**Batch: B2 Roll No.: 16014022050**

**Experiment No.: 1**

**Grade: AA / AB / BB / BC / CC / CD / DD**

**Signature of the staff in-charge with date**

Ccff

**Experiment No.: 2**

|  |
| --- |
| **TITLE:** Study of basic network administration commands and network configuration. |

**AIM:** Study networking commands –ping, traceroute, nslookup, arp, rarp, netstat, telnet.

**Expected Outcome of Experiment:**

**CO1:** Understand the fundamentals of network administration.

**Books / Journals / Websites Referred:**

1. *Linux Lab - Open source Technology : Ambavade –Dreamtech*
2. <http://manpages.ubuntu.com/manpages/trusty/man8/rarp.8.html>
3. <http://computernetworkingnotes.com/comptia-n-plus-study-guide/network-tool-command.html>

**Pre Lab / Prior Concepts:** Computer network

**New concepts to be learned:** Command line operation to handle networks.

**Theory**

Computers are connected in a network to exchange information or resources each other. Two or more computer connected through network media called computer network. There are number of network devices or media are involved to form computer network. Computer loaded with Windows and Linux Operating System can also be a part of network whether it is small or large network by its multitasking and multiuser natures. Maintaining of system and network up and running is a task of System / Network Administrator’s job.

Frequently used network configuration and troubleshoot commands in Linux/Windows are as follows:

1. **IFCONFIG/ IPCONFIG**

ifconfig (interface configurator) command is use to initialize an interface, assign IP Address to interface and enable or disable interface on demand. With this command you can view IP Address and Hardware / MAC address assign to interface and also MTU (Maximum transmission unit) size.

ifconfig with interface (eth0) command only shows specific interface details like IP Address, MAC Address etc. with -a options will display all available interface details if it is disable also.

Syntax: # ifconfig eth0

**To enable** or **disable** specific Interface, we use example command as follows.

Enable eth0: # ifup eth0

Disable eth0: # ifdown eth0

To Setting MTU Size:

By default, MTU size is 1500. We can set required MTU size with below command.

Replace XXXX with size.

Syntax: # ifconfig eth0 mtu XXXX

Set Interface in Promiscuous mode.

Network interface only received packets belongs to that particular NIC. If you put interface in promiscuous mode, it will receive all the packets. This is very useful to capture packets and analyse later. For this you may require superuser access.

Syntax: # ifconfig eth0 – promisc

1. **PING**

PING (Packet INternet Groper) command is the best way to test connectivity between two nodes. Whether it is Local Area Network (LAN) or Wide Area Network (WAN). Ping use ICMP (Internet Control Message Protocol) to communicate to other devices.

It verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) Echo Request messages. The receipt of corresponding Echo Reply messages are displayed, along with round-trip times. Ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution.

ping [-c count] [-i wait] [-l preload][-s packetsize] host

-c count

Stop after sending (and receiving) count ECHO\_RESPONSE packets.

-i wait

Wait wait seconds between sending each packet. The default is to

wait for one second between each packet. This option is

incompatible with the -f option.

-l preload

If preload is specified, ping sends that many packets as fast as

possible before falling into its normal mode of behavior.

-s packetsize

Specifies the number of data bytes to be sent. The default is

56, which translates into 64 ICMP data bytes when combined with

the 8 bytes of ICMP header data.

PING Command Example:

# ping 4.2.2.2

# ping -c 5 [www.tecmint.com](http://www.tecmint.com)

1. **TRACEROUTE/ TRACERT**

traceroute is a network troubleshooting utility which shows number of hops taken to reach destination also determine packets traveling path. Below we are tracing route to global DNS server IP Address and able to reach destination also shows path of that packet is traveling.

Syntax:

tracert [-d] [-h MaximumHops] [-j HostList] [-w Timeout] [TargetName]

Parameters

**-d:** Prevents tracert from attempting to resolve the IP addresses of intermediate routers to their names. This can speed up the display of tracert results.

**-h:** MaximumHops Specifies the maximum number of hops in the path to search for the target (destination). The default is 30 hops.

**-j:** HostList Specifies that Echo Request messages use the Loose Source Route option in the IP header with the set of intermediate destinations specified in HostListThe HostList is a series of IP addresses (in dotted decimal notation) separated by spaces.

**-w:** Timeout Specifies the amount of time in milliseconds to wait for the ICMP Time Exceeded or Echo Reply message corresponding to a given Echo Request message to be received. If not received within the time-out, an asterisk (\*) is displayed. The default time-out is 4000 (4 seconds).

1. **NETSTAT command**

Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols).

Netstat provides statistics for the following:

**Proto** **-** The name of the protocol (TCP or UDP).

**Local Address -** The IP address of the local computer and the port number being used. The name of the local computer that corresponds to the IP address and the name of the port is shown unless the -n parameter is specified. If the port is not yet established, the port number is shown as an asterisk (\*).

**Foreign Address -** The IP address and port number of the remote computer to which the socket is connected. The names that correspond to the IP address and the port are shown unless the -n parameter is specified. If the port is not yet established, the port number is shown as an asterisk (\*).

(state) Indicates the state of a TCP connection. The possible states are as follows:

CLOSE\_WAIT

CLOSED

ESTABLISHED

FIN\_WAIT\_1

FIN\_WAIT\_2

LAST\_ACK

LISTEN

SYN\_RECEIVED

SYN\_SEND

TIMED\_WAIT

Syntax:

netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]

Parameters

Used without parameters, netstat displays active TCP connections.

**-a** Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.

**-e** Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with -s.

**-n** Displays active TCP connections, however, addresses and port numbers are expressed numerically, and no attempt is made to determine names.

**-o** Displays active TCP connections and includes the process ID (PID) for each connection.

**-p** Shows connections for the protocol specified by Protocol.

**-s** Displays statistics by protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols. If the IPv6 protocol for Windows XP is installed, statistics are shown for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The -p parameter can be used to specify a set of protocols.

**-r** Displays the contents of the IP routing table.

Netstat (Network Statistic) command display connection info, routing table information etc. To displays routing table information use option as -r.

# netstat –r

1. **DIG**

Dig (domain information groper) query DNS related information like a record, CNAME, MX Record etc. This command mainly uses to troubleshoot DNS related query.

# dig [www.Ipadress.com](http://www.Ipadress.com)

1. **NSLOOKUP**

The name "nslookup" means "name server lookup". nslookup is a network administration command-line tool available for many computer operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record. It displays information from Domain Name System (DNS) name servers.

nslookup command also use to find out DNS related query.

**Example:**

C:\Documents and Settings\sysadm>nslookup itu.dk

Server:  ns3.inet.tele.dk

Address:  193.162.153.164

**Non-authoritative answer:**

Name: itu.dk

Address: 130.226.133.2

# nslookup www.Googel.com

1. **ROUTE**

Route command also shows and manipulate ip routing table. To see default routing table in Linux, type the following command.

# route

1. **ARP**

When we need an Ethernet (MAC) address we can use arp(address resolution protocol). In other words it shows the physical address of an host.

Syntax

**arp [-a [InetAddr] [-N IfaceAddr]] [-g [InetAddr] [-N IfaceAddr]] [-d InetAddr [IfaceAddr]] [-s InetAddr EtherAddr [IfaceAddr]]**

Parameters

Used without parameters, ping displays help.

**-a** [InetAddr] [-N IfaceAddr] Displays current ARP cache tables for all interfaces.

**-g** [InetAddr] [-N IfaceAddr] Identical to -a.

**-d** InetAddr [IfaceAddr] Deletes an entry with a specific IP address, where InetAddr is the IP address.

**-s** InetAddr EtherAddr [IfaceAddr] Adds a static entry to the ARP cache that resolves the IP address InetAddr to the physical address EtherAddr.

To add a static ARP cache entry to the table for a specific interface, use the IfaceAddr parameter where IfaceAddr is an IP address assigned to the interface ARP (Address Resolution Protocol) is useful to view / add the contents of the kernel’s ARP tables. To see default table use the command as.

# arp -e

Address HWtype HWaddress Flags Mask Iface

192.168.50.1 ether 00:50:56:c0:00:08 C eth0

1. **ETHTOOL**

ethtool is a replacement of mii-tool. It is to view, setting speed and duplex of your Network Interface Card (NIC). You can set duplex permanently in /etc/sysconfig/network-scripts/ifcfg-eth0 with ETHTOOL\_OPTS variable.

Syntax: # ethtool eth0

1. **TELNET**

The telnet command is used to communicate with another host using the TELNET protocol. If telnet is invoked without the host argument, it enters command mode, indicated by its prompt (telnet>) In this mode, it accepts and executes the commands listed below. If it is invoked with arguments, it performs an open command with those arguments.

To login to a remote machine, use this syntax:

**% telnet <hostname>**

The options are as follows:

-8 Specifies an 8-bit data path. This causes an attempt to negotiate the TELNET BINARY option on both input and output.

-E Stops any character from being recognized as an escape character.

-K Specifies no automatic login to the remote system.

1. **HOSTNAME**

hostname is to identify in a network. Execute hostname command to see the hostname of your box. You can set hostname permanently in /etc/sysconfig/network. Need to reboot box once set a proper hostname.

# hostname

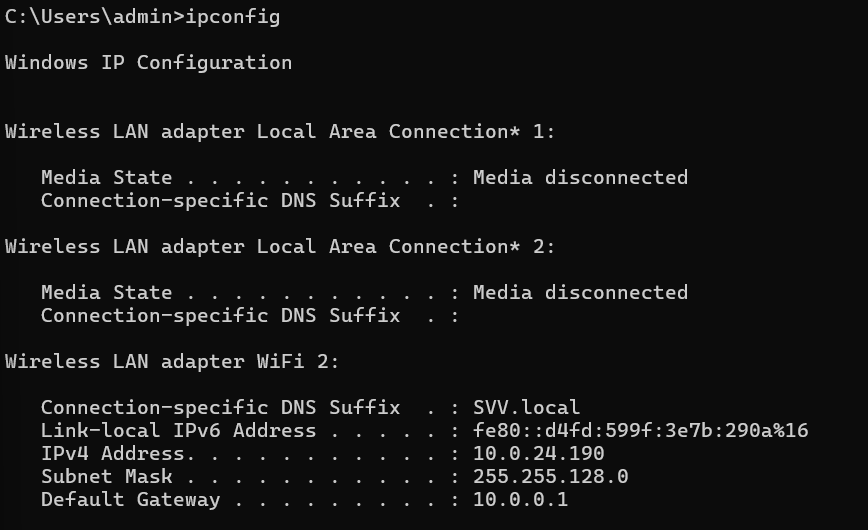
1. **SYSTEMINFO**

Display information about a system.

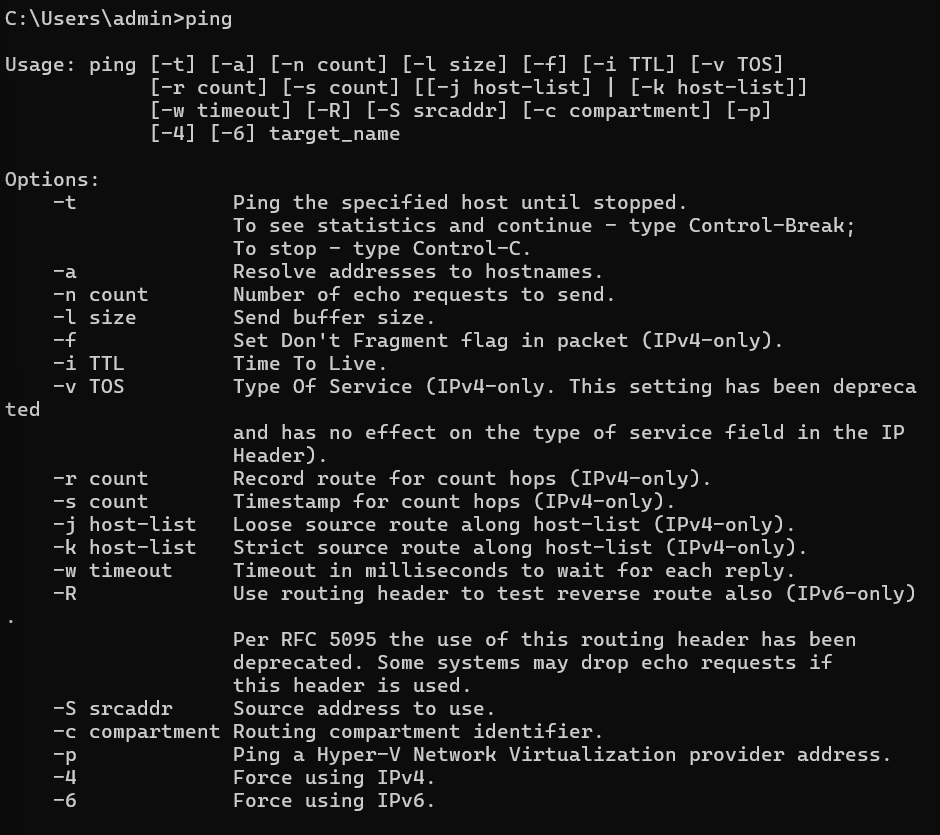
**Implementation**

Show the use of different network commands.

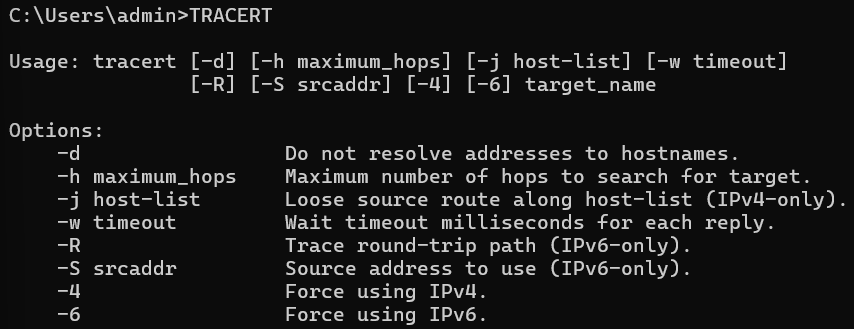
**ipconfig**



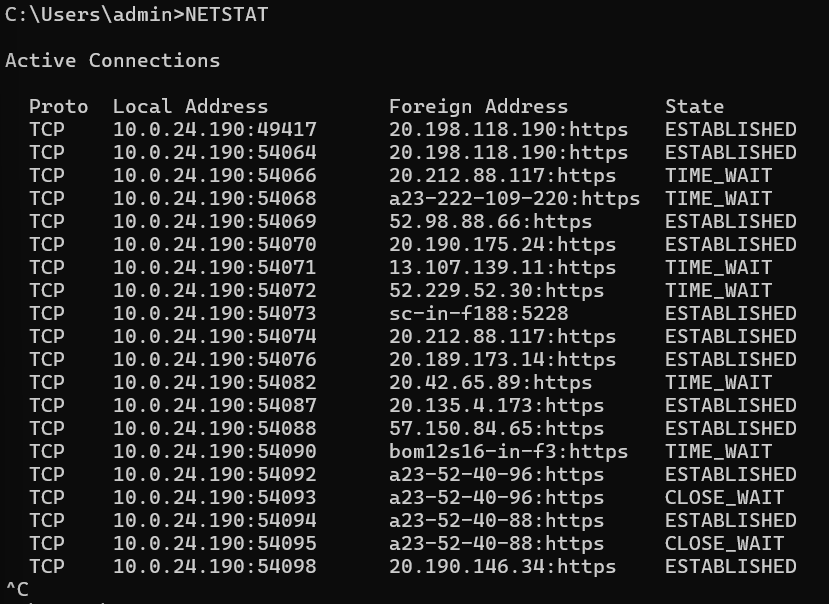
**ping**



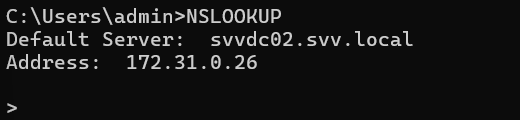
**tracert**

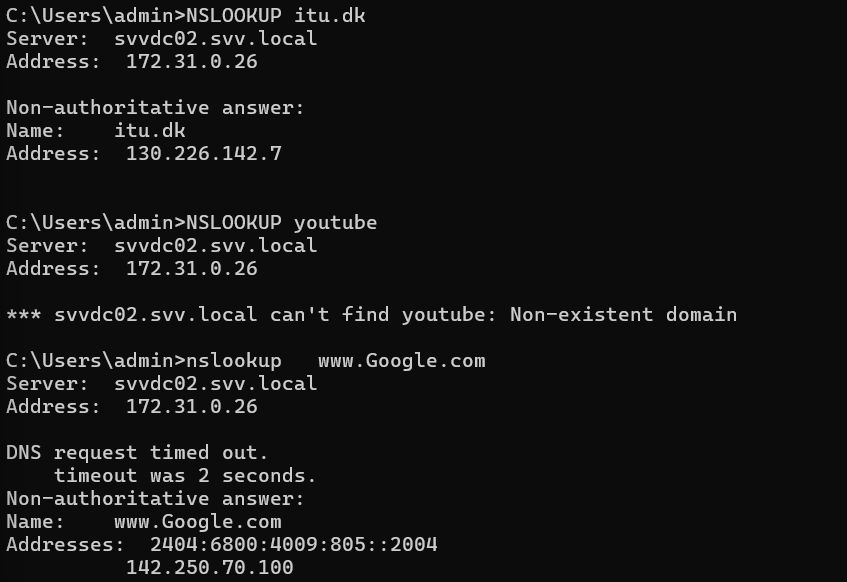


**netstat**



**nslookup**

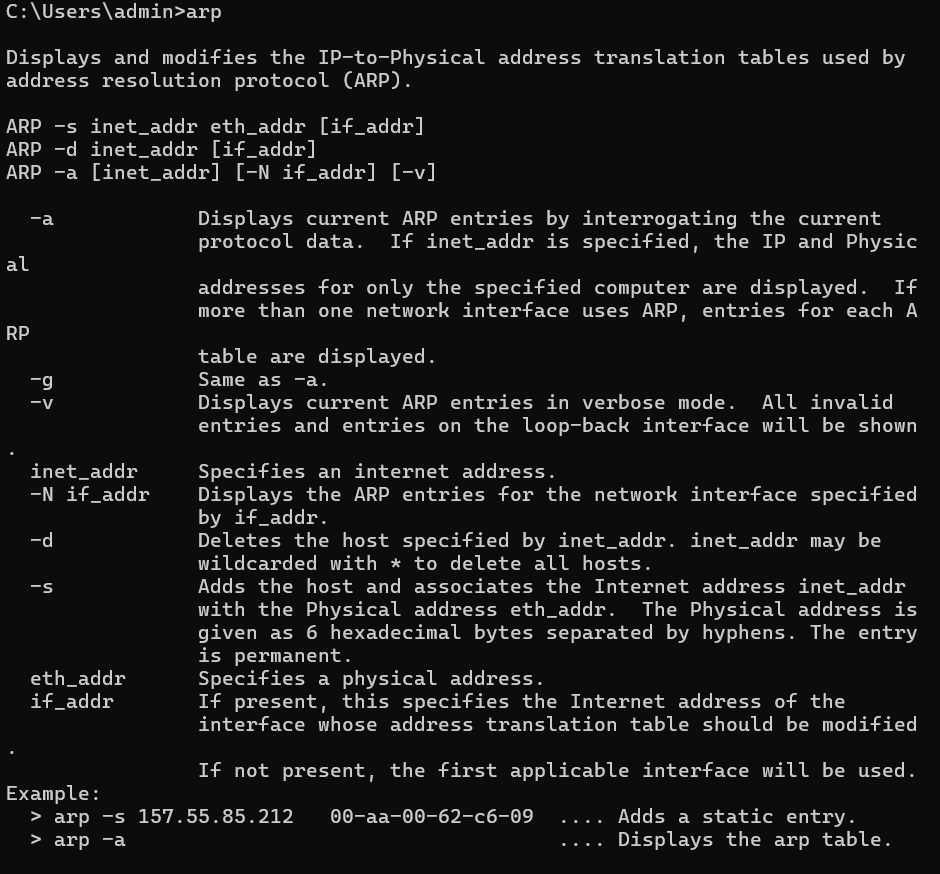




**route**



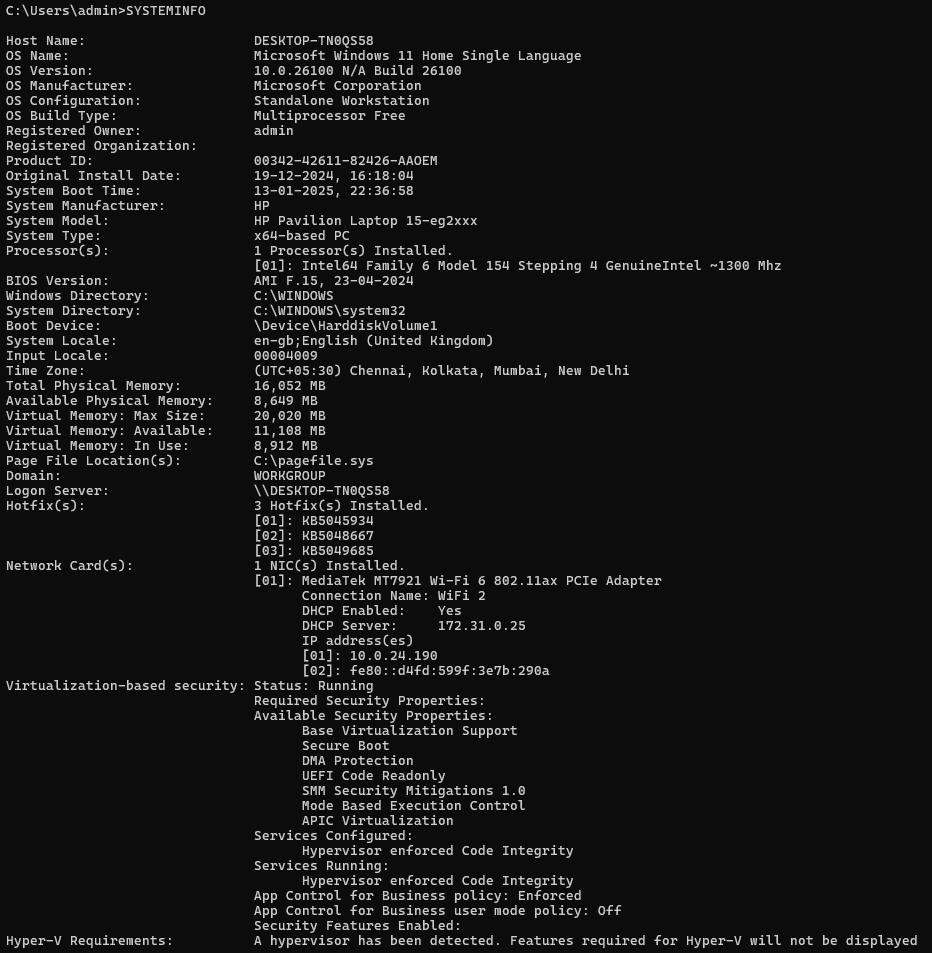
**arp**



**hostname**



**systeminfo**



**Conclusion:**

In this experiment, we explored various networking commands to analyze and troubleshoot network configurations and connectivity

like ping, ifconfig, and others, highlighting their functionality and limitations in different environments.

**Post Lab Questions:**

1. **Give details of minimum 5 commands which is not included in the write-up.**

WHOIS

* whois is used to query information about a domain name or IP address from a WHOIS database. It retrieves details like the domain registrar, registration dates, owner information, and DNS records.
* Syntax: whois <domain-name>

IP

* ip is a modern replacement for the ifconfig command. It provides more detailed control over network interfaces, IP addresses, and routing tables.
* Syntax: ip <command> <options>

TCPDUMP

* tcpdump is a packet analyzer used to capture and display network traffic. It is highly useful for troubleshooting network issues and analyzing data packets.
* Syntax: tcpdump [options] [filter]

NMAP

* nmap (Network Mapper) is a powerful tool for network scanning and security auditing. It can discover hosts, services, and vulnerabilities on a network.
* Syntax: nmap [options] <target>

IWCONFIG

* iwconfig is a command-line tool for configuring wireless network interfaces. It allows you to set parameters like SSID, mode, and frequency.
* Syntax: iwconfig <interface> [options]

1. **Give the reason why some commands are not working in the Lab.**

TRACEROUTE

* The traceroute or tracert command requires administrative privileges or root access to execute properly on most systems.
* Labs often operate in a restricted environment where permissions for network utilities are limited to prevent unauthorized use or accidental network disruptions.
* The tool also sends ICMP or UDP packets, which might be blocked by firewall rules configured by the university to maintain security.

DIG

* The dig command might not be installed by default on the lab machines. It is part of the BIND utilities, which may not be included in minimal installations of Linux or Windows systems.
* Alternatively, DNS-related queries might be restricted by the lab network policy to prevent misuse or external DNS lookups for security reasons.

ETHTOOL

* ethtool requires administrative/root privileges to access and modify network interface configurations. If you didn’t run the command with sudo or similar privilege escalation, it wouldn’t work.
* Some systems may not have ethtool installed, as it is specific to Linux systems and not commonly pre-installed on all distributions.
* Lab systems might restrict low-level network interface modifications to avoid interfering with network setups.

TELNET

* The telnet protocol is considered insecure as it transmits data (including passwords) in plaintext. Many modern systems and networks, especially in secure environments like university labs, disable Telnet in favor of more secure protocols like SSH.
* The Telnet client might not be installed on lab machines, as it is deprecated in many operating systems by default.
* The lab firewall or network policy might block Telnet traffic on port 23 to prevent unauthorized access or hacking attempts.