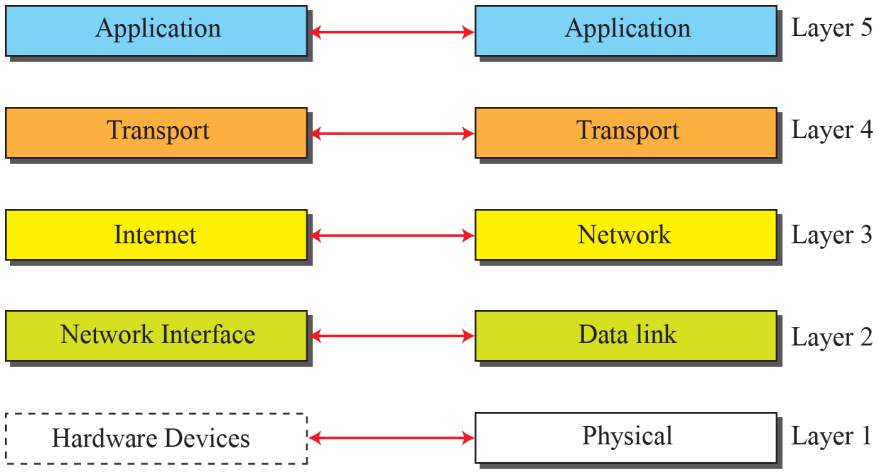
1. **Describe significant services of all layers in TCP/IP protocol suite along with encapsulation de capsulation process with necessary fig. 16 M**

TCP/IP PROTOCOL SUITE: ***Layers in the TCP/IP protocol suite***



2.33

Application Layer [PDU: Message]

- Provide a virtual terminal to the users.
- Deals with File transfer, access, management and remote login

Transport Layer [PDU: Segment]

- Deals with the process to process delivery of the data.
- This layer guarantees the data transmission.
- Two protocols are used.

  TCP (Transmission Control Protocol, connection oriented)

  UDP (User Datagram Protocol, connection less)
- Deals with Reliable end-to-end delivery of a message

Network Layer [PDU: Packet]

- Responsible for assigning logical address i.e. IP address.
- IP address is a 32 bit address like 172.16.25.41.
- Two main protocols works at this layer are IPV4, IPV6, ICMP, IGMP
- Deals with the host to host delivery of data i.e. end to end delivery of packet.
- Deals with formation of packets.
- Routers works at the Network layer which establishes the best delivery path (routing)

Data Link Layer [PDU: Frame]

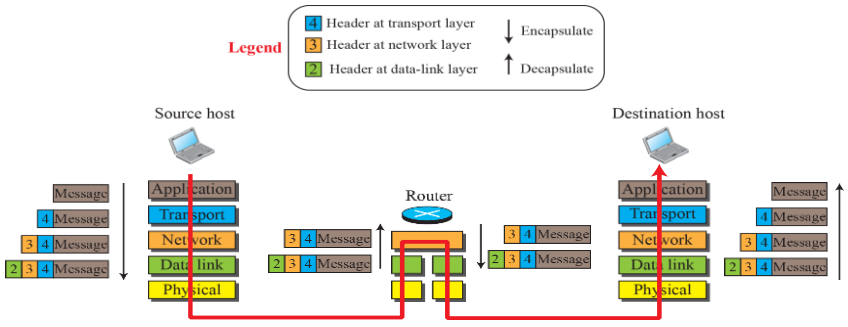
- Responsible for assigning physical address.
- Mac address is 48 bit address.
- Deals with the framing, error control, flow control, hop to hop delivery.

Physical Layer

- Convert frame to bits.
- Cables, hubs, connectors works at physical layers.
- Deals with formation of frame.

Encapsulation / Decapsulation

One of the important concepts in protocol layering in the Internet is encapsulation/ decapsulation



2.39

b. List different performance criteria of a network. 4M

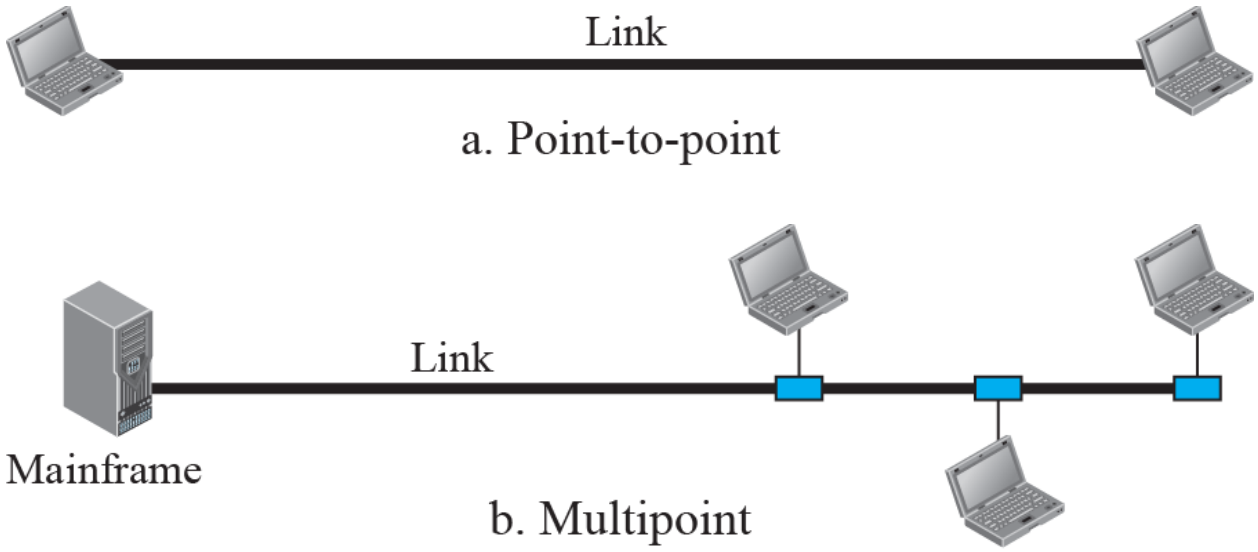
A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security

Performance- throughput & delay

Reliability- frequency of failure and the time it takes a link to recover from a failure
Security- protecting data from unauthorized access, damage and development.

2. **a. Explain different physical structure and network topologies with the help of diagrams. 16 M**

Physical Structures



Physical Topology
Refers to the way in which a network is laid out physically
Figure 1.4: A fully-connected mesh topology

Figure 1.4: ***A fully-connected mesh topology***

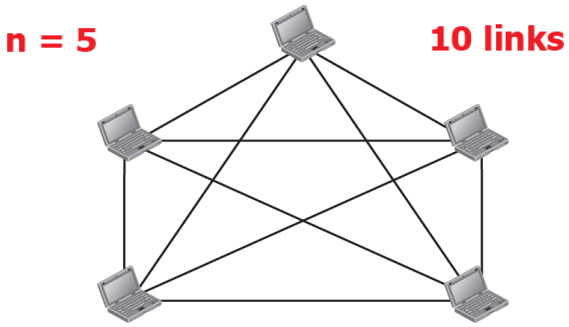
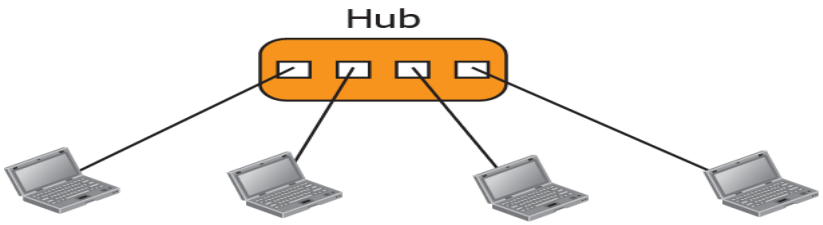


Figure 1.6: *A bus topology*

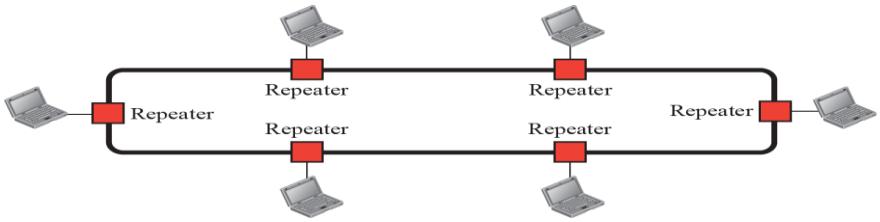
1.11

Figure 1.5: *A star topology*



1.10

Figure 1.7: *A ring topology*



1.12

b. Distinguish TCP/IP model with OSI model 4 M

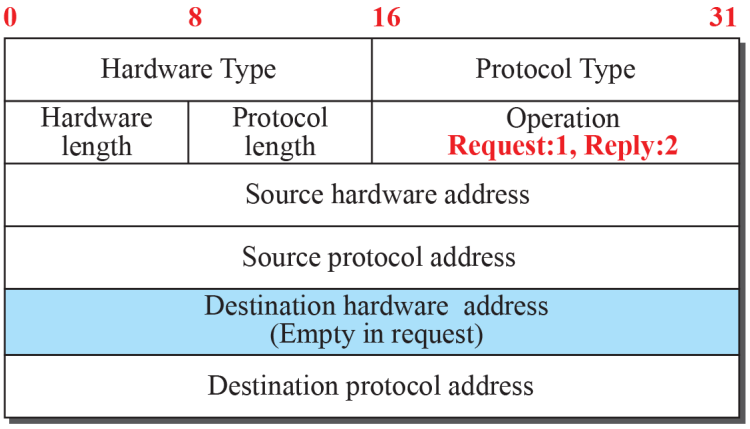
Comparison between OSI and TCP/IP

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. 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.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.

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

Figure 9.8: ***ARP packet***

Hardware type is type of link layer protocol and protocol type is type of network layer protocol



Hardware: LAN or WAN protocol
Protocol: Network-layer protocol

9.71

Hardware type: The hardware field defines the type of link layer protocol, for ETHERNET this field is '1'.

Protocol type: this field defines the network layer protocol which is IPV4 and set to (0086)16

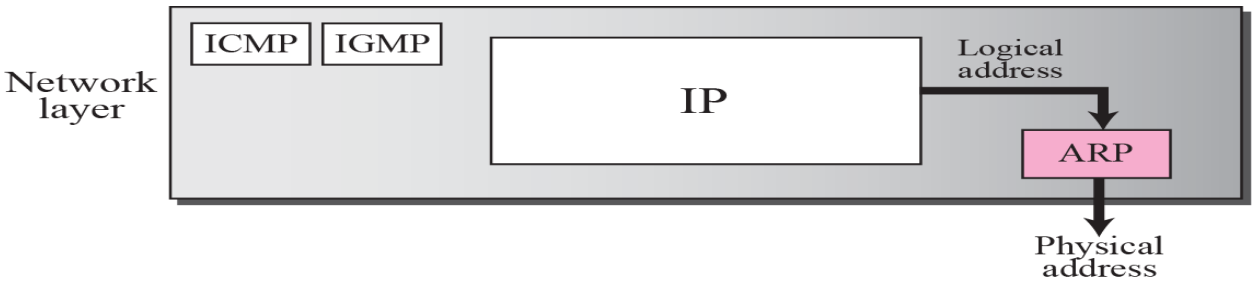
Hardware length: The hardware length field defines the length of hardware and set to (06)16

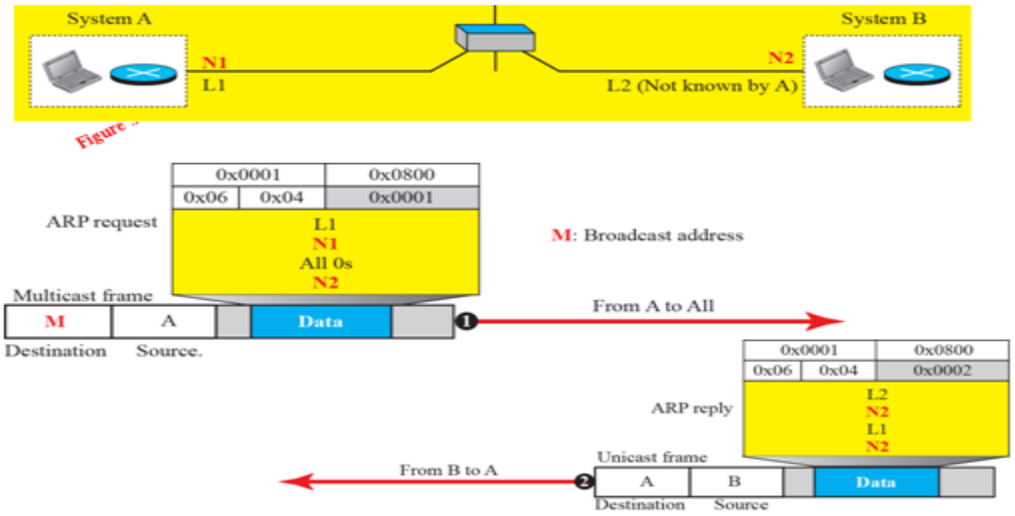
Protocol length: The field defines the length of protocol and set to (04)16.

Operation: For request the filed is set to ‘1’, For request the fields is set to ‘2’.

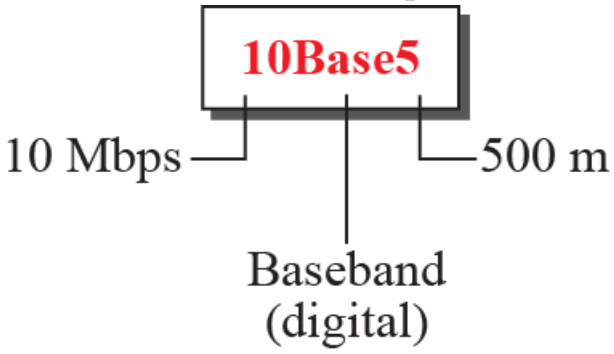
ARP with response and reply packet

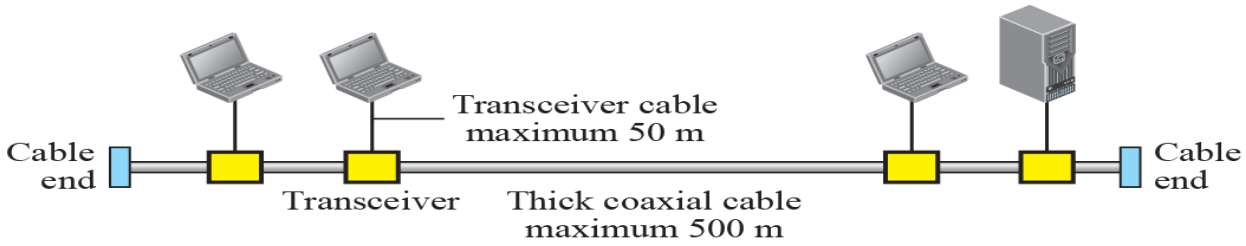
ARP is an network layer protocol which accepts a logical address from the IP protocol, maps the address to the corresponding physical address and pass it to the data link layer. The mapping of IP address to physical address is done by using ARP (Address Resolution Protocol).





b. write short notes on implementation of standard ethennet topologies. 8 M





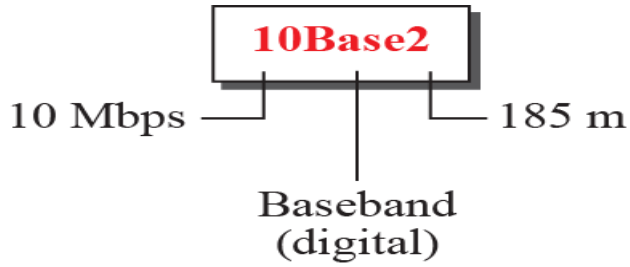
10Base5: thick Ethernet, or Thicknet.

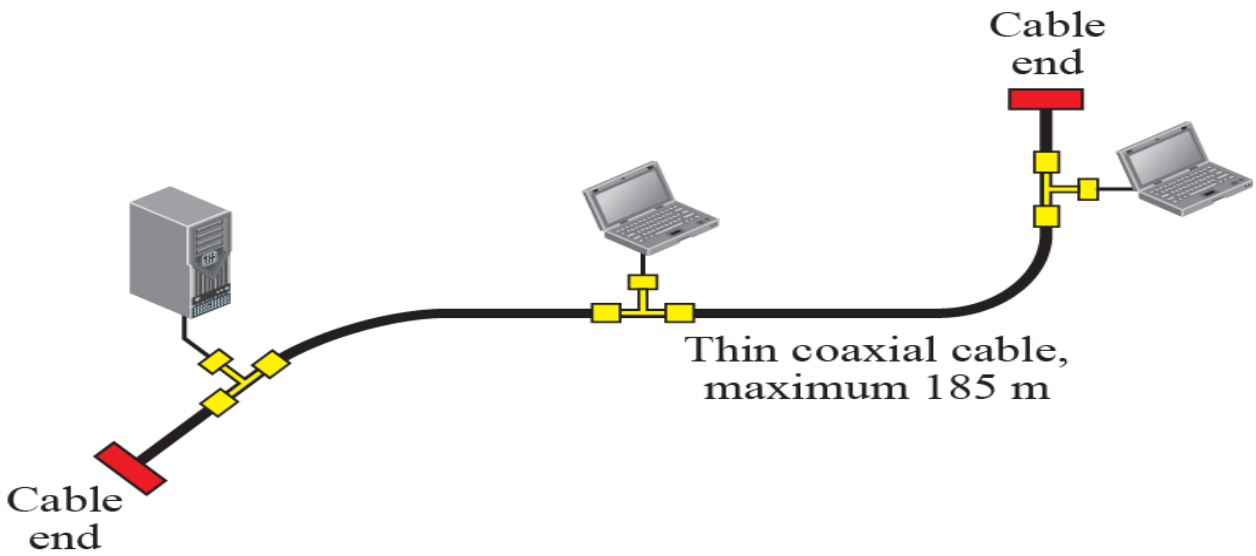
The nickname derives from the size of the cable, which is roughly the size of a garden hose and too stiff to bend with your hands.

10 Base 5 was the first Ethernet specification to use a bus topology with an external transceiver (transmitter/receiver) connected via a tap to a thick coaxial cable.

.

The transceiver is connected to the station via a transceiver cable that provides separate paths for sending and receiving





The second implementation is called 10Base2, thin Ethernet, or Cheaper net.

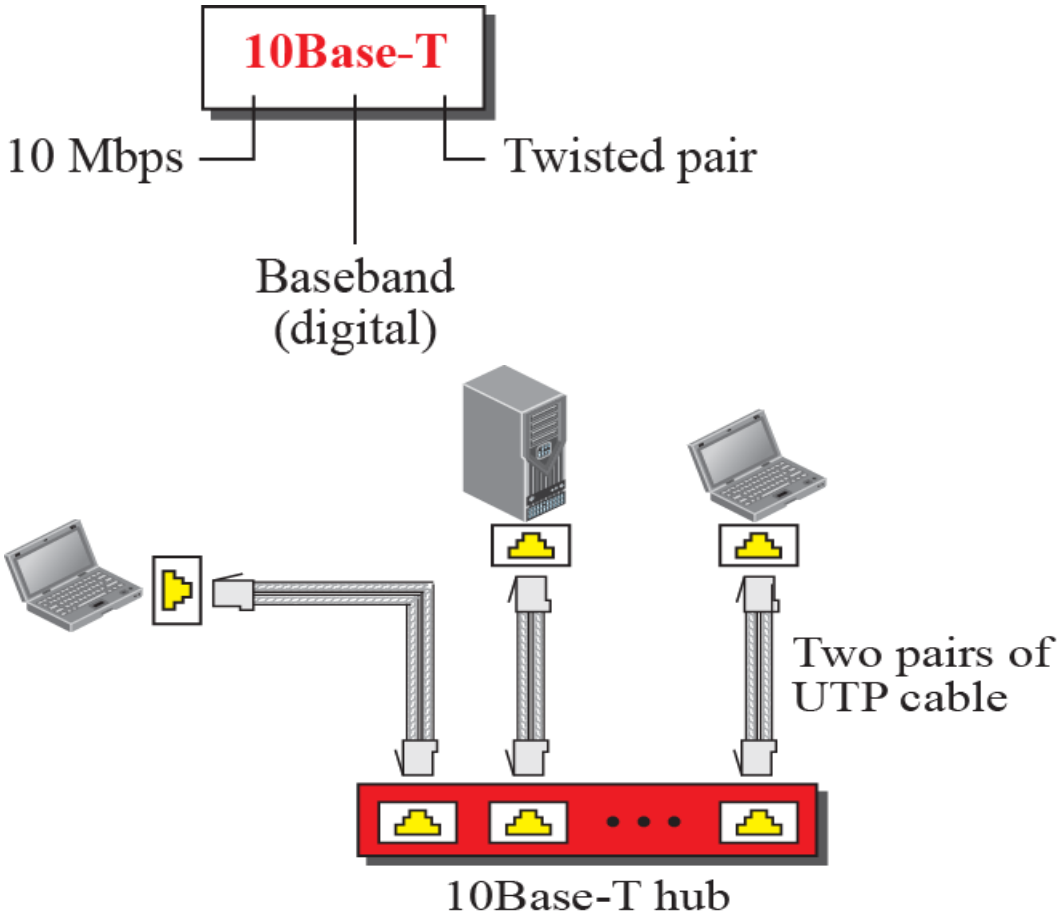
10 Base2 also uses a bus topology, but the cable is much thinner and more flexible.

In this case, the transceiver is normally part of the network interface card (NIC), which is installed inside the station.

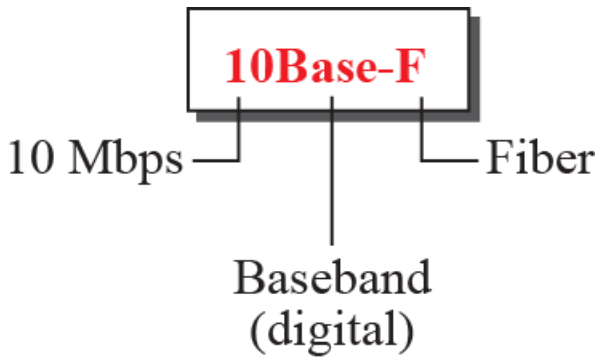
This implementation is more cost effective than 10Base 5 because thin coaxial cable is less expensive than thick coaxial

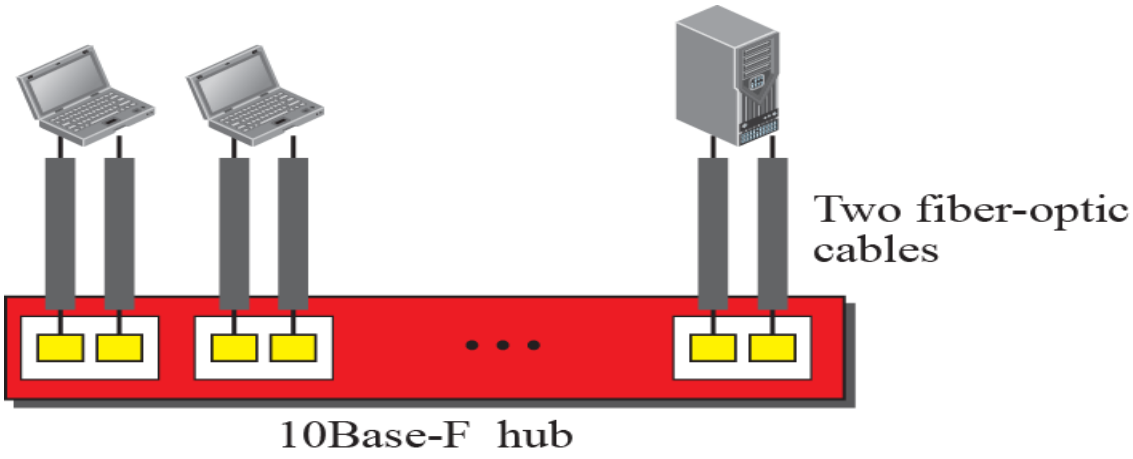
Installation is simpler because the thin coaxial cable is very flexible.

the length of each segment cannot exceed 185 m (close to 200 m)



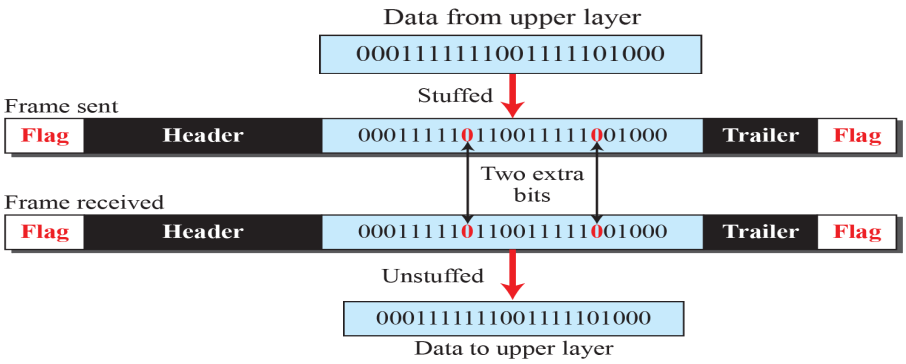
The third implementation is called 10 Base-T or twisted-pair Ethernet.
10 Base-T uses a physical star topology.
The stations are connected to a hub via two pairs of twisted cable
Note that two pairs of twisted cable create two paths (one for sending and one for receiving) between the station and the hub.
Any collision here happens in the hub.
Compared to 10Base 5 or 10 Base2, the hub actually replaces the coaxial cable as far as a collision is concerned.
The maximum length of the twisted cable here is defined as 100 m, to minimize the effect of attenuation in the twisted cable.





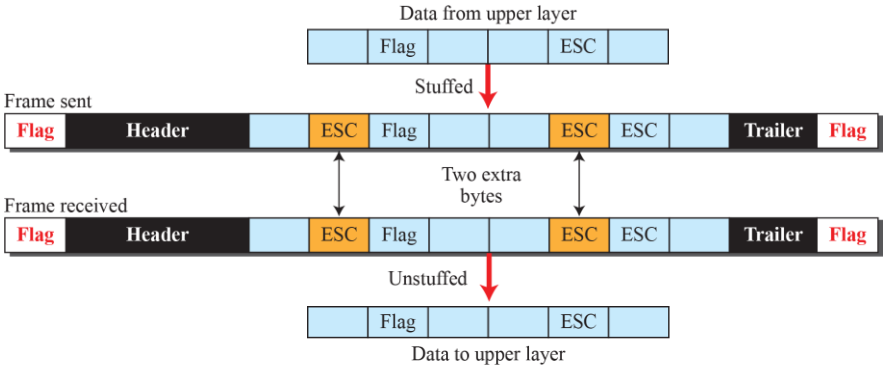
4. a. Descibe the concept of bit stuffing and byte suffing 10M

Figure 111.4: ***Bit stuffing and unstuffing***



11.80

Figure 111.2: ***Byte stuffing and unstuffing***



Byte stuffing is the process of adding one extra byte whenever there is a flag or escape character in the text

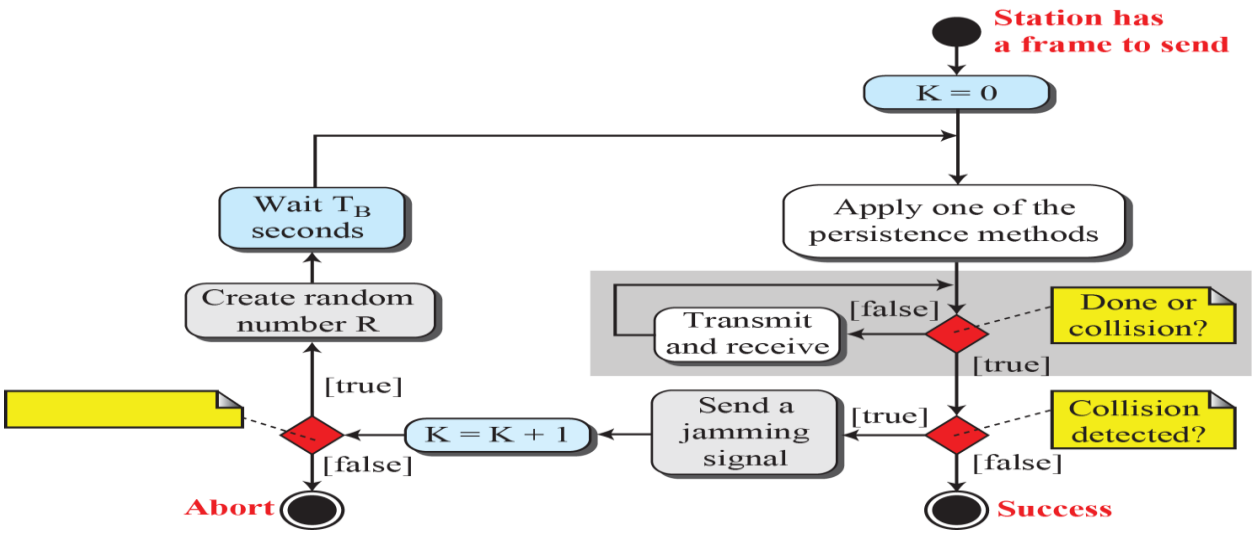
11.78

b. Explain CSMA/CD working with the help of flowchart. 6M

The CSMA method does not specify the procedure following a collision. Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.

In this method, 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.

- Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
- (CSMA/CD) augments the algorithm to handle the collision.
- a station monitors the medium after it sends a frame to see if the transmission was successful.
- If so, the station is finished. If, there is a collision, the frame is sent again.



c. List the characteristics of wireless LANS 4M

There are several characteristics of wireless LANs that either do not apply to wired LANs or the existence of which is negligible and can be ignored. We discuss some of these characteristics here to pave the way for discussing wireless LAN protocols.

Attenuation

The strength of electromagnetic signals decreases 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.

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.

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 objects. The result is that the receiver receives some signals at different phases (because they travel different paths). This makes the signal less recognizable.

Error

With the above characteristics of a wireless network, we can expect that errors and error detection are more serious issues in a wireless network than in a wired network. If we think about the error level as the measurement of signal-to-noise ratio (SNR), we can better understand why error detection and error correction and retransmission are more important in a wireless network. SNR measures the ratio of good stuff to bad stuff (signal to noise). If SNR is high, it means that the signal is stronger than the noise (unwanted signal), so we may be able to convert the signal to actual data. On the other hand, when SNR is low, it means that the signal is corrupted by the noise and the data cannot be recovered.

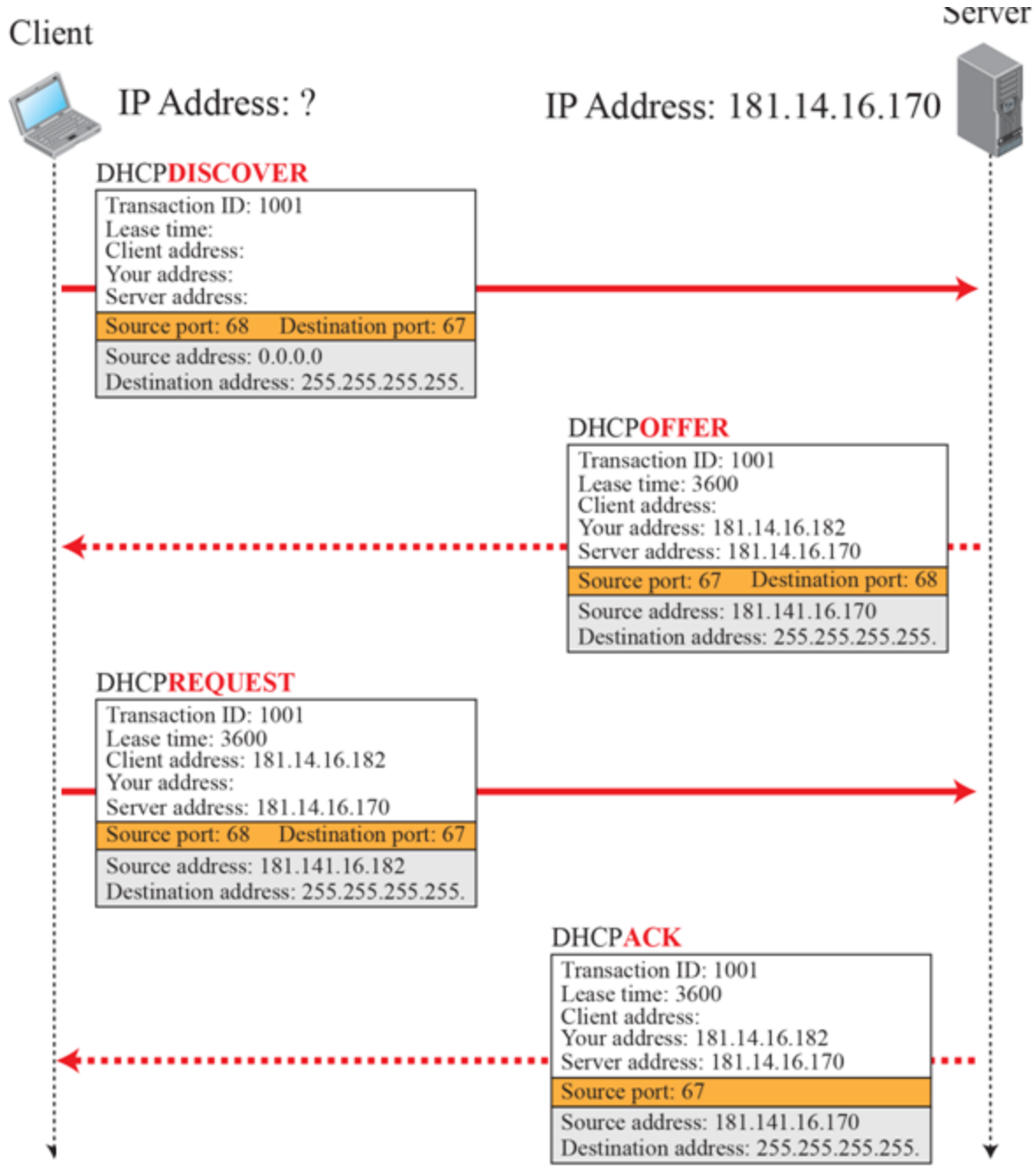
5 a. Explain working of DHCP 8M

After a block of addresses are assigned to an organization, the network administration can manually assign addresses to the individual hosts or routers.

However, address assignment in an organization can be done automatically using the Dynamic Host Configuration Protocol (DHCP).

DHCP is an application-layer program, using the client-server paradigm,

DHCP is a client-server protocol in which the client sends a request message and the server returns a response message



The joining host creates a DHCPDISCOVER message. The user datagram is encapsulated in an IP datagram with the source address set to 0.0.0.0 (“this host”) and the destination address set to 255.255.255.255 (broadcast address). The reason is that the joining host knows neither its own address nor the server address.

The DHCP server or servers (if more than one) responds with a DHCPOFFER message in which 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. the destination address is a broadcast address, in which the server allows other DHCP servers to receive the offer and give a better offer if they can.

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

Finally, the selected server responds with a DHCPACK message to the client if the offered IP address is valid. If the server cannot keep its offer (for example, if the address is offered to another host in between), the server sends a DHCPNACK message

b.Inpect the following MAC address 4M

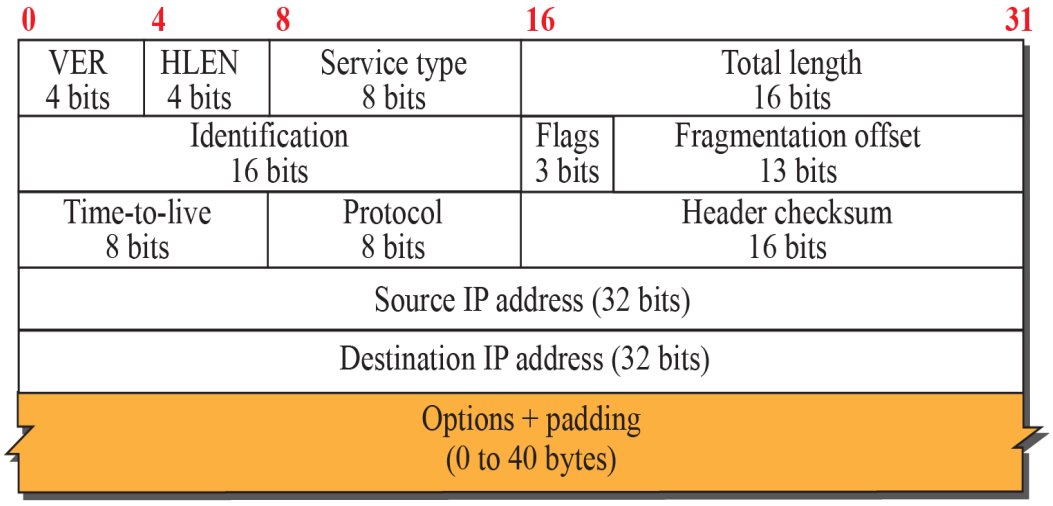
i) 4A:30:10:21:10:1A UNICASTING

2) 47:20:1B:2E:08:EE Multicasting

3) EF:FF:10:01:11:00MULTICASTING

4) FF:FF:FF:FF:FF:FF BROADCASTING

c. explain IPV4 datagram format with aneat diagram 8M



b. Header format

Version (VER). This 4-bit field defines the version of the IPv4 protocol. Currently the version is 4.

o Header length (HLEN). This 4-bit field defines the total length of the datagram header in 4 byte words. This field is needed because the length of the header is variable (between 20 and 60 bytes).

o Services. This field, previously called service type, is now called differentiated services.

The total length field defines the total length of the datagram including the header.

o Identification,Flags, Fragmentation offset.- used in fragmentation

Time to live. A datagram has a limited lifetime in its travel through an internet.

This field was originally designed to hold a timestamp, which was decremented by each visited router.

The datagram was discarded when the value became zero

Protocol. This 8-bit field defines the higher-level protocol that uses the services of the IPv4 layer. An IPv4 datagram can encapsulate data from several higher-level protocols such as TCP, UDP, ICMP, and IGMP. This field specifies the final destination protocol to which the IPv4 datagram is delivered

Checksum. The checksum

o Source address. This 32-bit field defines the IPv4 address of the source. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.

o Destination address. This 32-bit field defines the IPv4 address of the destination. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.

6. a. Explain simple implantation of NAT 10M

Many are not happy with one address; many have created small networks with several hosts and need an IP address for each host. With the shortage of addresses, this is a serious problem. A quick solution to this problem is called network address translation (NAT).

NAT enables a user to have a large set of addresses internally and one address, or a small set of addresses, externally.

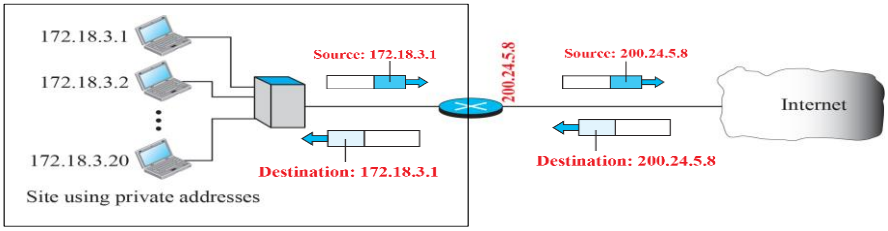
The traffic inside can use the large set; the traffic outside, the small set

In most situations, only a portion of computers in a small network need access to the Internet simultaneously.

A technology that can provide the mapping between the private and universal addresses, is Network Address Translation (NAT).

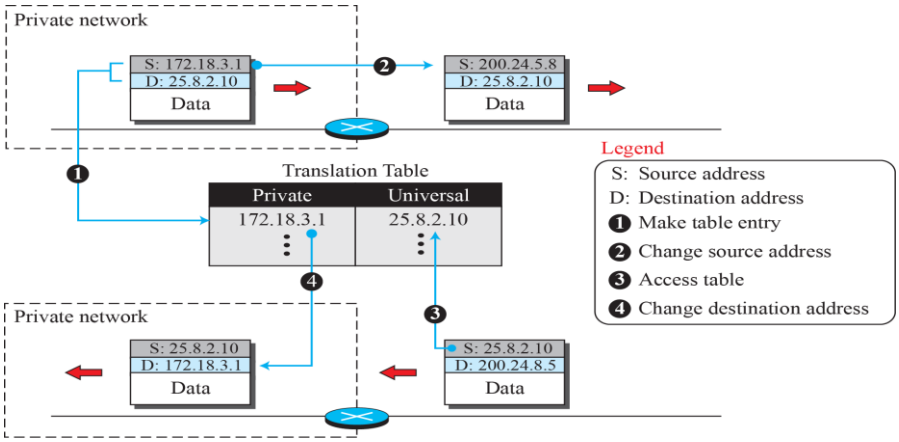
The technology allows a site to use a set of private addresses for internal communication and a set of global Internet addresses (at least one) for communication with the rest of the world.

Figure 18.30: Address translation



18.60

Figure 18.31: Translation



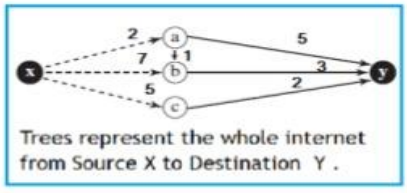
18.61

b. Explain distance vector algorithm using bellman ford equations 10M

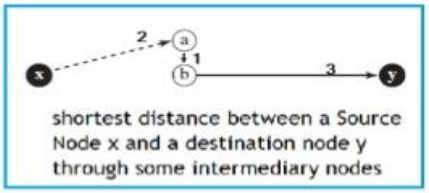
BELLMAN-FORD EQUATION

- Bellman-Ford 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.

- Equation $D_{xy} = \min\{(c_{xa} + D_{ay}), (c_{xb} + D_{by}), (c_{xc} + D_{cy}), (c_{xa} + c_{ab} + D_{by}), \ldots\ldots\}$



Trees represent the whole internet from Source X to Destination Y .



shortest distance between a Source Node x and a destination node y through some intermediary nodes

Figure 20.5: ***The first distance vector for an internet***

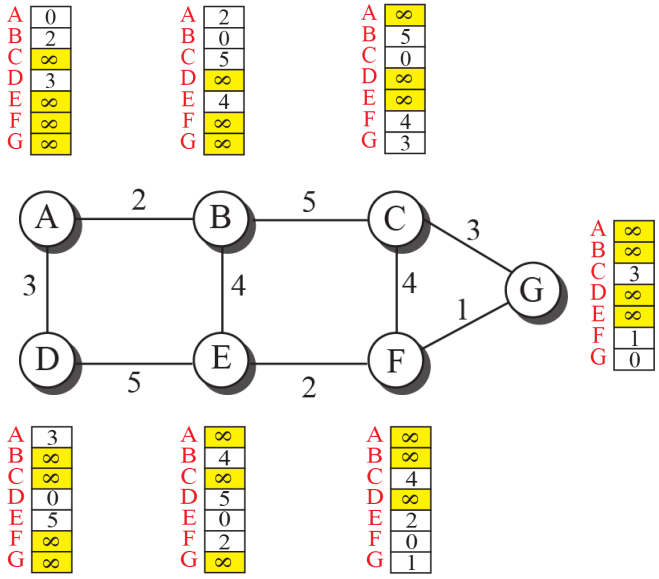
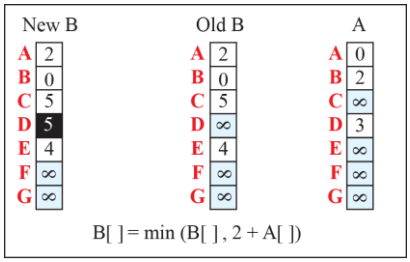
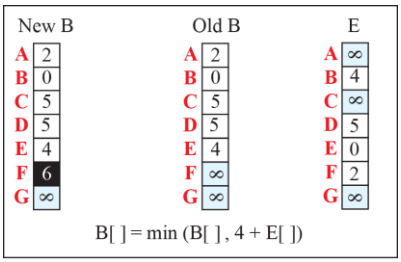


Figure 20.6: ***Updating distance vectors***



a. First event: B receives a copy of A's vector.

Note:
X[ ]: the whole vector

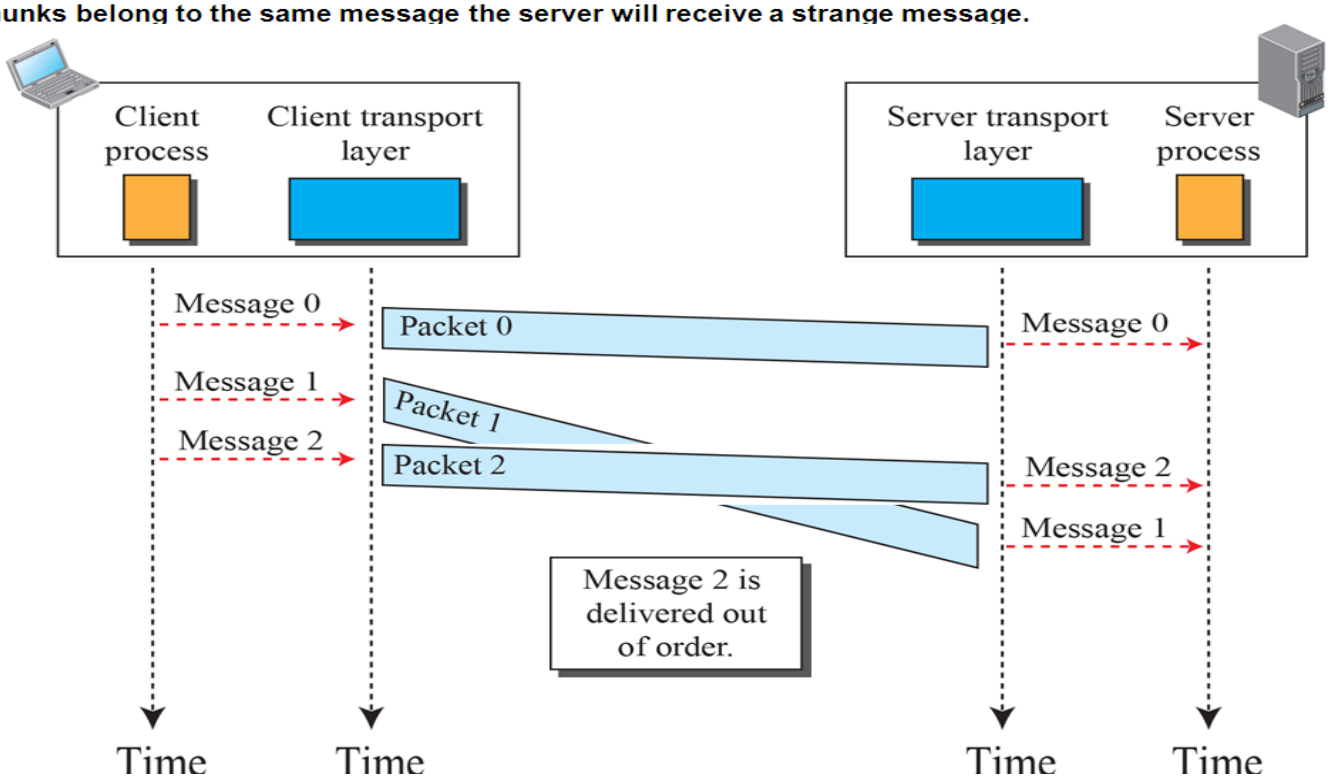


b. Second event: B receives a copy of E's vector.

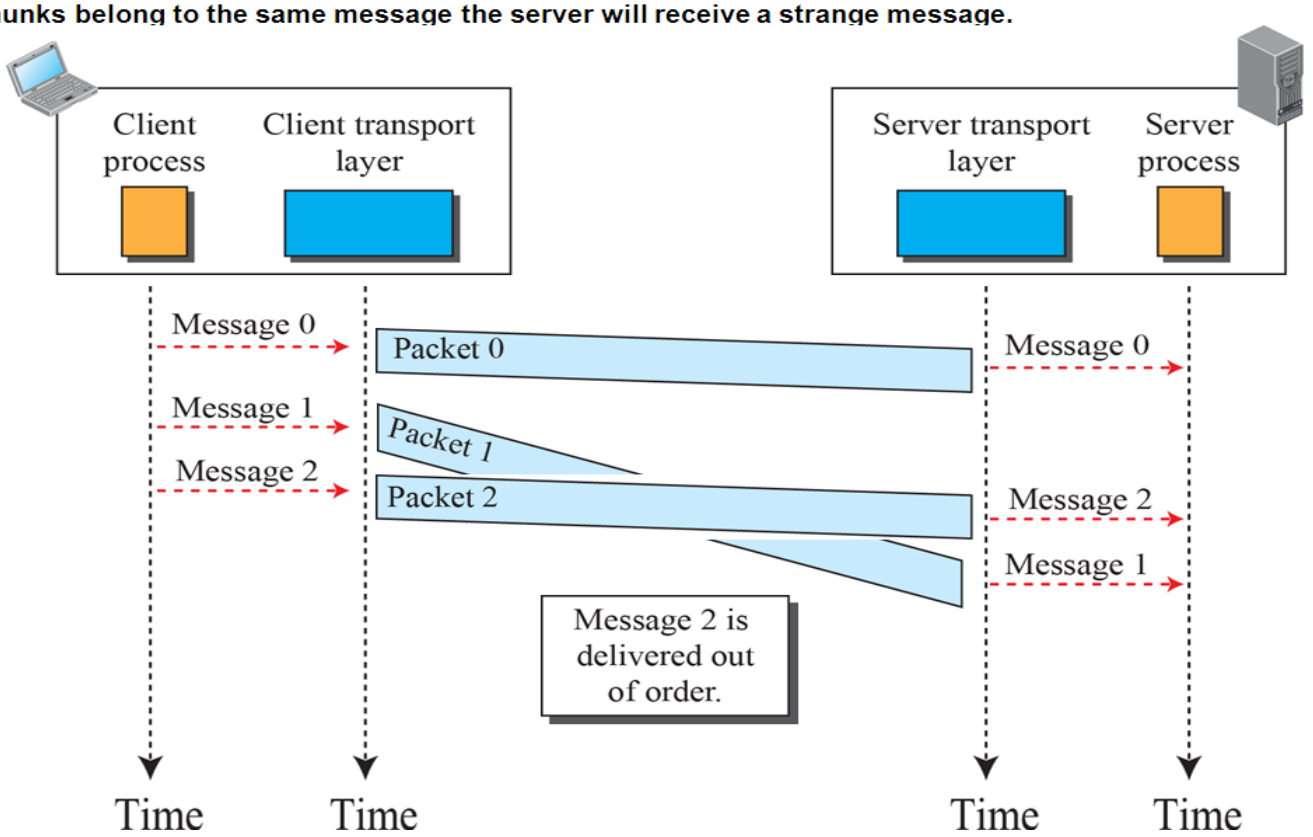
7. a Describe connections less and connection oriented servies provided by the transport layer. 14M

A transport-layer protocol, like a network-layer protocol, can provide two types of services: connectionless and connection-oriented.

Connectionless service- dividing the message in to chunks. T/L treats each chunks as independent unit. If 3 chunks belong to the same message the server will receive a strange message.



Connectionless service- dividing the message in to chunks. T/L treats each chunks as independent unit. If 3 chunks belong to the same message the server will receive a strange message.



b. Describe general services provided by UDP **6 M**

general services are provided by UDP.

1. Process to process communication using socket address
2. Connectionless services
3. No Flow control so no window mechanism
4. No error control

8a. Explain working of Go- Back- N protocol **10M**

To improve the efficiency of transmission (to fill the pipe), multiple packets must be in transition while the sender is waiting for acknowledgment.

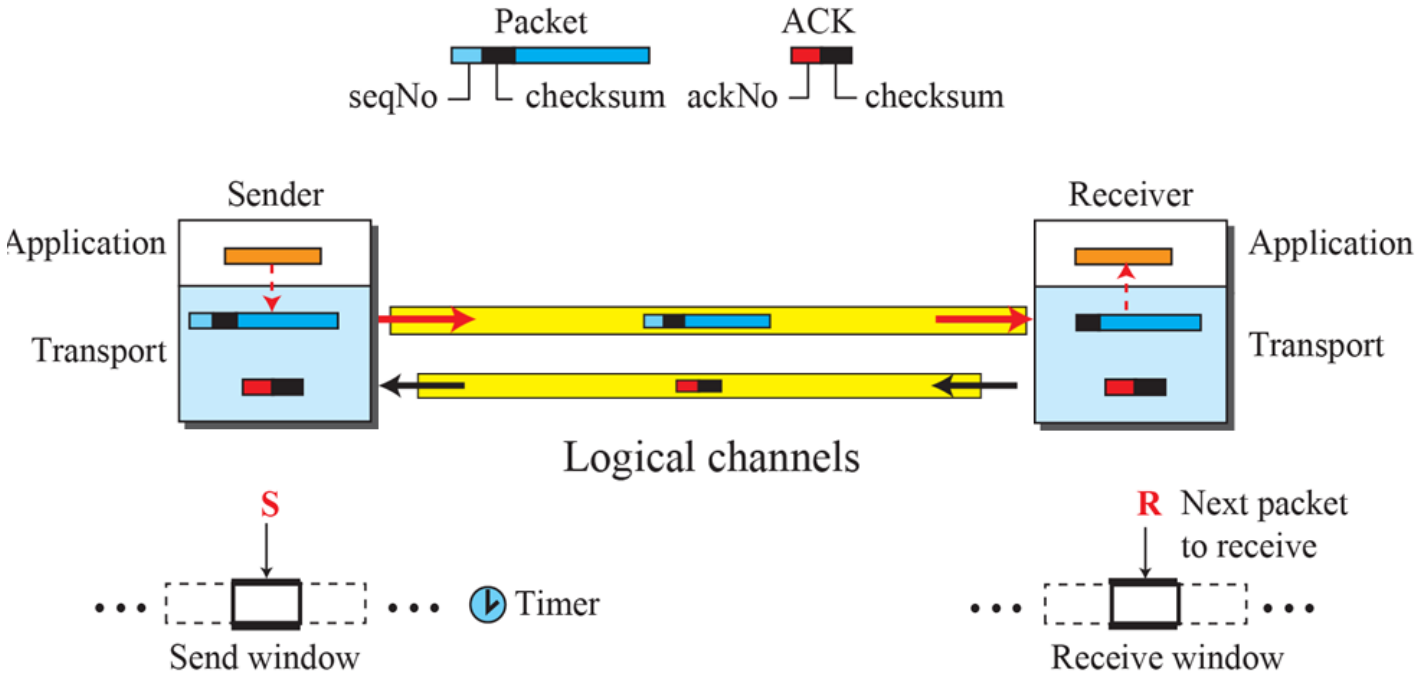
In other words, we need to let more than one packet be outstanding to keep the channel busy while the sender is waiting for acknowledgment.

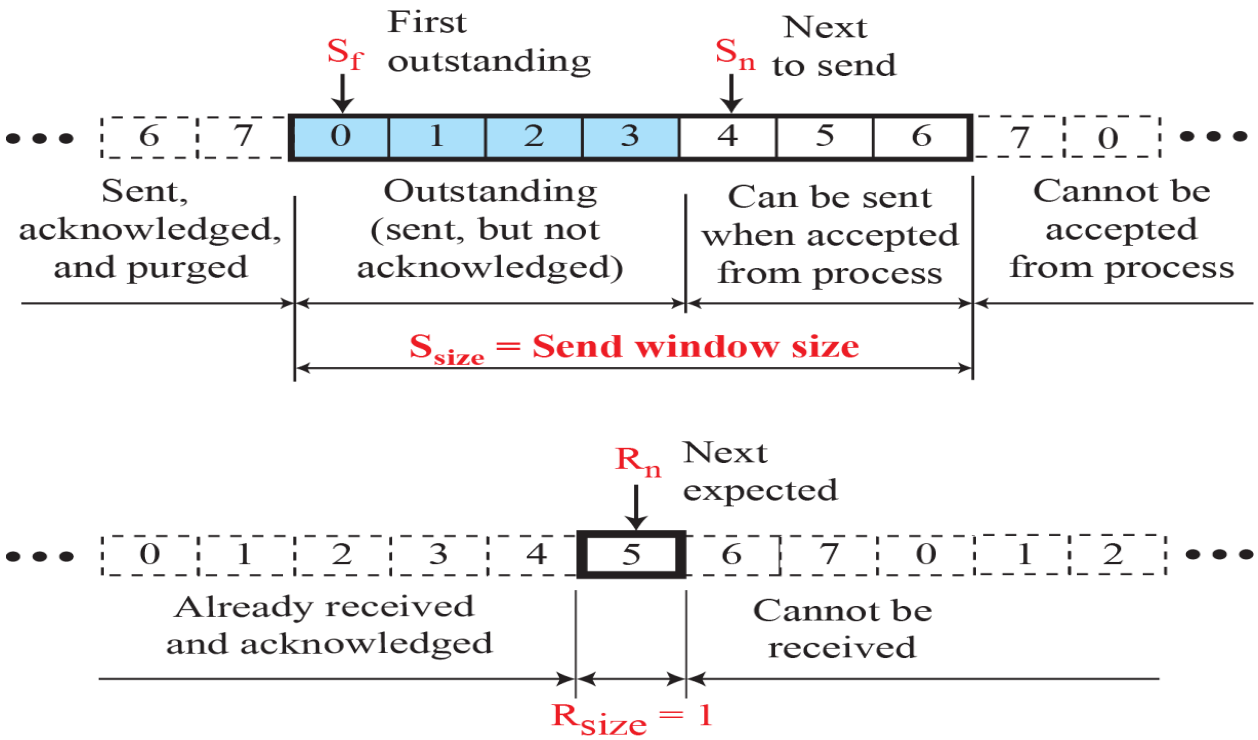
Ack.no. defines the seq.no. of the next packet expected

the sequence numbers are modulo 2^m, where m is the size of the sequence number field in bits.

Send window is an imaginary box of max. size= $2^m - 1$

Receive window is an imaginary box of size 1.

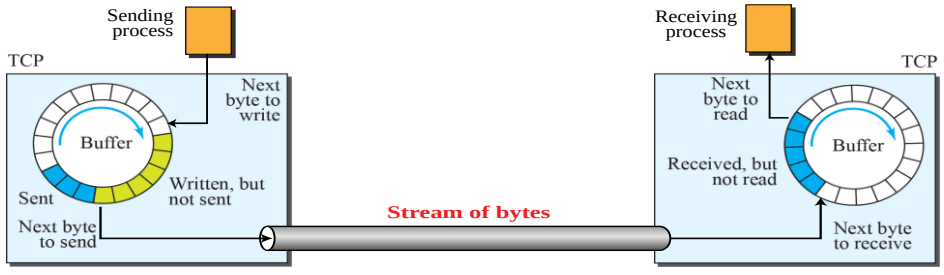




b. Describe sending and receiving buffers in TCP and explain how segments are created from the bytes in the buffers.

10M

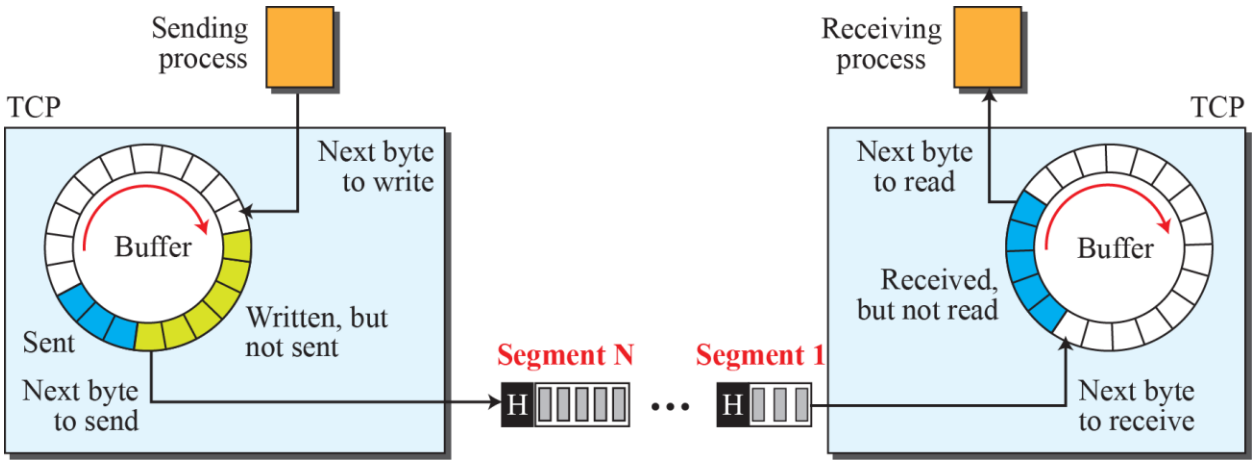
Figure 24.5: Sending and receiving buffers



TCP needs buffers for storage.

24.65

Because the sending and the receiving processes may not necessarily write or read data at the same rate, TCP needs buffers for storage. There are two buffers, the sending buffer and the receiving buffer, one for each direction



Although buffering handles the disparity between the speed of the producing and consuming processes, we need one more step before we can send data. The network layer, as a service provider for TCP, needs to send data in packets, not as a stream of bytes. At the

transport layer, TCP groups a number of bytes together into a packet called a segment. TCP adds a header to each segment (for control purposes) and delivers the segment to the network layer for transmission. The segments are encapsulated in an IP datagram and transmitted. This entire operation is transparent to the receiving process.

9. a. Explain architecture and format of electronic mail **10M**

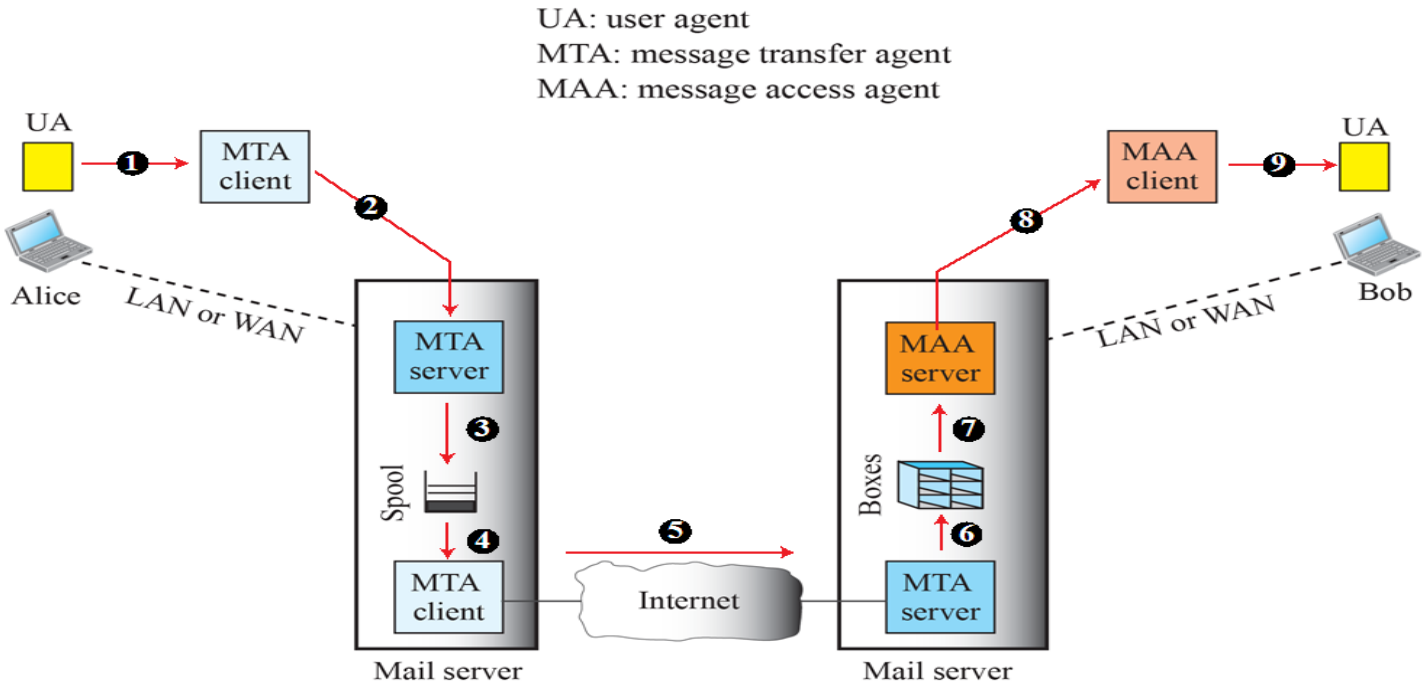
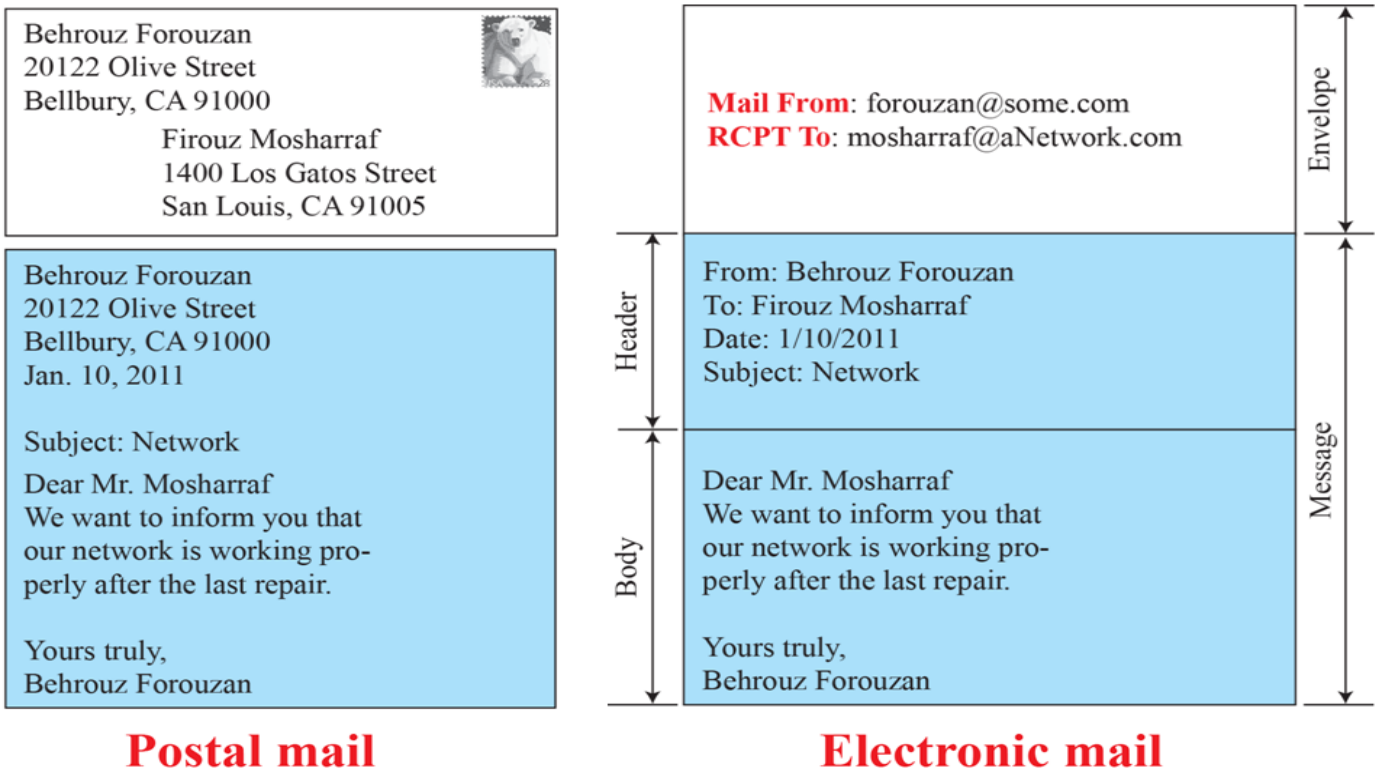
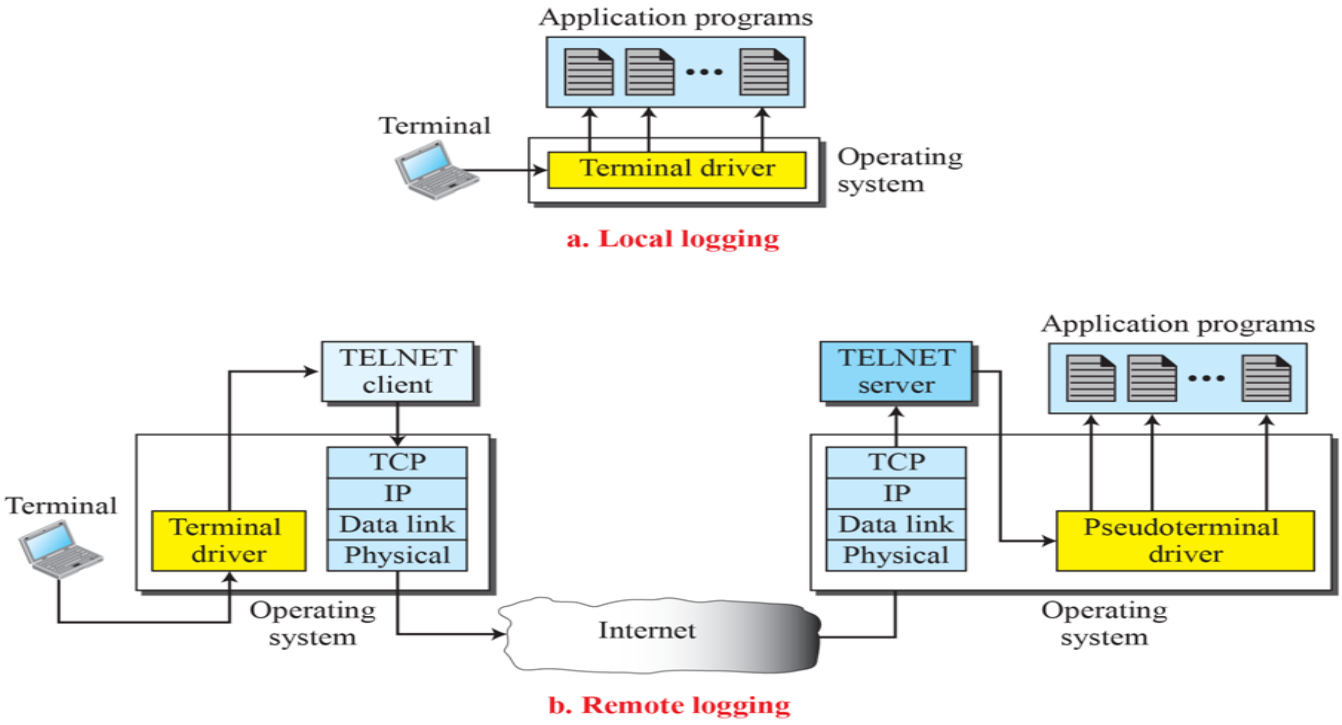


Figure 26.13: ***Format of an e-mail***



b. Distinguish local logging and remote logging **10M**

Figure 2.23: Local versus remote logging



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

Figure 26.3 shows an example of a nonpersistent connection. The client needs to access a file that contains one link to an image. The text file and image are located on the same server. Here we need two connections. For each connection, TCP requires at least three handshake messages to establish the connection, but the request can be sent with the third one. After the connection is established, the object can be transferred. After receiving an object, another three handshake messages are needed to terminate the connection

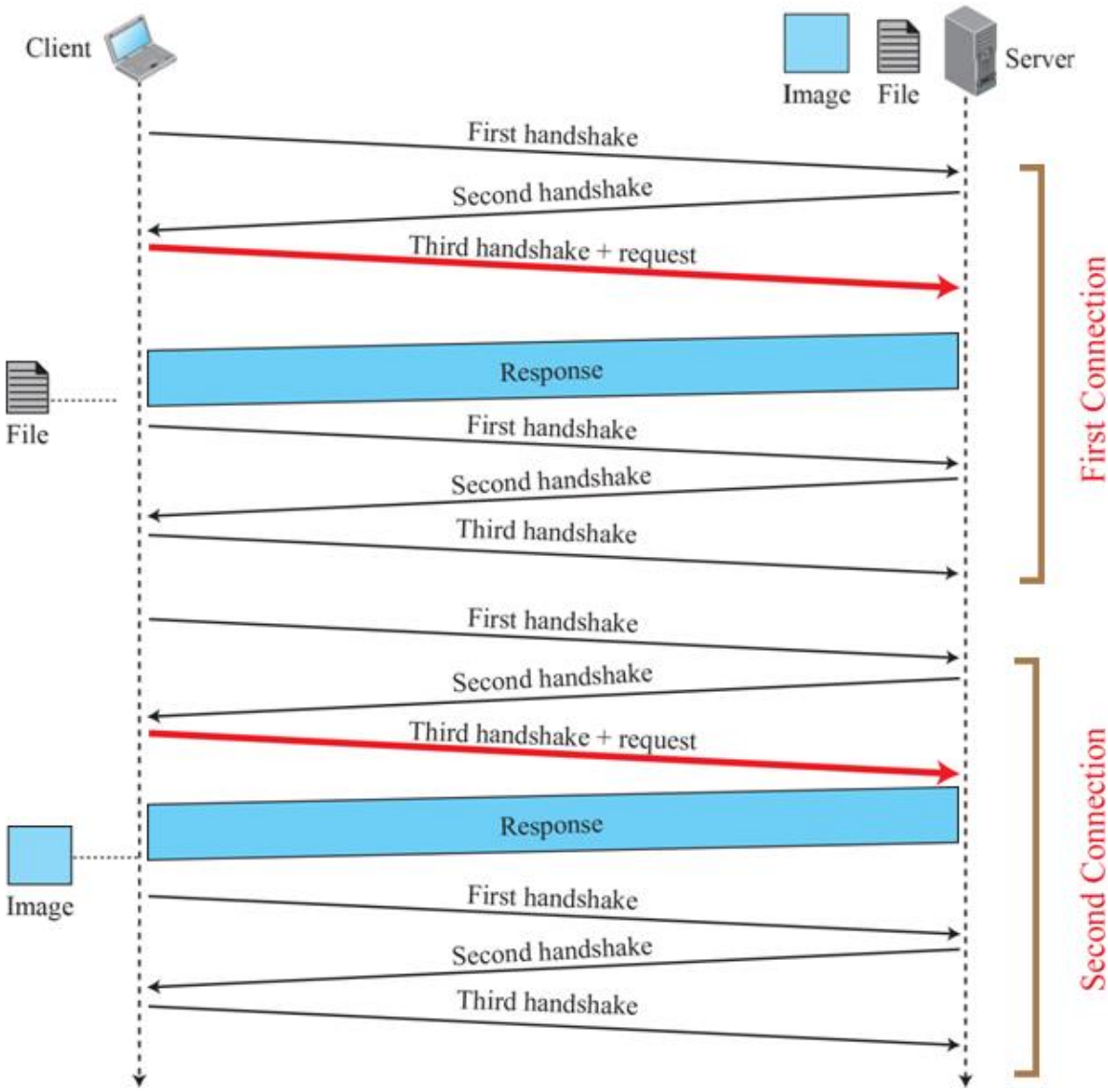
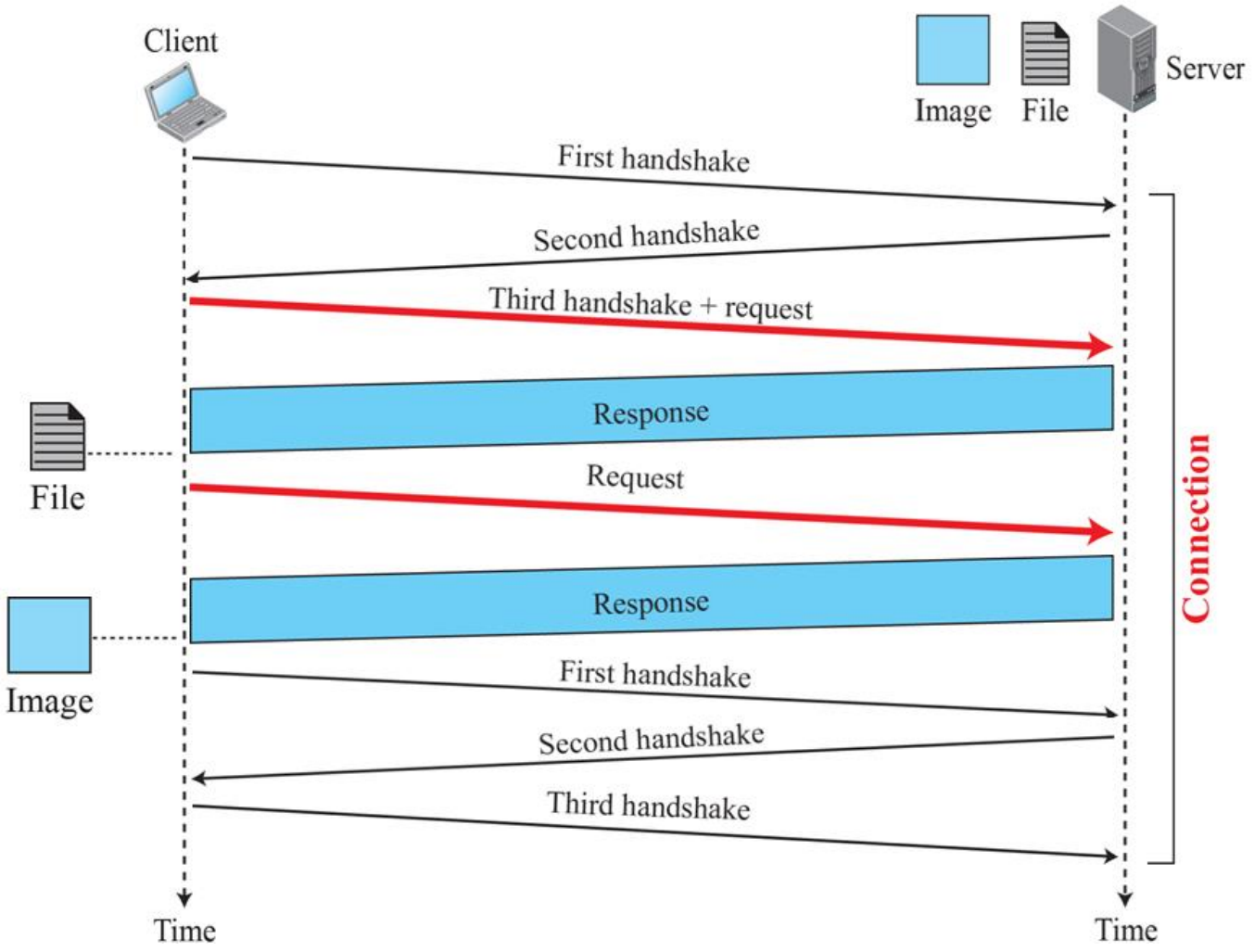


Figure 26.4 shows the same scenario as in Example 26.3, but using a persistent connection. Only one connection establishment and connection termination is used, but the request for the image is sent separately



b. Write a short note on DNS recursive and iterative resolutions

10 M

Mapping a name to an address is called name-address resolution. DNS is designed as a client-server application. A host that needs to map an address to a name or a name to an address calls a DNS client called a resolver. The resolver accesses the closest DNS server with a mapping request. If the server has the information, it satisfies the resolver; otherwise, it either refers the resolver to other servers or asks other servers to provide the information.

Figure 26.36: Recursive resolution

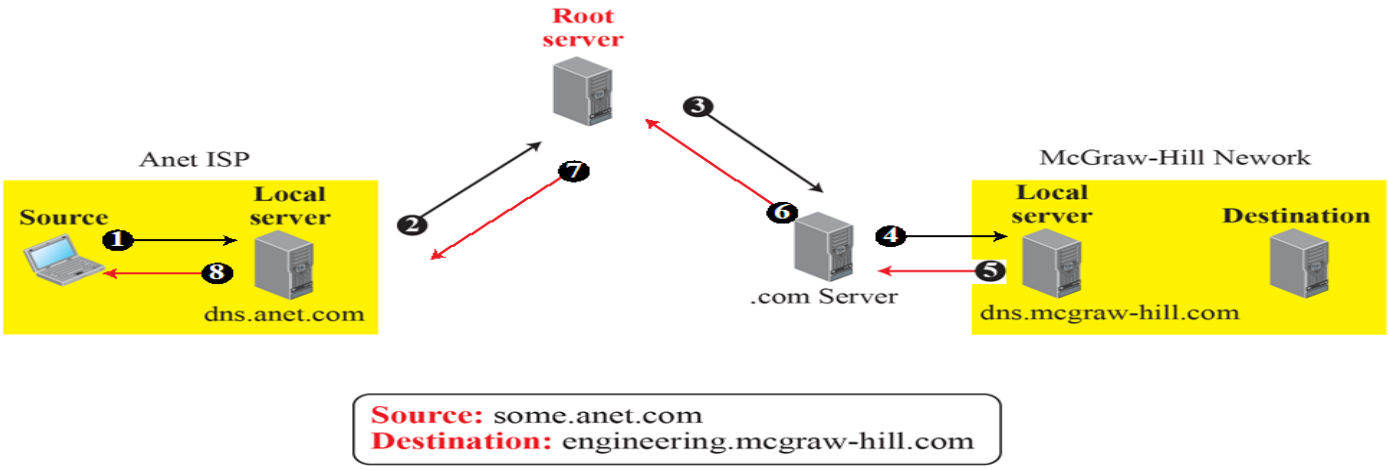


Figure 26.37: Iterative resolution