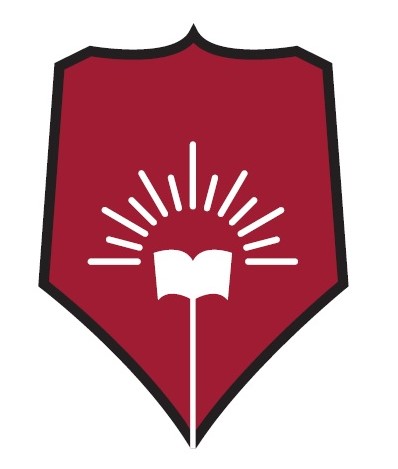
**Experiment No.: 1**

**Networking Commands**

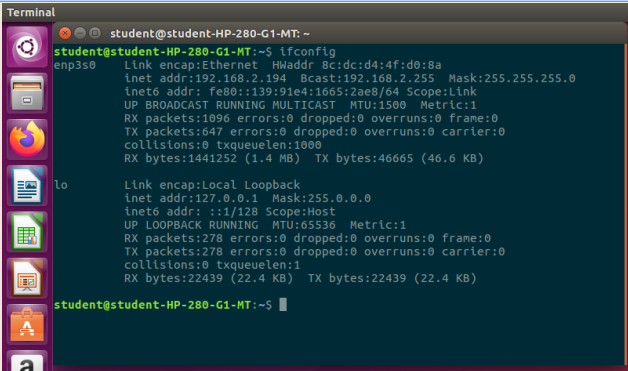
1. **Aim:** Use basic networking commands in Linux (ping, tracert, nslookup, netstat, ip, ifconfig, dig, route)
2. **Objectives:** To introduce concepts and fundamentals networking commands.
3. **Outcomes:** The learner will be able to

* Analyze the functioning of various networking commands.
* Use the commands for building networks.
* Recognize the need for networking commands in life-long learning.

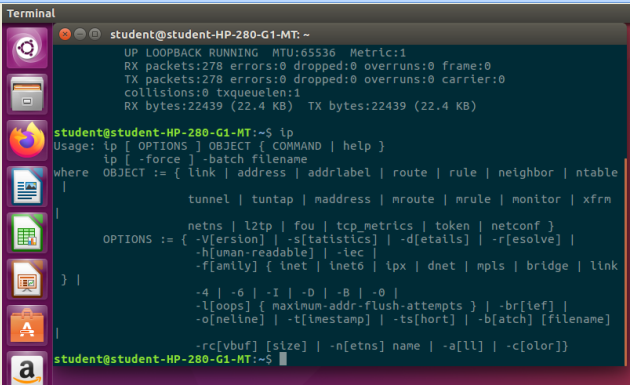
1. **Hardware/Software required:** Command Prompt
2. **Theory:**

Ifconfig:

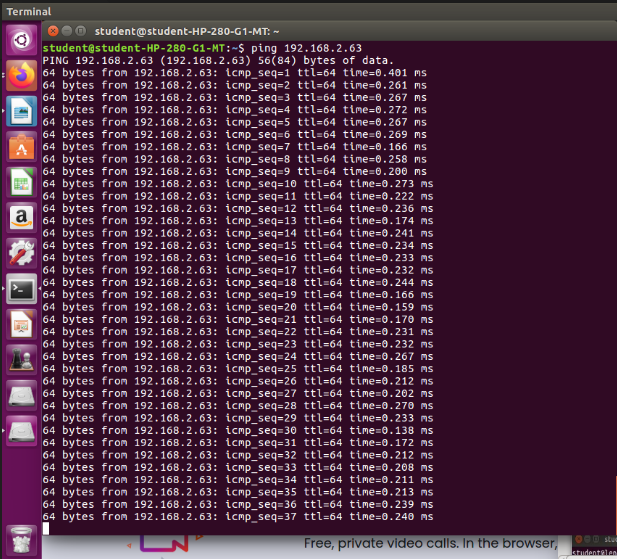
* The command ifconfig stands for interface configurator. This command enables us to initialize an interface, assign IP address, enable or disable an interface. It display route and network interface.
* You can view IP address, MAC address and MTU (Maximum Transmission Unit) with ifconfig command.



Ip: IP command is the newer version of the [ifconfig command](https://www.javatpoint.com/linux-ifconfig). It is a handy tool for configuring the network interfaces for [Linux](https://www.javatpoint.com/linux-tutorial) administrators. It can be used to assign and remove addresses, take the interfaces up or down, and much more useful tasks.



Ping:  
ping command stands for (Packet Internet Groper). It checks connectivity between two nodes to see if a server is available. It sends ICMP ECHO\_REQUEST packets to network hosts and displays the data on the remote server's response. It checks if a remote host is up, or that network interfaces can be reached. Further, it is used to check if a network connection is available between two devices. It is also handy tool for checking your network connection and verifying network issues. Ping command keeps executing and sends the packet until you interrupt.



Dig:

dig command stands for **Domain Information Groper**. This command is used for tasks related to DNS lookup to query DNS name servers. It mainly deals with troubleshooting DNS related problems. It is a flexible utility for examining the DNS (Domain Name Servers). It is used to perform the DNS lookups and returns the queried answers from the name server. Usually, it is used by most DNS administrators to troubleshoot the DNS problems. It is a straightforward tool and provides a clear output. It is more functional than other lookups tools.

The dig command supports plenty of command-line options. Additionally, it facilitates batch mode, which is useful for accessing the lookup requests from a file. If it is not specified to the dig command to query a specific name server, it will access each of the servers from **"/etc/resolv.conf**." The dig without any command-line options will perform an NS query for "." (the root).

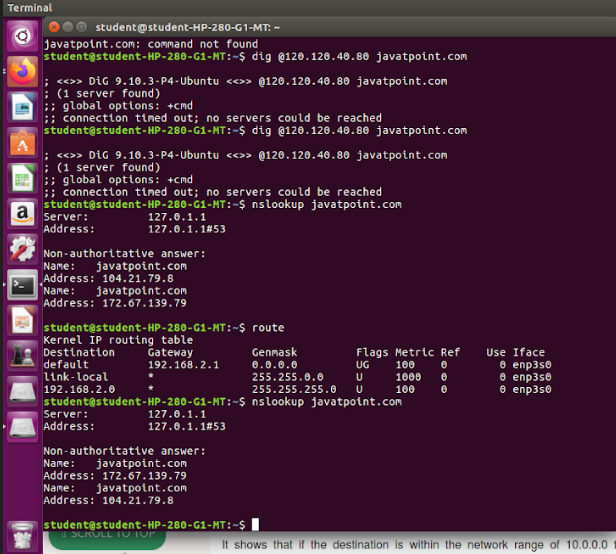
nslookup:

This command is also used to find DNS related query.

route:

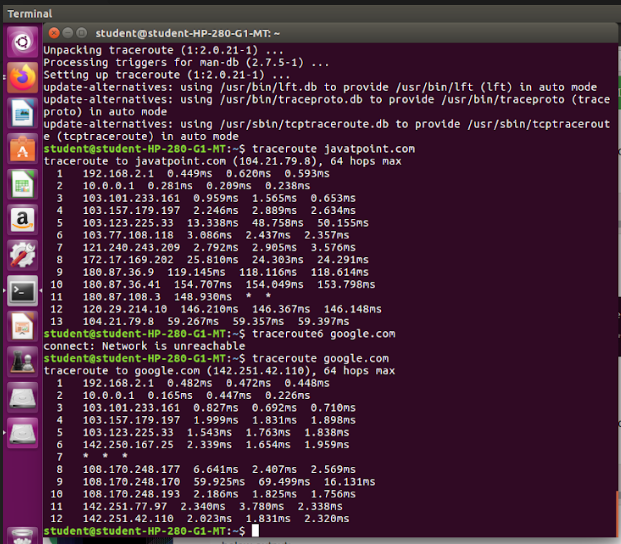
The route command displays and manipulate IP routing table for your system. A router is a

device which is basically used to determine the best way to route packets to a destination.



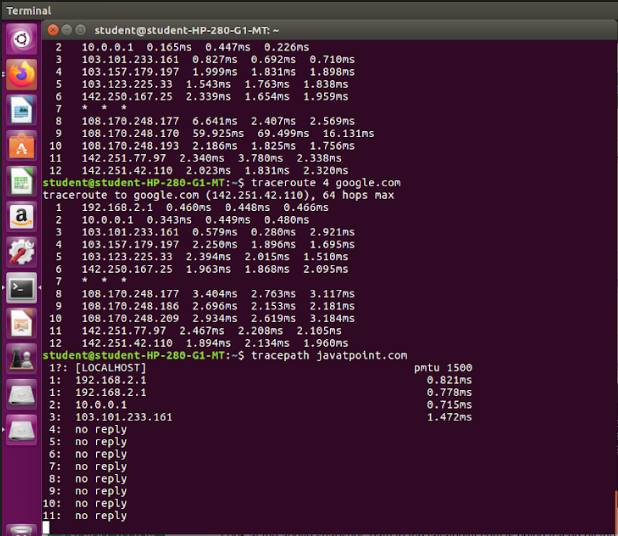
tracroute:

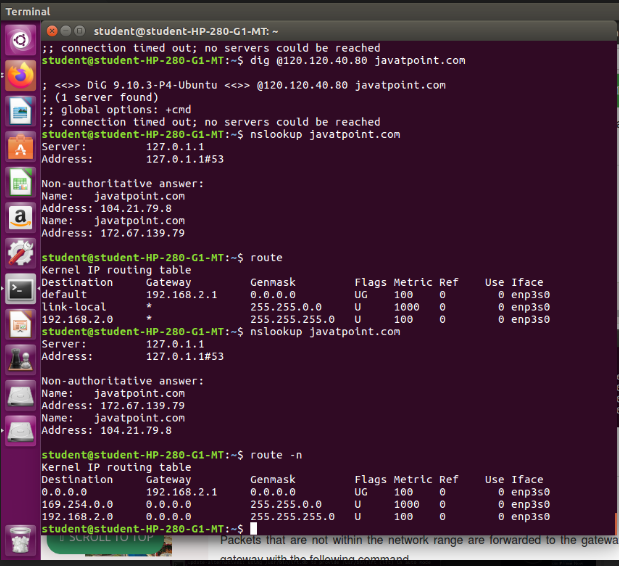
Traceroute command is a network troubleshooting utility that helps us determine the number of hops and packets traveling path required to reach a destination. It is used to display how the data transmitted from a local machine to a remote machine. Loading a web page is one of the common examples of the traceroute. A web page loading transfers data through a network and routers. The traceroute can display the routes, [IP](https://www.javatpoint.com/ip-full-form) addresses, and hostnames of routers over a network. It can be useful for diagnosing network issues.



tracepath:

It is similar to traceroute command, but it doesn't require root privileges. By default, it is installed in Ubuntu but you may have to download traceroute on Ubuntu. It traces the network path of the specified destination and reports each hop along the path. If you have a slow network then tracepath will show you where your network is weak.





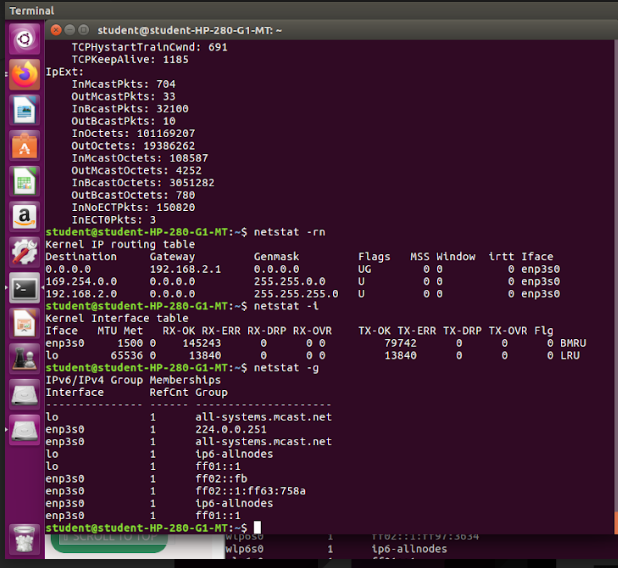
netstat :

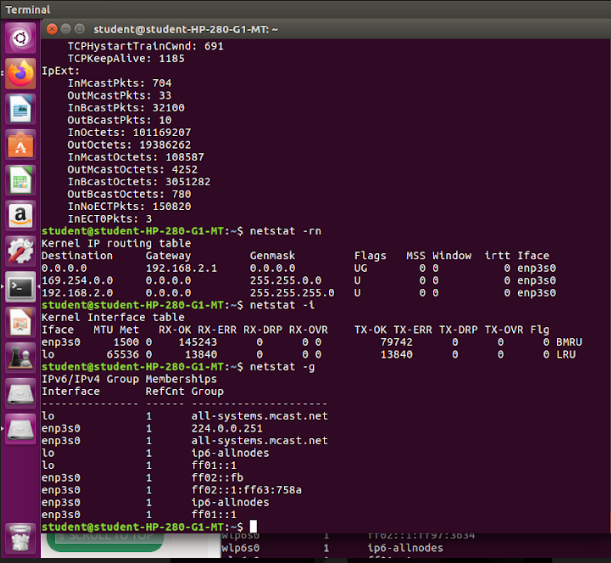
Linux netstat command stands for **Network statistics**. It displays information about different interface statistics, including open sockets, routing tables, and connection information. Further, it can be used to displays all the socket connections (including TCP, UDP). Apart from connected sockets, it also displays the sockets that are pending for connections. It is a handy tool for network and system administrators.

Sockets allow communication between two different processes on the same or different machines. To be more precise, it's a way to talk to other computers.

A socket is one endpoint of a two way communication link between two programs running on the network.

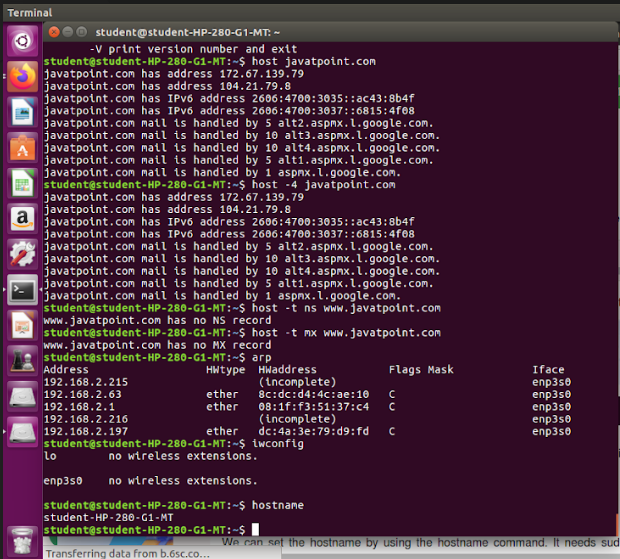
netstat –rn:





arp:

The command arp stands for **A**ddress **R**esoslution**P**rotocol. It allows us to view or add content into kernel's ARP table.



1. **Output Analysis:**

(Students should write output analysis based on the working of different networking networking commands used. Specify each scenario explicitly with output analysis)

1. **Additional Learning:**

(Students should write additional learning on their own based on what additionally they learnt after performing the experiment)

1. **Conclusion :**

(Students should write conclusion on their own)

1. **Viva Questions:**

* What is the difference between traceroute and ifconfig
* How to find IP address of a website.
* State the working of nslookup.
* How to determine whether a we are able to connect to a system or not?

1. **References:**
   1. A.S. Tanenbaum, “Computer Networks”, Pearson Education, (4e)
   2. B.A. Forouzan, “Data Communications and Networking”, TMH (5e).
2. James F. Kurose & K W Ross: Computer Networking: A Top Down Approach, Pearson Education (LPE)
3. <https://www.youtube.com/watch?v=OJ1gScTXqRc> (NPTEL)