Introduction to Computer Networks

1. Define protocol and explain its elements.
2. Describe the TCP/IP model and its layers.
3. Discuss function of each layer of TCP/IP protocol in detail.
4. Differentiate between Local Area Networks (LANs) and Wide Area Networks (WANs) with suitable examples.
5. Differentiate between a Local Area Network and a Wide Area Network. What is a Metropolitan Area Network (MAN), and how does it differ from a LAN and a WAN?
6. Differentiate among simplex, half-duplex, and full duplex modes of data flow in computer networks.
7. List and explain various interconnecting devices used in computer networks.
8. Briefly explain the OSI Model and its seven layers. Explain the functionality of each layer.
9. Differentiate the TCP/IP model and the OSI model. In which layer of the OSI model does data encryption typically occur, and how is this handled in the TCP/IP model? Explain the purpose of the Trailer at Data Link Layer.
10. Explain what headers and trailers are in networking, and describe how they are added and removed during data transmission.
11. Explain the role and functionality of the Transport Layer in the OSI model. How does it ensure reliable communication between devices?

Network Performance and Transmission Impairments

1. Describe transmission delay and propagation delay in computer networks.
2. Differentiate between bit rate and baud rate with an example.
3. Describe Data Rate Limits?
4. Explain the concept of calculating data rate for a noisy and noiseless channel.
5. Find the maximum bit rate for a noiseless channel with a bandwidth of 3000 Hz transmitting a signal with two signal levels.
6. A signal transmission begins through a medium with power "Pi" and its power is reduced to one-fourth at the receiver side. Determine the attenuation (loss of power) in decibels.
7. A signal travels through a transmission medium and its power is reduced to one third. Calculate the attenuation (loss of power) in decibel?
8. Assume that SNRdB=36 and the channel bandwidth is 4 MHz. Determine the channel capacity.
9. Calculate the transmission time required to send a frame of 1000 bits, given a sender's transmission rate of 1 Mbps.
10. Calculate the propagation time for a frame to travel from the sender to the receiver if they are located 500 kilometers apart, given a propagation speed of 2 x 10^8 meters per second.
11. Calculate the total time it takes for the sender to receive an acknowledgment from the receiver if the acknowledgment is sent immediately upon receiving the frame, using the Stop-and-Wait protocol.
12. Find the values for propagation delay and transmission delay for a 10 Mbyte message if the bandwidth of the network is 5 Mbps. Assume that the distance between the sender and the receiver is 25,000 km and that the signal travels at 3x10^8 m/s.
13. A channel has a 1-MHz bandwidth. The SNR for this channel is 63. Compute the capacity of the channel.
14. Compute the propagation time (in milliseconds) and the transmission time (in seconds) for a 4MByte message if the bandwidth of the network is 1 Mbps? Assume that the distance between the sender and the receiver is 36,000 km and that light travels at 2.4 x 10^8 m/s.

15. In digital transmission, the receiver clock is 0.1 percent faster than the sender clock. How many extra bits per second does the receiver receive if the data rate is 1 Kbps? How many if the data rate is 1 Mbps?
16. A signal has two data levels with a pulse duration of 1 ms. What will be the pulse rate and bit rate of the signal?

Energy Efficient Line Encoding

1. Draw the signal pattern for the binary data 11001011 using NRZ-I, NRZ-L, Manchester, Differential Manchester and AMI line coding techniques, assuming that the previous signal level was positive. Additionally, describe the advantages and disadvantages of each technique.
2. List and explain any three line-encoding schemes.
3. Apply the following coding techniques to the digital signal 1100101 and draw the signal pattern, assuming that the last signal level as positive: Polar NRZ-L, Polar NRZ-I, Polar RZ, Differential Manchester, Bi-Polar AMI.
4. Given that the previous signal level was positive, draw the signal pattern for the data 110100 using Polar RZ, Differential-Manchester, Unipolar NRZ, Bi-polar AMI, and 2B1Q coding techniques.
5. Explain and apply the NRZ and NRZ-I encoding algorithms to the data pattern 1011001011000111.
6. Explain and apply the RZ encoding algorithm to the data pattern 1011001011000111.
7. Explain and apply the Manchester encoding algorithm to the data pattern 1011001011000111.
8. Explain and apply the AMI encoding algorithm to the data pattern 1011001011000111.
9. Explain and apply the Pseudoternary encoding algorithm to the data pattern 1011001011000111.
10. Explain and apply the 2B1Q encoding algorithm to the data pattern 1011001011000111.

Switching Techniques

1. Differentiate between the three primary switching techniques: Circuit Switching, Packet Switching, and Message Switching. Provide examples of scenarios where each is most suitable.

Switching and Multiplexing Techniques

1. Four channels are multiplexed using synchronous Time Division Multiplexing. Suppose each channel sends 200 bytes/s and the multiplexer multiplexes 1 byte per channel. Determine the size of the frame, the duration of a frame, the frame rate, and the bit rate for the link.
2. Explain synchronous Time Division Multiplexing (TDM).
3. Five channels are multiplexed using TDM. If each channel sends 1000 bytes/s and we multiplex 1 byte per channel, show the frame traveling on the link, the size of the frame, the duration of a frame, the frame rate, and the bit rate for the link.
4. Explain how multiplexing and demultiplexing work.
5. Describe the concept of switching in computer networks. Provide a scenario where virtual circuit switching would be preferable over packet switching, and justify your choice.

Networking Devices

1. Mention which network devices break collision domains and broadcast domains.
2. Differentiate Repeater, Bridge and Hub. Also explain on which layer of TCP/IP Model, these components work.
3. Differentiate between Passive hub and repeater.

4. Explain the functions of a router.
5. Explain the functions of a switch.
6. Explain the functions of a repeater.
7. Provide a detailed description of the following network devices, including their operational mechanisms and functions within a network environment: Router, Hub, Switch
8. How does a bridge differ from a hub in terms of frame forwarding?
9. A network segment has a maximum cable length of 100 meters for reliable communication. If a repeater is added to the segment, describe how the repeater helps extend the network?
10. Differentiate among the functionalities of the hub, switch, and router with suitable examples.

Networking Topologies

1. What is a network topology? Explain the different types of network topologies.
2. Describe the advantages and disadvantages of bus network topology.
3. Discuss the advantages and disadvantages of Bus, Star, and Ring networking topologies.
4. Explain the ring topology, including its advantages and disadvantages.
5. Explain the star topology, including its advantages and disadvantages.
6. Describe how scalability differs between bus and star topologies as the number of nodes increases. What are the technical and physical limitations that come into play?
7. Compare the fault tolerance capabilities of ring, mesh, and star topologies. How does the degree of redundancy influence recovery time in each case?
8. A company wants to set up a new office network for 50 employees. Which topology would you recommend and why?
9. Compare and contrast the efficiency, scalability, and fault tolerance of four different topologies.
10. Consider 10 devices to create star, ring and bus topologies. Form such connections and find the number of cables and the number of ports required with devices in each case.
11. A university plans to set up a new network for its campus that requires high reliability and redundancy, ensuring that if one connection fails, others can still maintain communication. Select an appropriate topology for the given scenario.

Local Area Networks

1. If a switch is replaced by a hub in a LAN, what impact would it have on network efficiency?
2. Can switches completely eliminate collisions in Ethernet networks? Why or why not?
3. Discuss the collision domain and broadcast domain of the following interconnecting devices: Hub, Switch, Bridge, Router.
4. A university campus with three buildings needs a network. Each building has 200 devices, and all need access to the internet. Recommend a networking technology and justify its suitability.

Multiple Access Protocols

1. Explain the flowchart to demonstrate the working of the CSMA/CD protocol.
2. Explain how CSMA/CD works.
3. Define the term carrier sense in CSMA/CD.
4. Explain the working of the "p-persistent" CSMA persistence method with a suitable example.
5. Design a flowchart to represent the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) protocol's collision handling process, specifically focusing on the collision detection and abortion mechanism.

6. In CSMA (Carrier Sense Multiple Access) protocols, persistence methods play a critical role in managing how a station attempts to access the medium when it detects the carrier is idle. Explain the 1-persistent, Non-persistent, and p-persistent persistence methods in CSMA.
7. Explain the terms contention window and back off strategy with suitable examples.
8. Explain the terms NAV, and RTS and CTS with suitable examples.

Error Detection and Control

1. You want to send a 10-bit message (1101010110) using a CRC technique, where the CRC generator is 1011. Calculate the CRC code that needs to be appended to the message before transmission. Show your step-by-step calculations.
2. A bit stream 101001101 is transmitted using the standard CRC method. The generator polynomial is 11011. Obtain the actual bit string transmitted.
3. The following decimal numbers represent the 4-bit segments of a data message: 11, 6, 9, and 3. Compute the checksum value for the data message.
4. A 9-bit dataword 100110111 is being transmitted over a noisy channel using CRC with the generator 10011. Compute the CRC bits and the final codeword. If the received codeword is 100111111, determine whether the received message is error-free or corrupted.
5. Bob and Alice have shared a CRC generator 1001. Then Bob sent a codeword to Alice. Assume that Alice received the codeword '1010011'. Compute whether there is an error or not in the received codeword and also find the received dataword using CRC decoder.
6. Mention and explain any two error control techniques other than CRC with the help of an example.
7. Let the output after byte-stuffing is FLAG A B ESC ESC C ESC ESC ESC FLAG ESC FLAG D FLAG. Find the original data?
8. A bit string, 01111011111101111110, needs to be transmitted at the data link layer. What is the string actually transmitted after bit stuffing, assuming a flag of 01111110?
9. A binary string 10101111 is to be encoded using an even-parity Hamming code. How many check bits are needed to ensure that the receiver can detect and correct single-bit errors? Show the bit pattern transmitted.
10. Explain the Checksum error-detection technique.
11. Explain the Cyclic Redundancy Check (CRC) error-detection technique.
12. In the CRC checksum method, assume that the given frame for transmission is 1101011011 and the generator polynomial is G(x) = x4+x1+1. After implementing the CRC encoder, calculate the encoded-word sent from the sender side.
13. The following data is transmitted using the checksum method for error detection: 10011001111000100010010010000100. Divide the data into 8-bit words and calculate the checksum. Show all the steps involved in adding the 8-bit words and finding the complement.
14. At the receiver's side, perform the sum of all received 8-bit words including the checksum. What should the result be if no error occurred? Explain your answer.
15. Explain the data packet lost problem and missing packet problem in Stop-and-Wait protocol, along with their solutions using a timeline diagram.
16. Explain the duplicate packet problem in Stop-and-Wait protocol, along with solutions using a timeline diagram.
17. Consider the message 1101011011 that needs to be sent over a network. The divisor (or generator polynomial) used for CRC is 1011. Perform the CRC encoding process to find the remainder. Show the steps of division and the final CRC code that will be appended to the original message.

Reliable Data Delivery

1. Explain Automatic Repeat Request (ARQ).
2. Discuss the working of the stop-and-wait ARQ protocol with a suitable example.
3. In Go Back N, if every 7th packet that is being transmitted is lost and we have to send 15 packets, then how many transmissions are required?
4. In Go-back-N ARQ, explain with an example why the size of the sender window must be less than 2^m, where m is the number of bits used for the representation of sequence numbers.
5. State four points of difference between Stop and Wait and Go-Back-N protocol.
6. Describe how the Go-Back-N handles different missing data transmission through a timeline diagram.
7. Explain the reason for moving from the Stop-and-Wait Protocol to the Go-Back-N Protocol. Compare and contrast the Go-Back-N Protocol with Selective-Repeat with a suitable example.
8. Using 5-bit sequence numbers, what is the maximum size of the send and receive windows for Stop-and-Wait ARQ?
9. Using 5-bit sequence numbers, what is the maximum size of the send and receive windows for Go-Back-N ARQ?
10. Using 5-bit sequence numbers, what is the maximum size of the send and receive windows for Selective-Repeat ARQ?
11. If 4-bits are being used for sequence number, what will be the sequence number of the 30th frame if selective repeat protocol is employed.
12. Describe a scenario where a client is communicating with a server to download a file reliably, ensuring data is delivered in the correct order, lost or corrupted packets are retransmitted, and a connection is established before data transfer begins. Identify the protocol used.
13. Explain the general header format for the protocol used for reliable file transfer.
14. Explain the working principle of the Go-Back-N sliding window protocol. How does it handle the transmission of frames, and what happens if a frame is lost or corrupted? Discuss the significance of the window size in sliding window protocols.
15. Justify the way in which the receiver handle the out-of-order delivery of frames in the Go-Back-N protocol? How does this differ from the Selective Repeat protocol?

Flow Control

1. In a network communication system using the sliding window protocol, the propagation time is given as 1 ms and the transmission time is given as 49.5 ms. What should be the sender window size to get maximum efficiency?
2. In a network communication system using the sliding window protocol, the propagation time is given as 1 ms and the transmission time is given as 49.5 ms. What should be the minimum number of bits in the sequence field?
3. In a network communication system using the sliding window protocol, the propagation time is given as 1 ms and the transmission time is given as 49.5 ms. Assume that the number of bits in the sequence field is set to 5, then what is the maximum efficiency that we could get?
4. Describe the process of TCP flow control using the Advertisement Window during data transmission.
5. Discuss the implications of a smaller or larger Advertisement Window size on the efficiency of data transfer and network utilization.
6. Discuss the sliding window flow-control mechanism. Provide an example to justify your answer.
7. Differentiate Flow Control and Error Control. On which layer of TCP/IP Model, this mechanism takes place.

Routing and Forwarding

1. Define routing.
2. Define forwarding.
3. Explain Link state routing in detail.
4. Find shortest path from node 1 to node 6 using Dijkstra Algorithm with proper steps.
5. Difference between Interior Gateway Protocols (IGP) and Exterior Gateway Protocols (EGP).
6. Difference between Distance Vector Routing and Link State Routing.
7. Using Dijkstra's Algorithm, find the shortest path from Node A (start node) to all other nodes (B, C, D, E, F) in a given network with specified edge weights. Show the step-by-step process of Dijkstra's Algorithm.
8. Differentiate between Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) Protocol.
9. Differentiate RIPv2 with OSPF.
10. Specify the circumstances under which an end-host and router send an ICMP message.
11. Explain how to prepare the link state packet for each router when the link state routing protocol is implemented on routers. Also, explain how to create the Link State Database for a specific router when it receives the link state packets from every other router in the network.
12. Explain the concept of Distance Vector and Link state routing with examples.
13. Explain the three-way handshake mechanism used by TCP to establish a connection, and discuss the purpose of each step in the handshake process.
14. Describe the Leaky Bucket and Token Bucket algorithms used for congestion control. How do they regulate traffic flow?
15. Explain how to create a bridge learning table and describe all the steps for each entry in the table.
16. Explain the initial Distance Vector table for each node and find the shortest path from node A to node I of a network using the Distance Vector Routing protocol.
17. Illustrate the working of the OSPF protocol.
18. Your router has the following IP address on Ethernet0: 172.16.2.1/23. What is the range of valid host IDs (IPs) on the LAN interface attached to the router?
19. What is Dijkstra's algorithm? Illustrate its working to find the shortest path in a given network graph.

Routing (Static vs Dynamic)

1. Explain the advantages and disadvantages of dynamic routing.

Congestion Control

1. Explain the Congestion Control Policies and why is it important in network communication? How does congestion affect overall network performance and throughput? In implicit signaling, how do end systems detect congestion without explicit feedback from the network? Provide examples.
2. Describe the following closed-loop congestion control approaches: backpressure and choke packet.
3. Describe the behaviour of the TCP congestion control mechanism, specifying the time intervals where the TCP slow start and congestion avoidance phase starts, and the events that occur after the 16th and 22nd transmission round.

4. Illustrate the significance of the Backpressure closed-loop congestion control mechanism with suitable examples.
5. Illustrate the significance of the Explicit Signaling closed-loop congestion control mechanism with suitable examples.
6. Mark the following statement as True or False with justification: Congestion can be overcome if routers have an unlimited amount of storage for buffering packets.
7. What is a choke packet? How does congestion in the network occur? Explain the two broad categories of congestion control mechanisms.
8. Explain two policies each at the Transport, network, and data link layer to prevent congestion in the network.
9. What is congestion Control. Discuss any two open loop and two closed loop congestion control techniques in detail.
10. Explain the concept of congestion control in computer networks. Why is congestion control important for network performance?

Traffic Shaping

1. What is traffic shaping? Discuss the two techniques of traffic and their implementation.

IP Addressing and Subnetting

1. An organization is granted an address block 172.168.5.0/24. The administrator wants to create 32 subnets. Find the subnet mask. Also, find the first and last addresses in the first subnet.
2. Given a subnet mask as 255.255.255.224, deduce the total number of bits required to represent the number of hosts in the network, the total number of hosts that can be configured in the network, the total number of subnets if the network is Class A, and the total number of subnets if the network is Class C.
3. An ISP has a block of 1024 addresses. It needs to divide the addresses among 1024 customers. Does it need subnetting? Justify.
4. An ISP is granted a block of addresses starting with 120.60.4.0/22. The ISP wants to distribute these blocks to 50 organizations. Each organization needs 12 addresses. Design the subblocks and give the slash notation for each subblock. Find out available addresses after these allocations.
5. An organization is granted the block 101.17.100.0/24. The administrator wants to create 32 subnets of equal length in the block. Find the subnet mask.
6. An organization is granted the block 101.17.100.0/24. The administrator wants to create 32 subnets of equal length in the block. Find the number of addresses in each subnet.
7. An organization is granted the block 101.17.100.0/24. The administrator wants to create 32 subnets of equal length in the block. Find the first and last addresses in the first subnet.
8. An organization is granted the block 101.17.100.0/24. The administrator wants to create 32 subnets of equal length in the block. Find the first and last addresses in the last subnet.
9. What is subnetting? Consider a big single network having IP Address 100.11.22./24. It is to be subdivided into 4 subnets of equal size. Calculate the network address of each subnet, the total number of IP Addresses for each subnet, the total number of hosts that can be configured for each subnet and the range of IP Addresses for each subnet.
10. Given IP address of a host machine is 192.168.6.33/27. Find Network ID and Broadcast IP of its network?
11. One of the IP addresses of a given subnet is 170.24.56.74/22. Find the subnet-id, first IP address, and last IP address of the hosts in this subnet.

12. You are given a subnet mask as 255. 255. 254. 0. Deduce the total number of hosts that can be configured in the network.
13. You are given a subnet mask as 255. 255. 254. 0. Deduce the total number of subnets if the network is Class A.
14. Assume that 256 host address space is available at 202.224.154.0. Suppose that four groups A, B, C, and D, request 100, 55, 30 and 20 addresses, respectively. For each of these, give the first IP address assigned, the last IP address assigned, and the mask in the w.x.y.z/s notation.
15. Using the IP address and subnet mask, write out the network address for 192.149.24.191/24.
16. Using the IP address and subnet mask, write out the network address for 191.55.165.135/27.
17. Using the IP address and subnet mask, write out the network address for 200.10.5.68/28.
18. You have a network that needs 29 subnets while maximizing the number of host addresses available on each subnet. How many bits must you borrow from the host field to provide the correct subnet mask?
19. Discuss Classful IP addressing in detail. What is address inefficiency?
20. What is subnetting? An organization is assigned a class C network address of 201.35.2.0. The network administrator wants to create 3 sub-network. What will be the subnet Mask and the range of addresses in each sub-network.
21. Subnet the address 202.2.1.0/24 into subnets, each capable of supporting 64 hosts per subnet. Determine the new subnet mask to accommodate 64 hosts per subnet. For all the subnets created, provide the subnet address, first usable IP address, last usable IP address, and broadcast address.
22. An organization is assigned the IP address 192.168.1.0/26. Determine the subnet mask in dotted decimal format. Calculate the number of usable host addresses in this subnet. Identify the first usable IP address in the subnet. Identify the last usable IP address in the subnet. Determine the broadcast address for this subnet.
23. What is a classful addressing, and what role does it play in computer networks?

Network Layer Protocols

1. Illustrate an autonomous system with eight networks (N1 to N8) and eight routers (R1 to R8) where N1, N2, N3, N4, N5, and N6 are Ethernet LANs and N7 and N8 are point-to-point WANs. Router R1 connects N1 and N2, R2 connects N1 and N7, R3 connects N2 and N8, R4 connects N7 and N6, R5 connects N6 and N3, R6 connects N6 and N4, R7 connects N6 and N5, and R8 connects N8 and N5. Identify transient and stub network in this autonomous system.
2. Differentiate between IPv4 and IPv6.
3. Explain the concept and need of Fragmentation offset and TTL.

IPv4 Datagrams

1. Explain the significance of the Identification, Flags, and Time-to-live (TTL) fields in IPv4 header format.
2. In an IPv4 datagram, the M bit is 0, the value of HLEN is 5, the value of total length is 200, and the offset value is 200. Find out the number of the first byte and last byte in this datagram. How many bytes of data were originally sent by the source before the data in this fragment.
3. An IPv4 datagram has arrived with the following information in the header (in hexadecimal notation) 0x47 00 11 CC 70 11 22 52 25 87 11 15 1B E4 11 80 32 FE 15 11. Find out the size of the data in the datagram, source, and destination IP address (dotted decimal notation).
4. Illustrate the use of "Header Length" and "Protocol" fields in the IPv4 header format with a suitable example.

5. Consider an IP datagram with the More Fragments field value of 1 and the Total length field value as 2400. Also consider that the MTU of the underlying data link layer is 400 bytes. In how many fragments will the original IP datagram be fragmented? For each fragment, find the value of the Don't Fragment and More Fragments flags, offset field, identification field, and Total length field.
6. Which field of the IPv4 header changes from router to router?
7. What is the maximum data that the datagram at network layer can carry in a network with a Maximum Transmission Unit (MTU) of 200 bytes and an IP header of 20 bytes?
8. Suppose a datagram in network A with a Maximum Transmission Unit (MTU) of 520 bytes and an IP header of 20 bytes has to be sent to network B with a Maximum Transmission Unit (MTU) of 200 bytes and an IP header of 20 bytes. In network A, how many fragments will a datagram has to be fragmented and why?
9. Discuss the potential impact of fragmentation on network performance and efficiency.
10. Identify and explain the purpose of any six key fields in the IPv4 header.
11. A datagram of 3000 bytes (20 bytes of IP header + 2980 bytes IP payload) is being received at the router and to be forwarded to a link with MTU of 500 bytes. Find out the number of generated fragments, and the offset and total length for each fragment.
12. Draw IPV4 frame format.
13. An IPv4 packet has arrived with the first 8 bits as shown: 01000010 The receiver discards the packet. Why?
14. In an IPv4 packet, the value of HLEN is 1000 in binary. How many bytes of options are being carried by this packet?
15. In an IPv4 packet, the value of HLEN is 5, and the value of the total length field is 0x0028. How many bytes of data are being carried by this packet?
16. Explain the significance of an IPv4 packet header. List and describe the key fields present in the header, such as Version, Header Length, Total Length, and Time to Live (TTL).

Address Resolution Protocol (ARP)

1. Explain the working of Address Resolution Protocol (ARP). Define Proxy ARP.
2. Explain the key role of ARP in facilitating communication between devices within a local network.
3. Explain the ARP Packet Format.
4. Differentiate between ARP and RARP

Internet Control Message Protocol (ICMP)

1. Define ICMP and explain its role in the Internet Protocol suite. Highlight specific scenarios where ICMP is instrumental in network communication.
2. Identify and describe two ICMP message types commonly used for network troubleshooting. Provide an example of a situation where each message type would be deployed.
3. Explain the significance of the Source Quench ICMP error-reporting message.
4. Explain the significance of the Redirection ICMP error-reporting message.
5. Explain the ICMP protocol.

Dynamic Host Configuration Protocol (DHCP)

1. Describe the header format of Dynamic Host Configuration Protocol (DHCP).
2. Mark the following statement as True or False with justification: DHCP allows both manual and automatic assignments of IP addresses.

Process to Process Delivery (TCP/UDP)

1. Describe the header format of Transmission Control Protocol (TCP).
2. Compare TCP and UDP headers. List the fields in the TCP header that are missing from UDP header. Give the reason for their absence.
3. Draw the TCP Segment Format. Discuss the significance of the Window size field in this segment format.
4. Draw the TCP Segment Format. Discuss the significance of the Urgent pointer field in this segment format.
5. Explain the various parts of the UDP header.
6. Explain the various parts of the TCP header.
7. Why is the total length field missing in the TCP header?
8. Explain the process of connection establishment and connection termination phase of a TCP connection.
9. What is the minimum size of process data that can be encapsulated in a UDP datagram?
10. Suppose Alice, a corporate professional, needs to send a confidential email to Bob, a colleague in a different geographical location. Discuss and explain the essential application layer protocols required for ensuring a reliable email communication.
11. Discuss connection establishment, data transfer and connection termination phase of TCP with the help of timing diagrams. Assume a suitable value of random sequence number generated.
12. Describe the frame format of reliable and connection oriented transmission control protocol.

TCP Connection Establishment

1. Describe the three-way handshake process used during the establishment of a TCP connection. Provide a step-by-step explanation of the sequence of messages exchanged between the client and server.
2. Explain the TCP three-way handshake process with a labeled diagram. Why is it essential for establishing a reliable connection?

TCP Header Flags

1. Explain the significance of any four flags in the TCP (Transmission Control Protocol) header. Provide a detailed explanation for each flag and discuss their roles in facilitating reliable communication.

Stream Control Transmission Protocol (SCTP)

1. Define the term Transmission sequence number as used in Stream Control Transmission Protocol.
2. Define the term Stream sequence number as used in Stream Control Transmission Protocol.
3. Explain Stream Control Transmission Protocol (SCTP).

Sustainable Network Applications

1. Explain the DNS protocol.
2. Explain the SMTP protocol.
3. Which IP address would you ping to test the IP stack on the local host? Write a command to test it.
4. Discuss general architecture of an e-mail system including the three main components: user agent, message transfer agent, and message access agent.

5. A user wants to use a file transfer client to access a file transfer server running on a remote host. The user only knows the server name, such as afilesource.com. The TCP/IP suite uses DNS to resolve the hostname to an IP address before establishing a connection. List the six steps involved in resolving the hostname to an IP address using a DNS client and DNS server.
6. What is DNS (Domain Name System)? Explain how DNS resolves a domain name to an IP address.

IEEE 802.11

1. Draw the IEEE 802.11 frame format. Explain the sub-fields of the Frame Control (FC) field of the header.

Miscellaneous

1. If a periodic signal is decomposed into five sine waves with frequencies of 10, 50, 70, 80, and 120 Hz, then determine its bandwidth. Draw the spectrum, assuming all components have a maximum amplitude of 5 V.
2. Define piggybacking and its advantages.
3. In a leaky bucket system if the output rate is 5 KB/sec and input burst of 50 KB/sec for 10 sec and 10 KB/sec for 50 sec. Find out the bucket size in KB.
4. Explain what ping is.
5. Explain what pop is.
6. Explain what IMAP is.
7. Why are port addresses shorter than IP addresses?
8. An IPv4 fragment has arrived with an offset value of 100. How many bytes of data were originally sent by the source before the data in this fragment.
9. Mark the following statements as True or False with justification: The fragmenting policy in the IP layer dictates that fragment offsets be multiples of 8 bytes, therefore IP packets with less than 8 bytes of payload are not allowed.
10. Mark the following statement as True or False with justification: The network layer uses physical addresses to route data to destination hosts.