IP Address: A unique identifier assigned to each device on a network, allowing devices to communicate with one another. It can be IPv4 (e.g., 192.168.1.1) or IPv6 (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Router: A device that routes data packets between different networks, directing traffic from local networks (like a home network) to external networks, including the internet.

Switch: A networking device that connects devices within a local network, such as computers and printers, and forwards data to the correct device based on MAC addresses.

DNS (Domain Name System): A system that translates human-readable domain names (like www.example.com) into machine-readable IP addresses, enabling browsers to find websites on the internet.

DHCP (Dynamic Host Configuration Protocol): A protocol used to automatically assign IP addresses to devices on a network, simplifying network management by dynamically allocating addresses as needed.

LAN (Local Area Network): A network that connects devices within a limited geographical area, such as within a home, office, or building.

WAN (Wide Area Network): A network that connects devices over large geographical areas, such as between cities or countries, and is typically used to describe the internet.

MAC Address (Media Access Control Address): A unique identifier assigned to the network interface of a device, used for communication on the local network and ensuring data is delivered to the correct device.

Firewall: A security system designed to monitor and control incoming and outgoing network traffic based on predefined security rules, helping protect networks from unauthorized access.

VPN (Virtual Private Network): A service that creates a secure, encrypted connection over a public network (like the internet), allowing users to send and receive data as if they were on a private network.

Bandwidth: The maximum rate at which data can be transmitted over a network connection, usually measured in megabits per second (Mbps) or gigabits per second (Gbps).

Ping: A command-line utility used to test the reachability of a device on a network and measure the round-trip time it takes for a message to travel to the destination and back.

Throughput: The actual amount of data transmitted over a network in a given period of time, which may be lower than the bandwidth due to factors like congestion or latency.

Subnet: A smaller network created by dividing a larger network into more manageable segments. Subnetting improves network performance and security.

NAT (Network Address Translation): A method used in routers to translate private IP addresses within a local network to a single public IP address for communication over the internet.

QoS (Quality of Service): A technique used to manage and prioritize network traffic, ensuring that critical applications (e.g., video calls or VoIP) get the necessary bandwidth and performance for smooth operation.

SSID (Service Set Identifier): The name assigned to a wireless network, used by devices to identify and connect to that specific network.

TCP/IP (Transmission Control Protocol/Internet Protocol): A set of communication protocols that govern how data is transmitted and routed over the internet. TCP ensures data is correctly transmitted, while IP handles the addressing and routing.

Ping of Death: A type of network attack where oversized or malformed packets are sent to a target device, potentially causing it to crash or malfunction due to buffer overflow.

OSI Model (Open Systems Interconnection Model): A conceptual framework used to understand how different network protocols and services work. It divides network communication into seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.