

## Explore any 10 networking commands

### 1. ping

- **Usage:** `ping [hostname or IP address]`
- **Description:** Sends ICMP echo requests to check if a host is reachable. It helps diagnose network connectivity issues by measuring the response time between the source and destination.

### 2. ifconfig

- **Usage:** `ifconfig [interface]`
- **Description:** Displays or configures network interfaces. Commonly used to check the IP address, subnet mask, and status of network interfaces.

### 3. ip

- **Usage:** `ip addr show, ip route show, ip link show`
- **Description:** A powerful tool for network management, allowing configuration and display of IP addresses, routes, and network interfaces. It's a modern replacement for `ifconfig`.

### 4. netstat

- **Usage:** `netstat -an, netstat -rn`
- **Description:** Shows network connections, routing tables, and interface statistics. It helps identify open ports, active connections, and routing information.

### 5. traceroute

- **Usage:** `traceroute [hostname or IP address]`
- **Description:** Tracks the path packets take to reach a host, showing each hop and the delay between them. Useful for diagnosing where delays or connection issues occur.

### 6. nslookup

- **Usage:** `nslookup [domain name]`
- **Description:** Queries DNS to get the IP address associated with a domain name. Useful for diagnosing DNS-related issues or verifying DNS configuration.

### 7. dig

- **Usage:** `dig [domain name]`
- **Description:** Retrieves DNS information, similar to `nslookup` but provides more detailed output. It can display different record types like A, MX, TXT, and more.

### 8. arp

- **Usage:** `arp -a`
- **Description:** Displays or modifies the ARP (Address Resolution Protocol) table, which maps IP addresses to MAC addresses on a local network. It's useful for troubleshooting local network issues.

## 9. `tcpdump`

- **Usage:** `tcpdump -i [interface]`
- **Description:** Captures network packets on a specified interface for detailed analysis. Useful for diagnosing network issues, analyzing traffic, and detecting intrusions.

## 10. `ss`

- **Usage:** `ss -tuln`
- **Description:** Displays socket statistics, similar to `netstat`, but faster and with more features. Commonly used to view active connections and open ports.