# Computer Networks and Basic Terminologies

## 1 Computer Networks and its Features

A computer network is a collection of interconnected computers and other devices that share resources, exchange data, and communicate with each other through various communication channels. These devices, often called nodes, may include computers, printers, and other hardware devices.

### 1.1 Features of Computer Networks:

- **Resource Sharing:** Users can share hardware resources (e.g., printers, scanners) and software (e.g., applications, data files) over a network.
- **Data Communication:** Allows data transfer between devices across the network in a fast and secure way.
- **Scalability:** Networks can grow easily by adding new nodes (computers or devices) without disrupting existing services.
- **Reliability:** Redundancies and backups in the network can increase fault tolerance, ensuring services are available even during failures.
- **Security:** Advanced security protocols (like encryption, firewalls, access controls) ensure secure communication over the network.
- **Centralized Management:** Networks allow centralized administration of software, files, and devices, simplifying maintenance and support.
- **Cost Efficiency:** Sharing of resources and services across the network reduces the cost for organizations.
- **File Sharing:** Files and data can be shared easily between multiple users on the same network.
- **Collaboration:** Enables collaboration between users, allowing them to work on shared documents and projects in real-time.

## 2 Computer Network Components

Several hardware devices and components are involved in creating and maintaining a network. Key components include:

1. **Network Interface Card (NIC):**
   - **Function:** A NIC is a hardware component that enables a computer to connect to a network. It can be wired (Ethernet) or wireless (Wi-Fi).
   - **Role:** Each NIC has a unique MAC address, which is used for data transfer between devices on the network.
2. **Switch:**
   - **Function:** A switch is a device that connects multiple devices in a local area network (LAN). It uses MAC addresses to forward data to the appropriate device.
   - **Role:** Switches reduce the possibility of data collisions and manage the flow of data efficiently within a LAN.

3. **Hub:**
    - **Function:** A hub is a basic networking device that connects multiple devices but does not manage data intelligently like a switch.
    - **Role:** It broadcasts data to all connected devices, increasing the chance of collisions.
4. **Router:**
    - **Function:** A router connects different networks together (for example, a LAN to the internet). It directs data between networks using IP addresses.
    - **Role:** Routers can connect multiple networks and act as a gateway between a local network and the broader internet.
5. **Cables:**
    - **Types:** Various types of cables are used to transmit data, including:
        - Twisted Pair Cables (Ethernet): Common for LAN connections.
        - Coaxial Cable: Used for internet and cable TV services.
        - Fiber Optic Cable: Transmits data as light, enabling faster speeds over longer distances.
6. **Connectors:**
    - **Role:** Connectors like RJ45 (used with Ethernet cables) and BNC (used with coaxial cables) are used to establish connections between networking devices and cables.
7. **Modem:**
    - **Function:** A modem (modulator-demodulator) is used to convert digital signals from a computer into analog signals for transmission over telephone lines and vice versa.
    - **Role:** Modems allow computers and other devices to access the internet over a telephone line or cable network.

# 3 Layering & Protocols (OSI Model and its 7 Layers)

## 3.1 Introduction to OSI Model:

The Open Systems Interconnection (OSI) model is a conceptual framework that standardizes the functions of a communication system into seven distinct layers. It helps different networking protocols to work together and ensures interoperability between various network technologies.

## 3.2 7 Layers of the OSI Model:

1. **Physical Layer (Layer 1):**
    - **Function:** This layer is responsible for the physical connection between devices, such as cables, switches, and other hardware. It handles the transmission of raw data bits (0s and 1s) over the network.
    - **Examples:** Ethernet cables, hubs, repeaters.
2. **Data Link Layer (Layer 2):**
    - **Function:** The data link layer handles node-to-node data transfer and error detection. It packages raw bits into frames for transmission.
    - **Sub-layers:**
        - MAC (Media Access Control): Deals with the control of how devices in a network gain access to data.
        - LLC (Logical Link Control): Manages frame synchronization and error checking.
    - **Examples:** Switches, network interface cards (NIC).
3. **Network Layer (Layer 3):**

- **Function:** This layer is responsible for determining the best physical path for data to travel from the source to the destination using logical addressing (IP addresses).
- **Examples:** Routers, IP (Internet Protocol), ICMP (Internet Control Message Protocol).

4. **Transport Layer (Layer 4):**
   - **Function:** Ensures reliable data transfer between devices or hosts by providing flow control, error checking, and recovery of data. It breaks data into segments and ensures the correct delivery order.
   - **Protocols:** TCP (Transmission Control Protocol) for reliable communication, UDP (User Datagram Protocol) for faster, connectionless communication.
5. **Session Layer (Layer 5):**
   - **Function:** Manages and controls the establishment, maintenance, and termination of communication sessions between devices.
   - **Role:** It handles session restoration and synchronization.
   - **Examples:** RPC (Remote Procedure Call), NetBIOS.
6. **Presentation Layer (Layer 6):**
   - **Function:** This layer translates or formats data for the application layer. It handles encryption, compression, and data translation between different formats.
   - **Examples:** SSL (Secure Socket Layer), encryption formats like ASCII, EBCDIC.
7. **Application Layer (Layer 7):**
   - **Function:** This is the topmost layer that interacts directly with end-users. It provides services such as email, file transfer, and web browsing.
   - **Protocols:** HTTP (HyperText Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), DNS (Domain Name System).

## 3.3 Layering and Protocols:

Each layer in the OSI model has a specific set of protocols that define how data should be handled at that level. Protocols are sets of rules that define how to transmit and receive data across networks. Here's a brief overview of key protocols per layer:

- **Physical Layer:** Ethernet (for wired networks), IEEE 802.11 (Wi-Fi).
- **Data Link Layer:** Ethernet (802.3), ARP (Address Resolution Protocol).
- **Network Layer:** IP (Internet Protocol), ICMP.
- **Transport Layer:** TCP (guaranteed delivery, reliable), UDP (non-guaranteed, faster).
- **Session Layer:** PPTP (Point-to-Point Tunneling Protocol), SMB (Server Message Block).
- **Presentation Layer:** TLS/SSL (encryption protocols), JPEG, ASCII.
- **Application Layer:** HTTP, SMTP, FTP, DNS.

## 3.4 Importance of Layering:

- **Simplifies Design:** By breaking down communication into layers, developers can focus on a specific function without worrying about the entire process.
- **Interoperability:** Layering ensures that hardware and software developed by different vendors can work together.
- **Troubleshooting:** By isolating issues at a specific layer, it becomes easier to diagnose and resolve network problems.
- **Scalability and Flexibility:** Networks can be modified or expanded without affecting the whole system, as each layer works independently.

# 4 TCP/IP Model

The TCP/IP model, also known as the Internet Protocol Suite, is a conceptual framework used for network communications. It consists of four layers that work together to manage data transmission over networks, such as the internet. Each layer handles a specific set of functions to ensure that data can travel from one device to another, even if they are located on different networks. The TCP/IP model is simpler and more practical than the OSI model and has become the foundational model for network communication.

## 4.1 Overview of the TCP/IP Model Layers

The TCP/IP model consists of the following four layers:

- Application Layer
- Transport Layer
- Internet Layer
- Network Access Layer

Each layer serves specific purposes and utilizes various protocols to facilitate communication.

### 4.1.1 1. Application Layer

**Description:** The Application Layer is the top layer in the TCP/IP model, responsible for providing network services directly to the applications running on a device. This layer includes protocols that manage data formatting, file transfer, email transmission, and other end-user services.

**Functions of the Application Layer:**

- Facilitates communication between network applications.
- Provides network services such as file transfer, email, and web browsing.
- Manages user interface aspects and displays information in a readable format.

**Key Protocols in the Application Layer:**

- HTTP (HyperText Transfer Protocol): Used for web page requests and responses.
- HTTPS (HTTP Secure): HTTP with encryption for secure communication.
- FTP (File Transfer Protocol): Used for file transfers between systems.
- SMTP (Simple Mail Transfer Protocol): Used for sending emails.
- POP3 (Post Office Protocol) and IMAP (Internet Message Access Protocol): Used for retrieving emails.
- DNS (Domain Name System): Resolves domain names to IP addresses.
- SNMP (Simple Network Management Protocol): Used for network management and monitoring.
- DHCP (Dynamic Host Configuration Protocol): Assigns IP addresses dynamically to devices.

**Comparison with the OSI Model:** The Application Layer in TCP/IP combines functions of the OSI Model's Application, Presentation, and Session layers. It handles data formatting, session management, and provides a user interface.

### 4.1.2 2. Transport Layer

**Description:** The Transport Layer is responsible for ensuring reliable data transfer between devices. It provides end-to-end communication and error-checking mechanisms to ensure that data is delivered correctly and in the correct order. The two main protocols used at this layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

**Functions of the Transport Layer:**

- Establishes, maintains, and terminates connections between devices.
- Provides error-checking, data integrity, and flow control.
- Segments data into smaller units (called segments) for easier transmission.
- Reassembles segments at the receiving end in the correct order.

**Key Protocols in the Transport Layer:**

- **TCP (Transmission Control Protocol):**
  - Connection-oriented protocol that establishes a reliable connection before data transfer.
  - Ensures data integrity and delivery through acknowledgments, retransmissions, and flow control.
  - Suitable for applications where reliability is essential, such as web browsing, file transfers, and email.
- **UDP (User Datagram Protocol):**
  - Connectionless protocol that sends data without establishing a connection.
  - Faster than TCP but does not guarantee delivery or order, making it less reliable.
  - Suitable for real-time applications like video streaming, gaming, and VoIP where speed is prioritized over reliability.

**Comparison with the OSI Model:** The Transport Layer in TCP/IP corresponds to the Transport Layer in the OSI model. It handles similar functions like segmentation, error correction, and flow control, ensuring reliable data delivery.

#### 4.1.3 3. Internet Layer

**Description:** The Internet Layer is responsible for logical addressing, routing, and packet forwarding. It allows data to be sent across multiple networks, making it essential for creating an interconnected global internet. This layer determines the best path for data to travel from the source to the destination, managing IP addresses and packet routing.

**Functions of the Internet Layer:**

- Provides logical addressing using IP addresses.
- Routes packets across different networks.
- Fragments large packets into smaller ones if necessary for compatibility with underlying network protocols.
- Manages packet headers to ensure accurate delivery.

**Key Protocols in the Internet Layer:**

- **IP (Internet Protocol):**
  - The primary protocol for addressing and routing packets across networks.
  - Two versions in use: IPv4 (32-bit addresses) and IPv6 (128-bit addresses).
  - IP is a connectionless and unreliable protocol, meaning it does not guarantee delivery.
- **ICMP (Internet Control Message Protocol):**
  - Used for error messages and network diagnostics.
  - ICMP messages include the "ping" command, which tests connectivity between devices.

- **ARP (Address Resolution Protocol):**
  - Resolves IP addresses to MAC addresses on a local network.
  - Essential for devices within the same network to locate each other.
- **RARP (Reverse Address Resolution Protocol):**
  - Used by devices to request their own IP address if only a MAC address is known.
  - Mostly replaced by DHCP in modern networks.

**Comparison with the OSI Model:** The Internet Layer in TCP/IP maps to the OSI model's Network Layer, performing similar functions like logical addressing, routing, and path selection for data packets.

#### 4.1.4 4. Network Access Layer

**Description:** The Network Access Layer, also known as the Link Layer or Data Link Layer, is the bottom layer of the TCP/IP model. It handles the physical transmission of data between devices on the same network. This layer includes protocols that manage hardware addressing, access control, and the actual transmission of data over the physical medium.

**Functions of the Network Access Layer:**

- Defines how data is physically sent over network media (e.g., cables or wireless).
- Handles frame encapsulation and de-encapsulation, preparing packets for transmission over the physical network.
- Uses MAC addresses to ensure data reaches the correct device on a local network.
- Manages data link protocols and hardware addressing.

**Key Protocols in the Network Access Layer:**

- **Ethernet:**
  - A widely-used protocol for wired LANs, managing MAC addressing, and data framing.
  - Operates over twisted-pair cables and fiber optic cables.
- **PPP (Point-to-Point Protocol):**
  - A protocol for direct communication between two network nodes, often used in WAN connections.
  - Ensures encapsulation of data and basic error-checking.
- **Wi-Fi (IEEE 802.11):**
  - A wireless networking protocol used for local area networks.
  - Operates on radio frequencies and uses encryption to secure wireless communication.

**Comparison with the OSI Model:** The Network Access Layer combines functions of the OSI model's Data Link and Physical Layers, encompassing both the hardware aspects of data transmission and data link functions like framing and error detection.

| Aspect | TCP/IP Model | OSI Model |
|---|---|---|
| Number of Layers | 4 | 7 |
| Application Layer | Combines OSI's Application, Presentation, and Session Layers | Three separate layers: App |
| Network Interface Layer | Combines OSI's Physical and Data Link Layers | Two separate layers: Physi |
| Primary Use | Used as the foundation for the Internet | Mostly used as a theoretica |
| Layer Independence | Layers are more flexible and can overlap | Layers are more distinct ar |

### 4.2 Key Differences Between the TCP/IP Model and OSI Model

### 4.3 Practical Use of the TCP/IP Model

The TCP/IP model is used extensively in real-world networks, especially for internet communications. Each layer has specific protocols and tools for testing and managing network communication:

- **Application Layer Protocols:** Test connections and diagnose network services using tools like curl for HTTP requests or ping commands to test network latency.
- **Transport Layer Protocols:** Tools like netstat or traceroute can show TCP connections, routing paths, and check the health of connections at the Transport Layer.
- **Internet Layer Protocols:** Routing protocols like BGP and OSPF function at this layer, defining paths across the internet. Commands like ipconfig (Windows) or ifconfig (Linux) help manage IP settings.
- **Network Access Layer Protocols:** Network interface controllers (NICs) and physical networking hardware, including switches and routers, operate at this layer, using Ethernet standards for local data transfer.

### 4.4 Summary of the TCP/IP Model

The TCP/IP model is streamlined with only four layers compared to the OSI model's seven. The model is practical and closely aligns with internet protocols, making it highly effective for real-world network communication. Understanding each layer, along with its protocols and functions, is crucial for managing, troubleshooting, and designing robust network systems, whether for a private LAN or the global internet.

# 5 Network Topologies

# 6 Categories of Networks (LAN, WAN, PAN, MAN)

# 7 Network Architecture (Peer-to-Peer, Client-Server)

# 8 Physical Layer

### 8.1 Different Types of Transmission Media

Transmission media refers to the physical path through which data is transmitted from one device to another in a network. There are two main types: guided (wired) and unguided (wireless).

#### 8.1.1 1. Guided (Wired) Media:

These involve a physical connection for transmitting data. Examples include:

#### 8.1.2 2. Unguided (Wireless) Media:

These use electromagnetic waves to transmit data without a physical conductor.

| Topology | Description | Advantages | Disadvantages |
|---|---|---|---|
| Bus Topology | All devices are connected to a single central cable (backbone). Data travels along this cable, and each device listens for the data addressed to it. | - Simple and easy to install.<br>- Requires less cabling.<br>- Cost-effective for small networks.<br>- Easy to extend by connecting more devices. | - Entire network fails if the central cable fails.<br>- Limited by the number of devices (signal degradation).<br>- High collision rate with heavy traffic. |
| Ring Topology | Devices are connected in a circular fashion, and data travels in one direction (or sometimes both) around the ring, passing through each device. | - No data collisions due to unidirectional flow.<br>- Predictable performance since each device has equal access. | - If one device or connection fails, it can disrupt the entire network.<br>- Troubleshooting and adding/removing devices can be difficult. |
| Star Topology | All devices are connected to a central hub or switch. The hub acts as the central point for data communication between devices. | - Centralized management simplifies troubleshooting.<br>- Failure of one device doesn't affect others.<br>- Easy to add or remove devices. | - If the central hub/switch fails, the entire network goes down.<br>- Requires more cabling than bus and ring topologies. |
| Tree Topology | A combination of star and bus topology, where groups of star-configured networks are connected to a central bus. | - Scalable and allows for easy expansion.<br>- Centralized management.<br>- Hierarchical structure allows for segmentation of different network parts. | - Failure of the backbone will disrupt the entire network.<br>- Requires a lot of cabling and hardware. |
| Mesh Topology | Every device is connected to every other device. Can be fully connected (each device has a direct link to all others) or partially connected. | - High redundancy and fault tolerance (failure of one link doesn't affect the network).<br>- Data can be routed along multiple paths. | - Expensive and complex to install due to extensive cabling.<br>- Maintenance is challenging, especially in large networks. |

## 8.2 Transmission Switching

Transmission switching refers to how data is transmitted across a network. Two primary methods used are packet switching and circuit switching, each suited for different types of network communication.

### 8.2.1 Packet Switching

Packet switching is the most common method used in modern computer networks, including the internet. In this technique, data is divided into small chunks or "packets" that are transmitted independently across the network.

**Key Characteristics of Packet Switching:**

- **Data Fragmentation:** Large data is broken into small, manageable packets before transmission.
- **Dynamic Routing:** Each packet can take a different route to the destination, depending on network traffic and availability.
- **Reassembly:** At the destination, packets are reassembled in the correct order to reconstruct the original message.
- **Stateless:** There is no dedicated path between the sender and receiver, meaning that each packet is treated independently by the network.
- **Protocols Used:**TCP/IP: Transmission Control Protocol (TCP) and Internet Protocol (IP) are commonly used for packet switching, where TCP handles reordering and IP routes packets to their destination.

| Network Type | Description | Advantages | Disadvantages |
|---|---|---|---|
| LAN (Local Area Network) | A network that connects computers and devices within a small geographic area, such as a single building or campus. | - High data transfer speed.<br>- Cost-effective for small-scale networks.<br>- Easy to maintain and troubleshoot. | - Limited coverage to a specific area.<br>- Expanding the network can increase costs. |
| WAN (Wide Area Network) | A network that spans a large geographic area, often connecting multiple LANs across cities, countries, or even globally. | - Can cover large distances.<br>- Facilitates global communication.<br>- Allows organizations to connect remote branches. | - High setup and maintenance costs.<br>- Lower data transfer speeds compared to LANs.<br>- Complex management. |
| PAN (Personal Area Network) | A small network that connects personal devices (e.g., smartphones, laptops, wearables) within a short range, typically around 10 meters. | - Low cost and easy to set up.<br>- Useful for personal device connectivity (e.g., Bluetooth, Wi-Fi). | - Limited range and coverage.<br>- Suitable only for personal use or small areas. |
| MAN (Metropolitan Area Network) | A network that covers a larger geographic area than a LAN but is smaller than a WAN, often spanning a city or large campus. | - Covers a large area such as a city.<br>- Can provide high-speed internet or connectivity for a city or region. | - Expensive to build and maintain.<br>- More complex to manage than LAN. |

| Architecture | Description | Advantages | Disadvantages |
|---|---|---|---|
| Peer-to-Peer (P2P) | In a peer-to-peer architecture, each device (or "peer") acts as both a client and server. All devices share resources directly without a centralized server. | - Easy to set up and maintain.<br>- Low cost (no need for dedicated servers).<br>- Each peer can share files or resources directly. | - Lack of centralized management.<br>- Security is harder to enforce.<br>- Not scalable for large networks. |
| Client-Server | In a client-server architecture, clients (end-user devices) request services or resources from centralized servers, which respond to these requests. | - Centralized management of data and resources.<br>- Easy to enforce security and control.<br>- Scalable for larger networks. | - Higher cost due to the need for dedicated servers.<br>- Server failure can lead to the entire network being down. |

| Media Type | Description | Advantages | Disadvantages |
|---|---|---|---|
| Twisted Pair Cable | Consists of two insulated copper wires twisted together to reduce interference. Used for LANs (Ethernet cables). | - Inexpensive and easy to install.<br>- Widely used in LANs and telephone networks. | - Limited bandwidth and shorter transmission distance.<br>- Susceptible to electromagnetic interference. |
| Coaxial Cable | A single copper conductor with an insulating layer and metallic shield. Used for cable TV and internet connections. | - More resistant to interference compared to twisted pair.<br>- Higher bandwidth. | - Bulkier and more expensive than twisted pair.<br>- Still limited over long distances. |
| Fiber Optic Cable | Uses light to transmit data via glass or plastic fibers. Ideal for high-speed, long-distance transmission. | - Extremely high bandwidth.<br>- Immune to electromagnetic interference.<br>- Long-distance capability. | - Expensive to install and maintain.<br>- Fragile and difficult to splice or repair. |

**How It Works:**

1. **Data is divided:** Data (such as a file or message) is broken into multiple small packets.

| Media Type | Description | Advantages | Disadvantages |
|---|---|---|---|
| Radio Waves | Used for wireless communication in open spaces (e.g., Wi-Fi, Bluetooth). Works over long distances. | - Easy to deploy.<br>- Wide area coverage. | - Prone to interference and security vulnerabilities.<br>- Limited bandwidth. |
| Microwaves | High-frequency signals used for long-distance communication (e.g., satellite links, cellular networks). | - Suitable for long distances.<br>- Can carry large amounts of data. | - Requires line-of-sight communication.<br>- Affected by weather conditions. |
| Infrared | Uses infrared light for short-range communication (e.g., remote controls, some wireless devices). | - Secure, as signals do not pass through walls.<br>- Low interference. | - Limited to line-of-sight and short-range.<br>- Cannot pass through solid objects. |

2. **Packets are labeled:** Each packet contains information about its origin, destination, and sequence number to facilitate reassembly.
3. **Packets travel independently:** Each packet may follow different paths through the network depending on current traffic conditions.
4. **Reassembly at the destination:** Once all packets reach the destination, they are reassembled in the correct order based on their sequence number.

**Advantages of Packet Switching:**

- **Efficient Use of Network Resources:** Since no dedicated path is required, network bandwidth can be shared among many users, making it ideal for bursty data traffic like web browsing, emails, and file downloads.
- **Scalability:** Network resources can be dynamically allocated as needed, making it more scalable for large networks like the internet.
- **Fault Tolerance:** If a network link fails, packets can be rerouted to another path, ensuring the continuity of data transmission.
- **Cost-Effective:** Since multiple devices can use the same network resources, packet switching is more cost-efficient, especially in large networks.

**Disadvantages of Packet Switching:**

- **Out-of-Order Delivery:** Packets may arrive at their destination in different orders and must be reassembled, potentially causing delays.
- **Packet Loss:** Some packets may be lost during transmission, especially in congested networks, leading to the need for retransmission.
- **Latency and Jitter:** Network congestion or varying paths can cause delays (latency) or variations in the time it takes packets to reach the destination (jitter), making it less ideal for real-time applications like voice or video.

**Use Cases:**

- **Internet Traffic:** Web browsing, email, file transfers, and most data-intensive services use packet switching.
- **Video Streaming:** Services like Netflix and YouTube use adaptive streaming protocols over packet-switched networks.
- **VoIP (Voice over IP):** Although voice communication traditionally used circuit switching, modern VoIP services now use packet switching, despite potential latency issues.

### 8.2.2 Circuit Switching

Circuit switching is a traditional technique primarily used in telephone networks. In this method, a dedicated communication path (or "circuit") is established between two devices for the entire duration of the communication.

**Key Characteristics of Circuit Switching:**

- **Dedicated Path:** A direct communication path is established between the sender and receiver before data transfer begins, and it remains active throughout the session.
- **Connection-Oriented:** A connection must be set up before data transmission can occur. The connection is reserved solely for the communicating parties.
- **Fixed Bandwidth:** The circuit provides a guaranteed, fixed bandwidth throughout the communication session.
- **Continuous Transmission:** Data is transmitted as a continuous stream without breaks.

**How It Works:**

1. **Connection Establishment:** A dedicated communication path is set up between the sender and receiver before any data is transmitted. This is known as the "setup" phase.
2. **Data Transmission:** Once the path is established, data is transmitted along the dedicated path.
3. **Disconnection:** After the communication session is complete, the connection is terminated, and the path is released for other uses.

**Phases of Circuit Switching:**

1. **Setup Phase:** The connection is established.
2. **Data Transfer Phase:** Data is transmitted along the path.
3. **Teardown Phase:** The connection is closed, and resources are freed.

**Advantages of Circuit Switching:**

- **Guaranteed Bandwidth:** Since a dedicated path is reserved for the duration of the communication, users are guaranteed a fixed bandwidth, making it suitable for real-time communication like voice and video calls.
- **Low Latency:** Once the circuit is established, there is minimal delay or jitter because the data is sent along a direct, uninterrupted path.
- **Continuous Transmission:** Ideal for continuous data streams, ensuring no data loss during transmission.

**Disadvantages of Circuit Switching:**

- **Inefficient Resource Usage:** Resources (e.g., bandwidth) are reserved even when no data is being transmitted, making it inefficient for bursty traffic or idle periods.
- **Expensive:** Circuit switching can be more costly than packet switching, especially for long-duration calls or large-scale networks, because dedicated paths must be maintained.
- **Setup Time:** Establishing the connection can introduce a delay before actual data transmission begins, which can be problematic for very short messages or applications.

**Use Cases:**

- **Traditional Telephone Networks:** Circuit switching is the basis of the Public Switched Telephone Network (PSTN) and is used for voice calls.
- **Leased Lines:** Some businesses use circuit-switched networks for point-to-point communication, particularly when consistent bandwidth is essential.
- **Private Communications:** Dedicated circuits can be used for secure, uninterrupted communication between fixed locations.

### 8.2.3 Key Differences Between Packet Switching and Circuit Switching

| Feature | Packet Switching | Circuit Switching |
|---|---|---|
| Connection Type | No dedicated path. Data is broken into packets and sent independently. | Dedicated path is established for the entire session. |
| Efficiency | Efficient use of network resources. Multiple users can share the same bandwidth. | Less efficient. Bandwidth is reserved for one connection, even if not used fully. |
| Data Delivery | Packets may take different paths and arrive out of order. | Data is sent in a continuous stream along the dedicated path. |
| Delay (Latency) | Packets may experience delays or jitter, especially under network congestion. | Minimal delay once the circuit is established. |
| Cost | More cost-effective due to shared resources. | More expensive due to reserved resources. |
| Best Suited For | Data communication (e.g., emails, file transfers, web browsing). | Real-time communication (e.g., voice and video calls). |
| Failure Handling | Packets can be rerouted if a path fails, ensuring higher fault tolerance. | A single failure in the circuit can disrupt the communication session. |
| Overhead | Packet headers add overhead for reassembly and routing. | Minimal overhead once the circuit is established. |
| Bandwidth Utilization | Dynamic, can adjust to traffic needs. | Fixed, reserved for the duration of the connection. |

**Hybrid Approach (MPLS):** Multiprotocol Label Switching (MPLS) is a hybrid approach that incorporates elements of both packet and circuit switching. It is commonly used in enterprise networks to create virtual circuits for high-priority traffic, combining the efficiency of packet switching with the performance guarantees of circuit switching.

## 8.3 IP Address and MAC Address

### 8.3.1 IP Address:

- **Definition:** An IP address (Internet Protocol address) is a logical address assigned to each device connected to a network, used for identifying devices and routing data.
- **Types:**
  - IPv4: A 32-bit address written in dotted decimal format (e.g., 192.168.1.1).
  - IPv6: A 128-bit address written in hexadecimal (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- **Role:** Used for identifying devices across networks (local or global) and enabling data routing from source to destination.
- **Dynamic vs. Static IP:**
  - Static IP: Manually assigned and does not change.
  - Dynamic IP: Automatically assigned by DHCP (Dynamic Host Configuration Protocol).

### 8.3.2 MAC Address:

- **Definition:** A MAC address (Media Access Control address) is a unique 48-bit identifier assigned to the network interface card (NIC) of each device, usually written in hexadecimal format (e.g., 00:1A:2B:3C:4D:5E).
- **Role:** Operates at the Data Link Layer (Layer 2 of the OSI model) and is used for device identification within a local network.
- **Permanent Address:** Unlike IP addresses, MAC addresses are permanent and hardcoded into the device's network interface.

### 8.3.3 Features of IP Address and MAC Address

| Feature | IP Address | MAC Address |
|---|---|---|
| Function | Identifies devices over the network (Layer 3, Network Layer). | Uniquely identifies a device within a local network (Layer 2). |
| Addressing | Logical address assigned by network or ISP (dynamic or static). | Physical address, burned into the NIC by the manufacturer. |
| Format | IPv4: 32-bit (e.g., 192.168.0.1)<br>IPv6: 128-bit address | 48-bit hexadecimal (e.g., 00:1A:2B:3C:4D:5E) |
| Scope | Global (used for routing across multiple networks). | Local (within the same LAN segment). |

## 8.4 Bridges and Repeaters

Bridges and repeaters are network devices that enhance network performance by extending network segments and reducing data collisions.

### 8.4.1 Bridge:

- **Definition:** A bridge is a device that connects and filters traffic between two or more network segments, operating at the Data Link Layer (Layer 2). It uses MAC addresses to forward or filter traffic based on the destination.
- **Function:** Bridges reduce traffic by dividing the network into separate segments, only forwarding necessary data between them. This reduces collisions and enhances performance.

### 8.4.2 Repeater:

- **Definition:** A repeater amplifies and regenerates signals over long distances, operating at the Physical Layer (Layer 1). It ensures that the signal does not degrade as it travels across the network.
- **Function:** Repeaters do not filter traffic or distinguish between devices; they simply extend the network by regenerating weak signals.

### 8.4.3 Features of Bridges & Repeaters

## 8.5 Framing, Addressing, Flow Control & Access Control

### 8.5.1 Framing

- **Definition:** Framing is the process of dividing a continuous stream of data into smaller, manageable units called frames. These frames are critical in network communication for synchronization, error detection, and addressing.
- **Purpose:**
  - Allows receivers to detect the boundaries between frames.

| Feature | Bridge | Repeater |
|---|---|---|
| Layer | Operates at Data Link Layer (Layer 2) of the OSI model. | Operates at Physical Layer (Layer 1) of the OSI model. |
| Function | Connects two or more network segments, filtering and forwarding traffic based on MAC addresses. | Regenerates weak signals to extend network range. |
| Traffic Control | Reduces network traffic by filtering and forwarding only necessary data. | Does not filter traffic; simply amplifies signals for long-distance communication. |
| Network Type | Used in local networks (LANs) to divide network segments and manage traffic. | Used in any network where signals need to be strengthened, including LANs and WANs. |
| Collision Reduction | Helps in reducing collisions by segmenting the network. | Does not reduce collisions or manage traffic; just boosts signals. |
| Cost | More expensive and complex than repeaters, as it filters traffic. | Inexpensive and simple device for extending the network. |
| Use Case | Ideal for reducing congestion in larger LANs or connecting different network types (e.g., wired to wireless). | Useful for extending a network's physical distance. |

  - Helps recover from errors by retransmitting a specific frame rather than the entire data stream.

- **Types of Framing:**
  - Fixed-size framing: Each frame is of a constant size (e.g., ATM cells, which are always 53 bytes).
  - Variable-size framing: Each frame can have a different size, with start and end delimiters (e.g., Ethernet, HDLC).
- **Example:** In the Ethernet frame structure, the frame consists of a preamble, start frame delimiter (SFD), destination and source MAC addresses, the payload, and a CRC field for error checking. This frame ensures data integrity and communication across LANs.

#### 8.5.2 Addressing

- **Definition:** Addressing is the method by which devices or nodes in a network are uniquely identified for data transmission. Addressing occurs at multiple layers of the OSI model.
- **Layer 2 (Data Link Layer) Addressing:**
  - **MAC Address:** A unique identifier assigned to a network interface card (NIC) used for communication within a local network.
  - **Example:** Ethernet frames use MAC addresses (48-bit) in the header for device-level communication.
- **Layer 3 (Network Layer) Addressing:**
  - **IP Address:** Logical address assigned to devices participating in a network, used for communication across different networks.
  - **Example:** IPv4 addresses (32-bit) or IPv6 addresses (128-bit) are used in the IP header for routing across the internet.

#### 8.5.3 Flow Control

- **Definition:** Flow control is a technique used to ensure that the sender does not overwhelm the receiver by sending data too quickly. It prevents buffer overflow at the receiver side.
- **Methods of Flow Control:**
  - **Stop-and-Wait:** The sender transmits a single frame and waits for an acknowledgment before sending the next frame. Simple but inefficient for high-latency networks.

- **Sliding Window Protocol:** The sender can send multiple frames before needing an acknowledgment, controlled by the size of the window.

- **Example:** TCP uses a sliding window mechanism to adjust the flow of data dynamically based on the receiver's buffer capacity. It prevents congestion and data loss in high-speed networks.

#### 8.5.4 Access Control

- **Definition:** Access control is the process of managing how multiple devices share and access the communication medium without interference, especially in broadcast networks.

- **Access Control Techniques:**

  - **CSMA/CD (Carrier Sense Multiple Access with Collision Detection):** Used in wired Ethernet networks. Devices listen to the medium before transmitting. If a collision is detected, devices wait for a random backoff time before retransmitting.
  - **CSMA/CA (Collision Avoidance):** Used in wireless networks like Wi-Fi. Devices check for an idle channel before sending data and use acknowledgments to ensure transmission.

- **Example:** Wi-Fi uses CSMA/CA with Request to Send (RTS) and Clear to Send (CTS) signals to minimize collisions in a wireless environment.

### 8.6 Error Detection (Parity, CRC), Sliding Window, Stop-and-Wait Protocols

#### 8.6.1 Error Detection

**Parity**

- **Definition:** Parity is a simple error detection mechanism that adds an extra bit (parity bit) to a byte or word of data. It ensures that the total number of 1-bits in the data either remains even (even parity) or odd (odd parity).

- **Usage:** Parity can detect single-bit errors but cannot correct errors or detect multi-bit errors.

- **Types:**

  - **Even Parity:** The parity bit is set to ensure that the total number of 1-bits is even.
  - **Odd Parity:** The parity bit is set to ensure that the total number of 1-bits is odd.

- **Example:** For the byte 1011001, an even parity bit would be 0, and for odd parity, it would be 1.

**Cyclic Redundancy Check (CRC)**

- **Definition:** CRC is a more robust error-detection method used to detect accidental changes to raw data. It treats the data as a binary number, divides it by a pre-determined divisor (generator polynomial), and appends the remainder (CRC value) to the data. The receiver performs the same division and checks if the remainder matches.

- **Advantages:**

  - More effective than parity checks.
  - Capable of detecting burst errors (multiple-bit errors).

- **Example:** Ethernet frames use CRC-32 to detect errors in the transmitted frame. The sender computes the CRC of the frame data, and the receiver recomputes the CRC to verify the data's integrity.

### 8.6.2 Sliding Window Protocol

- **Definition:** The sliding window protocol is a flow control and error control mechanism used in reliable transmission protocols. It allows the sender to send multiple frames before needing an acknowledgment from the receiver. The size of the window controls how many frames can be in transit without acknowledgment.
- **Working:**
  - Sender maintains a window of frames that can be sent without waiting for an acknowledgment.
  - The receiver also has a window of frames that it expects to receive.
  - After receiving a frame, the receiver sends an acknowledgment, and the window slides forward.
  - If no acknowledgment is received within a certain timeout, the sender retransmits the unacknowledged frames.
- **Go-Back-N ARQ (Automatic Repeat reQuest):** The sender can transmit several frames but must retransmit the entire window if a single frame is lost.
- **Selective Repeat ARQ:** Only the erroneous or lost frames are retransmitted, which is more efficient.
- **Example:** TCP (Transmission Control Protocol) uses a sliding window protocol for reliable data transmission. The window size is adjusted dynamically based on network congestion and receiver's buffer size (using TCP's congestion control algorithms like AIMD).

### 8.6.3 Stop-and-Wait Protocol

- **Definition:** The stop-and-wait protocol is a simple form of error control and flow control. In this protocol, the sender sends one frame and waits for an acknowledgment (ACK) from the receiver before sending the next frame.
- **Mechanism:**
  - The sender transmits a frame and waits for an acknowledgment.
  - If the sender receives the acknowledgment, it sends the next frame.
  - If no acknowledgment is received within a timeout period, the sender retransmits the frame.
- **Pros:**
  - Simple and easy to implement.
  - Suitable for low-latency, low-error networks.
- **Cons:**
  - Inefficient in high-latency networks due to idle time while waiting for acknowledgments.
- **Example:** The Stop-and-Wait ARQ (Automatic Repeat reQuest) protocol is used to ensure that each frame is received correctly before proceeding to the next. If an acknowledgment is not received, the sender retransmits the frame, ensuring reliability.

# 9 Network Layer and Protocols

- **Definition:** Network layer protocols are responsible for packet forwarding including routing through different routers across networks.
- **Key Protocols:**
  - **Internet Protocol (IP):** Core protocol of the network layer responsible for addressing and routing packets across networks.
    - **IPv4:** Uses 32-bit addressing (e.g., 192.168.1.1).
    - **IPv6:** Uses 128-bit addressing (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

- **ICMP (Internet Control Message Protocol):** Used for error reporting and diagnostic purposes (e.g., ping, traceroute).
- **ARP (Address Resolution Protocol):** Maps a 32-bit IP address to a 48-bit MAC address within the local network.
- **RIP (Routing Information Protocol):** A distance vector routing protocol.
- **OSPF (Open Shortest Path First):** A link-state routing protocol.

## 9.1 Port

- **Definition:** A port is a logical identifier that helps distinguish different services or processes on a networked device. It is a 16-bit number associated with an IP address.
- **Port Ranges:**
  - **Well-known Ports:** 0-1023 (e.g., HTTP on port 80, HTTPS on port 443).
  - **Registered Ports:** 1024-49151.
  - **Dynamic/Private Ports:** 49152-65535.

## 9.2 Subnetting in Computer Networks

- **Definition:** Subnetting is the process of dividing a larger network into smaller, logical sub-networks (subnets) to improve routing efficiency and manageability.
- **Key Concepts:**
  - **Subnet Mask:** A 32-bit number used to differentiate the network and host portions of an IP address.
  - **Example:** 255.255.255.0 (/24) is a common subnet mask, indicating that the first 24 bits represent the network.
  - **CIDR (Classless Inter-Domain Routing):** A method of allocating IP addresses and routing that allows for flexible subnetting.
  - **Example:** A /24 subnet means 256 addresses ($2^8$).
- **Benefits:** Subnetting reduces broadcast traffic, improves security, and efficiently allocates IP addresses.

## 9.3 Public and Private IP Addresses

### 9.3.1 Public IP Addresses:

- Assigned by Internet Assigned Numbers Authority (IANA) for unique identification on the internet.
- **Example:** 172.217.16.78 (Google).

### 9.3.2 Private IP Addresses:

- Used within private networks and not routable on the public internet.
- **Ranges:**
  - 10.0.0.0 to 10.255.255.255
  - 172.16.0.0 to 172.31.255.255
  - 192.168.0.0 to 192.168.255.255
- **Example:** 192.168.1.1 (common in home networks).

NAT (Network Address Translation) is used to map private IPs to a public IP for internet communication.

## 9.4 IPv4 Address and IPv6 Address

### 9.4.1 IPv4 Address

- **Definition:** A 32-bit address divided into four octets (8 bits each), written in dotted-decimal notation (e.g., 192.168.0.1).
- **Total Addresses:** $\sim$4.3 billion ($2^{32}$).
- **Challenges:** Exhaustion of IPv4 addresses due to internet growth.

### 9.4.2 IPv6 Address

- **Definition:** A 128-bit address, written in hexadecimal and separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e
- **Total Addresses:** $\sim$340 undecillion ($2^{128}$), addressing the issue of IPv4 exhaustion.
- **Key Features:** Supports auto-configuration, better security with IPsec, and simpler routing.

## 9.5 Network Address Translation (NAT)

- **Definition:** NAT is a technique used to map private IP addresses within a local network to a single public IP address or a pool of public IP addresses.
- **Types:**
  - **Static NAT:** One-to-one mapping of private to public IPs.
  - **Dynamic NAT:** Maps private IPs to a pool of public IP addresses.
  - **PAT (Port Address Translation):** Multiple private IPs are mapped to a single public IP using different ports (also known as NAT Overload).
- **Purpose:** Conserves public IP addresses and adds a layer of security by hiding internal IPs.

## 9.6 Quality of Service (QoS) in Computer Networks

- **Definition:** QoS refers to mechanisms that manage network resources to ensure the performance of specific types of traffic (e.g., voice, video).
- **Key Features:**
  - **Traffic Shaping:** Controls the traffic entering a network to ensure compliance with bandwidth limits.
  - **Prioritization:** Assigning different priorities to different types of traffic (e.g., VoIP gets higher priority over HTTP traffic).
  - **Congestion Management:** Mechanisms like RED (Random Early Detection) and WRED to avoid congestion.
- **Application:** Used in real-time applications such as video conferencing, where latency and jitter must be minimized.

## 9.7 Internet Control Message Protocol (ICMP)

- **Definition:** ICMP is used for diagnostic and error-reporting purposes in network devices. It does not transport application data.
- **Common Uses:**
  - **Ping:** Sends ICMP Echo Request packets to check network connectivity.
  - **Traceroute:** Uses ICMP to trace the path packets take through a network by recording the IP addresses of routers they pass through.
- **Types:**
  - **ICMP Type 0:** Echo Reply (used in ping).
  - **ICMP Type 8:** Echo Request (used in ping).
  - **ICMP Type 3:** Destination Unreachable.

## 9.8 Routing Protocols & Routing Table

### 9.8.1 Routing Protocols

- **Definition:** Routing protocols define how routers communicate with each other to propagate information that enables packet forwarding.
- **Types:**
  - **Distance Vector:** Routes are advertised based on distance (e.g., RIP).
  - **Link State:** Each router has a full view of the network (e.g., OSPF).
  - **Hybrid:** Combines features of distance vector and link-state protocols (e.g., EIGRP).

### 9.8.2 Routing Table

- **Definition:** A routing table stores the routes to different network destinations.
- **Structure:**
  - **Destination Network:** The IP address range of the destination.
  - **Next Hop:** The IP address of the next router along the path.
  - **Metric:** The distance or cost to the destination.

## 9.9 Intradomain & Interdomain Routing

### 9.9.1 Intradomain Routing

- **Definition:** Routing within a single autonomous system (AS). These protocols are optimized for routing within an organization.
- **Example:** OSPF (Open Shortest Path First), RIP (Routing Information Protocol).

### 9.9.2 Interdomain Routing

- **Definition:** Routing between different autonomous systems (ASes) over the public internet.
- **Example:** BGP (Border Gateway Protocol) is the protocol used for interdomain routing, enabling internet-scale routing.

## 9.10 Distance Vector Routing Algorithm

- **Definition:** Distance Vector Routing uses distance (hop count or cost) to determine the best path to a destination.
- **Working:**
  - Each router maintains a table (vector) of the distance to each destination.
  - Routers exchange their tables with their immediate neighbors.
  - Routers update their table if they find a shorter path.
- **Example:** RIP (Routing Information Protocol) uses hop count as a metric, where each hop is considered a distance of 1.
- **Drawbacks:** Slow convergence and prone to routing loops.

### 9.11 Link State Routing Algorithm

- **Definition:** Link State Routing algorithms require each router to have a complete map of the network topology. Routers calculate the shortest path to every other router.
- **Working:**
  - Each router uses LSAs (Link State Advertisements) to share information about its direct links with all other routers.
  - Routers build a topology map and apply Dijkstra's algorithm to compute the shortest path.
- **Example:** OSPF (Open Shortest Path First) uses link-state routing to quickly adapt to changes in the network.
- **Advantages:** Faster convergence and loop-free.

## 10 Application Layer in OSI Model

- **Definition:** The application layer (Layer 7) is the topmost layer of the OSI model, responsible for providing network services directly to the end-users. It interacts with software applications to implement communication functionalities such as email, file transfer, and web browsing.
- **Functions:**
  - Identifying communication partners.
  - Establishing communication.
  - Ensuring that data is in a format usable by applications.
- **Example Protocols:** HTTP, FTP, SMTP, DNS.

### 10.1 World Wide Web (WWW) & How it Works?

- **Definition:** The World Wide Web is an information system that allows documents (webpages) to be accessed via the internet using browsers.
- **How It Works:**
  1. A user enters a URL in the web browser.
  2. The browser sends an HTTP/HTTPS request to the web server.
  3. The web server processes the request and sends back the HTML content.
  4. The browser renders the webpage.
- **Key Technologies:**
  - HTTP/HTTPS for communication.
  - HTML/CSS for webpage structure and design.
  - Web browsers to access and display content.

### 10.2 Application Layer Protocols in Computer Networks

**Common Protocols:**

- **HTTP/HTTPS (Hypertext Transfer Protocol):** Used for web traffic.
- **SMTP (Simple Mail Transfer Protocol):** Used for sending emails.
- **FTP (File Transfer Protocol):** Used for file transfer between a client and a server.
- **DNS (Domain Name System):** Used for domain name resolution.
- **DHCP (Dynamic Host Configuration Protocol):** Automatically assigns IP addresses to devices on a network.

### 10.2.1 Hypertext Transfer Protocol (HTTP)

- **Definition:** HTTP is an application-layer protocol used for transferring hypertext documents (web pages) on the World Wide Web. It defines how messages are formatted and transmitted, and how web servers and browsers should respond to requests.
- **Key Concepts:**
  - **HTTP Methods:**
    - GET: Requests data from the server.
    - POST: Submits data to be processed to the server.
  - **Stateless Protocol:** Each request is independent and unrelated to previous ones.
  - **HTTPS:** A secure version of HTTP that uses SSL/TLS encryption to protect data during transmission.

### 10.2.2 Simple Mail Transfer Protocol (SMTP)

- **Definition:** SMTP is a protocol for sending email messages between servers. It is part of the TCP/IP protocol suite and is used by most email systems for sending emails.
- **How it Works:**
  1. SMTP client establishes a connection to the SMTP server.
  2. The client sends the email content and recipient details.
  3. The SMTP server forwards the email to the recipient's mail server.
- **Ports:**
  - Port 25: Default port for SMTP.
  - Port 587: Used for SMTP with authentication.

### 10.2.3 File Transfer Protocol (FTP)

- **Definition:** FTP is a protocol used to transfer files between a client and a server over a network.
- **How it Works:**
  1. The user connects to an FTP server using a username and password.
  2. Files can be uploaded or downloaded to/from the server.
- **Modes:**
  - **Active Mode:** The server initiates the data connection.
  - **Passive Mode:** The client initiates the data connection.
- **Ports:**
  - Port 21: Control connection.
  - Port 20: Data connection.

### 10.2.4 DNS (Domain Name System)

- **Definition:** DNS is a hierarchical and decentralized naming system that translates human-readable domain names (e.g., www.google.com) into IP addresses (172.217.16.78).
- **How It Works:**
  1. A user enters a domain name in the browser.
  2. The DNS resolver queries multiple DNS servers to find the corresponding IP address.
  3. The browser uses the IP address to connect to the web server.

- **Components:**
  - **DNS Resolver:** Local server that handles queries.
  - **Root DNS Servers:** Top-level servers that respond to queries about top-level domains (TLDs).
  - **Authoritative DNS Servers:** Servers with specific domain information.

# 11 Transport Layer & its Protocols

- **Definition:** The transport layer (Layer 4 of the OSI model) provides reliable data transfer services to the upper layers. It is responsible for ensuring data is delivered error-free, in sequence, and without loss or duplication.
- **Key Functions:**
  - Segmentation: Breaking data into smaller segments.
  - Flow Control: Preventing overwhelming the receiver.
  - Error Control: Ensuring data integrity.
  - Multiplexing: Distinguishing data streams from different applications.
- **Protocols:**
  - **TCP (Transmission Control Protocol):** Provides reliable, connection-oriented communication.
  - **UDP (User Datagram Protocol):** Provides fast, connectionless communication.

## 11.1 User Datagram Protocol (UDP)

- **Definition:** UDP is a connectionless, unreliable transport protocol. It does not provide acknowledgment, retransmission, or sequencing, making it faster but less reliable than TCP.
- **Use Cases:** Suitable for applications where speed is more critical than reliability, such as video streaming, gaming, and VoIP.
- **Features:**
  - No Connection Establishment: No need to establish a connection before data transfer.
  - No Flow Control or Error Recovery: Relies on the application for error handling.
  - Faster Transmission: Due to minimal overhead.

## 11.2 Transmission Control Protocol (TCP)

- **Definition:** TCP is a connection-oriented transport protocol that provides reliable data transmission. It ensures data is delivered accurately and in order.
- **Key Features:**
  - Connection-Oriented: A connection must be established before data transfer.
  - Reliability: TCP uses acknowledgments, retransmission, and error checking.
  - Flow Control: Prevents sender from overwhelming the receiver.
  - Congestion Control: Adapts to network conditions to prevent congestion.

## 11.3 TCP 3-Way Handshake

- **Definition:** The TCP 3-Way Handshake is the process of establishing a connection between a client and a server in a reliable manner.
- **Steps:**
  1. **SYN:** The client sends a SYN (synchronize) packet to initiate the connection.
  2. **SYN-ACK:** The server responds with a SYN-ACK (synchronize-acknowledge) packet.
  3. **ACK:** The client sends an ACK (acknowledge) packet, establishing the connection.
- **Purpose:** Ensures both the client and server are ready for communication and synchronizes sequence numbers.

## 11.4 The Two Generals Problem in TCP

- **Definition:** The Two Generals Problem is a theoretical problem that demonstrates the difficulty of achieving consensus over an unreliable communication channel. It illustrates that reliable communication over an unreliable network (like TCP over IP) can never guarantee absolute certainty about message delivery.
- **Relation to TCP:** TCP solves this by using acknowledgments and retransmissions to minimize uncertainty, but it cannot completely eliminate it, highlighting that perfect reliability is unattainable in asynchronous networks.

## 11.5 TCP Flow Control

- **Definition:** TCP flow control ensures that the sender does not overwhelm the receiver with more data than it can process.
- **Mechanism:**
  - TCP uses a sliding window mechanism where the receiver advertises the amount of buffer space available.
  - The sender adjusts its transmission rate according to the receiver's advertised window size.
- **Purpose:** Prevents data loss by ensuring the sender transmits data at a rate the receiver can handle.

## 11.6 Sliding Window

- **Definition:** Sliding window is a flow control mechanism that allows the sender to send multiple frames before needing an acknowledgment, controlled by a "window size."
- **How It Works:** The sender can transmit a certain number of frames within the window without waiting for an acknowledgment.

## 11.7 Go-Back-N ARQ

- **Definition:** In Go-Back-N ARQ, the sender can send multiple frames, but if an error occurs in one frame, all subsequent frames must be retransmitted.
- **Disadvantage:** Inefficient in networks with high latency or packet loss.

## 11.8 Selective Repeat ARQ

- **Definition:** Selective Repeat ARQ allows only the erroneous frames to be retransmitted, making it more efficient than Go-Back-N.
- **Advantage:** Reduces the number of retransmissions, improving throughput.

## 11.9 TCP Congestion Control

- **Definition:** TCP congestion control prevents network congestion by adjusting the rate of data transmission based on the network's current state.
- **Mechanisms:**
  - **Slow Start:** TCP starts with a small congestion window (cwnd) and increases it exponentially until packet loss occurs.
  - **Congestion Avoidance:** After slow start, TCP increases the window size linearly to avoid congestion.
  - **Fast Retransmit:** When packet loss is detected, TCP retransmits the lost packet before waiting for a timeout.
  - **Fast Recovery:** Instead of going back to slow start, TCP reduces the window size and enters congestion avoidance mode.

## 11.10 Difference Between TCP and UDP

| **Feature** | **TCP** | **UDP** |
|---|---|---|
| Connection | Connection-oriented | Connectionless |
| Reliability | Provides reliability (ack, retransmit) | Unreliable, no error recovery |
| Flow Control | Uses sliding window for flow control | No flow control |
| Congestion Control | Uses congestion control mechanisms | No congestion control |
| Use Case | Suitable for file transfer, web traffic | Suitable for streaming, gaming |
| Speed | Slower due to overhead | Faster due to minimal overhead |