History of Networking:

- The roots of modern computer networking can be traced back to the 1960s with the development of packet-switching networks.
- ARPANET (Advanced Research Projects Agency Network), funded by the U.S. Department of Defense, was one of the earliest packet-switched networks, designed to facilitate communication between research institutions and universities.
- ARPANET continued to grow in the 1970s, connecting more research institutions and becoming the foundation for the development of the TCP/IP (Transmission Control Protocol/Internet Protocol) suite.
- The development of Ethernet by Xerox, Intel, and DEC (Digital Equipment Corporation) further fueled the growth of local area networks (LANs) in corporate environments.
- The 1990s witnessed the explosive growth of the Internet, fueled by advancements in networking technologies, increased connectivity, and the proliferation of the World Wide Web.
- The proliferation of mobile devices, such as smartphones and tablets, led to the development of wireless networking technologies, including Wi-Fi and cellular networks.
- The Internet of Things (IoT) emerged as a significant trend, connecting everyday objects and devices to the Internet and enabling new applications and services.
- The proliferation of high-speed broadband and mobile Internet connectivity continues to reshape how people live, work, and interact in an increasingly interconnected world.

Centralized Networking:

- In a centralized network architecture, control and decision-making authority are concentrated in a single location or entity.
- A central server or controller manages and coordinates network resources, services, and policies.
- Centralized networks often follow a hierarchical design, with multiple levels of devices and infrastructure.
- Network devices communicate with centralized servers for configuration, authentication, and policy enforcement.

Decentralized Networking:

- In a decentralized network, control and decision-making authority are distributed among multiple nodes or entities.
- Each node in the network has autonomy and can make local decisions based on its own knowledge and capabilities.

Peer-to-Peer Communication:

- Decentralized networks rely on peer-to-peer communication, where nodes communicate directly with each other without the need for centralized intermediaries.
- Each node may act as both a client and a server, sharing resources and services with other nodes in the network.

Server:

- Servers listen for incoming requests from clients and respond accordingly.
- They typically have higher processing power, memory, and storage capacity compared to clients.

- Examples include web servers, email servers, file servers, database servers, and application servers.

Functions:

- Servers handle client requests by processing data, executing commands, and providing access to resources.
- They manage and store data, perform computations, enforce security policies, and ensure reliable delivery of services.

Client:

- Clients initiate communication by sending requests to servers.
- They typically have user interfaces that allow users to interact with the network and access services.
- Examples include web browsers, email clients, file transfer programs, and database clients.

Functions:

- Clients send requests to servers for specific services, such as retrieving web pages, sending emails, or accessing files.
- They process responses received from servers and present them to users in a human-readable format.

Types of Network:

1. **Local Area Network (LAN):**

- **Scope:** Covers a small geographical area, such as a single building or campus.
- **Purpose:** Used for connecting devices within a limited area, allowing for file sharing, resource sharing (like printers), and communication.
- **Topology:** Common topologies include bus, ring, star, and mesh.

2. **Wide Area Network (WAN):**

- **Scope:** Spans a large geographical area, often connecting LANs across cities, countries, or continents.
- **Purpose:** Enables long-distance communication and data exchange between geographically dispersed locations.
- **Technologies:** Uses leased lines, satellites, or fiber optic cables.
- **Examples:** Internet, global corporate networks.

3. **Metropolitan Area Network (MAN):**

- **Scope:** Covers a city or metropolitan area.
- **Purpose:** Bridges the gap between LANs and WANs, providing high-speed connectivity for businesses and organizations within a city.
- **Examples:** City-wide Wi-Fi networks, municipal broadband networks.

4. **Personal Area Network (PAN):**

- **Scope:** Covers a very small area, typically within the immediate vicinity of an individual.
- **Purpose:** Connects personal devices, such as smartphones, tablets, laptops, and wearable devices.
- **Technologies:** Bluetooth, Wi-Fi Direct, NFC (Near Field Communication).
- **Examples:** Connecting a smartphone to a smartwatch or Bluetooth headphones.

5. **Storage Area Network (SAN):**

- **Scope:** Specialized network dedicated to providing access to storage resources.
- **Purpose:** Enables high-speed, block-level data transfer between servers and storage devices.
- **Technologies:** Fibre Channel, iSCSI.
- **Use Cases:** Enterprise data centers, database storage, virtualization.

6. **Wireless LAN (WLAN):**

- **Scope:** Wireless version of a LAN, allowing devices to connect to the network without physical cables.
- **Purpose:** Provides flexibility and mobility for devices within the coverage area.
- **Technologies:** Wi-Fi (IEEE 802.11 standards).
- **Use Cases:** Home networks, corporate offices, public hotspots.

7. **Campus Area Network (CAN):**

- **Scope:** Connects multiple LANs within a limited geographical area, such as a university campus or corporate headquarters.
- **Purpose:** Allows for centralized management and sharing of resources across departments or buildings.
- **Technologies:** Similar to LAN technologies (Ethernet, Wi-Fi).

LAN (Local Area Network) vs WAN (Wide Area Network)

LAN (Local Area Network) and WAN (Wide Area Network) are two types of networks with distinct characteristics, sizes, and purposes. Understanding the differences between them is essential for designing, implementing, and managing network infrastructures.

LAN (Local Area Network):

- **Scope:**
    - Covers a small geographic area, such as a single building, office, campus, or home.
    - Typically spans up to a few kilometers.
- **Purpose:**
    - Connects devices within the same location, allowing them to share resources and communicate.
    - Enables file sharing, printer sharing, and access to shared applications and services.
- **Ownership:**
    - Usually owned, controlled, and managed by a single organization, such as a company or educational institution.
- **Speed and Performance:**
    - Generally offers high-speed data transfer rates, often in the range of gigabits per second (Gbps).
    - Low latency and minimal data loss due to the short distances involved.
- **Topology:**
    - Common LAN topologies include star, bus, ring, and mesh.

    - The star topology, where devices connect to a central switch or hub, is prevalent in LANs.

- **Technologies:**

    - Ethernet (IEEE 802.3) is the most common technology used in LANs.
    - Wi-Fi (IEEE 802.11) is used for wireless LANs (WLANs), providing mobility within the coverage area.

- **Examples:**

    - Office networks within a building.
    - Home networks connecting devices like computers, printers, and smart devices.
    - School or university campus networks.

WAN (Wide Area Network):

- **Scope:**

    - Spans a large geographic area, connecting devices across cities, countries, or continents.
    - Can cover vast distances, often using public and private telecommunication services.

- **Purpose:**

    - Enables long-distance communication and data exchange between geographically dispersed locations.
    - Facilitates access to centralized resources, applications, and services from remote locations.

- **Ownership:**

    - Typically involves multiple organizations, service providers, and public networks.
    - Organizations lease WAN services from telecommunications providers or build their private WANs.

- **Speed and Performance:**

    - Data transfer rates in WANs can vary widely depending on the distance and network infrastructure.
    - Speeds can range from kilobits per second (Kbps) to gigabits per second (Gbps), with higher latencies compared to LANs.

- **Topology:**

    - WAN topologies include point-to-point, hub-and-spoke, and full mesh.
    - Point-to-point connections are common for direct links between two locations.
    - Hub-and-spoke configurations use a central site (hub) to connect to multiple remote sites (spokes).
    - Full mesh networks provide direct links between all sites, offering redundancy and fault tolerance.

- **Technologies:**

    - WAN technologies include leased lines, MPLS (Multiprotocol Label Switching), VPN (Virtual Private Network), and public internet connections.
    - Satellite links, fiber optics, and microwave links are used for long-distance communication.

- **Examples:**

    - Connecting branch offices of a multinational corporation.
    - Linking data centers located in different cities or countries.
    - Internet connectivity provided by ISPs (Internet Service Providers).
    - Telecommunication networks operated by phone companies.

Comparison Summary:

Feature	LAN	WAN
Scope	Small geographic area	Large geographic area
Purpose	Local device connectivity, resource sharing	Long-distance communication, centralized access
Speed	High-speed (Gbps)	Varies widely (Kbps to Gbps)
Ownership	Single organization	Multiple organizations, service providers
Topology	Star, bus, ring, mesh	Point-to-point, hub-and-spoke, full mesh
Technologies	Ethernet, Wi-Fi	Leased lines, MPLS, VPN, internet links
Examples	Office networks, home networks	Corporate networks, internet, telecom networks

Flavours of Ethernet

Ethernet, the most widely used technology for Local Area Networks (LANs), has evolved over the years with various standards and "flavors" to accommodate increasing data speeds, improve efficiency, and ensure compatibility. Here are some of the key flavors or versions of Ethernet:

1. **Ethernet:**

- **Speed:** 10 Mbps (Megabits per second)
- **Standard:** IEEE 802.3
- **Description:** The original Ethernet standard developed by Xerox, Intel, and Digital Equipment Corporation (DEC). It used coaxial cables and a bus topology.

2. **Fast Ethernet:**

- **Speed:** 100 Mbps
- **Standard:** IEEE 802.3u
- **Description:** Introduced to provide a significant speed boost over traditional Ethernet. Utilizes twisted pair or fiber optic cabling.

3. **Gigabit Ethernet:**

- **Speed:** 1 Gbps (Gigabit per second)
- **Standard:** IEEE 802.3ab
- **Description:** Offers ten times the speed of Fast Ethernet. Commonly used in modern networks for higher bandwidth requirements.

4. **10-Gigabit Ethernet:**

- **Speed:** 10 Gbps
- **Standard:** IEEE 802.3ae
- **Description:** Provides even greater speed for data-intensive applications, server connectivity, and backbone connections.

5. **100-Gigabit Ethernet:**

- **Speed:** 100 Gbps
- **Standard:** IEEE 802.3bj
- **Description:** Provides ultra-high-speed connectivity for data centers, cloud computing, and high-performance computing environments.

Media Access Control (MAC)

In computer networking, the Media Access Control (MAC) address is a unique identifier assigned to network interfaces for communication at the data link layer of the OSI model. It serves as a hardware address that uniquely identifies each device on a network. Here's an overview of MAC addresses:

1. **Definition:**

- **MAC Address:** A MAC address, also known as a physical address or hardware address, is a unique identifier assigned to a network interface controller (NIC) by the manufacturer. It is used to uniquely identify devices on a network.

2. **Format:**

- **Length:** A MAC address is 48 bits (6 bytes) long.
- **Hexadecimal:** Typically represented as 12 hexadecimal digits (0-9, A-F).
- **Example:** '00:1A:2B:3C:4D:5E'

3. **Usage:**

- **Uniqueness:** Each device on a network, such as computers, smartphones, printers, and routers, has a unique MAC address.
- **Packet Routing:** MAC addresses are used for packet routing within LANs. When a device sends data on the network, it includes the MAC address of the intended recipient.

4. **Types of MAC Addresses:**

- **Unicast:** The most common type, used for one-to-one communication. It identifies a specific device.
- **Multicast:** Used for one-to-many communication. Data is sent to a group of devices that share the same multicast address.

- **Broadcast:** Used for one-to-all communication. Data is sent to all devices on the network. Broadcasts typically use the MAC address 'FF:FF:FF:FF:FF:FF'.

CRC (Cyclic Redundancy Check)

CRC (Cyclic Redundancy Check) is an error-detecting technique used in networking and data communication to ensure the integrity of transmitted data. It is a type of checksum that detects errors caused by noise, interference, or data corruption during transmission. Here's an overview of CRC:

Purpose:

- **Error Detection:** CRC is used to detect errors in transmitted data by comparing the received data with a calculated checksum.

Cerrier Sence Multiple Access /Collision Detection

CSMA/CD stands for Carrier Sense Multiple Access with Collision Detection. It's a media access control method used in Ethernet networks to regulate access to the shared communication medium and manage collisions that occur when two or more devices transmit data simultaneously. Here's an overview of CSMA/CD:

Carrier Sense:

- Before transmitting, a device listens to the communication medium to ensure it's idle. If it detects a carrier (signal) indicating that another device is transmitting, it defers its transmission.

Collision Detection:

- While transmitting, the device continues to monitor the medium for the presence of other signals.
- If the device detects a collision (i.e., if it senses a different signal on the medium than what it's transmitting), it immediately stops transmitting to prevent data corruption.
- After detecting a collision, the transmitting device enters a backoff period, during which it waits for a random amount of time before attempting to retransmit.
- The backoff algorithm helps reduce the probability of another collision occurring when the device retries transmission.

ARP (Address Resolution Protocol)

ARP (Address Resolution Protocol) is a networking protocol used for mapping an IP address to a MAC (Media Access Control) address. It is an essential part of the TCP/IP protocol suite and plays a crucial role in communication within a Local Area Network (LAN). Here's an overview of ARP:

How ARP Works:

When a device wants to send data to another device on the same subnet, it needs to know the MAC address of the destination device.

- **ARP Request:**
    - The sending device broadcasts an ARP request packet to the entire network.

    - The ARP request includes the IP address of the destination device that the sender wants to communicate with.

- **ARP Reply:**

    - The device with the matching IP address sends an ARP reply packet back to the sender.
    - The ARP reply includes its MAC address, allowing the sender to create an ARP table entry.

- **ARP Table:**

    - Once the sender receives the ARP reply, it creates an entry in its ARP table.
    - The ARP table stores IP addresses and their corresponding MAC addresses for future reference.

- **ARP cache timer: 10 min**

- ARP cache timer will be refreshed if machine sends frame within span of 10 min.

- But after 10 min hs to follows the same procedure of ARP.