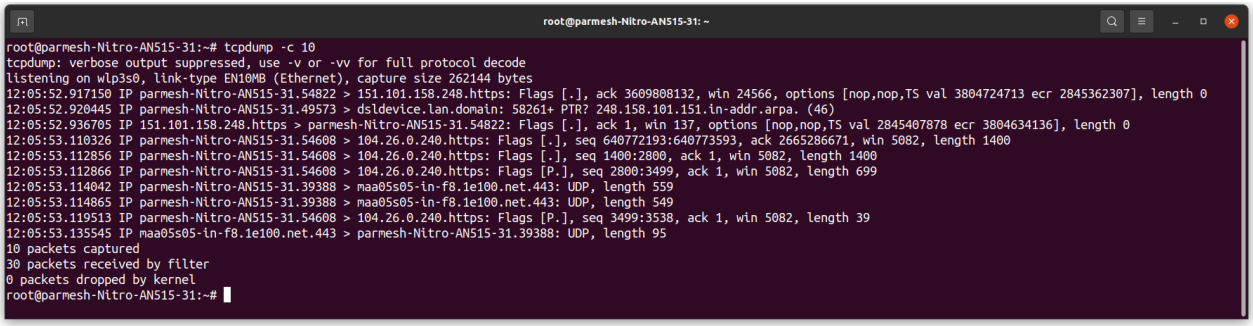
Lab1

Parmesh Mathur 2018A7PS0133G

1) tcpdump

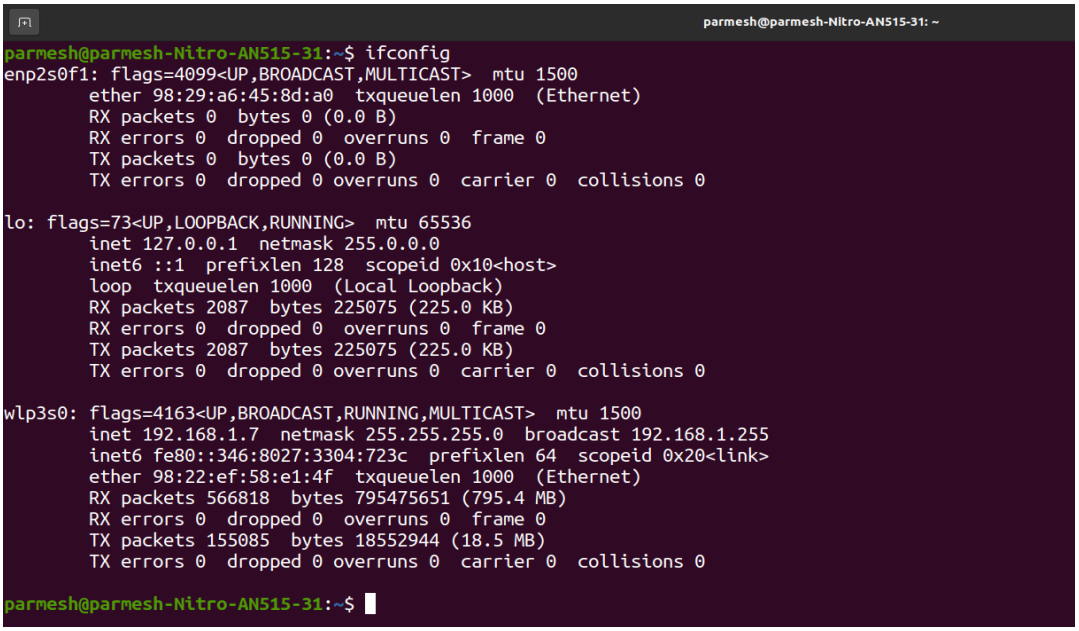
This command lists out all the packets passing through the top interface (wlp3s0 here) until interrrupted (or constricted using the -c flag as shown). Each line displays the details of each packet, like the time it is sent/received, the source and destination address and length.



```
root@parmesh-Nitro-AN515-31: ~
root@parmesh-Nitro-AN515-31:~# tcpdump -c 10
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:05:52.917150 IP parmesh-Nitro-AN515-31.54822 > 151.101.158.248.https: Flags [.], ack 3609808132, win 24566, options [nop,nop,TS val 3804724713 ecr 2845362307], length 0
12:05:52.920445 IP parmesh-Nitro-AN515-31.49573 > dsldevice.lan.domain: 58261+ PTR? 248.158.101.151.in-addr.arpa. (46)
12:05:52.936705 IP 151.101.158.248.https > parmesh-Nitro-AN515-31.54822: Flags [.], ack 1, win 137, options [nop,nop,TS val 2845407878 ecr 3804634136], length 0
12:05:53.110326 IP parmesh-Nitro-AN515-31.54608 > 104.26.0.240.https: Flags [.], seq 640772193:640773593, ack 2665286671, win 5082, length 1400
12:05:53.112856 IP parmesh-Nitro-AN515-31.54608 > 104.26.0.240.https: Flags [.], seq 1400:2800, ack 1, win 5082, length 1400
12:05:53.112866 IP parmesh-Nitro-AN515-31.54608 > 104.26.0.240.https: Flags [P.], seq 2800:3499, ack 1, win 5082, length 699
12:05:53.114042 IP parmesh-Nitro-AN515-31.39388 > maa05s05-in-f8.1e100.net.443: UDP, length 559
12:05:53.114865 IP parmesh-Nitro-AN515-31.39388 > maa05s05-in-f8.1e100.net.443: UDP, length 549
12:05:53.119513 IP parmesh-Nitro-AN515-31.54608 > 104.26.0.240.https: Flags [P.], seq 3499:3538, ack 1, win 5082, length 39
12:05:53.135545 IP maa05s05-in-f8.1e100.net.443 > parmesh-Nitro-AN515-31.39388: UDP, length 95
10 packets captured
30 packets received by filter
0 packets dropped by kernel
root@parmesh-Nitro-AN515-31:~#
```

2) Ifconfig

This command shows all the active interfaces on the system. It also shows us other details about them (like type and address) and the traffic passing through them.



```
parmesh@parmesh-Nitro-AN515-31: ~
parmesh@parmesh-Nitro-AN515-31:~$ ifconfig
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 2087  bytes 225075 (225.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2087  bytes 225075 (225.0 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 566818  bytes 795475651 (795.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 155085  bytes 18552944 (18.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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

3) dig

This command gives us info about the dns of www.google.com, which is a host that is present on the internet (indicated by the IN tag in the ANSWER SECTION), and has an IPv4 of 142.250.67.36 (from the last column in the ANSWER SECTION).

```
parmesh@parmesh-Nitro-AN515-31: ~
parmesh@parmesh-Nitro-AN515-31:~$ man dig
parmesh@parmesh-Nitro-AN515-31:~$ dig www.google.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7819
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.google.com.                IN      A

;; ANSWER SECTION:
www.google.com.         210     IN      A       142.250.67.36

;; Query time: 52 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sun Jan 24 23:47:26 IST 2021
;; MSG SIZE  rcvd: 59

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

4) arp

This command will display the contents of the ARP cache table. Here the cache table has only one entry, and th command shows the name of the host (its address when using the -n flag), its hardware address and the interface it is using.

```
parmesh@parmesh-Nitro-AN515-31: ~
parmesh@parmesh-Nitro-AN515-31:~$ man arp
parmesh@parmesh-Nitro-AN515-31:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
dsldevice.lan            ether   78:17:35:1e:d6:c0   C                     wlp3s0
parmesh@parmesh-Nitro-AN515-31:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.1              ether   78:17:35:1e:d6:c0   C                     wlp3s0
parmesh@parmesh-Nitro-AN515-31:~$
```

5) netstat

This command displays the information of the networking subsystems, like the open sockets, network conections and interfaces. Each row is a new entry and contains details about the corresponding entity.

```
parmesh@parmesh-Nitro-AN515-31: ~
parmesh@parmesh-Nitro-AN515-31:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 parmesh-Nitro-AN5:37314 74.125.24.188:https     ESTABLISHED
tcp        0      1 parmesh-Nitro-AN5:58006 594.bm-nginx-load:https SYN_SENT
tcp        0      0 parmesh-Nitro-AN5:57312 171.241.190.35.bc.:4070 ESTABLISHED
tcp        0      0 parmesh-Nitro-AN5:47462 maa05s05-in-f1.1e:https ESTABLISHED
tcp        0      0 parmesh-Nitro-AN5:36446 69.173.159.43:https     ESTABLISHED
tcp        0      0 parmesh-Nitro-AN5:51392 47.224.186.35.bc.:https ESTABLISHED
tcp        0      0 parmesh-Nitro-AN5:56248 151.101.158.248:https   ESTABLISHED
tcp        0      0 parmesh-Nitro-AN5:50094 103.229.206.238:https   ESTABLISHED
tcp        0      0 parmesh-Nitro-AN5:58026 69.173.159.48:https     ESTABLISHED
tcp        0      0 parmesh-Nitro-AN5:48666 a104-122-3-212.de:https ESTABLISHED
tcp        0      0 parmesh-Nitro-AN5:56250 151.101.158.248:https   ESTABLISHED
tcp        0      0 parmesh-Nitro-AN5:58028 69.173.159.48:https     ESTABLISHED
tcp        0      1 parmesh-Nitro-AN5:58002 594.bm-nginx-load:https SYN_SENT
tcp        0      0 parmesh-Nitro-AN5:56218 151.101.158.248:https   ESTABLISHED
tcp        0      0 parmesh-Nitro-AN5:52640 maa03s36-in-f5.1e:https ESTABLISHED
tcp        0      0 parmesh-Nitro-AN5:56544 25.224.186.35.bc.:https ESTABLISHED
tcp        1      0 parmesh-Nitro-AN5:58002 25.224.186.35.bc.:https CLOSE_WAIT
tcp        0      0 parmesh-Nitro-AN5:58034 25.224.186.35.bc.:https ESTABLISHED
udp        0      0 parmesh-Nitro-AN5:58130 hkg12s10-in-f2.1e10:443 ESTABLISHED
udp        0      0 parmesh-Nitro-AN5:38150 hkg12s10-in-f2.1e10:443 ESTABLISHED
udp        0      0 parmesh-Nitro-AN5:42971 hkg12s10-in-f2.1e10:443 ESTABLISHED
udp        0      0 parmesh-Nitro-AN5:35146 bom07s20-in-f2.1e10:443 ESTABLISHED
udp        0      0 parmesh-Nitro-AN5:35243 172.253.118.189:443     ESTABLISHED
udp        0      0 parmesh-Nitro-AN5:36544 hkg12s10-in-f2.1e10:443 ESTABLISHED
udp        0      0 parmesh-Nitro-AN5:44809 maa03s26-in-f14.1e1:443 ESTABLISHED
udp        0      0 parmesh-Nitro-AN:bootpc dsldevice.lan:bootps    ESTABLISHED
udp        0      0 parmesh-Nitro-AN5:57897 sb-in-f189.1e100.ne:443 ESTABLISHED
udp        0      0 parmesh-Nitro-AN5:53873 maa05s01-in-f3.1e10:443 ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    43962    /run/user/1000/systemd/notify
unix  2      [ ]         DGRAM                    34730    /run/wpa_supplicant/wlp3s0
unix  2      [ ]         DGRAM                    34748    /run/wpa_supplicant/p2p-dev-wlp3s0
unix  4      [ ]         DGRAM                    1583     /run/systemd/notify
unix  2      [ ]         DGRAM                    1597     /run/systemd/journal/syslog
unix  16     [ ]         DGRAM                    1607     /run/systemd/journal/dev-log
unix  8      [ ]         DGRAM                    1611     /run/systemd/journal/socket
unix  3      [ ]         SEQPACKET  CONNECTED     86259    @0000d
unix  3      [ ]         SEQPACKET  CONNECTED     86261    @0000e
unix  3      [ ]         SEQPACKET  CONNECTED     53086    @0000b
unix  3      [ ]         SEQPACKET  CONNECTED     53088    @0000c
unix  3      [ ]         STREAM     CONNECTED     67532
```

6) telnet

This command is used for interactive communication with an external host (either by invoking the host name with the command itself or by explicitly opening a connection with the host in the prompt). Typing the command will start a prompt.

```
parmesh@parmesh-Nitro-AN515-31: ~
parmesh@parmesh-Nitro-AN515-31:~$ telnet
telnet> ?
Commands may be abbreviated.  Commands are:

close           close current connection
logout          forcibly logout remote user and close the connection
display         display operating parameters
mode            try to enter line or character mode ('mode ?' for more)
open            connect to a site
quit            exit telnet
send            transmit special characters ('send ?' for more)
set             set operating parameters ('set ?' for more)
unset           unset operating parameters ('unset ?' for more)
status          print status information
toggle          toggle operating parameters ('toggle ?' for more)
slc             set treatment of special characters

z               suspend telnet
environ         change environment variables ('environ ?' for more)
telnet> quit
parmesh@parmesh-Nitro-AN515-31:~$
```

7) traceroute

This command traces the route to a particular host (www.google.com here). It lists out line by line the addresses that are communicated with before finally reaching the desired address (172.217.26.228).

```
parmesh@parmesh-Nitro-AN515-31: ~
parmesh@parmesh-Nitro-AN515-31:~$ traceroute www.google.com
traceroute to www.google.com (172.217.26.228), 64 hops max
  1   192.168.1.1  2.643ms  *  55.040ms
  2   171.76.72.1  6.588ms  7.484ms  5.204ms
  3   125.21.0.185  6.952ms  3.961ms  *
  4   182.79.142.218  30.104ms  13.275ms  11.907ms
  5   72.14.216.192  17.249ms  13.389ms  13.825ms
  6   *  182.79.239.193  92.143ms  *
  7   72.14.208.234  17.973ms  16.783ms  22.643ms
  8   10.252.240.158  12.508ms  15.263ms  11.185ms
  9   *  64.233.174.2  158.312ms  27.689ms
 10   *  72.14.236.174  46.680ms  40.224ms
 11   216.239.51.199  30.882ms  28.256ms  27.138ms
 12   172.217.26.228  40.162ms  *  242.828ms
parmesh@parmesh-Nitro-AN515-31:~$
```

8) ping

Using this command www.google.com (IP 142.250.67.196) receives and returns 10 packets of data, each of size 64 bytes (shown in the first column of each row). Each row shows the time delay from sending to receiving the packet (in milliseconds). The bottom row shows aggregate statistics and details of the packets transacted.

```
parmesh@parmesh-Nitro-AN515-31: ~
parmesh@parmesh-Nitro-AN515-31:~$ ping -c 10 www.google.com
PING www.google.com (142.250.67.196) 56(84) bytes of data.
64 bytes from bom12s08-in-f4.1e100.net (142.250.67.196): icmp_seq=1 ttl=118 time=36.8 ms
64 bytes from bom12s08-in-f4.1e100.net (142.250.67.196): icmp_seq=2 ttl=118 time=30.8 ms
64 bytes from bom12s08-in-f4.1e100.net (142.250.67.196): icmp_seq=3 ttl=118 time=47.3 ms
64 bytes from bom12s08-in-f4.1e100.net (142.250.67.196): icmp_seq=4 ttl=118 time=31.0 ms
64 bytes from bom12s08-in-f4.1e100.net (142.250.67.196): icmp_seq=5 ttl=118 time=34.9 ms
64 bytes from bom12s08-in-f4.1e100.net (142.250.67.196): icmp_seq=6 ttl=118 time=36.8 ms
64 bytes from bom12s08-in-f4.1e100.net (142.250.67.196): icmp_seq=7 ttl=118 time=30.8 ms
64 bytes from bom12s08-in-f4.1e100.net (142.250.67.196): icmp_seq=8 ttl=118 time=33.1 ms
64 bytes from bom12s08-in-f4.1e100.net (142.250.67.196): icmp_seq=9 ttl=118 time=40.7 ms
64 bytes from bom12s08-in-f4.1e100.net (142.250.67.196): icmp_seq=10 ttl=118 time=29.5 ms

--- www.google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 29.462/35.157/47.258/5.230 ms
parmesh@parmesh-Nitro-AN515-31:~$
```

P.T.O.

9) top

This command shows the state of the computer with respect to the resources being used by active processes. It also lists out some porcesses and their resource consumption details. This system is a single user process, hence USER is either ‘root’ or ‘parmesh’ for most processes.

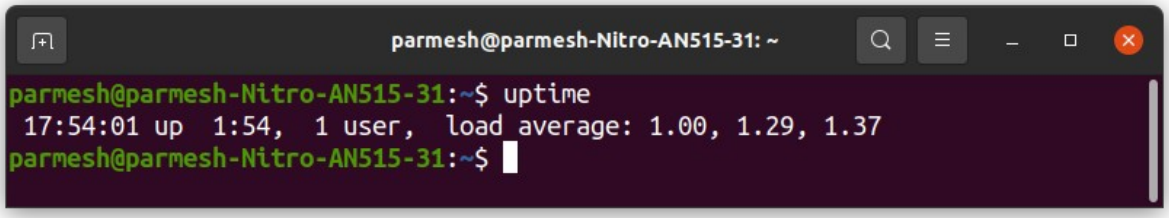
```
parmesh@parmesh-Nitro-AN515-31: ~
top - 12:31:09 up  2:06,  1 user,  load average: 0.90, 1.01, 1.07
Tasks: 286 total,   1 running, 285 sleeping,   0 stopped,   0 zombie
%Cpu(s):  3.0 us,  1.2 sy,  0.0 ni, 95.3 id,  0.5 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   7835.3 total,   2557.0 free,   2148.3 used,   3130.0 buff/cache
MiB Swap:    881.5 total,    881.5 free,      0.0 used.   4776.6 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   8201 parmesh   20   0 4106620 215220 123684 S   8.9   2.7   2:49.41 spotify
   1527 parmesh    9 -11 3318332  24640  19892 S   7.0   0.3   3:16.30 pulseaudio
   8378 parmesh   20   0 6155652 256612 140744 S   6.6   3.2   2:50.07 spotify
  10441 parmesh   20   0 5789440 127436  91056 S   3.6   1.6   0:06.22 chrome
   2964 parmesh   20   0 3368728 396896 137812 S   2.6   4.9   9:20.62 chrome
  10253 parmesh   20   0 5796788 131548  90324 S   2.3   1.6   0:08.31 chrome
   3093 parmesh   20   0 1494884 127540  80672 S   2.0   1.6   2:15.72 chrome
   3243 parmesh   20   0 9891.1m 276688 113872 S   1.7   3.4   2:02.30 chrome
   8344 parmesh   20   0  865616  89280  72812 S   1.3   1.1   0:29.13 spotify
   1771 parmesh   20   0 5052212 291388 103848 S   1.0   3.6   6:28.69 gnome-shell
     11 root      20   0       0      0      0 I   0.3   0.0   0:09.47 rcu_sched
    794 systemd+  20   0   24892  14268   9352 S   0.3   0.2   0:01.99 systemd-resolve
   1617 parmesh   20   0 1332440 100412  66720 S   0.3   1.3   6:52.16 Xorg
   3356 parmesh   20   0 1215140  70108  60088 S   0.3   0.9   0:30.11 chrome
   4470 parmesh   20   0  818460  54212  39528 S   0.3   0.7   0:17.79 gnome-terminal-
   7543 root      20   0       0      0      0 I   0.3   0.0   0:01.10 kworker/u16:2-phy0
  10579 parmesh   20   0   12016   4060   3256 R   0.3   0.1   0:00.09 top
      1 root      20   0  167908  11784   8456 S   0.0   0.1   0:04.68 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.01 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-kblockd
      9 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
     10 root      20   0       0      0      0 S   0.0   0.0   0:00.11 ksoftirqd/0
     12 root      rt   0       0      0      0 S   0.0   0.0   0:00.03 migration/0
     13 root     -51   0       0      0      0 S   0.0   0.0   0:00.00 idle_inject/0
     14 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
     15 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/1
     16 root     -51   0       0      0      0 S   0.0   0.0   0:00.00 idle_inject/1
     17 root      rt   0       0      0      0 S   0.0   0.0   0:00.12 migration/1
     18 root      20   0       0      0      0 S   0.0   0.0   0:00.09 ksoftirqd/1
     20 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/1:0H-kblockd
     21 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/2
     22 root     -51   0       0      0      0 S   0.0   0.0   0:00.00 idle_inject/2
     23 root      rt   0       0      0      0 S   0.0   0.0   0:00.12 migration/2
     24 root      20   0       0      0      0 S   0.0   0.0   0:00.06 ksoftirqd/2
     26 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/2:0H-kblockd
     27 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/3
```

10) wall

This command send all the other users of the system a message, that is taken either from standard input or from an existing text file. If the machine has only one user, no message will show up to the user who has put it up.

11) uptime

This command simply displays the amount of time that the system has been running for.



12) nslookup

This command helps us 'look up' the server corresponding to the name (www.google.com here) of a host. It also displays basic information like address of the host.