Module 1: Introduction to Networking

1. **What is a computer network?**
    - A computer network is a group of interconnected devices that communicate with each other to share resources like data, applications, and hardware (e.g., printers).
2. **What are the types of network topologies?**
    - Common types include **Bus**, **Star**, **Ring**, **Mesh**, and **Hybrid** topologies, each with its own layout and communication methods.
3. **Explain the difference between connection-oriented and connectionless services.**
    - **Connection-oriented services** (e.g., TCP) establish a dedicated connection before data transfer, while **connectionless services** (e.g., UDP) send data without establishing a connection.
4. **What are network protocols?**
    - Network protocols are rules that define how data is formatted, transmitted, and received across networks (e.g., HTTP, FTP, TCP/IP).
5. **What is the OSI model?**
    - The OSI model is a 7-layer conceptual framework for understanding and standardizing network communication functions, from physical transmission to application usage.
6. **List the seven layers of the OSI model.**
    - **Physical**, **Data Link**, **Network**, **Transport**, **Session**, **Presentation**, and **Application** layers.
7. **Explain the difference between the OSI and TCP/IP models.**
    - The **OSI model** has seven layers, while the **TCP/IP model** has four (Link, Internet, Transport, and Application). TCP/IP is more practical and used in real-world internet communication.
8. **What is a protocol hierarchy?**
    - Protocol hierarchy is the layering of protocols to manage data flow; each layer performs specific tasks to ensure data is transmitted and received efficiently.
9. **Define network topology.**
    - Network topology is the physical or logical layout of a network that shows the arrangement of nodes and the connecting lines between them.
10. **What are interconnection devices in networking?**
    - Interconnection devices like **routers**, **switches**, **hubs**, and **bridges** connect network components and manage data traffic.

Module 2: Physical Layer

1. **What is the electromagnetic spectrum?**
    - The electromagnetic spectrum is the range of all types of electromagnetic radiation, which includes radio, microwave, infrared, visible light, and others, used in communication.
2. **Name three types of guided transmission media.**
    - **Twisted pair cables**, **coaxial cables**, and **fiber optic cables**.
3. **What is a twisted pair cable?**
    - A twisted pair cable has pairs of wires twisted together to reduce interference and is commonly used in telephone and Ethernet networks.
4. **What is fiber optic cable?**
    - Fiber optic cable uses light to transmit data over long distances with high speed and minimal loss, suitable for internet and high-capacity networks.
5. **Explain the difference between guided and unguided media.**
    - **Guided media** (e.g., cables) directs signals along a specific path, while **unguided media** (e.g., radio waves) transmits signals through the air or space.
6. **What is attenuation?**
    - Attenuation is the loss of signal strength as it travels through a medium, affecting data transmission quality.
7. **How does a coaxial cable work?**
    - Coaxial cables transmit data as electrical signals within a central conductor, shielded by layers to prevent interference.
8. **What is bandwidth?**
    - Bandwidth is the range of frequencies a transmission medium can carry, determining data transmission capacity.
9. **What are the advantages of fiber optic cables over copper cables?**
    - Fiber optics offer **higher speed**, **longer transmission distances**, and **better resistance to electromagnetic interference**.
10. **What is multiplexing?**
    - Multiplexing is a method of combining multiple signals for transmission over a single medium to maximize efficiency.

Module 3: Data Link Layer

1. **What is the data link layer?**
    - The data link layer manages error detection and correction, frame synchronization, and flow control for data transferred across the network.

2. **What is framing?**
    - Framing is the process of dividing data into frames, each with headers and trailers, to manage error detection and control.
3. **Explain error detection and correction.**
    - Error detection identifies transmission errors using techniques like **parity checks** and **checksums**, while error correction fixes errors using algorithms like **Hamming Code**.
4. **What is flow control?**
    - Flow control regulates the data rate between sender and receiver to prevent overwhelming the receiver with too much data.
5. **Describe the Stop-and-Wait protocol.**
    - Stop-and-Wait is a simple flow control protocol where the sender transmits a frame and waits for an acknowledgment before sending the next frame.
6. **What is the Sliding Window protocol?**
    - Sliding Window protocol allows multiple frames to be sent before receiving an acknowledgment, improving data flow efficiency.
7. **What is CSMA/CD?**
    - **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)** is a protocol for managing data collisions in networks, commonly used in Ethernet.
8. **What is ALOHA protocol?**
    - ALOHA is a simple access protocol where devices send data whenever they want, risking collisions but useful in low-traffic networks.
9. **What is the purpose of the MAC (Medium Access Control) sublayer?**
    - MAC controls how devices access the transmission medium to ensure fair usage and prevent collisions.
10. **Explain CRC (Cyclic Redundancy Check).**
    - CRC is an error-detecting code that uses polynomial division to detect changes in transmitted data.

Module 4: Network Layer

1. **What is the network layer?**
    - The network layer manages data routing, addressing, and forwarding between devices across different networks.
2. **Explain IP addressing.**
    - IP addressing assigns unique identifiers (IP addresses) to devices, allowing them to communicate on a network.

3. **What is subnetting?**
    - Subnetting divides a large network into smaller sub-networks, improving management and security.
4. **Explain the purpose of IPv4 and IPv6.**
    - IPv4 and IPv6 are internet protocols with different address lengths (IPv4 has 32-bit, IPv6 has 128-bit) used to identify devices on networks.
5. **What is a routing algorithm?**
    - A routing algorithm finds the best path for data to travel from source to destination; examples include **Dijkstra's** and **Distance Vector** algorithms.
6. **What is NAT (Network Address Translation)?**
    - NAT maps private IP addresses to a single public IP address, allowing multiple devices to access the internet.
7. **Explain ARP and RARP.**
    - ARP translates IP addresses to MAC addresses, while RARP translates MAC addresses to IP addresses.
8. **What is ICMP used for?**
    - ICMP is used for error reporting and network diagnostics (e.g., using the **ping** command).
9. **What is congestion control?**
    - Congestion control manages network traffic to prevent data bottlenecks, ensuring efficient data transfer.
10. **What are QoS parameters?**
    - Quality of Service (QoS) parameters like bandwidth and latency help prioritize network traffic to meet application needs.

Module 5: Transport Layer

1. **What is the transport layer?**
    - The transport layer handles end-to-end communication, managing data flow control, segmentation, and reliability.
2. **What is the difference between TCP and UDP?**
    - **TCP** is connection-oriented with error correction and flow control, while **UDP** is connectionless and faster but less reliable.
3. **What are transport layer service primitives?**
    - Service primitives are basic operations like **send**, **receive**, and **connect** used by transport layer protocols.

4. **What is a socket?**
    - A socket is an endpoint for communication, created by binding an IP address and port for applications to send/receive data.
5. **Explain the TCP three-way handshake.**
    - The TCP three-way handshake (SYN, SYN-ACK, ACK) establishes a reliable connection between two devices.
6. **What is flow control in TCP?**
    - TCP flow control prevents data overload by adjusting the sending rate based on the receiver's capacity.
7. **What is TCP congestion control?**
    - TCP congestion control mechanisms like **Slow Start** and **Congestion Avoidance** adjust data transmission to prevent network congestion.
8. **What are TCP timers?**
    - TCP timers (e.g., **retransmission timer**) manage connection timeouts and retransmissions if acknowledgments are delayed.
9. **What is a TCP segment?**
    - A TCP segment is a packet with TCP header and data, used in communication between TCP layers.
10. **Explain Berkeley Sockets.**
    - Berkeley Sockets is a library for socket programming that enables network communication in applications.

Module 6: Application Layer

1. **What is the application layer?**
    - The application layer is the topmost layer, providing interfaces for user applications to access network services.
2. **What is DNS and its function?**
    - DNS (Domain Name System) translates human-readable domain names into IP addresses.
3. **Explain the purpose of HTTP.**
    - HTTP (Hypertext Transfer Protocol) is used for transferring web pages and other resources over the internet.
4. **What is SMTP?**
    - SMTP (Simple Mail Transfer Protocol) is used for sending and routing emails.

5. **What is FTP used for?**
    - FTP (File Transfer Protocol) is used to transfer files between computers on a network.
6. **Explain the concept of DHCP.**
    - DHCP (Dynamic Host Configuration Protocol) automatically assigns IP addresses to devices on a network.
7. **What is Telnet?**
    - Telnet is a protocol for remote login, allowing users to access another computer over a network.
8. **What is a resource record in DNS?**
    - A DNS resource record stores information like IP addresses, mail servers, and aliases for a domain.
9. **What is the difference between HTTP and HTTPS?**
    - HTTPS (HTTP Secure) encrypts data using SSL/TLS, providing secure communication compared to HTTP.
10. **What is a name server?**
    - A name server stores DNS records and provides domain name resolution, translating domains to IPs.