Computer Networks

**Experiment 2**

**Name:** Ayush Jain

**SAP ID**: 60004200132

**Div**: B2

**Branch**: Computer Engineering

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Aim**: To study & implement different networking devices.

Networking Commands:

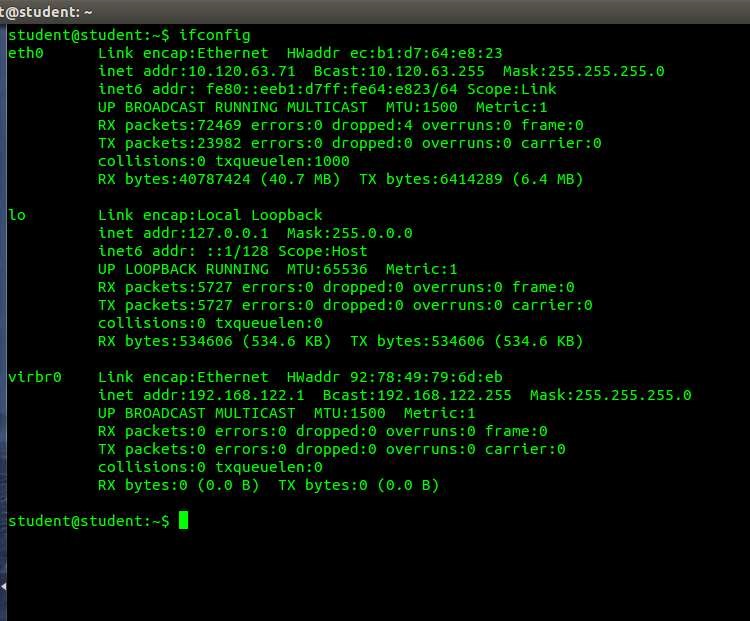
# **ifconfig :**

**Description** :- ifconfig stands for "interface configuration." It is used to view and change the configuration of the network interfaces on your system.

Running the ifconfig command with no arguments,

**Syntax** :- ifconfig

It displays information about all network interfaces currently in operation. The output resembles the following:



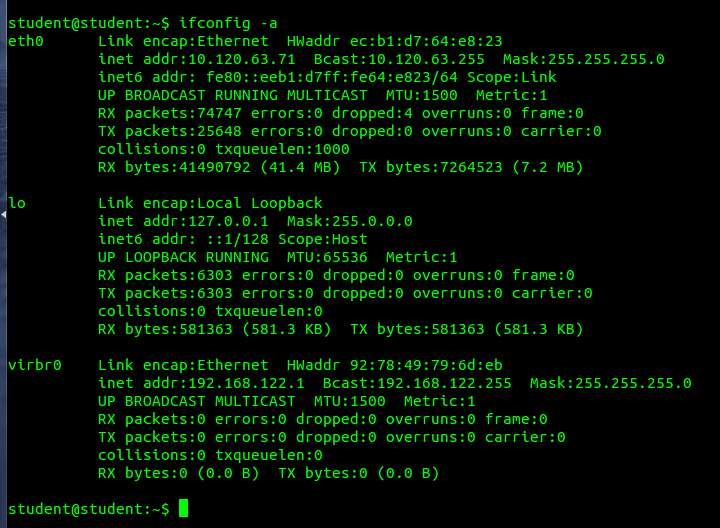
Here, eth0, lo and wlan0 are the names of the active network interfaces on the system.

* eth0 is the first Ethernet interface. (Additional Ethernet interfaces would be named eth1, eth2, etc.) This type of interface is usually a NIC connected to the network by a category 5 cable.
* lo is the loopback interface. This is a special network interface that the system uses to communicate with itself.
* wlan0 is the name of the first wireless network interface on the system.

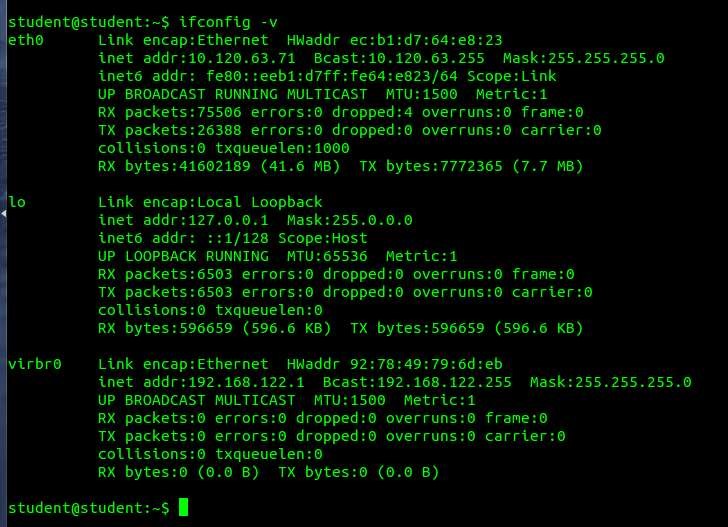
Additional wireless interfaces would be named wlan1, wlan2, etc.

These are the traditional naming conventions for network interfaces under Linux; other operating systems may have different names. For instance, under many BSD operating systems, Ethernet interfaces are named em0, em1, etc. Check your configuration, or consult your documentation, to determine the exact names of your interfaces.

* With argument -a :-



* With argument -v :-



* With argument -s :-



# **Ping :**

PING (Packet Internet Groper) command is used to check the network connectivity between host and server/host. This command takes as input the IP address or the URL and sends a data packet to the specified address with the message “PING” and get a response from the server/host this time is recorded which is called latency. Fast ping low latency means faster connection. Ping uses ICMP(Internet Control Message Protocol) to send an ICMP echo message to the specified host if that host is available then it sends ICMP reply message. Ping is generally measured in millisecond

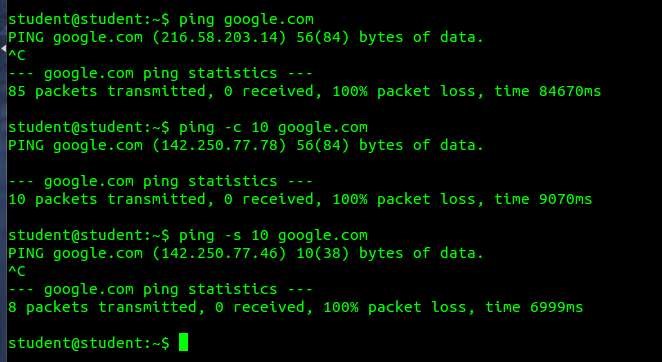
Controlling the number of pings:

Earlier we did not define the number of packets to send to the server/host by using c option we can do so.

Controlling the size of packets send:

Earlier a default sized packets were sent to a host but we can send light and heavy packet by using

-s option.



# **ip :**

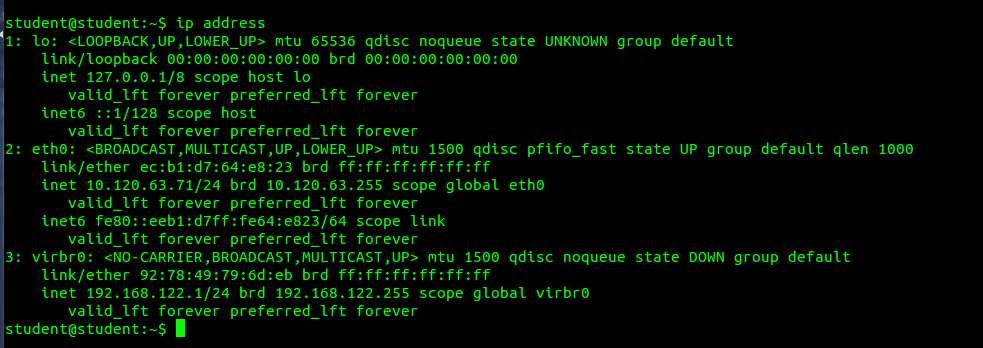
Ip command in Linux is present in the net-tools which is used for performing several network administration tasks. IP stands for Internet Protocol. This command is used to show or manipulate routing, devices, and tunnels. It is similar to ifconfig command but it is much more powerful with more functions and facilities attached to it. ip command is used to perform several tasks like assigning an address to a network interface or configuring network interface parameters.

It can perform several other tasks like configuring and modifying the default and static routing, setting up tunnel over IP, listing IP addresses and property information, modifying the status of the interface, assigning, deleting and setting up IP addresses and routes. Syntax:

ip [ OPTIONS ] OBJECT { COMMAND | help }

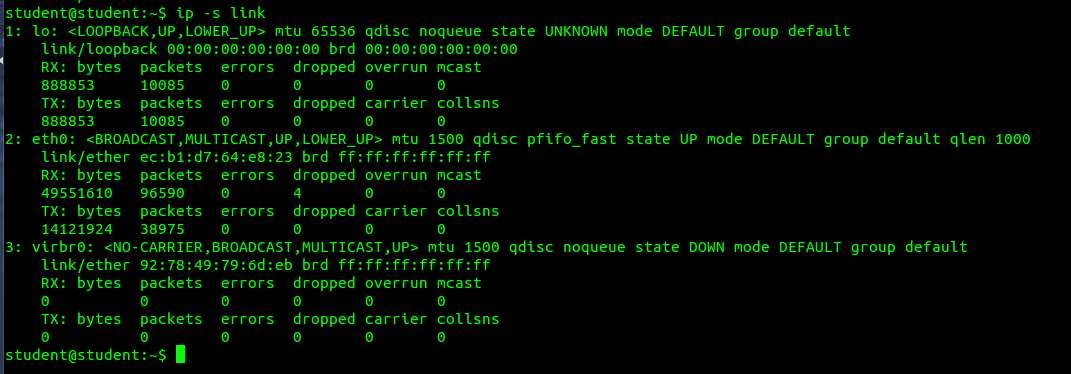
● ip address

This will show the information related to all interfaces available on our system, but if we want to view the information of any particular interface, add the options show followed by the name of the particular network interface.



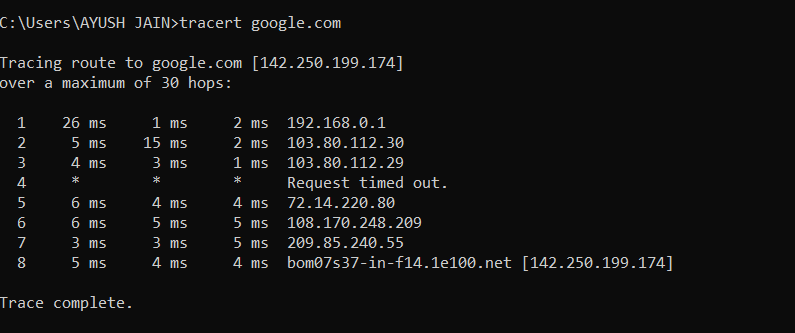
-**link**: It is used to display link layer information, it will fetch characteristics of the link layer devices currently available. Any networking device which has a driver loaded can be classified as an available device.

This link option when used with -s option is used to show the statistics of the various network interfaces.



# **Traceroute**

Traceroute command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all the hops that a packet takes. Below image depicts how traceroute command is used to reach the Google(172.217.26.206) host from the local machine and it also prints detail about all the hops that it visits in between.



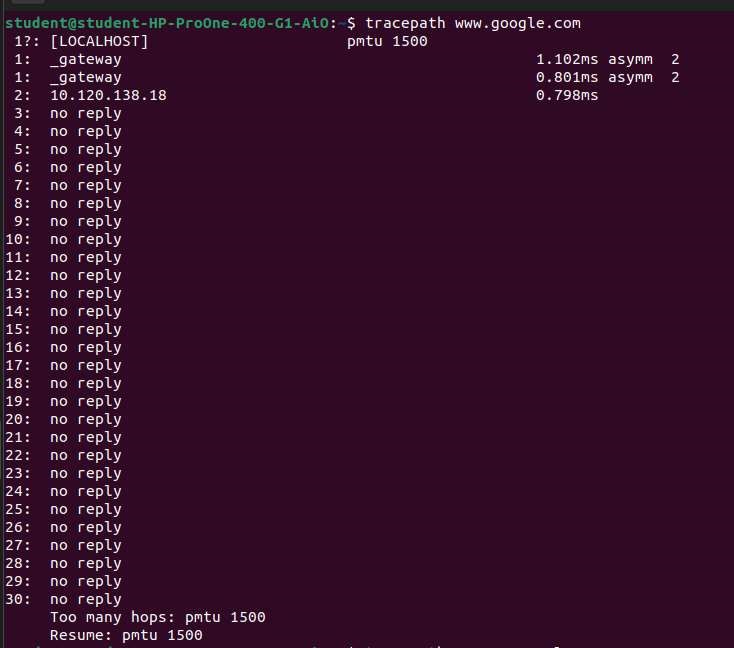
## **Tracepath**

Tracepath command in Linux is used to traces path to destination discovering MTU along this path. It uses UDP port or some random port. It is similar to traceroute, but it does not require superuser privileges and has no fancy options. tracepath6 is a good replacement for traceroute6 and classic example of the application of Linux error queues. The situation with IPv4 is worse because commercial IP routers do not return enough information in ICMP error messages. Probably, it will change, when they will be updated.

For now, it uses Van Jacobson’s trick, sweeping a range of UDP ports to maintain trace history.

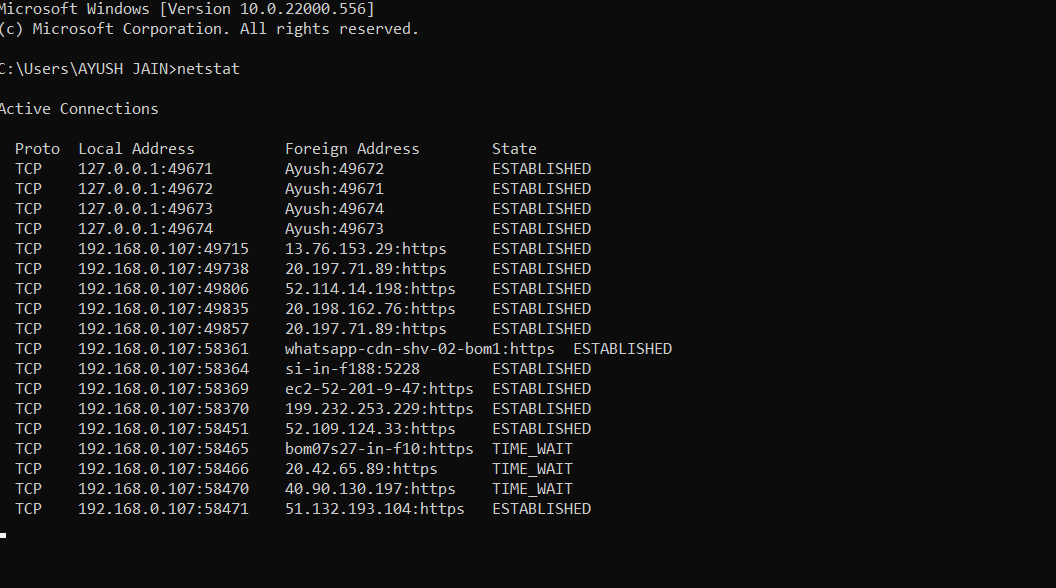
Syntax:

tracepath [-n] [-b] [-l pktlen] [-m max\_hops] [-p port] destination

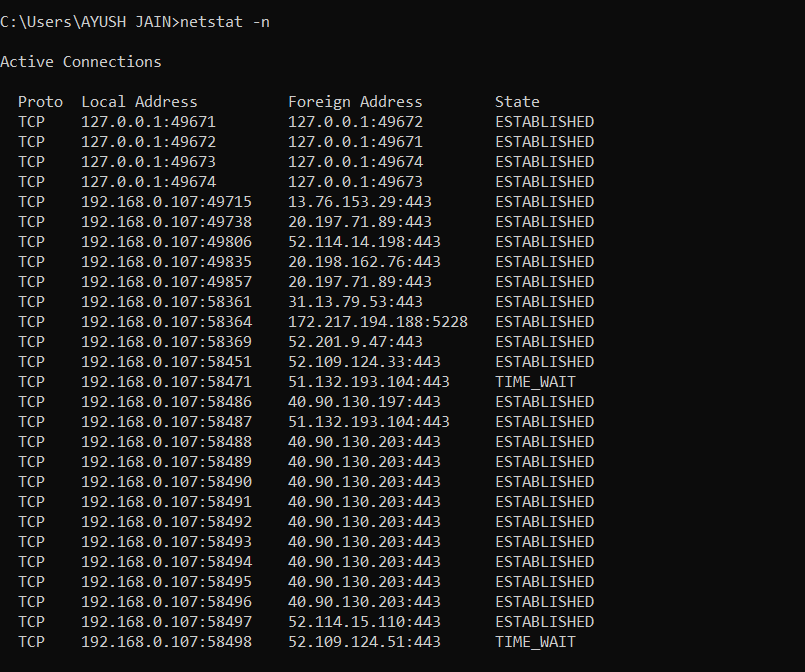


# **Netstat**

Netstat command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.,



* The following command to display active connections showing numeric IP address and port number instead of trying to determine the names
* Syntax :- netstat -n



## **Nslookup :**

Nslookup (stands for “Name Server Lookup”) is a useful command for getting information from the DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record. It is also used to troubleshoot DNS-related problems.

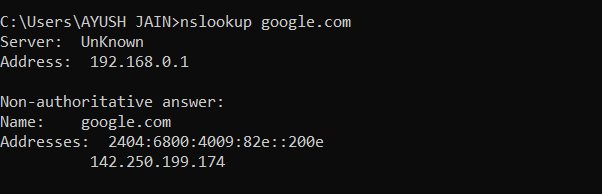
**Syntax:**

nslookup [option]

● Options of nslookup command:

nslookup google.com :

nslookup followed by the domain name will display the “A Record” (IP Address) of the domain. Use this command to find the address record for a domain. It queries to domain name servers and gets the details.

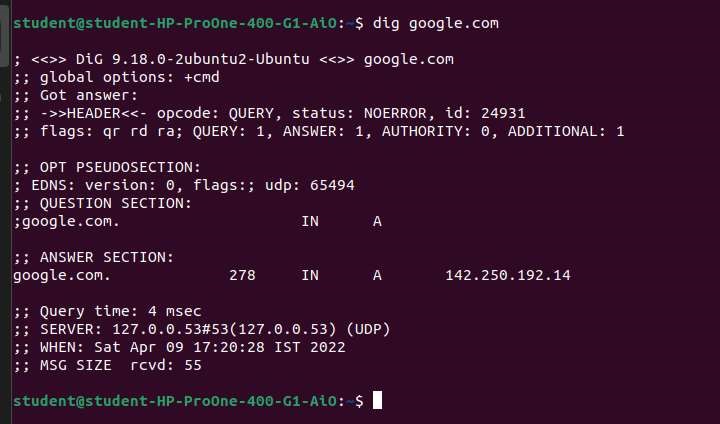


## **Dig :**

Dig command stands for Domain Information Groper. It is used for retrieving information about DNS name servers. It is basically used by network administrators. It is used for verifying and troubleshooting DNS problems and to perform DNS lookups. Dig command replaces older tools such as nslookup and the host.

**Syntax:**

dig [server] [name] [type]



● To remove comment lines.

dig geeksforgeeks.org +nocomments

This command makes a request and excludes the comment lines.

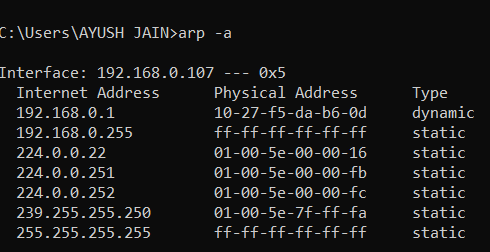


## **Arp**

arp command manipulates the System’s ARP cache. It also allows a complete dump of the ARP cache. ARP stands for Address Resolution Protocol. The primary function of this protocol is to resolve the IP address of a system to its mac address, and hence it works between level 2(Data link layer) and level 3(Network layer).

Syntax:

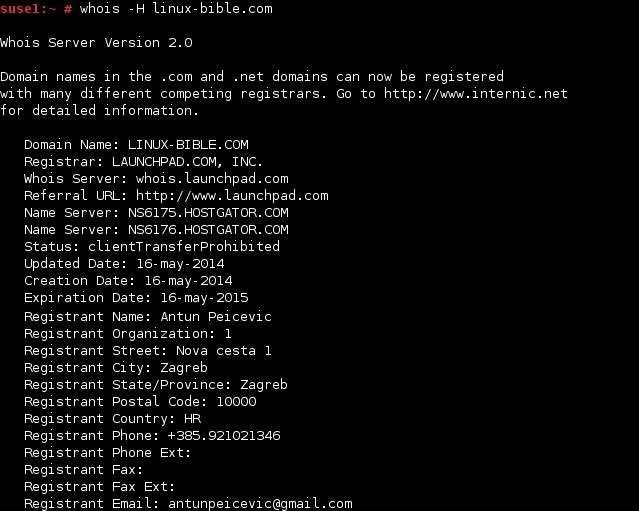
arp [-v] [-i if] [-H type] -a [hostname]



## **Whois :**

You can use the whois command in Linux to find out information about a domain, such as the owner of the domain, the owner’s contact information, and the nameservers that the domain is using.

For example, to find out domain information of linux-bible.com, we can use the following command:



### **Host :**

Host command in Linux system is used for DNS (Domain Name System) lookup operations. In simple words, this command is used to find the IP address of a particular domain name or if you want to find out the domain name of a particular IP address the host command becomes handy. You can also find more specific details of a domain by specifying the corresponding option along with the domain name.

**Syntax:**

host [-aCdlriTWV] [-c class] [-N ndots] [-t type] [-W time]

[-R number] [-m flag] hostname [server]

* Host domain\_name: This will print the IP address details of the specified domain

* Host IP\_Address: This will display the domain details of the specified IP Address.

