**Batch: D - 1 Roll No.: 16010122096**

**Experiment / assignment / tutorial No. 02**

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

**Signature of the Staff In-charge with date**

**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:**

1. 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.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

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

**2. 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

**3. 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).

4. **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

**5. 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

**6. 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

**7. ROUTE**

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

# route

**8. 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

**9 . 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

10. **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.

**11. 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

**12. SYSTEMINFO**

**Display information about a system.**

**IMPLEMENTATION:**

**Show the use of different network commands:**

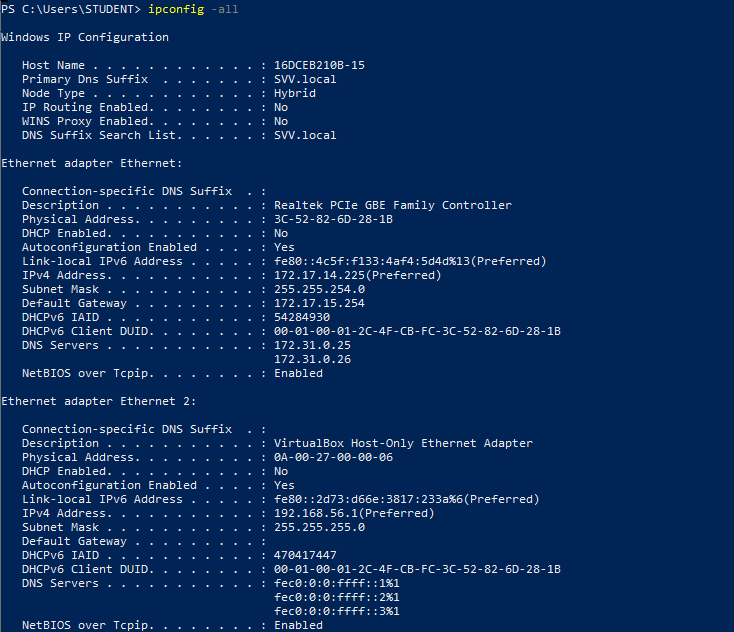
1] **ipconfig**

**ipconfig** is a command-line utility in Windows that displays the network configuration of the currently connected network interfaces. It is used to manage the IP addresses assigned to network devices.

**ipconfig /all** provides a comprehensive overview of all network interfaces on a Windows machine. The information displayed includes:

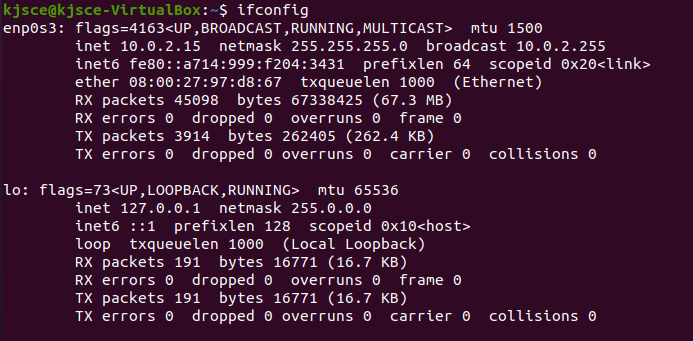
* Hostname
* Primary DNS suffix
* Node type
* IP routing enabled status
* WINS proxy enabled status
* Detailed adapter information (e.g., Ethernet adapter, Wireless adapter), which includes:
  + Description
  + Physical (MAC) address
  + DHCP enabled status
  + Autoconfiguration enabled status
  + IPv4 address
  + Subnet mask
  + Lease obtained and lease expires times
  + Default gateway
  + DHCP server
  + DNS servers

This command is especially useful for troubleshooting network issues, as it provides a complete snapshot of the network configuration.



**Ifconfig**

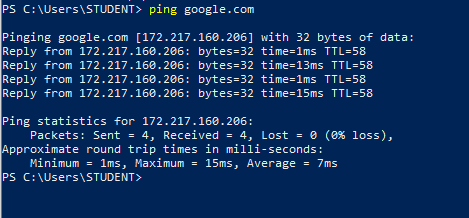
**ifconfig** is a command-line utility in Unix-like operating systems (Linux, macOS, BSD) used to configure, control, and query TCP/IP network interface parameters.



2] **ping**

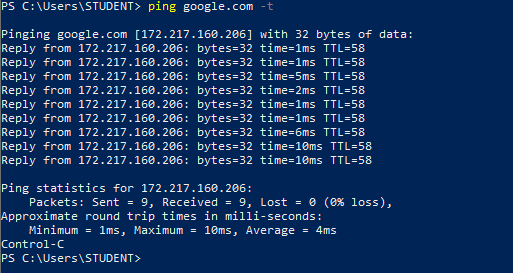
**ping** is a command-line utility used to test the reachability of a host on an Internet Protocol (IP) network. It works by sending Internet Control Message Protocol (ICMP) Echo Request messages to the target host and waits for Echo Reply messages. The primary purpose of the **ping** command is to diagnose connectivity issues and measure round-trip time (RTT).

**ping [hostname/IP address]**: Sends a series of ICMP Echo Request messages to the specified host and displays the replies.



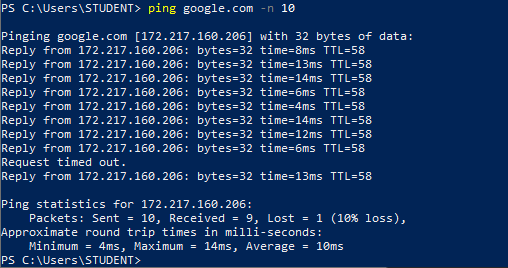
**ping -t** is used in Windows to continuously ping the specified host until the command is manually stopped (usually with Ctrl+C). This can be useful for monitoring the network connection over an extended period.

This command will keep sending ICMP Echo Request messages to google.com indefinitely until you interrupt it.



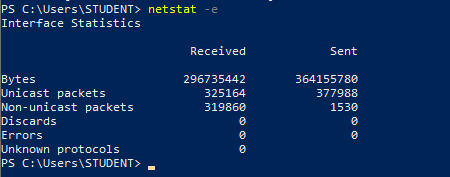
**ping -n 10** is used in Windows to send a specific number of ICMP Echo Request messages to the specified host. In this case, it will send 10 pings and then stop.

This command will send exactly 10 ICMP Echo Request messages to google.com and display the results.

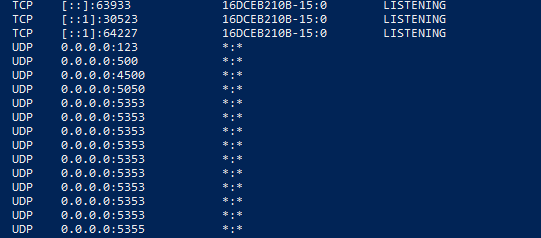
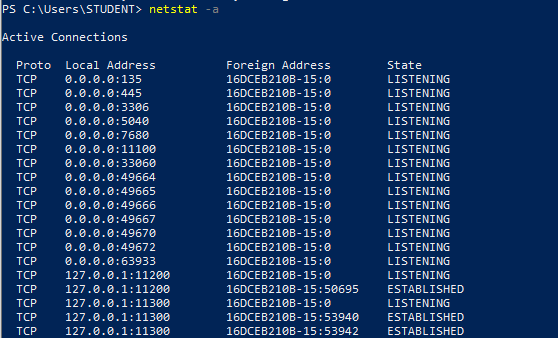


3] **netstat**

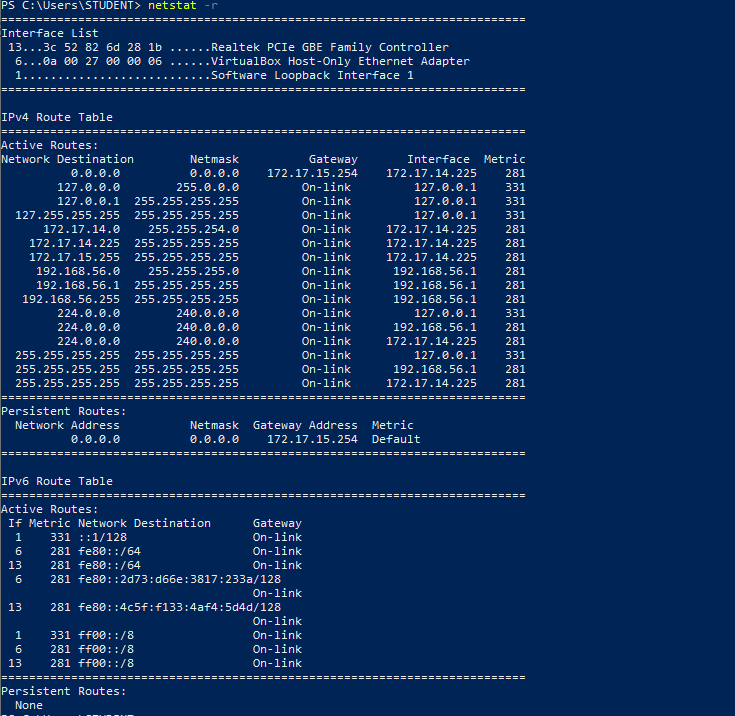
**netstat** (network statistics) is a command-line tool that displays network connections (both incoming and outgoing), routing tables, interface statistics, masquerade connections, and multicast memberships. It is available on Unix-like operating systems and Windows.

**netstat -e** displays Ethernet statistics, such as the number of bytes and packets sent and received, errors, and other detailed information about the network interfaces.

**netstat -a** displays all active connections and listening ports. This includes TCP and UDP connections, as well as the ports on which the computer is listening for incoming connections.



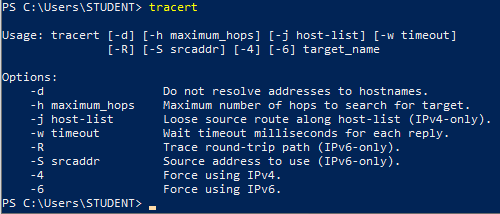
**netstat -r** displays the routing table, which shows the paths that network traffic takes to reach its destination. This includes the network destination, netmask, gateway, interface, and metric.



4] **tracert**

**tracert** (trace route) is a command-line utility in Windows that tracks the path packets take from one computer to another. It shows the route (path) and measures transit delays of packets across an IP network.

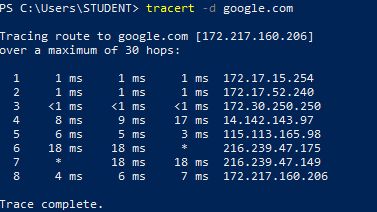
tracert without any arguments will provide you with the syntax and available options for the command, helping you understand how to use it effectively. It does not perform any trace route action by itself but instead acts as a guide for using the command.



**tracert [hostname/IP address]**: Traces the route to the specified host and displays each hop along the path. It helps identify where delays or failures occur in the network.



**tracert -d** is used to trace the route to the specified host without resolving IP addresses to hostnames. This can speed up the process since it skips DNS lookups.



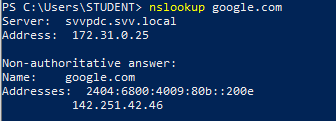
5] **nslookup**

**nslookup** is a command-line utility used for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record.

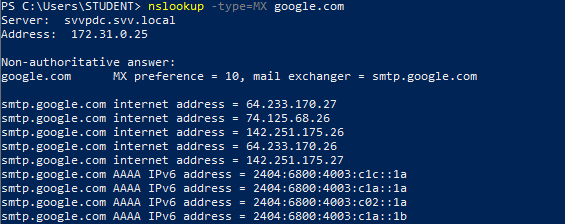
**nslookup**: Starts the nslookup interactive mode, where you can enter additional commands to query the DNS.

https://lh7-rt.googleusercontent.com/docsz/AD_4nXeOTpiutZXsGR6BWWNO2INTYjDSwDa7AXfFeWCW7jID59sozpw1ckOcaxt-4YlW3wMH87YWl4oTrVkcSvPe3eUDAJg64_mEdzfzh_oMzCBnS2epnNjy-oJ0yI7LCUUQ2i6PJtjktSzpWQ0wSEZVH0IGIqyz?key=KsE3YnGu7qcQZRfILHRKgA

When you use nslookup followed by a hostname (or an IP address), it performs a DNS lookup for that specific hostname or IP address, displaying the corresponding IP address or hostname.

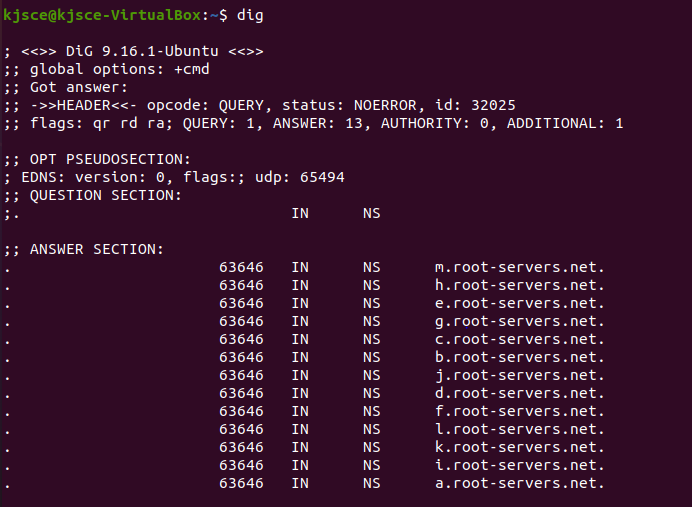


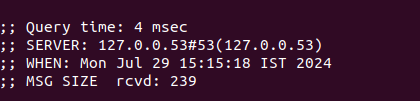
**nslookup -type=MX** specifies that you want to query the Mail Exchange (MX) records for the specified hostname. MX records are used to identify the mail servers responsible for receiving email on behalf of a domain.



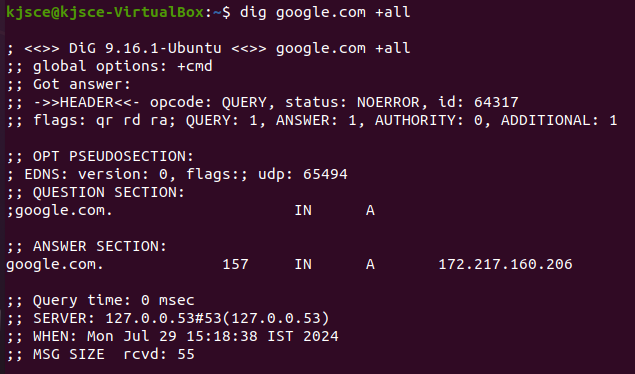
6] **dig**

**dig** (Domain Information Groper) is a command-line tool for querying DNS name servers. It is used to retrieve DNS records for a given domain name. dig is available on Unix-like operating systems





**dig [hostname] +all** provides detailed information about the DNS query process and the records returned. The +all option requests all possible output, giving you a comprehensive view of the DNS response.



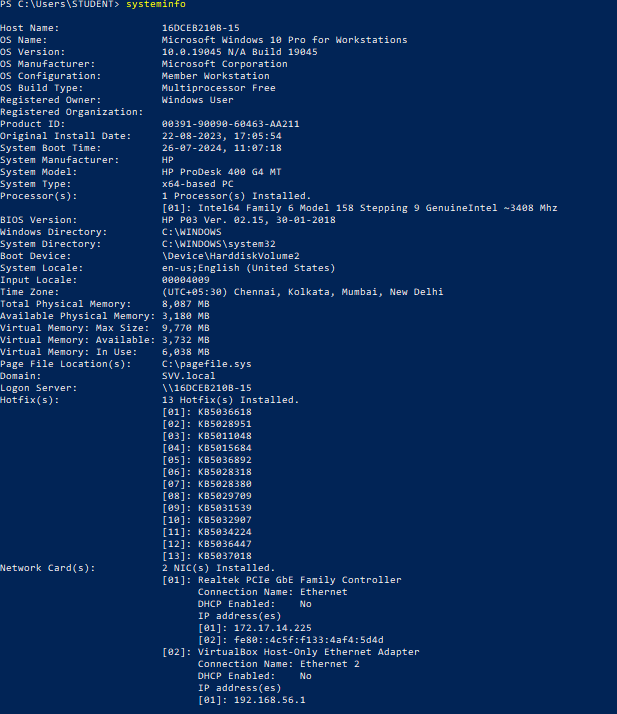
7] **hostname**

hostname command without any arguments displays the current hostname of the system.

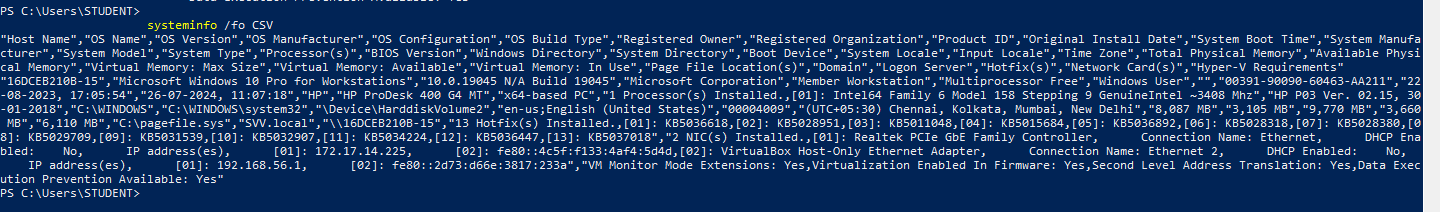
https://lh7-rt.googleusercontent.com/docsz/AD_4nXfJBhH7QfqZF2z_wWeQgCpbL7SFVPRD7lH9qg7xxBGf7BMk2A9zSAoVLuqfk5OcqKGd88cjYjwvNUHjFw_19pd_58HM_epBxpusFlSUoZWfkz9tmICIleo0uieTscJj-Rl0dWkBlB2YKFK6VLFX8jC4aYnD?key=KsE3YnGu7qcQZRfILHRKgA

8] **systeminfo**

systeminfo command without any arguments displays a comprehensive list of system configuration information.

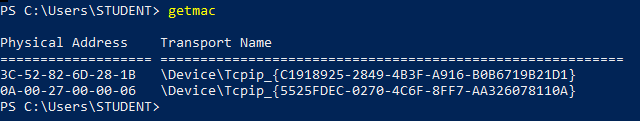


The systeminfo /fo csv command formats the output as comma-separated values (CSV). This can be useful for importing the data into a spreadsheet or for further processing.



9] **getmac**

**getmac** is a command-line utility used to display the Media Access Control (MAC) addresses for network adapters on a system. This is useful for identifying the hardware addresses of network interfaces.

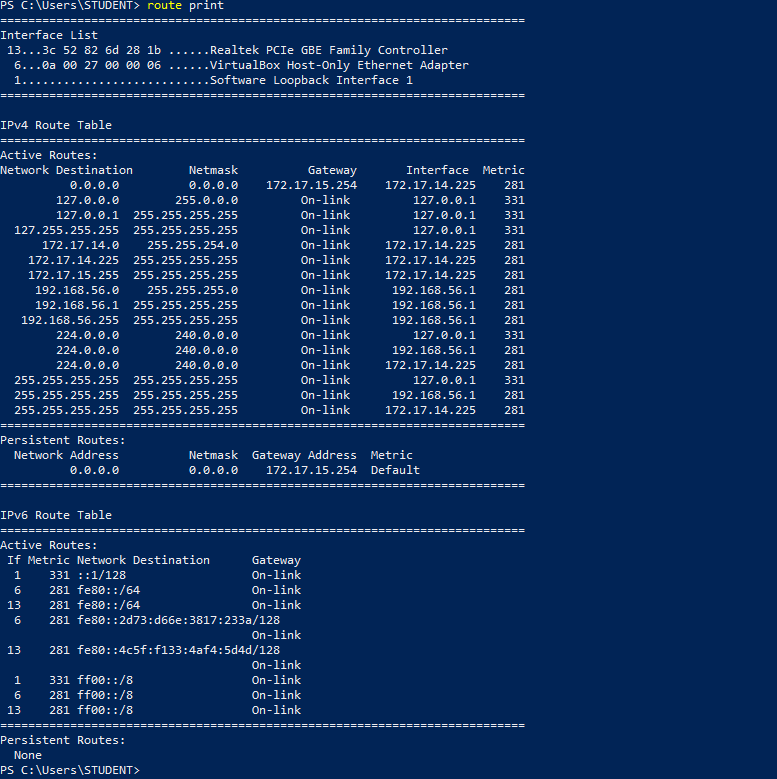


10] **route**

**route** is a command-line utility used to view and manipulate the IP routing table on a system. It allows you to add, delete, or modify routes.

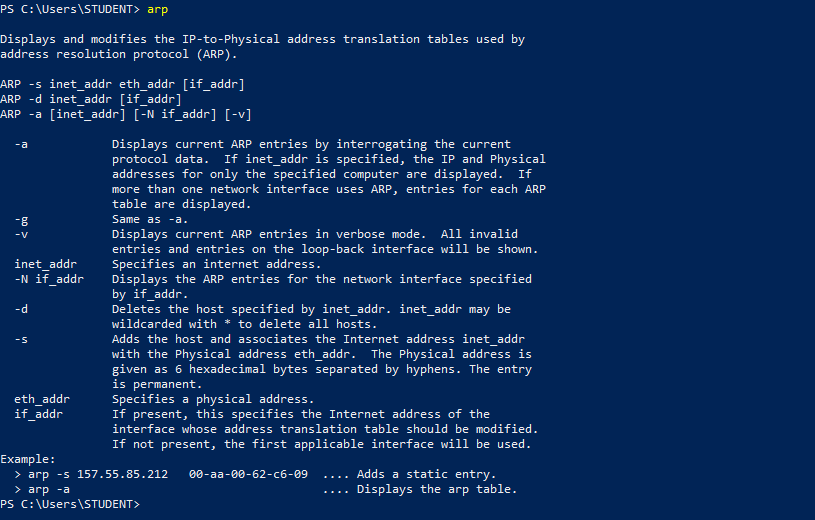


**route print** displays the current IP routing table, including all active routes and their metrics. This is useful for diagnosing network issues and understanding the routing decisions made by the system.



11] **arp**

**arp** (Address Resolution Protocol) is a command-line utility used to display and modify the ARP cache. The ARP cache maps IP addresses to MAC addresses, which is essential for network communication.



**CONCLUSION:** We learnt about different windows and unix network commands with different flags of each command.

**Post Lab Questions**