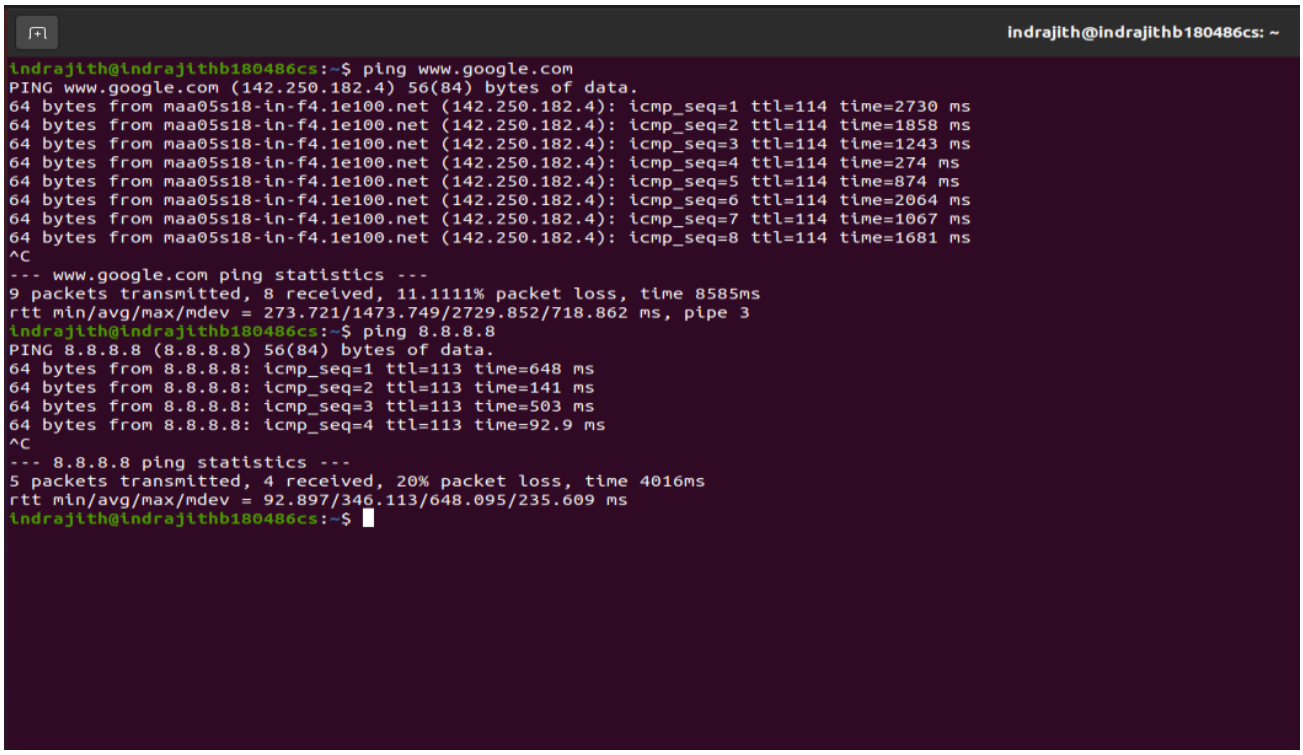
NETWORKS LAB
CS3093D
ASSIGNMENT 1

Submitted by,
Indrajith T S
B180486CS
S8 - Btech

NETWORK COMMANDS

1. **Ping**

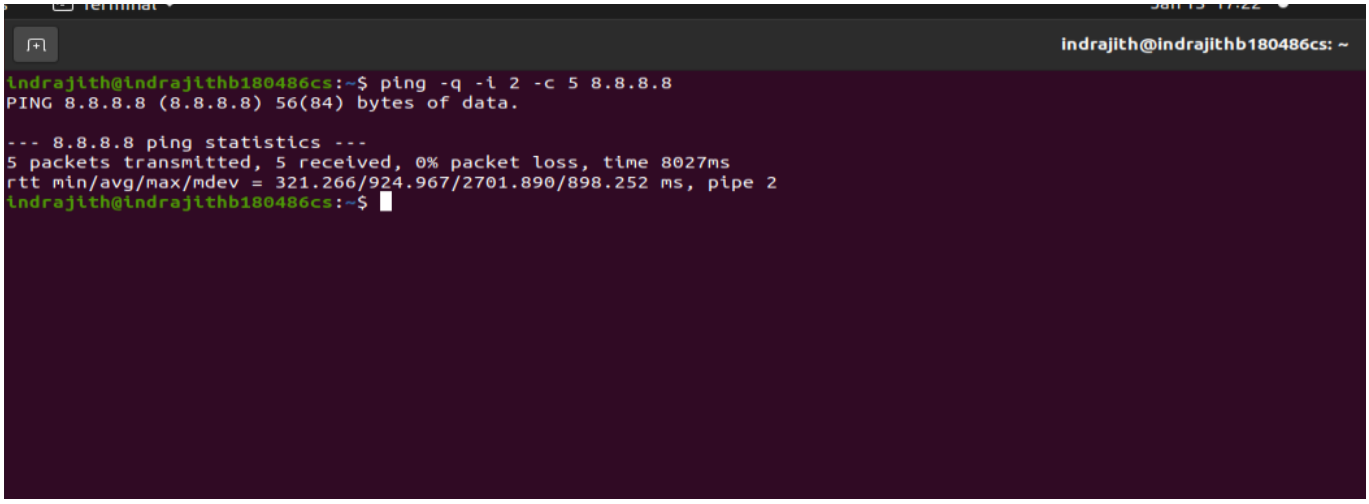
   Ping sends ICMP ECHO_REQUEST to network host specified by the address
   ping 8.8.8.8 to ping to google's primary dns
   ping www.google.com for pinging google using address

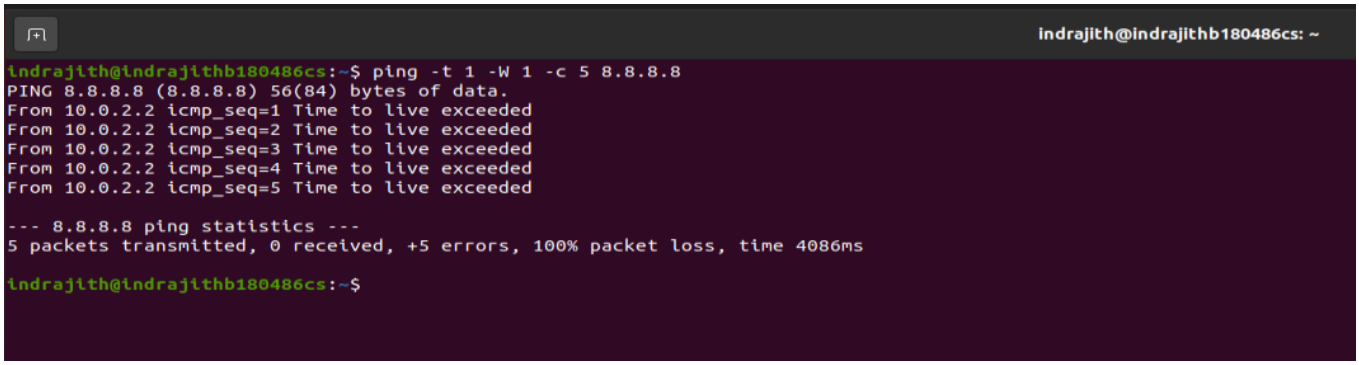


   Here host address is specified using its name and ip.

   Some other flags that can be used with the ping command are as follows

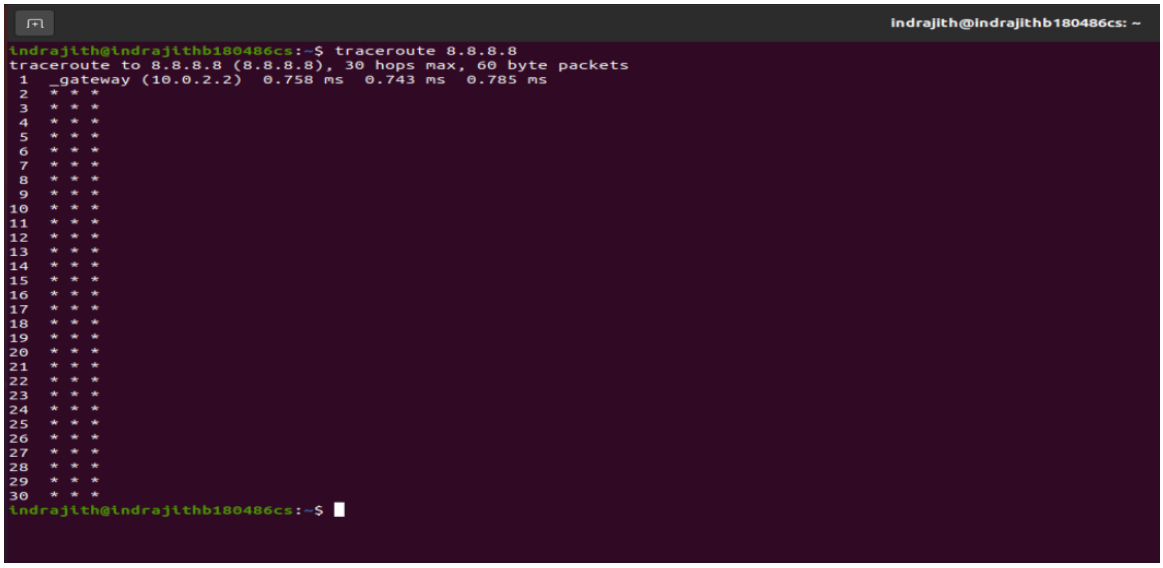
   Flag -s size is used to specify the size of a packet
   -c count is used to specify the no of packets
   -q for quiet output which is only the summary
   -i time for time interval
   -t ttl to set time to live
   -W timeout toset timeout in s in case of not reachable



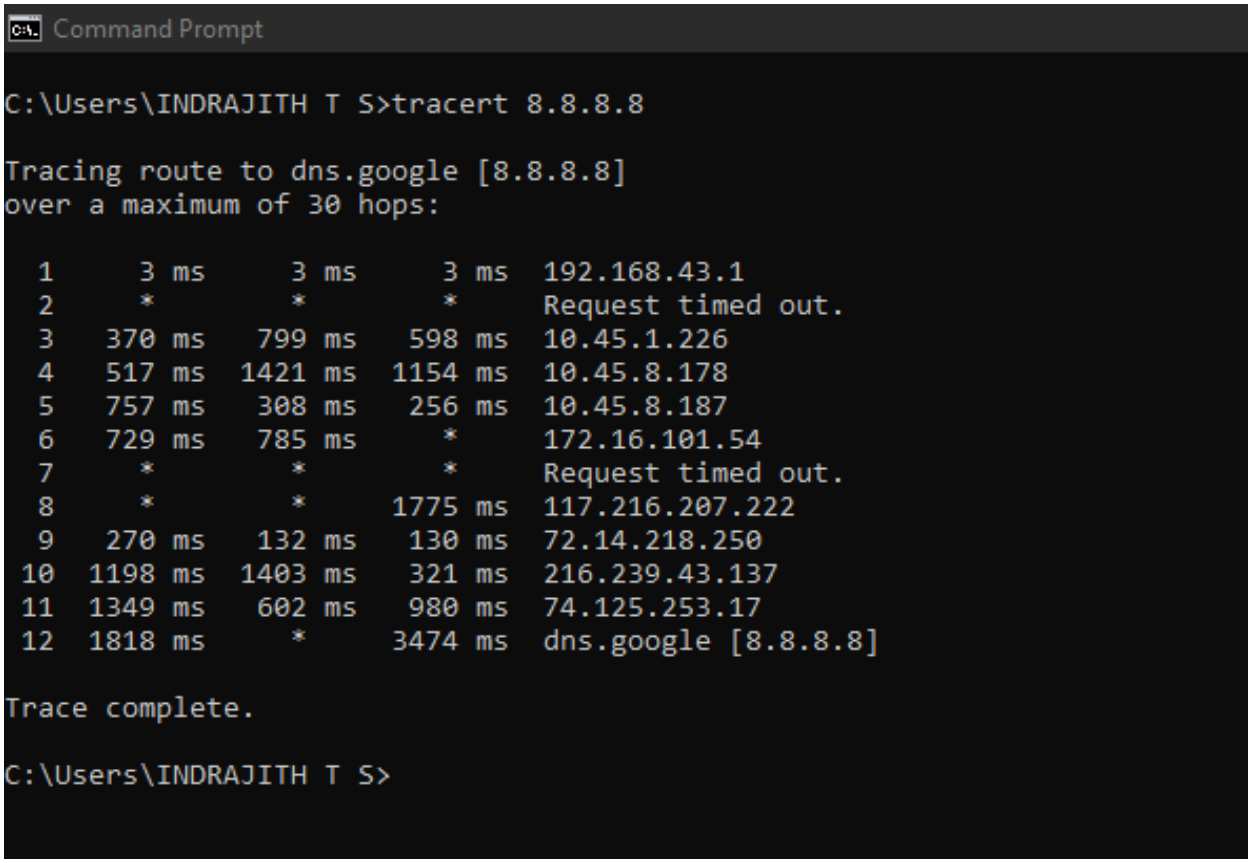


2. tracert/traceroute

It tracks the route packets take from an ip network on their way to the given host destination.



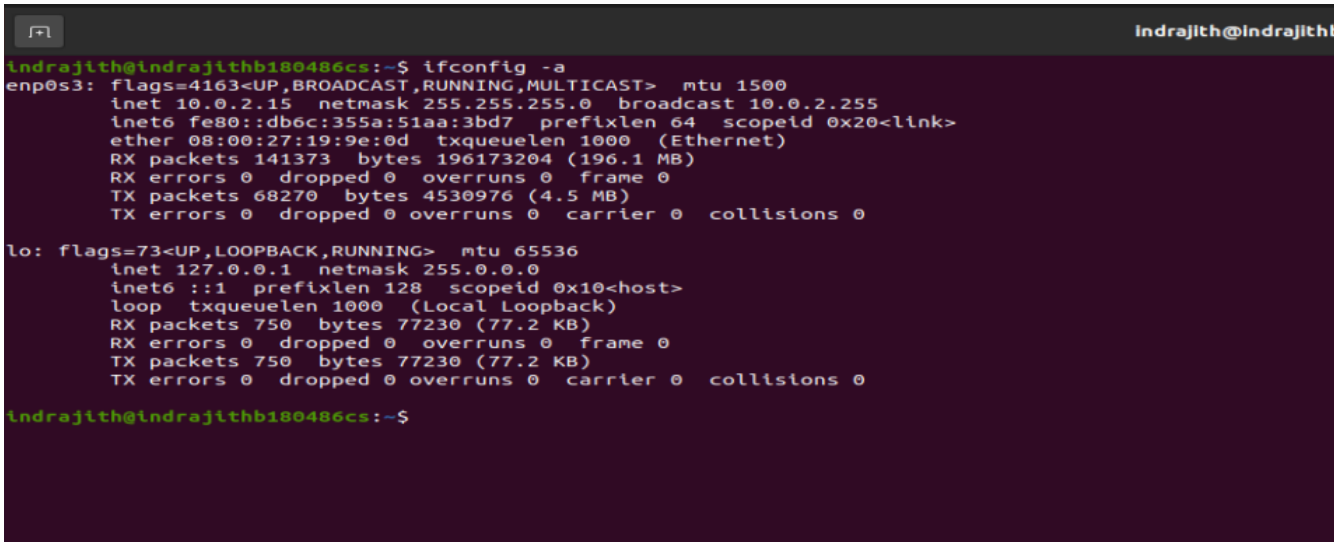
This shows the only path that exits through the gateway of the virtual machine.



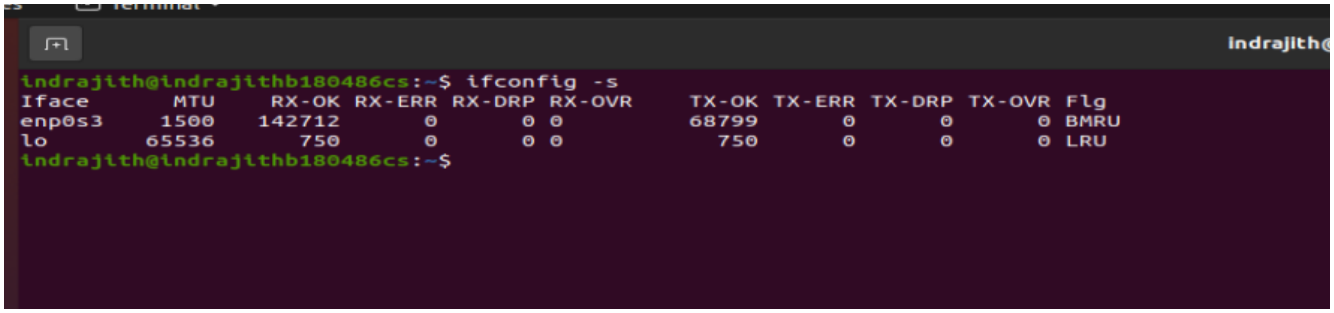
Tracert identifying all the routes from the host machine.

3. **ifconfig/ipconfig**

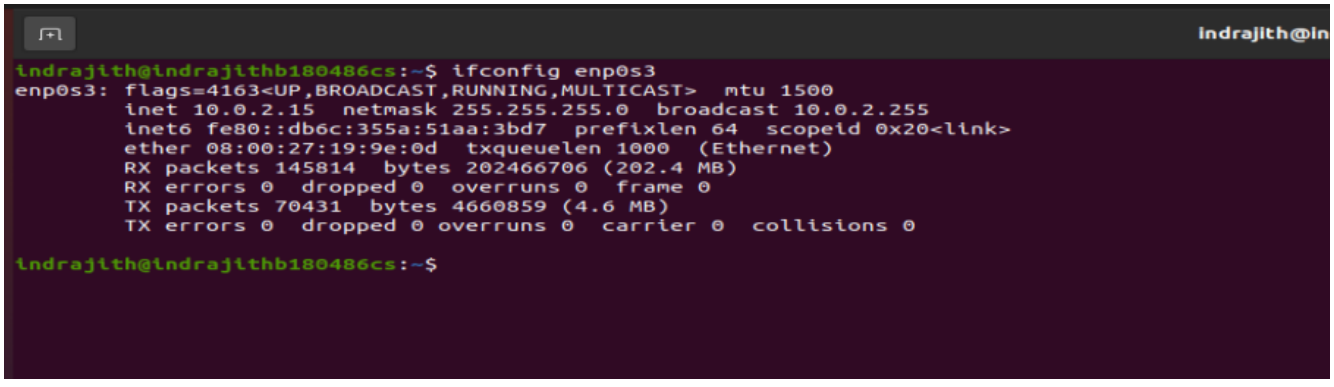
   Ifconfig is used to show the network details in linux
   - a for all list
   - s for short list
   - interface name for a specific interface details
   - down for deactivating up for activating



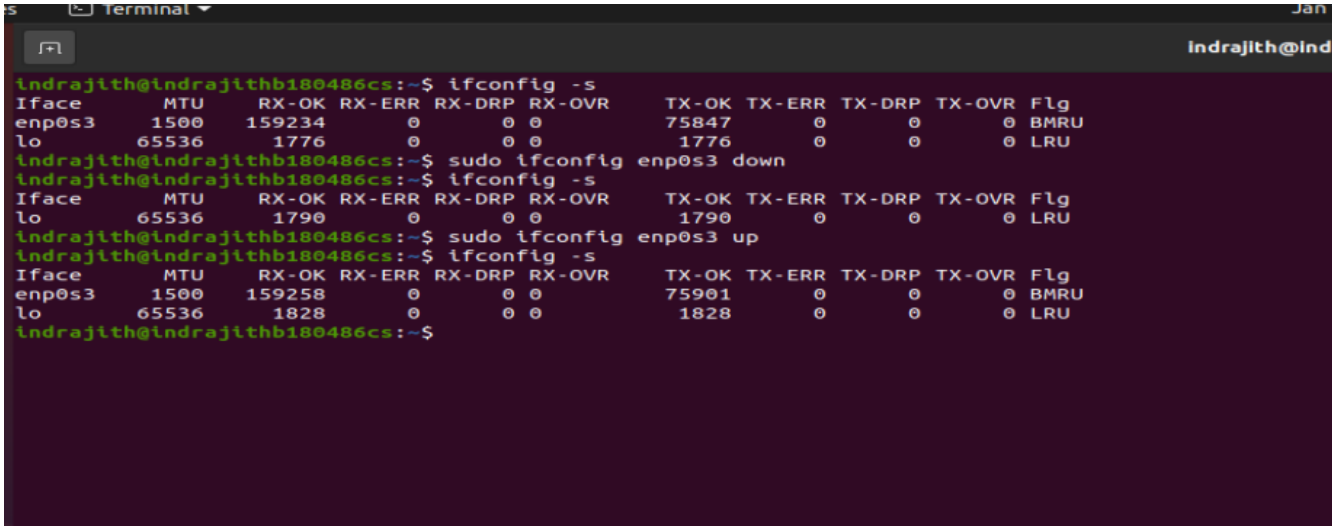
For all interfaces



Summary of interfaces

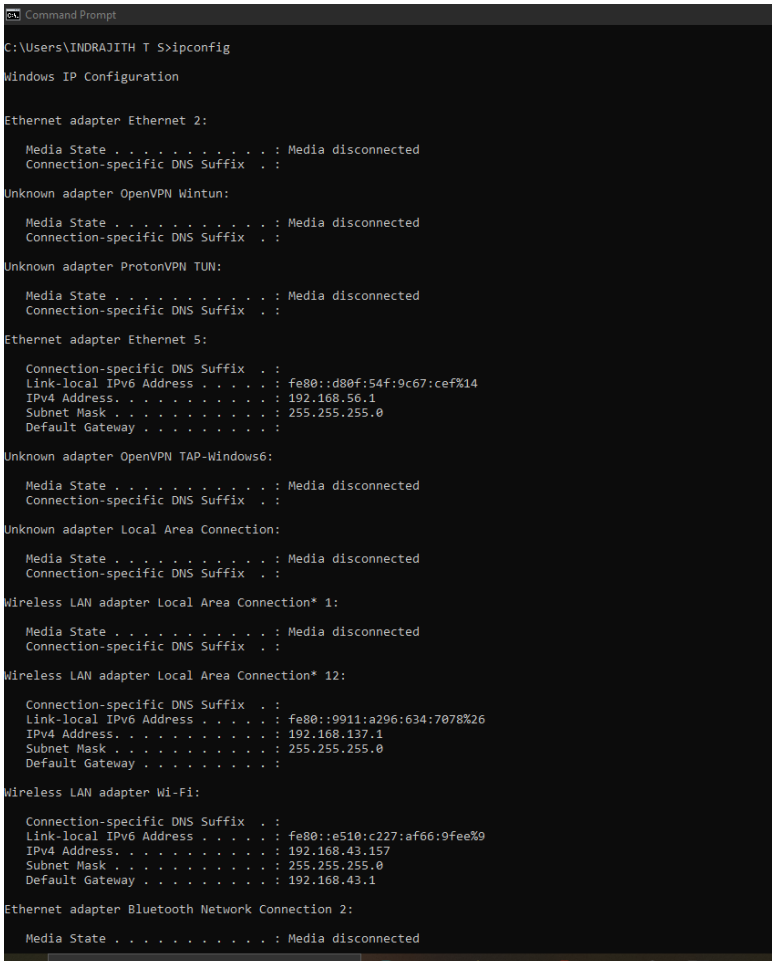


Detail of a specific interface



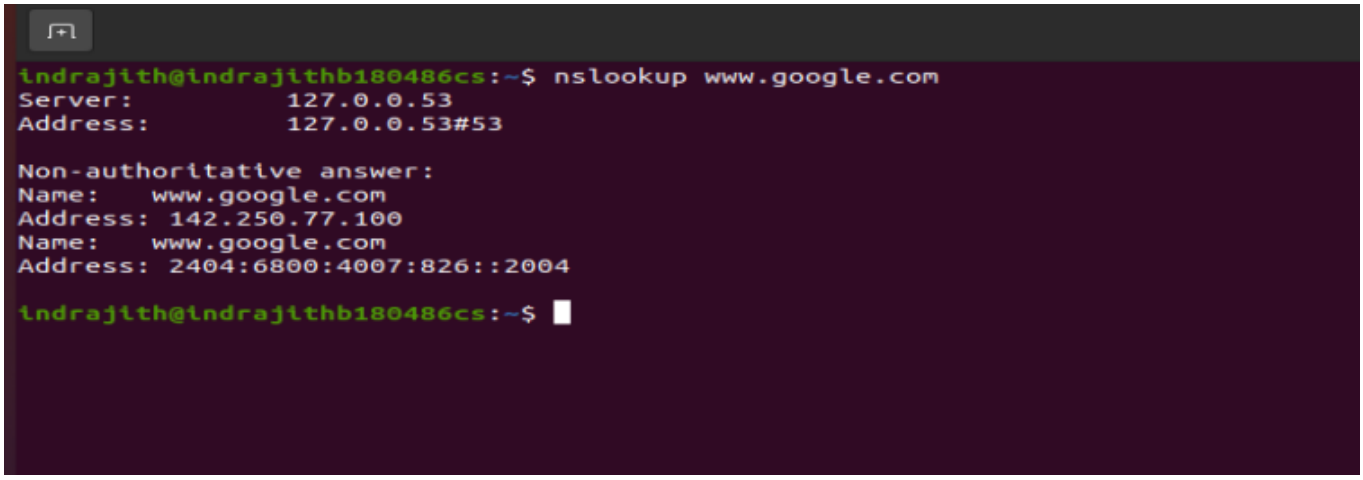
Changing the working status of interfaces

Ipconfig is the command used in windows

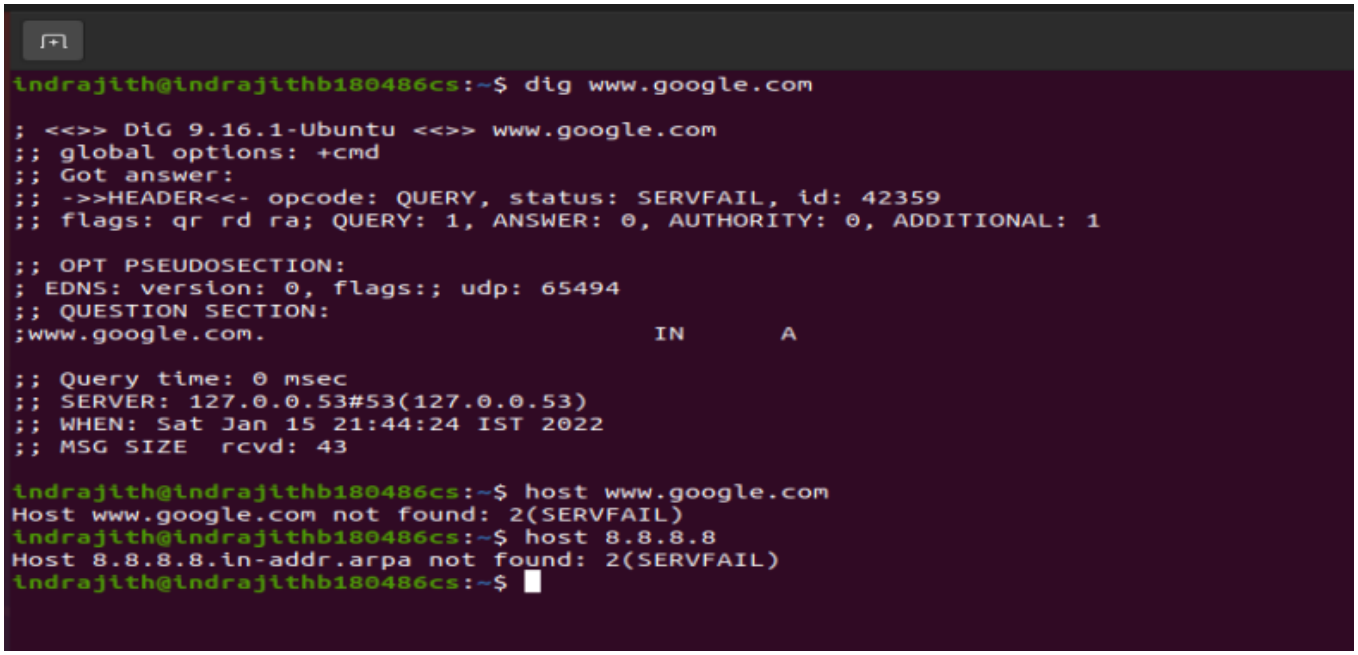


4. **dig/nslookup/host**

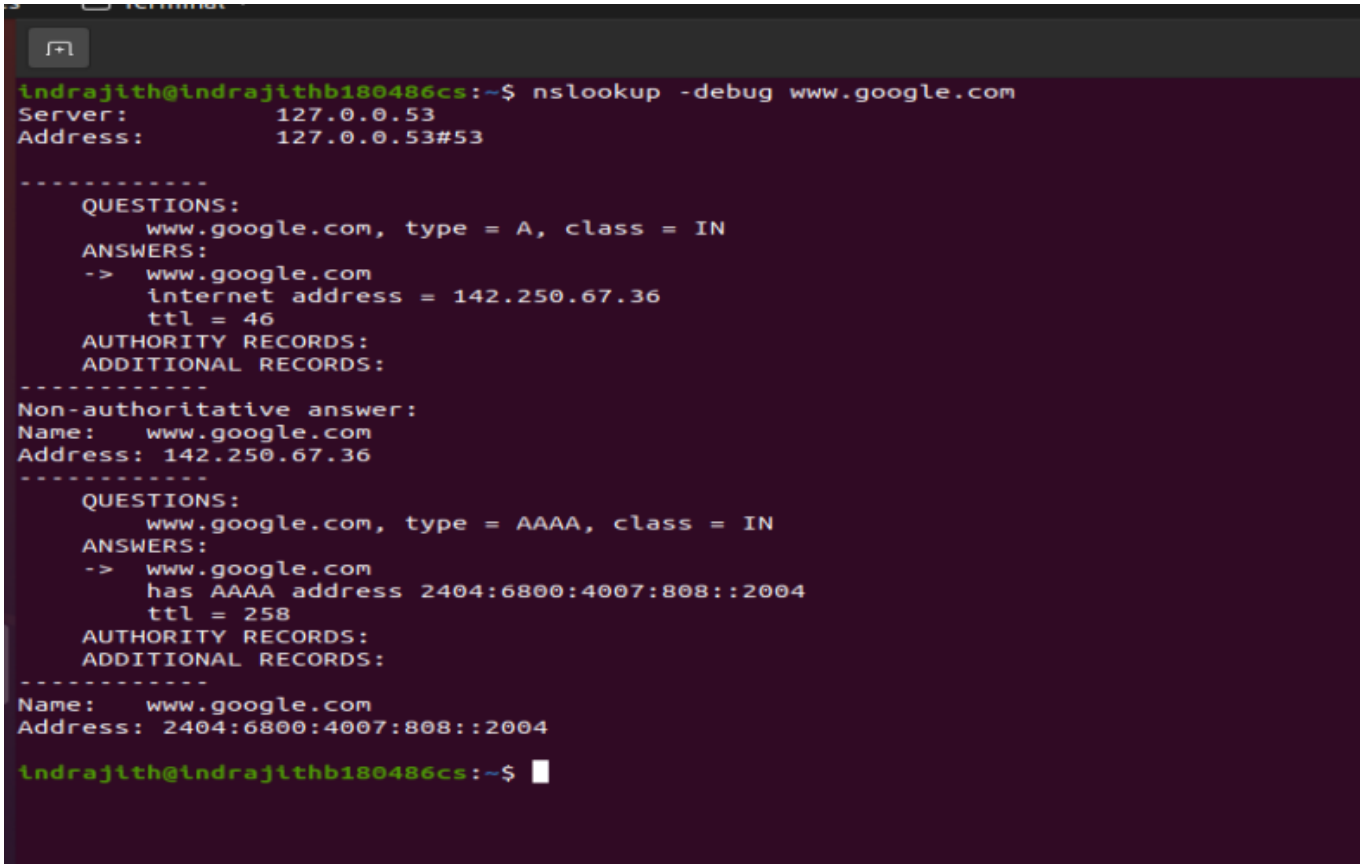
This is to query ineternet dns. This can be used to troubleshoot dns servers through interactive session.



nslookup of google



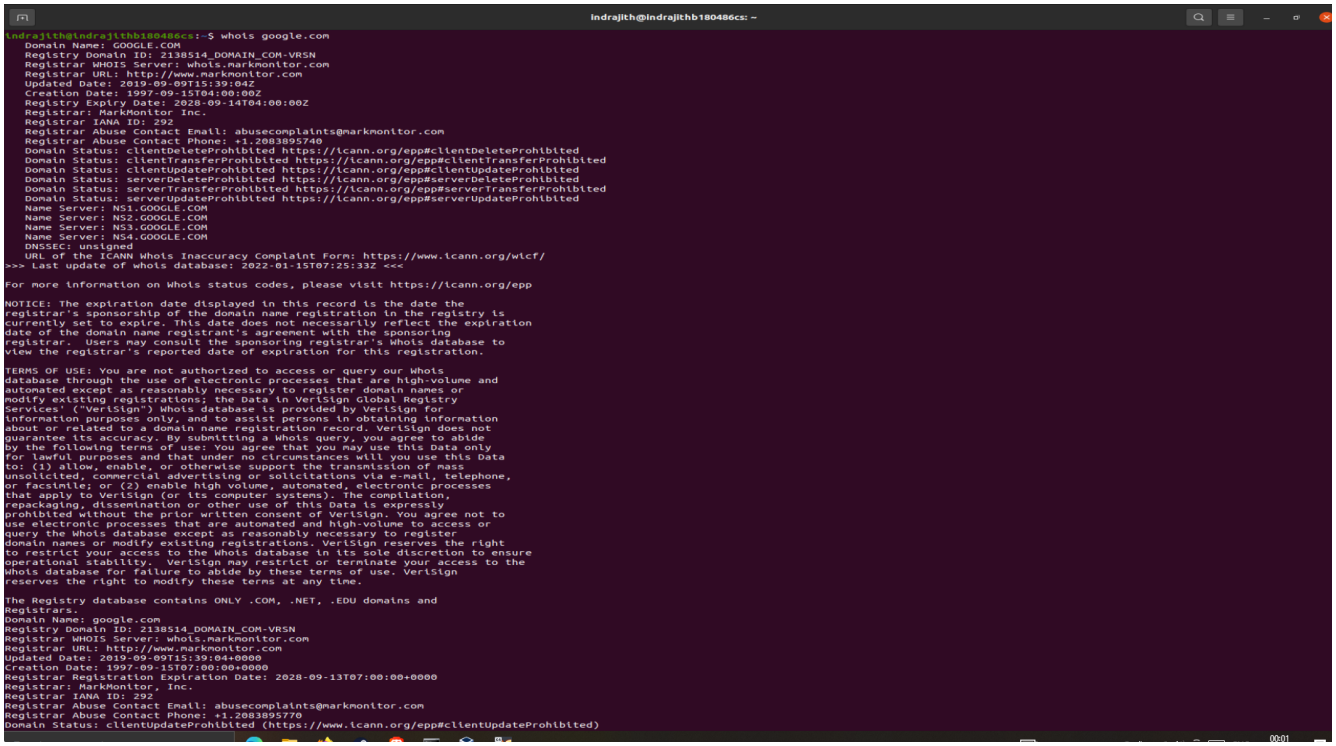
dig on google



debug on google

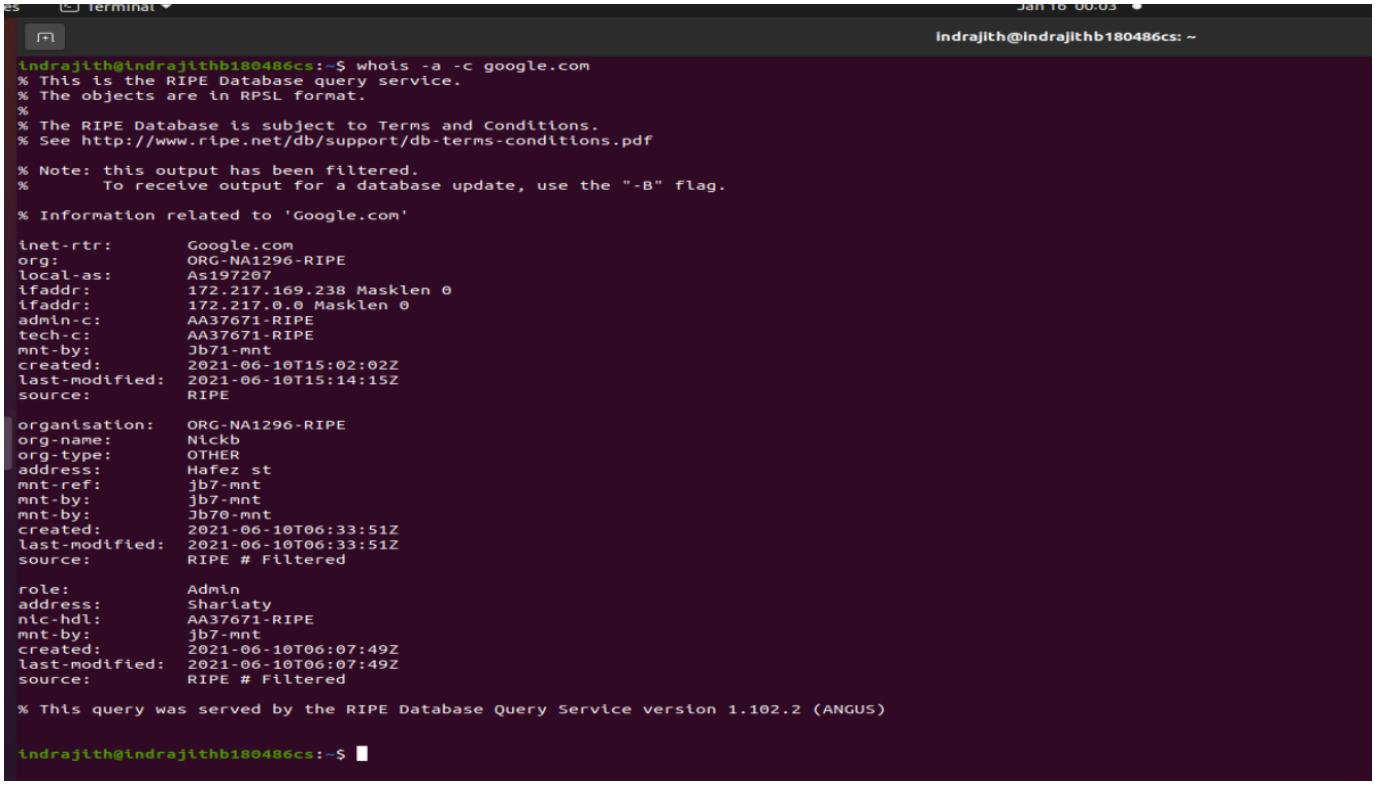
5. **whois**

This command provides details and information about the server that is provided.



Flag -p for all mirrored databases

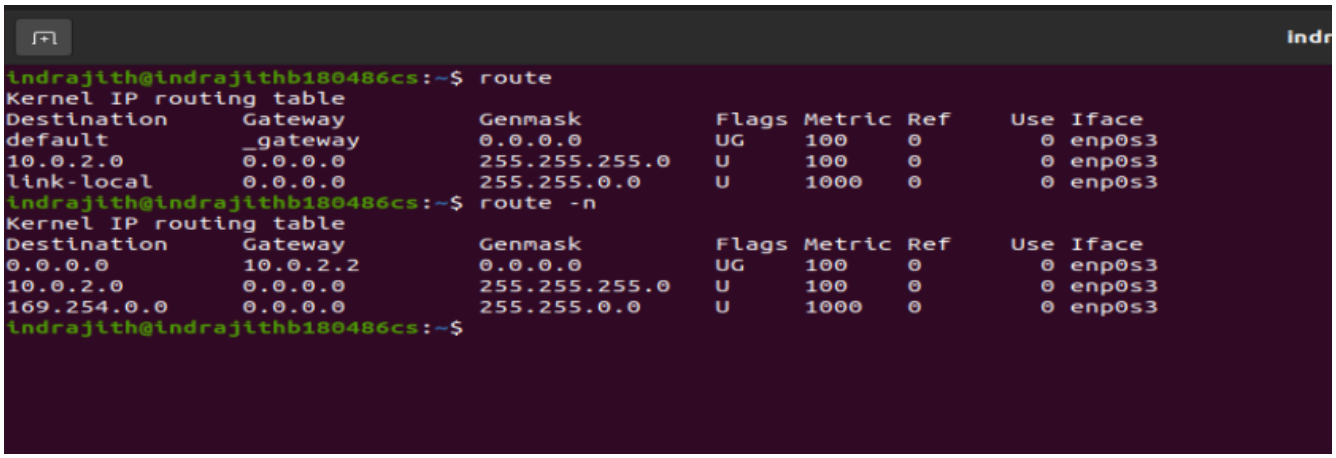
-c return the smallest ip range in with a reference to an irt object.



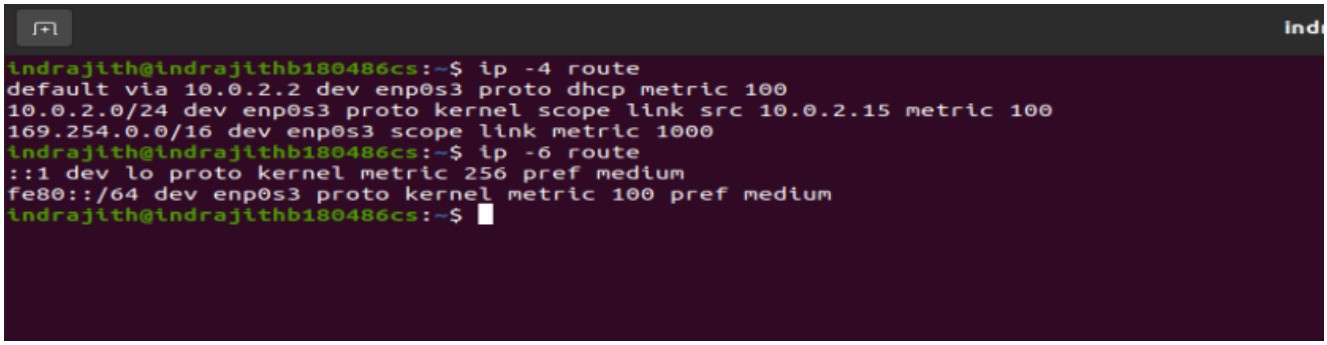
6. **route**

   This command is used to see the routing tables that is already established or to add another route as we wish.

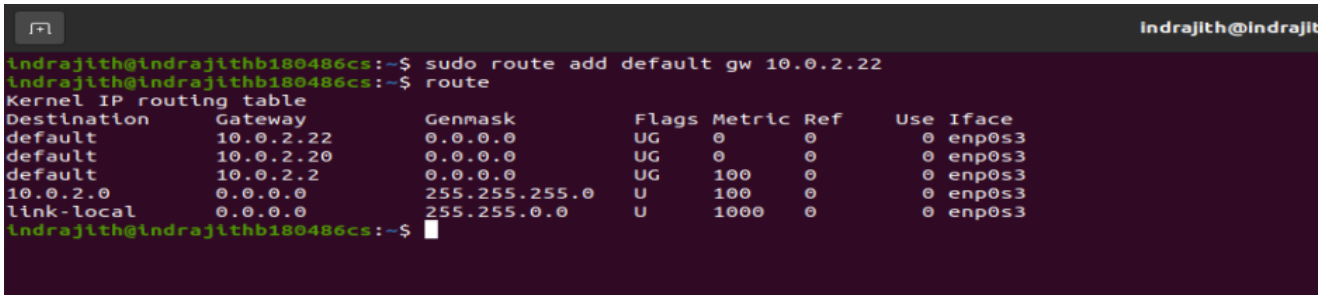
   Routing table in normal and complete numerical mode



   -4 flag for ipv4 and -6 flag for ipv6 with ip

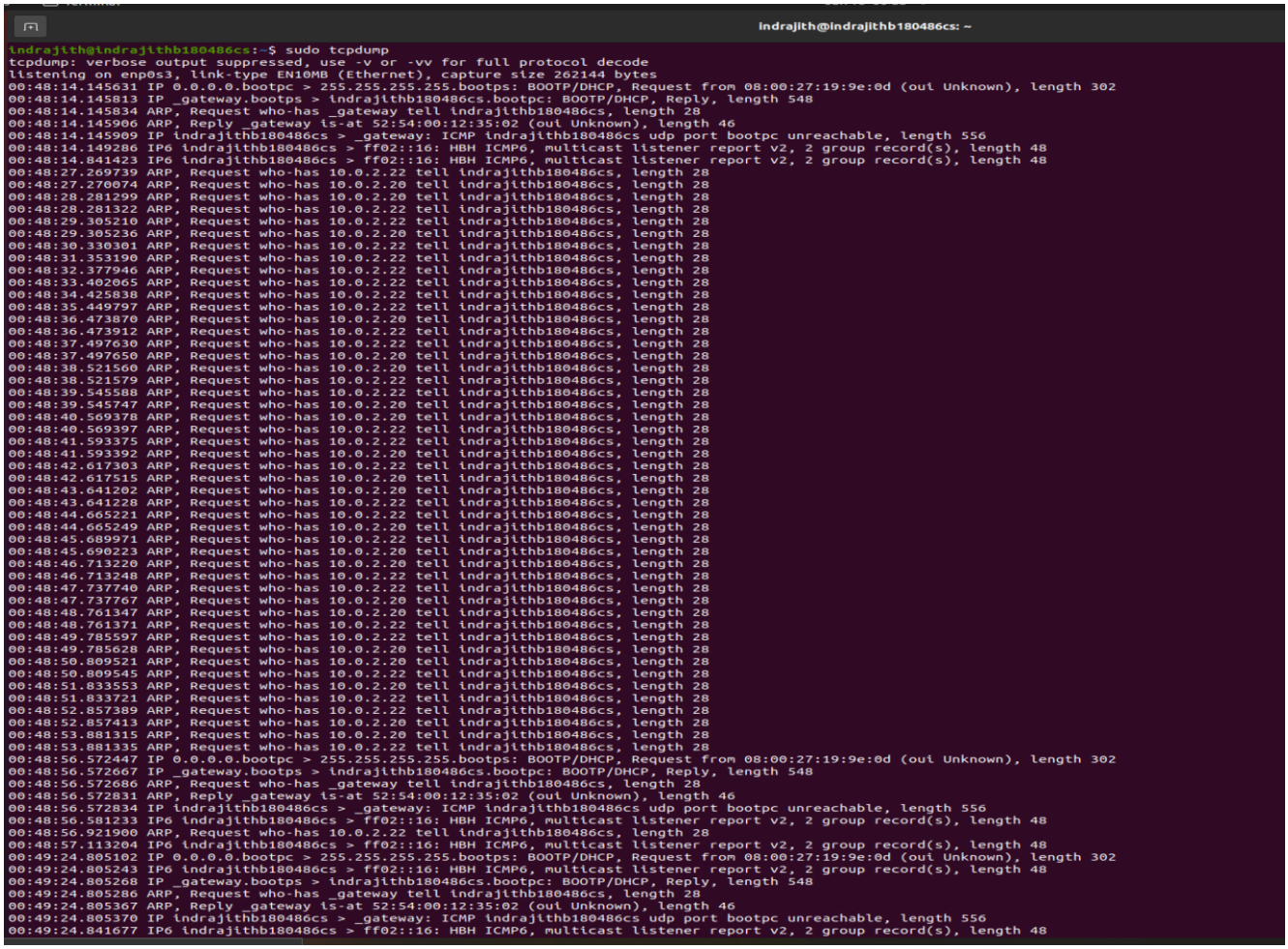


   Adding new routes

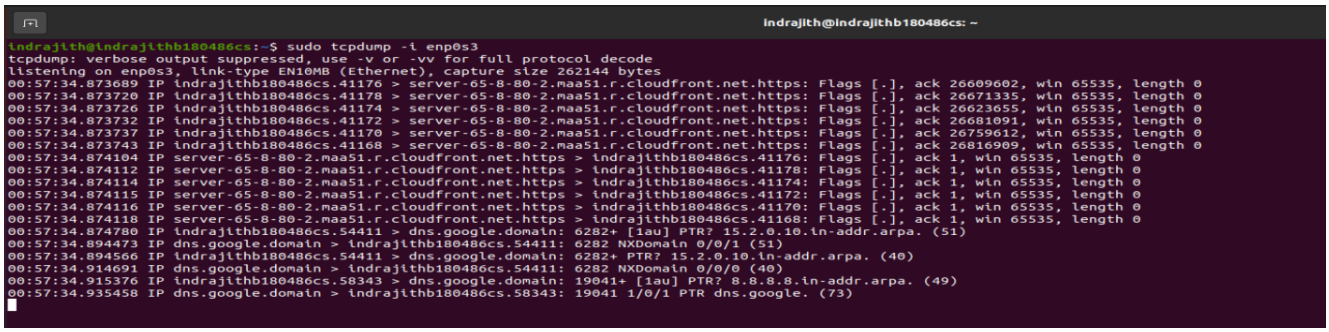


7. tcpdump

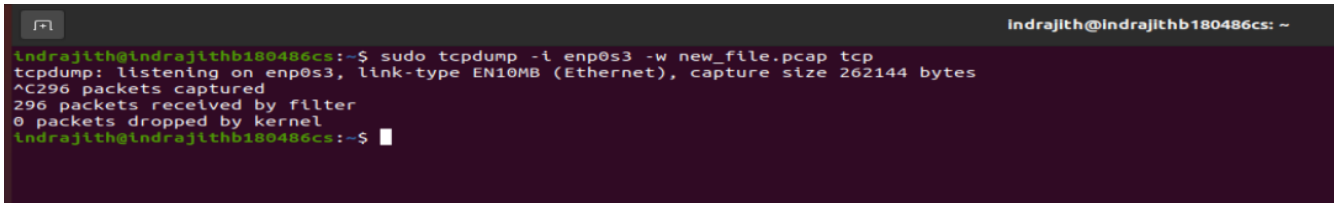
We need sudo permission to use this command. This command is used to listen to network traffic which prints the description of the contents of the packets.



We can listen to any particular interface using -i interface name command.



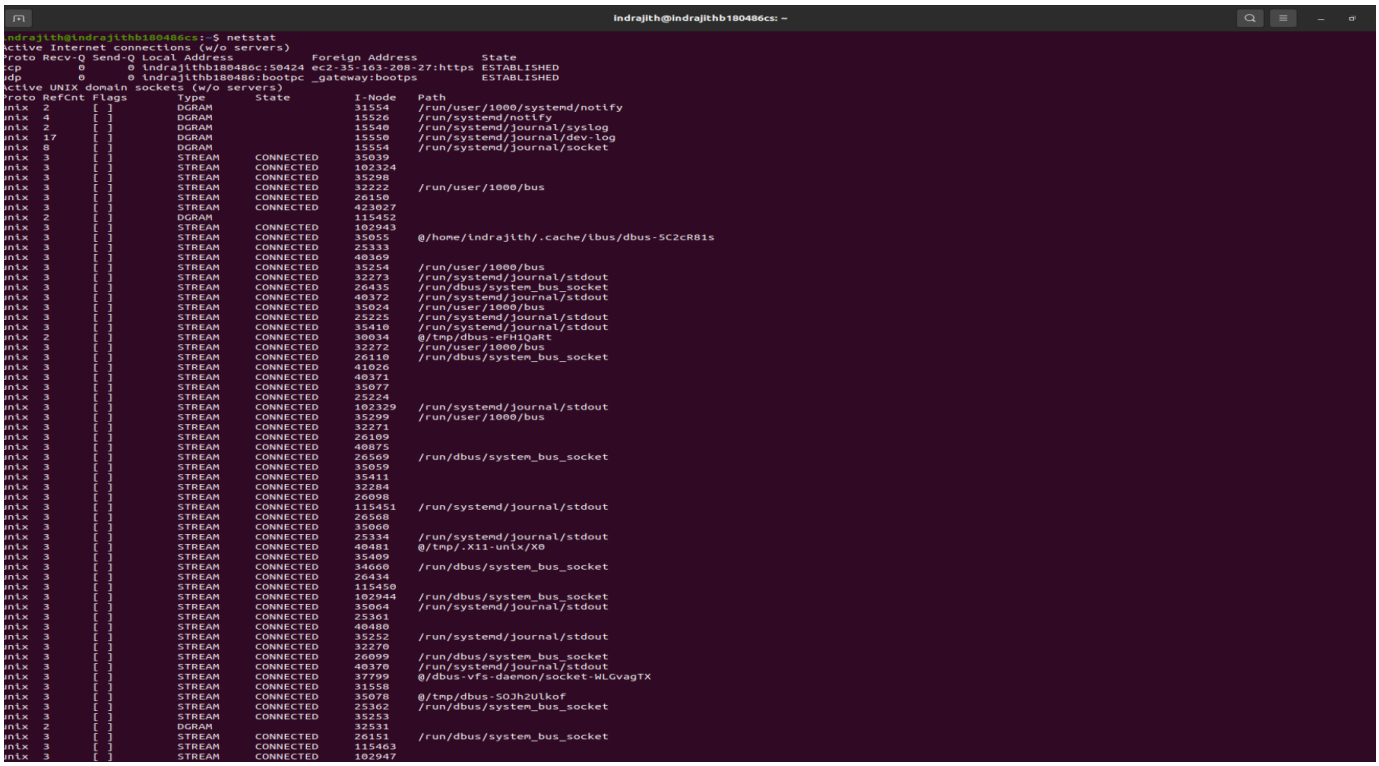
Filters can be applied to listening like specifying src and dst.
We can also apply a tcp filter using tcp.



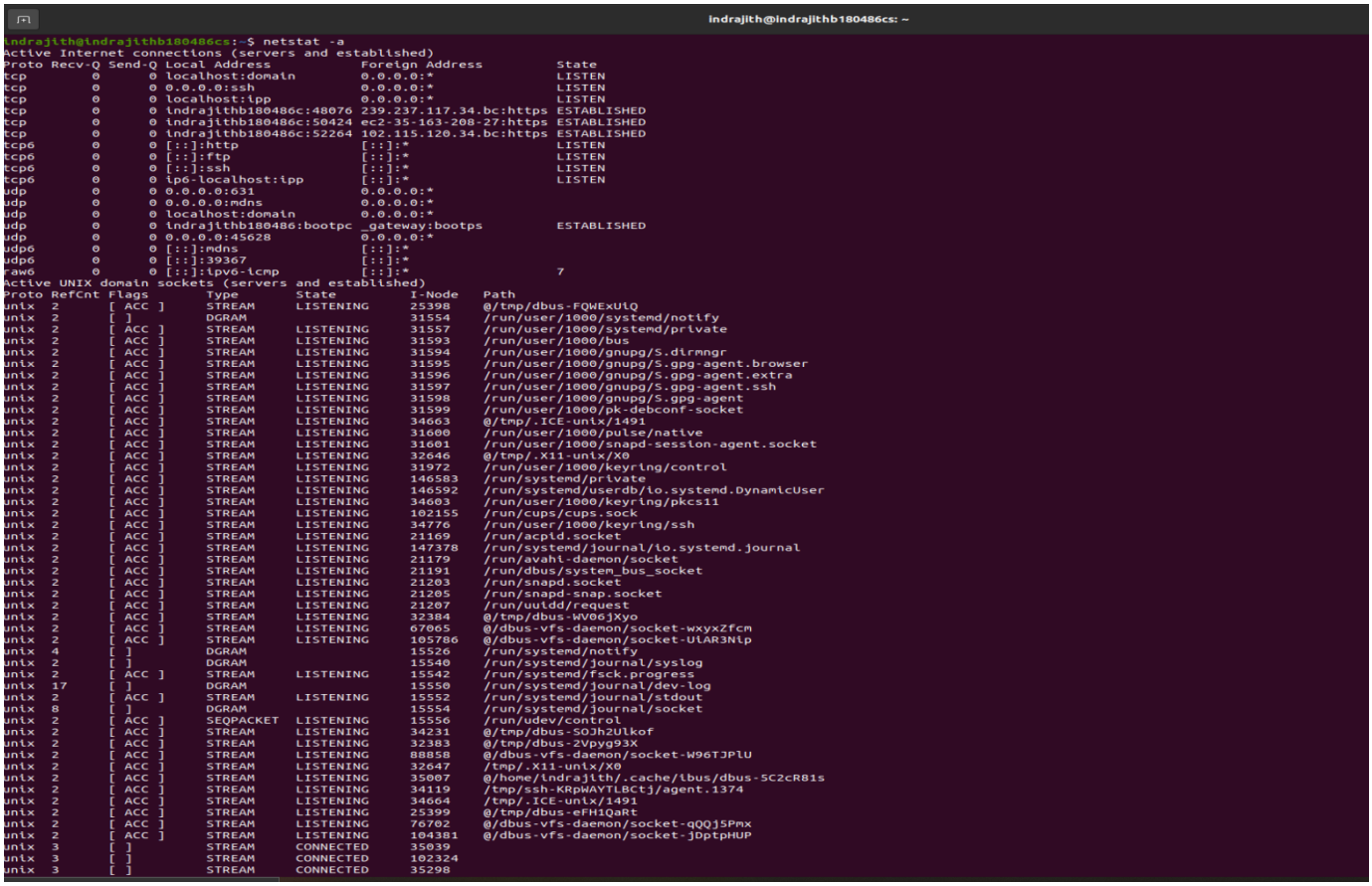
Also we can save the captured info into file using -w filename.pcap

8. netstat/ss

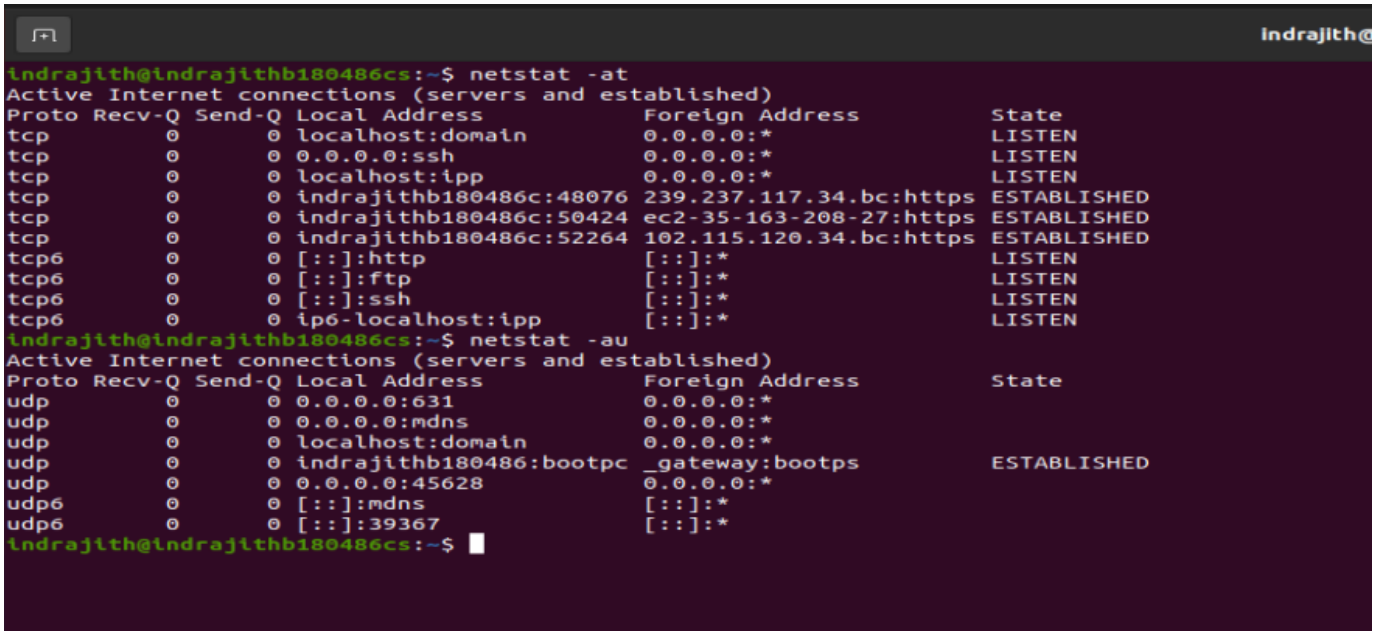
This network command prints network connections , routing tables, interface statistics etc.



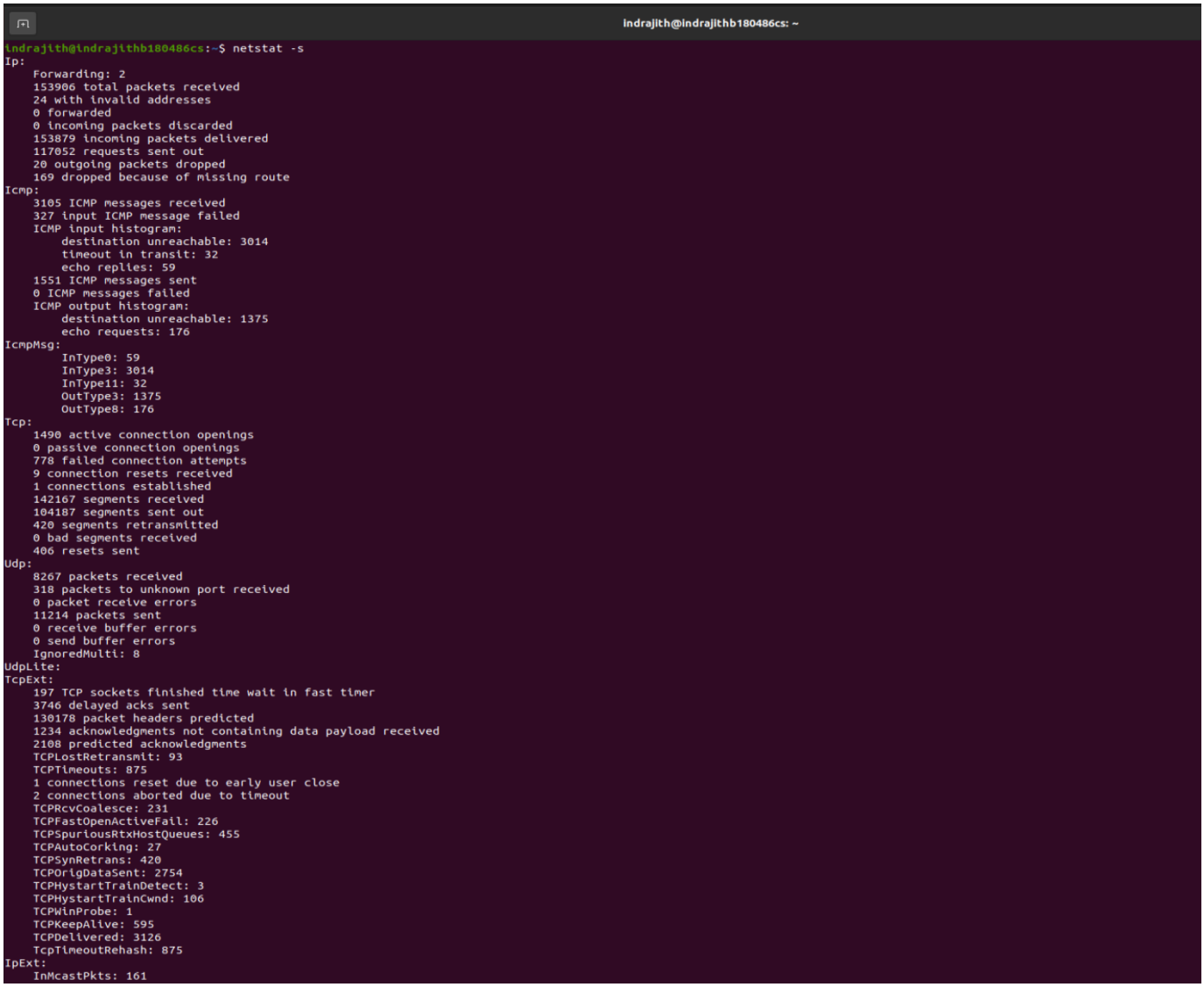
-a flag for all listening and non listening sockets.



-at for all tcp and -au for udp etc.

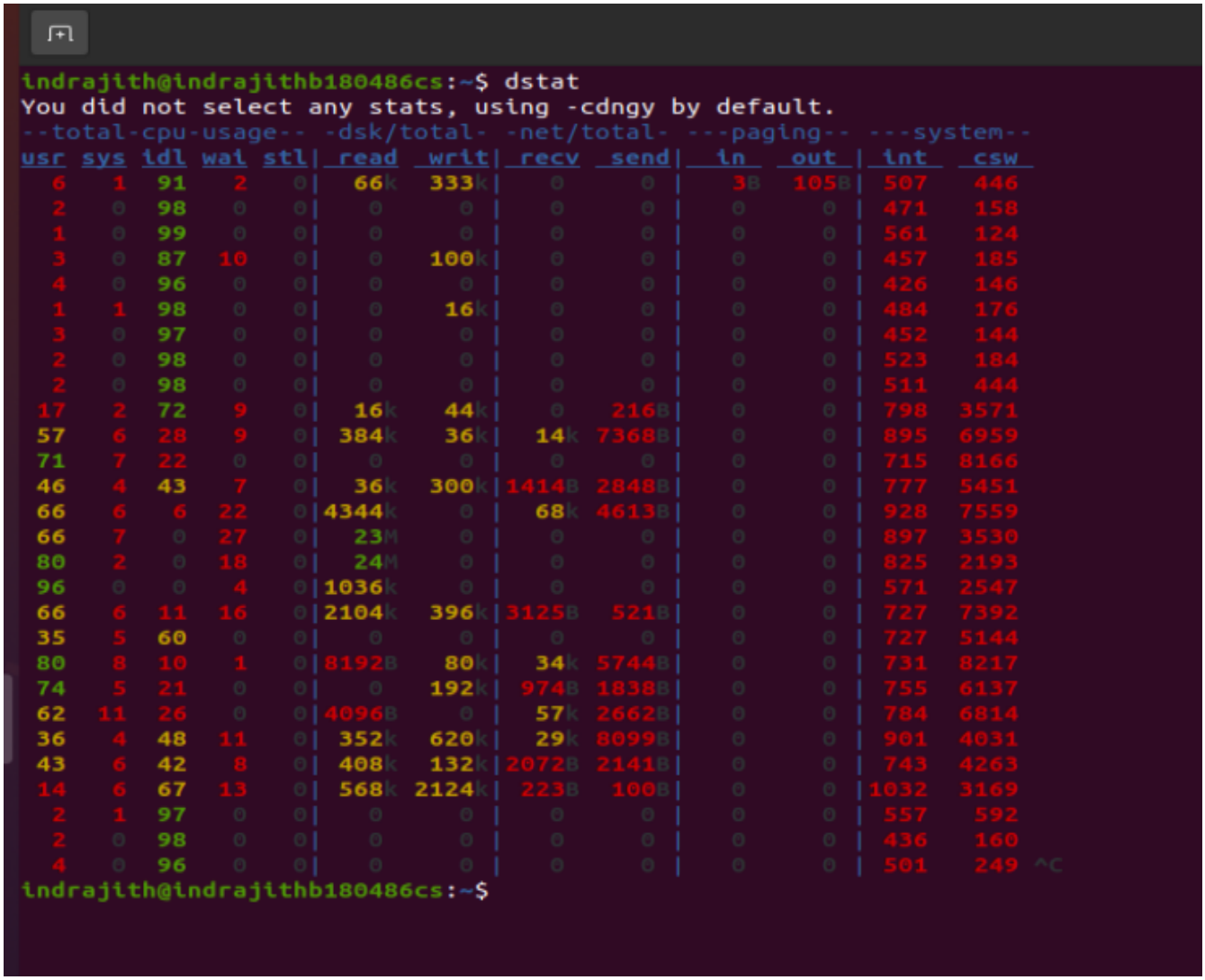


-s for statistics of all ports.



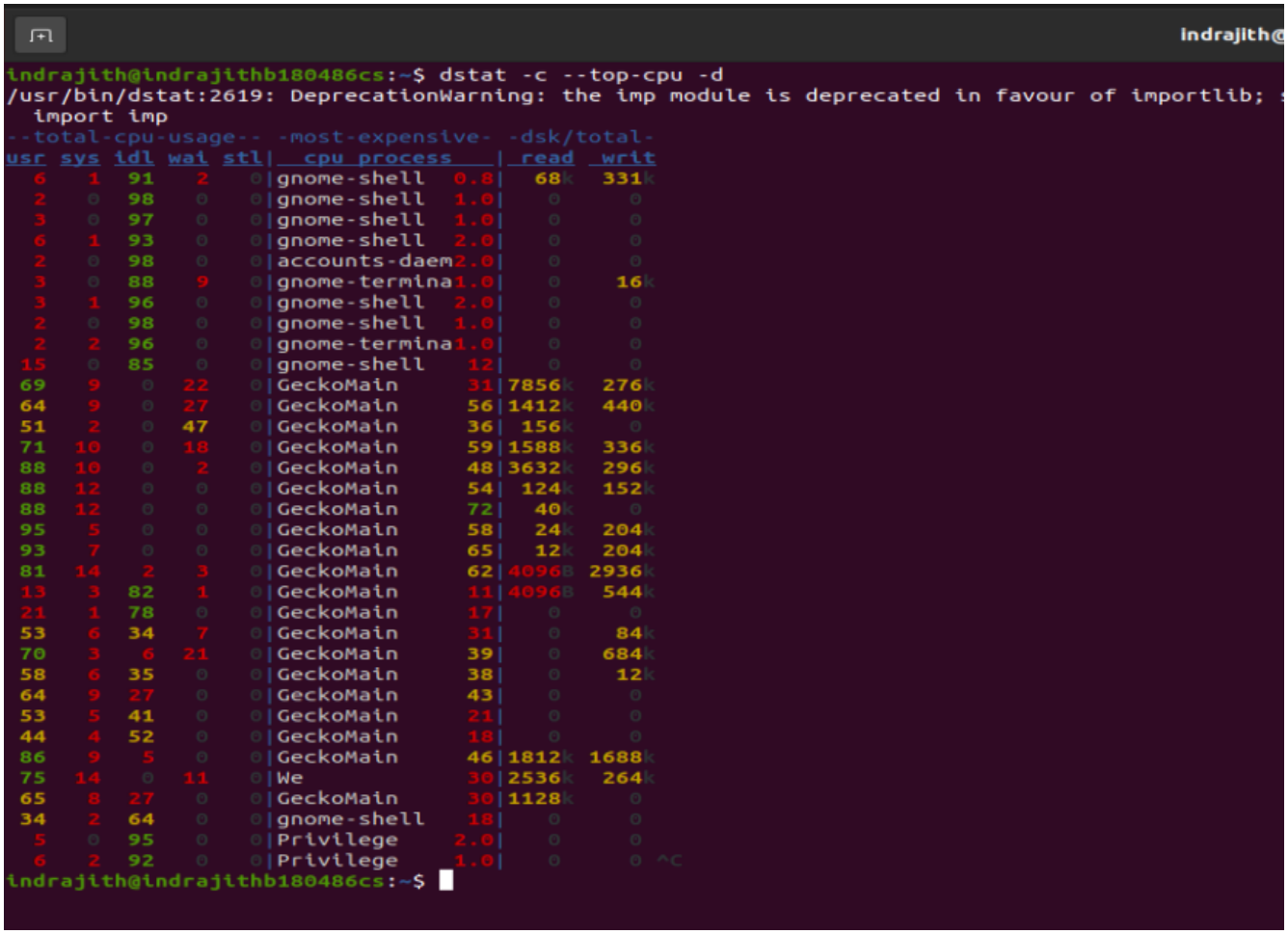
9. Dstat

It is the tool used for generating system resource statistics.



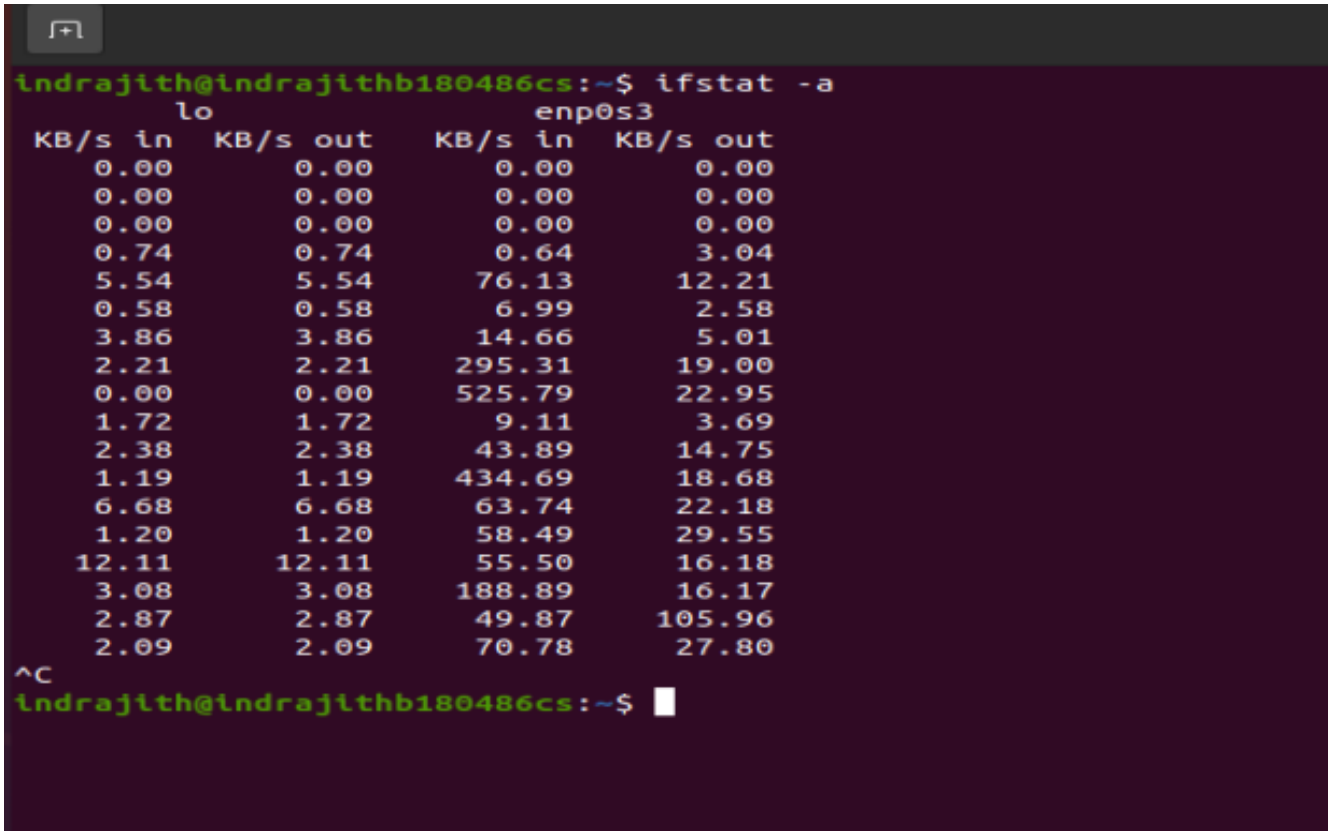
```
indrajith@indrajithb180486cs:~$ dstat
You did not select any stats, using -cdngy by default.
--total-cpu-usage-- -dsk/total- -net/total- ---paging-- ---system--
usr sys idl wai stl| read  writ| recv  send|  in   out | int   csw
  6   1  91   2   0|  66k  333k|   0     0 |  3B  105B| 507   446
  2   0  98   0   0|   0     0 |   0     0 |   0     0 | 471   158
  1   0  99   0   0|   0     0 |   0     0 |   0     0 | 561   124
  3   0  87  10   0|   0   100k|   0     0 |   0     0 | 457   185
  4   0  96   0   0|   0     0 |   0     0 |   0     0 | 426   146
  1   1  98   0   0|   0    16k|   0     0 |   0     0 | 484   176
  3   0  97   0   0|   0     0 |   0     0 |   0     0 | 452   144
  2   0  98   0   0|   0     0 |   0     0 |   0     0 | 523   184
  2   0  98   0   0|   0     0 |   0     0 |   0     0 | 511   444
 17   2  72   9   0|  16k   44k|   0   216B|   0     0 | 798  3571
 57   6  28   9   0| 384k   36k|  14k 7368B|   0     0 | 895  6959
 71   7  22   0   0|   0     0 |   0     0 |   0     0 | 715  8166
 46   4  43   7   0|  36k  300k|1414B 2848B|   0     0 | 777  5451
 66   6   6  22   0|4344k    0 |  68k 4613B|   0     0 | 928  7559
 66   7   0  27   0|  23M    0 |   0     0 |   0     0 | 897  3530
 80   2   0  18   0|  24M    0 |   0     0 |   0     0 | 825  2193
 96   0   0   4   0|1036k    0 |   0     0 |   0     0 | 571  2547
 66   6  11  16   0|2104k  396k|3125B  521B|   0     0 | 727  7392
 35   5  60   0   0|   0     0 |   0     0 |   0     0 | 727  5144
 80   8  10   1   0|8192B   80k|  34k 5744B|   0     0 | 731  8217
 74   5  21   0   0|   0   192k| 974B 1838B|   0     0 | 755  6137
 62  11  26   0   0|4096B    0 |  57k 2662B|   0     0 | 784  6814
 36   4  48  11   0| 352k  620k|  29k 8099B|   0     0 | 901  4031
 43   6  42   8   0| 408k  132k|2072B 2141B|   0     0 | 743  4263
 14   6  67  13   0| 568k 2124k| 223B  100B|   0     0 |1032  3169
  2   1  97   0   0|   0     0 |   0     0 |   0     0 | 557   592
  2   0  98   0   0|   0     0 |   0     0 |   0     0 | 436   160
  4   0  96   0   0|   0     0 |   0     0 |   0     0 | 501   249 ^C
indrajith@indrajithb180486cs:~$
```

-c flag is for cpu stats and -d for disk stats and also we can choose the top processes in cpu using –top-cpu flag

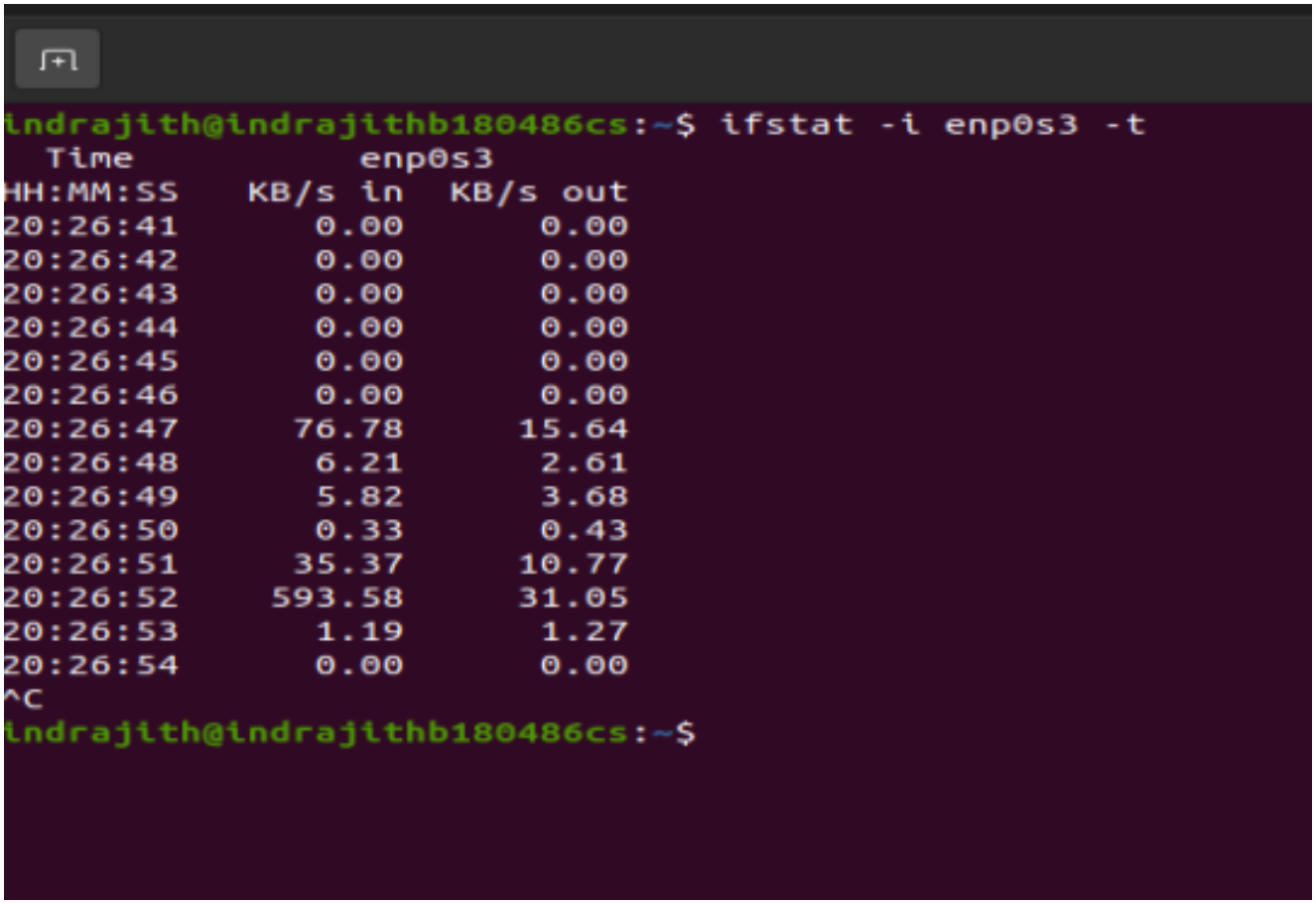


10. ifstat

ifstat command monitors non-loop network interfaces that are active. Flag -a is used to enable monitoring for all the interfaces.

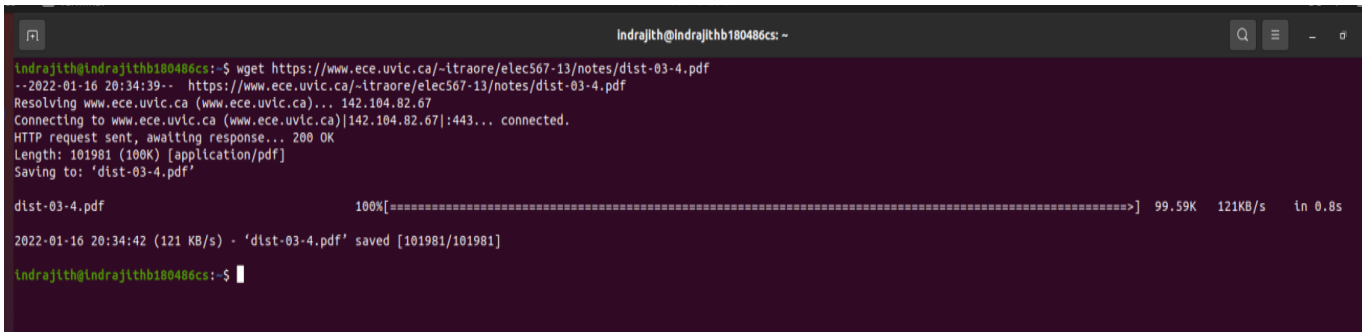


-i interface name is used to enable monitoring on a specific interface.
-t to average over each second.

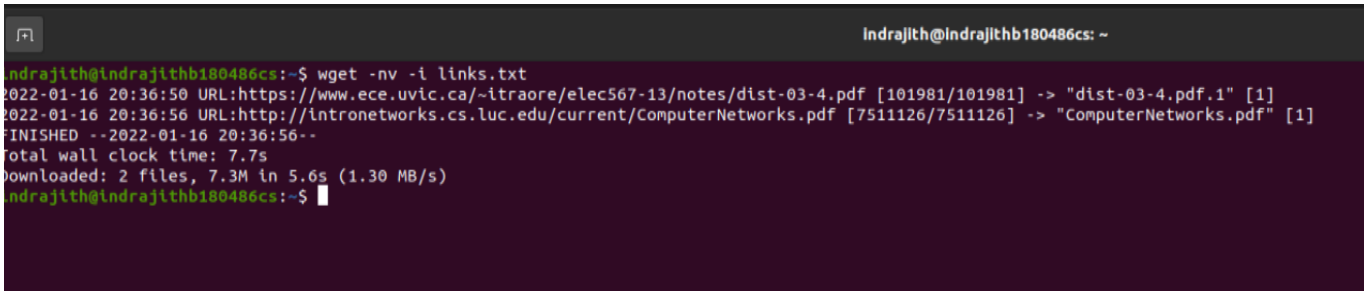


11. wget

wget command is used to download files from the internet without the use of an interactive gui. We specify the url of the file to download.



We can add multiple file links to a txt file and then use the -i filename to download multiple files that is given in the txt file.
-nv flag can be used to turn off the verbose output when we need to see only the summary.



12. tracepath

This traces the path to the destination ip. This is similar to traceroute but with lesser options thus dont need sudo permission.
-m flag can be used to decide the maximum number of hops.