**Assignment 6:**

# **MTMC-509 Programming Lab-I**

### **Basic Network Commands and Advanced Networking Commands**

**Networks Commands**

 **Listing Network Interfaces and IP Addresses**

* Use the ip addr show command to list the IP addresses and network interfaces on your system.
* Use the ifconfig command to display the IP addresses of all network interfaces. Compare the output of ip addr show with ifconfig. What differences do you observe?

 **Assigning an IP Address**

* Use the ip address add [IP\_address] dev eth0 command to assign a new IP address (e.g., 192.168.1.100/24) to the eth0 network interface. Replace [IP\_address] with the desired IP address.
* Verify the new IP address has been added using the ip addr show or ifconfig command.

 **Pinging a Remote Host**

* Use the ping [remote\_host] command (replace [remote\_host] with a domain such as google.com) to check if the host is reachable. Record the average round-trip time (RTT) for the packets.

 **Viewing Active Ports**

* Use the netstat -pnltu command to view active (listening) ports on your system. Which ports are currently listening for incoming connections?
* Use the netstat -tuln command to view TCP and UDP ports and their associated programs. Identify any significant services running on your system based on their ports.

 **Domain Information Using whois**

* Use the whois [domain\_name] command (replace [domain\_name] with a domain such as example.com) to retrieve detailed information about the domain, such as the registrar, registration date, and expiration date.
* Summarize the key details about the domain, including the registrar and registration status.

 **Performing DNS Lookups with dig**

* Use the dig [domain\_name] command to retrieve DNS information for a specific domain (replace [domain\_name] with a domain such as example.com). What are the primary DNS servers for the domain?
* Perform a reverse DNS lookup for an IP address using the dig -x [IP\_address] command. What information does the reverse DNS lookup reveal about the IP address?

 **Using host to Perform an IP Lookup**

* Use the host [domain\_name] command to perform an IP lookup for a domain. Record the IP addresses associated with the domain name.
* Compare the results of the host command with those of the dig command from earlier. Are the IP addresses consistent between the two commands?

 **Retrieving Local IP Address**

* Use the hostname -I command to display the local IP address of your system. Verify this by comparing it with the output of the ip addr show or ifconfig command.

 **DNS Lookup with nslookup**

* Use the nslookup [domain\_name] command to receive detailed information about a domain (replace [domain\_name] with a domain such as example.com).
* Compare the output of nslookup with the output of dig. Which command provides more detailed DNS information, and why might you use one over the other?

.

### **Other Useful Networking Commands**

1. **ip link show**
   * Display network interfaces and their status (up/down).
   * Example: ip link show
2. **ip route show**
   * Show the routing table for your system, including default gateways and routes.
   * Example: ip route show
3. **ifup / ifdown**
   * Bring a network interface up or down manually.
   * Example: sudo ifup eth0
   * Example: sudo ifdown eth0
4. **ss**
   * View socket statistics. A modern replacement for netstat.
   * Example: ss -tuln (List all listening TCP and UDP ports)
5. **traceroute [host]**
   * Trace the path packets take to reach a remote host.
   * Example: traceroute google.com
6. **mtr [host]**
   * A network diagnostic tool combining ping and traceroute for continuous analysis.
   * Example: mtr google.com
7. **nmap [options] [target]**
   * Network exploration and security auditing tool, useful for discovering hosts and services on a network.
   * Example: nmap -sP 192.168.1.0/24 (Ping scan a subnet)
8. **ip neigh show**
   * Show the ARP (Address Resolution Protocol) table for the system.
   * Example: ip neigh show
9. **tcpdump**
   * Capture and display packet traffic on a network interface.
   * Example: sudo tcpdump -i eth0
10. **ethtool [interface]**

* Display or modify the network interface settings, such as speed and duplex mode.
* Example: ethtool eth0

1. **curl [URL]**

* Transfer data from or to a server, commonly used for testing HTTP connections and APIs.
* Example: curl http://example.com

1. **wget [URL]**

* Retrieve files from the web, can download single or multiple files.
* Example: wget http://example.com/file.zip

1. **nmcli**

* Command-line tool to control NetworkManager, useful for managing network connections.
* Example: nmcli device show

1. **iwconfig**

* Configure wireless network interfaces and view their status.
* Example: iwconfig

1. **route**

* Show or modify the system's IP routing table.
* Example: route -n

1. **nc (Netcat)**

* Networking utility for reading/writing to network connections. Often used for port scanning, sending files, or testing services.
* Example: nc -zv 192.168.1.1 80 (Check if port 80 is open)

1. **arp**

* Display or modify the ARP cache, useful for diagnosing ARP issues.
* Example: arp -a

1. **iperf3**

* Network testing tool that measures bandwidth, delay, and packet loss.
* Example: iperf3 -c 192.168.1.1 (Run a bandwidth test to a remote host)

1. **ping6 [host]**

* Same as ping but used for testing connectivity with IPv6 hosts.
* Example: ping6 ipv6.google.com