UNIT I: Introduction and Application Layer

1. Data Communication:

This is like sending messages between computers or devices, like texting or calling your friends but with data.

- Process of sending and receiving data between devices.
- Involves a sender, receiver, and a medium (like a cable or wireless signal).
- Ensures data is transferred accurately and securely.

2. Networks:

A network is a group of computers connected to share information. The internet is a giant network that connects computers worldwide.

LAN (Local Area Network): Small network within a building (e.g., home, office).

WAN (Wide Area Network): Large network connecting different regions or countries (e.g., the internet).

MAN (Metropolitan Area Network): Covers a city or campus.

3. Network Types:

Peer-to-Peer: Devices communicate directly without a central server.

Client-Server: Devices communicate through a central server that manages requests.

4. Protocol Layering:

This is like breaking down communication into steps or layers. Each layer does a specific job, from preparing the message to delivering it.

Communication is broken into layers, each handling a specific task.

Common models: OSI Model (7 layers) and TCP/IP Model (4 layers).

Makes it easier to troubleshoot and develop network systems.

5. TCP/IP Protocol Suite:

The set of rules that computers use to communicate over the internet. TCP ensures data is delivered correctly, while IP makes sure it goes to the right place.

TCP (Transmission Control Protocol): Ensures data is delivered reliably and in the correct order.

IP (Internet Protocol): Routes data between devices on different networks.

Foundation of modern internet communication.

6. OSI Model:

This is another model that explains how data moves through different layers (7 in total) from one computer to another.

7 layers (Physical, Data Link, Network, Transport, Session, Presentation, Application).

Each layer has a specific function, from sending raw data (Physical) to interacting with user applications (Application).

7. Introduction to Sockets:

A socket is like the "door" through which data enters or leaves a computer when it communicates with another device.

Act as endpoints for sending and receiving data over a network.

Each socket is defined by an IP address and a port number.

Application Layer Protocols:

1. HTTP: Helps web browsers load websites.

   Used for browsing websites, transfers web pages.

Works on request-response basis (client sends request, server responds).

2. FTP: Moves files between computers.

Transfers files between computers.

Uses commands like upload (put) and download (get).

3. Email Protocols:

SMTP: Sends emails.

POP3: Downloads emails to your device.

IMAP: Keeps emails on a server so you can access them from any device.

MIME: Allows emails to send attachments like photos.

4. DNS: Turns website names into IP addresses (like looking up a phone number).

5. SNMP: Monitors and manages devices on a network (like routers).

UNIT II: Transport Layer

1. Introduction to Transport Layer:

Ensures data is sent correctly between computers, like sending a letter with a tracking number.

Handles end-to-end communication between devices.

Ensures data is delivered reliably, in order, and without errors.

2. UDP (User Datagram Protocol):

Sends data quickly but doesn't guarantee it arrives safely, like sending a message without knowing if the person received it.

Sends data without checking for errors or order.

Fast but unreliable (used in gaming, video streaming).

3. TCP (Transmission Control Protocol):

Sends data accurately and ensures it arrives in the right order. It’s like a delivery service confirming your package was received.

Reliable and ensures data is delivered correctly and in order.

Establishes a connection before sending data, like a phone call.

4. Connection Management:

TCP makes sure both computers are ready before sending data, like starting a phone call by saying "hello" first.

TCP creates a connection (3-way handshake) before transferring data.

Ensures both sender and receiver are ready to communicate.

5. Flow Control:

Controls the speed of data so one computer isn’t overwhelmed, like talking slowly so someone can understand you.

Manages the speed of data transmission.

Prevents overwhelming the receiver with too much data at once.

6. Congestion Control:

Prevents the network from getting overloaded, like keeping roads from getting too full of traffic.

Detects and manages network traffic to prevent overload.

Algorithms like TCP’s AIMD (Additive Increase/Multiplicative Decrease) help avoid congestion.

7. Congestion Avoidance (DECbit, RED):

Detects congestion early and adjusts traffic to avoid jams, like using traffic signals to avoid gridlock.

DECbit: Marks packets when congestion is detected, prompting the sender to slow down.

RED (Random Early Detection): Drops packets randomly to avoid network congestion early.

8. SCTP (Stream Control Transmission Protocol):

A combination of TCP and UDP that allows multiple data streams at once, like driving on multiple lanes of a highway.

Similar to TCP but supports multiple streams of data in a single connection.

Used for tasks like video calls where multiple data types are transmitted simultaneously.

9. Quality of Service (QoS):

Prioritizes important data like video calls, ensuring they get through faster than less important things.

Prioritizes important data (e.g., voice or video) to avoid delays.

Ensures critical applications get bandwidth first.

UNIT III: Network Layer

1. Switching:

Packet Switching: Breaks data into small packets to send them through the best route, like mailing pieces of a puzzle separately.

2. Internet Protocol:

IPv4: The most common type of IP address, like a digital address for your computer.

IP Addressing: Assigns a unique address to each device on a network.

Subnetting: Splits a large network into smaller ones, like dividing a city into neighborhoods.

IPv6: A newer version of IP addresses to replace IPv4 as more devices connect to the internet.

3. ARP (Address Resolution Protocol):

Matches IP addresses with physical hardware addresses, like matching a person's name with their home address.

4. RARP (Reverse Address Resolution Protocol):

Does the opposite of ARP—finds the IP address from a physical address.

5. ICMP (Internet Control Message Protocol):

Sends error messages, like when a website is down.

6. DHCP (Dynamic Host Configuration Protocol):

Automatically assigns IP addresses to devices on a network.

Routing:

1. Unicast Routing: Sends data from one device to another.

2. Routing Protocols:

Distance Vector Routing: Chooses the best path based on distance (like using the shortest route).

RIP (Routing Information Protocol): A simple routing protocol that uses distance to decide the best path.

Link State Routing: Chooses routes based on the current condition of the network.

OSPF (Open Shortest Path First): A protocol that finds the shortest path.

PathVector Routing: Tracks the full path a packet takes.

BGP (Border Gateway Protocol): The protocol that helps data travel between different networks, like how international mail travels between countries.

UNIT IV: Data Link and Physical Layers

1. Data Link Layer:

Responsible for moving data across a single link in a network, like a bridge between two buildings.

2. Framing:

Breaks data into small frames to send over the network.

3. Flow Control:

Manages data transmission speed so the receiving computer isn't overwhelmed.

4. Error Control:

Detects and corrects any errors in the transmitted data, like proofreading a letter before sending it.

5. DataLink Layer Protocols:

HDLC (HighLevel Data Link Control): A protocol that ensures reliable communication.

PPP (PointtoPoint Protocol): Used to establish a direct connection between two devices.

6. Media Access Control:

Controls who can use the network at any given time, like taking turns in a conversation.

7. Ethernet Basics:

The most common way to connect devices in a network using cables.

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

A method to avoid data collisions on a network, like making sure no one talks at the same time.

9. Virtual LAN (VLAN):

Creates separate networks within a larger network, like dividing classrooms into groups.

10. Wireless LAN (802.11):

A network that connects devices without cables, like WiFi.

Physical Layer:

1. Data and Signals:

   Converts data into signals (electrical or radio waves) that can be transmitted over a network.

2. Performance:

   Measures how fast data can be transmitted over the network.

3. Transmission Media:

   The physical materials (like cables or radio waves) used to send data.

4. Switching:

  Circuit Switching: Establishes a direct path between two devices, like a phone call.