

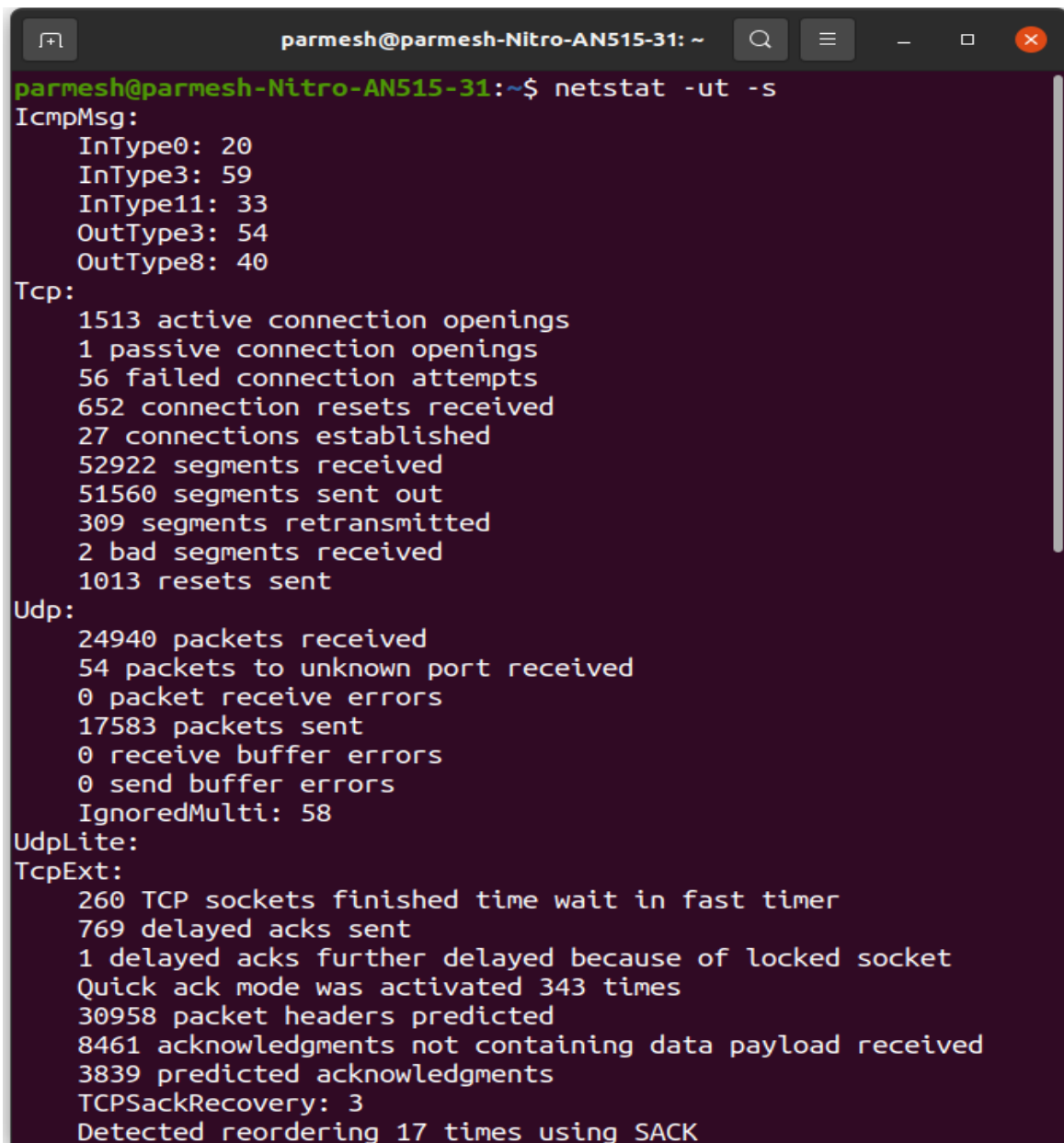
## Lab 2

Parmesh Mathur

2018A7PS0133G

### 1. See the statistics of TCP and UDP ports on Linux machine

The `netstat` command enables us to see the statistics (`-s` flag) of the TCP (`-t` flag) and UDP (`-u` flag). The statistics displayed include number of connections opened, failed attempts etc. It also shows information on other TCP/UDP based protocols in the output (e.g. `UdpLite`, `TcpExt`).

A terminal window titled 'parmesh@parmesh-Nitro-AN515-31: ~' with standard window controls. The command 'netstat -ut -s' has been executed, displaying network statistics for ICMP, TCP, UDP, UdpLite, and TcpExt. The output is as follows:

```
parmesh@parmesh-Nitro-AN515-31:~$ netstat -ut -s
IcmpMsg:
  InType0: 20
  InType3: 59
  InType11: 33
  OutType3: 54
  OutType8: 40
Tcp:
  1513 active connection openings
  1 passive connection openings
  56 failed connection attempts
  652 connection resets received
  27 connections established
  52922 segments received
  51560 segments sent out
  309 segments retransmitted
  2 bad segments received
  1013 resets sent
Udp:
  24940 packets received
  54 packets to unknown port received
  0 packet receive errors
  17583 packets sent
  0 receive buffer errors
  0 send buffer errors
  IgnoredMulti: 58
UdpLite:
TcpExt:
  260 TCP sockets finished time wait in fast timer
  769 delayed acks sent
  1 delayed acks further delayed because of locked socket
  Quick ack mode was activated 343 times
  30958 packet headers predicted
  8461 acknowledgments not containing data payload received
  3839 predicted acknowledgments
  TCPSackRecovery: 3
  Detected reordering 17 times using SACK
```

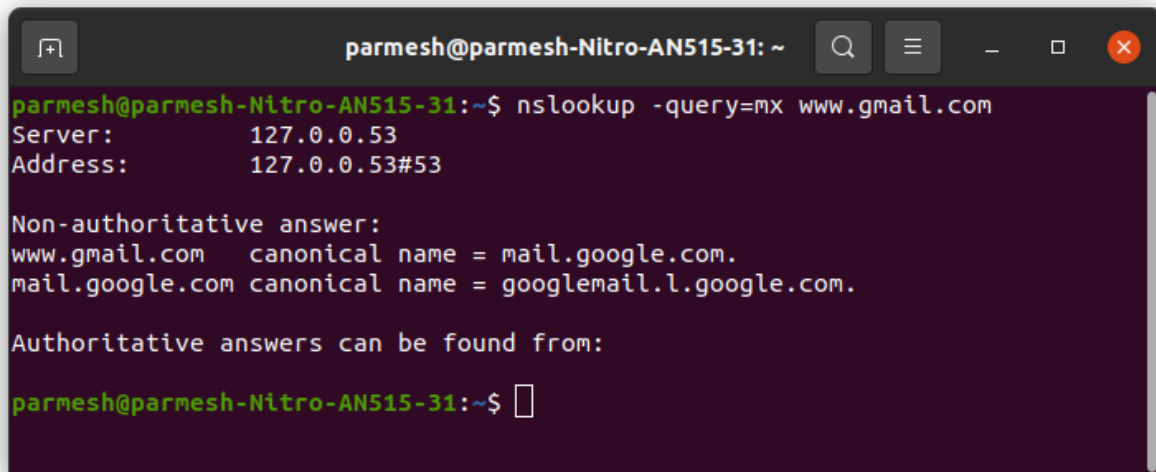
## 2. Enlist the listening ports on your machine

The `netstat` command is used to list the ports using the `-l` flag to filter out only the listening ports (shown in the `State` column of the outputs). As shown, the output is split into two separate lists, one which shows ports connected to the internet, and another for UNIX domain sockets.

```
parmesh@parmesh-Nitro-AN515-31: ~  
parmesh@parmesh-Nitro-AN515-31:~$ netstat -l  
Active Internet connections (only servers)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN  
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN  
tcp6       0      0 ip6-localhost:ipp      [::]:*                 LISTEN  
udp        0      0 localhost:domain        0.0.0.0:*                 
udp        0      0 0.0.0.0:631            0.0.0.0:*                 
udp        0      0 224.0.0.251:mdns       0.0.0.0:*                 
udp        0      0 0.0.0.0:mdns           0.0.0.0:*                 
udp        0      0 0.0.0.0:47647          0.0.0.0:*                 
udp6       0      0 [::]:49978             [::]:*                   
udp6       0      0 [::]:mdns              [::]:*                   
raw6       0      0 [::]:ipv6-icmp         [::]:*                 7  
Active UNIX domain sockets (only servers)  
Proto RefCnt Flags   Type       State         I-Node   Path  
unix    2      [ ACC ] STREAM    LISTENING    34879    /run/irqbalance//irqbalance843.sock  
unix    2      [ ACC ] SEQPACKET LISTENING    16166    /run/udev/control  
unix    2      [ ACC ] STREAM    LISTENING    48383    @/tmp/.ICE-unix/1874  
unix    2      [ ACC ] STREAM    LISTENING    43672    /run/user/1000/systemd/private  
unix    2      [ ACC ] STREAM    LISTENING    43677    /run/user/1000/bus  
unix    2      [ ACC ] STREAM    LISTENING    43678    /run/user/1000/gnupg/S.dirmngr  
unix    2      [ ACC ] STREAM    LISTENING    43679    /run/user/1000/gnupg/S.gpg-agent.browser  
unix    2      [ ACC ] STREAM    LISTENING    43680    /run/user/1000/gnupg/S.gpg-agent.extra  
unix    2      [ ACC ] STREAM    LISTENING    43681    /run/user/1000/gnupg/S.gpg-agent.ssh  
unix    2      [ ACC ] STREAM    LISTENING    43682    /run/user/1000/gnupg/S.gpg-agent  
unix    2      [ ACC ] STREAM    LISTENING    43683    /run/user/1000/pk-debconf-socket  
unix    2      [ ACC ] STREAM    LISTENING    43684    /run/user/1000/pulse/native  
unix    2      [ ACC ] STREAM    LISTENING    43685    /run/user/1000/snapd-session-agent.socket  
unix    2      [ ACC ] STREAM    LISTENING    42478    /tmp/.X11-unix/X0  
unix    2      [ ACC ] STREAM    LISTENING    42477    @/tmp/.X11-unix/X0  
unix    2      [ ACC ] STREAM    LISTENING    40771    /tmp/ssh-WiBX3CdKy0U3/agent.1766  
unix    2      [ ACC ] STREAM    LISTENING    48384    /tmp/.ICE-unix/1874  
unix    2      [ ACC ] STREAM    LISTENING    40525    /run/user/1000/keyring/control  
unix    2      [ ACC ] STREAM    LISTENING    43975    /run/user/1000/keyring/pkcs11  
unix    2      [ ACC ] STREAM    LISTENING    49220    /run/user/1000/keyring/ssh  
unix    2      [ ACC ] STREAM    LISTENING    59959    /tmp/.org.chromium.Chromium.TPR9Cw/SingletonSocket  
unix    2      [ ACC ] STREAM    LISTENING    79239    /tmp/OSL_PIPE_1000_SingleOfficeIPC_a54f96a3a234883654305711cb6766  
unix    2      [ ACC ] STREAM    LISTENING    16139    /run/systemd/private  
unix    2      [ ACC ] STREAM    LISTENING    16141    /run/systemd/userdb/io.systemd.DynamicUser  
unix    2      [ ACC ] STREAM    LISTENING    16152    /run/systemd/fsck.progress  
unix    2      [ ACC ] STREAM    LISTENING    16162    /run/systemd/journal/stdout  
unix    2      [ ACC ] STREAM    LISTENING    16933    /run/systemd/journal/io.systemd.journal  
unix    2      [ ACC ] STREAM    LISTENING    72381    @/dbus-vfs-daemon/socket-RYbS1GrE  
unix    2      [ ACC ] STREAM    LISTENING    45038    @/tmp/dbus-h6CrDGgp5X  
unix    2      [ ACC ] STREAM    LISTENING    35225    @/tmp/dbus-0h6hsgyW  
unix    2      [ ACC ] STREAM    LISTENING    55512    @/dbus-vfs-daemon/socket-1Y9EDGmA  
unix    2      [ ACC ] STREAM    LISTENING    33921    /run/acpid.socket  
unix    2      [ ACC ] STREAM    LISTENING    33923    /run/avahi-daemon/socket  
unix    2      [ ACC ] STREAM    LISTENING    33925    /run/cups/cups.sock  
unix    2      [ ACC ] STREAM    LISTENING    33927    /run/dbus/system_bus_socket  
unix    2      [ ACC ] STREAM    LISTENING    33929    /run/snapd.socket  
unix    2      [ ACC ] STREAM    LISTENING    33931    /run/snapd-snap.socket  
unix    2      [ ACC ] STREAM    LISTENING    33933    /run/uidd/request  
unix    2      [ ACC ] STREAM    LISTENING    44330    @/tmp/dbus-8a6d5NcM  
unix    2      [ ACC ] STREAM    LISTENING    47438    @/home/parmesh/.cache/ibus/dbus-tfq93qPM  
unix    2      [ ACC ] STREAM    LISTENING    35226    @/tmp/dbus-G6D4dnNT  
unix    2      [ ACC ] STREAM    LISTENING    44331    @/tmp/dbus-2w0I5jDL  
parmesh@parmesh-Nitro-AN515-31:~$
```

### 3. See the mail exchange (MX) record for [www.gmail.com](http://www.gmail.com)

The `-query=mx` option of `nslookup` is used to obtain the mail exchange records for any domain (specified in the command itself as shown). This command lists out the SMTP servers that handle the traffic for the domain.

A terminal window titled 'parmesh@parmesh-Nitro-AN515-31: ~' with search, menu, and window control icons. The command 'nslookup -query=mx www.gmail.com' is entered. The output shows the local server and address, followed by non-authoritative answers for canonical names, and a prompt for authoritative answers.

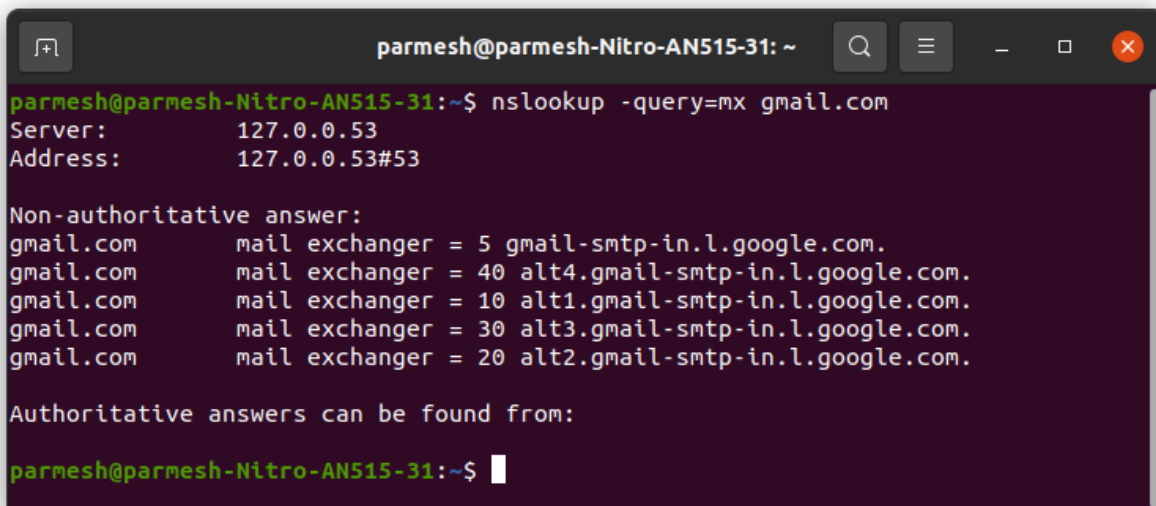
```
parmesh@parmesh-Nitro-AN515-31:~$ nslookup -query=mx www.gmail.com
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
www.gmail.com    canonical name = mail.google.com.
mail.google.com canonical name = googlemail.l.google.com.

Authoritative answers can be found from:

parmesh@parmesh-Nitro-AN515-31:~$
```

The command doesn't work for [www.gmail.com](http://www.gmail.com), but works for `gmail.com`, listing out the required server names.

A terminal window titled 'parmesh@parmesh-Nitro-AN515-31: ~' with search, menu, and window control icons. The command 'nslookup -query=mx gmail.com' is entered. The output shows the local server and address, followed by non-authoritative answers listing five mail exchangers for gmail.com, and a prompt for authoritative answers.

```
parmesh@parmesh-Nitro-AN515-31:~$ nslookup -query=mx gmail.com
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
gmail.com        mail exchanger = 5 gmail-smtp-in.l.google.com.
gmail.com        mail exchanger = 40 alt4.gmail-smtp-in.l.google.com.
gmail.com        mail exchanger = 10 alt1.gmail-smtp-in.l.google.com.
gmail.com        mail exchanger = 30 alt3.gmail-smtp-in.l.google.com.
gmail.com        mail exchanger = 20 alt2.gmail-smtp-in.l.google.com.

Authoritative answers can be found from:

parmesh@parmesh-Nitro-AN515-31:~$
```

#### 4. Display the all network interfaces on your machine

The `ifconfig` command is used, which lists all the interfaces on the machine using the `-a` flag, and other statistics entailed by each of interface.

```
parmesh@parmesh-Nitro-AN515-31: ~  
parmesh@parmesh-Nitro-AN515-31:~$ ifconfig -a  
enp2s0f1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500  
    ether 98:29:a6:45:8d:a0 txqueuelen 1000 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    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 4671 bytes 496554 (496.5 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4671 bytes 496554 (496.5 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
wlp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.7 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 fe80::346:8027:3304:723c prefixlen 64 scopeid 0x20<link>  
    ether 98:22:ef:58:e1:4f txqueuelen 1000 (Ethernet)  
    RX packets 75777 bytes 56968683 (56.9 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 66914 bytes 17257282 (17.2 MB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
parmesh@parmesh-Nitro-AN515-31:~$
```

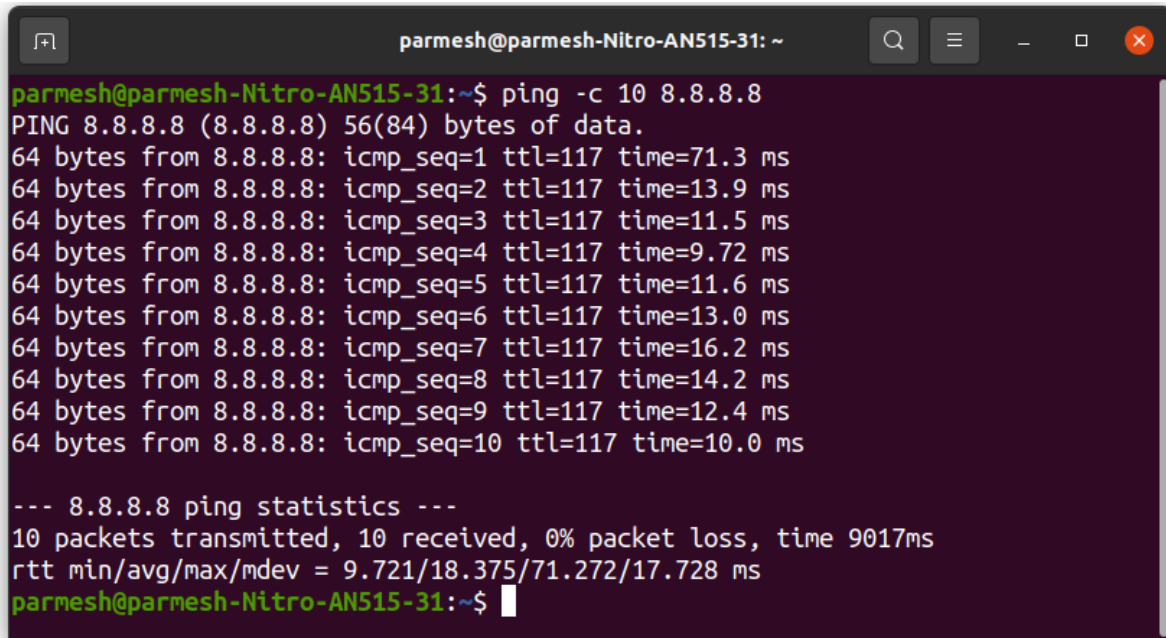
#### 5. A list of intermediate routers to reach 8.8.8.8 from your machine, with latency

The `traceroute` command is used to look up the intermediate addresses that are accessed to reach a particular host (passwd as an argument with the command). The latency for each step is individually in each row, in the latter 3 columns, which show the time for 3 separate packets.

```
parmesh@parmesh-Nitro-AN515-31: ~  
parmesh@parmesh-Nitro-AN515-31:~$ traceroute 8.8.8.8  
traceroute to 8.8.8.8 (8.8.8.8), 64 hops max  
 1  192.168.1.1  1.158ms  0.941ms  0.915ms  
 2  171.76.72.1  4.304ms  3.779ms  3.455ms  
 3  125.21.0.185  3.894ms  3.561ms  3.980ms  
 4  182.79.152.115  10.173ms  31.749ms  23.878ms  
 5  72.14.208.234  11.829ms  11.451ms  8.245ms  
 6  10.23.215.158  13.945ms  11.483ms  11.880ms  
 7  8.8.8.8  14.113ms  9.669ms  12.579ms  
parmesh@parmesh-Nitro-AN515-31:~$
```

## 6. Send 10 echo requests to 8.8.8.8 server from your machine

We use the `ping` command with the `-c` flag to limit the number of requests to 10. This command sends ICMP echo requests to the address passed in the argument.

A terminal window titled 'parmesh@parmesh-Nitro-AN515-31: ~' showing the execution of the 'ping -c 10 8.8.8.8' command. The output displays 10 individual ping results with their respective sequence numbers, TTLs, and response times. It concludes with a summary of the statistics: 10 packets transmitted, 10 received, 0% packet loss, and a total time of 9017ms.

```
parmesh@parmesh-Nitro-AN515-31:~$ ping -c 10 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=71.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=13.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=11.5 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=117 time=9.72 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=117 time=11.6 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=117 time=13.0 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=117 time=16.2 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=117 time=14.2 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=117 time=12.4 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=117 time=10.0 ms

--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9017ms
rtt min/avg/max/mdev = 9.721/18.375/71.272/17.728 ms
parmesh@parmesh-Nitro-AN515-31:~$
```

## 7. Get the IP address of [www.bits-pilani.ac.in](http://www.bits-pilani.ac.in) domain

The `nslookup` command can be used to return the IP address for any domain. The site is hosted on two different servers and hence two different IP addresses are shown (under the Non-authoritative answer).

A terminal window titled 'parmesh@parmesh-Nitro-AN515-31: ~' showing the execution of the 'nslookup www.bits-pilani.ac.in' command. The output shows the authoritative server (127.0.0.53) and then a non-authoritative answer with two different IP addresses for the domain: 103.144.92.33 and 14.139.243.20.

```
parmesh@parmesh-Nitro-AN515-31:~$ nslookup www.bits-pilani.ac.in
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
www.bits-pilani.ac.in canonical name = universe.bits-pilani.ac.in.
Name:   universe.bits-pilani.ac.in
Address: 103.144.92.33
Name:   universe.bits-pilani.ac.in
Address: 14.139.243.20

parmesh@parmesh-Nitro-AN515-31:~$
```