



Network Fundamentals

Network Types

<b>PAN (Personal Area Network)</b>	Small network for personal devices, e.g., Bluetooth connection between a phone and headset.
<b>LAN (Local Area Network)</b>	Network within a limited area, such as a home, school, or office. Ethernet and Wi-Fi are common technologies.
<b>MAN (Metropolitan Area Network)</b>	Larger network spanning a city or metropolitan area. Connects multiple LANs together.
<b>WAN (Wide Area Network)</b>	Network covering a large geographical area, such as the internet. Connects multiple LANs and MANs.
<b>VLAN (Virtual LAN)</b>	Logically separate networks within a physical network. Improves security and network management.
<b>SAN (Storage Area Network)</b>	A dedicated high-speed network connecting servers to storage devices, providing block-level access to data.

Network Topologies

<b>Bus Topology</b>	All devices connected to a single cable. Simple but vulnerable; a break in the cable disrupts the entire network.
<b>Star Topology</b>	All devices connected to a central hub or switch. More robust than bus, but the central device is a single point of failure.
<b>Ring Topology</b>	Devices connected in a circular fashion. Data travels in one direction. Failure of one device can disrupt the network.
<b>Mesh Topology</b>	Each device is connected to multiple other devices. Highly redundant but expensive to implement.
<b>Tree Topology</b>	Combines features of bus and star topologies. Hierarchical structure.
<b>Hybrid Topology</b>	A combination of two or more different topologies. Offers flexibility and customization.

Key Networking Devices

<b>Hub</b>	Simple device that broadcasts data to all connected devices. Operates at Layer 1 (Physical Layer).
<b>Switch</b>	Forwards data only to the intended recipient based on MAC address. Operates at Layer 2 (Data Link Layer).
<b>Router</b>	Forwards data between different networks based on IP address. Operates at Layer 3 (Network Layer).
<b>Firewall</b>	Security device that controls network traffic based on predefined rules. Can operate at multiple layers.
<b>Wireless Access Point (WAP)</b>	Allows wireless devices to connect to a wired network. Typically operates at Layer 2.
<b>Load Balancer</b>	Distributes network traffic across multiple servers to optimize performance and availability.

OSI and TCP/IP Models

OSI Model Layers

<b>Layer 7: Application</b>	Provides network services to applications (e.g., HTTP, SMTP, FTP).
<b>Layer 6: Presentation</b>	Handles data formatting, encryption, and decryption.
<b>Layer 5: Session</b>	Manages connections between applications.
<b>Layer 4: Transport</b>	Provides reliable or unreliable data delivery (e.g., TCP, UDP).
<b>Layer 3: Network</b>	Handles routing of data packets (e.g., IP).
<b>Layer 2: Data Link</b>	Provides error-free transmission of data frames (e.g., Ethernet).
<b>Layer 1: Physical</b>	Defines physical characteristics of the network (e.g., cables, connectors).

TCP/IP Model Layers

<b>Layer 4: Application</b>	Combines the functions of the OSI Application, Presentation, and Session layers. (e.g., HTTP, SMTP, DNS).
<b>Layer 3: Transport</b>	Provides reliable or unreliable data delivery (e.g., TCP, UDP).
<b>Layer 2: Internet</b>	Handles routing of data packets (e.g., IP).
<b>Layer 1: Network Access</b>	Combines the functions of the OSI Data Link and Physical layers (e.g., Ethernet, Wi-Fi).

Key Differences

The OSI model is a conceptual model, while TCP/IP is a practical implementation. The OSI model has seven layers, while TCP/IP has four layers. TCP/IP is more widely used than the OSI model in real-world networks.
--

## IP Addressing and Subnetting

### IP Address Classes

<b>Class A</b>	1.0.0.0 - 126.0.0.0 Supports a large number of hosts (16,777,214) with few networks (126).
<b>Class B</b>	128.0.0.0 - 191.255.0.0 Supports a moderate number of networks (16,384) and hosts (65,534).
<b>Class C</b>	192.0.0.0 - 223.255.255.0 Supports a large number of networks (2,097,152) with few hosts (254).
<b>Class D</b>	224.0.0.0 - 239.255.255.255 Used for multicast addressing.
<b>Class E</b>	240.0.0.0 - 255.255.255.254 Reserved for experimental purposes.

### Private IP Addresses

<b>10.0.0.0 - 10.255.255.255</b> (10.0.0.0/8) <b>172.16.0.0 - 172.31.255.255</b> (172.16.0.0/12) <b>192.168.0.0 - 192.168.255.255</b> (192.168.0.0/16) Used for internal networks and are not routable on the public internet.
---

### Subnetting Basics

<b>Subnet Mask</b>	A 32-bit number that separates the network and host portions of an IP address. Indicates the number of bits used for the network address.
<b>CIDR Notation</b>	Shorthand representation of a subnet mask. <code>/n</code> indicates that the first <code>n</code> bits are used for the network address (e.g., <code>/24</code> represents a subnet mask of 255.255.255.0).
<b>Subnetting Process</b>	Involves borrowing bits from the host portion to create subnets. This allows a single network to be divided into smaller, more manageable networks.

## Common Networking Protocols

### Transport Layer Protocols

<b>TCP (Transmission Control Protocol)</b>	Connection-oriented protocol that provides reliable, ordered, and error-checked delivery of data. Used for applications like HTTP, SMTP, and FTP.
<b>UDP (User Datagram Protocol)</b>	Connectionless protocol that provides fast but unreliable delivery of data. Used for applications like DNS, VoIP, and streaming.

### Application Layer Protocols

<b>HTTP (Hypertext Transfer Protocol)</b>	Used for transferring web pages and other content between web servers and browsers. Port 80 (default).
<b>HTTPS (HTTP Secure)</b>	Secure version of HTTP that uses SSL/TLS encryption. Port 443 (default).
<b>DNS (Domain Name System)</b>	Translates domain names to IP addresses. Port 53 (default).
<b>SMTP (Simple Mail Transfer Protocol)</b>	Used for sending email. Port 25 (default).
<b>POP3 (Post Office Protocol version 3)</b>	Used for retrieving email from a mail server. Port 110 (default).
<b>IMAP (Internet Message Access Protocol)</b>	Used for retrieving and managing email on a mail server. Port 143 (default).
<b>FTP (File Transfer Protocol)</b>	Used for transferring files between computers. Ports 20 and 21 (default).
<b>SSH (Secure Shell)</b>	Used for secure remote access to a computer. Port 22 (default).