# Computer Networking Glossary

## Computer Networking

Connecting computers and devices to share resources and data.

## IP Address

A unique number given to a device for communication in a network.

## IPv4 vs IPv6

IPv4 uses 32-bit addresses (like 192.168.1.1). IPv6 uses 128-bit addresses (like 2001:db8::1).

## Public vs Private IP

Public IP is reachable over the internet. Private IP is used only in local networks.

## Subnet Mask

A number that separates the network and device portions of an IP.

## MAC Address

A unique hardware ID for a network card.

## DNS

Domain Name System — changes names like google.com into IP numbers.

## DHCP

Dynamic Host Configuration Protocol — automatically gives IP addresses.

## TCP vs UDP

TCP is reliable and slow. UDP is fast but not always reliable.

## HTTP vs HTTPS

HTTPS is HTTP plus encryption for security.

## FTP

File Transfer Protocol — moves files between computers.

## SMTP

Simple Mail Transfer Protocol — sends emails.

## IMAP vs POP3

IMAP keeps emails on the server. POP3 downloads and removes them.

## Firewall

A security tool that filters network traffic.

## Proxy Server

A middleman between you and the internet.

## NAT

Network Address Translation — lets many devices share one public IP.

## VPN

Virtual Private Network — encrypts traffic for security.

## Ping

A tool to check if a device is online.

## Traceroute

Shows the path data takes to reach a target.

## Bandwidth

The maximum data transfer rate.

## Latency

The delay before data moves.

## Jitter

Variation in delay.

## Packet Loss

When packets fail to reach the destination.

## Port Number

A number identifying a service (e.g., 80 for web).

## OSI Model

7-layer framework to understand networks.

## TCP/IP Model

4-layer real-world model of networking.

## ARP

Maps IP to MAC addresses.

## ICMP

Protocol used by ping and traceroute.

## SSL/TLS

Protocols for secure communication.

## WebSocket

Keeps a constant connection between client and server.

## REST API

Uses HTTP/HTTPS for communication.

## MQTT

Lightweight protocol for IoT devices.

## SNMP

Manages network devices.

## Unicast/Multicast/Broadcast

One-to-one, one-to-many, one-to-all communication.

## VLAN

Virtual Local Area Network — splits a network.

## QoS

Quality of Service — gives priority to some traffic.

## Load Balancing

Shares traffic across servers.

## Failover

Switches to backup if main fails.

## CDN

Content Delivery Network — caches content near users.

## Packet Sniffer

Tool to capture network traffic (e.g., Wireshark).

## Socket

An endpoint for sending or receiving data.

## DNS Caching

Stores DNS lookups for speed.

## Reverse DNS

Finds domain from IP.

## TCP Handshake

Steps to start a connection (SYN → SYN-ACK → ACK).

## MTU

Maximum Transmission Unit — largest allowed packet size.

## Fragmentation

Splitting packets into smaller ones.

## Keep-Alive

Signal to keep a connection open.

## Stateful vs Stateless

Stateful keeps session info (TCP). Stateless does not (HTTP).

## Proxy vs Reverse Proxy

Proxy sits between client and server. Reverse proxy distributes traffic to servers.

## Honeypot

Fake system to trick attackers.

## DDoS

Distributed Denial of Service — attack flooding traffic.

## Compression

Reduces data size (like GZIP).

## HTTP/2 vs HTTP/1.1

HTTP/2 is faster with multiplexing.

## QUIC

New faster protocol by Google.

## TLS Handshake

Process to set up secure HTTPS.

## Sticky Session

Keeps user on the same server.

## Deep Packet Inspection

Looks inside packets for analysis.

## Anycast IP

Same IP on many servers, routes to closest.

## Zero Trust

Security model — never trust, always verify.

## Binary

Base-2 system (0 and 1).

## Hexadecimal

Base-16 system (0–9, A–F).

## ASCII

Maps characters to numbers in binary.

## Unicode

Standard for representing characters in all languages.

## Bit Rate

Bits per second transmitted.

## Baud Rate

Signal changes per second.

## Bit vs Byte

1 byte = 8 bits.

## Nibble

4 bits (half a byte).

## NIC

Network Interface Card — connects device to network.

## Switch

Connects multiple devices in a LAN.

## Hub

Basic device sending data to all ports.

## Router

Connects different networks.

## Modem

Converts digital data to signals for internet.

## Access Point

Extends wireless coverage.

## PoE

Power over Ethernet — carries power and data in one cable.

## Loopback Address

127.0.0.1 — test your own device.

## Packet

A small unit of network data.

## Encapsulation

Wrapping data with headers before sending.

## Decapsulation

Removing headers at destination.

## Frame

Packet at the Data Link layer.

## RARP

Reverse ARP — maps MAC to IP.

## DHCP Lease

Time an IP is assigned before renewal.

## TTL

Time To Live — limits packet lifetime.

## DNS Propagation

Time for DNS changes to spread.

## NAT Loopback

Accessing public IP from inside same network.

## VLAN Trunking

Carrying multiple VLANs on one link.

## IGMP

Manages multicast groups.

## Network Segmentation

Splits network for security.

## SSL Offloading

Moves encryption work from server to another device.

## IPsec

Protocol suite to secure IP.

## MPLS

Fast routing technique.

## Default Gateway

Router that forwards traffic outside.

## Static vs Dynamic IP

Static = manual. Dynamic = automatic.

## Broadcast Domain

Area where broadcasts reach all.

## Collision Domain

Area where devices share bandwidth.

## Half vs Full Duplex

Half = one way. Full = both ways at once.

## Patch Cable

Short Ethernet cable.

## Crossover Cable

Cable with reversed wiring to connect similar devices.

## Ethernet Speeds

10 Mbps, 100 Mbps, 1 Gbps.

## PoE Switch

Switch that delivers power via Ethernet.

## Throughput

Actual speed achieved.

## Topology

Layout of a network (star, mesh, etc.).

## Star Topology

All devices connect to central hub/switch.

## Mesh Topology

Devices connect to many others for redundancy.

## Choke Point

Bottleneck slowing traffic.

## DNS Spoofing

Fake DNS replies to mislead users.

## ARP Spoofing

Fake ARP messages to redirect traffic.

## Packet Fragmentation

Breaking packets into smaller ones.

## IPv6 Compression

Shortening long IPv6 addresses.

## Socket Timeout

Maximum wait before failure.

## Captive Portal

Login page before using public Wi-Fi.

## Network Loop

When packets loop endlessly.