Networking & Administration Cheatsheet

A comprehensive cheat sheet covering essential networking and system administration concepts, commands, and configurations.

Networking Fundamentals

OSI Model

Layer 7: Application	Provides network services to applications. (e.g., HTTP, SMTP, DNS)
Layer 6: Presentation	Deals with data representation, encryption, and decryption. (e.g., SSL/TLS)
Layer 5: Session	Manages connections between applications. (e.g., session establishment, termination)
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, MAC addresses)
Layer 1: Physical	Deals with physical transmission of data. (e.g., cables, connectors)

Common Protocols

TCP	Transmission Control Protocol - Reliable, connection-oriented protocol.
UDP	User Datagram Protocol - Unreliable, connectionless protocol.
IP	Internet Protocol - Responsible for addressing and routing packets.
HTTP	Hypertext Transfer Protocol - Used for web communication.
HTTPS	HTTP Secure - Secure web communication using SSL/TLS.
DNS	Domain Name System - Translates domain names to IP addresses.
DHCP	Dynamic Host Configuration Protocol - Automatically assigns IP addresses to devices.

IP Addressing

IP addresses are logical addresses assigned to network interfaces.

IPv4: 32-bit address (e.g., 192.168.1.1)
IPv6: 128-bit address (e.g., 2001:db8::1)

Subnet Mask: Used to determine the network and host portions of an IP address. (e.g., 255.255.255.0)

CIDR Notation: Represents the subnet mask as a suffix to the IP address. (e.g., 192.168.1.0/24)

Private IP Addresses: Used within private networks (e.g., 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)

Public IP Addresses: Used on the internet and are globally routable.

System Administration Basics

User Management (Linux)

`useradd <username>`	Create a new user account.
`passwd <username>`	Set or change the password for a user.
`userdel <username>`	Delete a user account.
`usermod`	Modify a user account
`groupadd <groupname>`	Create a new group.
`groupdel <groupname>`	Delete a group.
`gpasswd -a <username> <groupname>`	Add a user to a group.
`id <username>`	Display user identity (UID, GID, groups).

File Permissions (Linux)

File permissions control access to files and directories.

Permissions: `r` (read), `w` (write), `x` (execute)
Users: `u` (user), `g` (group), `o` (others)

`chmod <permissions> <file>` - Change file permissions.

Example: `chmod 755 myfile.sh` (rwxr-xr-x)

`chown <user>:<group> <file>` - Change file ownership.

`ls -l` - List files with detailed permissions.

Process Management (Linux)

`ps`	Display running processes.
`top`	Display real-time system resource usage.
`kill <PID>`	Terminate a process by its PID.
`pkill <processname>`	Terminate a process by name.
`bg`	Move a process to the background.
`fg`	Move a process to the foreground.
`nohup <command> &`	Run a command that persists after logout.

Network Configuration

ifconfig/ip (Linux)

`ifconfig` (deprecated)	Display network interface configuration.
`ip addr show`	Display network interface addresses.
`ip link show`	Display network interface link status.
`ip route show`	Display routing table.
`ip addr add <ip>/<cidr> dev <interface>`	Add an IP address to an interface.
`ip link set dev <interface> up`	Enable a network interface.
`ip link set dev <interface> down`	Disable a network interface.

netstat/ss

`netstat -tulnp` (deprecated)	Display listening TCP and UDP ports.
`ss -tulnp`	Display listening TCP and UDP ports (using `ss`).
`netstat -rn` (deprecated)	Display routing table.
`ss -s`	Display network statistics.

Firewall (iptables/firewalld)

iptables (legacy):

`iptables -L` - List firewall rules.

`iptables -A INPUT -p tcp --dport 22 -j ACCEPT` - Allow SSH traffic.

`iptables -P INPUT DROP` - Set default policy to drop incoming traffic.

firewalld (modern):

`firewall-cmd --state` - Check firewall status.

`firewall-cmd --zone=public --add-port=80/tcp --permanent` - Allow HTTP traffic.

`firewall-cmd --reload` - Apply changes.

Troubleshooting

Network Troubleshooting

`ping <host>`	Check network connectivity to a host.
`traceroute <host>`	Trace the route packets take to reach a host.
`nslookup <domain>`	Query DNS servers to resolve domain names.
`tcpdump -i <interface> <filter>`	Capture and analyze network traffic.
`wireshark`	Graphical network protocol analyzer.
`mtr <host>`	Combines ping and traceroute functionality.

System Troubleshooting

`dmesg`	Display kernel messages (useful for hardware issues).
`journalctl`	Query systemd journal logs.
`free -m`	Display memory usage.
`df -h`	Display disk space usage.
`uptime`	Show system uptime and load averages.
`vmstat`	Report virtual memory statistics.

Log Analysis

Log files provide valuable information for troubleshooting and security analysis.

Common Log Locations (Linux):

`/var/log/syslog` or `/var/log/messages` - System logs

`/var/log/auth.log` - Authentication logs

`/var/log/apache2/` or `/var/log/nginx/` - Web server logs

`grep <pattern> <logfile>` - Search for specific patterns in log files.

`tail -f <logfile>` - Monitor a log file in real-time.

`awk` and `sed` - Powerful text processing tools for log analysis.