# Networking Fundamentals

## Introduction to Networking

---

### 1. What is Networking?

Networking refers to the practice of connecting multiple computing devices or systems to share resources, exchange data, and communicate with one another. This can be achieved using physical cables, wireless signals, or a combination of both. Networks facilitate resource sharing (e.g., printers, files) and enable seamless communication (e.g., emails, video calls).

Key Elements of Networking

- Nodes: Devices such as computers, printers, or servers within a network.
- Links: Physical or wireless communication pathways between nodes.
- Protocols: Rules and conventions for data exchange, like TCP/IP.

---

### 2. Definition of a Network

A network is a system of interconnected devices designed to share information and resources efficiently. Networks are classified by size, functionality, and structure (e.g., LAN, WAN, VPN).

---

### 3. Data Transmission Modes

Data transmission is the process of transferring data between devices through a communication channel. Transmission modes define the direction and simultaneity of data flow.

#### 3.1 Simplex Mode

- Definition: Data flows in one direction only.
- Example: Keyboard to a computer, Television broadcasting.
- Advantages: Simple and cost-effective.
- Disadvantages: Lack of two-way communication.

#### 3.2 Half-Duplex Mode

- Definition: Data flows in both directions but only one direction at a time.
- Example: Walkie-Talkies, two-way radios.
- Advantages: Better resource utilization compared to simplex.
- Disadvantages: Slower due to the alternating flow.

#### 3.3 Full-Duplex Mode

- Definition: Data flows simultaneously in both directions.
- Example: Telephone communication, video calls.
- Advantages: Fast and efficient communication.
- Disadvantages: Higher cost and complexity.

## 4. Real-Life Examples of Networking Applications

### 4.1 Business Communication

- Email Systems: Employees share updates, memos, and reports.
- Cloud Computing: Collaboration through shared cloud services like Google Workspace.

### 4.2 Social Networking and Entertainment

- Social Media Platforms: Networks like Facebook and LinkedIn connect millions globally.
- Streaming Services: Platforms like Netflix rely on content delivery networks (CDNs).

### 4.3 Healthcare

- Hospitals use internal networks to manage patient records and diagnostics.
- Telemedicine allows doctors to consult with patients remotely via the Internet.

### 4.4 Smart Homes and IoT

- Devices like smart thermostats, security systems, and voice assistants connect via home networks.

### 4.5 Education

- Virtual classrooms and e-learning platforms facilitate remote education.

## 5. Importance of Networking

Networking underpins the modern digital world. Its benefits include:

- Resource Sharing: Shared printers, storage devices, and internet connections.
- Cost Efficiency: Reduces hardware redundancy by centralizing resources.
- Communication: Enables instant messaging, video conferencing, and data sharing.
- Accessibility: Allows remote access to files, applications, and systems.

## 6. Summary Table: Data Transmission Modes

| Mode | Direction | Simultaneity | Examples |
|---|---|---|---|
| **Simplex** | **One-way** | **No** | **Keyboard to computer, TV broadcasting** |
| **Half-Duplex** | **Two-way** | **Alternating directions** | **Walkie-Talkies** |
| **Full-Duplex** | **Two-way** | **Simultaneous** | **Telephone, video calls** |

This table summarizes the key distinctions among the three data transmission modes.

## Types of Networks

## 1. Introduction to Networks

A network is classified based on its scale, purpose, and geographic area. These classifications help in designing networks that meet specific requirements for businesses, individuals, or organizations. Common types include PAN, LAN, MAN, WAN, GAN, and VPN.

# 2. Types of Networks

### 2.1 PAN (Personal Area Network)

- Definition: A network used for communication among personal devices like smartphones, laptops, and wearables within a small area, typically a few meters.
- Features:
  - Coverage: Up to 10 meters.
  - Devices: Bluetooth, Infrared, or USB-based communication.
- Example:
  - Connecting a smartphone to a smartwatch or wireless headphones.

---

### 2.2 LAN (Local Area Network)

- Definition: A network connecting devices within a limited area, such as an office, school, or home.
- Features:
  - Coverage: Up to 1 kilometer.
  - High speed, low latency.
  - Uses Ethernet cables or Wi-Fi.
- Example:
  - Office network connecting computers, printers, and servers.
  - Wi-Fi network in a coffee shop.

---

### 2.3 MAN (Metropolitan Area Network)

- Definition: A network spanning a city or large campus, larger than a LAN but smaller than a WAN.
- Features:
  - Coverage: 1–50 kilometers.
  - Typically owned by governments or ISPs.
- Example:
  - Cable TV networks.
  - City-wide public Wi-Fi.

---

### 2.4 WAN (Wide Area Network)

- Definition: A network that spans a large geographic area, such as countries or continents.

- Features:
  - Coverage: Global reach.
  - Slower speeds compared to LAN and MAN.
- Example:
  - The Internet.
  - Corporate networks connecting offices in different countries.

### 2.5 GAN (Global Area Network)

- Definition: A network designed for worldwide communication. It interconnects WANs and LANs using satellites or global fiber optic infrastructure.
- Features:
  - Truly global coverage.
  - High scalability.
- Example:
  - Satellite communication systems like Starlink.
  - International banking networks.

### 2.6 VPN (Virtual Private Network)

- Definition: A secure network created over a public network like the Internet.
- Features:
  - Encrypts data to ensure privacy.
  - Connects users to remote resources securely.
- Example:
  - Remote employees accessing company servers.
  - Browsing securely on public Wi-Fi.

## 3. Comparison of Network Types

| Type | Coverage Area | Speed | Cost | Example |
|---|---|---|---|---|
| PAN | Up to 10 meters | High | Low | Bluetooth headphones |
| LAN | 1 kilometer | Very High | Moderate | Office network |
| MAN | 1–50 kilometers | Medium | High | City-wide Wi-Fi |
| WAN | Global | Low | Very High | The Internet |
| GAN | Worldwide | Medium | Very High | Satellite communication |
| VPN | Virtual, over any distance | Depends | Low to High | Secure remote office access |

## 4. Practical Examples and Use Cases

### 4.1 PAN:

- Syncing data between a smartphone and a fitness tracker.

### 4.2 LAN:

- Shared printers in a university lab.
- Multiplayer gaming on a home network.

### 4.3 MAN:

- Metro Ethernet services for businesses.
- WiMAX providing broadband across a city.

### 4.4 WAN:

- Global e-commerce platforms like Amazon.
- Video conferencing between multinational offices.

### 4.5 GAN:

- Real-time international stock market data exchange.
- Satellite-based emergency communication.

### 4.6 VPN:

- Employees accessing sensitive company files while traveling.
- Masking IP addresses for privacy.

## 5. Key Considerations for Network Selection

1. Purpose: Choose based on the need (e.g., personal use, business).
2. Budget: Larger networks like GAN and WAN are costly.
3. Security: VPN adds encryption for sensitive data.
4. Scalability: Future-proof solutions like WAN or GAN for global operations.

## 6. Summary Table

| Network Type | Best For | Advantages | Disadvantages |
|---|---|---|---|
| PAN | Personal device connectivity | Convenient and inexpensive | Limited range |
| LAN | Small organizations | High speed, low cost | Limited to small areas |
| MAN | Large campuses or cities | Covers large areas effectively | Expensive infrastructure |
| WAN | Global operations | Connects remote locations | High latency, costly |
| GAN | Global communications | Truly worldwide coverage | Highly complex and costly |
| VPN | Secure remote access | Encrypts data, cost-effective | Relies on public networks |

# Network Topology

### 1. Introduction to Network Topology

Network topology refers to the arrangement of devices (nodes) in a network and how they are interconnected, either physically or logically. It determines how data flows, how devices communicate, and the network's reliability and performance.

Key Components in Network Topology

- Nodes: Devices such as computers, printers, and routers.
- Links: Connections between nodes, which can be wired or wireless.

### 2. Types of Network Topologies

### 2.1 Star Topology

- Structure:
  All nodes are connected to a central hub or switch.
- Data Flow:
  Communication occurs via the central hub.

Advantages:

1. Easy to set up and manage.
2. Failure of a single node doesn’t affect the network.
3. Centralized management and troubleshooting.

Disadvantages:

1. Hub failure disrupts the entire network.
2. Requires more cabling than other topologies.

Applications:

- Office LANs, home networks.

### 2.2 Ring Topology

- Structure:
  Nodes are connected in a circular manner, with each node linked to two others.
- Data Flow:
  Data travels in one direction (unidirectional) or both directions (bidirectional).

Advantages:

1. Simple to install and expand.
2. Data flows in a predictable manner.

Disadvantages:

1. A single node or cable failure can disrupt the network.
2. Troubleshooting is challenging.

Applications:

- Telecommunications, fiber optic networks.

---

### 2.3 Bus Topology

- Structure:
  All nodes are connected to a single central cable called the "bus."
- Data Flow:
  Data travels along the bus, and all nodes receive it.

Advantages:

1. Cost-effective for small networks.
2. Easy to set up with minimal cabling.

Disadvantages:

1. A cable fault disrupts the entire network.
2. Limited scalability and performance decline with more nodes.

Applications:

- Early LANs, small-scale setups.

---

### 2.4 Mesh Topology

- Structure:
  Every node is connected to every other node.
- Data Flow:
  Data can take multiple paths to its destination.

Advantages:

1. Highly reliable with no single point of failure.
2. Efficient routing and fault tolerance.

Disadvantages:

1. Expensive due to the number of connections required.
2. Complex to install and maintain.

Applications:

- Military communication, critical systems like banking networks.

---

### 2.5 Tree Topology

- Structure:
  A hierarchical combination of star and bus topologies.
- Data Flow:
  Data flows between layers of nodes in a structured hierarchy.

Advantages:

1. Scalable and easy to expand.
2. Suitable for large networks with distinct layers.

Disadvantages:

1. Higher cabling requirements.
2. Central backbone failure affects the entire network.

Applications:

- Corporate networks, hierarchical systems like university networks.

---

### 2.6 Hybrid Topology

- Structure:
  A mix of two or more different topologies.
- Data Flow:
  Depends on the combined topologies.

**Advantages:**

1. Flexible and scalable.
2. Can be tailored to specific needs.

**Disadvantages:**

1. Expensive and complex to set up.
2. Challenging to troubleshoot.

**Applications:**

- Large enterprises, data centers.

---

### 3. Comparison of Network Topologies

| Topology | Structure | Advantages | Disadvantages | Best Use Cases |
|---|---|---|---|---|
| **Star** | **Centralized** | **Easy to manage; scalable** | **Hub failure disrupts the network** | **Small offices, home networks** |
| **Ring** | **Circular** | **Predictable data flow** | **Vulnerable to single-point failures** | **Fiber optic networks, telecom** |
| **Bus** | **Linear single cable** | **Cost-effective, minimal cabling** | **Cable failure affects all; not scalable** | **Small, temporary networks** |

| | | | | |
|---|---|---|---|---|
| **Mesh** | **Fully interconnected** | **High reliability, fault tolerance** | **Expensive; complex to maintain** | **Critical systems, military applications** |
| **Tree** | **Hierarchical** | **Scalable for large networks** | **Backbone failure affects the network** | **Corporate or university networks** |
| **Hybrid** | **Mixed** | **Flexible, tailored for needs** | **Expensive; complex to troubleshoot** | **Data centers, large enterprises** |

### 4. Practical Examples of Topologies

1. **Star Topology:**
   - A school's computer lab where all systems connect to a central switch.
2. **Ring Topology:**
   - Used in token ring networks and metropolitan area networks.
3. **Bus Topology:**
   - Early Ethernet networks with coaxial cables.
4. **Mesh Topology:**
   - Air traffic control systems where reliability is critical.
5. **Tree Topology:**
   - A company with separate branches, each acting as a star within a hierarchical structure.
6. **Hybrid Topology:**
   - A large company combining star and mesh for scalability and reliability.

# 4. Networking Devices

### 1. Introduction to Networking Devices

Networking devices are essential components that enable communication, data transfer, and connectivity in a network. They are classified based on their functionality, layer of operation, and purpose in the network.

### 2. Overview and Working of Networking Devices

### 2.1 Hub

- Definition: A basic networking device that connects multiple computers in a network. It operates at the physical layer (Layer 1) of the OSI model.
- Working:

    - Receives data from one port and broadcasts it to all other connected ports.
    - No intelligence; cannot filter or direct traffic.
- Usage:
    - Small networks with minimal data traffic.
    - Legacy systems.

### 2.2 Repeater

- Definition: A device that regenerates and amplifies signals to extend the network's range.
- Working:
    - Receives weak or degraded signals.
    - Amplifies and retransmits them.
- Usage:
    - Long-distance wired or wireless communication.

### 2.3 Bridge

- Definition: A device that connects two or more LAN segments to create a single network. It operates at the data link layer (Layer 2).
- Working:
    - Filters and forwards data based on MAC addresses.
- Usage:
    - Reduces network traffic by dividing large networks into smaller segments.

### 2.4 Switch

- Definition: An advanced version of a hub operating at the data link layer (Layer 2) and sometimes at the network layer (Layer 3).
- Working:
    - Receives data frames and forwards them to the specific device based on MAC or IP addresses.
    - Maintains a MAC address table for efficient communication.
- Usage:
    - Backbone of modern LANs due to its speed and efficiency.

### 2.5 Router

- Definition: A device that routes data packets between different networks. It operates at the network layer (Layer 3).
- Working:
    - Uses IP addresses to determine the best path for data transmission.
    - Supports multiple protocols like RIP, OSPF, and BGP.
- Usage:
    - Connects LANs to the Internet.

    - Enables communication between different networks.

### 2.6 NIC (Network Interface Card)

- Definition: A hardware component that allows devices to connect to a network.
- Working:
    - Converts data from a computer into signals for transmission over the network.
    - Supports wired (Ethernet) or wireless (Wi-Fi) communication.
- Usage:
    - Essential for all devices participating in a network.

### 2.7 Gateway

- Definition: A device that connects networks using different communication protocols.
- Working:
    - Translates and forwards data between incompatible networks.
    - Operates at all layers of the OSI model, primarily focusing on higher layers.
- Usage:
    - Connecting enterprise networks to external networks.

### 2.8 Modem (Modulator-Demodulator)

- Definition: A device that converts digital signals to analog for transmission over telephone lines and vice versa.
- Working:
    - Modulation for outgoing signals.
    - Demodulation for incoming signals.
- Usage:
    - Provides Internet connectivity in homes and offices.

---

## 3. Comparison of Networking Devices

| Device | OSI Layer | Primary Function | Key Feature | Example Usage |
|---|---|---|---|---|
| **Hub** | **Physical** | **Connects multiple devices** | **Broadcasts to all ports** | **Small, legacy networks** |
| **Repeater** | **Physical** | **Extends signal range** | **Amplifies weak signals** | **Extending Ethernet cable limits** |
| **Bridge** | **Data Link** | **Connects and segments LANs** | **Filters traffic using MAC** | **Dividing large networks** |
| **Switch** | **Data Link/Network** | **Intelligent device for traffic forwarding** | **MAC/IP-based forwarding** | **Office LANs** |
| **Router** | **Network** | **Routes data between networks** | **Supports multiple protocols** | **Home Internet connectivity** |

| | | | | |
|---|---|---|---|---|
| **NIC** | **Data Link** | **Enables network communication** | **Wired or wireless transmission** | **Laptops, desktops** |
| **Gateway** | **All** | **Connects dissimilar networks** | **Protocol conversion** | **Enterprise Internet access** |
| **Modem** | **Physical/Data Link** | **Converts analog to digital signals** | **Modulation and demodulation** | **Home broadband** |

**4. Practical Usage Scenarios**

4.1 Hub

- Small-scale, legacy office setups.

4.2 Repeater

- Extending a wireless network in a large home or campus.

4.3 Bridge

- Connecting two departments in an organization without changing the network structure.

4.4 Switch

- Central device in LANs for efficient device communication.

4.5 Router

- Connecting a home network to the Internet using ISP-provided equipment.

4.6 NIC

- Enabling network access for IoT devices or laptops.

4.7 Gateway

- Translating communication between IoT devices using proprietary protocols and the Internet.

4.8 Modem

- Providing broadband access in homes using DSL or fiber technology.

**5. Advantages of Networking Devices**

1. Improved Connectivity: Ensures seamless communication across devices and networks.
2. Enhanced Performance: Devices like switches and routers optimize traffic flow.
3. Scalability: Easily expand networks with bridges and routers.
4. Security: Gateways provide protocol-specific security and filtering.

# 5. OSI and TCP/IP Models

**1. Introduction to OSI and TCP/IP Models**

The OSI (Open Systems Interconnection) and TCP/IP models are conceptual frameworks used to understand and design network communication. Both models are essential for network protocols and offer a structured way of describing how data flows across a network.

---

**2. OSI Model (7 Layers)**

The OSI Model consists of 7 layers. Each layer performs specific tasks and communicates with the layers directly above and below it. Below is a detailed breakdown of each layer:

**2.1 Layer 1: Physical Layer**

- Function:
  Deals with the transmission of raw bitstreams over a physical medium (cables, fiber optics).
- Protocols and Technologies:
  - Ethernet, USB, Bluetooth.
  - Fiber Optic, Wi-Fi, and other physical transmission mediums.
- Real-life Example:
  - A computer's NIC (Network Interface Card) connecting to a network via an Ethernet cable.

**2.2 Layer 2: Data Link Layer**

- Function:
  Provides error detection and correction, and organizes data into frames for the next layer.
- Protocols:
  - Ethernet (MAC), PPP, Frame Relay.
- Real-life Example:
  - Switches operate at this layer to forward frames based on MAC addresses.
  -

**2.3 Layer 3: Network Layer**

- Function:
  Responsible for logical addressing, routing, and packet forwarding between devices across different networks.
- Protocols:
  - IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol).
- Real-life Example:
  - Routers forward data between devices on different networks using IP addresses.

**2.4 Layer 4: Transport Layer**

- Function:
  Ensures end-to-end communication and data integrity between devices. Manages flow control, error recovery, and data segmentation.
- Protocols:
  - TCP (Transmission Control Protocol), UDP (User Datagram Protocol).
- Real-life Example:
  - Web browsing (HTTP/HTTPS) uses TCP for reliable communication.

### 2.5 Layer 5: Session Layer

- Function:
  Establishes, manages, and terminates communication sessions between devices.
- Protocols:
  - NetBIOS, RPC (Remote Procedure Call).
- Real-life Example:
  - A video conferencing system that maintains an active session between users.

### 2.6 Layer 6: Presentation Layer

- Function:
  Translates data between the application and the network. It handles data encryption, compression, and format conversion.
- Protocols:
  - SSL/TLS, JPEG, ASCII.
- Real-life Example:
  - SSL/TLS encryption for secure web browsing.

### 2.7 Layer 7: Application Layer

- Function:
  Directly interacts with the end-user applications. Provides services like email, file transfer, and web browsing.
- Protocols:
  - HTTP, HTTPS, FTP, SMTP, IMAP, DNS.
- Real-life Example:
  - A web browser (like Chrome) using HTTP/HTTPS to retrieve and display web pages.

---

### 3. TCP/IP Model (4 Layers)

The TCP/IP Model is a simpler, more streamlined model that serves as the foundation of the Internet. It consists of 4 layers.

3.1 Layer 1: Link Layer (Network Interface Layer)

- Function:
  Deals with physical network connections and data link protocols.
- Protocols:
  - Ethernet, Wi-Fi, ARP.
- Real-life Example:
  - A computer connecting to a network via Ethernet or Wi-Fi.

### 3.2 Layer 2: Internet Layer

- Function:
  Responsible for addressing, routing, and data packet delivery across networks.
- Protocols:
  - IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP.
- Real-life Example:
  - A router forwarding IP packets to the correct destination.

### 3.3 Layer 3: Transport Layer

- Function:
  Manages end-to-end communication between devices.
- Protocols:
  - TCP, UDP.
- Real-life Example:
  - Web servers use TCP for reliable delivery of web pages.

### 3.4 Layer 4: Application Layer

- Function:
  Supports end-user applications and facilitates network services like file transfer and email.
- Protocols:
  - HTTP, FTP, SMTP, DNS, Telnet.
- Real-life Example:
  - A user accessing a web page using HTTP or sending an email using SMTP.

---

## 5. OSI vs. TCP/IP Models

| OSI Model | TCP/IP Model |
|---|---|
| **Layer 7: Application** | **Layer 4: Application** |
| **Layer 6: Presentation** | **Layer 3: Transport** |

| | |
|---|---|
| **Layer 5: Session** | **Layer 2: Internet** |
| **Layer 4: Transport** | **Layer 1: Link** |
| **Layer 3: Network** | **(No direct equivalent)** |
| **Layer 2: Data Link** | |
| **Layer 1: Physical** | |

- Difference in Layer Structure: OSI has more detailed layers (7) compared to TCP/IP (4). However, they fulfill similar functions.

---

### 5. Real-life Protocol Examples

- HTTP/HTTPS (Application Layer):
  Web browsing over the internet, utilizing TCP/IP and SSL/TLS for secure communication.
- DNS (Application Layer):
  Resolves domain names to IP addresses, allowing users to access websites by name (e.g., google.com).
- TCP (Transport Layer):
  Provides reliable communication for web browsing, file transfer, and email services.
- IP (Internet Layer):
  Routing data packets between devices on different networks.

---

### 6. Summary of OSI and TCP/IP Models

- OSI Model is more comprehensive and used for educational purposes, with 7 layers that clearly separate different functions in the network.
- TCP/IP Model is the practical model, specifically designed for the Internet, using 4 layers but still fulfilling the same basic functions.

---

# 6. IP Addressing and Address Types

---

### 1. Introduction to IP Addressing

IP addressing is a system used to identify devices on a network using a unique identifier called an IP address. These addresses allow devices to send and receive data over the internet or a local network.

---

### 2. Types of Addresses

### 2.1 IP Address

- Definition: A numerical label assigned to each device on a network to identify it and allow communication.
- Format:
  - IPv4 (32-bit): e.g., 192.168.1.1
  - IPv6 (128-bit): e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334

### 2.2 MAC Address

- Definition: A unique identifier assigned to network interfaces for communications at the data link layer.
- Format: A 48-bit address in hexadecimal (e.g., 00:14:22:01:23:45).
- Usage: Ensures devices can communicate on the local network (LAN).

### 2.3 Port Address

- Definition: A logical endpoint for communication, used by transport layer protocols like TCP and UDP.
- Format: A 16-bit number (e.g., HTTP uses port 80, HTTPS uses port 443).
- Usage: Specifies which application the data should be delivered to on the device.

---

## 3. IP Address Classes

- Class A:
  - IP Range: 0.0.0.0 to 127.255.255.255
  - Supports large networks with over 16 million hosts.
- Class B:
  - IP Range: 128.0.0.0 to 191.255.255.255
  - Suitable for medium-sized networks.
- Class C:
  - IP Range: 192.0.0.0 to 223.255.255.255
  - Ideal for small networks with up to 254 hosts.
- Class D:
  - IP Range: 224.0.0.0 to 239.255.255.255
  - Used for multicast communication.
- Class E:
  - IP Range: 240.0.0.0 to 255.255.255.255
  - Reserved for experimental purposes.

---

## 4. IP Addressing Mechanism

- Static IP Addressing: A fixed IP address assigned to a device, ensuring it remains the same across reboots.

- Dynamic IP Addressing (DHCP): Automatically assigns an IP address to a device from a pool of addresses.

# Introduction to Important Network Protocols

Network protocols are essential sets of rules that govern how data is transmitted and received between devices over a network. Different protocols serve different purposes, and understanding these is crucial for network management, troubleshooting, and security.

---

## 2. DNS (Domain Name System)

### 2.1 Definition

The **Domain Name System (DNS)** is a hierarchical naming system for resources connected to the internet or a private network. It translates human-readable domain names (e.g., google.com) into machine-readable IP addresses (e.g., 172.217.14.206).

### 2.2 DNS Working

- **Step 1: DNS Query Initiation**
  A user types a URL (e.g., www.example.com) in their browser. The browser first checks if the IP address corresponding to that domain is already cached in the local DNS cache.
- **Step 2: DNS Resolution**
  If the address is not cached, the request is sent to a DNS resolver (typically provided by the ISP). The resolver will then query the DNS hierarchy to resolve the domain name into an IP address.
- **Step 3: Recursive Querying**
  The DNS resolver performs a recursive query by contacting different DNS servers, starting with the **Root DNS Server**, then to a **Top-Level Domain (TLD) Server** (e.g., .com, .org), and finally to an **Authoritative DNS Server** that holds the actual IP address.
- **Step 4: Return of IP Address**
  Once the IP address is found, it is returned to the DNS resolver, which then passes it back to the client (the browser in this case).
- **Step 5: Caching**
  The resolved IP address is cached on the client machine and DNS resolver for future use to reduce latency and unnecessary queries.

### 2.3 Types of DNS Records

- **A Record (Address Record):** Maps a domain to an IPv4 address.
- **AAAA Record:** Maps a domain to an IPv6 address.

- **CNAME Record (Canonical Name):** Alias for another domain name.
- **MX Record (Mail Exchange):** Specifies mail servers for a domain.
- **PTR Record (Pointer):** Resolves IP addresses to domain names (reverse DNS lookup).
- **NS Record (Name Server):** Specifies authoritative name servers for a domain.

### 2.4 Real-Life Example

When you type www.google.com into a browser, a DNS query is sent, and the domain name is resolved to **216.58.217.46**, which the browser uses to establish the connection.

---

## 3. DHCP (Dynamic Host Configuration Protocol)

### 3.1 Definition

DHCP is a network management protocol used to assign IP addresses and other network configuration details dynamically to devices on a network.

### 3.2 Working

- A device (client) sends a **DHCP Discover** message when it connects to the network.
- The DHCP server responds with an available IP address in a **DHCP Offer**.
- The client sends a **DHCP Request** to confirm the address.
- The server sends a **DHCP Acknowledgement** with the final IP address assignment.

---

## 4. TCP (Transmission Control Protocol)

### 4.1 Definition

TCP is a connection-oriented protocol used for reliable data transmission between devices over a network. It ensures data integrity and guarantees delivery of packets in the correct order.

### 4.2 Features

- **Three-Way Handshake:** Establishes a reliable connection.
- **Flow Control and Error Checking:** Ensures data is transmitted without errors.
- **Connection Establishment:** Before data is transmitted, TCP ensures a stable connection between the sender and receiver.

---

## 5. UDP (User Datagram Protocol)

### 5.1 Definition

UDP is a connectionless protocol used for faster data transmission with no guarantee of reliability, order, or data integrity.

### 5.2 Features

- **Faster but Unreliable:** Suitable for applications like video streaming and online gaming where speed is prioritized over reliability.
- **No Connection Establishment:** Data packets are sent without establishing a connection.

---

## 6. SMTP (Simple Mail Transfer Protocol)

### 6.1 Definition

SMTP is a protocol used for sending and relaying email messages between mail servers.

### 6.2 Working

- The client sends an email request to the SMTP server.
- The SMTP server processes the message and forwards it to the recipient's mail server.
- The message is then retrieved by the recipient using IMAP or POP3.

---

## 7. ARP (Address Resolution Protocol)

### 7.1 Definition

ARP is used to map a 32-bit IP address to a MAC address in a local network.

### 7.2 Working

- When a device needs to communicate with another device in the local network, it sends an ARP request to find the MAC address corresponding to a known IP address.
- The device with the matching IP address replies with its MAC address.

---

## 8. ICMP (Internet Control Message Protocol)

### 8.1 Definition

ICMP is used for sending error messages and diagnostic information in IP networks.

### 8.2 Working

- **Ping:** ICMP is used in the **Ping** command to test the reachability of a host.
- **Destination Unreachable:** Sends an error message if a packet cannot reach its destination.

---

## 9. POP3 (Post Office Protocol version 3)

### 9.1 Definition

POP3 is a protocol used by email clients to retrieve emails from a mail server.

### 9.2 Working

- Downloads email messages from the server to the local device.
- Once downloaded, emails are removed from the server, making them inaccessible from other devices.

---

## 10. IMAP (Internet Message Access Protocol)

### 10.1 Definition

IMAP is a protocol used for retrieving email messages from a mail server.

### 10.2 Working

- Emails are stored on the server and accessed remotely.

- Multiple devices can access and manage the same mailbox.

---

### 11. FTP (File Transfer Protocol)

#### 11.1 Definition

FTP is a protocol used for transferring files between devices over a network.

#### 11.2 Working

- **Active Mode:** The client establishes a connection with the server on one port and the server connects back to the client on another port.
- **Passive Mode:** The server listens on a port, and the client connects to it.

---

### 12. HTTP (Hypertext Transfer Protocol)

#### 12.1 Definition

HTTP is the protocol used to request and transfer web pages over the internet.

#### 12.2 Working

- Clients (browsers) send HTTP requests to web servers for web page resources.
- Servers respond with HTML, images, or other content, which the browser displays to the user.

---

### 13. HTTPS (Hypertext Transfer Protocol Secure)

#### 13.1 Definition

HTTPS is a secure version of HTTP that uses encryption (SSL/TLS) to secure data transmission between the client and server.

#### 13.2 Working

- Encrypts the data exchanged between the browser and the server, preventing interception by third parties.

---

### 14. Telnet

#### 14.1 Definition

Telnet is a protocol used for remote login to devices over a network.

#### 14.2 Working

- Establishes a virtual terminal connection to remote devices, allowing administrators to manage systems from a distance.

---

### 15. Summary of Important Protocols

- **DNS:** Resolves domain names to IP addresses, enabling web browsing and services.
- **DHCP:** Automatically assigns IP addresses to devices on a network.
- **TCP and UDP:** Manage reliable and fast communication, respectively.

- **SMTP, POP3, IMAP:** Email communication protocols.
- **ARP and ICMP:** Handle address resolution and error reporting.
- **FTP, HTTP, HTTPS:** File transfer and web browsing protocols.

# 8. Subnet and Subnetting

Subnetting is a technique used to divide a large network into smaller, more manageable sub-networks or subnets. It involves partitioning an IP network into subnets to improve network performance, security, and efficient IP address utilization. This technique is essential in both small and large-scale networks.

---

### 1. Introduction to Subnetting

### 1.1 Definition of Subnetting

Subnetting is the process of dividing a network into smaller subnetworks. A subnet is a logical subdivision of an IP network. Subnetting helps organize a network, reduces broadcast traffic, and improves security by isolating different sections of the network. Subnetting involves borrowing bits from the host portion of an IP address to create additional networks.

---

### 2. Why Do We Need Subnetting?

### 2.1 Efficient IP Address Usage

- IP addresses, especially IPv4 addresses, are limited. Subnetting helps ensure efficient allocation of these addresses.
- Without subnetting, an organization may waste large blocks of IP addresses, leaving them underutilized.

### 2.2 Network Organization

- Subnetting allows better network organization by grouping devices into logical segments (e.g., departmental or functional divisions), making management easier.

### 2.3 Security and Isolation

- Different subnets can be isolated for security purposes, ensuring that a compromised device in one subnet does not affect other parts of the network.

### 2.4 Reducing Broadcast Traffic

- When a network is subdivided into smaller subnets, broadcast traffic is limited to each subnet, which reduces the overall traffic on the entire network.

### 2.5 Scalability

- Subnetting allows the network to grow by creating more subnets as needed, facilitating network expansion.

## 3. Understanding IP Addressing and Subnet Masks

### 3.1 Components of an IP Address

An IP address consists of two parts:

- **Network Portion**: Identifies the network to which the device belongs.
- **Host Portion**: Identifies the specific device within that network.

The subnet mask is used to determine which part of the IP address corresponds to the network and which part corresponds to the host.

### 3.2 Subnet Mask

A subnet mask is a 32-bit number that is used to differentiate the network and host portions of an IP address. It consists of a series of 1's followed by 0's.

- The 1's represent the network portion.
- The 0's represent the host portion.

Example:

- **Subnet Mask (IPv4)**: 255.255.255.0 or /24 in CIDR notation (Classless Inter-Domain Routing)

## 4. CIDR Notation (Classless Inter-Domain Routing)

### 4.1 What is CIDR?

CIDR is a method used to allocate IP addresses more efficiently. It replaces the traditional class-based system (Class A, B, C, etc.) with a more flexible approach to subnetting.

CIDR notation specifies the network prefix by indicating the number of bits used for the network portion.

- For example, 192.168.1.0/24 means the first 24 bits are used for the network part, and the remaining 8 bits are for hosts.

## 5. Steps for Subnetting

### 5.1 Step 1: Identify the Network Address and Subnet Mask

- Identify the network address and its default subnet mask based on the class of the IP address (Class A, B, or C).
- Example: 192.168.1.0 with subnet mask 255.255.255.0.

### 5.2 Step 2: Determine the Number of Subnets Needed

- Decide how many subnets you need based on network requirements (e.g., for different departments or branches).

### 5.3 Step 3: Determine the Number of Host Bits to Borrow

- Calculate how many bits are needed to create the required number of subnets. You can use the formula:

2n≥required subnets2^n \geq \text{{required subnets}}2n≥required subnets
Where n is the number of bits borrowed from the host portion.

### 5.4 Step 4: Calculate New Subnet Mask

- Once you know how many bits to borrow, update the subnet mask. Add the borrowed bits to the original subnet mask.

### 5.5 Step 5: Calculate the Subnet Addresses

- List the range of addresses for each subnet, considering the subnet mask.

### 5.6 Step 6: Assign IP Addresses to Hosts

- Assign IP addresses within each subnet to individual devices, ensuring that you do not assign the network or broadcast address.

---

## 6. Subnetting Examples

### 6.1 Example 1: Subnetting Class C IP Address (192.168.1.0/24)

- **Objective:** Create 4 subnets.
- **Step 1:** Identify the class and default subnet mask:
  - Class C: 192.168.1.0, Subnet Mask: 255.255.255.0
- **Step 2:** Borrow 2 bits from the host portion.
  - 2^2 = 4 subnets
- **Step 3:** New subnet mask becomes 255.255.255.192 or /26.
  - Borrowing 2 bits gives 6 bits for hosts, which gives a maximum of 62 hosts per subnet.
- **Step 4:** Subnet Addresses:
  - Subnet 1: 192.168.1.0/26 (Range: 192.168.1.1 - 192.168.1.62)
  - Subnet 2: 192.168.1.64/26 (Range: 192.168.1.65 - 192.168.1.126)
  - Subnet 3: 192.168.1.128/26 (Range: 192.168.1.129 - 192.168.1.190)
  - Subnet 4: 192.168.1.192/26 (Range: 192.168.1.193 - 192.168.1.254)

---

### 6.2 Example 2: Subnetting Class B IP Address (172.16.0.0/16)

- **Objective:** Create 8 subnets.
- **Step 1:** Identify the class and default subnet mask:
  - Class B: 172.16.0.0, Subnet Mask: 255.255.0.0
- **Step 2:** Borrow 3 bits from the host portion.
  - 2^3 = 8 subnets
- **Step 3:** New subnet mask becomes 255.255.224.0 or /19.
  - Borrowing 3 bits gives 13 bits for hosts, allowing for 8190 hosts per subnet.
- **Step 4:** Subnet Addresses:
  - Subnet 1: 172.16.0.0/19 (Range: 172.16.0.1 - 172.16.31.254)

    - Subnet 2: 172.16.32.0/19 (Range: 172.16.32.1 - 172.16.63.254)
    - And so on...

---

### 6.3 Example 3: Subnetting Class A IP Address (10.0.0.0/8)

- **Objective:** Create 16 subnets.
- **Step 1:** Identify the class and default subnet mask:
    - Class A: 10.0.0.0, Subnet Mask: 255.0.0.0
- **Step 2:** Borrow 4 bits from the host portion.
    - 2^4 = 16 subnets
- **Step 3:** New subnet mask becomes 255.240.0.0 or /12.
- **Step 4:** Subnet Addresses:
    - Subnet 1: 10.0.0.0/12 (Range: 10.0.0.1 - 10.15.255.254)
    - Subnet 2: 10.16.0.0/12 (Range: 10.16.0.1 - 10.31.255.254)
    - And so on...