Code No: 155AN **R18**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

B. Tech III Year I Semester Examinations, August - 2022

COMPUTER NETWORKS

(Computer Science and Engineering)

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

Answer any five questions

All questions carry equal marks

- - -

1.a) What is the importance of layered architecture in network models? Discuss in detail.
b) Differentiate between TCP/IP network model and ISO-OSI reference model. [7+8]

2.a) Discuss about Network hardware components in detail.
b) What are the advantages of fiber optic cables? Explain with a neat sketch. [7+8]

3.a) What are the design issues of Data Link Layer? Explain in detail.

b) Compare and contrast CSMA/CD and CSMA/CA for channel allocation. [7+8]

4. What are various types of Error Detection methods?Explain about Cyclic Redundancy Check Error Detection Method with suitable examples. [15]

5.a) Define Routing. Explain Distance Vector Routing Algorithm with an example.

b) What are the advantages and limitations of flooding? [9+6]

6.a) Describe link state vector routing algorithm example.
b) How to achieve quality of service using leaky bucket algorithm. [7+8]

7.a) Explain connection management in the transport layer.
b) Compare and contrast TCP and UDP Protocols. [7+8]

8.a) What are the major components in E-mail system? And explain the role of SMTP for sending and receiving messages.

b) Discuss about HTTP request and response mechanisms. [8+7]

---ooOoo---

ANSWER KEY

1.a) What is the importance of layered architecture in network models? Discuss in detail.

1. Modularity: Layered architecture allows networks to be structured in modular layers, each responsible for specific functions, such as data encapsulation, routing, or application support.
2. Abstraction: Each layer hides the complexities of lower layers, enabling developers to focus on specific functionalities without worrying about the entire network structure.
3. Ease of Understanding: It simplifies network design, implementation, and troubleshooting by breaking down complex tasks into manageable parts. 4. Interoperability: Different layers can communicate using standardized protocols, promoting interoperability between heterogeneous systems and devices.
5. Flexibility: Allows for the modification or upgrading of individual layers without affecting others, facilitating scalability and adaptation to new technologies.
6. Efficiency: Optimizes network performance by distributing tasks among specialized layers, reducing redundancy and improving overall efficiency. 7. Fault Isolation: Problems can be localized to specific layers, making it easier to identify and resolve issues without disrupting the entire network. 8. Security: Implementing security measures at each layer enhances overall network security by providing multiple lines of defense against various types of threats.
9. Standardization: Encourages the development of standardized protocols and interfaces, promoting compatibility and reducing integration costs.
10.Scalability: Supports growth of network infrastructure by adding new layers or upgrading existing ones to accommodate increased demands or emerging technologies.

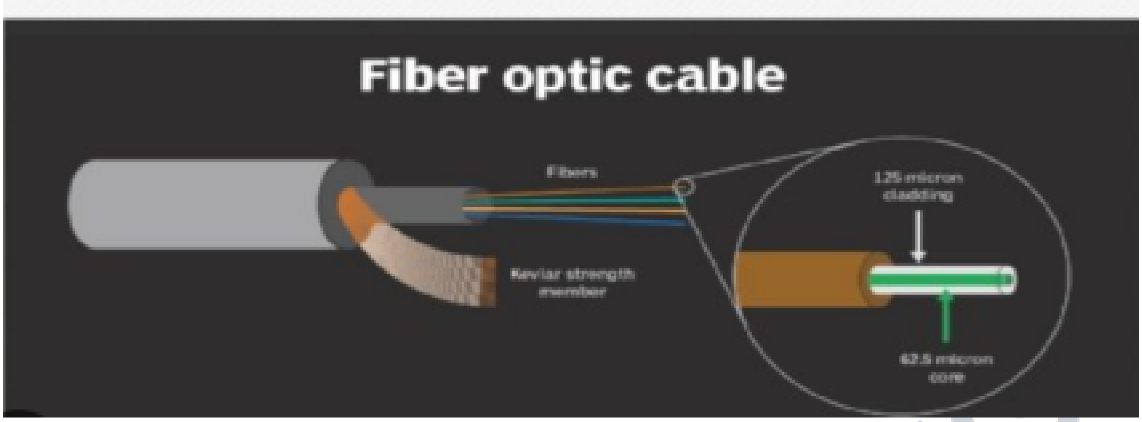
b) Differentiate between TCP/IP network model and ISO-OSI reference model.

TCP/IP Network Model:
1. Layers: TCP/IP model has four layers: Application, Transport, Internet, and Link.
2. Development: Developed by the U.S. Department of Defense (DoD) in the 1970s for ARPANET.
3. Protocols: Key protocols include TCP (Transmission Control Protocol), UDP (User Datagram Protocol), IP (Internet Protocol), and others like HTTP, FTP, SMTP.
4. Scope: Widely used in the Internet and intranets, forming the basis of modern internet communication.
5. Connection-Oriented: TCP provides reliable, connection-oriented communication between devices.

6. Addressing: Uses IP addresses (IPv4 and IPv6) for addressing devices in networks.
7. Example: Used extensively for data transmission and communication across the internet, providing reliable transmission through TCP and lightweight transmission through UDP.
OSI Reference Model:
1. Layers: OSI model has seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.
2. Development: Developed by the International Organization for Standardization (ISO) in the late 1970s and early 1980s.
3. Protocols: Each layer of the OSI model represents a specific function, but it does not specify protocols. Actual protocols like TCP/IP, IPX/SPX, and others are implementations that can be mapped onto its layers.
4. Scope: Used as a conceptual framework to understand and describe network protocols and interactions.
5. Connection-Oriented: OSI does not prescribe specific protocols but includes layers that can support both connection-oriented (Transport layer) and connectionless (Network layer) communication.
6. Addressing: Does not specify addressing schemes directly but defines a framework within which various addressing schemes can be implemented.
7. Example: While not directly implemented in networks, the OSI model is used for teaching and understanding networking concepts and serves as a reference point for protocol development.

2.a) Discuss about Network hardware components in detail. 1. Network Interface Cards (NICs): Connect computers to networks, translating data for transmission.
2. Switches: Connect devices within a LAN, forwarding data based on MAC addresses for efficient communication.
3. Routers: Connect different networks (LANs or WANs), forwarding data based on IP addresses.
4. Modems: Convert digital data for transmission over telephone lines or cable systems.
5. Access Points (APs): Enable wireless devices to connect to wired networks via Wi-Fi.
6. Firewalls: Monitor and control network traffic to protect against unauthorized access and threat.
7. Repeaters: Amplify and extend network signals over long distances. 8. Hubs: Basic devices connecting Ethernet devices within a LAN (mostly obsolete).
9. Cables and Connectors: Transmit data signals between devices, including Ethernet cables and fiber optics.
10.Power over Ethernet (PoE) Devices: Provide power and data over Ethernet cables for devices like IP cameras and wireless access points.

b) What are the advantages of fiber optic cables? Explain with a neat sketch.



1. High Bandwidth: Fiber optic cables can carry much more data than copper cables due to their higher bandwidth capacity.
2. Low Attenuation: They experience minimal signal loss over long distances, enabling transmission over greater distances without degradation.
3. Immunity to EMI: Fiber optic cables are not susceptible to electromagnetic interference, ensuring reliable data transmission in electrically noisy environments.
4. Security: They do not radiate signals and are difficult to tap without detection, enhancing data security.
5. Lightweight and Small Size: Fiber optic cables are thinner and lighter than copper cables, making them easier to install and maintain. 6. Long Distances: Fiber optic signals can travel much longer distances without needing regeneration compared to electrical signals in copper cables.

3.a) What are the design issues of Data Link Layer? Explain in detail.

1. Frame Synchronization: Ensuring proper timing alignment between sender and receiver.
2. Error Detection and Correction: Detecting and recovering from transmission errors.
3. Flow Control: Regulating data flow to match receiver capabilities.
4. Error Recovery: Strategies for retransmitting lost or corrupted frames. 5. Addressing: Assigning unique identifiers (MAC addresses) to devices. 6. Media Access Control: Managing access to shared communication channels.
7. Frame Ordering: Ensuring correct sequencing of transmitted frames. 8. Efficiency: Optimizing use of available bandwidth and resources. 9. Security: Implementing measures to prevent unauthorized access and data interception.
10.Compatibility: Ensuring interoperability with different network technologies and protocols.

b) Compare and contrast CSMA/CD and CSMA/CA for channel allocation.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection):

1. Method: Listens to the medium before transmitting and detects collisions. 2. Use: Common in Ethernet networks with shared media.
3. Collision Handling: Devices stop transmitting upon collision detection and retry after a random backoff period.
4. Efficiency: Effective for wired networks, manages collisions to optimize throughput.
CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance):
1. Method: Listens to the medium and waits for a clear channel before transmitting.
2. Use: Used in wireless networks to avoid collisions due to hidden terminals.
3. Collision Avoidance: Uses a virtual carrier sensing mechanism to avoid collisions.
4. Efficiency: Suitable for wireless environments where collisions are more problematic.

4. What are various types of Error Detection methods?Explain about Cyclic Redundancy Check Error Detection Method with suitable example.
1. Parity Check: Adds a parity bit to detect single bit errors.
2. Checksum: Sum of data units used to detect errors; often used in TCP/IP. 3. Cyclic Redundancy Check (CRC): Uses polynomial division for error detection.
4. Efficiency: CRC is efficient due to its ability to detect a wide range of errors with minimal computational overhead.
5. Implementation: Widely used in digital networks (Ethernet) and storag devices (hard drives, CDs).
6. Polynomial Selection: CRC uses a generator polynomial chosen based on desired error detection capabilities.
7. Division Process: Involves dividing the data by the polynomial and using the remainder as the CRC.
8. Error Detection: If the recalculated CRC at the receiver matches the received CRC, no errors are detected.
9. Example: Applying CRC-3 to data `101101` gives a CRC remainder of `011`.
10.Reliability: Provides robust error detection, suitable for noisy communication channels.

5.a) Define Routing. Explain Distance Vector Routing Algorithm with an example.
1. Routing Definition: Determines paths for network traffic from source to destination.
2. Distance Vector Routing: Each router maintains a table of shortest paths using distance vectors.
3. Initialization: Routers start with own distances as 0 and others as infinity. 4. Exchange: Routers share distance vectors periodically with neighbors. 5. Update: Routers update vectors based on received information, selecting shortest

paths.
6. Example: Router A knows direct paths to B and C; updates inform A of paths via B and C to D.
7. Efficiency: Simple implementation but slower convergence compared to link-state routing.
8. Scalability: Suitable for small to medium-sized networks due to overhead and convergence issues.
9. Routing Loops: Can suffer from routing loops if not managed with mechanisms like split horizon.
10.Algorithm Types: Examples include RIP (Routing Information Protocol) for IPv4 and EIGRP (Enhanced Interior Gateway Routing Protocol).

b) What are the advantages and limitations of flooding?
1. Advantages: Simple to implement and effective in unknown or dynamic network topologies.
2. Robustness: Ensures message delivery even in the presence of failures or multiple paths.
3. Redundancy: Provides backup routes and fault tolerance. 4. Scalability: Can be used in networks of varying sizes without major adjustments.
5. Limitations: Causes network congestion by broadcasting every packet to all nodes.
6. Traffic Control: Lacks mechanisms to control or prioritize traffic. 7. Duplicate Packets: May result in duplicates reaching destinations without additional controls.
8. Security Concerns: Vulnerable to misuse for flooding attacks and resource exhaustion.
9. Efficiency: Inefficient use of bandwidth and network resources.
10.Practical Use: Often used in specialized applications or specific network scenarios where simplicity and redundancy are prioritized over efficiency.

6.a) Describe link state vector routing algorithm example.
1. Topology Discovery: Routers begin with knowledge of their immediate neighbors and their link costs.
2. Link State Advertisements (LSAs): Routers periodically broadcast LSAs to all routers, detailing their neighbors and link costs.
3. Database Construction: Each router maintains a database (Link State Database) containing received LSAs from all routers.
4. Shortest Path Calculation: Dijkstra's algorithm is used to calculate the shortest path from each router to all other routers.
5. Shortest Path Tree (SPT): Each router constructs a Shortest Path Tree rooted at itself based on the shortest paths calculated.
6. Routing Table Creation: From the SPT, routers create routing tables that specify the next hop for each destination.

7. Efficiency: Efficient use of network resources due to periodic updates and localized computation.
8. Scalability: Suitable for large networks as it scales well with the number of routers and links.
9. Fast Convergence: Rapid convergence to optimal paths after network changes due to distributed computation and flooding.
10.Example: Routers A, B, C, and D exchange LSAs to build a complete network topology and compute shortest paths for routing decisions.

b) How to achieve quality of service using leaky bucket algorithm. 1. Concept: Treats the network traffic like water flowing into a bucket with a leak.
2. Token Bucket: Maintains a token bucket that fills at a constant rate. Each token represents permission to send a fixed amount of data (e.g., one packet).
3. Token Consumption: Packets can only be sent if there are tokens available in the bucket.
4. Bucket Overflow: Excess tokens beyond the bucket's capacity are discarded (bucket overflow).
5. Traffic Shaping: Smooths out bursty traffic by controlling the rate at which packets are allowed into the network.
6. QoS Implementation: Ensures that traffic adheres to predefined traffic shaping rules, such as maintaining a constant bit rate or prioritizing certain types of traffic.
7. Advantages: Provides a mechanism to regulate traffic flow, preventing network congestion and ensuring fair allocation of resources.
8. Limitations: Requires accurate configuration of parameters like bucket size and token rate to achieve desired QoS.
9. Applications: Used in networks to enforce Service Level Agreements (SLAs) and prioritize critical applications.
10.Example: In a network, a Leaky Bucket Algorithm implementation ensures that VoIP traffic is given higher priority, preventing voice quality degradation during peak traffic periods.

7.a) Explain connection management in transport layer.
1. Purpose: Manages establishment, maintenance, and termination of communication sessions.
2. Three-Way Handshake: Initiates connection with SYN, confirms with SYN-ACK, completes with ACK.
3. Connection State: Tracks connection phases like establishment, data transfer, and termination.
4. Reliability: Ensures data integrity through error detection, retransmission of lost packets, and flow control.
5. Flow Control: Regulates data flow to prevent overwhelming receivers and network congestion.

6. Error Handling: Detects and manages errors like lost or out-of-order packets.
7. Protocols: TCP (Transmission Control Protocol) and SCTP (Stream Control Transmission Protocol) manage connections at this layer.
8. Session Persistence: Maintains session state to manage ongoing data exchanges.
9. Examples: Used in web browsing (HTTP over TCP), file transfer (FTP), and email (SMTP).
10.Termination: Graceful closure using a four-way handshake (FIN, ACK-FIN, ACK).

b) Compare and contrast TCP and UDP Protocols.

● TCP:

1. Connection-Oriented: Establishes a connection before data transfer. 2. Reliability: Ensures delivery through error detection, retransmission, and acknowledgment.
3. Ordered: Guarantees delivery in the order sent.
4. Overhead: Higher due to connection setup and maintenance.

● UDP:

1. Connectionless: No setup required before sending data.
2. Unreliable: Does not guarantee delivery; packets may be lost or arrive out of order.
3. Speed: Lower latency and faster transmission due to minimal overhead. 4. Applications: Used for real-time applications like video streaming, VoIP, and gaming.

● Use Cases:

1. TCP: Web browsing (HTTP), email (SMTP), file transfer (FTP). 2. UDP: Video conferencing (RTP), DNS, streaming media (UDP-based protocols).

8.a) What are the major components in E-mail system? And explain the role of SMTP for sending and receiving messages.

1. User Agents: Interfaces for composing and managing emails (e.g., Outlook, Gmail).
2. Mail Servers: Store, route, and deliver emails using MTAs and MDAs. 3. Mail Protocols: SMTP for sending, POP3/IMAP for receiving and managing emails.
4. Email Addresses: Unique identifiers formatted as username@domain. 5. DNS: Translates domain names to IP addresses for email routing. 6. Message Format (MIME): Defines email structure and attachments. 7. Spam Filters: Filters out unsolicited emails to protect users. 8. Encryption (TLS/SSL): Secures email transmission and authentication. 9. Forwarding and Aliases: Redirects emails based on rules or aliases. 10.Archiving and Backup: Stores copies of emails for compliance and recovery.

b) Discuss about HTTP request and response mechanisms. 1. Protocol: HTTP manages client-server communication for web resources. 2. Request: Clients (e.g., browsers) send requests to servers for resources. 3. Response: Servers reply with requested resources or status information. 4. Request Components: Methods (e.g., GET, POST), URL, headers, and optional body data.

5. HTTP Methods: GET (retrieve), POST (submit), PUT (upload), DELETE (remove).

6. Response Components: Status codes (e.g., 200 OK, 404 Not Found), headers, and body content.

7. Status Codes: Indicate success (2xx), redirection (3xx), client errors (4xx), server errors (5xx).

8. Stateless: Each request is independent; servers don't retain session data without mechanisms like cookies.

9. Security: HTTPS encrypts data for secure transmission.

10.Efficiency: Uses headers to convey metadata and optimize data exchange.