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

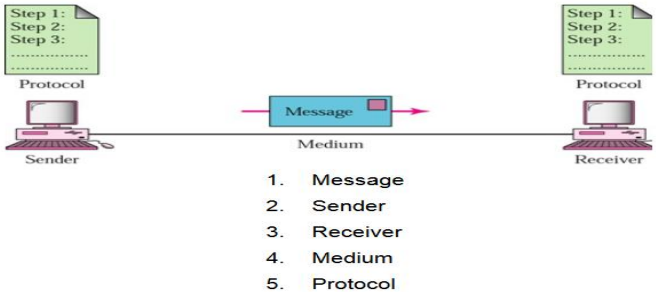
Internal Assessment Test 1 – November. 2021

Sub:	Computer Communication Networks					Sub Code:	18EC71	Branch	ECE
Date:	/11/2021	Duration:	90 min's	Max Marks:	50	Sem / Sec:	VII		OBE

Answer any five questions

		MARKS	CO	RBT
1	**(a) Explain the major components of data communication with a neat diagram.**	[5+5]	CO1	L2

Solution:



Message: The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

Sender: The sender is the device that sends the data message. It can be a computer, Work station, telephone handset, video camera, and so on.

Receiver: The receiver is the device that receives the message. It can be a computer, Work station, telephone handset, television, and so on.

Transmission medium: The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

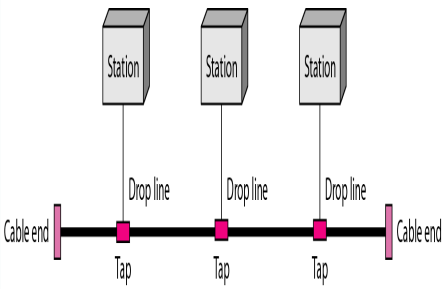
Protocol: A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices.

(b) Explain network topologies with figures, also mention merits and demerits.

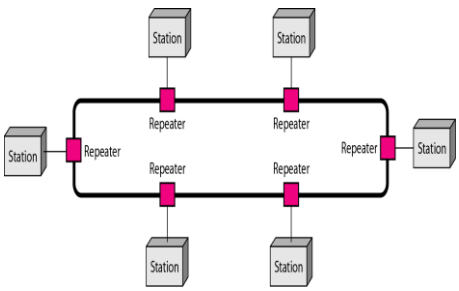
Solution:

Network Topologies: It describes the geometric arrangement of components that make up the LAN

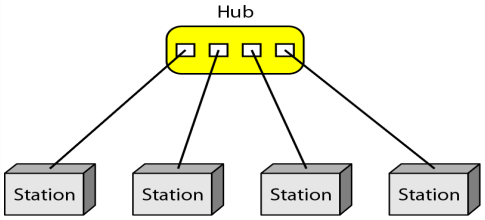
Topologies: Bus, Star, Ring, Mesh



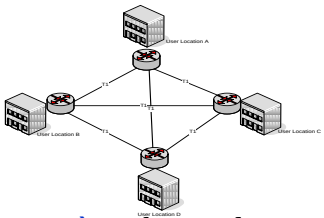
Bus Topology



Ring Topology



Star Topology


`Mesh Topology

Mesh Topology: In a mesh topology, every device has a dedicated point-to-point link to every
other device. One practical example of a mesh topology is the connection of telephone regional
offices in which each regional office needs to be connected to every other regional office

Ring Topology In a ring topology, 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.

Star Topology Here each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. The controller acts as an 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

Bus Topology It is multipoint topology. One long cable acts as a **backbone** to link all the devices in a network.

2	Explain stop and wait protocol. Also discuss acknowledgement, timer and sequence no with the help of flow diagram.	[5+5]	CO1	L2

Solution:
Stop-and-Wait protocol, which uses both flow and error control. In this protocol, the sender sends one frame at a time and waits for an acknowledgment before sending the next one. To detect corrupted frames, we need to add a CRC to each data frame. When a frame arrives at the receiver site, it is
checked. If its CRC is incorrect, the frame is corrupted and silently discarded. The silence of the receiver is a signal for the sender that a frame was either corrupted or lost. Every time the sender sends a frame, it starts a timer. If an acknowledgment arrives before the timer expires, the timer is stopped and the sender sends the next frame (if it has one to send). If the timer expires, the sender resends the previous frame, assuming that the frame was either lost or corrupted. This means that the sender needs to keep a copy of the frame until its acknowledgment arrives. When the corresponding acknowledgment arrives, the sender discards the copy and sends the next frame if it is ready. Figure shows the outline for the Stop-and-Wait protocol. Note that only one frame and one acknowledgment can be in the channels at any time.

Figure 11.10 *Stop-and-Wait protocol*

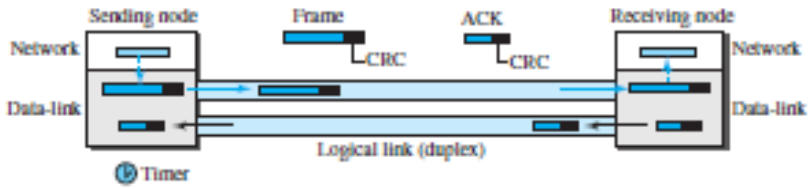
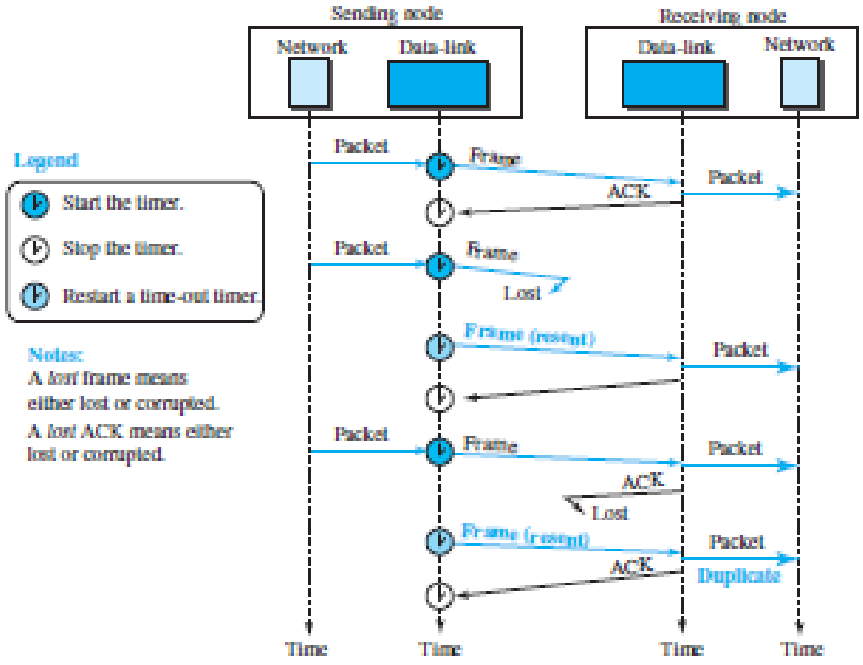


Figure 11.12 *Flow diagram for Example 11.3*



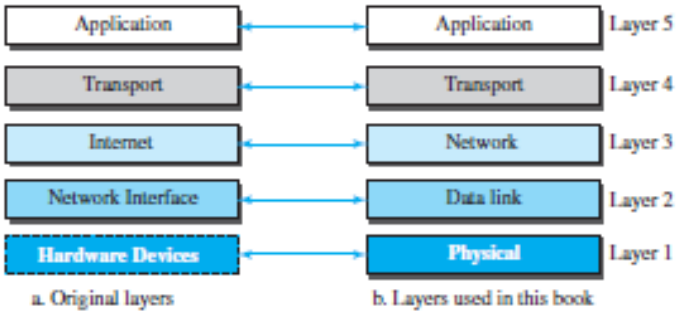
3 (a) Compare TCP/IP and OSI reference model. [7+3] CO1 L2

Solution:

Comparison between OSI and TCP/IP

OSI(Open System Interconnection)	**TCP/IP(Transmission Control Protocol / In 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 protoc around which the Internet has developed. It is communication protocol, which allows connec 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 n guarantees delivery of packets. Still the TCP/I 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 Presenta or Session layer.

Figure 2.4 *Layers in the TCP/IP protocol suite*



(b) Explain encapsulation and decapsulation with neat figure.

Encapsulation at the Source Host

At the source, we have only encapsulation.

1. At the application layer, the data to be exchanged is referred to as a *message*. A message normally does not contain any header or trailer, but if it does, we refer to the whole as the message. The message is passed to the transport layer.

2. The transport layer takes the message as the 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, such as information needed for flow, error control, or congestion control. The result is the 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.

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 hosts and some more information used for error checking of the header, fragmentation information, and so on. The result is the network-layer packet, called a *datagram*. The network layer then passes the packet to the data-link layer.

4. 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 router). The result is the link-layer packet, which is called a *frame*. The frame is passed to the physical layer for transmission.

Decapsulation and Encapsulation at the Router

At the router, we have both decapsulation and encapsulation because the router is connected to two or more links.

1. After the set of bits are 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 to which the datagram is to be delivered. The contents of the datagram should not be changed by the network layer in the router unless there is a need to fragment the datagram if it is too big to be passed through the next link. The datagram is then passed to the data-link layer of the next link.

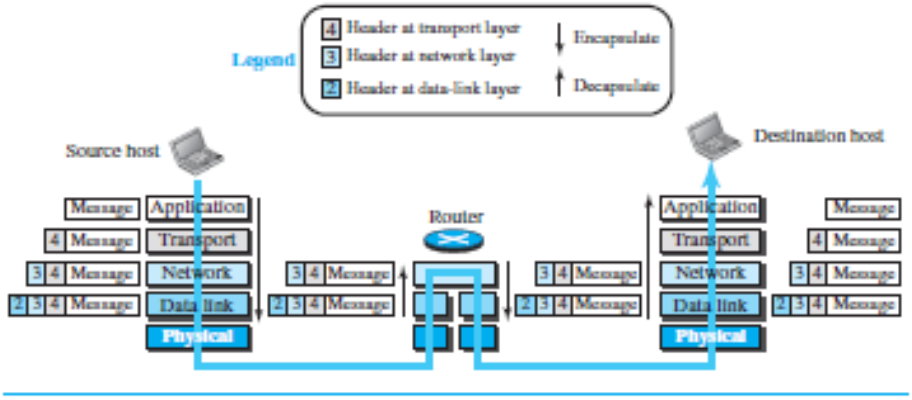
3. The data-link layer of the next link encapsulates the datagram in a frame and passes it to the physical layer for transmission.

Decapsulation at the Destination Host

At the 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. It is necessary to say that decapsulation in the host

involves error checking.

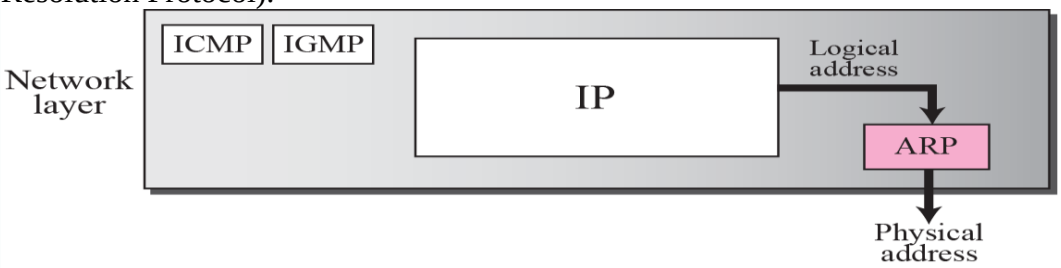
Figure 2.8 *Encapsulation/Decapsulation*



4 Explain Address Resolution Protocol (ARP) operation. Explain ARP request and response packet format with neat diagrams. [5+5] CO1 L1

Solution:

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



ARP packet

0	8	16
Hardware Type		Protocol Type
Hardware length	Protocol length	Operation Request:1, Reply:
Source hardware address		
Source protocol address		
Destination hardware address (Empty in request)		
Destination protocol address		

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

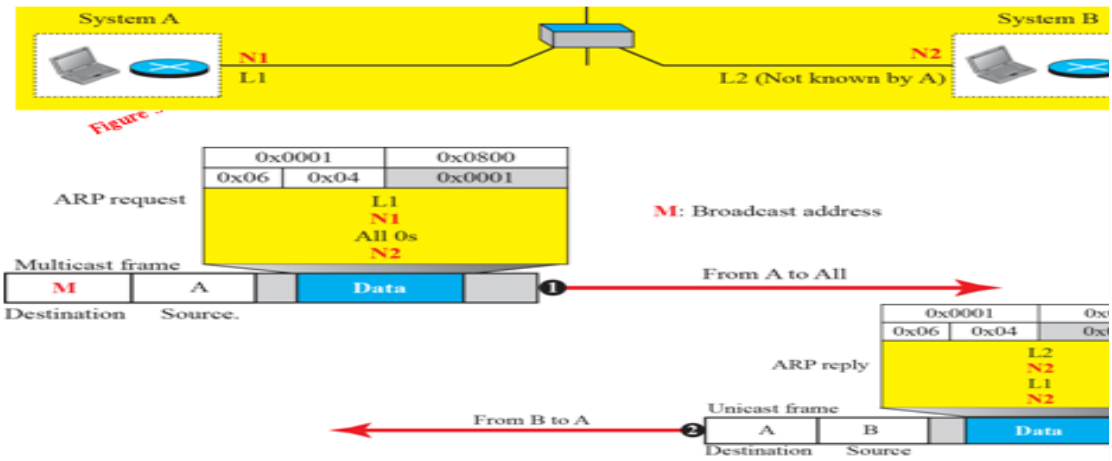
Protocol type: this field defines the network layer protocol which is IPV4 and set to (0086)16

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 field is set to '1', for request the fields is set to '2'.

ARP operation using message exchange



5 (a) A slotted ALOHA network transmits 200-bit frames on a shared channel of 200 Kbps. Find the vulnerable time and throughput if the system produces: a) 1000 frames/sec b) 500 frames/sec c) 250 frames/sec. [6+4] CO2 L2

Solution

This situation is similar to the previous exercise except that the network is using slotted ALOHA instead of pure ALOHA. The frame transmission time is 200/200 kbps or 1 ms.

a. In this case G is 1. So $S = G \times e^{-G} = 0.368$ (36.8 percent). This means that the throughput is $1000 \times 0.0368 = 368$ frames. Only 368 out of 1000 frames will probably survive. Note that this is the maximum throughput case, percentagewise.

b. Here G is 1/2. In this case $S = G \times e^{-G} = 0.303$ (30.3 percent). This means that the throughput is $500 \times 0.0303 = 151$. Only 151 frames out of 500 will probably survive.

c. Now G is 1/4. In this case $S = G \times e^{-G} = 0.195$ (19.5 percent). This means that the throughput is $250 \times 0.195 = 49$. Only 49 frames out of 250 will probably survive.

(b) Write a short note on pure ALOHA with necessary figure.

The original ALOHA protocol is called ***pure ALOHA.*** This is a simple but elegant protocol. The idea is that each station sends a frame whenever it has a frame to send (multiple access). However, since there is only one channel to share, there is the possibility of collision between frames from different stations as shown in fig.12.2

Figure 12.2 *Frames in a pure ALOHA network*

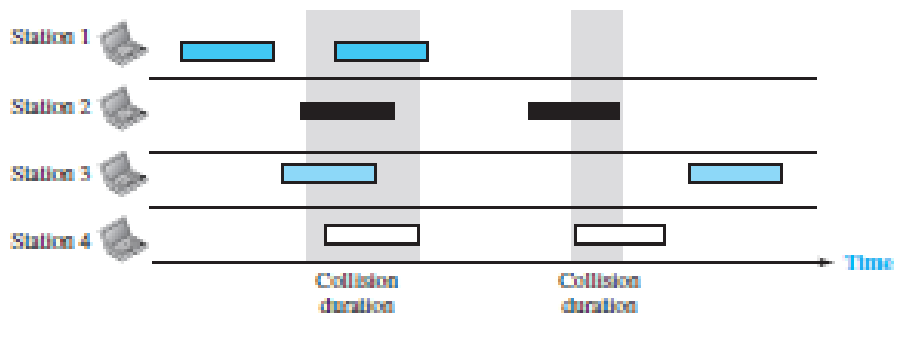
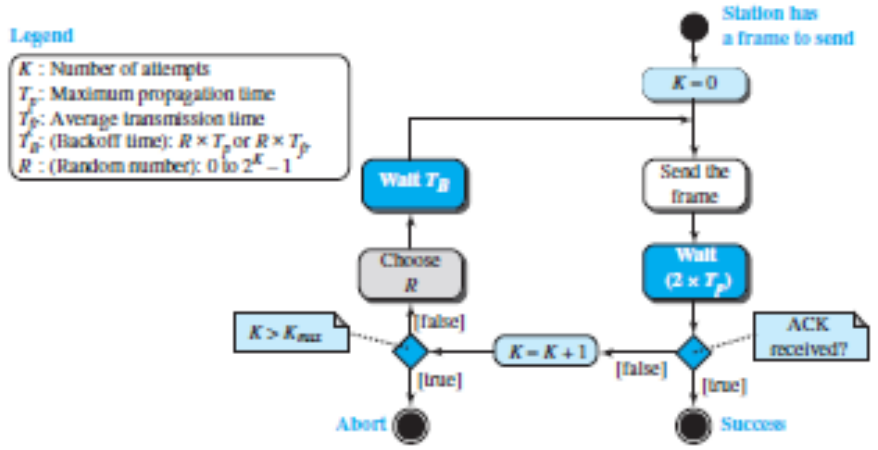


Figure 12.2 shows that only two frames survive: one frame from station 1 and one frame from station 3. The pure ALOHA protocol relies on acknowledgments from the receiver. When a station sends a frame, it expects the receiver to send an

acknowledgment. If the acknowledgment does not arrive after a time-out period, the station assumes that the frame (or the acknowledgment) has been destroyed and resends the frame. Pure ALOHA dictates that when the time-out period passes, each station waits a random amount of time before resending its frame. The randomness will help avoid more collisions. We call this time the *backoff time TB*. Pure ALOHA has a second method to prevent congesting the channel with retransmitted frames. After a maximum number of retransmission attempts *Kmax*, a station must give up and try later. Figure 12.3 shows the procedure for pure ALOHA based on the above strategy.

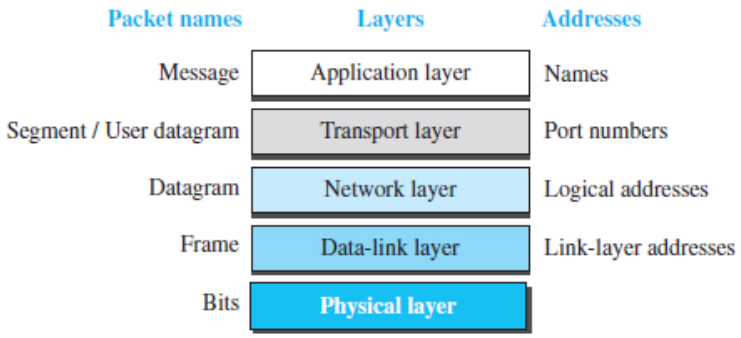
Figure 12.3 *Procedure for pure ALOHA protocol*



6 (a) Write short note on different types of addressing. [4+6] CO1 L1

Four types of addressing methods used are the following :
Physical address
Logical address (IP)
Port address and
Specific address
Figure 2.9 shows the addressing at each layer. As the figure shows, there is a relationship between the layer, the address used in that layer, and the packet name at that layer. At the application layer, we normally use names to define the site that provides services, such as *someorg.com*, or the e-mail address, such as *somebody@coldmail.com.* At the transport layer, addresses are called port numbers, and these define the application-layer programs at the source and destination. Port numbers are local addresses that distinguish between several programs running at the same time. At the network-layer, the addresses are global, with the whole Internet as the scope. A network-layer address uniquely defines the connection of a device to the Internet. The logical address or network layer address also known as IP address used on the internet is currently a 32-bit address .
The link-layer addresses, sometimes called MAC addresses, are locally defined addresses, each of which defines a specific host or router in a network (LAN or WAN). The Ethernet (LAN) uses a 48-bit (6-byte) physical address which is normally produced in the **network interfacing card (NIC)**.
The physical addresses change for each and every trip a packet takes, but the logical and port addresses basically will remain as it is.

Figure 2.9 *Addressing in the TCP/IP protocol suite*



(b) Explain bit stuffing and de-stuffing with necessary figure.

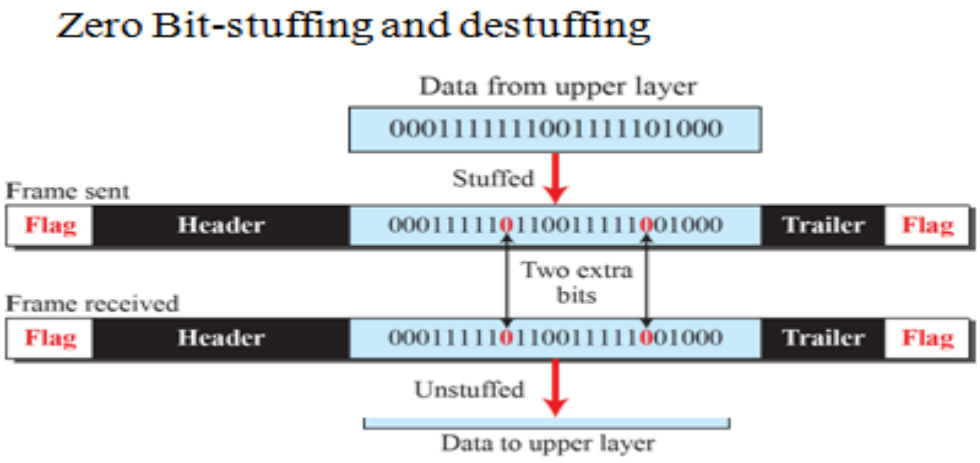
Solution:

Bit oriented approach uses a special 8-bit pattern flag 01111110 as the delimiter to define the beginning and the end of the frame.

In a bit-oriented protocol, the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio, video, and so on. However, in addition to headers and trailer (which store error detection and correction algorithm like cyclic redundancy check (crc)), we still need a delimiter or flag to separate one frame to another frame.

Zero Bit-stuffing and destuffing

- If the data pattern resembles the flags pattern then receiver can mistaken it as flag. Hence a zero bit is stuffed at the transmitter after consecutive '5' ones called as zero bit stuffing.
- This stuffed zero bit is destuffed at the receiver back called as zero bit destuffing.



7	Explain protocol layering with the principles. With a neat diagram, explain the layers in TCP/IP protocol suite.	[3+7]	CO2 L1

In data communication and networking, a protocol defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively. When communication is simple, we may need only one simple protocol; when the communication is complex, we may need to divide the task between different layers, in which case we need a protocol at each layer, or **protocol layering.**

Advantages of protocol layering:

Protocol layering enables us to divide a complex task into several smaller and simpler tasks.

Protocol layering allows us to separate the services from the implementation. A layer needs to be able to receive a set of services
from the lower layer and to give the services to the upper layer; we don't care about how the layer is implemented.

Communication does not always use only two end systems; there are intermediate systems that need only some layers, but not all layers. If we did not use protocol layering, we would have to make each intermediate system as complex as the end systems, which makes the whole system more expensive.

Principles of protocol layering:

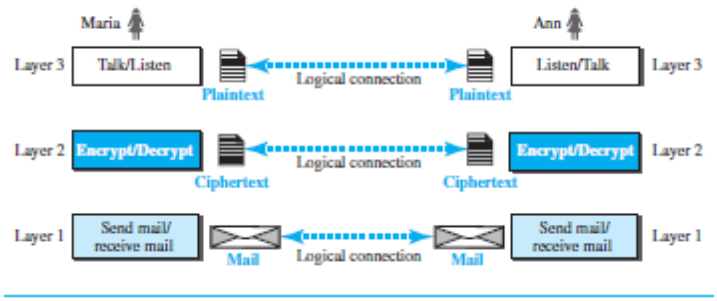
First Principle

The first principle dictates that if we want bidirectional communication, we need to make each layer so that it is able to perform two opposite tasks, one in each direction. For example, the third layer task is to listen (in one direction) and *talk* (in the other
direction). The second layer needs to be able to encrypt and decrypt. The first layer needs to send and receive mail.

Second Principle

The second principle that we need to follow in protocol layering is that the two objects under each layer at both sites should be identical. For example, the object under layer 3 at both sites should be a plaintext letter. The object under layer 2 at both sites should be a cipher text letter. The object under layer 1 at both sites should be a piece of mail.

Figure 2.3 *Logical connection between peer layers*



TCP/IP PROTOCOL SUITE

1) The TCP/IP protocol suite was developed DOD of USA in early 1970's.

2) Protocol suite means a set of protocols organized in different layers performing some different task.

3) It is hierarchical protocol suite.

4) TCP/IP is a five-layer model

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 work at physical layers.
- Deals with formation of frame**.**

Course Instructor **Chief Course Instructor**