Networking Fundamentals Cheatsheet

A comprehensive cheat sheet covering essential networking concepts, protocols, and tools. Ideal for students, network administrators, and software developers looking to grasp the fundamentals of computer networks.

Network Fundamentals

Network Types

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

Network Topologies

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

Key Networking Devices

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

OSI and TCP/IP Models

OSI Model Layers

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

TCP/IP Model Layers

Layer 4: Application	Combines the functions of the OSI Application, Presentation, and Session layers. (e.g., HTTP, SMTP, DNS).
Layer 3: Transport	Provides reliable or unreliable data delivery (e.g., TCP, UDP).
Layer 2: Internet	Handles routing of data packets (e.g., IP).
Layer 1: Network Access	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

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

Private IP Addresses

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

Subnetting Basics

Subnet Mask	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.
CIDR Notation	Shorthand representation of a subnet mask. `/n` indicates that the first `n` bits are used for the network address (e.g., `/24` represents a subnet mask of 255.255.255.0).
Subnetting Process	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

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

Application Layer Protocols

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