Module-I: Introduction to Networks

1. Network Topology:

- Definition: Network Topology refers to the physical or logical layout of devices in a network and how they are interconnected.

- Types: Common topologies include bus, star, ring, mesh, and hybrid.

- Importance: Determines how data flows within a network and impacts its performance and scalability.

2. Network Architecture:

- Definition: Network Architecture encompasses the design principles, protocols, and technologies used to build and maintain a network.

- Components: Includes network devices, communication protocols, and network services.

- Importance: Ensures that networks are reliable, secure, and efficient in transmitting data.

3. Reference Models:

- Definition: Reference Models provide a standardized framework for understanding and implementing network communication protocols.

- Examples: OSI (Open Systems Interconnection) model and TCP/IP (Transmission Control Protocol/Internet Protocol) model.

- Purpose: Helps in developing interoperable network systems and troubleshooting network issues.

4. Example Networks (ARPANET, NSFNET, Internet):

- ARPANET: One of the earliest packet-switched networks, developed by the U.S. Department of Defense in the 1960s.

- NSFNET: A high-speed network backbone funded by the National Science Foundation, crucial for early internet development.

- Internet: The global network of networks that connects billions of devices worldwide.

5. Physical Layer:

- Definition: The Physical Layer is the lowest layer of the OSI model, responsible for transmitting raw data bits over a physical medium.

- Transmission Media: Includes copper wires, fiber optics, and wireless transmission.

- Functions: Handles data encoding, signaling, and physical connection establishment.

Module-II: The Data Link Layer

6. Data Link Layer Design Issues:

- Framing: Divides data into frames for transmission and adds necessary control information.

- Error Detection and Correction: Techniques like CRC and parity checking to ensure data integrity.

- Flow Control: Regulates data flow between sender and receiver to prevent data loss.

7. Elementary Data Link Protocols:

- HDLC (High-Level Data Link Control): A versatile protocol used for point-to-point and multipoint communication.

- PPP (Point-to-Point Protocol): Commonly used for establishing a direct connection between two nodes.

8. Sliding Window Protocols:

- Definition: Sliding window protocols allow multiple frames to be transmitted before receiving an acknowledgment.

- Advantages: Enhances network efficiency by utilizing the available bandwidth effectively.

9. Protocol Verification Methods:

- Testing: Ensures that protocols function correctly under various conditions.

- Simulation: Simulates network behavior to evaluate protocol performance.

10. Channel Allocation Multiple Access Protocols:

- CSMA/CD (Carrier Sense Multiple Access with Collision Detection): Used in Ethernet networks to manage access to the shared medium.

- Token Ring: Uses a token-passing mechanism to control access in a ring network topology.

11. IEEE 802 Standards:

- Ethernet (802.3): Defines standards for wired LAN technologies.

- Wi-Fi (802.11): Specifies standards for wireless LAN technologies.

Module-III: The Network Layer

12. Network Layer Design Issues:

- Routing: Determines the path data packets should take in a network to reach their destination.

- Congestion Control: Manages network traffic to prevent congestion and ensure efficient data

transmission.

13. Routing Algorithms:

- Shortest Path Routing: Algorithms like Dijkstra's and Bellman-Ford find the shortest path between nodes.

- Distance Vector Routing: Uses hop count to determine the best path.

14. Internetworking Network Layer in Internet:

- IP (Internet Protocol): The core protocol of the Internet layer, responsible for addressing and routing packets across different networks.

- Routers: Devices that forward packets based on IP addresses to enable internetwork communication.

Module-IV: The Transport Protocols

15. Transport Service:

- Definition: Provides end-to-end communication services for applications running on different hosts.

- Reliable Communication: Ensures data delivery and integrity.

16. Transport Protocols (UDP, TCP):

- UDP (User Datagram Protocol): Connectionless protocol suitable for applications where speed is more critical than reliability.

- TCP (Transmission Control Protocol): Reliable, connection-oriented protocol that guarantees data delivery.

17. Internet Transport Protocols:

- UDP and TCP: Widely used transport protocols in the Internet for various applications, such as web browsing, email, and streaming.

18. Performance Issues:

- Throughput: Measure of data transfer rate.

- Latency: Delay in data transmission.

- Congestion Control: Techniques to manage network congestion for optimal performance

Module-V: The Application Layer

19. Application Layer Design Issues:

- Interface: Defines how applications interact with the network services.

- Protocols: Establish rules for communication between applications.

20. Domain Name System (DNS):

- Function: Translates domain names into IP addresses for locating resources on the Internet.

- Hierarchy: Organized in a hierarchical structure for efficient name resolution.

21. Electronic Mail:

- SMTP (Simple Mail Transfer Protocol): Used for sending email messages between servers.

- POP3 (Post Office Protocol version 3): Retrieves emails from a mail server to a client device.

22. World Wide Web:

- HTTP (Hypertext Transfer Protocol): Facilitates communication between web servers and clients for data transfer.

- HTTPS (Hypertext Transfer Protocol Secure): Secure version of HTTP using encryption for data protection.

23. Other Applications:

- FTP (File Transfer Protocol): Transfers files between systems over a network.

- VoIP (Voice over Internet Protocol): Transmits voice communications over the Internet.

24. Network Security:

- Basic Cryptography: Techniques like encryption and decryption to secure data during transmission.

- Symmetric and Asymmetric Cryptography: Methods for encryption where keys are shared (symmetric) or asymmetric (public-private key pairs).