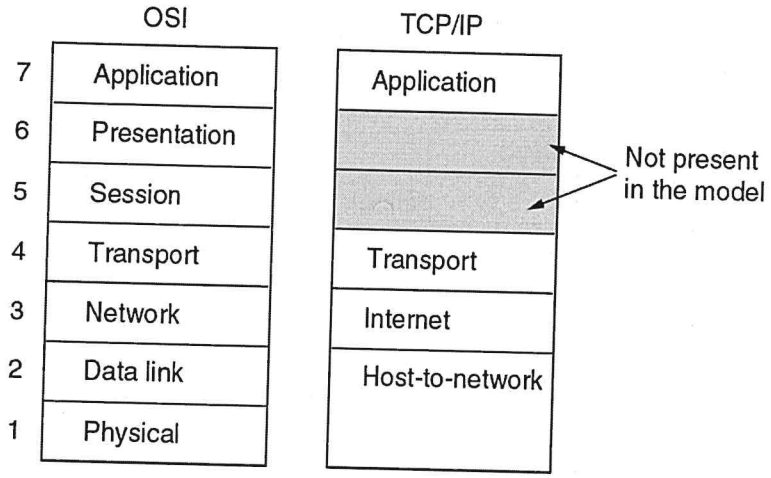
Shri Vile Parle Kelavani Mandal's
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING
(Autonomous College Affiliated to the University of Mumbai)
NAAC Accredited with "A" Grade (CGPA : 3.18)

Academic Year (2021-22)
Year: 2 Semester: IV
Program: B. Tech. (Computer Engg.)
Subject: Computer Networks
Date:
Max. Marks: 75
Time: 10: 30 am to 1:30 pm
Duration: 3 Hours

RE(EXAMINATION

ANSWER KEY

Question No.		Max. Marks
Q1 (a)	**The TCP/IP reference model**  **The Link Layer** • The lowest layer in the model, the link layer describes what links such as serial lines and classic Ethernet must do to meet the needs of this connectionless internet layer. • It is not really a layer at all, in the normal sense of the term, but rather an interface between hosts and transmission links. **The Internet Layer** • Its job is to permit hosts to inject packets into any network and have them travel independently to the destination (potentially on a different network). • They may even arrive in a completely different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired. **The Transport Layer** • The layer above the internet layer in the TCP/IP model is now usually called the transport layer. • It is designed to allow peer entities on the source and destination hosts to carry on a	[5]

conversation, just as in the OSI transport layer.

- Two end-to-end transport protocols have been defined here.

The Application Layer

- On top of the transport layer is the application layer.
- It contains all the higher-level protocols.
- The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP).
- Domain Name System (DNS), for mapping host names onto their network addresses, HTTP, the protocol for fetching pages on the World Wide Web, and RTP, the protocol for delivering real-time media such as voice or movies.

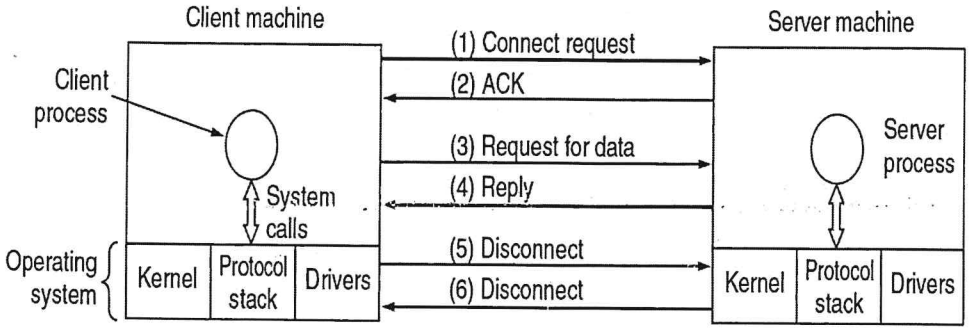
OR

i. **Service Primitives**

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

[2]

Five service primitives for implementing a simple connection-oriented service.



ii. **Protocol:** a protocol is an agreement between the communicating parties on how communication is to proceed.

To reduce their design complexity, most networks are organized as a **stack of layers or levels**, each one built upon the one below it.

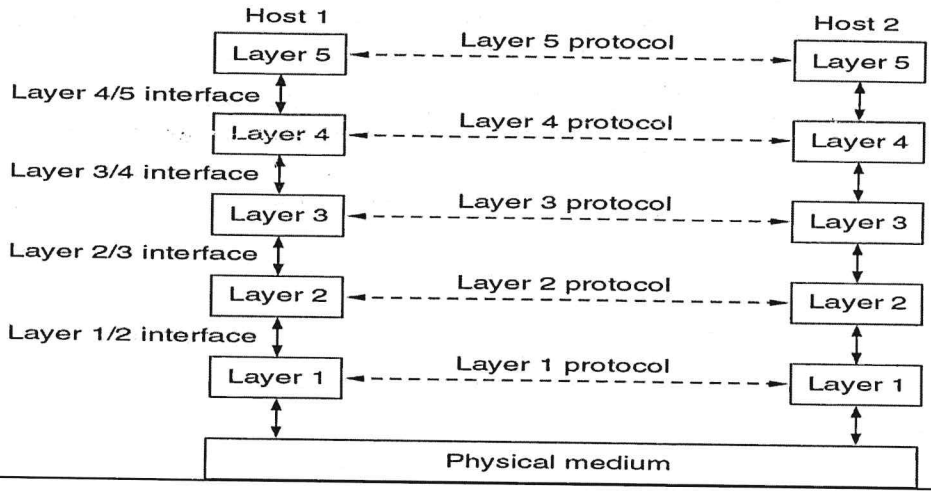
[3]

The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network.

The purpose of each layer is to offer certain services to the higher layers while shielding those layers from the details of how the offered services are actually implemented.

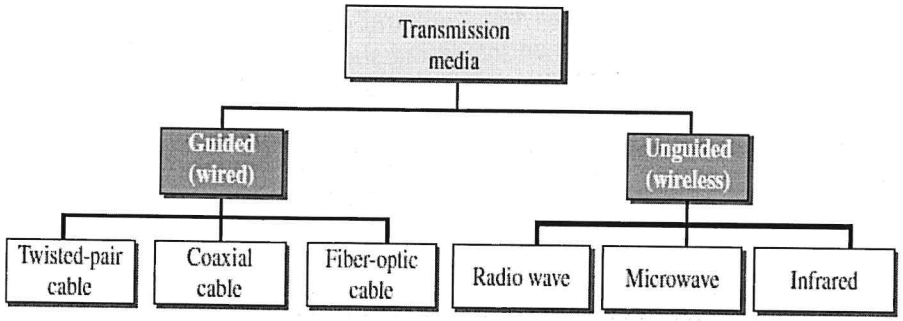
In a sense, each layer is a kind of virtual machine, offering certain services to the layer above it.

When **layer n** on one machine carries on a conversation with **layer n** on another machine, the rules and conventions used in this conversation are collectively known as the **layer n protocol.**



Q1 (b)

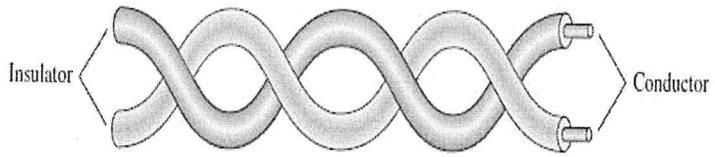
Major classes of guided media



[10]

- Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable.
- A signal traveling along any of these media is directed and contained by the physical limits of the medium.
- Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current.
- Optical fiber is a cable that accepts and transports signals in the form of light.

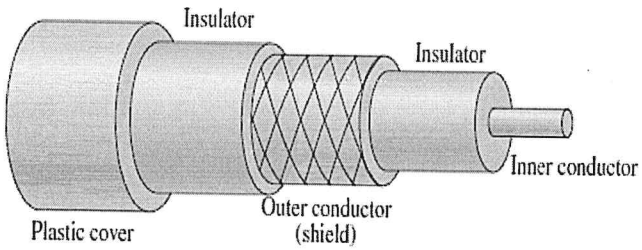
Twisted-Pair Cable



- A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together.
- One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference.
- The receiver uses the difference between the two.
- In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals.
- If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources
- (e.g., one is closer and the other is farther). This results in a difference at the receiver.
- By twisting the pairs, a balance is maintained.
- For example, suppose in one twist, one wire is closer to the noise source and the other is farther; in the next twist, the reverse is true.
- Twisting makes it probable that both wires are equally affected by external influences (noise or crosstalk).

Coaxial Cable

- Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted-pair cable, in part because the two media are constructed quite differently.
- Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two.
- The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit.
- This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.

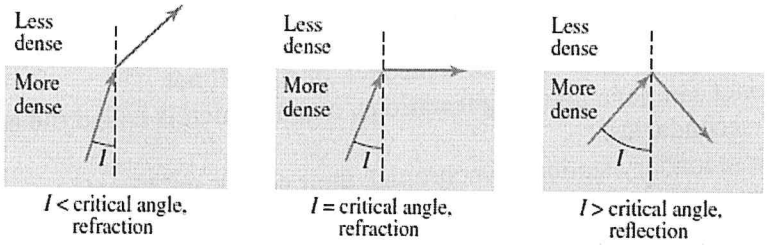


Fiber-Optic Cable

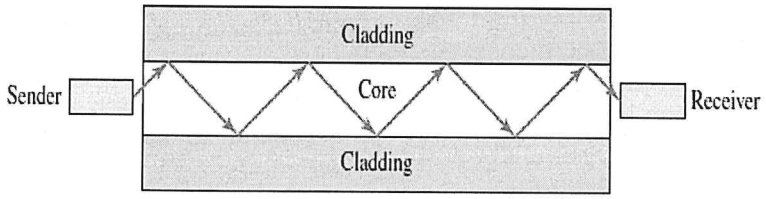
- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- To understand optical fiber, we first need to explore several aspects of the nature of light.
- Light travels in a straight line as long as it is moving through a single uniform substance.
- If a ray of light traveling through one substance suddenly enters another substance (of

a different density), the ray changes direction.

- Figure shows how a ray of light changes direction when going from a more dense to a less dense substance.



- As the figure shows, if the angle of incidence I (the angle the ray makes with the line perpendicular to the interface between the two substances) is less than the critical angle, the ray refracts and moves closer to the surface.
- If the angle of incidence is equal to the critical angle, the light bends along the interface.
- If the angle is greater than the critical angle, the ray reflects (makes a turn) and travels again in the denser substance.
- Optical fibers use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic.
- The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.



Q2 (a)

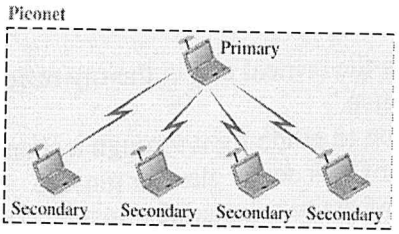
i. Bluetooth Architecture [6]

- Bluetooth defines two types of networks: piconet and scatternet.

Piconets:

- A Bluetooth network is called a piconet, or a small net.
- A piconet can have up to eight stations, one of which is called the primary; the rest are called secondaries.
- All the secondary stations synchronize their clocks and hopping sequence with the primary.
- The communication between the primary and secondary stations can be one-to-one or one-to-many.

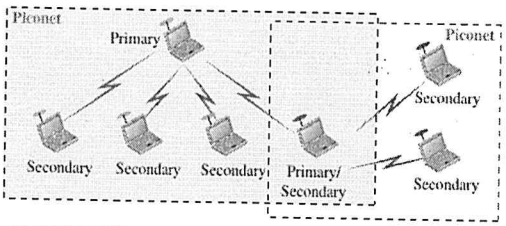
Figure 15.17 *Piconet*



Scatternet

- Piconets can be combined to form what is called a scatternet.
- A secondary station in one piconet can be the primary in another piconet.
- This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet.
- A station can be a member of two piconets.
- Figure illustrates a scatternet.

Figure 15.18 *Scatternet*



ii. The advantages of optical fiber over twisted-pair and coaxial cable [4]

– **Greater Bandwidth**

Copper cables were originally designed for voice transmission and have a limited bandwidth. Fiber optic cables provide more bandwidth for carrying more data than copper cables of the same diameter. Within the fiber cable family, single mode fiber delivers up to twice the throughput of multimode fiber.

- **Faster Speeds**

Fiber optic cables have a core that carries light to transmit data. This allows fiber optic cables to carry signals at speeds that are only about 31 percent slower than the speed of light—faster than Cat5 or Cat6 copper cables. There is also less signal degradation with fiber cables.

- **Longer Distances**

Fiber optic cables can carry signals much farther than the typical 328-foot limitation for copper cables. For example, some 10 Gbps single mode fiber cables can carry signals almost 25 miles. The actual distance depends on the type of cable, the wavelength and the network.

- **Better Reliability**

Fiber is immune to temperature changes, severe weather and moisture, all of which can hamper the connectivity of copper cable. Plus, fiber does not carry electric current, so it's not bothered by electromagnetic interference (EMI) that can interrupt data transmission. It also does not present a fire hazard like old or worn copper cables can.

OR

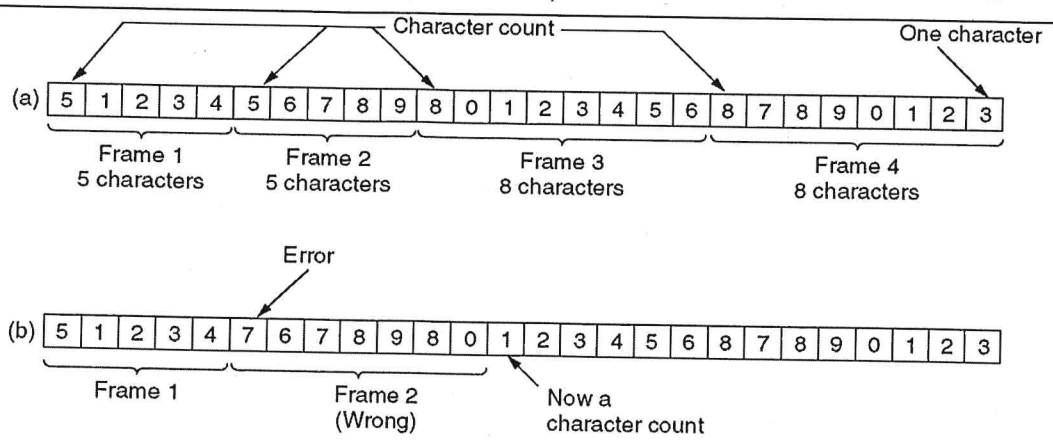
Framing:

The data link layer, on the other hand, needs to pack bits into frames, so that each frame is distinguishable from another. [10]

- **There are four methods of Framing**
  - Character count
  - Flag bytes with byte stuffing.
  - Starting and ending flags, with bit stuffing.
  - Physical layer coding violations

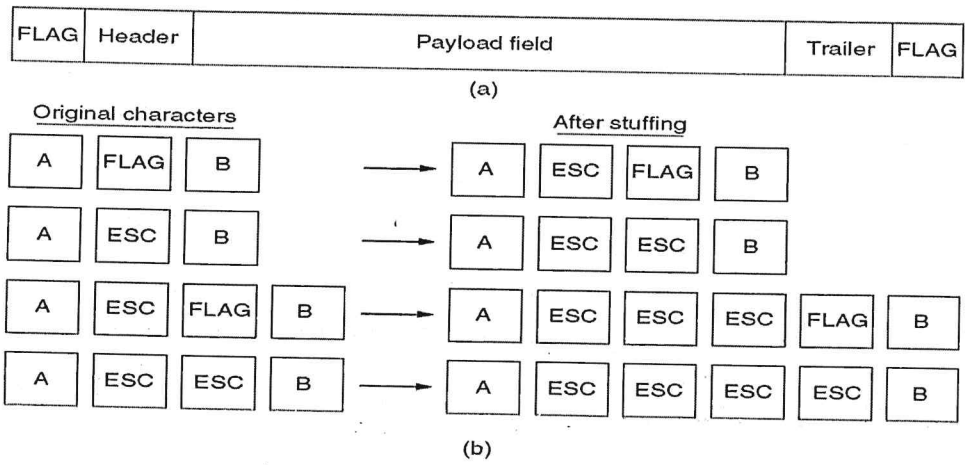
Character count

- The first framing method uses a field in the header to specify the number of characters in the frame.
- When the data link layer at the destination sees the character count, it knows how many characters follow and hence where the end of the frame is.



Flag bytes with byte stuffing

- The second framing method gets around the problem of resynchronization after an error by having each frame start and end with special bytes.
- In the past, the starting and ending bytes were different, but in recent years most protocols have used the same byte, called a flag byte, as both the starting and ending delimiter, as shown in Fig. as FLAG.
- In this way, if the receiver ever loses synchronization, it can just search for the flag byte to find the end of the current frame. Two consecutive flag bytes indicate the end of one frame and start of the next one.



- A serious problem occurs with this method when binary data, such as object programs or floating-point numbers, are being transmitted.
- It may easily happen that the flag byte's bit pattern occurs in the data.
- This situation will usually interfere with the framing.
- One way to solve this problem is to have the sender's data link layer insert a special escape byte (ESC) just before each "accidental" flag byte in the data.
- The data link layer on the receiving end removes the escape byte before the data are given to the network layer.
- This technique is called **byte stuffing or character stuffing.**
- Thus, a framing flag byte can be distinguished from one in the data by the absence

or presence of an escape byte before it.

Starting and ending flags, with bit stuffing

- The new technique allows data frames to contain an arbitrary number of bits and allows character codes with an arbitrary number of bits per character.
- It works like this.
- Each frame begins and ends with a special bit pattern, 01111110 (in fact, a flag byte).
- Whenever the sender's data link layer encounters five consecutive 1s in the data, it automatically stuffs a 0 bit into the outgoing bit stream.
- This bit stuffing is analogous to byte stuffing, in which an escape byte is stuffed into the outgoing character stream before a flag byte in the data.
- When the receiver sees five consecutive incoming 1 bits, followed by a 0 bit, it automatically destuffs (i.e., deletes) the 0 bit.
- Just as byte stuffing is completely transparent to the network layer in both computers, so is bit stuffing.
- If the user data contain the flag pattern, 01111110, this flag is transmitted as 011111010 but stored in the receiver's memory as 01111110. Figure gives an example of bit stuffing

(a) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

(b) 0 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 0 0 1 0

Stuffed bits

(c) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

Physical layer coding violations

- The last method of framing is only applicable to networks in which the encoding on the physical medium contains some redundancy.
- For example, some LANs encode 1 bit of data by using 2 physical bits.
- Normally, a 1 bit is a high-low pair and a 0 bit is a low-high pair.
- The scheme means that every data bit has a transition in the middle, making it easy for the receiver to locate the bit boundaries.
- The combinations high-high and low-low are not used for data but are used for delimiting frames in some protocols.

Q2 (b)	**The services provided by data link layer to the network layer.** • The function of the data link layer is to provide services to the network layer. • The principal service is transferring data from the network layer on the source machine to the network layer on the destination machine. • On the source machine is an entity, call it a process, in the network layer that hands	[5]

some bits to the data link layer for transmission to the destination.

- The job of the data link layer is to transmit the bits to the destination machine so they can be handed over to the net- work layer there, as shown in Fig. (a).
- The actual transmission follows the path of Fig.(b), but it is easier to think in terms of two data link layer processes communicating using a data link protocol.

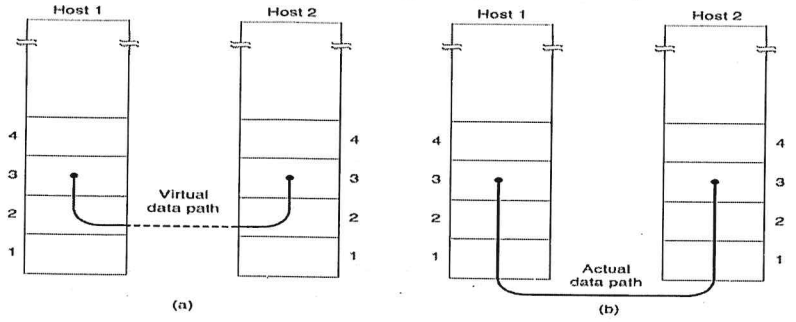


Figure 3-2. (a) Virtual communication. (b) Actual communication.

- Three reasonable possibilities that we will consider in turn are:
  - Unacknowledged connectionless service.
  - Acknowledged connectionless service.
  - Acknowledged connection-oriented service.

Unacknowledged connectionless service

- It consists of having the source machine send independent frames to the destination machine without having the destination machine acknowledge them.
- Ethernet is a good example of a data link layer that provides this class of service.
- No logical connection is established beforehand or released afterward.
- If a frame is lost due to noise on the line, no attempt is made to detect the loss or recover from it in the data link layer.

Acknowledged connectionless service

- The next step up in terms of reliability is acknowledged connectionless service.
- When this service is offered, there are still no logical connections used, but each frame sent is individually acknowledged.
- In this way, the sender knows whether a frame has arrived correctly or been lost.
- If it has not arrived within a specified time interval, it can be sent again.
- This service is useful over unreliable channels, such as wireless systems.
- 802.11 (WiFi) is a good example of this class of service.

Acknowledged connection-oriented service

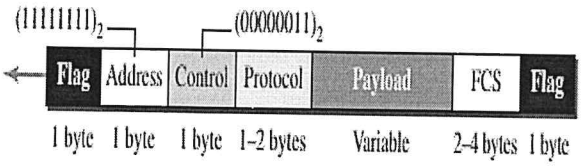
- The most sophisticated service the data link layer can provide to the network layer is connection-oriented service.
- With this service, the source and destination machines establish a connection before any data are transferred.
- Each frame sent over the connection is numbered, and the data link layer guarantees that each frame sent is indeed received.
- Furthermore, it guarantees that each frame is received exactly once and that all frames are received in the right order.
- Connection-oriented service thus provides the network layer processes with the equivalent of a reliable bit stream.
- It is appropriate over long, unreliable links such as a satellite channel or a long-distance telephone circuit.

Q3 (a)

Point-to-Point Protocol (PPP) frame format. [5]

- PPP uses a character-oriented (or byte-oriented) frame. Figure shows the format of a PPP frame. The description of each field follows:

Figure 11.20 *PPP frame format*

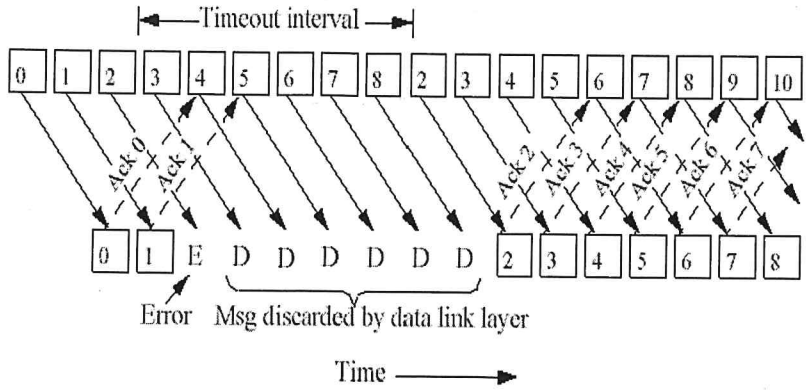


- **Flag.** A PPP frame starts and ends with a 1-byte flag with the bit pattern 01111110.
- **Address.** The address field in this protocol is a constant value and set to 11111111 (broadcast address).
- **Control.** This field is set to the constant value 00000011 (imitating unnumbered frames in HDLC).
- **Protocol.** The protocol field defines what is being carried in the data field: either user data or other information.
- This field is by default 2 bytes long, but the two parties can agree to use only 1 byte.
- **Payload field.** This field carries either the user data or other information that we will discuss shortly.
- The data field is a sequence of bytes with the default of a maximum of 1500 bytes; but this can be changed during negotiation.
- The data field is byte-stuffed if the flag byte pattern appears in this field.
- Because there is no field defining the size of the data field, padding is needed if the size is less than the maximum default value or the maximum negotiated value.
- **FCS.** The frame check sequence (FCS) is simply a 2-byte or 4-byte standard CRC.

OR

Go Back N Sliding Window protocol. [5]

- The sliding window method using cumulative ACK is known as the Go-Back-N protocol.
- Receiver window size is 1.
- In this method, if one frame is lost or damaged all frames sent, since the last frame acknowledged are retransmitted.
- For example, sender may send frames 1,2,3,4 and get an NAK with a value of 2.
- The NAK acknowledges everything that came before it, and asks for frame 2 (and subsequent frames) to be resent.
- NAK number refer to the next expected frame number.
- Example: In the following figure, frame 2 has an error, then all subsequent frames are discarded.
- After timeout sender sends all frames from frame 2.



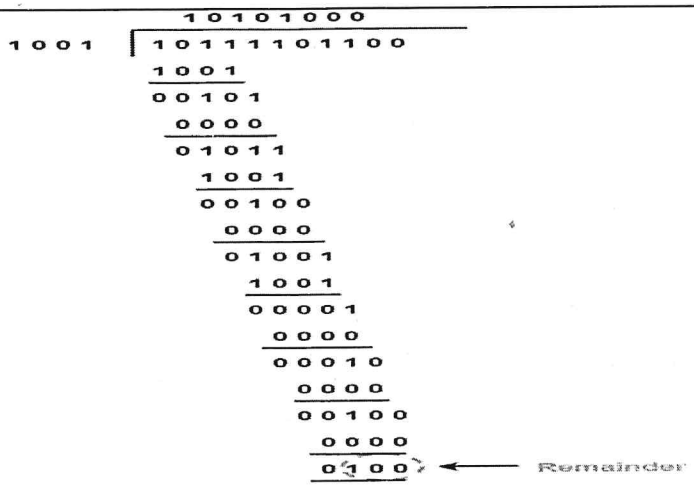
Q3 (b)

[10]

- **Part-01:**
  - The generator polynomial $G(x) = x^3 + 1$ is encoded as 1001.
  - Clearly, the generator polynomial consists of 4 bits.
  - So, a string of 3 zeroes is appended to the bit stream to be transmitted.
  - The resulting bit stream is 10011101000.
  - Now, the binary division is performed as-

```
          1 0 0 0 1 1 0 0
      ┌──────────────────
1 0 0 1 | 1 0 0 1 1 1 0 1 0 0 0
        1 0 0 1
        ---------
        0 0 0 0 1
          0 0 0 0
          ---------
          0 0 0 1 1
            0 0 0 0
            ---------
            0 0 1 1 0
              0 0 0 0
              ---------
              0 1 1 0 1
                1 0 0 1
                ---------
                0 1 0 0 0
                  1 0 0 1
                  ---------
                  0 0 0 1 0
                    0 0 0 0
                    ---------
                    0 0 1 0 0
                      0 0 0 0
                      ---------
                      0 1 0 0   <-- CRC
```

- From here, CRC = 100.
- Now,
- The code word to be transmitted is obtained by replacing the last 3 zeroes of 10011101000 with the CRC.
- Thus, the code word transmitted to the receiver = 10011101100.
- **Part-02:**
- According to the question,
- Third bit from the left gets inverted during transmission.
- So, the bit stream received by the receiver = 10111101100.
- Now,
- Receiver receives the bit stream = 10111101100.
- Receiver performs the binary division with the same generator polynomial as-



- From here,
  - The remainder obtained on division is a non-zero value.
  - This indicates to the receiver that an error occurred in the data during the transmission.
  - Therefore, receiver rejects the data and asks the sender for retransmission.

OR

[10]

High-level Data Link Control (HDLC) Protocol

- High-level Data Link Control (HDLC) is a bit-oriented protocol for communication over point-to-point and multipoint links.
- It implements the Stop-and-Wait protocol.
- Although this protocol is more a theoretical issue than practical, most of the concept defined in this protocol is the basis for other practical protocols such as PPP.

Configurations and Transfer Modes

- HDLC provides two common transfer modes that can be used in different configurations:
  - normal response mode (NRM) and
  - asynchronous balanced mode (ABM).
- In normal response mode (NRM), the station configuration is unbalanced.
- We have one primary station and multiple secondary stations.
- A primary station can send commands; a secondary station can only respond.
- The NRM is used for both point-to-point and mul- tipoint links.

Figure 11.14 *Normal response mode*

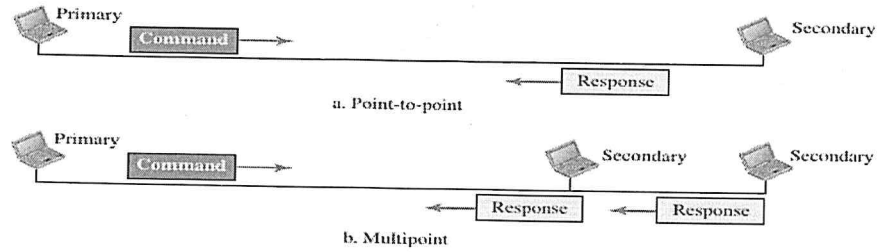
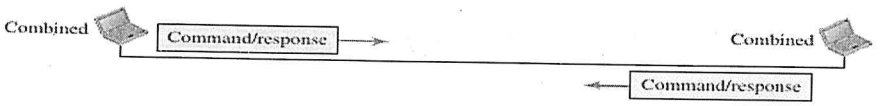
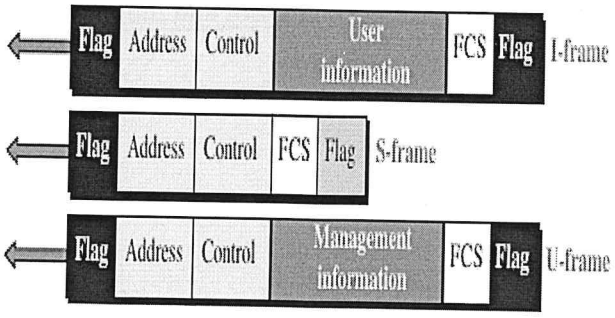


Figure 11.15 *Asynchronous balanced mode*



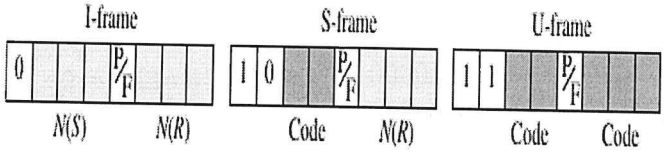
- **Framing**
- To provide the flexibility necessary to support all the options possible in the modes and configurations just described, HDLC defines three types of frames: information frames (I-frames), supervisory frames (S-frames), and unnumbered frames (U-frames).
- Each type of frame serves as an envelope for the transmission of a different type of message.
- I-frames are used to data-link user data and control information relating to user data (piggy- backing).
- S-frames are used only to transport control information. U-frames are reserved for system management. Information carried by U-frames is intended for managing the ink itself.
- Each frame in HDLC may contain up to six fields, as shown in Figure 11.16: a beginning flag field, an address field, a control field, an information field, a frame check sequence (FCS) field, and an ending flag field.
- In multiple-frame transmissions, the ending flag of one frame can serve as the beginning flag of the next frame.

Figure 11.16 *HDLC frames*



- **Flag field.** This field contains synchronization pattern 01111110, which identifies both the beginning and the end of a frame.
- **Address field.** This field contains the address of the secondary station.
- If a primary station created the frame, it contains a to address. If a secondary station creates the frame, it contains a from address.
- The address field can be one byte or several bytes long, depending on the needs of the network.
- **Control field.** The control field is one or two bytes used for flow and error control.
- **Information field.** The information field contains the user's data from the network layer or management information. Its length can vary from one network to another.
- **FCS field.** The frame check sequence (FCS) is the HDLC error detection field.
- It can contain either a 2- or 4-byte CRC.
- The control field determines the type of frame and defines its functionality.
- The format is specific for the type of frame, as shown in Figure.

Figure 11.17 *Control field format for the different frame types*



Control Field for I-Frames

- I-frames are designed to carry user data from the network layer. In addition, they can include flow- and error-control information (piggybacking).
- The subfields in the control field are used to define these functions.
- The first bit defines the type.
- If the first bit of the control field is 0, this means the frame is an I-frame.
- The next 3 bits, called N(S), define the sequence number of the frame.
- Note that with 3 bits, we can define a sequence number between 0 and 7.

Control Field for I-Frames

- The last 3 bits, called N(R), correspond to the acknowledgment number when piggybacking is used.
- The single bit between N(S) and N(R) is called the P/F bit.
- The P/F field is a single bit with a dual purpose.
- It has meaning only when it is set (bit = 1) and can mean poll or final. It means poll when the frame is sent by a primary station to a secondary (when the address field contains the address of the receiver).
- It means final when the frame is sent by a secondary to a primary (when the address field contains the address of the sender).

Control Field for S-Frames

- Supervisory frames are used for flow and error control whenever piggybacking is either impossible or inappropriate. S-frames do not have information fields.
- If the first 2 bits of the control field are 10, this means the frame is an S-frame.
- The last 3 bits, called N(R), correspond to the acknowledgment number (ACK) or

	negative acknowledgment number (NAK), depending on the type of S-frame. • The 2 bits called code are used to define the type of S-frame itself. **Control Field for U-Frames** • Unnumbered frames are used to exchange session management and control information between connected devices. • Unlike S-frames, U-frames contain an information field, but one used for system management information, not user data. • As with S-frames, however, much of the information carried by U-frames is contained in codes included in the control field. U-frame codes are divided into two sections: a 2-bit prefix before the P/F bit and a 3-bit suffix after the P/F bit. • Together, these two segments (5 bits) can be used to create up to 32 different types of U-frames.	
Q4 (a)	Let us first find the value of header fields before answering the questions: VER = 0x4 = 4 HLEN =0x5 = 5 →5*4 = 20 Service =0x00 = 0 Total Length = 0x0054 = 84 Identification = 0x0003 = 3 Flags and Fragmentation = 0x0000 →D = 0 M= 0 offset = 0 Time to live = 0x20 = 32 Protocol = 0x06 = 6 Checksum = 0x5850 Source Address: 0x7C4E0302 = 124.78.3.2 Destination Address: 0xB40E0F02 = 180.14.15.2 – We can then answer the questions: – a. If we calculate the checksum, we get 0x0000. The packet is not corrupted. – b. Since the length of the header is 20 bytes, there are no options. – c. Since M = 0 and offset = 0, the packet is not fragmented. – d. The total length is 84. Data size is 64 bytes (84 −20). – e. Since the value of time to live = 32, the packet may visit up to 32 more routers. – f. The identification number of the packet is 3. – g. The type of service is normal. **OR** **i. The fields related to fragmentation in IPv4 datagram.** – The fields that are related to fragmentation and reassembly of an IP datagram are the identification, flags, and fragmentation offset fields. **Identification.** – This 16-bit field identifies a datagram originating from the source host. – The combination of the identification and source IP address must uniquely define a datagram as it leaves the source host. – To guarantee uniqueness, the IP protocol uses a counter to label the datagrams. – The counter is initialized to a positive number. – When the IP protocol sends a datagram, it copies the current value of the counter to the identification field and increments the counter by one. – As long as the counter is kept in the main memory, uniqueness is guaranteed.	[8] [4]

- When a datagram is fragmented, the value in the identification field is copied into all fragments.
- In other words, all fragments have the same identification number, which is also the same as the original datagram.
- The identification number helps the destination in reassembling the datagram.
- It knows that all fragments having the same identification value should be assembled into one datagram.

Flags.

- This is a three-bit field.
- The first bit is reserved (not used).
- The second bit is called the do not fragment bit.
- If its value is 1, the machine must not fragment the datagram.
- If it cannot pass the datagram through any available physical network, it discards the datagram and sends an ICMP error message to the source host.
- If its value is 0, the datagram can be fragmented if necessary.
- The third bit is called the more fragment bit.
- If its value is 1, it means the datagram is not the last fragment; there are more fragments after this one.
- If its value is 0, it means this is the last or only fragment

Figure 7.7 *Flags field*

Fragmentation offset.

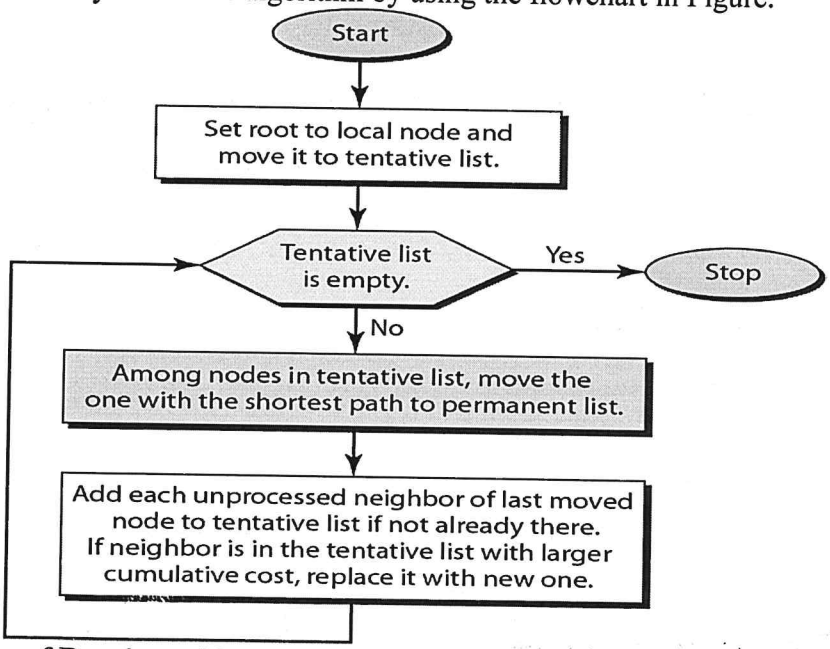
- This 13-bit field shows the relative position of this fragment with respect to the whole datagram.
- It is the offset of the data in the original datagram measured in units of 8 bytes.
- Figure 7.8 shows a datagram with a data size of 4000 bytes fragmented into three fragments.
- The bytes in the original datagram are numbered 0 to 3999.
- The first fragment carries bytes 0 to 1399.
- The offset for this datagram is 0/8 = 0.
- The second fragment carries bytes 1400 to 2799; the offset value for this fragment is 1400/8 = 175.
- Finally, the third fragment carries bytes 2800 to 3999. The offset value for this fragment is 2800/8 = 350

ii. Address Depletion

- The flaws in classful addressing scheme combined with the fast growth of the Internet led to the near depletion of the available addresses.
- Yet the number of devices on the Internet is much less than the 2^{32} address space.
- We have run out of class A and B addresses, and a class C block is too small for most midsize organizations.
- One solution that has alleviated the problem is the idea of classless addressing.
- Classful addressing, which is almost obsolete, is replaced with classless addressing.

[4]

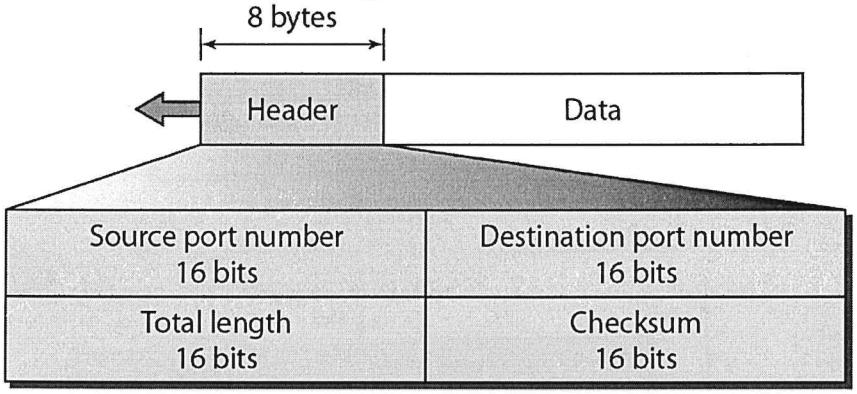
	Classless Addressing – To overcome address depletion and give more organizations access to the Internet, classless addressing was designed and implemented. – In this scheme, there are no classes, but the addresses are still granted in blocks. – **Address Blocks** – In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a block (range) of addresses. – The size of the block (the number of addresses) varies based on the nature and size of the entity. – For example, a household may be given only two addresses; a large organization may be given thousands of addresses. – An ISP, as the Internet service provider, may be given thousands or hundreds of thousands based on the number of customers it may serve. – **Restriction:** – To simplify the handling of addresses, the Internet authorities impose three restrictions on classless address blocks: – 1. The addresses in a block must be contiguous, one after another. – 2. The number of addresses in a block must be a power of 2 (1, 2, 4, 8, ...). – 3. The first address must be evenly divisible by the number of addresses.	
Q4 (b)	**Building Routing Tables in Link State Routing** – In link state routing, four sets of actions are required to ensure that each node has the routing table showing the least-cost node to every other node. – 1. Creation of the states of the links by each node, called the link state packet (LSP). – 2. Dissemination of LSPs to every other router, called flooding, in an efficient and reliable way. – 3. Formation of a shortest path tree for each node. – 4. Calculation of a routing table based on the shortest path tree. – **Creation of Link State Packet (LSP)** – A link state packet can carry a large amount of information. – For the moment, however, we assume that it carries a minimum amount of data: – the node identity, – the list of links, – a sequence number, and – age. – The first two, node identity and the list of links, are needed to make the topology. – The third, sequence number, facilitates flooding and distinguishes new LSPs from old ones. – The fourth, age, prevents old LSPs from remaining in the domain for a long time. – **Flooding of LSPs** – After a node has prepared an LSP, it must be disseminated to all other nodes, not only to its neighbors. – The process is called flooding and based on the following: – 1. The creating node sends a copy of the LSP out of each interface. – 2. A node that receives an LSP compares it with the copy it may already have. – If the newly arrived LSP is older than the one it has (found by checking the sequence number), it discards the LSP. – If it is newer, the node does the following: – a. It discards the old LSP and keeps the new one. – b. It sends a copy of it out of each interface except the one from which the packet	[7]

	arrived. – This guarantees that flooding stops somewhere in the domain (where a node has only one interface). – **Formation of Shortest Path Tree** – Dijkstra Algorithm After receiving all LSPs, each node will have a copy of the whole topology. – However, the topology is not sufficient to find the shortest path to every other node; a shortest path tree is needed. – A tree is a graph of nodes and links; one node is called the root. – All other nodes can be reached from the root through only one single route. – A shortest path tree is a tree in which the path between the root and every other node is the shortest. – What we need for each node is a shortest path tree with that node as the root. – The Dijkstra algorithm creates a shortest path tree from a graph. – The algorithm divides the nodes into two sets: tentative and permanent. – It finds the neighbors of a current node, makes them tentative, examines them, and if they pass the criteria, makes them permanent. – We can informally define the algorithm by using the flowchart in Figure.  – **Calculation of Routing table** – Table from Shortest Path Tree Each node uses the shortest path tree protocol to construct its routing table. – The routing table shows the cost of reaching each node from the root.	
Q5 (a)	**Solution: -** • a. The source port number is 0x0532 (1330 in decimal). • b. The destination port number is 0x0017 (23 in decimal). • c. The sequence number is 0x00000001 (1 in decimal). • d. The acknowledgment number is 0x00000000 (0 in decimal). • e. The header length is 0x5 (5 in decimal). There are 5 × 4 or 20 bytes of header. • f. The control field is 0x002. This indicates a SYN segment used for connection establishment. • g. The window size field is 0x07FF (2047 in decimal).	[8]

OR

User Datagram Protocol (UDP): [8]

- The User Datagram Protocol (UDP) is called a connectionless, unreliable transport protocol.
- It does not add anything to the services of IP except to provide process-to-process communication instead of host-to-host communication.
- Also, it performs very limited error checking.
- If UDP is so powerless, why would a process want to use it?
- With the disadvantages come some advantages.
- UDP is a very simple protocol using a minimum of overhead.
- If a process wants to send a small message and does not care much about reliability, it can use UDP.
- Sending a small message by using UDP takes much less interaction between the sender and receiver than using TCP or SCTP.
- **User Datagram**
- UDP packets, called user datagrams, have a fixed-size header of 8 bytes.
- Figure shows the format of a user datagram.



Source port number.

- This is the port number used by the process running on the source host.
- It is 16 bits long, which means that the port number can range from 0 to 65,535.
- If the source host is the client (a client sending a request), the port number, in most cases, is an ephemeral port number requested by the process and chosen by the UDP software running on the source host.
- If the source host is the server (a server sending a response), the port number, in most cases, is a well-known port number.

Destination port number.

- This is the port number used by the process running on the destination host. It is also 16 bits long.
- If the destination host is the server (a client sending a request), the port number, in most cases, is a well-known port number.
- If the destination host is the client (a server sending a response), the port number, in most cases, is an ephemeral port number.
- In this case, the server copies the ephemeral port number it has received in the request packet.

Length.

- This is a 16-bit field that defines the total length of the user datagram, header plus data.

	• The 16 bits can define a total length of 0 to 65,535 bytes. • However, the total length needs to be much less because a UDP user datagram is stored in an IP datagram with a total length of 65,535 bytes. • The length field in a UDP user datagram is actually not necessary. • A user datagram is encapsulated in an IP datagram. • There is a field in the IP datagram that defines the total length. • There is another field in the IP datagram that defines the length of the header. • So if we subtract the value of the second field from the first, we can deduce the length of a UDP datagram that is encapsulated in an IP datagram. • UDP length = IP length - IP header's length. **Checksum.** • This field is used to detect errors over the entire user datagram (header plus data).	
Q5 (b)	**SMTP Mail Transfer Phases** • The process of transferring a mail message occurs in three phases: connection establishment, mail transfer, and connection termination. • **Connection Establishment:** • After a client has made a TCP connection to the well-known port 25, the SMTP server starts the connection phase. • This phase involves the following three steps: • 1. The server sends code 220 (service ready) to tell the client that it is ready to receive mail. If the server is not ready, it sends code 421 (service not available). • 2. The client sends the HELO message to identify itself, using its domain name address. • This step is necessary to inform the server of the domain name of the client. • 3. The server responds with code 250 (request command completed) or some other code depending on the situation. • **Message Transfer:** • After connection has been established between the SMTP client and server, a single message between a sender and one or more recipients can be exchanged. • This phase involves eight steps. Steps 3 and 4 are repeated if there is more than one recipient. • 1. The client sends the MAIL FROM message to introduce the sender of the message. It includes the mail address of the sender (mailbox and the domain name). This step is needed to give the server the return mail address for returning errors and reporting messages. • 2. The server responds with code 250 or some other appropriate code. • 3. The client sends the RCPT TO (recipient) message, which includes the mail address of the recipient. • 4. The server responds with code 250 or some other appropriate code. • 5. The client sends the DATA message to initialize the message transfer. • 6. The server responds with code 354 (start mail input) or some other appropriate message. • 7. The client sends the contents of the message in consecutive lines. Each line is terminated by a two-character end-of-line token (carriage return and line feed). The message is terminated by a line containing just one period. • 8. The server responds with code 250 (OK) or some other appropriate code. • **Connection Termination:** • After the message is transferred successfully, the client terminates the connection. • This phase involves two steps. • 1. The client sends the QUIT command.	[7]

	• 2. The server responds with code 221 or some other appropriate code.	