- **LAN (Local Area Network):**
    - A network confined to a small geographical area, such as a home, office, or building.
    - Typically connects computers, printers, and other devices within close proximity.
    - Operates using Ethernet, Wi-Fi, or both.
    - High-speed data transfer rates (typically 1 Gbps or more in modern networks).
- **WAN (Wide Area Network):**
    - A network that spans a large geographical area, often connecting multiple LANs.
    - Uses public networks like telephone lines, fiber-optic cables, or satellite connections.
    - Slower compared to LANs due to broader geographical coverage.
    - Examples: The Internet, corporate networks connecting offices in different cities or countries.

Key Features

- **LAN Features:**
    - Ownership: Typically owned and managed by a single organization or individual.
    - Setup Cost: Relatively low.
    - Security: Easier to secure due to limited access points.
    - Examples: Home networks, campus networks.
- **WAN Features:**
    - Ownership: Can involve multiple entities (ISPs, telecom providers, organizations).
    - Setup Cost: High, due to infrastructure needs.
    - Security: Challenging to secure due to broader access points.
    - Examples: Internet, enterprise WANs connecting international offices.

Applications

- **LAN:**
    - Sharing files and resources within an office.
    - Gaming and media streaming in homes.
- **WAN:**
    - Internet connectivity.
    - Corporate network connections for distributed offices.

Switch

- **Definition:**
  - A network device that connects devices within a LAN.
  - Operates at the Data Link Layer (Layer 2) of the OSI model but can also function at Layer 3.
- **Functions:**
  - Forwards data based on MAC addresses.
  - Creates a separate collision domain for each connected device.
  - Provides efficient data delivery by directing packets only to the intended device.
- **Types:**
  - Managed Switches: Allow configuration, monitoring, and management.
  - Unmanaged Switches: Plug-and-play devices with no configuration.
- **Applications:**
  - Used in LANs for connecting computers, printers, and servers.

Router

- **Definition:**
  - A network device that connects different networks (e.g., LAN to WAN).
  - Operates primarily at the Network Layer (Layer 3) of the OSI model.
- **Functions:**
  - Routes data packets based on IP addresses.
  - Enables communication between devices on different networks.
  - Provides Network Address Translation (NAT) for private to public IP translation.
- **Types:**
  - Wired Routers: Use cables for connections.
  - Wireless Routers: Include Wi-Fi for wireless connectivity.
- **Applications:**
  - Connects LANs to the Internet.
  - Facilitates communication between remote office networks.

IP Address (Internet Protocol Address)

- **Definition:**
  - A unique numerical identifier assigned to each device in a network to facilitate communication.
  - Acts as the address for sending and receiving data packets.
- **Format:**
  - Binary number written in human-readable formats like:
    - IPv4: 32-bit address, written as four decimal numbers separated by periods (e.g., 192.168.1.1).
    - IPv6: 128-bit address, written as eight groups of hexadecimal numbers separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Types of IP Addresses

1. **Based on Permanence:**
   - **Static IP Address:**
     - Manually assigned.
     - Permanent and does not change unless manually updated.
     - Suitable for servers, printers, and devices requiring constant access.
   - **Dynamic IP Address:**
     - Automatically assigned by DHCP.
     - Changes periodically.
     - Ideal for home networks and general use.
2. **Based on Accessibility:**
   - **Public IP Address:**
     - Globally unique and accessible over the Internet.
     - Assigned by Internet Service Providers (ISPs).
   - **Private IP Address:**
     - Used within private networks.
     - Not directly accessible from the Internet.
     - Examples: 192.168.x.x, 10.x.x.x.
3. **Based on Version:**
   - **IPv4:**
     - 32-bit address, offering approximately 4.3 billion unique addresses.
     - Example: 192.0.2.1.
   - **IPv6:**
     - 128-bit address, offering a vast address space.
     - Developed to overcome IPv4 exhaustion.
     - Example: 2001:0db8:0000:0000:0000:8a2e:0370:7334.

OSI Model

Definition:

The Open Systems Interconnection (OSI) Model is a conceptual framework that standardizes the functions of a networking system into seven distinct layers.

Developed by the International Organization for Standardization (ISO) in 1984.

Provides guidelines for how data is transmitted, received, and processed over a network.

The 7 Layers of the OSI Model

1. **Layer 1: Physical Layer**
    - **Function:**
        - Deals with the physical connection between devices.
        - Transmits raw binary data (0s and 1s) through cables, radio waves, or optical fibers.
    - **Devices:** Cables, switches, hubs, repeaters.
    - **Examples:** Ethernet, USB, Bluetooth.

2. **Layer 2: Data Link Layer**
    - **Function:**
        - Ensures error-free transmission of data by detecting and correcting errors in the Physical Layer.
        - Divided into two sublayers:
            - **Logical Link Control (LLC):** Manages communication between devices.
            - **Media Access Control (MAC):** Manages access to the physical medium.
    - **Devices:** Switches, network interface cards (NICs).
    - **Examples:** Ethernet (IEEE 802.3), Wi-Fi (IEEE 802.11).

3. **Layer 3: Network Layer**
    - **Function:**
        - Manages data routing, addressing, and delivery between devices on different networks.
        - Uses logical addressing like IP addresses.
    - **Devices:** Routers, Layer 3 switches.
    - **Examples:** IPv4, IPv6.

4. **Layer 4: Transport Layer**
    - **Function:**
        - Ensures reliable data transfer through error detection, flow control, and retransmission.
        - Protocols manage how data is segmented and reassembled.
    - **Protocols:** TCP (Transmission Control Protocol), UDP (User Datagram Protocol).
    - **Examples:** Email (SMTP), web browsing (HTTP/HTTPS).
5. **Layer 5: Session Layer**
    - **Function:**
        - Establishes, maintains, and terminates communication sessions between devices.
        - Manages dialog control and synchronization.
    - **Examples:** Remote Procedure Call (RPC), NetBIOS.
6. **Layer 6: Presentation Layer**
    - **Function:**
        - Translates data between application and network formats.
        - Manages encryption, compression, and data encoding.
    - **Examples:** SSL/TLS encryption, JPEG, PNG.
7. **Layer 7: Application Layer**
    - **Function:**
        - Provides network services directly to user applications.
        - Interfaces with software to facilitate network communication.
    - **Examples:** Web browsers, email clients, FTP software.

Importance of the OSI Model

- **Standardization:**
    - Helps different vendors' technologies to interoperate.
- **Troubleshooting:**
    - Provides a structured approach to diagnose network issues.
- **Flexibility:**
    - Enables scalability and integration of new technologies.
- **Layer Isolation:**
    - Changes in one layer do not affect others.

Real-World Example

When sending an email:

- **Application Layer:** User sends an email via SMTP.
- **Presentation Layer:** Data is encrypted with SSL/TLS.
- **Session Layer:** Session is established between sender and receiver.
- **Transport Layer:** TCP ensures reliable data transfer.
- **Network Layer:** Data is routed using IP addresses.
- **Data Link Layer:** Frames are sent to the receiver's MAC address.
- **Physical Layer:** Binary data is transmitted through the network medium.

Subnetting

Introduction

- **Definition:**
  - Subnetting is the process of dividing a larger network (IP address range) into smaller, more manageable subnetworks or subnets.
  - It improves network performance and security by segmenting traffic and reducing congestion.
- **Purpose:**
  - Efficient utilization of IP addresses.
  - Enhances network security by isolating subnet traffic.
  - Simplifies management of large networks.

Key Concepts in Subnetting

1. **Subnet Mask:**
   - A 32-bit number that determines how an IP address is divided into the network and host portions.
   - Example:
     - IP Address: 192.168.1.1
     - Subnet Mask: 255.255.255.0
2. **CIDR Notation (Classless Inter-Domain Routing):**
   - Denotes the number of bits used for the network portion.
   - Example: `/24` means the first 24 bits are used for the network.
3. **Subnet Address:**

    - The first IP address in a subnet, identifying the network.
    - Example: 192.168.1.0/24.
4. **Broadcast Address:**
    - The last IP address in a subnet, used to communicate with all devices in the subnet.
    - Example: 192.168.1.255/24.
5. **Host Range:**
    - All usable IP addresses between the subnet and broadcast addresses.
    - Example: 192.168.1.1 to 192.168.1.254 in a /24 subnet.

How Subnetting Works

- **Step 1: Identify the Network Requirements:**
    - Number of subnets needed.
    - Number of hosts per subnet.
- **Step 2: Calculate the Subnet Mask:**
    - Subtract the number of host bits from 32 (IPv4).
    - Example:
        - For 30 hosts, you need 5 bits (2^5 = 32 addresses).
        - Subnet mask: `/27` or 255.255.255.224.
- **Step 3: Allocate Subnets:**
    - Divide the IP range using the subnet mask.
    - Example: A /24 network (256 addresses) can be divided into eight /27 subnets, each with 32 addresses.

Benefits of Subnetting

- **Improved Security:**
    - Traffic within a subnet is isolated from other subnets.
- **Efficient IP Allocation:**
    - Prevents wastage of IP addresses.
- **Enhanced Network Performance:**
    - Reduces congestion by localizing traffic within subnets.
- **Simplified Troubleshooting:**
    - Smaller networks are easier to diagnose and manage.

Practical Example

- **Network:** 192.168.0.0/24 (256 IPs)
- **Requirement:** 4 subnets with equal hosts.

- **Solution:**
  - Subnet mask: /26 (64 IPs per subnet).
  - Subnets:
    - 192.168.0.0 - 192.168.0.63
    - 192.168.0.64 - 192.168.0.127
    - 192.168.0.128 - 192.168.0.191
    - 192.168.0.192 - 192.168.0.255

Topic: DNS Basics

- **Definition:**
  - DNS (Domain Name System) is a hierarchical naming system that translates human-readable domain names (e.g., www.example.com) into IP addresses (e.g., 192.168.1.1) that computers use to identify each other on the network.
- **Purpose:**
  - Simplifies internet navigation by replacing numeric IP addresses with easy-to-remember domain names.

Key Components of DNS

1. **Domain Name:**
   - The human-readable identifier for a resource, such as `example.com`.
2. **IP Address:**
   - The numerical address corresponding to a domain name.
3. **DNS Server:**
   - A server that resolves domain names to IP addresses.

How DNS Works

1. **User Request:**
   - A user enters a domain name in a browser (e.g., www.example.com).
2. **Recursive Resolver:**
   - The resolver queries DNS servers to resolve the domain into an IP address.
3. **Root DNS Servers:**
   - The query starts at a root server, which directs the resolver to the appropriate Top-Level Domain (TLD) server (e.g., .com, .org).
4. **TLD DNS Servers:**

    - Directs the query to the authoritative DNS server for the domain.
5. **Authoritative DNS Server:**
    - Returns the IP address associated with the domain name.
6. **Response:**
    - The resolver sends the IP address to the browser, which connects to the web server hosting the website.

Types of DNS Servers

1. **Recursive Resolver:**
    - Acts as an intermediary between the user and DNS hierarchy.
2. **Root Server:**
    - The top of the DNS hierarchy; contains information about TLD servers.
3. **TLD Server:**
    - Maintains information about domains under a specific TLD (e.g., .com, .net).
4. **Authoritative Server:**
    - Holds the definitive record for a specific domain.

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):**
    - Redirects one domain name to another.
- **MX Record (Mail Exchange):**
    - Specifies mail servers for a domain.
- **PTR Record (Pointer Record):**
    - Resolves an IP address to a domain name (reverse DNS lookup).

Common DNS Issues

- **DNS Propagation Delay:**
    - Changes in DNS records take time to propagate worldwide.
- **DNS Spoofing:**
    - Attackers modify DNS data to redirect users to malicious sites.
- **DNS Server Failure:**
    - Can result in websites being inaccessible.

DNS Security Measures

- **DNSSEC (DNS Security Extensions):**
  - Adds cryptographic signatures to DNS data to prevent tampering.
- **Firewall Rules:**
  - Restricts access to DNS servers to prevent unauthorized queries.
- **Regular Updates:**
  - Ensures DNS server software is up-to-date to prevent vulnerabilities.

.