Network Terminologies

1.) IP Address (Internet Protocol Address)

- A unique string of numbers identifying each device on a network.
- IPv4 addresses consist of four decimal numbers separated by dots (e.g., 192.168.1.1).
- IPv6 addresses use a hexadecimal format, allowing for more unique addresses (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
- Used to route data packets to the correct destination on a network.
- Essential for devices to communicate over the Internet and local networks.

2.) MAC Address (Media Access Control Address)

- A unique identifier assigned to network interfaces for communications within a network segment.
- Typically formatted as six groups of two hexadecimal digits, separated by hyphens or colons (e.g., 00:1A:2B:3C:4D:5E).
- Used within the local network to ensure that data packets are delivered to the correct device.
- Hardcoded into the network interface card (NIC) and generally not changeable.
- Plays a crucial role in network security and device identification.

3.) Router

- A networking device that forwards data packets between computer networks.
- Directs traffic on the Internet by connecting different networks (e.g., LANs, WANs, ISP networks).
- Uses IP addresses to determine the best path for data packets to travel.
- Can provide additional functions like network address translation (NAT) and dynamic host configuration protocol (DHCP).
- Essential for creating larger and more complex network architectures.

4.) DNS (Domain Name System)

- A hierarchical system that translates human-readable domain names into IP addresses.
- Enables users to access websites and services using easily remembered names (e.g., www.example.com).
- Consists of distributed databases maintained by various organizations.
- DNS servers perform the lookup process to find the IP address associated with a domain name.
- Fundamental for the operation of the Internet, allowing seamless access to online resources.

5.) Firewall

- A network security device that monitors and controls incoming and outgoing traffic based on security rules.
- Establishes a barrier between a trusted internal network and an untrusted external network (e.g., the Internet).
- Can be hardware-based, software-based, or a combination of both.
- Protects networks from unauthorized access, malware, and cyberattacks.
- Often includes features like packet filtering, stateful inspection, and virtual private network (VPN) support.