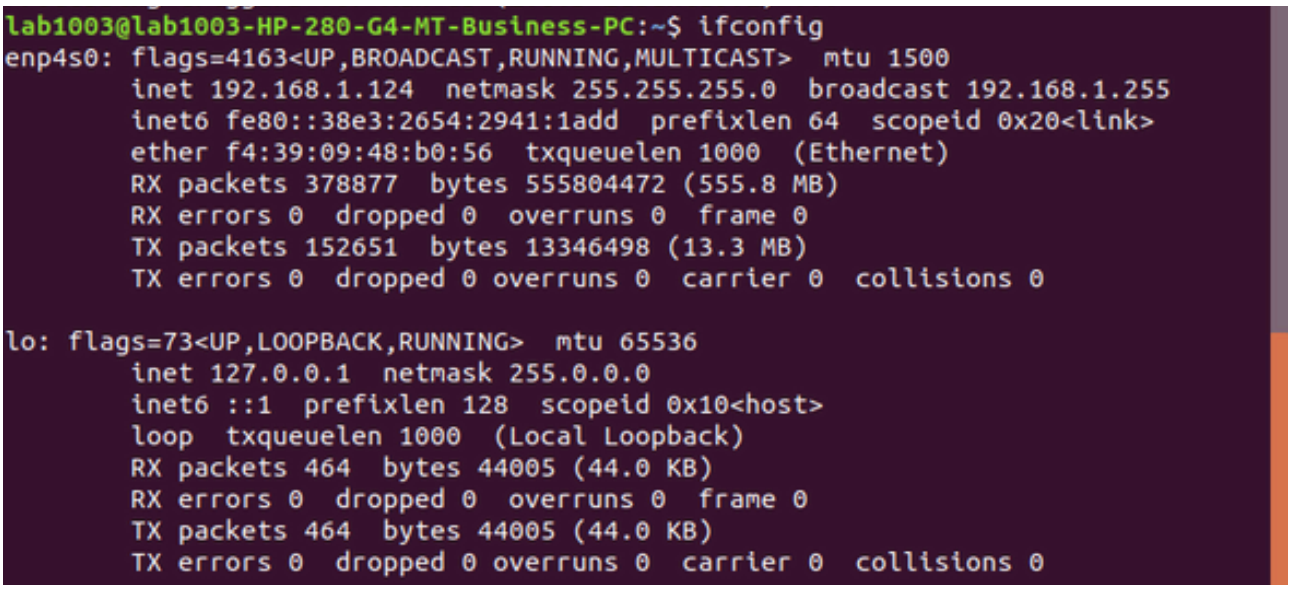
1. Ifconfig



Used to view information about all network interfaces on your Linux system

1. ifconfig -a

To get info about both active and inactive network interfaces, run ifconfig with the -a option

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ ifconfig -a
enp4s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.124  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::38e3:2654:2941:1add  prefixlen 64  scopeid 0x20<link>
        ether f4:39:09:48:b0:56  txqueuelen 1000  (Ethernet)
        RX packets 387038  bytes 557076809 (557.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 153479  bytes 13412208 (13.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 593  bytes 56956 (56.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 593  bytes 56956 (56.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

1. ifconfig -s

Use the -s flag with ifconfig to display a concise summary of every active interface

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ ifconfig -s
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp4s0    1500   387402      0      0 0        153493      0      0      0 BMRU
lo       65536      597      0      0 0           597      0      0      0 LRU
```

1. ifconfig -v

As opposed to the -s flag, the verbose option (-v) prints a more detailed output. Depending on the system, the outcome is either the same as ifconfig without arguments or slightly more in-depth.

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ ifconfig -v
enp4s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.124  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::38e3:2654:2941:1add  prefixlen 64  scopeid 0x20<link>
        ether f4:39:09:48:b0:56  txqueuelen 1000  (Ethernet)
        RX packets 387582  bytes 557116000 (557.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 153498  bytes 13413315 (13.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 597  bytes 57612 (57.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 597  bytes 57612 (57.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

1. ifconfig | grep inet

The grep command is used to search for patterns in text. When you pipe the output of ifconfig to grep, it will search for all lines that contain the string "inet". This will print all of the IP addresses that are assigned to the system's interfaces.

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ ifconfig | grep inet
        inet 192.168.1.124  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::38e3:2654:2941:1add  prefixlen 64  scopeid 0x20<link>
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
```

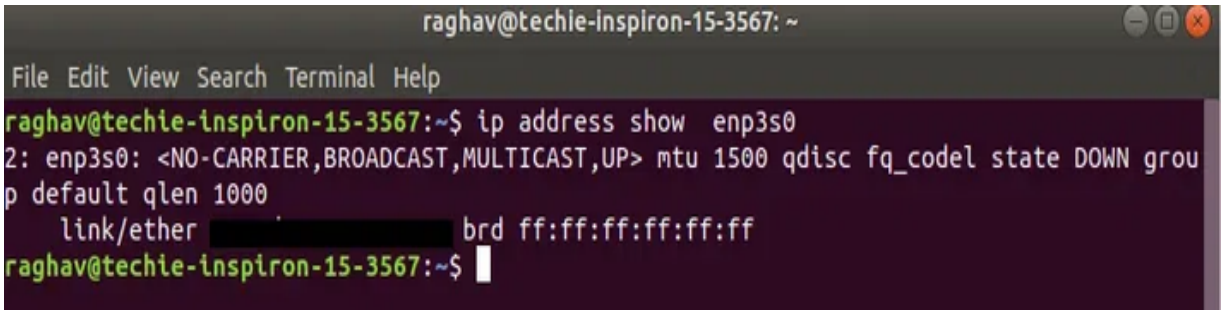
1. ip address

This option is used to show all IP addresses associated with all network devices.

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp4s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether f4:39:09:48:b0:56 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.124/24 brd 192.168.1.255 scope global dynamic noprefixroute e
np4s0
       valid_lft 5207sec preferred_lft 5207sec
    inet6 fe80::38e3:2654:2941:1add/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

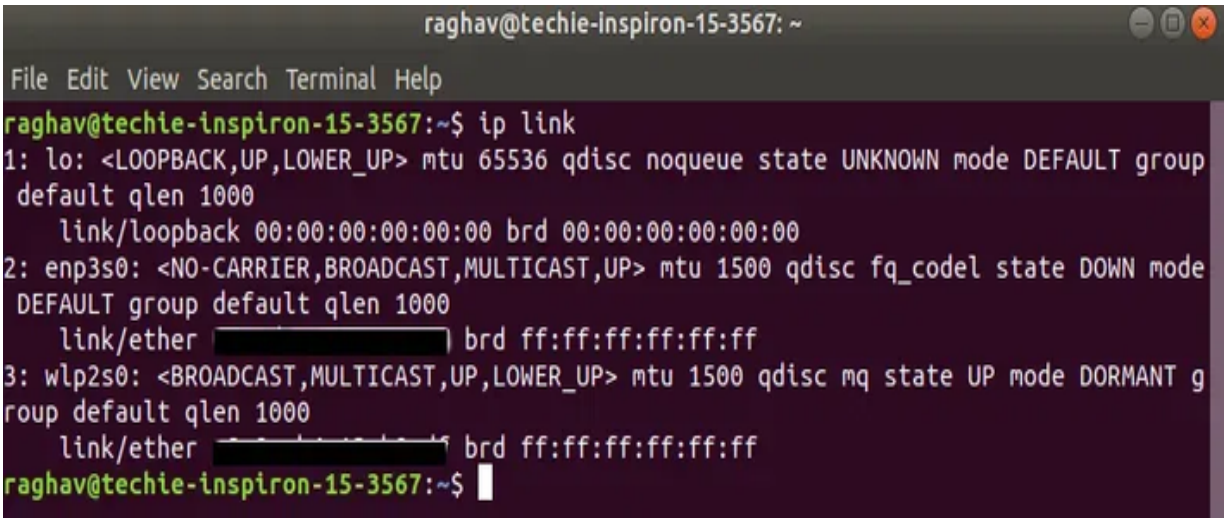
1. ip addr show enp3s0

Use if we want to view the information of any particular interface



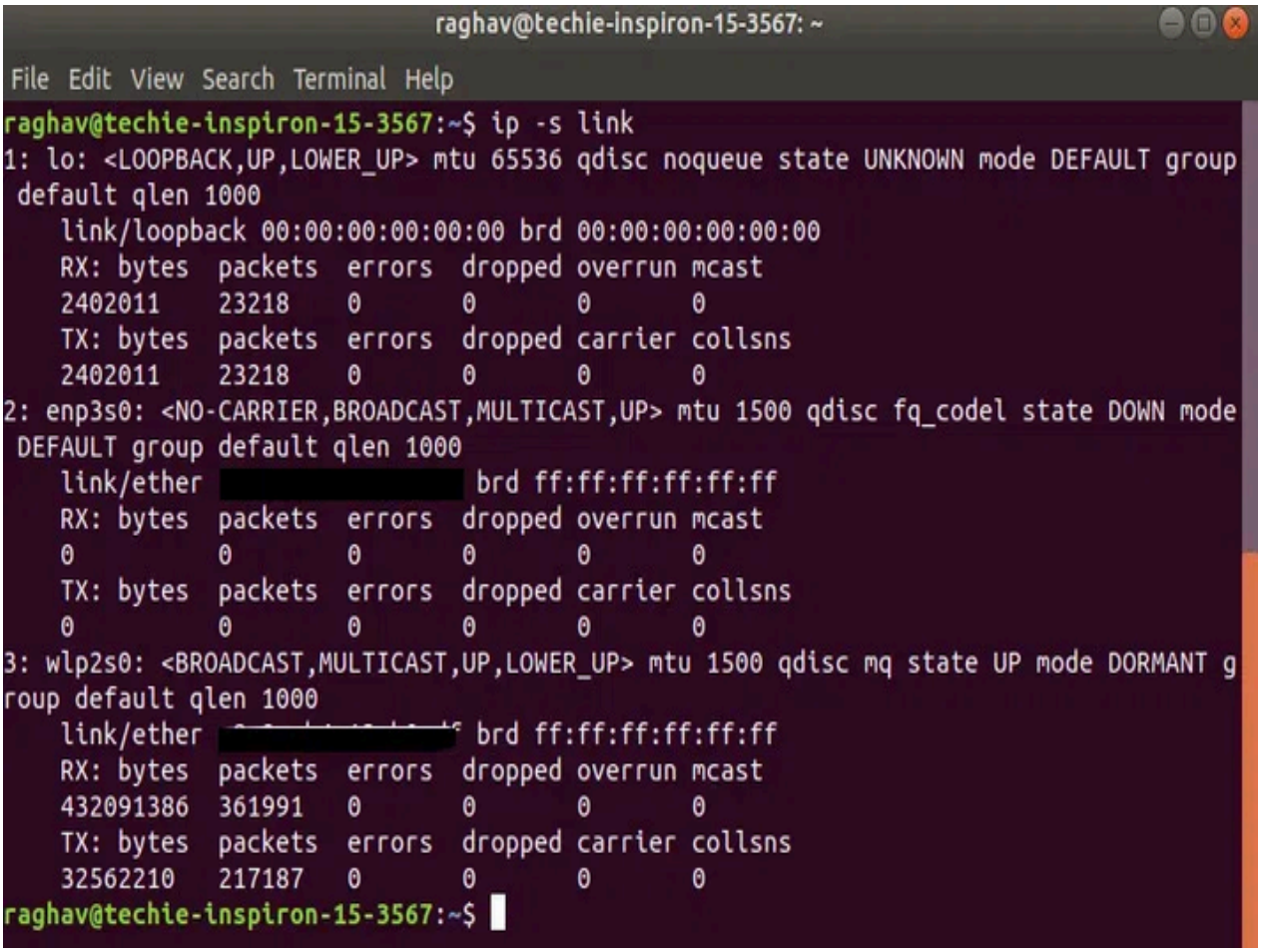
1. ip link

It is used to display link layer information



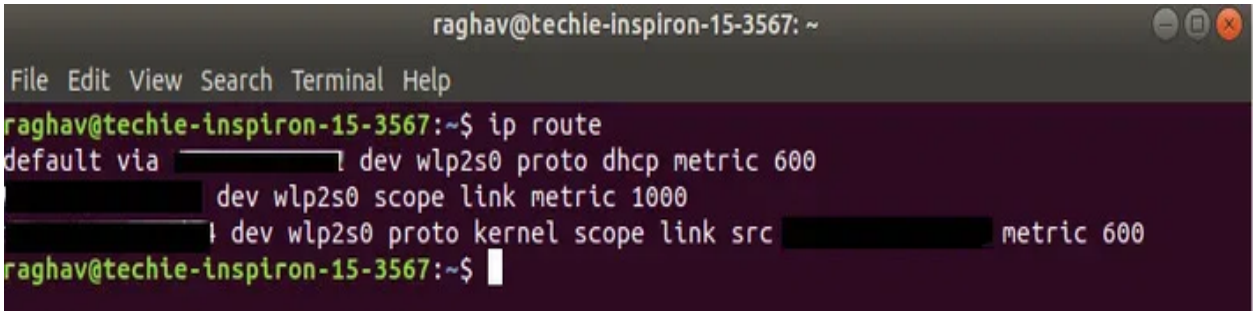
1. ip -s link

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



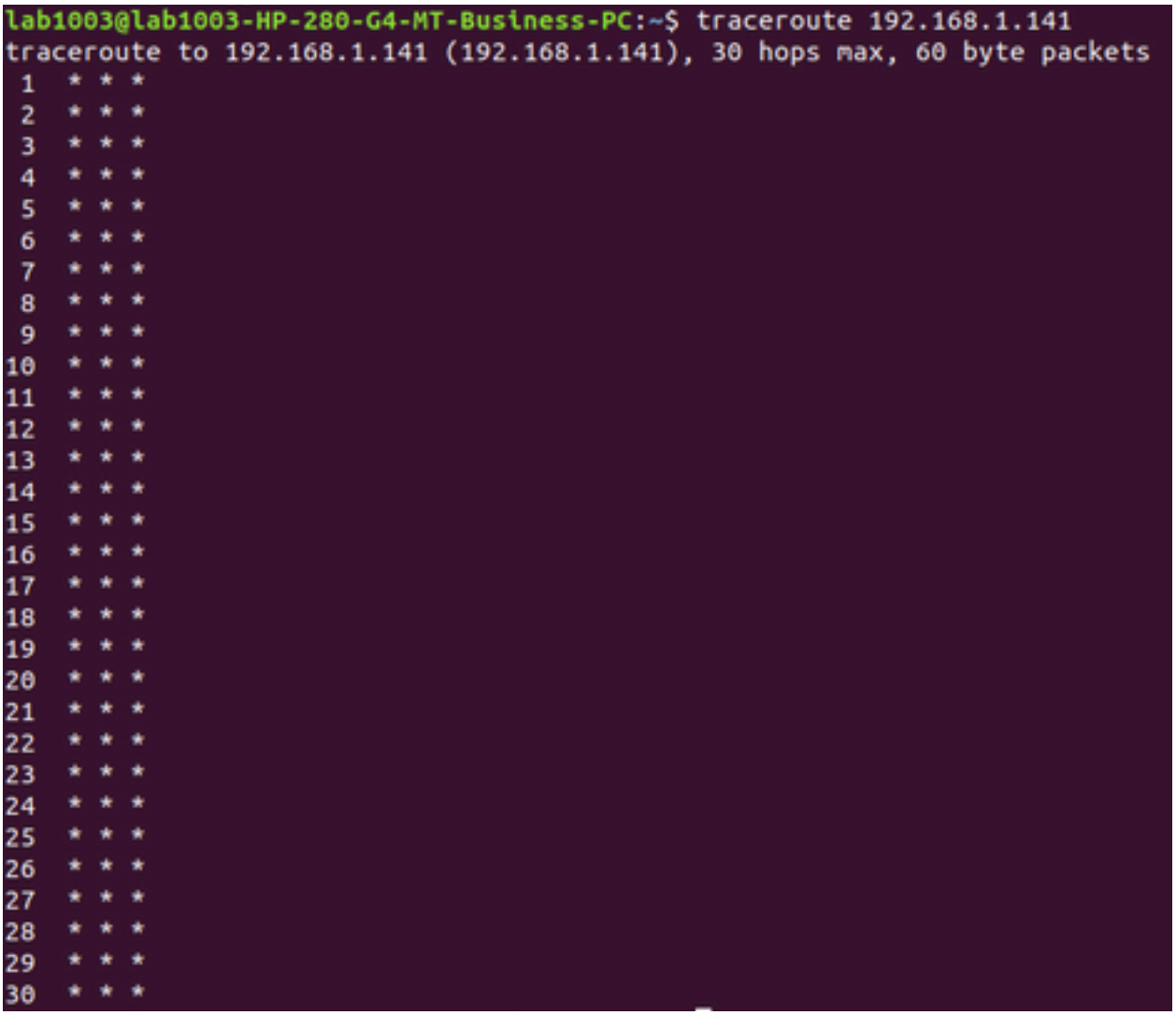
1. ip route

This command helps you to see the route packets your network will take as set in your routing table. The first entry is the default route.



1. traceroute 192.168.1.141

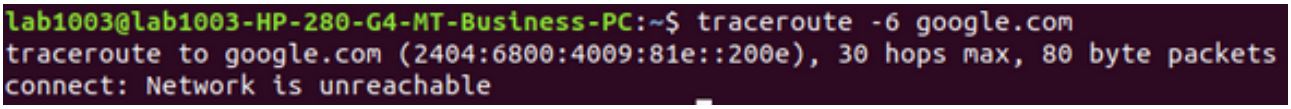
tracks the path a packet takes from source to destination on an IP network


lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ traceroute 192.168.1.141
traceroute to 192.168.1.141 (192.168.1.141), 30 hops max, 60 byte packets
1 * * *
2 * * *
3 * * *
4 * * *
5 * * *
6 * * *
7 * * *
8 * * *
9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *

1. traceroute -4 google.com

Use ip version 4 i.e. use IPv4

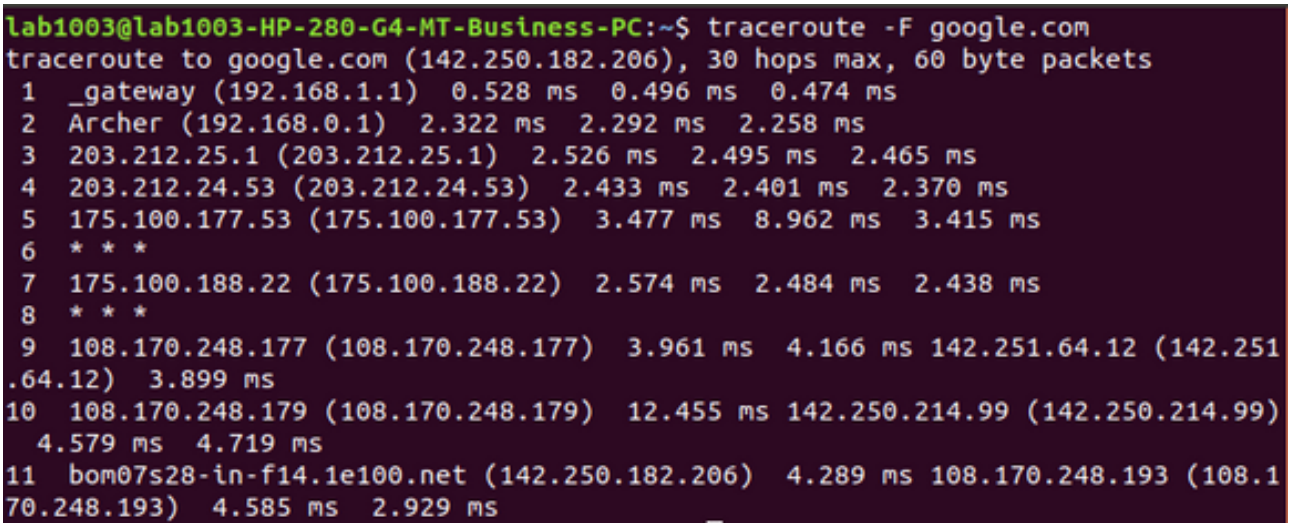
1. traceroute -6 google.com



use ip version 6 i.e. use IPv6

1. traceroute -F google.com

Do not fragment packet



1. traceroute -m 5 google.com

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ traceroute -m 5 google.com
traceroute to google.com (142.250.182.206), 5 hops max, 60 byte packets
 1  _gateway (192.168.1.1)  0.489 ms  0.454 ms  0.431 ms
 2  * * *
 3  * * *
 4  * * *
 5  175.100.177.53 (175.100.177.53)  3.575 ms  3.544 ms  3.756 ms
```

Set the max number of hops for the packet to reach the destination.Default value is 30.

(ping reference – www.geeksforgeeks.org)

1. ping www.google.com

To check your internet connection

```
administrator@GFG19566-LAPTOP:~/practice$ ping www.google.com
PING www.google.com (142.250.194.100) 56(84) bytes of data.
64 bytes from del12s04-in-f4.1e100.net (142.250.194.100): icmp_seq=1 ttl=116 time=1.60 ms
64 bytes from del12s04-in-f4.1e100.net (142.250.194.100): icmp_seq=2 ttl=116 time=1.15 ms
64 bytes from del12s04-in-f4.1e100.net (142.250.194.100): icmp_seq=3 ttl=116 time=1.17 ms
64 bytes from del12s04-in-f4.1e100.net (142.250.194.100): icmp_seq=4 ttl=116 time=1.14 ms
^C
--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.136/1.264/1.599/0.193 ms
```

1. ping -c 2 www.geeksforgeeks.org

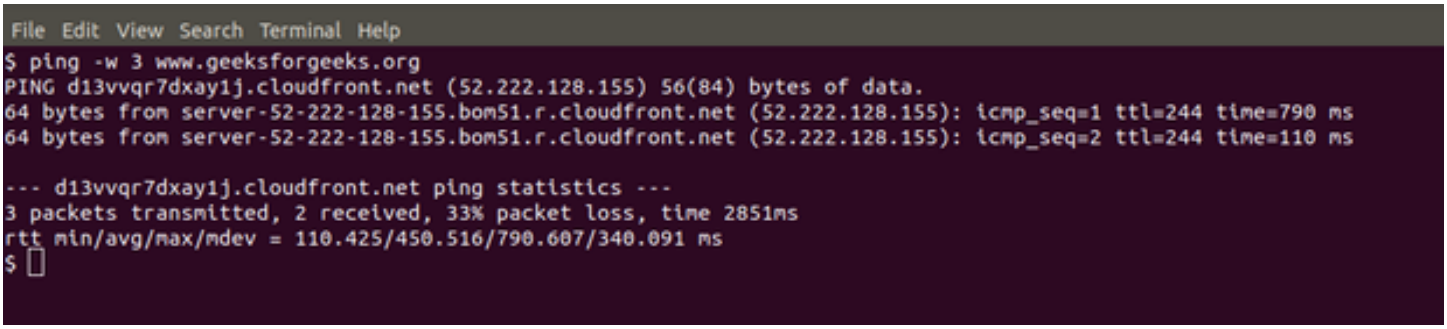
used to define the number of packets to send to the server/host

```
administrator@GFG19566-LAPTOP:~/practice$ ping -c 2 www.geeksforgeeks.org
PING a1991.dscr.akamai.net (23.223.243.58) 56(84) bytes of data.
64 bytes from a23-223-243-58.deploy.static.akamaitechnologies.com (23.223.243.58): icmp_seq=1
 ttl=54 time=4.70 ms
64 bytes from a23-223-243-58.deploy.static.akamaitechnologies.com (23.223.243.58): icmp_seq=2
 ttl=54 time=4.71 ms

--- a1991.dscr.akamai.net ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 4.703/4.704/4.706/0.001 ms
```

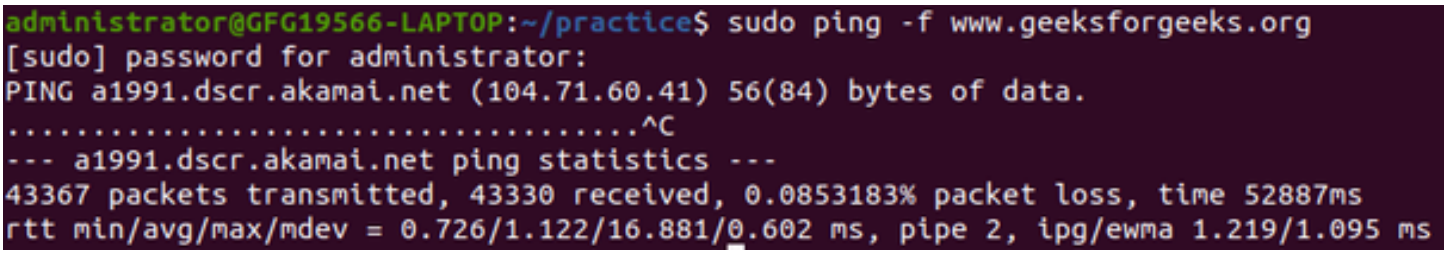
1. ping -w 3 www.geeksforgeeks.org

This command instructs the system to stop pinging the specified website after waiting for 3 seconds.



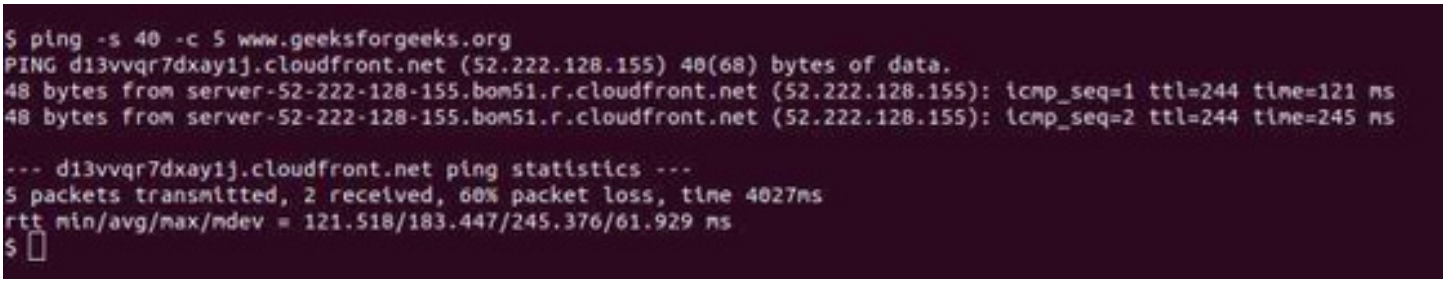
1. ping -f www.geeksforgeeks.org

To flood a network with PING packets for testing network performance, use the `-f` option with the PING command.



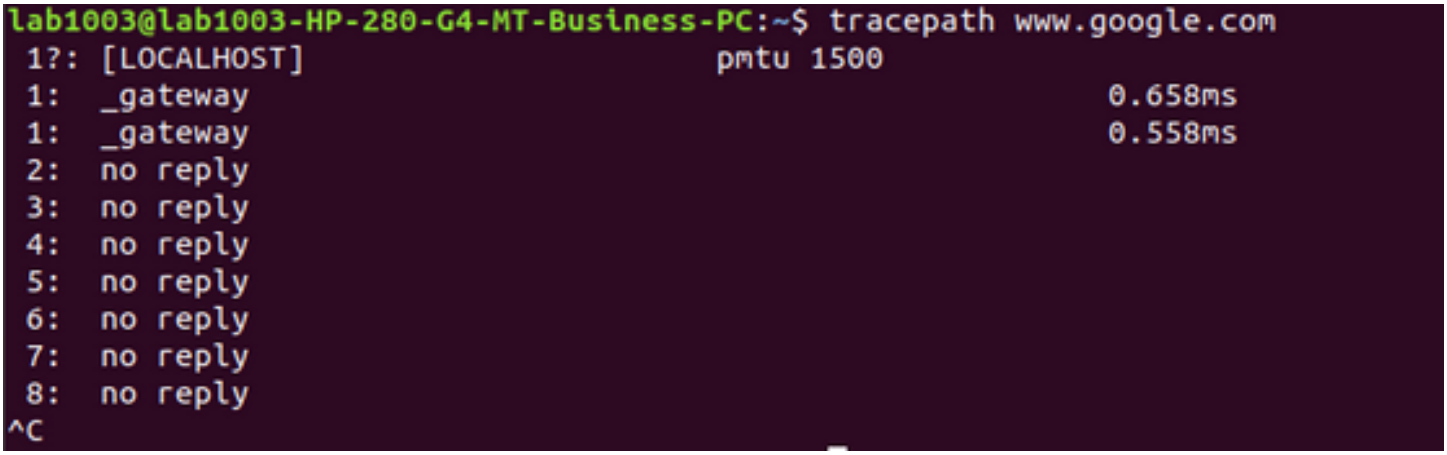
1. ping -s 40 www.geeksforgeeks.org

we can send light and heavy packet to host by using -s option.



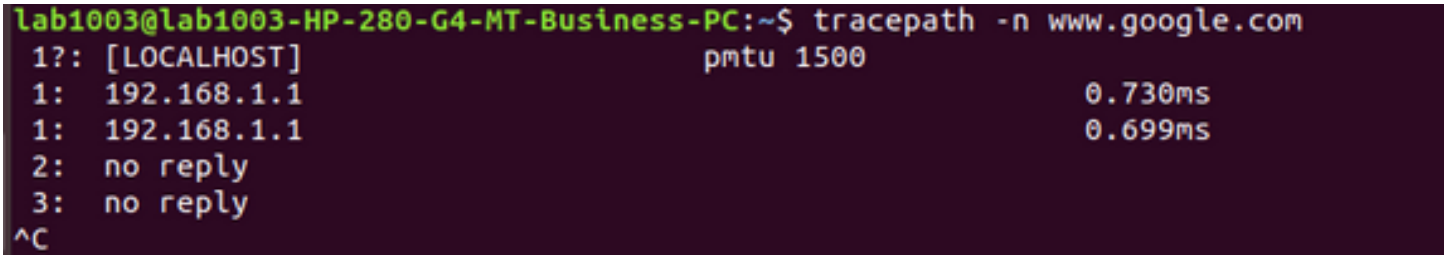
1. tracepath

It will print the general syntax of the command along with the various options that can be used with the tracepath command as well as gives a brief description about each option.



1. tracepath -n www.google.com

This option prints primarily IP addresses numerically



1. tracepath -b www.makemytrip.com

This option print both of host names and IP addresses

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ tracepath -b www.google.com
 1?: [LOCALHOST]                      pmtu 1500
 1:  _gateway (192.168.1.1)                                0.745ms
 1:  _gateway (192.168.1.1)                                0.724ms
 2:  no reply
 3:  no reply
 4:  no reply
^C
```

1. tracepath -m 31 www.google.com

This option will set maximum hops (or maximum TTLs) to max_hops instead of 30

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ tracepath -m 31 www.google.com
 1?: [LOCALHOST]                      pmtu 1500
 1:  _gateway                                              0.837ms
 1:  _gateway                                              0.728ms
 2:  no reply
 3:  no reply
 4:  no reply
 5:  no reply
 6:  no reply
 7:  no reply
 8:  no reply
 9:  no reply
10:  no reply
^C
```

1. tracepath -p 8080 www.google.com

This option will set the initial destination port to use

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ tracepath -p 8080 www.google.com
 1?: [LOCALHOST]                      pmtu 1500
 1:  _gateway                                              0.748ms
 1:  _gateway                                              0.833ms
 2:  Archer                                                1.490ms
 3:  Archer                                                1.351ms pmtu 1480
 3:  203.212.25.1                                          1.923ms
 4:  203.212.24.53                                         2.093ms
 5:  175.100.177.53                                       11.035ms
 6:  172.16.2.202                                         44.995ms
 7:  175.100.188.22                                        3.164ms asymm 11
 8:  no reply
```

1. netstat

generates displays that show network status and protocol statistics

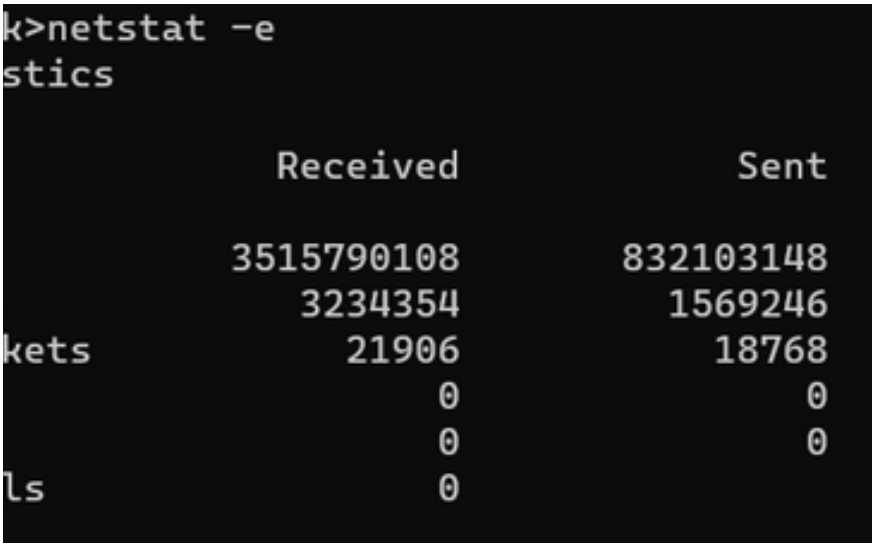
```
>netstat

ns

ddress          Foreign Address        State
.1:49670        LAPTOP-6BJ1JG3N:49671  ESTABLISHED
.1:49671        LAPTOP-6BJ1JG3N:49670  ESTABLISHED
.1:49672        LAPTOP-6BJ1JG3N:49673  ESTABLISHED
.1:49673        LAPTOP-6BJ1JG3N:49672  ESTABLISHED
.29.184:58220   20.198.118.190:https   ESTABLISHED
.29.184:58260   20.198.119.84:https    ESTABLISHED
.29.184:58975   152.195.38.76:http     LAST_ACK
.29.184:59462   20.212.88.117:https    ESTABLISHED
.29.184:59545   1drv:https             ESTABLISHED
.29.184:59547   1drv:https             ESTABLISHED
.29.184:59555   20.189.173.12:https    ESTABLISHED
.29.184:59560   51.116.253.168:https   TIME_WAIT
.29.184:59566   52.109.124.29:https    TIME_WAIT
.29.184:59569   52.109.124.29:https    TIME_WAIT
.29.184:59577   52.178.17.234:https    ESTABLISHED
.29.184:59579   13.107.4.254:https     ESTABLISHED
.29.184:59580   152.195.38.76:http     ESTABLISHED
.29.184:59583   204.79.197.222:https   ESTABLISHED
.29.184:59584   51.104.15.253:https    ESTABLISHED
01:1:6019:d949:70fa:542a:ce47]:58299  sh-in-f188:5228        ESTABLISHED
01:1:6019:d949:70fa:542a:ce47]:58349  [2606:4700:8ca3:98df:bdd7:7a:3150:c532]:https  CLOSE_WAIT
01:1:6019:d949:70fa:542a:ce47]:58350  bom07s28-in-x03:http   CLOSE_WAIT
01:1:6019:d949:70fa:542a:ce47]:58351  [2606:4700:8d70:bc89:5ed7:b41:3fd7:3718]:https  CLOSE_WAIT
01:1:6019:d949:70fa:542a:ce47]:59175  [2603:1063:2202:14::3]:https  ESTABLISHED
01:1:6019:d949:70fa:542a:ce47]:59298  [2606:4700:8d72:883b:10d7:b41:6810:e095]:https  ESTABLISHED
01:1:6019:d949:70fa:542a:ce47]:59321  whatsapp-cdn6-shv-01-pnq1:https  ESTABLISHED
01:1:6019:d949:70fa:542a:ce47]:59570  [2405:200:1630:a00::312c:d929]:https  ESTABLISHED
01:1:6019:d949:70fa:542a:ce47]:59571  [2405:200:1630:a00::312c:d929]:https  CLOSE_WAIT
01:1:6019:d949:70fa:542a:ce47]:59574  [2405:200:1630:a00::312c:d91a]:https  ESTABLISHED
01:1:6019:d949:70fa:542a:ce47]:59575  [2405:200:1630:a00::312c:d91a]:https  CLOSE_WAIT
01:1:6019:d949:70fa:542a:ce47]:59576  [2603:1046:c04:c0f::2]:https  ESTABLISHED
01:1:6019:d949:70fa:542a:ce47]:59581  [2603:1030:13:201::254]:https  ESTABLISHED
01:1:6019:d949:70fa:542a:ce47]:59582  [2603:1063:27:2::254]:https  ESTABLISHED
```

1. netstat -e

displays Ethernet statistics, including the number of bytes and packets sent and received.



1. netstat -n

displays network connections and listening ports in numerical format (IP addresses and port numbers) instead of resolving them to hostnames and service names.

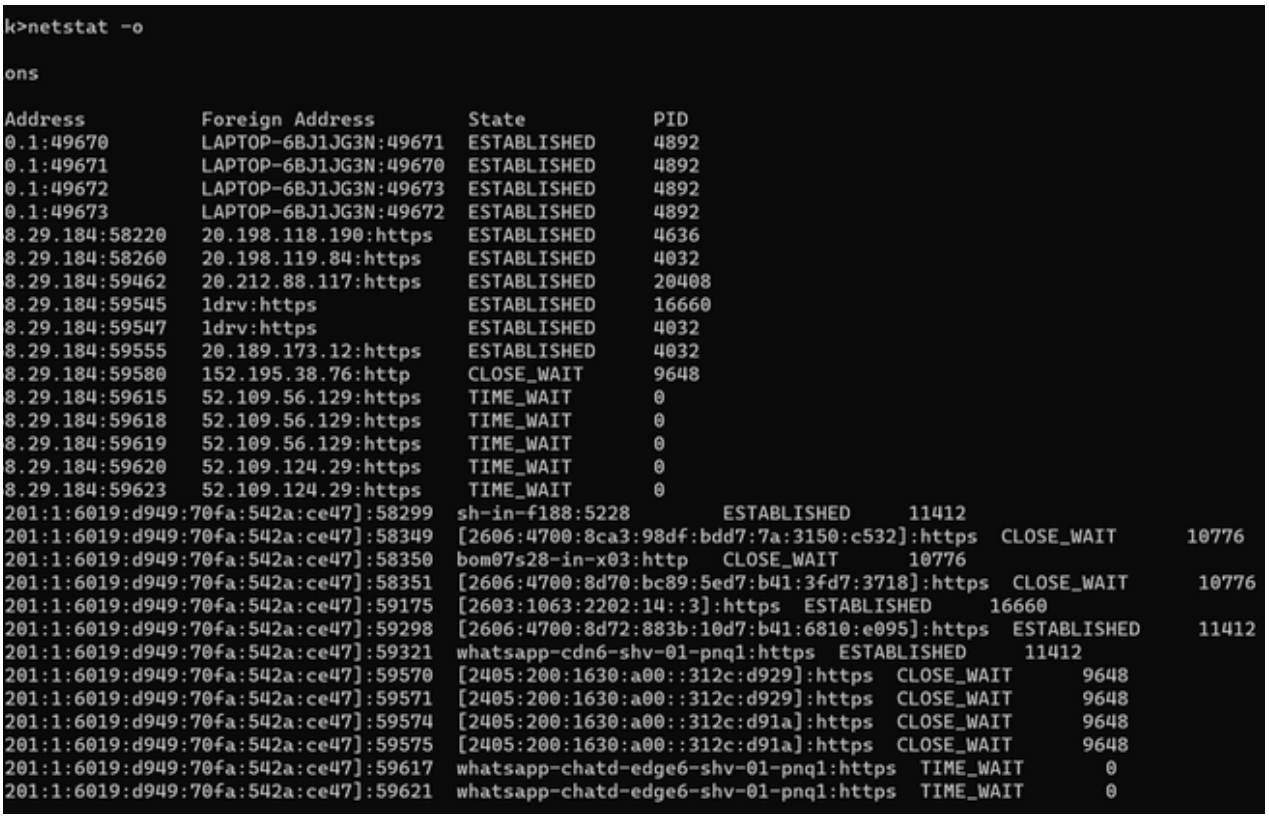
```
k>netstat -n

ons

Address          Foreign Address        State
0.1:49670        127.0.0.1:49671        ESTABLISHED
0.1:49671        127.0.0.1:49670        ESTABLISHED
0.1:49672        127.0.0.1:49673        ESTABLISHED
0.1:49673        127.0.0.1:49672        ESTABLISHED
8.29.184:58220   20.198.118.190:443     ESTABLISHED
8.29.184:58260   20.198.119.84:443      ESTABLISHED
8.29.184:59462   20.212.88.117:443      ESTABLISHED
8.29.184:59545   13.107.42.12:443       ESTABLISHED
8.29.184:59547   13.107.42.12:443       ESTABLISHED
8.29.184:59555   20.189.173.12:443      ESTABLISHED
8.29.184:59580   152.195.38.76:80       CLOSE_WAIT
8.29.184:59609   52.109.124.29:443      TIME_WAIT
8.29.184:59613   52.109.56.129:443      TIME_WAIT
8.29.184:59614   157.240.242.61:443     TIME_WAIT
8.29.184:59615   52.109.56.129:443      TIME_WAIT
8.29.184:59618   52.109.56.129:443      TIME_WAIT
8.29.184:59619   52.109.56.129:443      TIME_WAIT
201:1:6019:d949:70fa:542a:ce47]:58299  [2404:6800:4003:c1c::bc]:5228  ESTABLISHED
201:1:6019:d949:70fa:542a:ce47]:58349  [2606:4700:8ca3:98df:bdd7:7a:3150:c532]:443  CLOSE_WAIT
201:1:6019:d949:70fa:542a:ce47]:58350  [2404:6800:4009:81e::2003]:80  CLOSE_WAIT
201:1:6019:d949:70fa:542a:ce47]:58351  [2606:4700:8d70:bc89:5ed7:b41:3fd7:3718]:443  CLOSE_WAIT
201:1:6019:d949:70fa:542a:ce47]:59175  [2603:1063:2202:14::3]:443  ESTABLISHED
201:1:6019:d949:70fa:542a:ce47]:59298  [2606:4700:8d72:883b:10d7:b41:6810:e095]:443  ESTABLISHED
201:1:6019:d949:70fa:542a:ce47]:59321  [2a03:2880:f26e:c2:face:b00c:0:167]:443  ESTABLISHED
201:1:6019:d949:70fa:542a:ce47]:59570  [2405:200:1630:a00::312c:d929]:443  CLOSE_WAIT
201:1:6019:d949:70fa:542a:ce47]:59571  [2405:200:1630:a00::312c:d929]:443  CLOSE_WAIT
201:1:6019:d949:70fa:542a:ce47]:59574  [2405:200:1630:a00::312c:d91a]:443  CLOSE_WAIT
201:1:6019:d949:70fa:542a:ce47]:59575  [2405:200:1630:a00::312c:d91a]:443  CLOSE_WAIT
201:1:6019:d949:70fa:542a:ce47]:59607  [2402:6800:764:a000::8000]:80  TIME_WAIT
201:1:6019:d949:70fa:542a:ce47]:59608  [2a03:2880:f26e:c9:face:b00c:0:7260]:443  TIME_WAIT
201:1:6019:d949:70fa:542a:ce47]:59611  [2a03:2880:f26e:c9:face:b00c:0:7260]:443  TIME_WAIT
201:1:6019:d949:70fa:542a:ce47]:59616  [2a03:2880:f26e:c9:face:b00c:0:7260]:443  TIME_WAIT
201:1:6019:d949:70fa:542a:ce47]:59617  [2a03:2880:f26e:c9:face:b00c:0:7260]:443  ESTABLISHED
```

1. netstat -o

displays active network connections and includes the process ID (PID) associated with each connection.



```
k>netstat -o

ons

Address          Foreign Address        State           PID
0.1:49670        LAPTOP-6BJ1JG3N:49671  ESTABLISHED     4892
0.1:49671        LAPTOP-6BJ1JG3N:49670  ESTABLISHED     4892
0.1:49672        LAPTOP-6BJ1JG3N:49673  ESTABLISHED     4892
0.1:49673        LAPTOP-6BJ1JG3N:49672  ESTABLISHED     4892
8.29.184:58220   20.198.118.190:https   ESTABLISHED     4636
8.29.184:58260   20.198.119.84:https    ESTABLISHED     4032
8.29.184:59462   20.212.88.117:https    ESTABLISHED     20408
8.29.184:59545   1drv:https             ESTABLISHED     16660
8.29.184:59547   1drv:https             ESTABLISHED     4032
8.29.184:59555   20.189.173.12:https    ESTABLISHED     4032
8.29.184:59580   152.195.38.76:http     CLOSE_WAIT      9648
8.29.184:59615   52.109.56.129:https    TIME_WAIT       0
8.29.184:59618   52.109.56.129:https    TIME_WAIT       0
8.29.184:59619   52.109.56.129:https    TIME_WAIT       0
8.29.184:59620   52.109.124.29:https    TIME_WAIT       0
8.29.184:59623   52.109.124.29:https    TIME_WAIT       0
201:1:6019:d949:70fa:542a:ce47]:58299  sh-in-f188:5228        ESTABLISHED     11412
201:1:6019:d949:70fa:542a:ce47]:58349  [2606:4700:8ca3:98df:bdd7:7a:3150:c532]:https  CLOSE_WAIT      10776
201:1:6019:d949:70fa:542a:ce47]:58350  bom07s28-in-x03:http   CLOSE_WAIT      10776
201:1:6019:d949:70fa:542a:ce47]:58351  [2606:4700:8d70:bc89:5ed7:b41:3fd7:3718]:https  CLOSE_WAIT      10776
201:1:6019:d949:70fa:542a:ce47]:59175  [2603:1063:2202:14::3]:https  ESTABLISHED     16660
201:1:6019:d949:70fa:542a:ce47]:59298  [2606:4700:8d72:883b:10d7:b41:6810:e095]:https  ESTABLISHED     11412
201:1:6019:d949:70fa:542a:ce47]:59321  whatsapp-cdn6-shv-01-pnq1:https  ESTABLISHED     11412
201:1:6019:d949:70fa:542a:ce47]:59570  [2405:200:1630:a00::312c:d929]:https  CLOSE_WAIT      9648
201:1:6019:d949:70fa:542a:ce47]:59571  [2405:200:1630:a00::312c:d929]:https  CLOSE_WAIT      9648
201:1:6019:d949:70fa:542a:ce47]:59574  [2405:200:1630:a00::312c:d91a]:https  CLOSE_WAIT      9648
201:1:6019:d949:70fa:542a:ce47]:59575  [2405:200:1630:a00::312c:d91a]:https  CLOSE_WAIT      9648
201:1:6019:d949:70fa:542a:ce47]:59617  whatsapp-chatd-edge6-shv-01-pnq1:https  TIME_WAIT       0
201:1:6019:d949:70fa:542a:ce47]:59621  whatsapp-chatd-edge6-shv-01-pnq1:https  TIME_WAIT       0
```

1. netstat -r

The -r option of netstat displays the IP routing table. Here is a sample display produced by netstat -r run on machine tenere.

```
ik>netstat -r
===========================================================

 a6 5e 99 ......Microsoft Wi-Fi Direct Virtual Adapter
 a6 5e 99 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 a6 5e 99 ......Realtek RTL8852AE WiFi 6 802.11ax PCIe Adapter
 a6 5e 9a ......Bluetooth Device (Personal Area Network)
 ec ac 29 ......Realtek PCIe GbE Family Controller
...............Software Loopback Interface 1
===========================================================

le
===========================================================

ation        Netmask          Gateway       Interface  Metric
0.0          0.0.0.0     192.168.29.1   192.168.29.184     35
0.0        255.0.0.0         On-link         127.0.0.1    331
0.1  255.255.255.255         On-link         127.0.0.1    331
255  255.255.255.255         On-link         127.0.0.1    331
9.0    255.255.255.0         On-link    192.168.29.184    291
184  255.255.255.255         On-link    192.168.29.184    291
255  255.255.255.255         On-link    192.168.29.184    291
0.0        240.0.0.0         On-link         127.0.0.1    331
0.0        240.0.0.0         On-link    192.168.29.184    291
255  255.255.255.255         On-link         127.0.0.1    331
255  255.255.255.255         On-link    192.168.29.184    291
===========================================================
tes:


le
===========================================================

work Destination      Gateway
0                     fe80::1a82:8cff:fee9:7cb9
/128                  On-link
5:201:1:6019::/64     On-link
5:201:1:6019:2b57:8769:d6b2:11ef/128
                      On-link
```

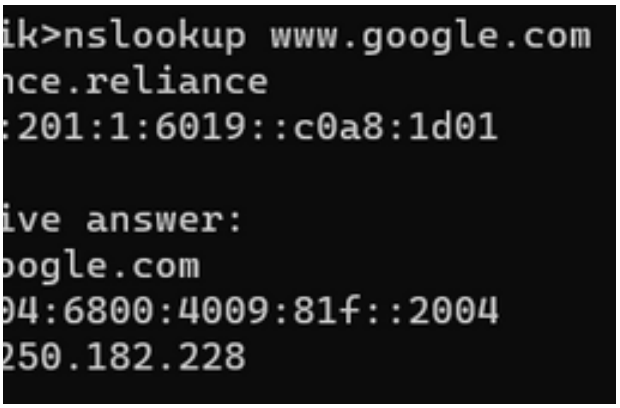
1. nslookup

used for querying the Domain Name System (DNS) to obtain information about domain names, IP addresses, and related DNS records.

```
tik>nslookup
r:  reliance.reliance
5:201:1:6019::c0a8:1d01
```

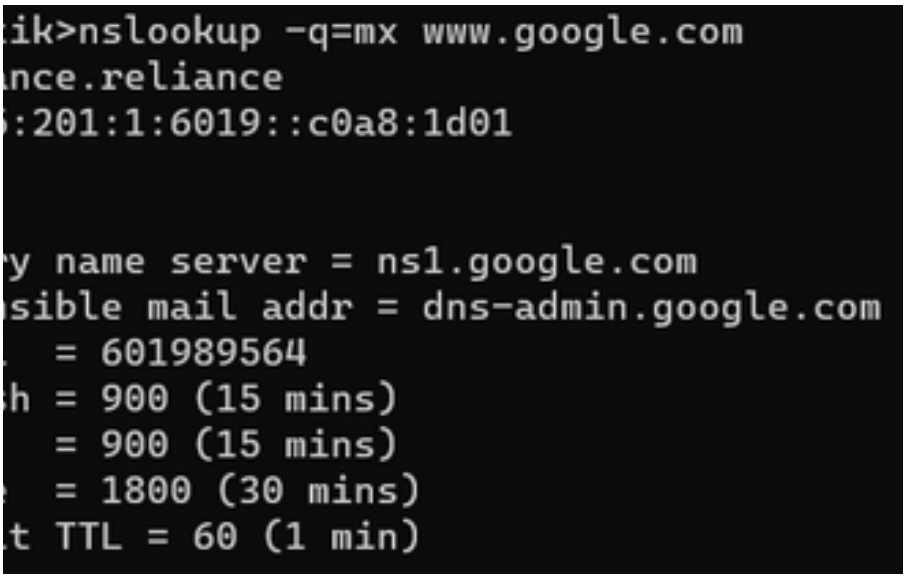
1. nslookup www.google.com

retrieve and display the IP address associated with the domain name "www.google.com" by querying the DNS.



1. nslookup -q=mx www.google.com

Initiates a DNS query specifically for Mail Exchange (MX) records. This will retrieve and display the mail servers responsible for handling email for the specified domain.



1. nslookup -type=ns wikipedia.org

This command queries the DNS for the authoritative Name Server (NS) records for the domain "example.com."

```
tik>nslookup -type=ns wikipedia.org
ance.reliance
5:201:1:6019::c0a8:1d01

tive answer:
   nameserver = ns1.wikimedia.org
   nameserver = ns2.wikimedia.org
   nameserver = ns0.wikimedia.org
```

1. nslookup -type=any google.com

Lookup for any record We can also view all the available DNS records using the -type=any option.

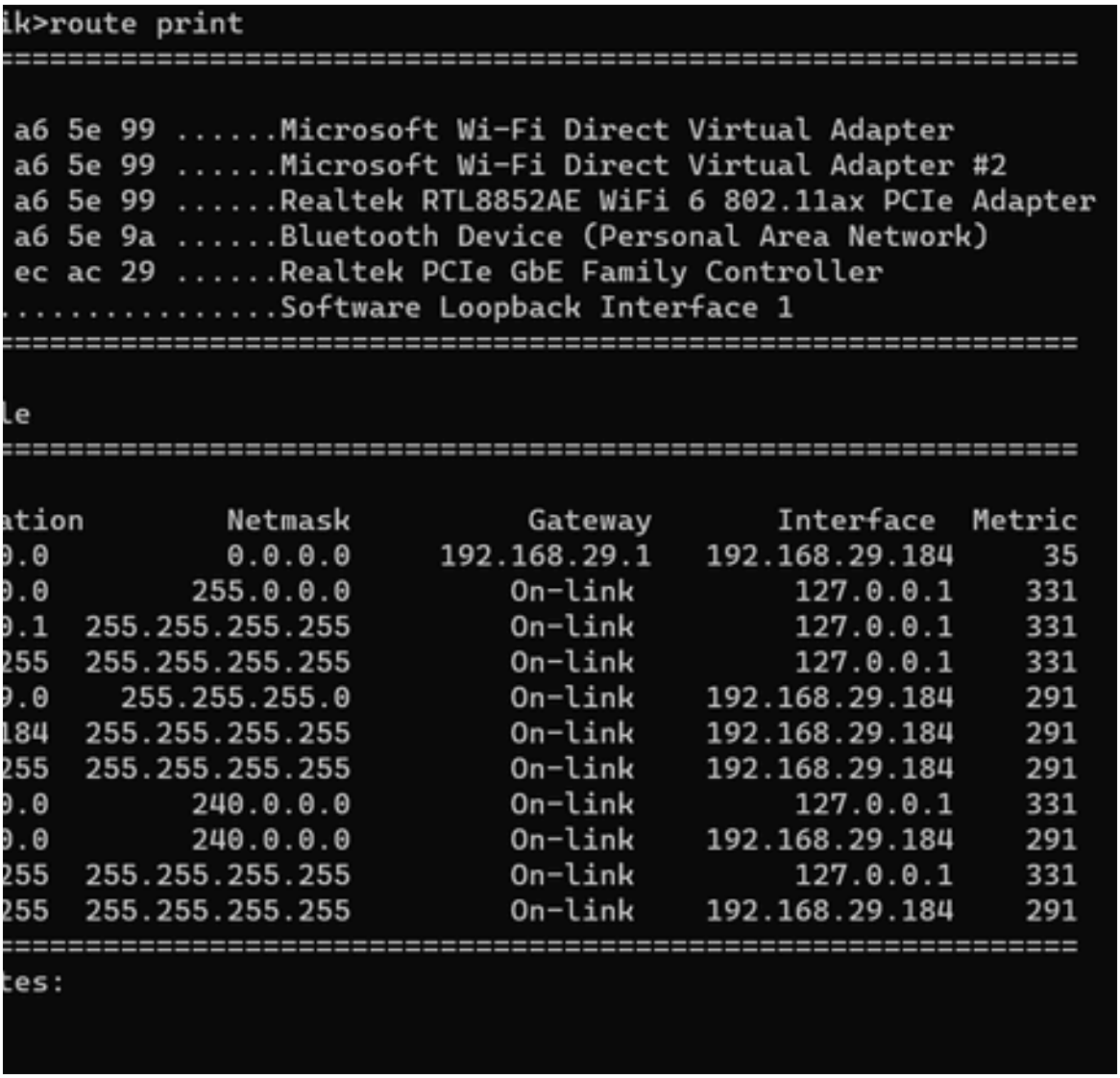
```
ik>nslookup -type=any google.com
nce.reliance
:201:1:6019::c0a8:1d01

ive answer:
   internet address = 142.250.77.46
   AAAA IPv6 address = 2404:6800:4009:81c::200e

y name server = ns1.google.com
sible mail addr = dns-admin.google.com
  = 601989564
h = 900 (15 mins)
  = 900 (15 mins)
  = 1800 (30 mins)
t TTL = 60 (1 min)
   nameserver = ns4.google.com
   nameserver = ns2.google.com
   nameserver = ns3.google.com
   nameserver = ns1.google.com
```

1. route print

display the current IP routing table.



1. route print -6

displays only the IPv6 routing table. This command provides information about IPv6 routes.

```
tik>route print -6
===========================================================
t
d a6 5e 99 ......Microsoft Wi-Fi Direct Virtual Adapter
d a6 5e 99 ......Microsoft Wi-Fi Direct Virtual Adapter #2
d a6 5e 99 ......Realtek RTL8852AE WiFi 6 802.11ax PCIe Adapter
d a6 5e 9a ......Bluetooth Device (Personal Area Network)
3 ec ac 29 ......Realtek PCIe GbE Family Controller
..................Software Loopback Interface 1
===========================================================

ble
===========================================================
:
twork Destination      Gateway
/0                     fe80::1a82:8cff:fee9:7cb9
1/128                  On-link
05:201:1:6019::/64     On-link
05:201:1:6019:2b57:8769:d6b2:11ef/128
                       On-link
05:201:1:6019:d949:70fa:542a:ce47/128
                       On-link
80::/64                On-link
80::7680:a94b:5d3:9a0e/128
                       On-link
00::/8                 On-link
00::/8                 On-link
===========================================================
utes:
```

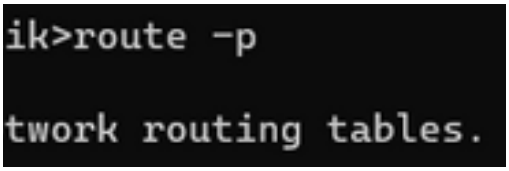
1. route -F

The ROUTE -F command is used in Windows to flush the IPv4 routing table. It clears all entries from the routing table, effectively removing all configured routes.

```
tik>route -F
 operation requires elevation.
```

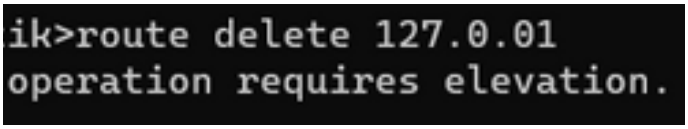
1. route -p

manipulates network routing tables



1. route delete 127.0.01

used to remove a specific route from the routing table.



1. hostname

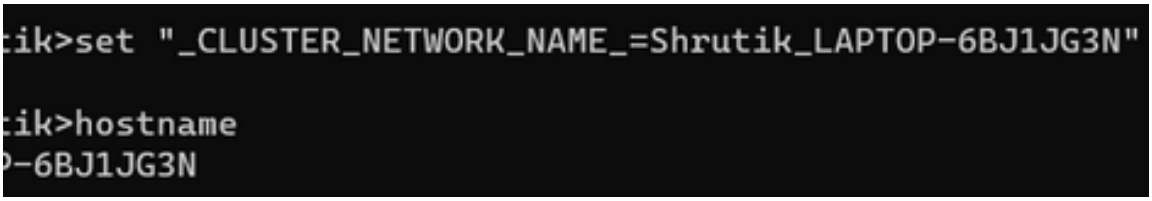
In Windows, running HOSTNAME in the command prompt will display the current hostname of the computer.

1. echo %COMPUTERNAME%

displays the name of the computer in uppercase

1. set "_CLUSTER_NETWORK_NAME_=Shrutik_LAPTOP-6BJ1JG3N"

To alter the hostname output

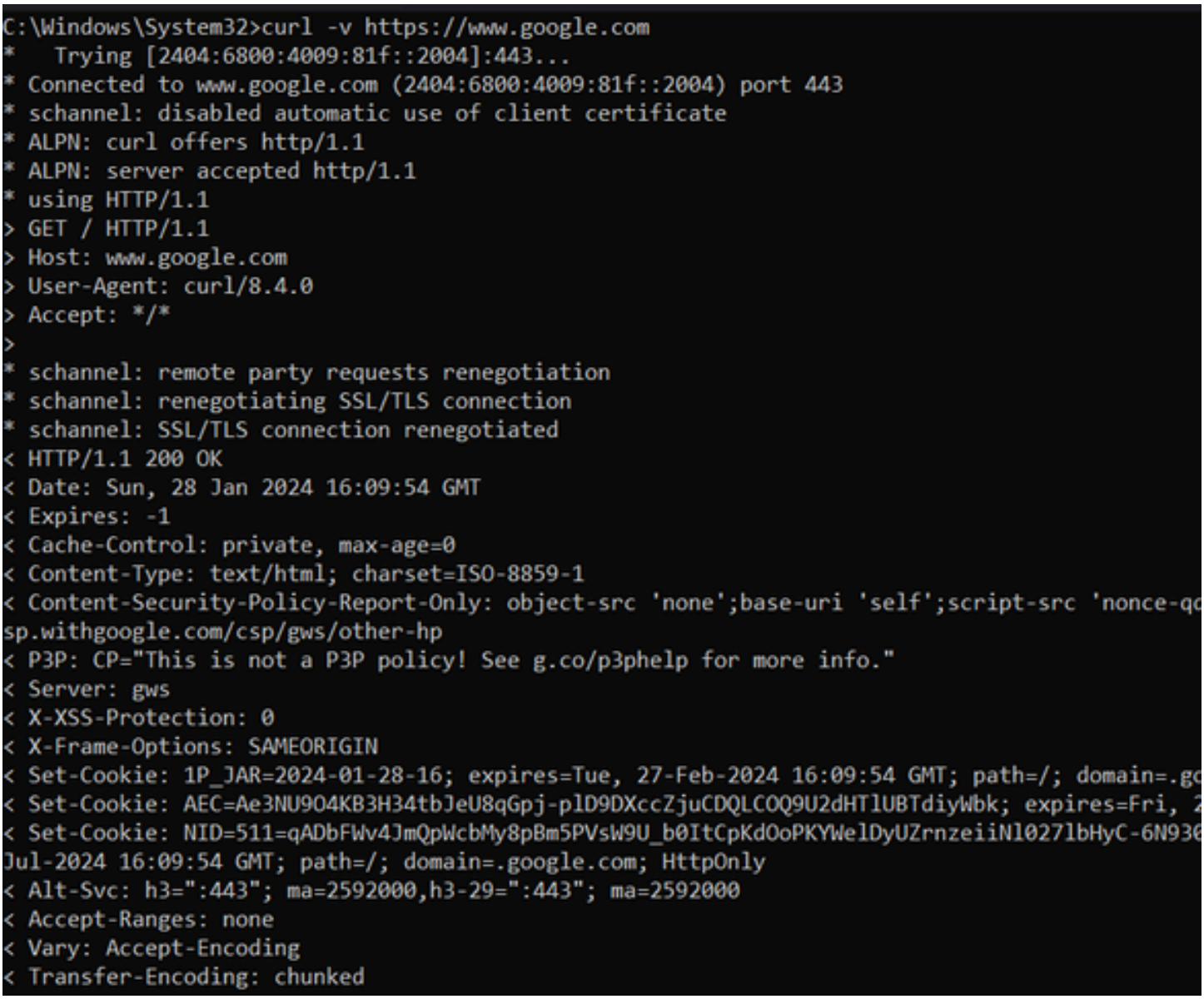


1. curl www.google.com

This command sends a GET request to "https://www.google.com" and displays the response on the terminal.

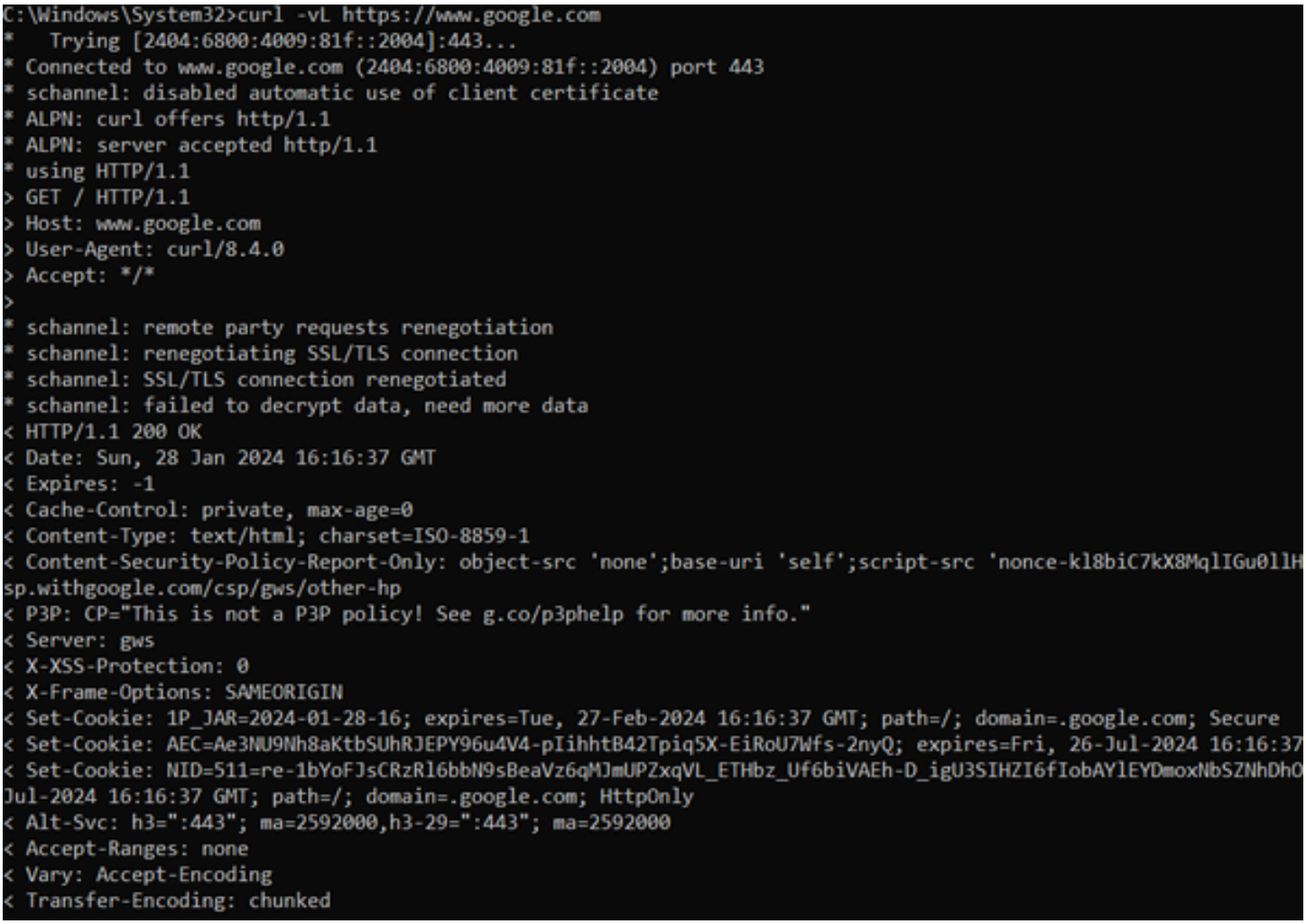
1. curl -v https://www.google.com

used to switch on verbose mode



1. curl -vL https://www.google.com

used to ask for both verbose mode and that curl follows HTTP redirects



1. curl -A "shrutik gupta" https://www.google.com

used to pass on an argument to an option

1. arp /a

used to display the arp cache tables for all interfaces, type

```
tik>arp /a

2.168.29.184 --- 0x8
dress      Physical Address      Type
1          18-82-8c-e9-7c-b9     dynamic
255        ff-ff-ff-ff-ff-ff     static
           01-00-5e-00-00-16     static
           01-00-5e-00-00-fb     static
           01-00-5e-00-00-fc     static
.250       01-00-5e-7f-ff-fa     static
.255       ff-ff-ff-ff-ff-ff     static
```

1. arp -s 192.168.1.2 ab:cd:ef:gh:ij:kl

used to add a new entry to the ARP cache

```
ARP entry added for 192.168.1.2
```

1. arp -d 192.168.1.2

used to remove an entry from the ARP cache

```
ARP entry removed for 192.168.1.2
```

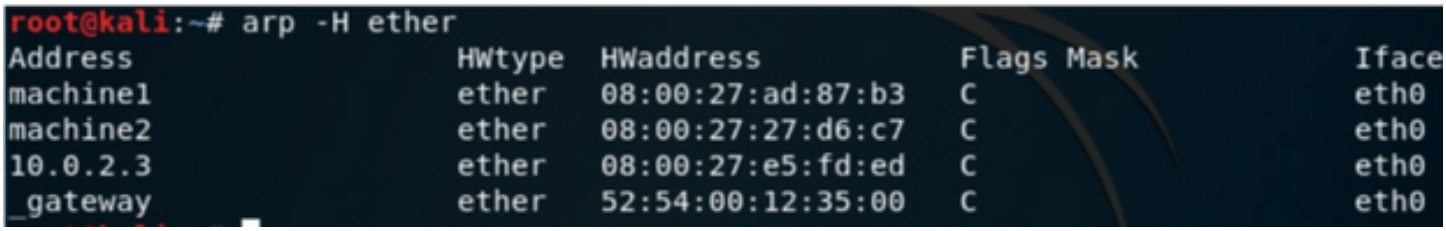
1. arp -v

This option shows the verbose information.

```
root@kali:~# arp -v
Address                  HWtype  HWaddress           Flags Mask            Iface
machine1                 ether   08:00:27:ad:87:b3   C                     eth0
machine2                 ether   08:00:27:27:d6:c7   C                     eth0
10.0.2.3                 ether   08:00:27:e5:fd:ed   C                     eth0
_gateway                 ether   52:54:00:12:35:00   C                     eth0
Entries: 4      Skipped: 0      Found: 4
```

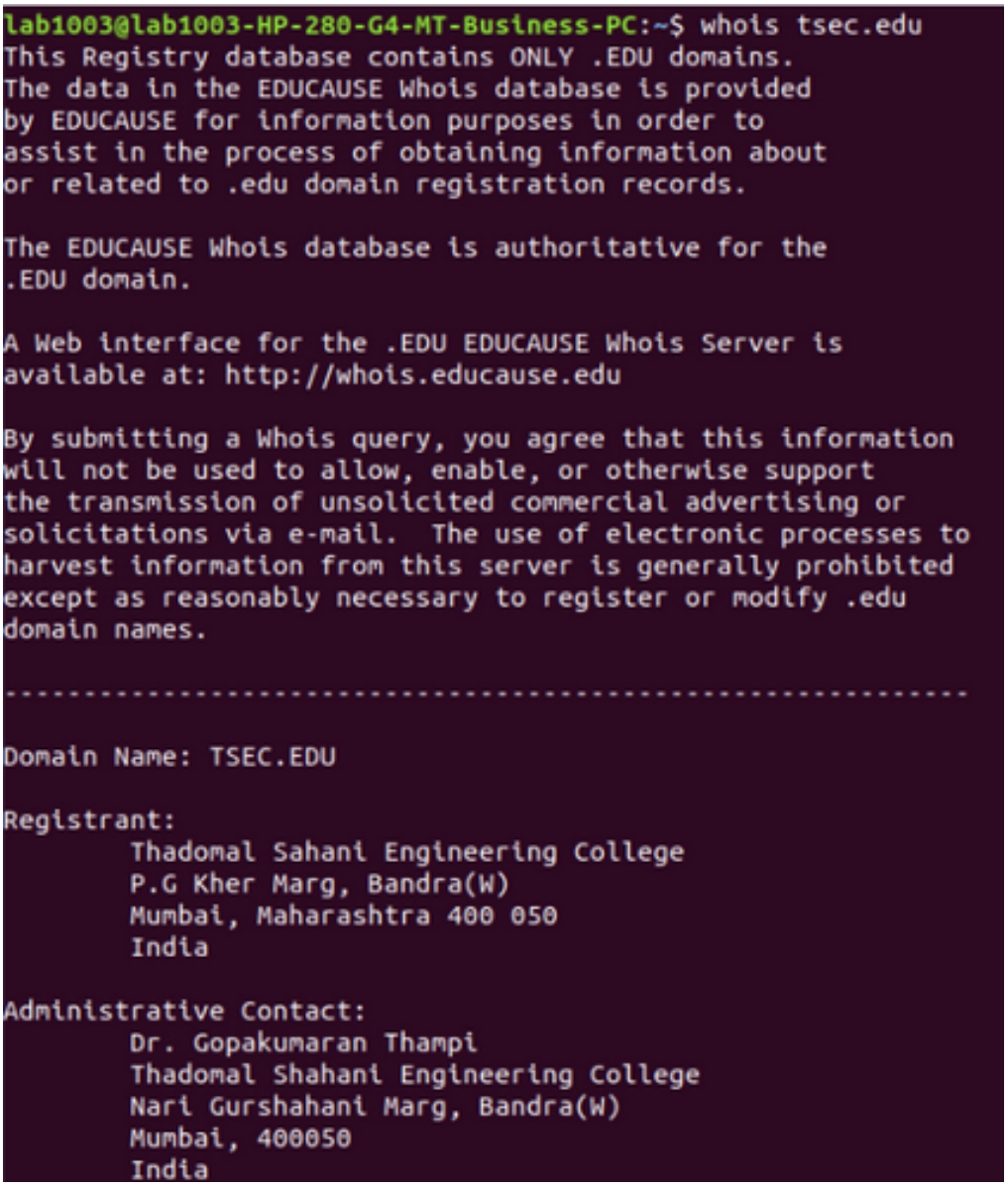
1. arp -H ether

This tells arp which class of entries it should check for.



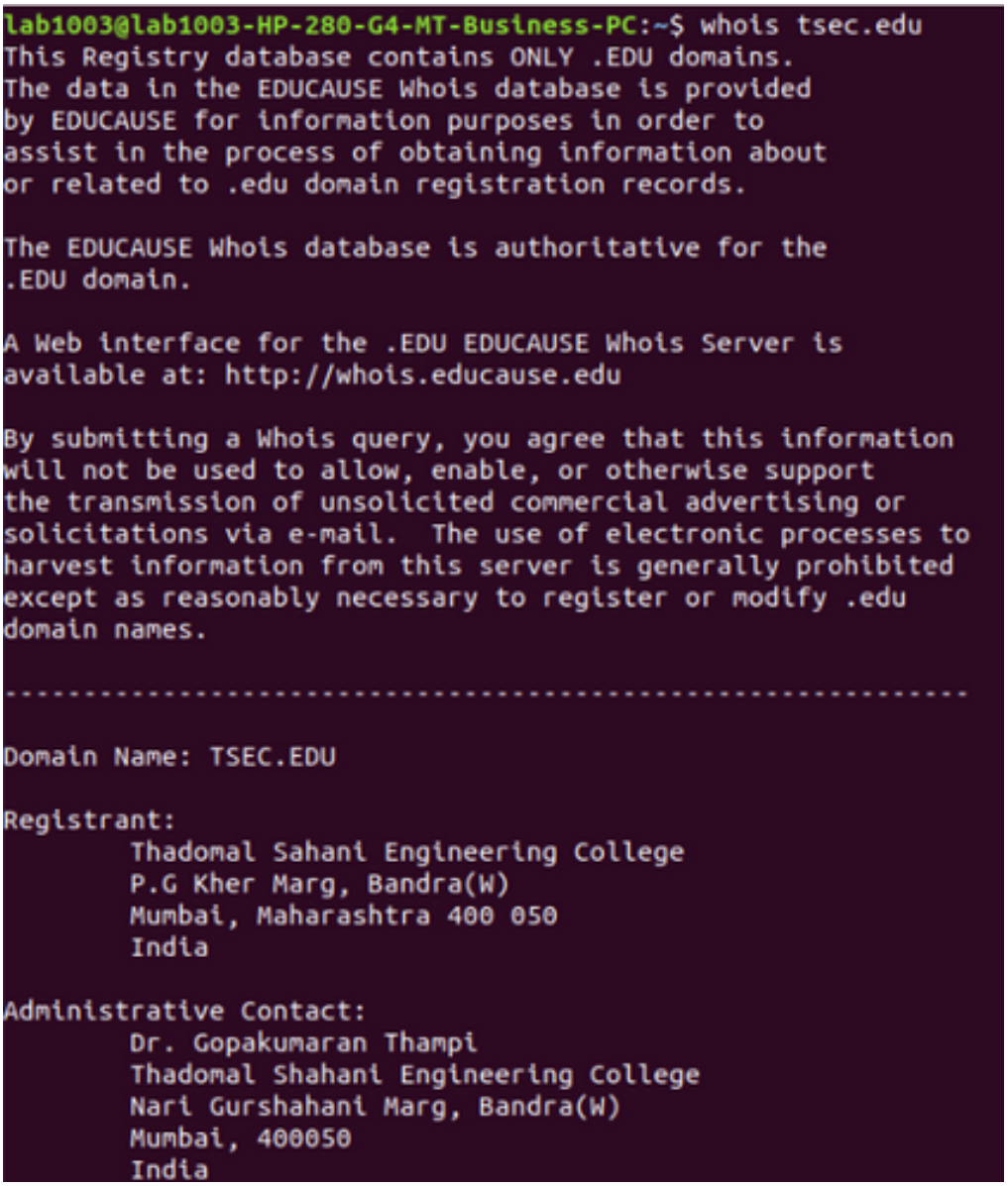
1. whois tsec.edu

WHOIS is used to query a database and retrieve information about the registration details of domain names, including ownership, registration and expiration dates, name servers, and contact information.



1. whois -H tsec.edu

When you use the ‘whois’ command, the output often includes legal disclaimers. If you want to hide these disclaimers, you can use the -H flag.



1. whois -i tsec.edu

By default, the ‘whois’ command is case-sensitive. However, you can make it case-insensitive by using the -i flag.

```
---------------------------------------------------------------

Domain Name: TSEC.EDU

Registrant:
        Thadomal Sahani Engineering College
        P.G Kher Marg, Bandra(W)
        Mumbai, Maharashtra 400 050
        India

Administrative Contact:
        Dr. Gopakumaran Thampi
        Thadomal Shahani Engineering College
        Nari Gurshahani Marg, Bandra(W)
        Mumbai, 400050
        India
```

1. whois -l tsec.edu

If you're writing a script and need the output of the 'whois' command to be on one line, you can use the -l flag.

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ whois tsec.edu
This Registry database contains ONLY .EDU domains.
The data in the EDUCAUSE Whois database is provided
by EDUCAUSE for information purposes in order to
assist in the process of obtaining information about
or related to .edu domain registration records.

The EDUCAUSE Whois database is authoritative for the
.EDU domain.

A Web interface for the .EDU EDUCAUSE Whois Server is
available at: http://whois.educause.edu

By submitting a Whois query, you agree that this information
will not be used to allow, enable, or otherwise support
the transmission of unsolicited commercial advertising or
solicitations via e-mail.  The use of electronic processes to
harvest information from this server is generally prohibited
except as reasonably necessary to register or modify .edu
domain names.
```

1. ss

The output returns a list of open non-listening sockets with established connections.

```
~ $ ss
Netid  State      Recv-Q Send-Q Local Address:Port    Peer Address:Port
u_seq  ESTAB      0      0      @00026 40545          * 40546
u_seq  ESTAB      0      0      @00025 40543          * 40544
u_str  ESTAB      0      0       * 47336              * 47335
u_str  ESTAB      0      0       * 37615              * 37616
u_str  ESTAB      0      0       * 37263              * 36819
u_str  ESTAB      0      0       * 37816              * 37817
u_str  ESTAB      0      0       * 40173              * 40174
u_str  ESTAB      0      0       * 38066              * 39294
```

1. ss --all

List all listening and non-listening connections with

```
~ $ ss -a
Netid  State      Recv-Q Send-Q Local Address:Port               Peer Address:Port
nl     UNCONN     0      0      rtnl:avahi-daemon/911      *
nl     UNCONN     0      0      rtnl:1828717503            *
nl     UNCONN     0      0      rtnl:chrome/4111           *
nl     UNCONN     0      0      rtnl:vmnet-natd/1562       *
nl     UNCONN     0      0      rtnl:kernel                *
nl     UNCONN     0      0      rtnl:vmnet-bridge/1495     *
nl     UNCONN     0      0      rtnl:chrome/4058           *
nl     UNCONN     0      0      rtnl:dnsmasq/1170          *
```

1. ss --listen

used to display only listening sockets, which are omitted by default

```
~ $ ss -l
Netid  State      Recv-Q Send-Q Local Address:Port               Peer Address:Port
nl     UNCONN     0      0      rtnl:avahi-daemon/911      *
nl     UNCONN     0      0      rtnl:1828717503            *
nl     UNCONN     0      0      rtnl:chrome/4111           *
nl     UNCONN     0      0      rtnl:vmnet-natd/1562       *
nl     UNCONN     0      0      rtnl:kernel                *
nl     UNCONN     0      0      rtnl:vmnet-bridge/1495     *
nl     UNCONN     0      0      rtnl:chrome/4058           *
nl     UNCONN     0      0      rtnl:dnsmasq/1170          *
```

1. ss --tcp

used to list TCP connections

```
~ $ ss -t
State      Recv-Q Send-Q   Local Address:Port                 Peer Address:Port
ESTAB      0      0        192.168.100.2:34494              108.177.126.188:5228
ESTAB      0      0        192.168.100.2:45618              142.250.184.150:https
ESTAB      0      0        192.168.100.2:39146                   52.85.7.80:https
```

1. ss -udp

used to show a list of UDP connections

```
~ $ ss -u
Recv-Q Send-Q        Local Address:Port                  Peer Address:Port
0      0             192.168.100.2:36036               216.58.206.206:https
```

(reference – www.thegeekstuff.com)

1. dig redhat.com

When you pass a domain name to the dig command, by default it displays the A record

```
$ dig redhat.com

; <<>> DiG 9.7.3-RedHat-9.7.3-2.el6 <<>> redhat.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62863
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 3

;; QUESTION SECTION:
;redhat.com.                    IN      A

;; ANSWER SECTION:
redhat.com.             37      IN      A       209.132.183.81

;; AUTHORITY SECTION:
redhat.com.             73      IN      NS      ns4.redhat.com.
redhat.com.             73      IN      NS      ns3.redhat.com.
redhat.com.             73      IN      NS      ns2.redhat.com.
redhat.com.             73      IN      NS      ns1.redhat.com.

;; ADDITIONAL SECTION:
ns1.redhat.com.         73      IN      A       209.132.186.218
ns2.redhat.com.         73      IN      A       209.132.183.2
ns3.redhat.com.         73      IN      A       209.132.176.100
```

1. dig redhat.com +noall +answer

+noanswer – Turn off the answer section

```
$ dig redhat.com +noall +answer

; <<>> DiG 9.7.3-RedHat-9.7.3-2.el6 <<>> redhat.com +noall +answer
;; global options: +cmd
redhat.com.             60      IN      A       209.132.183.81
```

1. dig redhat.com MX +noall +answer

To query MX records, pass MX as an argument to the dig command

```
$ dig redhat.com  MX +noall +answer

; <<>> DiG 9.7.3-RedHat-9.7.3-2.el6 <<>> redhat.com MX +noall +answer
;; global options: +cmd
redhat.com.             513     IN      MX      5 mx1.redhat.com.
redhat.com.             513     IN      MX      10 mx2.redhat.com.
```

1. dig redhat.com NS +noall +answer

To query the NS record use the type NS

```
$ dig redhat.com NS +noall +answer


; <<>> DiG 9.7.3-RedHat-9.7.3-2.el6 <<>> redhat.com NS +noall +answer
;; global options: +cmd
redhat.com.             558     IN      NS      ns2.redhat.com.
redhat.com.             558     IN      NS      ns1.redhat.com.
redhat.com.             558     IN      NS      ns3.redhat.com.
redhat.com.             558     IN      NS      ns4.redhat.com.
```

1. dig @ns1.redhat.com redhat.com

By default dig uses the DNS servers defined in your /etc/resolv.conf file. If you like to use a different DNS server to perform the query, specify it in the command line as @dnsserver.

```
$ dig @ns1.redhat.com redhat.com

; <<>> DiG 9.7.3-RedHat-9.7.3-2.el6 <<>> @ns1.redhat.com redhat.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20963
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;redhat.com.                    IN      A

;; ANSWER SECTION:
redhat.com.             60      IN      A       209.132.183.81

;; AUTHORITY SECTION:
redhat.com.             600     IN      NS      ns1.redhat.com.
redhat.com.             600     IN      NS      ns4.redhat.com.
redhat.com.             600     IN      NS      ns3.redhat.com.
redhat.com.             600     IN      NS      ns2.redhat.com.
```

1. mtr -t baeldung.com

The -t option indicates we want to see the output in the curses-based terminal

```
$ mtr -t baeldung.com
                        My traceroute [v0.94]
myhome (192.168.0.7)                          2022-06-08T01:41:48+0700
Keys:   Help   Display mode   Restart statistics   Order of fields   quit
                                    Packets           Pings
Host                               Loss% Snt Last Avg  Best Wrst StDev
1. _gateway                        0.0%  21  4.8  4.7  3.3  12.0 1.9
2. 11.68.93.1                      0.0%  21  12.9 14.5 11.9 22.2 2.7
3. bex-0005-pele.fast.net.id       0.0%  21  19.4 17.6 14.3 27.3 3.5
4. bex-0005-pele.fast.net.id       0.0%  21  21.9 18.2 13.6 33.7 5.0
5. fm-dyn-www-73-22-333.fast.net.id 0.0% 21  16.9 19.1 15.6 35.4 4.9
6. fm-dyn-www-136-22-333.fast.net.i 0.0% 20  24.1 20.5 16.0 41.9 5.8
7. 172.66.40.248                   0.0%  20  16.2 17.4 14.6 22.8 2.3
```

1. mtr -o ‘SA’ -t baeldung.com

Suppose we are only interested in the Snt and Avg columns. We could launch mtr with the -o option.

```
$ mtr -o 'SA' -t baeldung.com
                      My traceroute  [v0.94]
myhome (192.168.0.7)                              2022-06-10T02:41:12+0700
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                              Packets
           Pings                                              Snt   Avg
 1. _gateway                                                    8   3.9
 2. 11.68.93.1                                                  8  14.9
 3. bel-cgom-pend.fast.net.id                                   8  15.9
 4. bel-cgom-pend.fast.net.id                                   8  16.6
 5. lynx-static-333-56-777-888.lynx.net.id                      7  29.4
 6. lynx-static-333-56-777-888.lynx.net.id                      7  30.9
 7. 13335.sgw.equinix.com                                       7  31.8
 8. 162.158.160.15                                              7  32.2
 9. 172.66.43.8                                                 7  29.7
```

1. mtr -m 3 -t baeldung.com

we can use the -m option to limit the nodes that we want to investigate.

```
$ mtr -m 3 -t baeldung.com
                     My traceroute  [v0.94]
myhome (192.168.0.7)                              2022-06-16T01:07:58+0700
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                 Packets               Pings
 Host                          Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. _gateway                    0.0%     4    6.7   5.0   4.3   6.7   1.2
 2. 11.68.93.1                  0.0%     4   13.2  14.1  13.2  15.3   0.9
 3. bel-cgom-pend.fast.net.id   0.0%     4   17.9  17.2  15.1  19.1   1.7
```

1. mtr -f 3 -t baeldung.com

We can filter out the first two hops using the -f option.

```
$ mtr -f 3 -t baeldung.com
                     My traceroute  [v0.94]
myhome (192.168.0.7)                              2022-06-16T01:33:03+0700
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                 Packets               Pings
 Host                          Loss%   Snt   Last   Avg  Best  Wrst StDev
 3. bel-cgom-pend.fast.net.id   0.0%    13   82.7  31.4  14.3  90.4  26.5
 4. bel-cgom-pend.fast.net.id   0.0%    13   98.0  29.8  14.4  98.0  25.9
 5. fm-dyn-333-22-92-876.fast.  0.0%    13   49.4  39.1  15.1 205.3  51.6
 6. fm-dyn-333-456-62-876.fast  0.0%    12   94.6  29.1  14.7  94.6  24.4
 7. 172.66.40.248               0.0%    12   25.3  32.4  15.1  97.7  27.9
```

1. mtr -r baeldung.com

we can let mtr do the job for a while and read the result later with the -r option.

```
Start: 2022-06-16T03:04:54+0700
HOST: myhome                          Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- _gateway                       0.0%    10    5.6   5.1   3.5   9.6   1.8
  2.|-- 11.68.93.1                     0.0%    10   13.8  13.6  11.3  14.8   1.1
  3.|-- bel-cgom-pend.fast.net.id       0.0%    10   16.6  18.1  14.9  32.6   5.2
  4.|-- bel-cgom-pend.fast.net.id       0.0%    10   15.5  17.2  14.7  23.8   2.8
  5.|-- fm-dyn-222-11-92-133.fast       0.0%    10   15.6  17.2  15.1  23.1   2.6
  6.|-- fm-dyn-122-122-62-133.fas       0.0%    10   18.6  18.9  15.7  27.7   3.5
  7.|-- 172.66.40.248                   0.0%    10   16.5  16.8  14.3  25.0   3.1
```

Conclusion: LO1 Achieved.