R18

Code No: 155AN

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech III Year I Semester Examinations, January/February - 2023
COMPUTER NETWORKS
(Common to CSE, CSBS, CESE, CSE(AIML), CSE(DS), CSE(IOT))

Time: 3 Hours **Max. Marks: 75**

Note: i) Question paper consists of Part A, Part B.
ii) Part A is compulsory, which carries 25 marks. In Part A, Answer all questions.
iii) In Part B, Answer any one question from each unit. Each question carries 10 marks and may have a, b as sub questions.

PART – A

(25 Marks)

1.a)	What is ARPANET?	[2]
b)	Write about Co-axial cable transmission media?	[3]
c)	What is framing?	[2]
d)	What are the advantages of sliding window protocol?	[3]
e)	What is non-adaptive routing?	[2]
f)	What is meant by congestion?	[3]
g)	What is the function of transport layer?	[2]
h)	What is UDP?	[3]
i)	What is the function of application layer?	[2]
j)	What is DNS?	[3]

PART – B

(50 Marks)

2.	Explain the TCP/IP reference model.	[10]
	OR	
3.	Explain about fiber optics transmission media.	[10]
4.	Explain the stop-and-wait protocol.	[10]
	OR	
5.	Explain about wireless LAN.	[10]
6.	Explain the shortest-path routing algorithm.	[10]
	OR	
7.a)	Explain the IPV4 header.	
b)	What is packet fragmentation?	[5+5]
8.	Explain the elements of transport layer.	[10]
	OR	
9.	Explain the TCP transmission policy.	[10]
10.	Explain about HTTP.	[10]
	OR	
11.	Explain about streaming audio.	[10]

---ooOoo---

Answer key

PART - A

1. a) What is ARPANET?

ARPANET was the precursor to the modern internet, developed by the US Department of Defense. It was the first network to use packet switching, laying the foundation for today's interconnected networks.

b)Write about Co-axial cable transmission media?

Coaxial cables are used for transmitting electrical signals, commonly in television and internet applications. They consist of a central copper conductor surrounded by an insulating layer, a conductive shield, and an outer insulating layer, providing good noise immunity and bandwidth.

c)What is framing?

Framing refers to the process of dividing data into manageable units for transmission over a network. It involves adding special control characters or bits at the beginning and end of data packets to delineate them from other packets.

d)What are the advantages of sliding window protocol?

Sliding window protocols allow for efficient flow control and error recovery in data transmission. They optimize network bandwidth by enabling multiple frames to be in transit simultaneously, thus improving throughput.

e)What is non-adaptive routing?

Non-adaptive routing uses fixed paths for data transmission regardless of network conditions or traffic load. It lacks the ability to dynamically adjust routes based on real-time changes in the network.

f)What is meant by congestion?

Congestion occurs when network resources, such as bandwidth or router processing capacity, are overloaded by excessive data traffic. It leads to increased delays, packet loss, and reduced network performance.

g)What is the function of transport layer?

The transport layer ensures reliable data transfer between nodes on a network. It manages end-to-end communication, error-checking, flow control, and

multiplexing/demultiplexing of data streams.

h)What is UDP?

UDP (User Datagram Protocol) is a connectionless protocol in the transport layer of the Internet Protocol suite. It provides a simple, unreliable, and low-overhead way to send datagrams between hosts without error-checking or flow control.

i)What is the function of application layer?

The application layer enables communication between applications or software programs running on different devices. It provides protocols and data structures for specific tasks like email, file transfer, and remote access.

j)What is DNS?

DNS (Domain Name System) is a decentralized naming system for computers, services, or other resources connected to the internet. It translates domain names (like example.com) into IP addresses that computers use to identify each other on the network.

PART - B

2. Explain the TCP/IP reference model.

1.Layers: TCP/IP model has four layers: Application, Transport, Internet, and Link.
2.Application Layer: Handles communication functions between applications, like HTTP, FTP, SMTP.
3.Transport Layer: Provides reliable data transfer (TCP) or best-effort (UDP) between hosts.
4.Internet Layer: Routes data packets across networks using IP addresses.
5.Link Layer: Deals with physical connections and data framing over the network medium.
6.Packet: Information is broken into packets at the internet layer for transmission.
7.Routing: Determines the best path for packets to reach their destination.
8.Protocols: TCP, UDP, IP, and others define rules for communication and data handling.
9.Decentralized: Unlike OSI, TCP/IP model is not strictly hierarchical.
10.Foundation: Basis for the modern internet, designed for robustness and scalability.

3. Explain about fiber optics transmission media.

1.Structure: Consists of a core (inner optical material) surrounded by cladding (outer material with lower refractive index), both typically made of glass or plastic.
2.Light Propagation: Data is transmitted as light pulses that bounce off the core-cladding interface, guided by total internal reflection, minimizing signal loss.
3.Bandwidth: Offers high bandwidth and low attenuation over long distances, suitable for high-speed data transmission.
4.Advantages: Immune to electromagnetic interference (EMI), secure against tapping, and less susceptible to environmental factors like lightning compared to copper cables.
5.Types: Single-mode fiber (SMF) for long-distance, high-bandwidth applications; multi-mode fiber (MMF) for shorter distances and lower bandwidths.
6.Installation: Requires specialized equipment and careful handling due to its delicate nature.
7.Applications: Used extensively in telecommunications networks, internet backbone infrastructure, and high-speed data connections.
8.Cost Consideration: Initially expensive to install but offers long-term cost savings due to high reliability and bandwidth capacity.
9.Upgrades: Continual advancements in technology enhance data rates and efficiency of fiber optic networks.
10.Future Trends: Increasing adoption in consumer broadband, data centers, and emerging technologies like 5G networks and Internet of Things (IoT).

4. Explain the stop-and-wait protocol.

1.Sender sends a frame: The sender sends a single frame (or packet) to the receiver.
2.Receiver acknowledges: Upon receiving the frame correctly, the receiver sends an acknowledgment (ACK) back to the sender indicating successful reception.
3.Timeout: If the sender doesn't receive an ACK within a specified time (timeout period), it assumes the frame was lost or corrupted and retransmits the same frame.
4.Handling duplicates: If the receiver receives a duplicate frame due to a timeout, it sends the same ACK again to confirm receipt and discards the duplicate frame to avoid processing it twice.
5.Flow control: This protocol ensures a reliable one-way flow of data. Only when the sender receives an ACK does it send the next frame, preventing overflow at the receiver.
6.Advantages: Simple to implement and effective for small networks or scenarios with low error rates.

7.Disadvantages: Inefficient for high-latency networks or networks with high error rates because it waits for an ACK before sending the next frame, leading to underutilization of bandwidth.
8.Use cases: Commonly used in situations where reliable delivery is crucial but network conditions are stable, such as in local area networks (LANs) or some serial communication links.
9.Alternatives: Sliding window protocols like Go-Back-N and Selective Repeat offer higher efficiency by allowing multiple frames to be in transit simultaneously.
10.Implementation: Often implemented in software at the transport layer using timers and sequence numbers to manage frame transmission and acknowledgment.

5. Explain about wireless LAN.

1.Wireless Technology: Uses radio waves to transmit data between devices instead of physical cables, providing mobility and flexibility in network connectivity.
2.Components: Typically includes wireless access points (APs) or routers that broadcast signals, wireless client devices (e.g., laptops, smartphones) that connect to these access points, and sometimes a wired network infrastructure for connectivity to the internet.
3.Standards: Governed by IEEE 802.11 standards, with variants like 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac (Wi-Fi 5), and 802.11ax (Wi-Fi 6), each offering different speeds, frequencies, and ranges.
4.Access Points: Serve as central hubs where wireless clients connect, manage network traffic, and provide connectivity to wired networks or the internet.
5.Advantages: Enables convenient connectivity for mobile devices, allowing users to access resources, share files, and use services without being tethered to a specific location.
6.Security: Requires robust security measures (like WPA3 encryption, MAC filtering, and strong passwords) to protect against unauthorized access and data breaches, given the broadcast nature of radio waves.
7.Range and Coverage: Coverage area depends on factors like frequency, power output of devices, physical obstacles, and interference from other electronic devices.
8.Speeds: Offers varying data transfer speeds, from tens of Mbps to several Gbps depending on the standard and implementation (e.g., 802.11ac and 802.11ax).
9.Applications: Widely used in homes, businesses, public spaces, and educational institutions for internet access, VoIP (Voice over IP), streaming media, IoT (Internet of Things) connectivity, and more.
10.Evolution: Continual advancements in standards and technology improve performance, security, and efficiency, adapting to growing demands for higher

data rates and more connected devices in modern networks.

6. Explain the shortest-path routing algorithm.

1.Graph Representation: The network is represented as a graph, where nodes represent routers or network locations, and edges represent the connections (links) between them. Each edge has a weight or cost associated with it, indicating the distance, latency, or other metric.
2.Dijkstra's Algorithm: One of the most commonly used shortest-path algorithms is Dijkstra's algorithm, which starts from a source node and calculates the shortest path to all other nodes in the network.
3.Initialization: Begin at the source node and set its initial distance to zero. All other nodes are initialized with an infinite distance, indicating that they are initially unreachable.
4.Relaxation: Iteratively select the node with the smallest distance (from the set of nodes not yet processed), known as the current node. Update the distances to its neighboring nodes by considering the cost of the edge plus the distance to the current node. If this new distance is smaller than the previously known distance, update it.
5.Selection: Mark the current node as processed once all its neighbors have been examined. Repeat the process until all nodes have been processed or the destination node is reached.
6.Path Reconstruction: After the algorithm completes, the shortest path from the source node to any destination node can be reconstructed by tracing back from the destination using the recorded shortest paths.
7.Metrics: The "shortest" path can refer to different metrics depending on the application, such as minimizing hop count, delay, or maximizing available bandwidth.
8.Applications: Used extensively in routing protocols (like OSPF and IS-IS) within computer networks to determine optimal paths for data packets based on network conditions and constraints.
9.Complexity: Dijkstra's algorithm is efficient for networks with non-negative edge weights and operates in O((V+E)logV)O((V + E) \log V)O((V+E)logV) time complexity using a priority queue for efficient node selection.
10.Variants: Other algorithms like Bellman-Ford and Floyd-Warshall algorithm also exist for finding shortest paths in different types of networks or with different constraints (e.g., negative weights, all-pairs shortest paths).

7. a) Explain the IPV4 header.

1.Version (4 bits): Indicates the IP version. For IPv4, this value is 4.
2.Header Length (4 bits): Specifies the length of the IP header in 32-bit words. Minimum value is 5 (20 bytes).
3.Type of Service (8 bits): Specifies the priority and handling of the packet, often referred to as Differentiated Services Code Point (DSCP).

4.Total Length (16 bits): Indicates the total length of the IP packet, including the header and data, in bytes.
5.Identification (16 bits): Used for uniquely identifying the fragments of an original IP packet.
6.Flags (3 bits): Controls or identifies fragments. The three flags are: Reserved (always 0), Don't Fragment (DF), and More Fragments (MF).
7.Fragment Offset (13 bits): Specifies the position of a fragment in the original packet, measured in 8-byte units.
8.Time to Live (TTL) (8 bits): Limits the lifespan of a packet. Each router that processes the packet decrements the TTL by 1. The packet is discarded when TTL reaches 0.
9.Protocol (8 bits): Indicates the protocol used in the data portion of the IP packet. Common values are 6 for TCP and 17 for UDP.
10.Header Checksum (16 bits): Provides error-checking of the header. It is recalculated at each hop because certain fields (like TTL) change.

b) What is packet fragmentation?
1.Definition: Packet fragmentation is the process of splitting a large IP packet into smaller fragments to fit the network's MTU size.
2.MTU: Maximum Transmission Unit (MTU) is the largest packet size a network can handle without fragmentation.
3.Fragmentation Need: Occurs when a packet exceeds the MTU of any network segment along its path.
4.Identification: Each fragment retains the same identification number as the original packet for reassembly purposes.
5.Flags: The "More Fragments" (MF) flag is set in all fragments except the last one.
6.Offset: The "Fragment Offset" field specifies the position of the fragment's data within the original packet.
7.Reassembly: Fragments are reassembled at the destination using the identification, MF flag, and fragment offset.
8.Overhead: Fragmentation increases overhead due to additional headers for each fragment.
9.Packet Loss: Loss of any fragment necessitates the retransmission of the entire original packet, increasing the likelihood of data loss.
10.Avoidance: Path MTU Discovery (PMTUD) is used to avoid fragmentation by determining the smallest MTU along the packet's path and adjusting the packet size accordingly.

8. Explain the elements of transport layer.
1.Segmentation and Reassembly: Data from the application layer is divided into smaller segments for transmission. These segments are reassembled into the original data at the destination.

2.Connection Management: Manages the establishment, maintenance, and termination of connections between devices. This includes creating a connection-oriented session (TCP) or using a connectionless approach (UDP).
3.Flow Control: Ensures that the sender does not overwhelm the receiver with too much data at once. This is achieved through mechanisms like TCP's sliding window protocol.
4.Error Detection and Correction: Provides mechanisms to detect and correct errors in transmitted data, ensuring reliable communication. TCP, for example, uses checksums for error detection and retransmissions for error correction.
5.Multiplexing and Demultiplexing: Allows multiple applications to share the same network connection by assigning unique identifiers (port numbers) to each application session.
6.Ports and Sockets: Utilizes port numbers to distinguish between different services and applications on a device. Sockets combine IP addresses and port numbers to establish unique communication endpoints.
7.Congestion Control: Manages network congestion to prevent packet loss and ensure efficient data transfer. TCP uses algorithms like slow start, congestion avoidance, and fast recovery to control congestion.
8.Quality of Service (QoS): Provides different levels of service quality based on the type of data being transmitted, ensuring that critical applications receive the necessary bandwidth and low latency.
9.Reliability: Ensures that data is delivered accurately and in order. TCP provides reliability through acknowledgments (ACKs) and retransmissions.
10.Protocol Support: Supports different transport layer protocols like TCP (Transmission Control Protocol) for reliable, connection-oriented communication, and UDP (User Datagram Protocol) for fast, connectionless communication.

9. Explain the TCP transmission policy.
1.Three-Way Handshake: Establishes connections using SYN, SYN-ACK, and ACK packets.
2.Data Segmentation: Divides large data into smaller segments for transmission.
3.Flow Control: Manages data transmission rate using a sliding window mechanism.
4.Error Detection: Uses checksums to detect errors in transmitted segments.
5.Retransmission: Resends segments if acknowledgments (ACKs) are not received.
6.Congestion Control: Employs algorithms like slow start and congestion avoidance to manage network congestion.
7.ACKs: Uses cumulative and selective acknowledgments to confirm data receipt.
8.Timers: Manages retransmissions and connection states with various timers.
9.Four-Way Termination: Closes connections gracefully with FIN and ACK

packets.
10.Nagle's Algorithm: Reduces small packet transmissions by combining them.

10. Explain about HTTP.

1.Protocol: HTTP (HyperText Transfer Protocol) is used for transferring hypermedia documents like HTML.
2.Client-Server Model: Operates on a request-response model where clients request resources and servers provide them.
3.Stateless: Each HTTP request is independent, meaning the server does not retain information about previous requests.
4.Methods: Common HTTP methods include GET (retrieve data), POST (submit data), PUT (update data), DELETE (remove data).
5.Status Codes: Responses include status codes indicating the result, such as 200 (OK), 404 (Not Found), 500 (Internal Server Error).
6.Headers: Both requests and responses contain headers that provide metadata, such as content type and length.
7.URLs: Resources are identified and accessed using Uniform Resource Locators (URLs).
8.Sessions: Although stateless, sessions can be managed using cookies, tokens, or session IDs.
9.HTTPS: Secure version of HTTP that uses SSL/TLS to encrypt data, ensuring secure communication.
10.Versions: HTTP has different versions, with HTTP/1.1 and HTTP/2 being widely used, and HTTP/3 in development.

11. Explain about streaming audio.

1.Real-Time Transmission: Audio data is sent in real-time, allowing users to listen to it as it is being transmitted, without waiting for the entire file to download.
2.Streaming Protocols: Common protocols used for streaming audio include RTSP (Real-Time Streaming Protocol), HLS (HTTP Live Streaming), and DASH (Dynamic Adaptive Streaming over HTTP).
3.Buffering: A small amount of data is preloaded into a buffer to ensure smooth playback even if there are temporary interruptions in the network connection.
4.Compression: Audio files are often compressed using codecs like MP3, AAC, or Opus to reduce file size and bandwidth usage without significantly compromising quality.
5.Adaptive Streaming: The quality of the audio stream can adjust dynamically based on the user's network conditions, providing a balance between quality and smooth playback.
6.Continuous Playback: Users can start listening to audio almost immediately, and playback continues seamlessly as more data is streamed.
7.Bandwidth Efficiency: Streaming conserves bandwidth by transmitting only

the portion of the audio file that the user listens to, rather than downloading the entire file.

8.Live and On-Demand: Streaming audio can be used for both live broadcasts (like radio stations or live events) and on-demand content (like podcasts or music libraries).

9.Player Software: Requires a media player or web browser capable of handling streaming protocols and audio codecs to decode and play the streamed audio.

10.Accessibility: Provides users with easy access to a vast range of audio content without the need for large storage space on their devices.