Lab 1 Network Commands

1) tcpdump

```
vaibhav@Jarvis:~$ sudo su
[sudo] password for vaibhav:
root@Jarvis:/home/vaibhav# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
14:54:42.384355 IP 74.125.24.189.443 > Jarvis.54831: UDP, length 44
14:54:42.385435 IP Jarvis.38696 > 192.168.43.1.domain: 54741+ PTR? 15.2.0.10.in-addr.arpa. (40)
14:54:42.390598 IP 192.168.43.1.domain > Jarvis.38696: 54741 NXDomain 0/0/0 (40)
14:54:42.391139 IP Jarvis.52935 > 192.168.43.1.domain: 47286+ PTR? 189.24.125.74.in-addr.arpa. (44)
14:54:42.411677 IP Jarvis.54831 > 74.125.24.189.443: UDP, length 33
14:54:43.079267 IP 192.168.43.1.domain > Jarvis.52935: 47286 NXDomain 0/1/0 (104)
14:54:43.079909 IP Jarvis.60276 > 192.168.43.1.domain: 42162+ PTR? 1.43.168.192.in-addr.arpa. (43)
14:54:43.086866 IP 192.168.43.1.domain > Jarvis.60276: 42162 NXDomain 0/0/0 (43)
14:54:44.766379 IP Jarvis.38798 > 49.44.208.83.http: Flags [.], ack 51904003, win 64239, length 0
14:54:44.766404 IP Jarvis.39132 > 104.22.11.214.https: Flags [.], ack 185937151, win 65535, length 0
14:54:44.766410 IP Jarvis.34814 > maa03s19-in-f110.1e100.net.http: Flags [.], ack 51712003, win 64239, length 0
14:54:44.766899 IP Jarvis.58652 > 192.168.43.1.domain: 46510+ PTR? 83.208.44.49.in-addr.arpa. (43)
14:54:44.766953 IP 49.44.208.83.http > Jarvis.38798: Flags [.], ack 1, win 65535, length 0
14:54:44.766959 IP 104.22.11.214.https > Jarvis.39132: Flags [.], ack 1, win 65535, length 0
14:54:44.766960 IP maa03s19-in-f110.1e100.net.http > Jarvis.34814: Flags [.], ack 1, win 65535, length 0
14:54:45.068658 IP 192.168.43.1.domain > Jarvis.58652: 46510 ServFail 0/0/0 (43)
14:54:45.069143 IP Jarvis.57427 > 192.168.43.1.domain: 58849+ PTR? 83.208.44.49.in-addr.arpa. (43)
14:54:45.125963 IP 192.168.43.1.domain > Jarvis.57427: 58849 ServFail 0/0/0 (43)
14:54:45.126627 IP Jarvis.46815 > 192.168.43.1.domain: 33599+ PTR? 214.11.22.104.in-addr.arpa. (44)
14:54:45.243910 IP 192.168.43.1.domain > Jarvis.46815: 33599 NXDomain 0/1/0 (106)
14:54:45.244543 IP Jarvis.42398 > 192.168.43.1.domain: 49749+ PTR? 110.196.58.216.in-addr.arpa. (45)
14:54:45.285840 IP 192.168.43.1.domain > Jarvis.42398: 49749 2/0/0 PTR maa03s19-in-f110.1e100.net., PTR del11s05-in-f14.1e100.net. (115)
^C
22 packets captured
22 packets received by filter
0 packets dropped by kernel
```

tcpdump command allows the user to display the information of the packets that are being received or transmitted over the network connected to the computer. It prints the contents of the network packets. This description comes along with the time at which the packets are being transmitted and received and also the information of two machines among which they are being transmitted.

2) ifconfig

```
root@Jarvis:/home/vaibhav# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::4008:a47:49ac:698b  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:fd:57:df  txqueuelen 1000  (Ethernet)
        RX packets 412746  bytes 569537166 (569.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 94568  bytes 8519437 (8.5 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 1350  bytes 138918 (138.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1350  bytes 138918 (138.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Ifconfig is used to configure, enable and disable the network interfaces. It displays the status of the currently active interfaces. It can also be used to set the IP Address and netmask of the network interface.

3) **dig**

```
root@Jarvis:/home/vaibhav# dig

; <<>> DiG 9.16.1-Ubuntu <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2510
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       169118  IN      NS      f.root-servers.net.
.                       169118  IN      NS      g.root-servers.net.
.                       169118  IN      NS      h.root-servers.net.
.                       169118  IN      NS      i.root-servers.net.
.                       169118  IN      NS      j.root-servers.net.
.                       169118  IN      NS      k.root-servers.net.
.                       169118  IN      NS      l.root-servers.net.
.                       169118  IN      NS      m.root-servers.net.
.                       169118  IN      NS      a.root-servers.net.
.                       169118  IN      NS      b.root-servers.net.
.                       169118  IN      NS      c.root-servers.net.
.                       169118  IN      NS      d.root-servers.net.
.                       169118  IN      NS      e.root-servers.net.

;; Query time: 79 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Jan 25 15:10:54 IST 2021
;; MSG SIZE  rcvd: 239
```

dig(Domain Information Groper) is used to receive information of DNS name servers. It displays the answers to the query provided that are returned from the server names specified. It also gives us information about the query time, the server, when was the query made and the message size received.

4) **arp**

```
root@Jarvis:/home/vaibhav# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   52:54:00:12:35:02   C                     enp0s3
```

arp(Address Resolution Protocol) is used to display/manipulate the kernel's IPv4 neighbor network cache. It can find the MAC Address of a network neighbor for a given IPv4 Address.

5) **netstat**

```
root@Jarvis:/home/vaibhav# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 Jarvis:43946           104.25.132.119:https    ESTABLISHED
tcp        0      0 Jarvis:57598           ec2-23-23-120-57.:https ESTABLISHED
tcp        0      0 Jarvis:59254           104.26.7.139:https      ESTABLISHED
tcp        0      0 Jarvis:39866           151.101.154.109:https   ESTABLISHED
tcp        0      0 Jarvis:37346           89.207.16.201:https     ESTABLISHED
tcp        0      0 Jarvis:50566           104.18.13.5:https       ESTABLISHED
tcp        0      0 Jarvis:49542           ip21.67-202-110.s:https ESTABLISHED
tcp        0      0 Jarvis:58918           104.18.102.194:https    ESTABLISHED
tcp        1      0 Jarvis:53104           49.44.184.210:http      CLOSE_WAIT
tcp        0      0 Jarvis:59832           49.44.150.150:https     ESTABLISHED
tcp        0      0 Jarvis:43506           ec2-3-227-190-204:https ESTABLISHED
tcp        0      0 Jarvis:49562           ip21.67-202-110.s:https TIME_WAIT
tcp        0      0 Jarvis:36236           104.16.18.94:https      ESTABLISHED
tcp        0      0 Jarvis:60004           49.44.150.150:https     ESTABLISHED
tcp        0      0 Jarvis:51318           74.125.24.188:5228      ESTABLISHED
tcp        0      1 Jarvis:34676           594.bm-nginx-load:https SYN_SENT
tcp        0      0 Jarvis:59994           49.44.150.150:https     ESTABLISHED
^C
```

It gives information about the Linux Networking Subsystem. It displays a list of open sockets.

6) **telnet**

```
root@Jarvis:/home/vaibhav# telnet localhost
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
Jarvis login: vaibhav
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-56-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be installed immediately.
0 of these updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
*** System restart required ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

telnet command is used to provide a bidirectional interactive text-based communication facility using the TELNET protocol.

7) **traceroute**

```
vaibhav@Jarvis:~$ traceroute google.com
traceroute to google.com (172.217.24.238), 64 hops max
  1   10.0.2.2  0.438ms  0.359ms  0.284ms
  2   *  *  *
  3   *  *  *
  4   *  *  *
  5   *  *  *
  6   *  *  *
  7   *  *  *
  8   *  *  *
```

traceroute prints the path taken by the package to reach the host. It gives info about all the hops that a packet takes to reach the host machine.

8) **ping**

```
root@Jarvis:/home/vaibhav# ping localhost
PING localhost (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.015 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.020 ms
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.021 ms
^C
--- localhost ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2034ms
rtt min/avg/max/mdev = 0.015/0.018/0.021/0.002 ms
root@Jarvis:/home/vaibhav# ping www.google.com
PING www.google.com (216.58.221.36) 56(84) bytes of data.
64 bytes from kul01s10-in-f36.1e100.net (216.58.221.36): icmp_seq=1 ttl=110 time=44.7 ms
64 bytes from kul01s10-in-f36.1e100.net (216.58.221.36): icmp_seq=2 ttl=110 time=227 ms
64 bytes from kul01s10-in-f36.1e100.net (216.58.221.36): icmp_seq=3 ttl=110 time=62.8 ms
^C
--- www.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 44.692/111.435/226.829/81.929 ms
```

Ping (Packet Internet Groper) is used to check the network connectivity between the 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.

9) top

```
top - 16:02:48 up  1:30,  3 users,  load average: 0.91, 0.65, 0.38
Tasks: 277 total,   1 running, 276 sleeping,   0 stopped,   0 zombie
%Cpu(s): 17.2 us,  2.4 sy,  0.0 ni, 79.6 id,  0.2 wa,  0.0 hi,  0.6 si,  0.0 st
MiB Mem :   5417.8 total,    520.6 free,   2107.3 used,   2790.0 buff/cache
MiB Swap:    925.5 total,    910.1 free,     15.3 used.   2883.8 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
  22598 vaibhav   20   0  731052 228964  91324 S  43.9   4.1   5:16.85 chrome
   7898 vaibhav   20   0 4827088 383656 126288 S  30.6   6.9   5:33.18 gnome-shell
   7362 vaibhav   20   0  864804  99736  58240 S   7.6   1.8   1:17.38 Xorg
  22557 vaibhav   20   0  965052 286104 127500 S   4.7   5.2   1:45.96 chrome
  22601 vaibhav   20   0  390824  99320  66396 S   1.0   1.8   0:22.45 chrome
  59422 vaibhav   20   0 4631356 129236  87924 S   0.7   2.3   0:01.62 chrome
  59714 vaibhav   20   0 4616460 124608  80624 S   0.7   2.2   0:00.92 chrome
     11 root      20   0       0      0      0 I   0.3   0.0   0:01.16 rcu_sched
    216 root       0 -20       0      0      0 I   0.3   0.0   0:00.50 kworker/1:1H-kblockd
    218 root      20   0       0      0      0 S   0.3   0.0   0:00.83 jbd2/sda5-8
      1 root      20   0  105852  13344   8428 S   0.0   0.2   4:44.13 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.00 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   0:00.07 ksoftirqd/0
     12 root      rt   0       0      0      0 S   0.0   0.0   0:00.02 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   0:02.48 migration/1
     18 root      20   0       0      0      0 S   0.0   0.0   0:00.08 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   0:02.47 migration/2
     24 root      20   0       0      0      0 S   0.0   0.0   0:00.11 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
     28 root     -51   0       0      0      0 S   0.0   0.0   0:00.00 idle_inject/3
     29 root      rt   0       0      0      0 S   0.0   0.0   0:02.47 migration/3
     30 root      20   0       0      0      0 S   0.0   0.0   0:00.31 ksoftirqd/3
     32 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/3:0H-kblockd
     33 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kdevtmpfs
     34 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 netns
     35 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tasks_kthre
     36 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kauditd
     38 root      20   0       0      0      0 S   0.0   0.0   0:00.00 khungtaskd
     39 root      20   0       0      0      0 S   0.0   0.0   0:00.00 oom_reaper
```

top provides a dynamic real-time view of the Linux Processes. It displays information about the processes and the threads that are currently managed by the kernel.

10) wall

```
vaibhav@Jarvis:~$ who
vaibhav  :0           2021-01-25 14:32 (:0)
vaibhav  pts/1        2021-01-25 15:35 (localhost)
vaibhav@Jarvis:~$ wall Vaibhav
vaibhav@Jarvis:~$ wall Computer Networks Lab 1
```

```
root@Jarvis:/home/vaibhav# telnet localhost
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
Jarvis login: vaibhav
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-56-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be installed immediately.
0 of these updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
*** System restart required ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


Broadcast message from vaibhav@Jarvis (pts/2) (Mon Jan 25 15:35:51 2021):

Vaibhav


Broadcast message from vaibhav@Jarvis (pts/2) (Mon Jan 25 15:36:19 2021):

Computer Networks Lab 1
```

It is used to display messages/contents of files/standard input on the terminals of all the logged-in users.

11) uptime

```
root@Jarvis:/home/vaibhav# uptime
 16:09:59 up  1:37,  3 users,  load average: 0.91, 0.68, 0.45
```

It displays information such as how long the system has been running, current time, number of users logged on and the system load averages for 1, 5 and 15 minutes.

12) nslookup

```
vaibhav@Jarvis:~$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 172.217.166.238
Name:   google.com
Address: 2404:6800:4002:809::200e
```

nslookup(Name Server Lookup) is a used to get information from the DNS server. It is used to obtain domain name or IP address mapping or any other specific DNS record.