UNIT I: INTRODUCTION AND APPLICATION LAYER

1. Data Communication and Networks

Data Communication: The process of transferring data between two or more devices. It involves the transmission of digital or analog data over communication channels such as cables, fiber optics, or wireless signals.

Networks: A collection of interconnected devices (computers, servers, switches, routers) that share data and resources.

Network Types: LAN (Local Area Network), WAN (Wide Area Network), MAN (Metropolitan Area Network), and PAN (Personal Area Network).

2. Protocol Layering and Models

Protocol Layering: The use of multiple layers to break down communication tasks into manageable parts. Each layer handles specific tasks and interacts with adjacent layers.

TCP/IP Protocol Suite: A set of communication protocols used for the Internet. It includes four layers:

Application Layer: Provides network services to end-users (e.g., HTTP, FTP, DNS).

Transport Layer: Provides end-to-end communication and data flow control (e.g., TCP, UDP).

Network Layer: Handles routing of packets across networks (e.g., IP).

Data Link and Physical Layers: Manages data transmission between devices over physical media (e.g., Ethernet).

OSI Model: A reference model with seven layers (Application, Presentation, Session, Transport, Network, Data Link, Physical) that standardizes the functions of a network.

3. Introduction to Sockets

Sockets: Endpoints for sending and receiving data between devices over a network. Sockets provide a way for programs to communicate using standard protocols like TCP or UDP.

4. Application Layer Protocols

HTTP (Hypertext Transfer Protocol): A protocol used for transmitting web pages over the Internet. It operates on a request-response model where the client requests resources and the server responds.

FTP (File Transfer Protocol): A protocol used to transfer files between a client and a server on a

network.

Email Protocols:

SMTP (Simple Mail Transfer Protocol): Used for sending emails from a client to a server or between servers.

POP3 (Post Office Protocol 3): Used for retrieving emails from a server to a client. Downloads the email and often deletes it from the server.

IMAP (Internet Message Access Protocol): Used for retrieving emails. Keeps the emails on the server, allowing multiple devices to access the mailbox.

MIME (Multipurpose Internet Mail Extensions): Extends email formats to support text in different character sets, attachments, audio, and video.

DNS (Domain Name System): Translates domain names (e.g., www.example.com) into IP addresses that computers use to identify each other on the network.

SNMP (Simple Network Management Protocol): Used for monitoring and managing network devices (routers, switches, servers).

UNIT II: TRANSPORT LAYER

1. Introduction to Transport Layer

Transport Layer: Responsible for end-to-end communication between devices, providing reliable or unreliable data transfer, error checking, and flow control.

2. Transport-Layer Protocols

UDP (User Datagram Protocol): A connectionless protocol that provides fast, but unreliable data transmission. It's used for applications where speed is critical (e.g., online gaming, streaming).

TCP (Transmission Control Protocol): A connection-oriented protocol that provides reliable data transmission, error detection, and correction. It establishes a connection before transmitting data and ensures all packets arrive in the correct order.

3. TCP Concepts

Connection Management: Establishes a connection between a client and server using a three-way handshake (SYN, SYN-ACK, ACK) before data transmission.

Flow Control: Mechanism to control the rate of data transmission between sender and receiver to prevent congestion. TCP uses the sliding window protocol for flow control.

Congestion Control: TCP mechanisms to avoid congestion in a network:

Congestion Avoidance (DECbit, RED):

DECbit: Uses explicit feedback from routers to control congestion.

RED (Random Early Detection): Randomly drops packets before a router's buffer overflows to signal congestion.

SCTP (Stream Control Transmission Protocol): Provides reliable, message-oriented transmission. It supports multihoming (multiple IP addresses) and multiple streams for faster recovery from errors.

Quality of Service (QoS): Techniques to manage and prioritize network traffic to ensure a certain level of performance, reliability, and availability.

UNIT III: NETWORK LAYER

1. Switching: Packet Switching

Packet Switching: Divides data into small packets, which are transmitted over the network independently. It is efficient and suitable for data networks like the Internet.

2. Internet Protocol (IP)

IPv4 (Internet Protocol version 4): The most widely used version of IP, providing a 32-bit address space (e.g., 192.168.0.1). Supports up to 4.3 billion unique addresses.

IP Addressing: Each device on a network is assigned an IP address, which includes a network and host identifier.

Subnetting: Divides an IP network into smaller sub-networks (subnets) to efficiently manage IP address allocation and improve security.

IPv6 (Internet Protocol version 6): A newer version of IP with a 128-bit address space (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334). Provides a vastly larger address pool and supports features like auto-configuration, better security, and multicast.

3. Protocols in the Network Layer

ARP (Address Resolution Protocol): Resolves IP addresses to MAC (Media Access Control) addresses, enabling devices to communicate over Ethernet.

RARP (Reverse Address Resolution Protocol): Allows a device to request its IP address from a server, based on its MAC address.

ICMP (Internet Control Message Protocol): Used for sending error messages and operational information (e.g., "ping" command).

DHCP (Dynamic Host Configuration Protocol): Automatically assigns IP addresses and other network configuration settings to devices on a network.

4. Routing and Routing Protocols

Unicast Routing: Routing protocols that send data from one source to one specific destination.

Distance Vector Routing: Routing protocols like RIP that use distance (hop count) to determine the best path.

- **RIP (Routing Information Protocol):** Uses hop count as a metric; suitable for small networks.

Link State Routing: Protocols like OSPF that use the state of network links to calculate the shortest path.

- **OSPF (Open Shortest Path First):** Determines the shortest path based on multiple metrics; suitable for larger, complex networks.

Path-Vector Routing: Protocols like BGP that maintain the entire path of the route to ensure stable routing.

- **BGP (Border Gateway Protocol):** Used for routing between different networks (autonomous systems) on the Internet.