K - 53131

Register No.

BTech Degree Examination May 2023

Fifth Semester

Information Technology

20ITT51 – COMPUTER NETWORKS

(Regulations 2020)

Time: Three hours Maximum: 100 marks

Answer all Questions

Part – A (10 × 2 = 20 marks)

1. Differentiate between port address, logical address, and physical address. [CO1,K2]

2. How many 8-bit characters can be transmitted per second over a 9600 baud serial communication link using asynchronous mode of transmission with one start bit, eight data bits, two stop bits, and one parity bit? [CO1,K3]

3. A sender sends a series of packets to the same destination using 5-bit sequence numbers. If the sequence number starts with 0, what is the sequence number after sending 100 packets? [CO2,K3]

4. Identify the purpose of ARP and RARP is data link layer. [CO2,K1]

5. What should be the subnet mask for an organisation that has a class B network and wishes to form subnets for 64 departments? [CO3,K3]

6. Draw the IPV4 datagram format. [CO3,K1]

7. What is the maximum size of data that the application layer can pass on to the TCP layer? [CO4,K3]

8. Define piggybacking and its usefulness. [CO4,K1]

9. Write your inference from the URL https://172.16.24.10:81/exam. [CO5,K3]

10. Why should there be limitations on anonymous FTP? What could a dishonest user do? [CO5,K2]

Part – B (5 × 16 = 80 marks)

11. a. i) Define Topology. Illustrate and compare the various topologies by which a network can be built. Analyze how a single-point failure will affect the network in each case. (8) [CO1,K1]

ii) Discuss in detail the different types of guided transmission media with suitable diagrams and list their applications. (8) [CO1,K1]

(OR)

b. i) Outline the functions of any four layers in the OSI network model with suitable diagrams. (8) [CO1,K1]

ii) Enumerate the characteristics of different modes of data transmission with their relative merits and demerits. (8) [CO1,K1]

12. a. i) Explain the role of MAC and LLC sublayers in the datalink layer according to IEEE standard. Write a detailed note on 802.3 MAC frame. (8) [CO2,K2]

ii) A sender needs to send the following three data items 0xABCC, 0x02BC, and 0xEEEE. (8) [CO2,K3]

1) Find the checksum at the sender and receiver site, if there is no error.

2) Find the checksum at the receiver site, if the first data item is changed to 0xABCE and the second data item is changed to 0x02BA.

(OR)

b. i) Illustrate how carrier senses multiple access techniques increase the performance by minimizing the chance of collision. (8) [CO2,K2]

ii) How does the Cyclic Redundancy Check work? Use the following CRC polynomial 1011 to obtain the checksum for the dataword 10110010. Show that single-bit error can be detected by modifying the above dataword and applying the CRC checksum. (8) [CO2,K3]

13. a. i) With a neat diagram, describe the various fields of IPv4 header and illustrate their significance. (8) [CO3,K2]

ii) Illustrate how the link state algorithm works for the graph consisting of 5 nodes A, B, C, D, and E. The link costs are: C(A,B)=2, C(B,E)=3, C(A,C)=3, C(C,D)=5 , C(B,D)=4. (8) [CO3,K3]

(OR)

b. i) Compare classful and classless addressing. Describe the solutions for handling the scarcity of IP addresses. (8) [CO3,K2]

ii) Assume that the shortest distance between nodes a, b, c, d to node y and the costs from node x to a, b, c, d are as follows: (8) [CO3,K3]

D(a,y)=5, D(b,y)=6, D(c,y)=4, D(d,y)=3

C(x,a)=2, C(x,b)=1, C(x,c)=3, C(x,d)=1

What is the shortest distance between node x and y, D(x,y), according to the Bellman-Ford equation?

14. a. i) What are the services provided by the User Datagram Protocol? Draw the UDP header and discuss its fields. (8) [CO4,K2]

ii) A system uses the Stop-and-Wait ARQ Protocol. If each packet carries 1000 bits of data, how long does it take to send 1 million bits of data, if the distance between the sender and receiver is 2500 km and the propagation speed is 1.25×10^8 m? Ignore transmission, waiting, and processing delays. Assume no data or control frame is lost or damaged. (8) [CO4,K3]

(OR)

b. i) Identify the various ways to improve the Quality-of-Service on the Internet. Discuss with their merits and demerits. (8) [CO4,K2]

ii) Develop a bidirectional algorithm for Go-Back-N ARQ Protocol using piggybacking. Assume that both parties use the same algorithm. (8) [CO4,K3]

15. a. i) Explain the organization of name servers in DNS. Discuss how iterative and recursive resolution works in DNS. (8) [CO5,K2]

ii) Describe in detail how telnet helps to establish a connection to a remote system with suitable example. (8) [CO5,K2]

(OR)

b. i) Using different scenarios, describe the architecture of e-mail system in detail. (8) [CO5,K2]

ii) Discuss the role of SNMP in network management. (8) [CO5,K2]

Bloom's Taxonomy Level	Remembering (K1)	Understanding (K2)	Applying (K3)	Analysing (K4)	Evaluating (K5)	Creating (K6)
Percentage	21	47	32	–	–	–

KONGU ENGINEERING COLLEGE, PERUNDURAI, ERODE- 638 060
B.Tech Degree Examination June 2023
Fifth semester
Information Technology
20ITT51-Computer Networks
(Regulations 2020)
Answer key

PART – A (10 × 2 = 20 marks)

1. **Port address, logical address and physical address:** **[CO1,K2]**

Port address:

Each application run with a port number (logically) on the computer. This port number for application is decided by the Kernel of the OS and is called port address.

Logical address:

If a packet passes the network boundary, another addressing system is needed for source and destination called logical address.
This addressing is used to identify the device or a particular network on the internet.
This address can be changed by changing the host position on the network.

Physical address:

If frames are to be distributed to different systems on the network, data link layer adds a header to the frame to define the sender and receiver.
Each system having a NIC (Network Interface Card) through which two systems physically connected with each other with cables.
The address of the NIC is called Physical or MAC address.

2. **Asynchronous transmission mode:** **[CO1,K3]**

The total number of bits transmitted for each character is 1 + 8 + 1 + 2 = 12 bits. Number of 8-bit characters that can be transmitted per second is 9600 baud / 12 bits = 800 characters per second.

3. **Sequence number of packets:** **[CO2,K3]**

With 5 bits, we have a total of 2^5 = 32 possible sequence numbers ranging from 00000 to 11111.
100 % 32 = 4
Therefore, after sending 100 packets, the sequence number will be the 4th number after 00000, which is 00100.

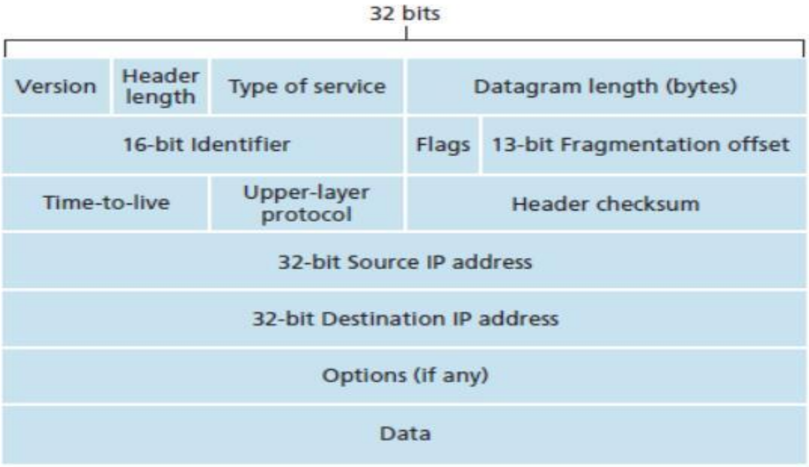
4. **Purpose of ARP and RARP in data link layer:** **[CO2,K1]**

- The purpose of ARP is to map an IP address to a physical (MAC) address within a local network.
- RARP, on the other hand, serves the reverse purpose. It is used to obtain the IP address of a device when the physical (MAC) address is known.

5. **Subnet mask:** **[CO3,K3]**

The size of network ID is 16 bit in class B networks. So bits after 16th bit must be used to create 64 departments. Total 6 bits are needed to identify 64 different departments. Therefore, subnet mask will be 255.255.252.0.

6. **IPv4 datagram format:** **[CO3,K1]**



7. **Maximum data size passing from application layer to TCP layer:** **[CO4,K3]**

Application layer can send any size of data. There is no limit defined by standards.

8. **Piggybacking and its usefulness:** **[CO4,K1]**

When a packet is carrying data from A to B, it can also carry acknowledgement about arrived packets from B and vice versa is called Piggybacking. To improve the efficiency of bidirectional communication, this technique is used.

The usefulness of piggybacking can be observed in various scenarios:

- Acknowledgment and Data Transmission.
- Link-Layer Control Frames
- Protocol Efficiency
- Time-Sensitive Applications

9. **Inference from URL, "https://l72.16.24.10:81/exam":** **[CO5,K3]**

https denotes application protocol
172.16.24.10 denotes IP address
81 denotes port number
exam denotes pathname

10. **Limitations on anonymous FTP:** **[CO5,K2]**

- Less control over who is accessing your FTP server as it is completely public
- It can compromise the whole system if not used properly

PART – B (5 × 16 = 80 marks)

11.a.i) Topology, its types and single-point failure: **[CO1,K1]**

Two or more devices connect to a link. Two or more links form a topology.

Topology is defined as

(1) The way in which a network is laid out physically.

(2)The geometric representation of the relationship of all the links and nodes to one-another.

The various types of topologies are: Bus, Ring, Star, Mesh.

- **(2)**

BUS TOPOLOGY

- Bus topology is a network type in which every computer and network device is connected to single cable.
- The long single cable acts as a backbone to link all the devices in a network.
- When it has exactly two endpoints, then it is called Linear Bus topology.
- It transmits data only in one direction.

A single point of failure in a bus topology will cause the entire network to be disrupted, as the failure of a single node or connection can result in the loss of communication across the network. **- (1)**

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.
- Each device in the ring incorporates a repeater.
- When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

In a ring topology, a single point failure can lead to a complete network outage. If any node or connection in the ring fails, the communication between all nodes is disrupted. **- (1)**

STAR TOPOLOGY

- In a star topology, each device has a dedicated point-to-point link only to a central controller, 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.

In a star topology, a single point failure of the central hub will cause the entire network to be affected. All communication between nodes relies on the central hub, so its failure disrupts the entire network. **- (2)**

MESH TOPOLOGY

- In a mesh topology, every device has a dedicated point-to-point link to every other device.
- The term dedicated means that the link carries traffic only between the two devices it connects.
- The number of physical links in a fully connected mesh network with n nodes is given by n (n – 1) / 2.

A single point failure in a mesh topology has limited impact. The network provides multiple paths between nodes, so if one connection fails, alternative routes can be used to maintain communication. - **(2)**

11.a.ii) Different types of guided transmission media: [CO1,K1]

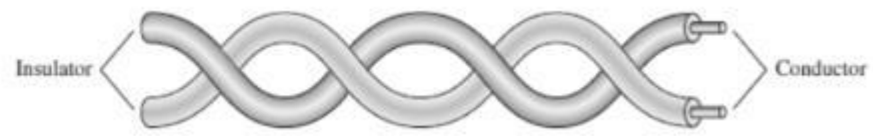
Guided transmission media is defined as the physical medium through which the signals are transmitted. It is also known as bounded media.

Types of guided media: Twisted Pair Cable, Coaxial Cable, Fibre Optic Cable - **(2)**

1. TWISTED PAIR CABLE

- Twisted pair is a physical media made up of a pair of cables twisted with each other.
- A twisted pair cable is cheap as compared to other transmission media.
- Installation of the twisted pair cable is easy, and it is a lightweight cable.
- The frequency range for twisted pair cable is from 0 to 3.5KHz.
- A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.

- **(1)**



Applications:

Telephone and DSL lines, LANs - **(1)**

2. COAXIAL CABLE

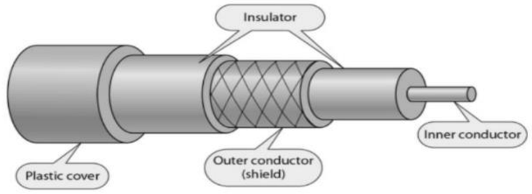
o Coaxial cable(Coax) is a very commonly used transmission media, for example,TV wire is usually a coaxial cable.

o The name of the cable is coaxial as it contains two conductors parallel to each other.

o It has a higher frequency as compared to Twisted pair cable.

o The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh.

o The middle core is made up of non-conductive cover that separates the inner conductor from the outer conductor.o The middle core is responsible for the data transferring whereas the copper mesh prevents from the EMI(Electromagnetic interference). - **(1)**



Applications:

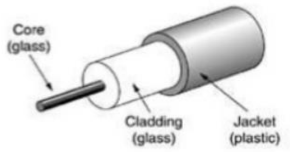
Analog and digital telephone networks, Cable TV networks and traditional Ethernet LANs.

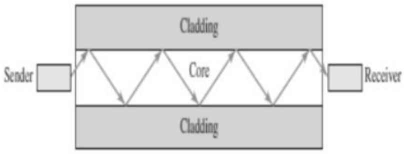
- **(1)**

FIBRE OPTIC CABLE

o Fibre optic cable is a cable that uses electrical signals for communication.

o Fibre optic is a cable that holds the optical fibres coated in plastic that are used to send the data by pulses of light.
o The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring.
o Fibre optics provide faster data transmission than copper wires **- (1)**





Applications:

Backbone networks and LANs **- (1)**

(or)

11.b.i) Functions of any four layers in OSI model: [CO1,K1]

1. PHYSICAL LAYER

The physical layer coordinates the functions required to transmit a bit stream over a physical medium.
The physical layer is concerned with the following functions:

¬ **Physical characteristics of interfaces and media** - The physical layer defines the characteristics of the interface between the devices and the transmission medium.

¬ **Representation of bits** - To transmit the stream of bits, it must be encoded to signals. The physical layer defines the type of encoding.

¬ **Signals:** It determines the type of the signal used for transmitting the information.

¬ **Data Rate or Transmission rate** - The number of bits sent each second –is also defined by the physical layer.

¬ **Synchronization of bits** - The sender and receiver must be synchronized at the bit level. Their clocks must be synchronized.

¬ **Line Configuration** - In a point-to-point configuration, two devices are connected together through a dedicated link. In a multipoint configuration, a link is shared between several devices.

¬ **Physical Topology** - The physical topology defines how devices are connected to make a network. Devices can be connected using a mesh, bus, star or ring topology.

¬ **Transmission Mode** - The physical layer also defines the direction of transmission between two devices: simplex, half-duplex or full-duplex.

2. DATA LINK LAYER

It is responsible for transmitting frames from one node to the next node.
The other responsibilities of this layer are

¬ **Framing** - Divides the stream of bits received into data units called frames.

¬ **Physical addressing** – If frames are to be distributed to different systems on the network , data link layer adds a header to the frame to define the sender and receiver.

¬ **Flow control-** If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender ,the Data link layer imposes a flow ctrl mechanism.

¬ **Error control**- Used for detecting and retransmitting damaged or lost frames and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.

¬ **Medium Access control** -Used to determine which device has control over the link at any given time.

3. NETWORK LAYER

This layer is responsible for the delivery of packets from source to destination.
It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
The other responsibilities of this layer are

¬ **Logical addressing** - If a packet passes the network boundary, we need another addressing system for source and destination called logical address. This addressing is used to identify the device on the internet.

¬ **Routing** – Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.

4. TRANSPORT LAYER

It is responsible for Process to Process delivery. That is responsible for source-to destination (end-to-end) delivery of the entire message, It also ensures whether the message arrives in order or not.
The other responsibilities of this layer are

¬ **Port addressing / Service Point addressing** - The header includes an address called
port address / service point address. This layer gets the entire message to the correct process on that computer.

¬ **Segmentation and reassembly** - The message is divided into segments and each segment is assigned a sequence number. These numbers are arranged correctly on the arrival side by this layer.

¬ **Connection control** - This can either be connectionless or connection oriented.

□ The connectionless treats each segment as an individual packet and delivers to the destination.

□ The connection-oriented makes connection on the destination side before the delivery. After the delivery the termination will be terminated.

¬ **Flow control** - The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.

¬ **Error Control** - Error control is performed end-to-end rather than across the single link..

5. SESSION LAYER

This layer establishes, manages and terminates connections between applications. The other responsibilities of this layer are

¬ **Dialog control** - Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.

¬ **Synchronization**- Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data,then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

6. PRESENTATION LAYER

It is concerned with the syntax and semantics of information exchanged between two systems. The other responsibilities of this layer are

¬ **Translation** – Different computers use different encoding system, this layer is responsible for interoperability between these different encoding methods. It will change the message into some common format.

¬ **Encryption and decryption**-It means that sender transforms the original information to another form and sends the resulting message over the n/w. and vice versa.

¬ **Compression and expansion**-Compression reduces the number of bits contained in the information particularly in text, audio and video.

7. APPLICATION LAYER

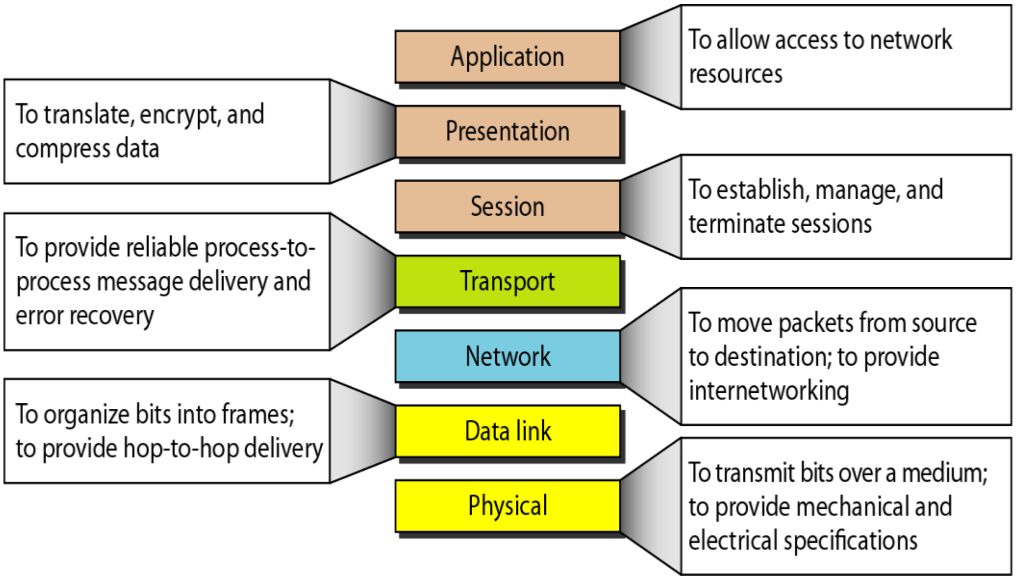
This layer enables the user to access the network. It handles issues such as network transparency, resource allocation, etc. This allows the user to log on to remote user. The other responsibilities of this layer are

¬ **FTAM (File Transfer, Access, Management)** - Allows user to access files in a remote host.

¬ **Mail services** - Provides email forwarding and storage.

¬ **Directory services** - Provides database sources to access information about various sources and objects.

Any four layers - each 2 marks


Application
To allow access to network resources
To translate, encrypt, and compress data
Presentation
Session
To establish, manage, and terminate sessions
To provide reliable process-to-process message delivery and error recovery
Transport
Network
To move packets from source to destination; to provide internetworking
To organize bits into frames; to provide hop-to-hop delivery
Data link
Physical
To transmit bits over a medium; to provide mechanical and electrical specifications

- **(2)**

11.b. ii) Characteristics of different modes of data transmission with merits and demerits: [CO1,K1]

TRANSMISSION MODES

o The way in which data is transmitted from one device to another device is known as transmission mode.

o The transmission mode is also known as the communication or directional mode and is defined in the physical layer.

o Each communication channel has a direction associated with it, and transmission media provide the direction.

Types of Transmission mode

The Transmission mode is divided into three categories:

o Simplex Mode

o Half-duplex Mode

o Full-duplex mode (Duplex Mode) **- (2)**

1. SIMPLEX MODE

o In Simplex mode, the communication is unidirectional, i.e., the data flow in one direction.

o A device can only send the data but cannot receive it or it can receive the data but cannot send the data.

o This transmission mode is not very popular as mainly communications require the two-way exchange of data. The simplex mode is used in the business field as in sales that do not require any corresponding reply.

o The radio station is a simplex channel as it transmits the signal to the listeners but never allows them to transmit back.o Keyboard and Monitor are the examples of the simplex mode as a keyboard can only accept the data from the user and monitor can only be used to display the data on the screen.

o The main advantage of the simplex mode is that the full capacity of the communication channel can be utilized during transmission.

Advantage of Simplex mode:

o In simplex mode, the station can utilize the entire bandwidth of the communication channel, so that more data can be transmitted at a time.

Disadvantage of Simplex mode:

o Communication is unidirectional, so it has no inter-communication between devices. **- (2)**

2. HALF-DUPLEX MODE

o In a Half-duplex channel, direction can be reversed, i.e., the station can transmit and receive the data as well.
o Messages flow in both the directions, but not at the same time.
o The entire bandwidth of the communication channel is utilized in one direction at a time.
o In half-duplex mode, it is possible to perform the error detection, and if any error occurs, then the receiver requests the sender to retransmit the data.
o A Walkie-talkie is an example of the Half-duplex mode.
o In Walkie-talkie, one party speaks, and another party listens. After a pause, the other speaks and first party listens. Speaking simultaneously will create the distorted sound which cannot be understood.

Advantage of Half-duplex mode:

o In half-duplex mode, both the devices can send and receive the data and also can utilize the entire bandwidth of the communication channel during the transmission of data.

Disadvantage of Half-Duplex mode:

o In half-duplex mode, when one device is sending the data, then another has to wait, this causes the delay in sending the data at the right time. **- (2)**

3. FULL-DUPLEX MODE

o In Full duplex mode, the communication is bi-directional, i.e., the data flow in both the directions.
o Both the stations can send and receive the message simultaneously.
o Full-duplex mode has two simplex channels. One channel has traffic moving in one direction, and another channel has traffic flowing in the opposite direction.
o The Full-duplex mode is the fastest mode of communication between devices.
o The most common example of the full-duplex mode is a Telephone network.When two people are communicating with each other by a telephone line, both can talk and listen at the same time.

Advantage of Full-duplex mode:

o Both the stations can send and receive the data at the same time.

Disadvantage of Full-duplex mode:

o If there is no dedicated path exists between the devices, then the capacity of the communication channel is divided into two parts. **- (2)**

12.a.i) MAC and LLC sublayers: [CO2,K2]

Media Access Control (MAC) Sublayer: The MAC sublayer handles the access to the physical media and controls how devices in a network gain access to the shared communication medium. Its primary functions include: **- (2)**

a. Media Access Control: The MAC sublayer is responsible for managing and controlling access to the network medium to prevent data collisions when multiple devices attempt to transmit simultaneously. It implements various access control mechanisms, such as CSMA/CD (Carrier Sense Multiple Access with Collision Detection) in Ethernet networks.

b. Framing: The MAC sublayer encapsulates higher-level data into frames, adding necessary control information, such as source and destination addresses, error-checking information, and synchronization bits. It prepares the data for transmission over the physical medium.

c. Addressing: MAC sublayer uses physical addresses, also known as MAC addresses or Ethernet addresses, to uniquely identify devices in a network. These addresses are typically assigned by the manufacturer and are embedded in the network interface card (NIC) of each device.

d. Error Detection: The MAC sublayer performs error detection using techniques such as the Cyclic Redundancy Check (CRC). It appends a CRC checksum to each frame, allowing the receiver to verify the integrity of the received data.

Logical Link Control (LLC) Sublayer: The LLC sublayer sits above the MAC sublayer and provides a common interface for different network protocols. Its main functions include: **- (2)**

a. Protocol Multiplexing: The LLC sublayer enables multiplexing of different network layer protocols, allowing multiple protocols to share the same physical medium. It uses Service Access Points (SAPs) to interface with higher-layer protocols.

b. Flow Control: LLC sublayer implements flow control mechanisms to regulate the flow of data between the sender and receiver. It ensures that a fast sender does not overwhelm a slower receiver by using techniques like sliding window protocol.

c. Error Control: The LLC sublayer handles error control at the data link layer. It may implement error detection and retransmission mechanisms to ensure reliable delivery of data.

The **802.3 MAC frame** consists of the following components:

Preamble: A 7-byte field containing alternating 0s and 1s to help the receiver synchronize its clock with the incoming data.

Start Frame Delimiter (SFD): A 1-byte field that marks the end of the preamble and indicates the start of the frame.
Destination MAC Address: A 6-byte field that represents the MAC address of the intended recipient device.

Source MAC Address: A 6-byte field that contains the MAC address of the sender device.

EtherType or Length: A 2-byte field used to indicate either the type of the upper-layer protocol being carried (EtherType) or the length of the payload.

Payload: The actual data being transmitted, which can vary in size. It includes the upper-layer protocol data, such as IP packets or other network layer data.

Frame Check Sequence (FCS): A 4-byte field containing a CRC checksum calculated over the entire frame (including the MAC addresses, EtherType/Length, and payload). It allows the receiver to verify the integrity of the received. **- (4)**

12.a.ii) Checksum calculation: [CO2,K3]

At the Sender Site:

a) Initialize a preset CRC value. Let's say the preset value is 0xFFFF (16 bits).

b) Convert the data items into binary format: Data item 1: 0xABCC (16 bits) -> 1010101111001100 Data item 2: 0x02BC (16 bits) -> 0000001010111100 Data item 3: 0xEEEE (16 bits) -> 1110111011101110

c) Append the preset value (0xFFFF) to the left of the binary data items: Preset value: 1111111111111111 Data item 1: 1010101111001100 Data item 2: 0000001010111100 Data item 3: 1110111011101110

d) Perform the CRC division: Divide the binary representation of each data item by the polynomial 0x8005 (1000000000000101).

e) Apply the CRC algorithm to calculate the remainder (checksum) for each data item: Data item 1: Remainder = CRC(1010101111001100) = 0101011000011001 Data item 2: Remainder = CRC(0000001010111100) = 0100001111011111 Data item 3: Remainder = CRC(1110111011101110) = 1110001011101010

f) The calculated remainders are the CRC checksums for the respective data items: Checksum for Data item 1: 0101011000011001 Checksum for Data item 2: 0100001111011111 Checksum for Data item 3: 1110001011101010 **- (2)**

At the Receiver Site: The receiver needs to check the integrity of the received data using the CRC checksum. Here's how it can be done:

a) Receive the data items and their corresponding checksums.

b) Convert the received data items into binary format.

c) Append the preset value (0xFFFF) to the left of the received binary data items.

d) Perform the CRC division using the same polynomial (0x8005).

e) Calculate the remainder for each received data item.

f) Compare the calculated remainders with the received checksums.

If the calculated remainders match the received checksums for all data items, it indicates that there is no error in the transmitted data. - **(2)**

2) Checksum at the receiver site when the first and second data items are changed.
At the Receiver Site:
a) Initialize the same preset CRC value, 0xFFFF (16 bits).

b) Convert the modified data items into binary format: Modified Data item 1: 0xABCE (16 bits) -> 1010101111001110 Modified Data item 2: 0x02BA (16 bits) -> 0000001010111010 Data item 3: 0xEEEE (16 bits) -> 1110111011101110

c) Append the preset value (0xFFFF) to the left of the binary data items: Preset value: 1111111111111111 Modified Data item 1: 1010101111001110 Modified Data item 2: 0000001010111010 Data item 3: 1110111011101110

d) Perform the CRC division: Divide the binary representation of each data item by the polynomial 0x8005 (1000000000000101).

e) Apply the CRC algorithm to calculate the remainder (checksum) for each data item: Modified Data item 1: Remainder = CRC(1010101111001110) = 0101011000000111 Modified Data item 2: Remainder = CRC(0000001010111010) = 0000000101101010 Data item 3: Remainder = CRC(1110111011101110) = 1110001011101010

f) The calculated remainders are the new CRC checksums for the respective data items: Checksum for Modified Data item 1: 0101011000000111 Checksum for Modified Data item 2: 0000000101101010 Checksum for Data item 3: 1110001011101010

So, the checksum at the receiver site, when the first data item is changed to 0xABCE and the second data item is changed to 0x02BA, are: Checksum for Modified Data item 1: 0101011000000111 Checksum for Modified Data item 2: 0000000101101010 Checksum for Data item 3: 1110001011101010 - **(2)**

(or)

12.b.i) CSMA techniques increase performance and reduce collisions: [CO2,K2]

List of CSMA techniques **- (2)**

Carrier Sense: Before transmitting data, a device implementing CSMA listens to the carrier to check if it is currently busy or idle. If the carrier is busy (i.e., another device is currently transmitting), the device waits until the carrier becomes idle. This carrier sensing mechanism helps avoid collisions by ensuring that multiple devices do not transmit simultaneously.

Collision Detection: In addition to carrier sensing, CSMA techniques often employ collision detection mechanisms. If multiple devices sense an idle carrier at the same time and attempt to transmit simultaneously, collisions can still occur. However, with collision detection, devices can identify collisions during the transmission process. When a collision is detected, the devices involved take specific actions to resolve the collision and retransmit the data.

- (2)

Random Backoff and Exponential Backoff: CSMA-based protocols typically employ backoff mechanisms to minimize the chances of collisions after a detected collision. After a collision, the devices involved wait for a random period of time before attempting to retransmit. This random backoff helps reduce the probability of another collision occurring. If collisions persist, exponential backoff may be applied, where the waiting period is increased exponentially for subsequent retransmission attempts.

- (2)

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA): CSMA/CA is a variation of CSMA used in wireless networks where collision detection is not as effective as in wired networks. CSMA/CA includes additional techniques to minimize the chance of collisions. These techniques involve using acknowledgments, request-to-send (RTS), and clear-to-send (CTS) signals to reserve the wireless medium, as well as a virtual carrier sensing mechanism to avoid hidden node and exposed node problems. **- (2)**

12.b.ii) Working of CRC and single bit error detection: [CO2,K3]

Cyclic Redundancy Check (CRC) is an error-detection technique used to verify the integrity of data transmitted over a network or stored in storage devices. CRC works by generating a checksum, a fixed-size value appended to the data, which can be used to detect any errors during transmission or storage. **- (2)**

1. Dataword: 10110010
2. Polynomial: 1011
3. Append Zeroes: Append three zeroes (the degree of the polynomial minus one) to the dataword: Dataword with zeroes: 10110010000
4. Perform CRC Division: Start with the first four bits of the modified dataword and perform the XOR operation (modulo-2 division) with the polynomial. Repeat this process for the remaining bits.
5.

│ Quotient │ Dividend │

Divisor │ XOR Result │ Remainder │

```
──────────────────┼───────────────────┤ │ │ 10110010000 │ 1011 │ │ │
│ 1 │ 1011 │ │ 0001 │ 0010 │ │ 1 │ 0010 │ │ 0001 │ 0000 │ │ 0 │ 0000 │ │ │ │
│ 0 │ 0000 │ │ │ │ │ 0 │ 0000 │ │ │ │ │ 0 │ 0000 │ │ │ │
└──────────────┴──────────────────────┴──────────────────┴────
──────────────────┴───────────────────┘
```

6. CRC Checksum: The remainder obtained from the division process is the CRC checksum:
CRC Checksum: 0010 - **(4)**

To show that a single-bit error can be detected, let's modify the dataword by flipping one bit and then recalculate the CRC checksum.

Modified Dataword: 10110011

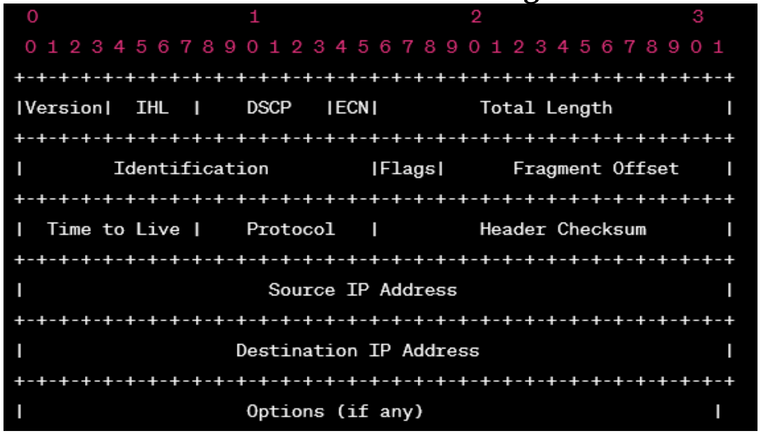
Performing the same CRC division process:

```
┌───────────────┬───────────────────────┬──────────────────┬─────────
─────────────┬──────────────────┐ │ Quotient │ Dividend │ Divisor │ XOR
Result │ Remainder │
├───────────────┼───────────────────────┼──────────────────┼─────────
─────────────┼──────────────────┤ │ │ 10110011000 │ 1011 │ │ │ │ 1 │ 1011 │
│ 0001 │ 0010 │ │ 1 │ 0011 │ │ 0000 │ 0001 │ │ 0 │ 0001 │ │ │ │ │ 0 │ 0000 │ │ │ │
│ 0 │ 0000 │ │ │ │ │ 0 │ 0000 │ │ │ │
└───────────────┴───────────────────────┴──────────────────┴─────────
─────────────┴──────────────────┘
```

The new CRC checksum obtained is 0001. - **(2)**

By comparing the received CRC checksum (0010) with the recalculated CRC checksum (0001) for the modified dataword, we can detect that a single-bit error has occurred. If the checksums do not match, it indicates the presence of an error in the data.

13.a.i) Various fields of IPv4 header and its significance: **[CO3,K2]**



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |    DSCP   |ECN|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source IP Address                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination IP Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options (if any)                          |
```

- **(2)**

Significance of each field in the IPv4 header:

*Version (*4 bits): It indicates the version of the IP protocol being used. For IPv4, the value is 4.

IHL (Internet Header Length) (4 bits): It represents the length of the IPv4 header in 32-bit words. This field is essential for parsing the header correctly.

DSCP (Differentiated Services Code Point) (6 bits): It is used to prioritize packets or provide different levels of service quality for different types of traffic. It allows for Quality of Service (QoS) implementation.

ECN (Explicit Congestion Notification) (2 bits): It provides a mechanism for indicating network congestion to endpoints to ensure a more reliable and efficient data transmission.

Total Length (16 bits): It indicates the total length of the IPv4 packet, including the header and data, measured in bytes.

Identification (16 bits): It is used to uniquely identify a fragmented IP packet and is used for reassembling the fragments at the receiving end.

Flags (3 bits): The flags field contains control bits for IP packet fragmentation. It includes the "Don't Fragment" (DF) bit and the "More Fragments" (MF) bit.

Fragment Offset (13 bits): It specifies the position of the data fragment within the original IP packet. It helps in reassembling the fragments correctly. - **(3)**

Time to Live (TTL) (8 bits): It indicates the maximum number of hops (routers) the packet can traverse before being discarded. Each router decrements the TTL value by 1.

Protocol (8 bits): It indicates the upper-layer protocol to which the packet's payload belongs. For example, TCP has a value of 6, UDP has a value of 17, etc.

Header Checksum (16 bits): It provides error detection for the IPv4 header by verifying the integrity of the header during transmission.

Source IP Address (32 bits): It represents the IP address of the sender or the source of the packet.

Destination IP Address (32 bits): It represents the IP address of the intended recipient or the destination of the packet.

Options (variable length): This field is optional and used for various purposes, such as specifying security options, routing control, or timestamping. If present, it can increase the overall length of the IPv4 header. - **(3)**

13.a.ii) Link state algorithm: **[CO3,K3]**

Step 1: Initialization

1. Create a table to store the information about the nodes and their respective distances from the source node.
2. Set the distance of the source node to 0 and all other nodes' distances to infinity (or a very high value).

Step 2: Selecting the Node with Minimum Distance

Choose the node with the smallest distance as the current node. Initially, this will be node A since its distance is 0.

Step 3: Update Neighboring Nodes

1. For the selected node (current node), calculate the tentative distances from the current node to its neighboring nodes.
2. Compare the tentative distances with the current distances stored in the table. If the tentative distance is smaller, update the table with the new distance and set the current node as the previous node for the neighboring node.

Node	Distance from Source	Previous Node
A	0	None
B	5	A
C	3	A
D	Infinity	None
E	3	B

Step 4: Select the Next Current Node

1. Select the node with the smallest distance from the table, which is node C (with a distance of 3).
2. Repeat the process of updating the table for node C's neighboring nodes.

Node	Distance from Source	Previous Node

A	0	None
B	5	A
C	3	A
D	8	C
E	3	B

Step 5: Continue the Process

1. Select the node with the smallest distance from the table, which is node E (with a distance of 3).
2. Update the table for node E's neighboring nodes.

Node	Distance from Source	Previous Node
A	0	None
B	5	A
C	3	A
D	8	C
E	3	B

Step 6: Final Result

1. Continue this process until all nodes have been selected as the current node.
2. The table will contain the shortest distance from the source node (A) to each of the other nodes, along with their respective previous nodes.

Node	Distance from Source	Previous Node
A	0	None
B	5	A

C	3	A
D	8	C
E	3	B

Each step carries 1 mark

Using the information in the table, we can determine the shortest path from the source node (A) to any other node in the graph. For example, the shortest path from A to D would be A → C → D with a total cost of 8. **- (2)**

(or)

13.b.i) Classful vs classless addressing: [CO3,K2]

Classful addressing and classless addressing are two different approaches to assigning IP addresses and managing IP networks.

1. Classful Addressing:

- In classful addressing, IP addresses are divided into three classes: Class A, Class B, and Class C.
- Each class has a fixed range of IP addresses, with Class A having a large number of network addresses but fewer host addresses, and Class C having a smaller number of network addresses but more host addresses.
- Classful addressing assumes that all networks within a class have the same size.
- It is based on a hierarchical structure, where the first few bits of an IP address determine the class and network portion, and the remaining bits represent the host portion.
- Classful addressing does not allow for subnetting or variable network sizes. **- (2)**

2. Classless Addressing:

- Classless addressing, also known as Classless Inter-Domain Routing (CIDR), was introduced to overcome the limitations of classful addressing.
- In classless addressing, IP addresses are represented with a network prefix, which indicates the number of bits used for the network portion.
- The network prefix can have variable lengths, allowing for more flexible allocation of IP addresses and efficient use of address space.
- Classless addressing supports subnetting, which enables the division of a network into smaller subnets with different sizes.
- It provides more precise control over IP address allocation and allows for efficient utilization of IP address blocks. **- (2)**

Handling the scarcity of IP addresses: Due to the increasing number of devices connected to the internet, the scarcity of IP addresses has become a significant concern. Here are some solutions to address this issue:

1. Network Address Translation (NAT):

- NAT allows multiple devices within a private network to share a single public IP address.
- It translates private IP addresses to a public IP address when communicating over the internet.
- NAT conserves IP address space by reducing the number of globally unique IP addresses required.

2. IPv6 Adoption:

- IPv6 is the latest version of the Internet Protocol, designed to replace IPv4.
- IPv6 uses a 128-bit address space, providing a significantly larger number of unique IP addresses compared to IPv4.
- Transitioning to IPv6 enables the allocation of a much larger pool of IP addresses to accommodate the growing number of devices.

3. IP Address Conservation Techniques:

- Various techniques have been developed to conserve IPv4 addresses, such as:
    - Dynamic IP address allocation: ISPs assign IP addresses dynamically to users, allowing reuse of addresses when not in use.
    - Classless Inter-Domain Routing (CIDR): As mentioned earlier, CIDR allows for efficient allocation of IP addresses by using variable-length network prefixes.
    - Subnetting and supernetting: Subnetting breaks down larger networks into smaller subnets, reducing the number of addresses required per subnet. Supernetting combines multiple smaller networks into a larger one, minimizing the number of routing table entries.

Any two techniques with 2 marks each

13.b.ii) Shortest distance using Bellman-Ford equation: [CO3,K3]

The Bellman-Ford equation is used to find the shortest path between nodes in a weighted graph. It iteratively calculates the shortest distance from a source node to all other nodes.

- (2)

In this case, we have the following distances and costs:

$D(a, y) = 5$ $D(b, y) = 6$ $D(c, y) = 4$ $D(d, y) = 3$ $C(x, a) = 2$ $C(x, b) = 1$ $C(x, c) = 3$ $C(x, d) = 1$

To calculate the shortest distance between node x and node y, D(x, y), using the Bellman-Ford equation, we start by initializing the distance of all nodes except x to positive infinity and the distance of x to 0.

$D(x, x) = 0$ $D(v, x) = \infty$ (for all $v \neq x$)

Then, we iterate through the graph repeatedly, updating the distances until convergence. Each iteration involves relaxing the edges by considering all possible paths from x to other nodes and updating the distances if a shorter path is found.

Here is the step-by-step process:

1. Initialize distances: $D(a, x) = C(x, a) = 2$ $D(b, x) = C(x, b) = 1$ $D(c, x) = C(x, c) = 3$ $D(d, x) = C(x, d) = 1$ $D(y, x) = \infty$
2. Iteration 1: $D(y, x) = \min(D(y, x), D(a, x) + D(a, y)) = \min(\infty, 2 + 5) = 7$
3. Iteration 2: $D(y, x) = \min(D(y, x), D(b, x) + D(b, y)) = \min(7, 1 + 6) = 7$ (no change)
4. Iteration 3: $D(y, x) = \min(D(y, x), D(c, x) + D(c, y)) = \min(7, 3 + 4) = 7$ (no change)
5. Iteration 4: $D(y, x) = \min(D(y, x), D(d, x) + D(d, y)) = \min(7, 1 + 3) = 4$ - **(5)**

After four iterations, the distances have converged, and the shortest distance from node x to node y, D(x, y), is 4. - **(1)**

14.a.i) Services provided by UDP, its header and fields: [CO4,K2]

UDP SERVICES

Process-to-Process Communication

 UDP provides process-to-process communication using socket addresses, a combination of IP addresses and port numbers.

Connectionless Services

 UDP provides a connectionless service.

 There is no connection establishment and no connection termination .

 Each user datagram sent by UDP is an independent datagram.

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

 The user datagrams are not numbered.

 Each user datagram can travel on a different path.

Flow Control

 UDP is a very simple protocol.

 There is no flow control, and hence no window mechanism.

 The receiver may overflow with incoming messages.

 The lack of flow control means that the process using UDP should provide for this service, if needed.

Error Control

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

 This means that the sender does not know if a message has been lost or duplicated.

 When the receiver detects an error through the checksum, the user datagram is silently

discarded.

 The lack of error control means that the process using UDP should provide for this service, if needed. **- (2)**

Checksum

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

 The pseudoheader is the part of the header in which the user datagram is to be encapsulated with some fields filled with 0s.

Optional Inclusion of Checksum

¬ The sender of a UDP packet can choose not to calculate the checksum.

¬ In this case, the checksum field is filled with all 0s before being sent.

¬ In the situation where the sender decides to calculate the checksum,but it happens that the result is all 0s, the checksum is changed to all 1s before the packet is sent.

¬ In other words, the sender complements the sum two times.

Congestion Control

- Since UDP is a connectionless protocol, it does not provide congestion control.
- UDP assumes that the packets sent are small and sporadic(occasionally or at irregular intervals) and cannot create congestion in the network.
- This assumption may or may not be true, when UDP is used for interactive real time transfer of audio and video.

Encapsulation and Decapsulation

- To send a message from one process to another, the UDP protocol encapsulates and decapsulates messages.

Queuing

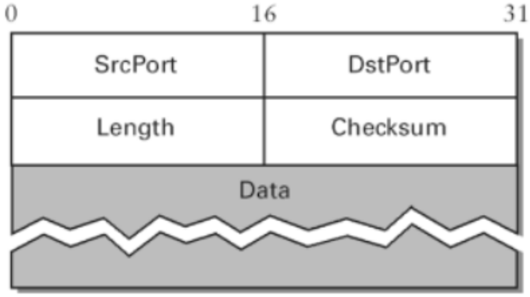
- In UDP, queues are associated with ports.
- At the client site, when a process starts, it requests a port number from the operating system.
- Some implementations create both an incoming and an outgoing queue associated with each process.
- Other implementations create only an incoming queue associated with each process.

Multiplexing and Demultiplexing

- In a host running a transport protocol suite, there is only one UDP but possibly several processes that may want to use the services of UDP.
- To handle this situation, UDP multiplexes and demultiplexes. **- (2)**

UDP DATAGRAM (PACKET) FORMAT

- UDP packets are known as user datagrams.
- These user datagrams, have a fixed-size header of 8 bytes made of four fields, each of 2 bytes (16 bits).



- (2)

Source Port Number

¬ Port number used by process on source host with 16 bits long.

¬ If the source host is client (sending request) then the port number is an temporary one requested by the process and chosen by UDP.

¬ If the source is server (sending response) then it is well known port number.

Destination Port Number

¬ Port number used by process on Destination host with 16 bits long.

¬ If the destination host is the server (a client sending request) then the port number is a well known port number.

¬ If the destination host is client (a server sending response) then port number is an temporary one copied by server from the request packet.

Length

¬ This field denotes the total length of the UDP Packet (Header plus data)

¬ The total length of any UDP datagram can be from 0 to 65,535 bytes.

Checksum

¬ UDP computes its checksum over the UDP header, the contents of the message body, and something called the pseudoheader.

¬ The pseudoheader consists of three fields from the IP header—protocol number, source IP address, destination IP address plus the UDP length field.

Data

¬ Data field defines the actual payload to be transmitted.

¬ Its size is variable. - **(2)**

14.a.ii) Stop and Wait ARQ protocol: **[CO4,K3]**

Given:

- Packet size (data): 1000 bits
- Total data to be sent: 1 million bits (1,000,000 bits)
- Distance between sender and receiver: 2500 km (2,500,000 meters)
- Propagation speed: 1.25 × 10^8 m/s

To calculate the **propagation delay**, we divide the distance by the propagation speed:

Propagation delay = Distance / Propagation speed Propagation delay = 2,500,000 meters / (1.25 × 10^8 m/s) Propagation delay = 0.02 seconds (20 milliseconds) - **(2)**

In the stop-and-wait ARQ protocol, after sending each packet, the sender waits for an acknowledgment (ACK) from the receiver before sending the next packet. So, the total time required to send the data is the sum of the time to transmit the packets and the propagation delay.

To calculate the **time to transmit the packets**, we divide the total data by the packet size:

Number of packets = Total data / Packet size Number of packets = 1,000,000 bits / 1000 bits Number of packets = 1000 packets

Since each packet requires an ACK, the total number of transmissions (including both data and ACK) is twice the number of packets. - **(2)**

Total number of transmissions = 2 * Number of packets Total number of transmissions = 2 * 1000 Total number of transmissions = 2000 transmissions

The time to transmit the packets can be calculated by multiplying the transmission time per packet by the total number of packets:

Transmission time per packet = Packet size / Transmission speed

Since we are ignoring transmission delays, we only need to consider the propagation delay.

Transmission time per packet = Packet size / Transmission speed Transmission time per packet = 1000 bits / Transmission speed - **(2)**

Finally, we calculate the **total time to send 1 million bits**:

Total time = (Transmission time per packet + Propagation delay) * Total number of transmissions

Total time = [(1000 bits / Transmission speed) + 0.02 seconds] * 2000 transmissions - **(2)**

As we don't have the specific transmission speed, we cannot provide a precise time value without that information. However, with the given information, you can substitute the transmission speed into the formula and calculate the total time accordingly.

(or)

14.b.i) Various techniques to improve QoS in networks, its merits and demerits: [CO4,K2]

Quality of Service (QoS) Mechanisms: QoS mechanisms prioritize certain types of network traffic over others to ensure better performance for critical applications. This can be achieved through techniques such as: - **(2)**

- Traffic prioritization: Assigning different priorities to different types of traffic, such as voice or video, to ensure their timely delivery.
- Traffic shaping: Regulating the flow of network traffic to prevent congestion and ensure a smooth user experience.
- Packet classification and marking: Labeling packets based on their priority or class, enabling routers to prioritize and handle them accordingly. - **(2)**

Merits: QoS mechanisms provide control over network resources, ensuring that critical applications receive the required bandwidth and reduced latency. It can enhance the user experience for real-time applications like VoIP or video conferencing. - **(2)**

Demerits: Implementing QoS mechanisms can be complex and require careful configuration. There is also a risk of favoring specific types of traffic over others, potentially leading to unfairness or discrimination. QoS mechanisms may also increase network overhead and introduce additional complexity to network management. - **(2)**

14.b.ii) Bidirectional algorithm for Go-Back-N ARQ protocol using piggybacking: [CO4,K3]

1. Sender-side (Transmitter):

- The sender maintains a window of consecutive sequence numbers for sent frames.
- When a frame is ready to be sent, it is placed in the window and transmitted to the receiver.
- The sender starts a timer for the oldest unacknowledged frame in the window. - **(2)**

2. Receiver-side:

- The receiver maintains a window of consecutive sequence numbers for received frames.

- When a frame is received successfully, it sends an acknowledgment (ACK) frame back to the sender.
- If a frame is received out of order or is detected as an error, the receiver discards the frame but still sends an ACK for the highest in-order frame. - **(2)**

3. Piggybacking:

- The receiver piggybacks its ACK on a data frame when there is an opportunity.
- If the sender receives a data frame with an ACK, it knows that all frames up to that ACKed frame have been successfully received.

4. Timeout and retransmission:

- If the sender's timer expires, it retransmits all unacknowledged frames in the window.
- The receiver, upon receiving a duplicate frame, sends an ACK for the last in-order frame it received. - **(2)**

5. Bidirectional communication:

- Both the sender and receiver can send data frames and ACK frames simultaneously, allowing for bidirectional communication. - **(2)**

15.a.i) Organization of name servers, Iterative and recursive resolution in DNS: [CO5,K2]

The organization of name servers in the Domain Name System (DNS) follows a hierarchical structure, allowing efficient and scalable resolution of domain names. The DNS system consists of multiple types of name servers, including *root servers, top-level domain (TLD) servers, authoritative servers, and caching resolvers.* - **(2)**

Iterative Resolution: In iterative resolution, the resolver sends queries starting from the root server and works its way down the hierarchy until it reaches the authoritative name server. Each server in the hierarchy provides the resolver with the best information it has, such as the address of the next server to contact. The resolver makes subsequent queries to the next server until it receives a response from the authoritative server with the final answer. - **(3)**

Recursive Resolution: In recursive resolution, the resolver delegates the responsibility of finding the answer to the DNS hierarchy. It sends the query to the caching resolver, which performs the iterative resolution on behalf of the client. The caching resolver sends queries to the appropriate servers and collects the responses until it obtains the final answer. Once it has the answer, the caching resolver sends it back to the client. - **(3)**

15.a.ii) Establishing connection to remote system through Telnet: [CO5,K2]

1. *Initiating the Telnet Session:* The user initiates a Telnet session by running a Telnet client program on their local computer. The Telnet client establishes a connection with the Telnet

server running on the remote system.

2. *TCP Connection Establishment:* The Telnet client uses the Transmission Control Protocol (TCP) to establish a connection with the remote system. It sends a TCP SYN (Synchronize) packet to the remote system's IP address and port number associated with the Telnet service (usually port 23).

3. *TCP Handshake:* The remote system's Telnet server receives the SYN packet and responds with a SYN-ACK (Synchronize-Acknowledge) packet, acknowledging the request and indicating its readiness to establish a connection.

- (2)

4. *Client ACKnowledgement:* The Telnet client receives the SYN-ACK packet from the remote system and sends an ACK (Acknowledgment) packet back to the remote system, confirming the connection establishment.

5. *Telnet Protocol Negotiation:* Once the TCP connection is established, the Telnet client and server engage in Telnet protocol negotiation. They exchange various control information to establish the terminal settings and modes for the Telnet session. This negotiation allows both ends to agree on parameters such as character encoding, terminal type, and options like echo mode.

6. *User Authentication:* If required, the Telnet server may prompt the user for authentication credentials (username and password) to verify the user's identity before granting access to the remote system. The authentication process can vary depending on the security configuration of the remote system.

- (2)

7. *Interactive Session:* Upon successful authentication, the Telnet client and server enter an interactive session. The user can now execute commands on the remote system as if they were physically present at the remote terminal. The Telnet client sends user input as individual keystrokes or commands to the Telnet server, which processes and executes them on the remote system.

8. *Data Exchange:* During the Telnet session, the Telnet client sends user input and commands to the Telnet server. The server executes those commands and sends the output back to the client. The client receives the output and displays it on the user's local terminal.

9. *Session Termination:* The Telnet session can be terminated by the user or by the remote system. The user can typically send a command or special character sequence (e.g., Ctrl+] in some Telnet clients) to initiate the session termination. The Telnet client sends a TCP FIN (Finish) packet to the Telnet server, indicating its intention to close the connection. The server responds with a FIN-ACK packet, and both sides acknowledge the termination, closing the connection.

- (2)

Example: Let's say you want to establish a Telnet connection to a remote system with the IP address 192.168.0.100. You run a Telnet client program on your local computer and specify the IP address of the remote system and the Telnet port (usually port 23). The Telnet client establishes a TCP connection with the remote system, negotiates the Telnet protocol settings, and prompts you for authentication if required. Once authenticated, you can interact with the remote system by entering commands and receiving the output on your local terminal. Finally, you can terminate the Telnet session by sending a termination command or closing the Telnet client. **- (2)**

(or)

15.b.i) Architecture of e-mail system in different scenarios: [CO5,K2]

Scenario 1: Sending an Email Locally within the Same Domain:

a. User Composes Email: A user uses an email client application (such as Outlook, Thunderbird, or Gmail) on their device to compose an email message.

b. Local Mail Transfer Agent (MTA): The email client connects to the local Mail Transfer Agent, which is responsible for sending outgoing emails within the same domain.

c. MTA Routes the Email: The local MTA routes the email to the appropriate Mail Delivery Agent (MDA) within the same domain.

d. Mail Delivery Agent (MDA): The MDA receives the email from the MTA and stores it in the recipient's mailbox on the mail server.

e. Recipient Accesses Email: The recipient's email client application connects to the mail server using protocols like POP3 (Post Office Protocol) or IMAP (Internet Message Access Protocol) to retrieve the email from their mailbox. **- (2)**

Scenario 2: Sending an Email to an External Domain:

a. User Composes Email: Similar to Scenario 1, the user composes an email using their email client application.
b. Local MTA: The email client connects to the local MTA.
c. Domain Name System (DNS) Resolution: The MTA checks the email recipient's domain (e.g., recipient@example.com) and performs a DNS lookup to find the Mail Exchange (MX) records for that domain.
d. Routing to the Recipient's Mail Server: The MTA determines the recipient's Mail Exchange server (provided by the MX records) and establishes a connection to that server.
e. Remote MTA: The local MTA hands over the email to the remote MTA responsible for the recipient's domain.
f. Mail Delivery: The remote MTA delivers the email to the appropriate MDA for the recipient's mailbox.
g. Recipient Accesses Email: The recipient's email client retrieves the email from their mailbox on their mail server using POP3 or IMAP. **- (2)**

Scenario 3: Webmail Service:

a. User Composes Email: The user accesses a webmail interface provided by a webmail service (e.g., Gmail, Yahoo Mail) through their web browser.

b. Webmail Server: The webmail service has its own mail server infrastructure. The user's email is composed and stored on the webmail server.

c. Outgoing Email: When the user sends the email, the webmail server acts as the local MTA and follows a similar process as described in Scenario 2 to deliver the email to the recipient's mail server.

d. Incoming Email: When someone sends an email to the user's webmail address, the sender's MTA delivers the email to the recipient webmail server directly using SMTP (Simple Mail Transfer Protocol).

e. User Accesses Email: The user logs into the webmail service using their credentials, and the webmail server presents the email messages stored on their server through the webmail interface. **- (2)**

15.b.ii) Role of SNMP in network management: [CO5,K2]

Device Monitoring and Management: SNMP allows administrators to monitor the status and performance of network devices such as routers, switches, servers, and printers. SNMP agents installed on these devices provide valuable information about device health, utilization, errors, and other metrics. Administrators can use SNMP management systems to collect this data and gain insights into the overall network performance.

Fault Management: SNMP helps detect and report faults in network devices. By monitoring SNMP traps and notifications, administrators can receive real-time alerts about device failures, errors, or unusual events. This allows for proactive fault management, enabling swift identification and resolution of network issues.

- (3)

Configuration Management: SNMP facilitates the management and configuration of network devices. Administrators can use SNMP to remotely modify device settings, update firmware, and configure parameters such as IP addresses, routing tables, and access control policies. SNMP's standardized protocol allows for seamless and consistent configuration across various network devices.

Performance Monitoring: SNMP enables performance monitoring by collecting and analyzing data on network device performance and utilization. SNMP management systems can retrieve SNMP variables, such as CPU usage, memory utilization, network traffic, and interface statistics, allowing administrators to identify performance bottlenecks, plan capacity upgrades, and optimize network resources.

- (2)

Network Inventory and Asset Management: SNMP assists in maintaining an inventory of network devices and their attributes. By querying SNMP-enabled devices, administrators can gather information such as device type, manufacturer, model, firmware version, and serial number. This helps in asset tracking, license management, and ensuring hardware compatibility in the network environment.

Security Management: SNMP supports security management by providing authentication and access control mechanisms. SNMPv3, the most secure version of SNMP, incorporates features such as message encryption, user authentication, and access control lists (ACLs). These features help safeguard SNMP communications and ensure that only authorized administrators can access and manage network devices.

Trend Analysis and Reporting: By collecting historical SNMP data, administrators can perform trend analysis and generate reports on network performance, availability, and resource utilization. This information is valuable for capacity planning, troubleshooting, and evaluating network performance against defined service level agreements (SLAs). **- (3)**

Bloom's Taxonomy Level	Remembering (K1)	Understanding (K2)	Applying (K3)	Analysing (K4)	Evaluating (K5)	Creating (K6)
Percentage	21	47	32	--	--	--