a packet to send to another host with IP address N2 and physical address L2 (which is unknown to the first host). The two hosts are on the same network.

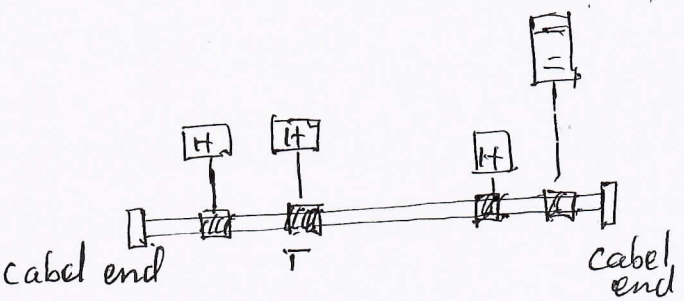


Marks

3.b) Write a short note on implementation of standard Ethernet topologies. 10

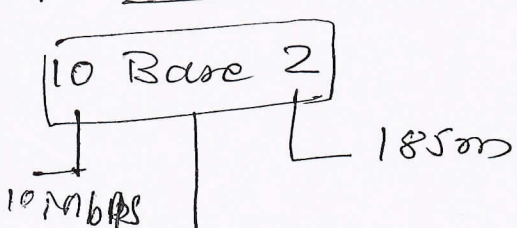
* 10 Base 5

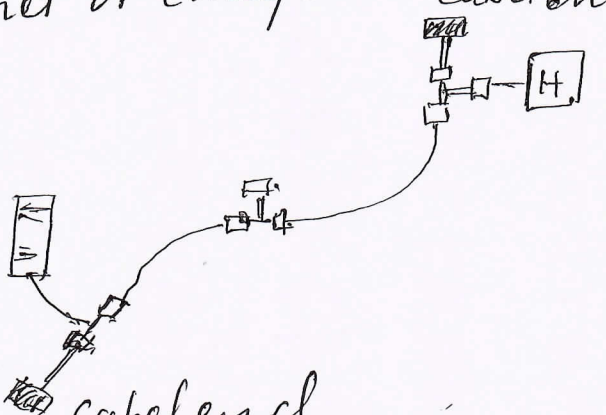




- Also called 10 Base 5, Thick Ethernet or Thicknet 2
- First ethernet specification to use a bus topology with an external transceiver (transmitter/receiver) connected via a thick coaxial cable.
- Maximum length is 500 m
- Encoding: Manchester

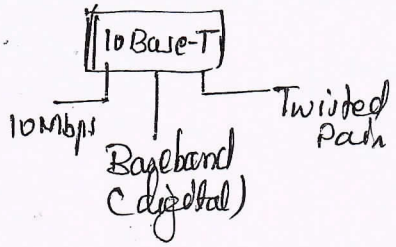
* 10 Base 2: Thin Ethernet or cheapernet

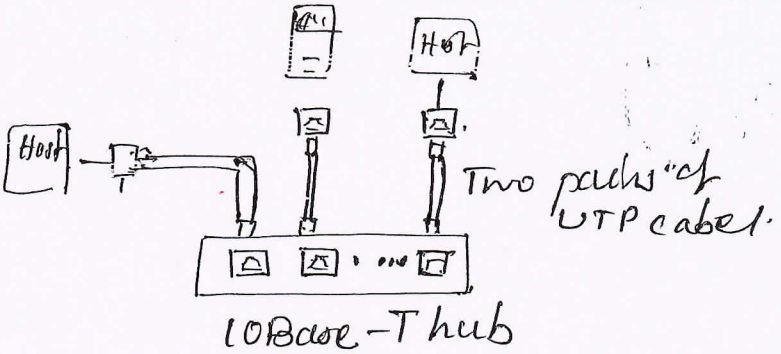




- Uses bus topology and cable is much thinner and more flexible 2
- Transceiver is normally part of the Network Interface Card (NIC), which is installed inside the station
- Less expensive than thick coaxial and the connections are much cheaper than taps.
- Encoding: Manchester.

* 10Base-T (Twisted pair ethernet)
  * Uses Star topology
  * Stations are connected to a hub via two pairs of twisted cable.

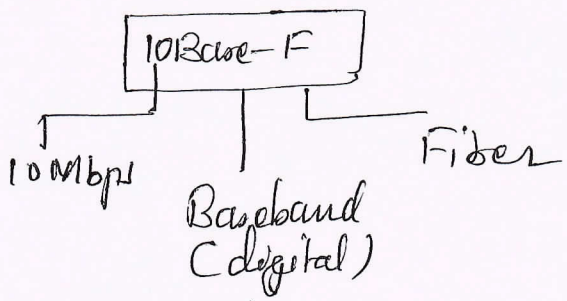


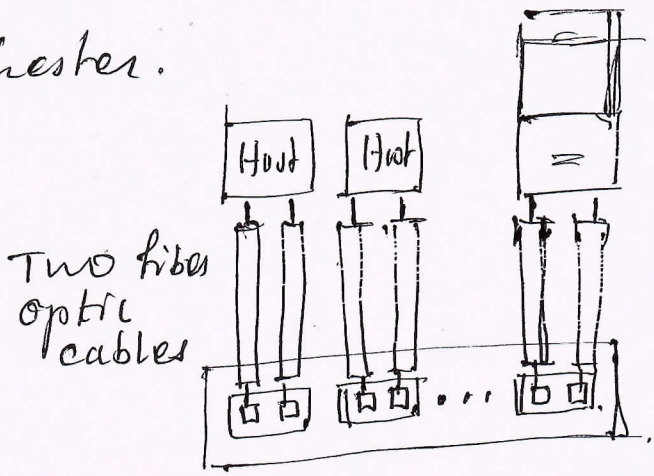


2

* Two pairs of twisted cable create two paths (one for sending and one for receiving) between station and hub.
* Encoding: Manchester.

* 10 Base F





2

- 10Base F uses a star topology to connect stations to a hub.
- The stations are connected to the hub using two fiber-optic cables.
- Encoding: Manchester.

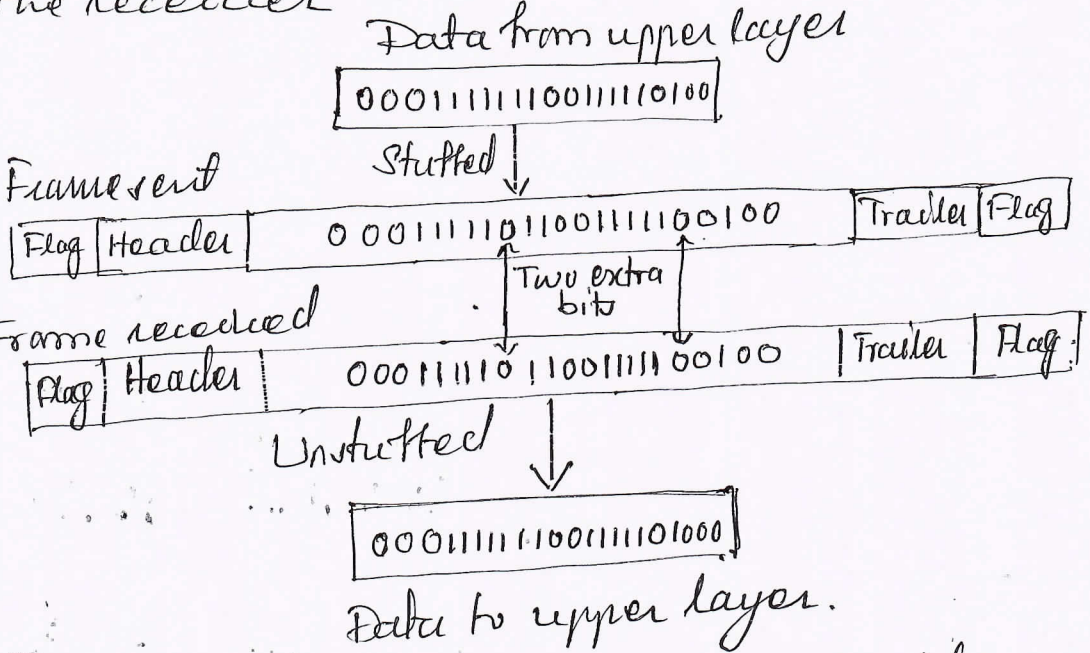
4. a) Describe the concept of bit stuffing and byte stuffing.

* Bit Stuffing

- Bit stuffing is the procen of adding one extra 0 whenever five consecutive 1s follow a 0 in the data, so that the receiver doesnot mistake the pattern 01111110 for a flag.

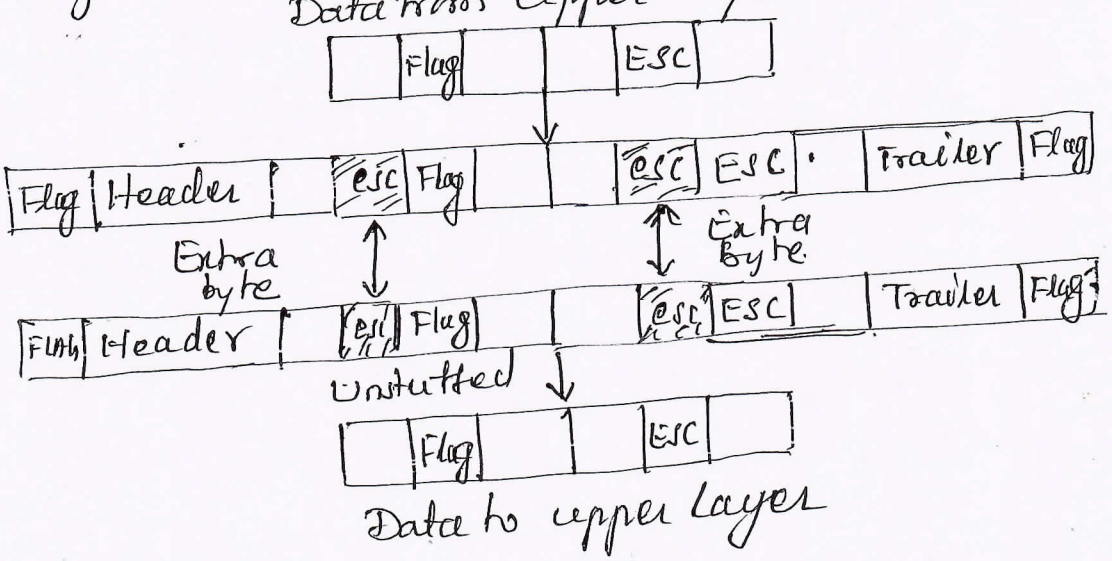
Mark

* Figure shows bit stuffing at the sender and bit-removal at the receiver
* Note that even if we have a '0' after the 1's we still stuff a '0'. The '0' will be removed by the receiver



5

* Byte stuffing is the process of adding one extra byte whenever there is a flag or escape character in the text.
* Figure shows Byte stuffing and unstuffing.



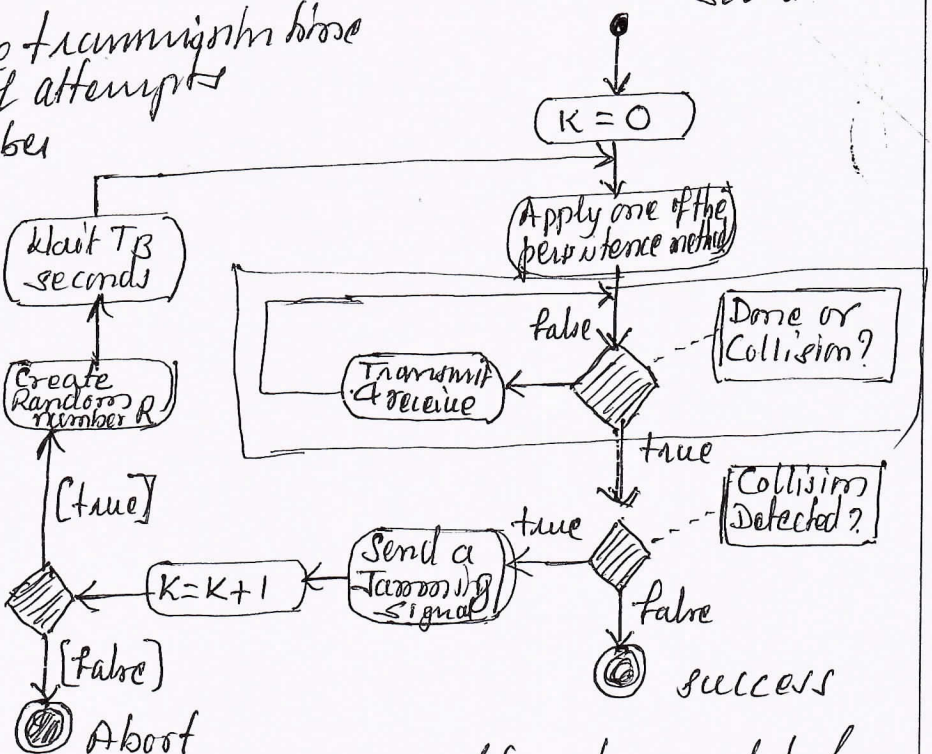
5

Marks

4.6) Explain CSMA/CD working with the help of flowchart — 6

* Flow diagram for the CSMA/CD

Legend:
Tfr : Frame average transmission time
K : Number of attempts
r : random number 0 to $2^K - 1$
TB : (Back off time) = R X Tfr



3

* There is need to sense the channel before we start sending the frame using one of the persistence process
* In CSMA/CD, transmission and collision are continuous processes.
* The station transmits and receives continuously and simultaneously using two different ports or a bidirectional port.
* We use a loop to show that transmission is a continuous process
* We constantly monitor in order to detect one of the two conditions: either transmission is finished or a collision is detected. Either event stops transmission.
* When we convert of loop, if a collision has not been detected, it means that transmission is complete, the entire frame is transmitted.

3

Marks

otherwise collision has occurred.

* Short jamming signal is sent to make sure that all stations became aware of the collision.

4.c) List the characteristics of Wireless Lan — 04

* Characteristics of wireless LAN:

(i) Interference: Receiver may receive signals not only from the intended sender, but also from other senders. — 1

(ii) Multipath propagation: A receiver may receive more than one signal from the same sender because of electromagnetic waves can be reflected back from obstacles such as walls, the ground, or objects. — 2

(iii) Error: Errors and error detection are more serious issues in a wireless networks than in a wired network — 1

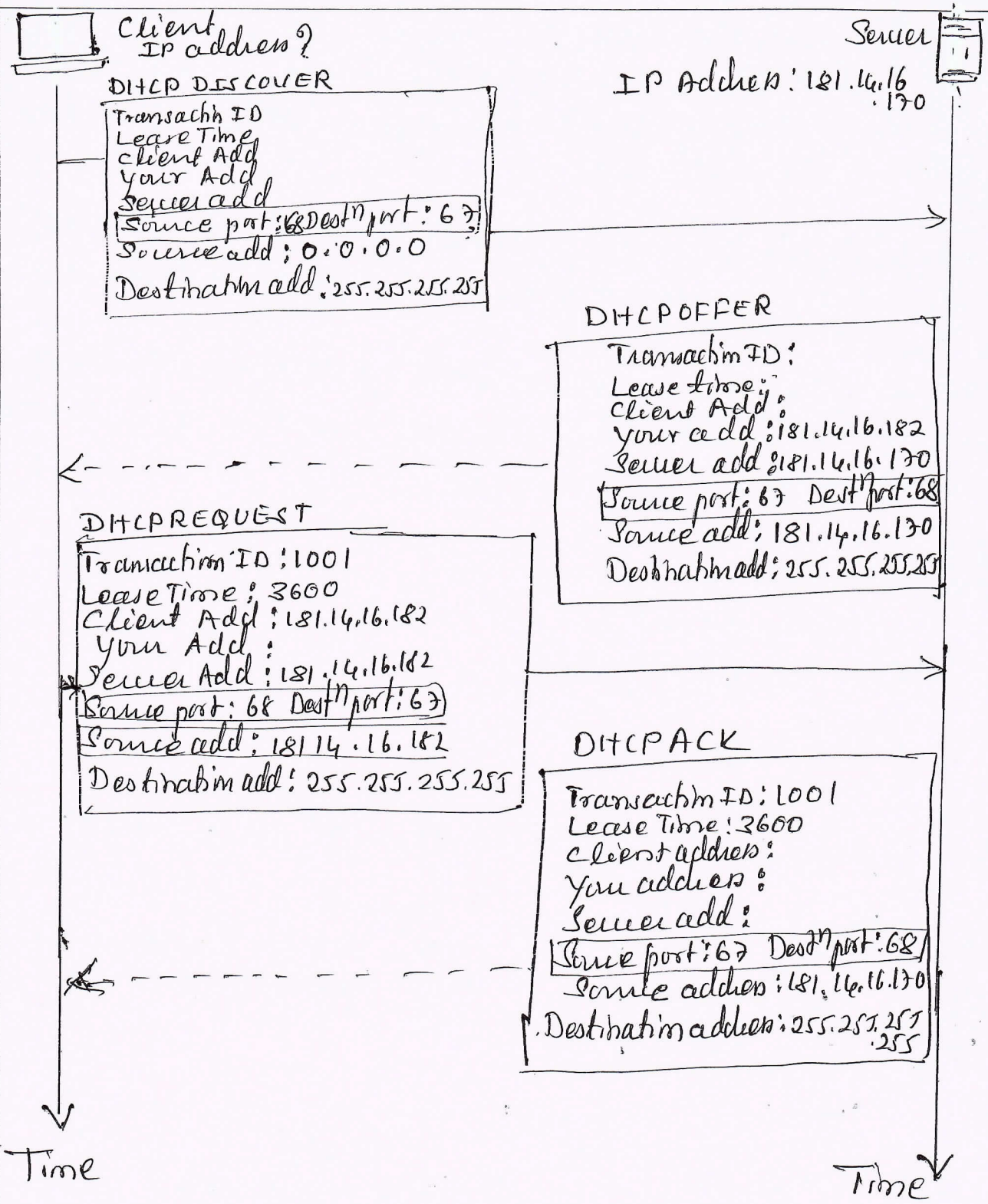
5.a) Explain working of DHCP (Dynamic Host Configuration Protocol) — 08

Figure shows working of DHCP

* 1. * The joining host creates a DHCPDISCOVER message in which only the transaction-ID field is set to a random number. No other field can be set because the host has no knowledge with which to do so.

* This message is encapsulated in a UDP user data gram with the source port set to 68 and the destination port set to 67.

* The user datagram is encapsulated in an IP datagram with the source address set to 0.0.0.0 (this host) and destination address set to 255.255.255.255



4

2. The DHCP server or servers (if more than one) responds with a DHCPOFFER message in the your address field defines the offered IP address for the joining host and the server address field includes the IP address of the server
* It also includes the lease time for which the host can keep the IP address.

Marks

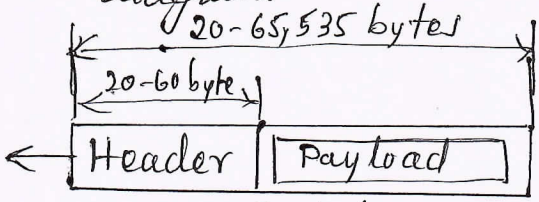
3. * The joining host receives one or more offers and selects the best of them. The joining host then sends a DHCPREQUEST message to server that has given the best offer.

4. * Finally the selected server responds with a DHCPACK message to the client if the offered IP address is valid 4

* If the server cannot keep its offer, the server sends a DHCPNACK message and the client needs to repeat the process.

5.b) (i) Unicast 04
(ii) Multicast
(iii) Multicast.
(iv) Broadcast

5.c) Explain IPV4 datagram format with a neat diagram. 08



a. IP datagram

Legend
VER: Version Number
HLEN: Header Length
byte: 8 bits

VER 4 bits	HLEN 4-bits	Service type 8-bits	Total Length 16-bits
Identification 16-bits		Flags 3-bits	Fragmentation offset 13-bits
Time to live 8 bits	Protocol 8-bits		Header Checksum 16 bits
Source IP address (32-bits)			
Destination IP address (32-bits)			
Options + padding (0 to 40 bytes)			

b. Header. 4

* Figure shows the IPv4 datagram format
* A datagram is a variable length packet ~~consisting of data~~ consisting of two parts : header and payload (data)
The header is 20 to 60 bytes in length and contains information essential to routing and delivery

> Version Number (VER): Defines the version of IPv4 protocol, which, obviously has the value of 4.

> Header Length : The 4-bit header length (HLEN) field defines the total length of the datagram header in 4-byte words

> Service type : * In the original design of the IP header this field was referred to as type of service (TOS)
* In the late 1990s IETF redefined the field to provide differential services (DiffServ)

> Total Length : * Defines the total length (header plus data) of the IP datagram in bytes
* Helps the receiving device to know when the packet is completely arrived.
* The header length can be found by multiplying the value in the HLEN field by 4

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

> 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.

> Time-to-Live : Used to control the maximum number of hops (routers) visited by the datagram

> Protocol : Consists of unique 8-bit number
* This field to define to which protocol the payload should be delivered

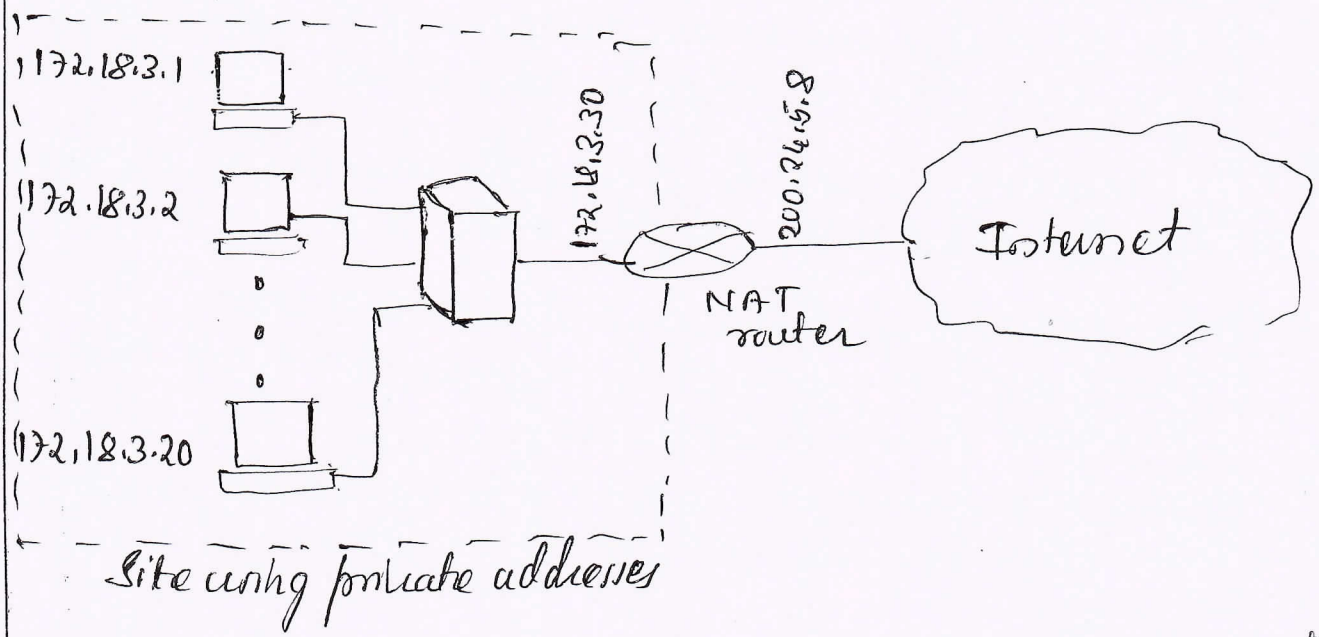
> Header Checksum : IP adds header checksum field to check the header, but not the payload

Marks

- Source and destination address:
  - Defines 32 bit source and destination address
- Options: Options are used for network testing & debugging
- Payload: Payload or data is the packet coming from other protocols that use the services of IP.

6.a) Explain a simple implementation of Network Address Translation (NAT) 10

- Network Address Translation (NAT) is the technology which provides mapping between the private and universal addresses and at the same time support virtual — private networks
- The technology allows a site to use a set of — private addresses for internal communication and a set of global Internet addresses (at least one) for communication with the rest of the world. 5
- The site must have only one connection to the global Internet through a NAT-capable router that runs NAT software.
- Figure shows a simple implementation of NAT



5

Marks

* As figure shows, the private network uses private addresses. The router that connects the network to the global address uses one private address and one global address.
* The private network is invisible to the rest of the Internet
* The rest of the internet sees only the NAT router with the address 200.24.5.8

6.b) Explain distance vector routing algorithm using Bellman Ford algorithm 10

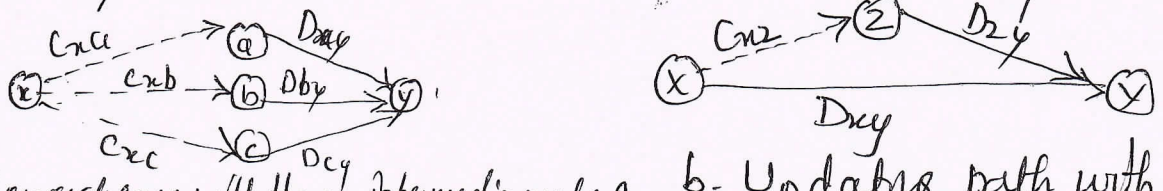
* Bellman - Ford Equation
  - This equation is used to find the least cost (shortest distance) between a source node x and a destination node y, through some intermediary nodes (a, b, c...) when the costs between the source and the intermediary nodes and the least costs between the intermediary nodes and the destination are given
  - General case: D_{ij} is the shortest distance and C_{ij} is the cost between nodes i and j

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

  - In distance-vector routing, normally we want 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 equation becomes simpler, as shown below

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

* Graphical idea behind Bellman-Ford equation



a) General case with three intermediary nodes b. Updating path with new cost

4

Marks

* We can say that the Bellman-Ford Equation enables us to build a new least-cost path from previously established least cost path
* In the above figure we can think of (a→y), (b→y), and (c→y) as previously established least-cost paths and (x→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 established least-cost trees if we use the equations repeatedly

```
Distance_Vector Routing()
{
 //Initialize
   D[myself] = 0
 for (y=1 to N)
 { if(y is a neighbor)
      D[y] = c[myself][y]
   else
      D[y] = ∞
 }
 send vector [D[1], D[2], ... D[N]]
   to all neighbors
 // update
 repeat (forever)
 { wait (for a vector Dw from a neighbor
        w or any change in the table)
   for (y=1 to N)
   {
     D[y] = min[D[y], (c[myself][w]
                + Dw[y])]
   }
   if (any change in vector
     send vector
     {D[1], D[2], ... D[N]} to all
      neighbors
   }
 } // End of Distance Vector
```

2

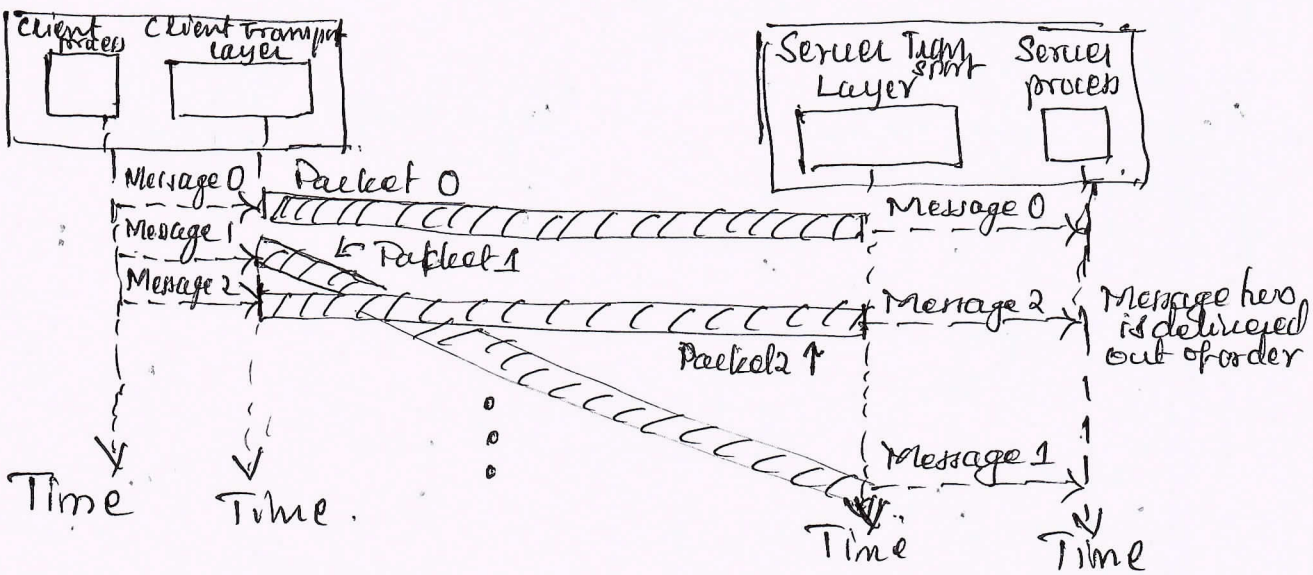
7.a) Describe connectionless and connection-oriented services provided by the transport layer. — 14

** Connectionless Service

) The source process (application program) needs to to divide its message into chunks of data of the size acceptable by the transport layer and 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
  - The application layer encapsulates it in a packet and sends it
  - Since there is no dependency between the packets at the transport layer, the packets may arrive out of order at the destination and will be delivered out of order to the server process

2



3

- Above figure shows the movement of packet using time line
- At client side three chunks of messages are delivered to the client transport layer in order (0, 1 and 2)
- Because of the extra delay in transportation of the second packet, the delivery of messages at the server is not in order (0, 2, 1)
- The two problems arise because of no coordination between two transport layers of client & server
  - If the three chunks of data belong to same message, the server process may receive strange message.

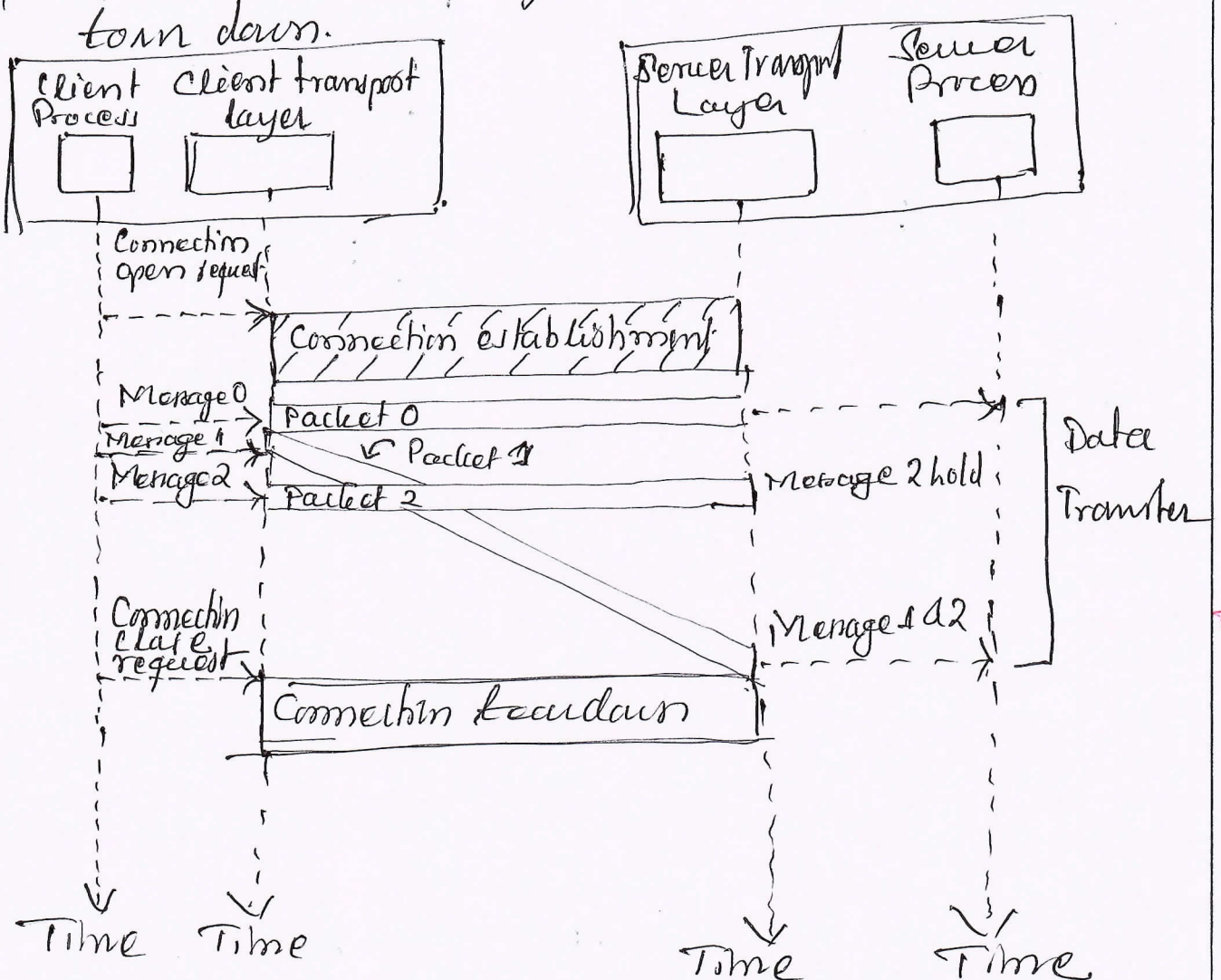
2

(ii) Transport layer has no idea of lost packet (receiving)

- We can say that no flow control, error control, or congestion control can be effectively implemented in a connectionless service.

Connection-oriented service

- The client and the server host need to establish a logical connection between themselves.
- Data exchange can only happen after the connection establishment. 2
- After data exchange connection needs to be torn down.



3

- There is coordination between the two end hosts
- We can implement flow control, error control and congestion control in a connection oriented protocol 2

MARKS

8.a) Explain working of Go-back-N protocol. 10

* To improve the efficiency of transmission, multiple packets must be in transition while the sender is waiting for acknowledgment.
* We need to let more than one packet be outstanding to keep the channel busy while the sender is waiting for acknowledgment
* The key to Go-back-N is that we can send several packets before receiving acknowledgments but receiver can buffer only buffer one packet 2
* We keep a copy of the sent packets until the acknowledgements arrive.

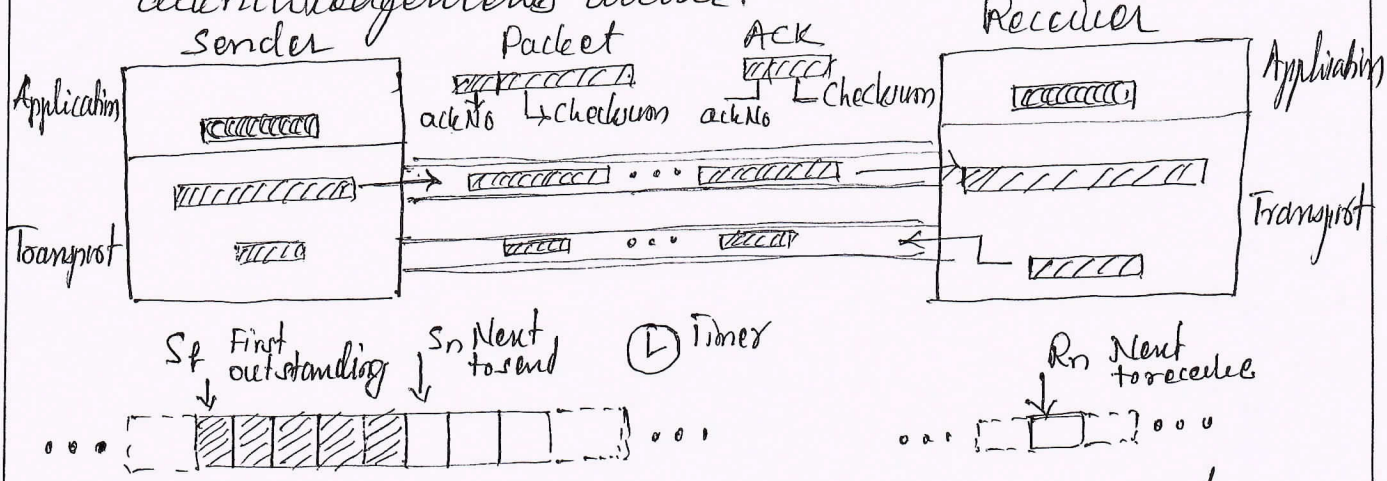


Fig. Go-Back-N Protocol

* Sequence Numbers.
  - The sequence numbers are modulo 2^m, where m is the size of the sequence number field in bits. 1
* Acknowledgment Numbers
  - An acknowledgment number in this protocol is cumulative and defines the sequence number of the next packet expected. 1
* Send window: The send window is an imaginary box covering the sequence numbers of the data packet that can be in transit or can be sent. 1

MARK

7.b) Describe the general services provided by UDP. 6

* General Services provided by UDP

i) Provides process-to-process communication using socket addresses, a combination of IP address and port numbers.

ii) Connectionless Service

There is no relationship between the different user datagrams even if they are coming from the same source process and going to the same destination program.

iii) Flow Control 3

- No flow control, and hence no window mechanism
- The receiver may overflow with incoming messages

iv) Error Control

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

v) Checksum: UDP checksum calculation includes three sections: a pseudoheader, the UDP header, and the data coming from the application layer.

vi) Congestion Control: UDP does not provide congestion control

vii) Queuing: In UDP, queues are associated with ports 3

viii) * Multiplexing & Demultiplexing

UDP provides multiplexing and Demultiplexing service.

all

MARKS

> The maximum size of the send window is $2^m - 1$, where m is the size of the sequence number fields in bits.

> The send window can slide one or more slots when an error-free ACK with ackNo greater than or equal to Sf and less than Sn (in modular arithmetic) arrives.

* Receive window

> The receive window is an abstract concept defining an imaginary box of size 1 with a single variable Rn. The window slides when a correct packet has arrived. 1

> Sliding occurs one slot at a time. 1

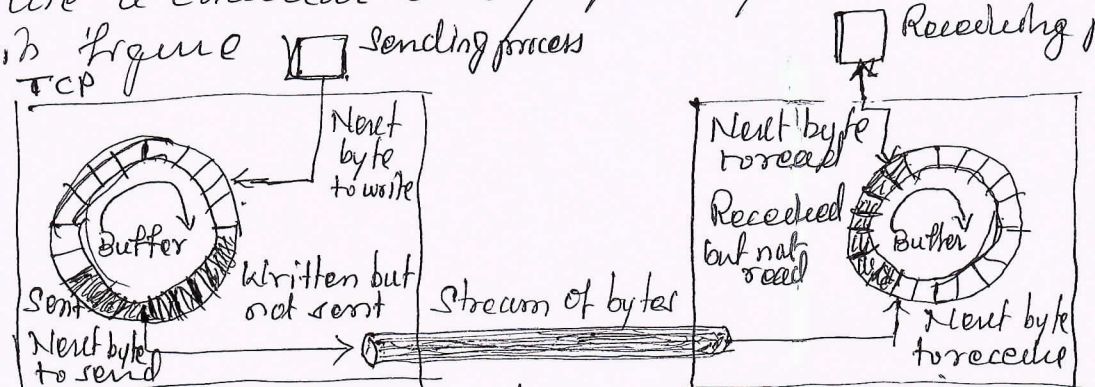
* Timers: Go-Back-N protocol uses one timer 1

* Resending packets: When the timer expires, the sender resends all outstanding packets 1

8.b > Describe Sending and Receiving buffers in TCP, and explain how segments are created from the bytes in the buffers. 10

* TCP needs buffers for storage. There are two buffers, the sending buffer and the receiving buffer, one for each direction

* Diagram One way to implement a buffer is to use a circular array of 1-byte locations as shown in figure



5

> The figure shows the movement of data is one-direction. At the sender, the buffer has three types

of chambers.

- The white section contains empty chambers that can be filled by the sending process (producer).
- The colored area holds bytes that have been sent but not yet acknowledged. The TCP sender keeps these bytes in the buffer until it receives an acknowledgment
- The shaded area contains bytes to be sent by the sending TCP

3 =

* The operation of the buffer at the receiver
  - The circular buffer is divided at two areas shown as white and colored.
  - The white area contains empty chambers to be filled by bytes received from the network.
  - The colored section contain received bytes that can be read by the receiving process
  - When the byte is read by the receiving process, the chamber is recycled and added to the pool of empty chambers.

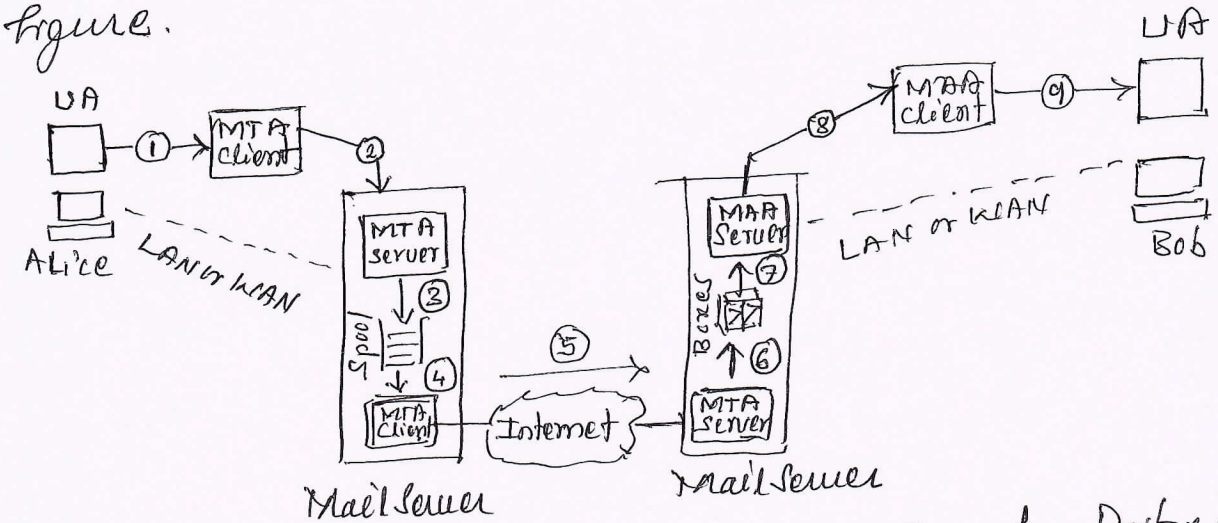
2 =

Marks

9.a) Explain the architecture and format of electronic mail — 10

* Email architecture

Let us consider a common scenario, as shown in figure.



UA: User Agent; MTA: Message Transfer Protocol.

MAA: Message access agent. — 3

- Alice sender of the email.
- Bob receiver of the email.
- Alice and Bob are connected via a LAN or WAN to two mail servers
- Administrator has created one mail box for each user where the received messages are stored
- A mail box is part of a server hard drive, a special file with permission restrictions. Only the owner of the mail box has access to it
- The administrator has also created a queue (Spool) to store messages waiting to be sent. — 2

* A simple e-mail from Alice to Bob takes nine different steps as shown in above figure.
- Alice and Bob use three different agents:
  - a user agent (UA), a message transfer agent (MTA), and a message access agent (MAA)

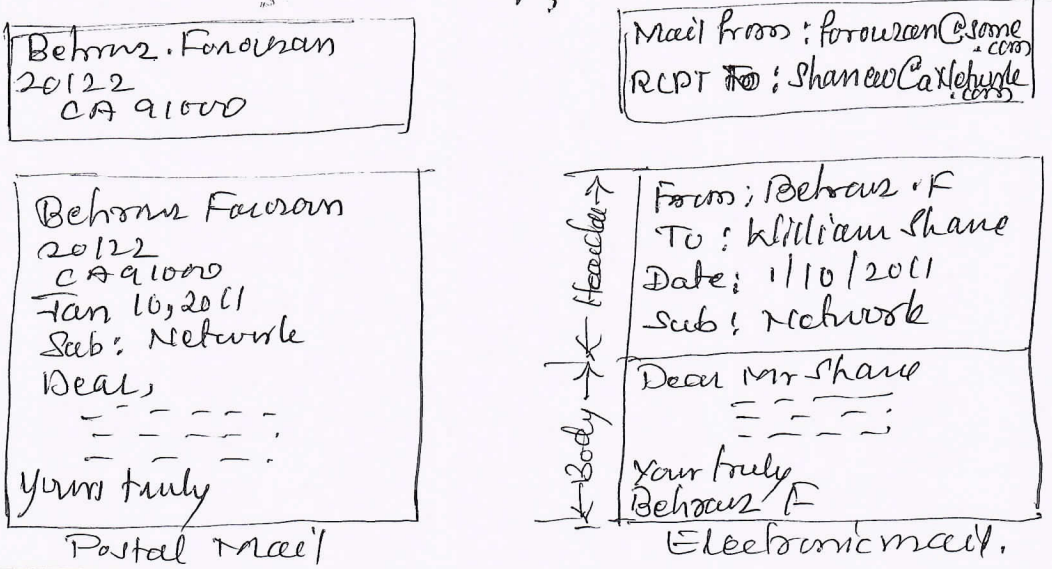
When Alice needs to send a message to Bob, she runs a UA program to prepare the message and send it to her mail server.

- The mail server at her site uses a queue (spool) to store messages waiting to be sent
- The message needs to be sent through the Internet from Alice's site to Bob's site using an MTA.
- Two Message Transfer Agents are need: one - client and one server
- The electronic mail system needs two UAs, two pairs of MTAs (client and server), and a pair of MAAs (client and server)

* User Agents (UA). It provides service to the user to make the process of sending and receiving a message easier.
  - A user agent is a software package (program) that composes, reads, replies to, and forwards messages
  - It also handles local mailboxes on the user's computers.

* Sending Mail: To send mail, the user, through the UA, creates mail that looks very similar to postal mail. It has an envelope and a message.

2



3

Marks

9.6) Distinguish between Local Logging and Remote Logging — 10

* When a user logs into a local system, it is called local logging. As a user types at a terminal or at a workstation running a terminal emulator, the keystrokes are accepted by the terminal driver.
* The terminal driver, in turn, interprets the — 3
combination of characters and invokes the desired application program or utility

* Remote logging
  * When a user wants to access an application program or utility located on a remote machine, user performs remote logging
  * The user sends the keystrokes to the terminal driver where the local operating system accepts the characters but does not interpret them.
  * The characters ~~are~~ are sent to the TELNET client which transforms, which transforms the characters into a universal character set called Network — Virtual Terminal (NVT) characters and delivers them to local TCP/IP stack — 3
  * The commands or text, in NVT form, travel through the Internet and arrive at TCP/IP — stack at the remote machine. Here the characters are delivered to the operating system and passed to the TELNET server, which changes the characters to the corresponding characters understandable by the remote computer.

Figure — 5

Marks

10. a) Explain persistent and non-persistent connections in HTTP. 10M

* Persistent Connections

- HTTP version 1.1 specifies a persistent connection by default.
- In a persistent connection, the server leaves the connection open for more requests after sending a response
- The server can close the connection at the request of a client or if a time-out has been reached 3
- The sender usually sends the length of the data with each response.
- In case of dynamically created document, the server informs the client that the length is not known and closes the connection after sending the data so the client knows that the end of the data has been reached.
- Time and resources are saved using persistent connections Example — 2

* Non-persistent Connections

- In a non-persistent connection, one TCP connection is made for each request/response
- The following lists the steps in this strategy:
  - The client opens a TCP connection and sends a request
  - The server sends the response and closes the connection
  - The client reads the data until it encounters an end-of-file marker; it then closes the connection 3
- In this strategy, if a file contains links to N different pictures in different files (all located on the same server), the connection must be opened and closed N+1 times.

Marks

} The nonpersistent strategy imposes high overhead on the server because server needs N+1 different buffers each time a connection is opened.

Example - 2

10.b} Write a short note on DNS recursive and iterative solutions. 10

* Resolution : A host that needs to map an address to a name or a name to an address calls a DNS client called a resolver

} A resolution can be either recursive or iterative

* Recursive Resolution

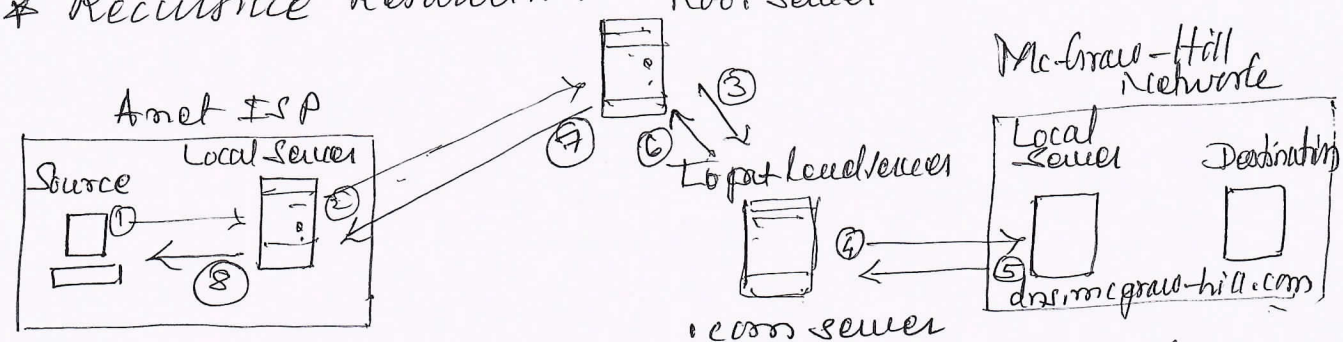


Figure shows a simple example of a recursive resolution. We assume that an application program running on a host named some.anet.com needs to find the IP address of another host named engineering.mcgraw-hill.com to send a message to. The source host is connected to the Anet ISP ; the destination host is connected to the Mc Graw-Hill network. 2

} Application program on source host calls the DNS resolver (client) to find the IP address of the destination host 3

} Request is sent to DNS server (event 2)

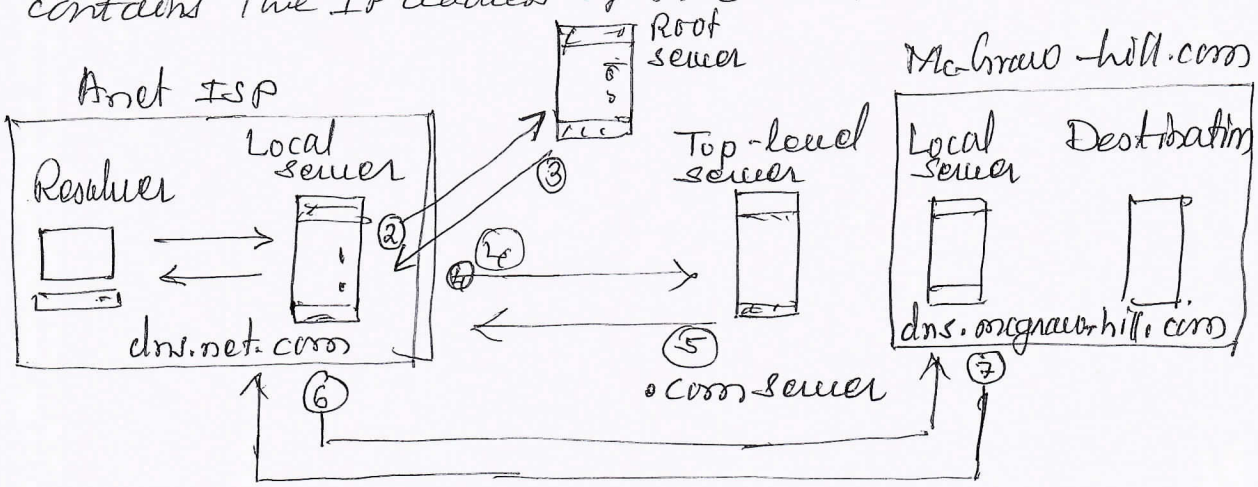
} The query is sent to top-level-domain server (event 3)

} The query is sent to dns.mcgraw-hill.com (event 4)

- The IP address is now sent back to the top-level DNS server (event 5), then back to the root server (event 6), then back to the IPS DNS server, which may cache it for the future queries (event 7), and finally back to the source host (event 8).

Iterative Resolution

- An iterative resolution, each server that does not know the mapping sends the IP address of the next server back to the one that requested it
- Figure shows the flow of information in an iterative resolution in the same scenario as the one depicted in recursive resolution
- Normally the iterative resolution takes place between two local servers: the original resolver gets the final answer from the local server. 3
- Message shown by the events 2, 4, and 6 contain the same query. However message shown by event 3 contains the IP address of the top-level domain server.
- event 5 contains the IP address of the McGraw-Hill local DNS server, and the message shown by event 7 contains the IP address of the destination.



2

Fig. Iterative Solution