**TROUBELSHOOTING**

These tools are crucial for network troubleshooting and diagnosing connectivity issues in a Linux environment. They provide insights into network performance, routing, and DNS resolution, enabling administrators to identify and resolve problems efficiently.

* ***ifconfig Command:***

**Purpose:**

Display or configure network interface parameters.

**Usage:**

ifconfig [interface] [options]

**Examples:**

ifconfig eth0

**Notes:**

ifconfig shows information about all network interfaces by default.

Use it to configure network interfaces, set IP addresses, enable or disable interfaces, and more.

* ***ping Command:***

**Purpose:**

Test network connectivity by sending ICMP echo requests to a host.

**Usage:**

ping [options] hostname\_or\_IP

**Examples:**

ping google.com or ping 192.168.1.1

**Notes:**

ping is a basic tool to check if a host is reachable and estimate round-trip time.

Common options include -c (specifying the number of packets) and -i (setting the interval between packets).

* ***traceroute Command:***

**Purpose:**

Trace the route that packets take to reach a destination.

**Usage:**

traceroute [options] hostname\_or\_IP

**Examples:**

traceroute google.com or traceroute 192.168.1.1

**Notes:**

traceroute displays the IP addresses and round-trip times of packets as they traverse through routers to reach the destination.

Helpful for diagnosing network routing issues.

* ***DNS Troubleshooting Tools:***

1. ***dig (Domain Information Groper):***

**Purpose:**

Query DNS servers for information.

**Usage:**

dig [options] [domain] [query\_type]

**Example:**

dig google.com A

**Notes:**

dig is a powerful DNS diagnostic tool that provides detailed information about DNS queries, including the IP addresses associated with a domain.

1. ***nslookup:***

**Purpose:**

Query DNS servers interactively.

**Usage:**

nslookup [domain] [server]

**Example:**

nslookup google.com

**Notes:**

nslookup allows for interactive querying of DNS servers, providing information about domain names and their corresponding IP addresses.

1. ***host:***

**Purpose:**

Obtain DNS information about a domain.

**Usage:**

host [options] [domain]

**Example:**

host google.com

**Notes:**

host is a simple command to look up DNS information, including IP addresses and domain name aliases.

1. ***tcpdump:***

**Purpose:**

Capture and analyze network traffic.

**Usage:**

tcpdump [options] [expression]

**Example**:

tcpdump -i eth0 port 53

**Notes:**

tcpdump can be used to capture DNS traffic, allowing analysis of DNS queries and responses for troubleshooting purposes.