# Lab 2: Introduction to Basic Networking Tools and Commands

## Objective:

To become familiar with key networking tools and commands used for troubleshooting issues, diagnosing problems, and managing network settings.

## Theory:

### Networking commands play a crucial role in helping users and administrators maintain and troubleshoot computer networks. These tools are used to inspect network configurations, test connectivity, manage settings, and monitor data flow across networks. Whether it's identifying IP-related issues, checking server availability, or managing routing paths, these commands assist in locating and resolving faults effectively. By learning how to use such commands, one can gain better control over network behavior and ensure smoother communication between devices

### .ipconfig / ifconfig

**Purpose:** Display IP address and other important network configuration details.

* **ipconfig** – used in Windows systems
* **ifconfig** – used in Linux and macOS
* **Use Case:** These commands help users view their device's current network setup, including IP address, subnet mask, and default gateway. This information is essential for troubleshooting connectivity problems and verifying proper network settings.

A screenshot of a computer code

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

### 2.ping

**Purpose**: Test if another device is reachable

* Example: ping google.com

**Use Case:** The ping command sends ICMP echo request packets to a specified address (like a website or IP) and waits for a reply. It helps verify if the destination is active and reachable. This command is useful for checking internet connectivity, diagnosing network delays, or confirming whether a remote server is up and responsive.

A white screen with black numbers and numbers

AI-generated content may be incorrect.

### 3. tracert / traceroute

* **Purpose:** See the path data takes through the network.
* tracert – Windows
* traceroute – Linux/macOS
* **Use Case:** These commands display the route that packets follow to reach a destination by showing each hop along the path. This helps identify where delays or failures occur in the network, making it useful for troubleshooting slow connections or pinpointing network issues.  
  **Example:** tracert google.com

A screenshot of a computer

AI-generated content may be incorrect.

### 4.netstat

**Purpose:** View active network connections and open ports.

**Use Case:** The netstat command displays all current network connections along with the ports that are being used or are listening for incoming connections. This information is valuable for diagnosing issues related to server ports, monitoring network activity, and identifying unauthorized connections.

**Example:** netstat -an

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

### 5.nslookup

**Purpose:** Check DNS (Domain Name System) resolution.

**Use Case:** The nslookup command is used to query DNS servers and convert domain names into their corresponding IP addresses. It helps troubleshoot DNS-related problems by verifying if a domain name is properly resolved.  
**Example:** nslookup google.com

A white screen with black text

AI-generated content may be incorrect.

### 6.arp

**Purpose:** Show the mapping between IP addresses and MAC addresses.

**Use Case:** The arp command displays the local network’s Address Resolution Protocol table, listing IP addresses along with their corresponding MAC addresses. This helps in identifying devices on the local network and troubleshooting address resolution issues.  
**Example:** arp -a

A computer code with numbers and letters

AI-generated content may be incorrect.

**7.hostname**

**Purpose:** Shows the computer’s name on the network

* **Example:** hostname

It is used for identifying the system on the network.



**8. Telnet**  
**Purpose:** Used to test if a specific port on a remote host is open and accepting connections.

* **Example:** telnet google.com 80
* **Use Case:** Helpful for checking connectivity to services running on specific ports, such as web servers (port 80). However, Telnet is often disabled or blocked by default due to security concerns.



A screenshot of a computer

AI-generated content may be incorrect.

Conclusion:

This lab offered practical experience with key networking commands, helping to build a stronger grasp of how networks operate. By applying these tools in real scenarios, it became clearer how they contribute to keeping networks stable and functional. These commands are crucial for monitoring, identifying, and resolving network problems, making them essential for effective network management and support.