UCS 1511 - Network Lab

Exercise 01 - Network Commands

Name:	Mahesh Bharadwaj K
Reg No:	185001089
Semester:	V
Date:	August 23, 2020

Aim:

To Learn and understand the use of commands like tcpdump, netstat, ifconfig, nslookup and traceroute, ping .

1. tcpdump

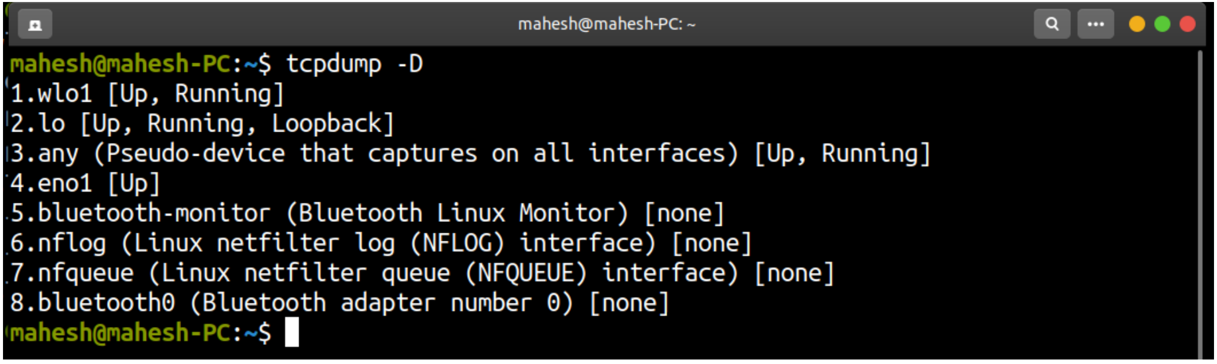
- **Description:**
  Tcpdump prints out a description of the contents of packets on a network interface that matches the boolean expression specified.
- **Syntax:** tcpdump [options]

Table 1: Options and their meanings

Option	Meaning
-D	List of interfaces tcpdump can track
-i ⟨*interface*⟩	Listen on specified interface
-c ⟨*count*⟩	Exit after receiving ‘count’ packets

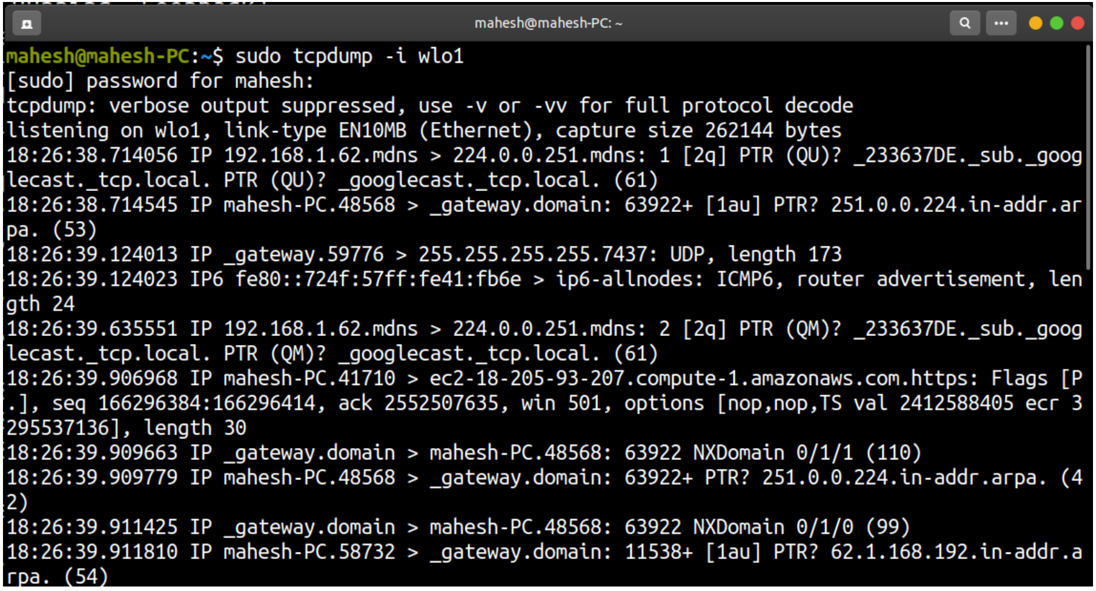
- **Output:**

Figure 1: **Listing Interfaces**



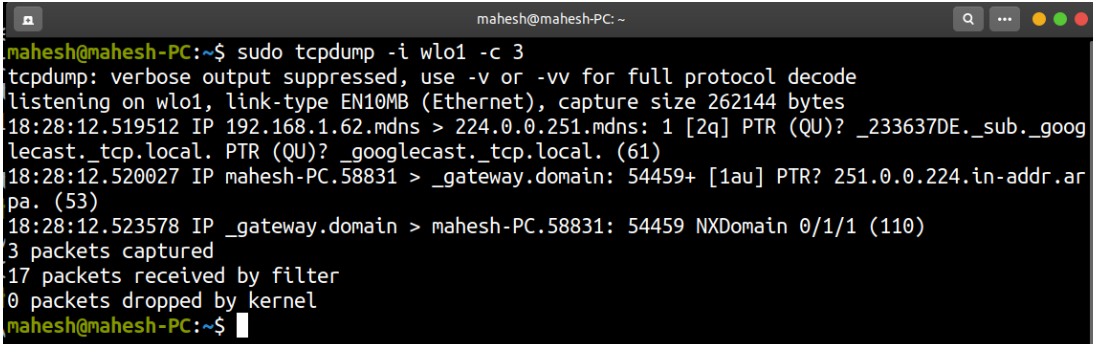
```
mahesh@mahesh-PC:~$ tcpdump -D
1.wlo1 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.eno1 [Up]
5.bluetooth-monitor (Bluetooth Linux Monitor) [none]
6.nflog (Linux netfilter log (NFLOG) interface) [none]
7.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
8.bluetooth0 (Bluetooth adapter number 0) [none]
mahesh@mahesh-PC:~$
```

Figure 2: **tcpdump for a particular interface**



```
mahesh@mahesh-PC:~$ sudo tcpdump -i wlo1
[sudo] password for mahesh:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
18:26:38.714056 IP 192.168.1.62.mdns > 224.0.0.251.mdns: 1 [2q] PTR (QU)? _233637DE._sub._goog
lecast._tcp.local. PTR (QU)? _googlecast._tcp.local. (61)
18:26:38.714545 IP mahesh-PC.48568 > _gateway.domain: 63922+ [1au] PTR? 251.0.0.224.in-addr.ar
pa. (53)
18:26:39.124013 IP _gateway.59776 > 255.255.255.255.7437: UDP, length 173
18:26:39.124023 IP6 fe80::724f:57ff:fe41:fb6e > ip6-allnodes: ICMP6, router advertisement, len
gth 24
18:26:39.635551 IP 192.168.1.62.mdns > 224.0.0.251.mdns: 2 [2q] PTR (QM)? _233637DE._sub._goog
lecast._tcp.local. PTR (QM)? _googlecast._tcp.local. (61)
18:26:39.906968 IP mahesh-PC.41710 > ec2-18-205-93-207.compute-1.amazonaws.com.https: Flags [P
.], seq 166296384:166296414, ack 2552507635, win 501, options [nop,nop,TS val 2412588405 ecr 3
295537136], length 30
18:26:39.909663 IP _gateway.domain > mahesh-PC.48568: 63922 NXDomain 0/1/1 (110)
18:26:39.909779 IP mahesh-PC.48568 > _gateway.domain: 63922+ PTR? 251.0.0.224.in-addr.arpa. (4
2)
18:26:39.911425 IP _gateway.domain > mahesh-PC.48568: 63922 NXDomain 0/1/0 (99)
18:26:39.911810 IP mahesh-PC.58732 > _gateway.domain: 11538+ [1au] PTR? 62.1.168.192.in-addr.a
rpa. (54)
```

Figure 3: **Listing 'count' packets**



```
mahesh@mahesh-PC:~$ sudo tcpdump -i wlo1 -c 3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
18:28:12.519512 IP 192.168.1.62.mdns > 224.0.0.251.mdns: 1 [2q] PTR (QU)? _233637DE._sub._goog
lecast._tcp.local. PTR (QU)? _googlecast._tcp.local. (61)
18:28:12.520027 IP mahesh-PC.58831 > _gateway.domain: 54459+ [1au] PTR? 251.0.0.224.in-addr.ar
pa. (53)
18:28:12.523578 IP _gateway.domain > mahesh-PC.58831: 54459 NXDomain 0/1/1 (110)
3 packets captured
17 packets received by filter
0 packets dropped by kernel
mahesh@mahesh-PC:~$
```

2. netstat

- **Description:**
  Print network connections, routing tables, interface statisics, masquerade connections, and multicast memberships.

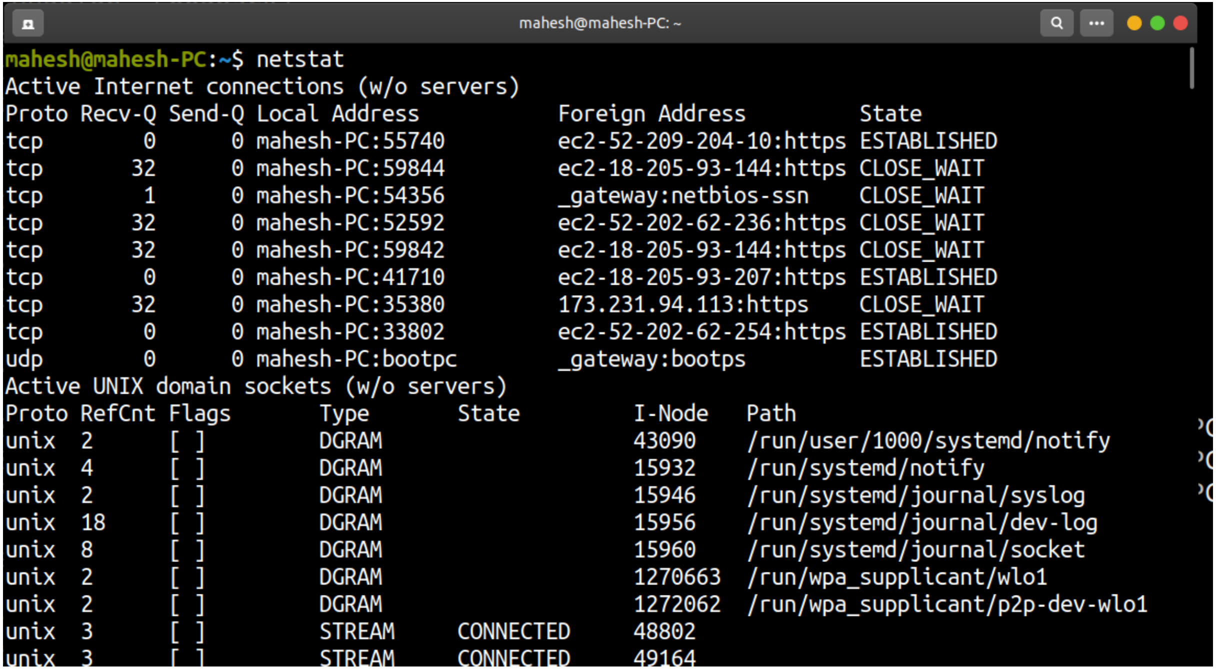
- **Syntax:** netstat [options]

Table 2: Option and their meanings

Option	Meaning
-a	Show both listening and non-listening sockets.
-s	Display summary statistics for each protocol.
-t	All TCP ports
-u	All UDP ports
-l	Listening ports

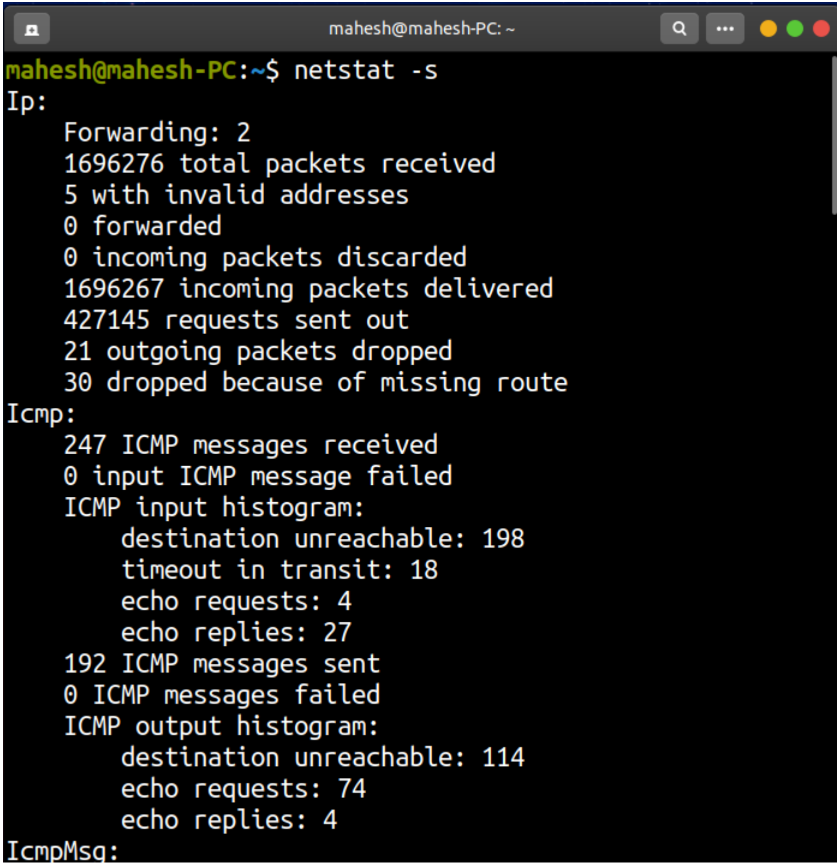
- **Output:**

Figure 4: **Output of netstat**



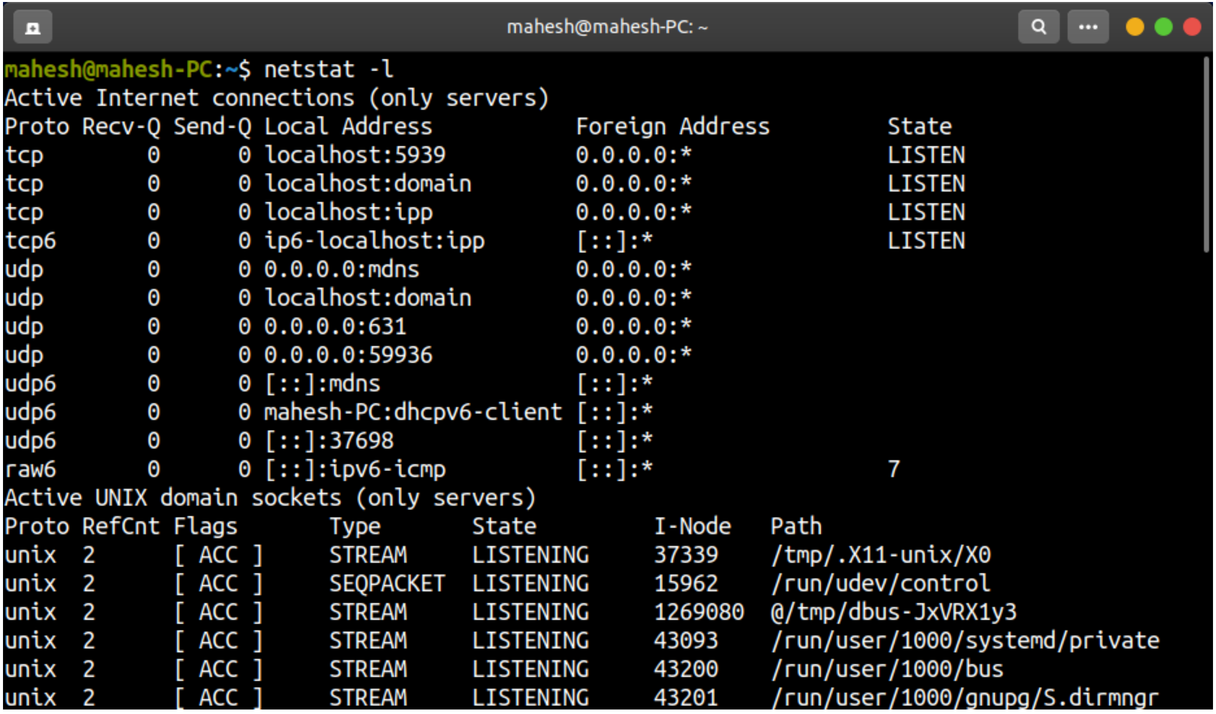
```
mahesh@mahesh-PC:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 mahesh-PC:55740         ec2-52-209-204-10:https ESTABLISHED
tcp       32      0 mahesh-PC:59844         ec2-18-205-93-144:https CLOSE_WAIT
tcp        1      0 mahesh-PC:54356         _gateway:netbios-ssn    CLOSE_WAIT
tcp       32      0 mahesh-PC:52592         ec2-52-202-62-236:https CLOSE_WAIT
tcp       32      0 mahesh-PC:59842         ec2-18-205-93-144:https CLOSE_WAIT
tcp        0      0 mahesh-PC:41710         ec2-18-205-93-207:https ESTABLISHED
tcp       32      0 mahesh-PC:35380         173.231.94.113:https    CLOSE_WAIT
tcp        0      0 mahesh-PC:33802         ec2-52-202-62-254:https ESTABLISHED
udp        0      0 mahesh-PC:bootpc        _gateway:bootps         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    43090    /run/user/1000/systemd/notify
unix  4      [ ]         DGRAM                    15932    /run/systemd/notify
unix  2      [ ]         DGRAM                    15946    /run/systemd/journal/syslog
unix  18     [ ]         DGRAM                    15956    /run/systemd/journal/dev-log
unix  8      [ ]         DGRAM                    15960    /run/systemd/journal/socket
unix  2      [ ]         DGRAM                    1270663  /run/wpa_supplicant/wlo1
unix  2      [ ]         DGRAM                    1272062  /run/wpa_supplicant/p2p-dev-wlo1
unix  3      [ ]         STREAM     CONNECTED     48802
unix  3      [ ]         STREAM     CONNECTED     49164
```

Figure 5: **Statistics for protocols**



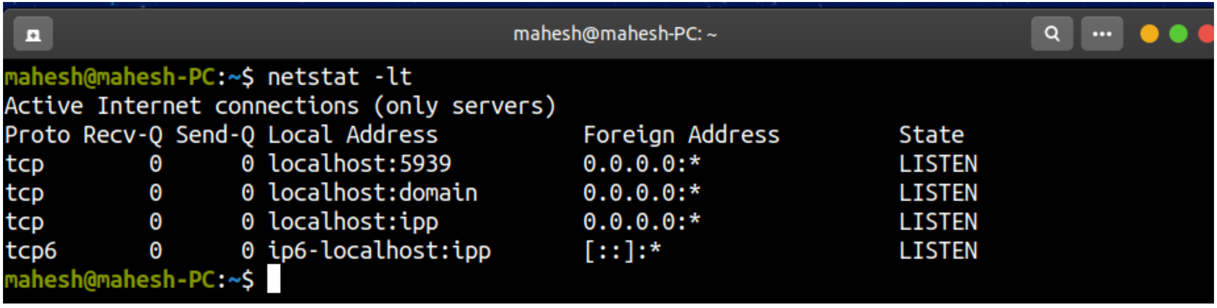
```
mahesh@mahesh-PC:~$ netstat -s
Ip:
    Forwarding: 2
    1696276 total packets received
    5 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    1696267 incoming packets delivered
    427145 requests sent out
    21 outgoing packets dropped
    30 dropped because of missing route
Icmp:
    247 ICMP messages received
    0 input ICMP message failed
    ICMP input histogram:
        destination unreachable: 198
        timeout in transit: 18
        echo requests: 4
        echo replies: 27
    192 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 114
        echo requests: 74
        echo replies: 4
IcmpMsg:
```

Figure 6: **Listening ports**



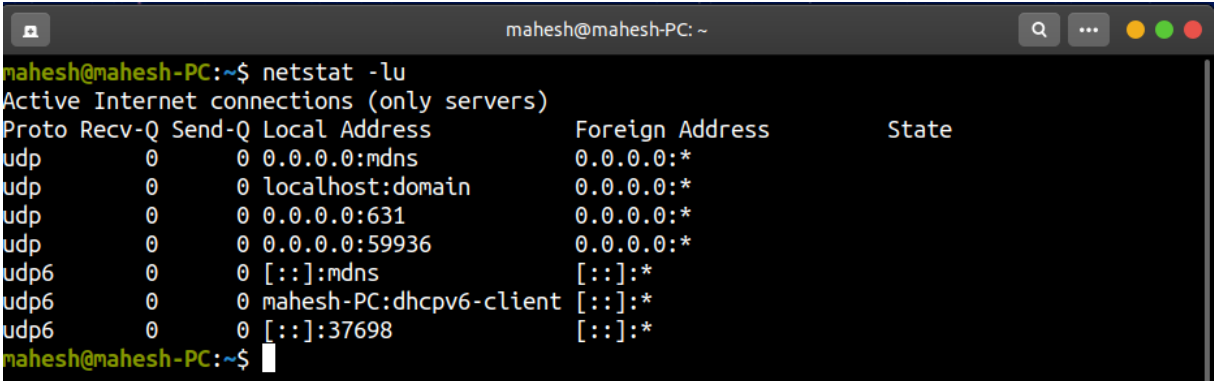
```
mahesh@mahesh-PC:~$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:5939          0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
udp        0      0 0.0.0.0:mdns            0.0.0.0:*
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp        0      0 0.0.0.0:59936           0.0.0.0:*
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 mahesh-PC:dhcpv6-client [::]:*
udp6       0      0 [::]:37698              [::]:*
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     37339    /tmp/.X11-unix/X0
unix  2      [ ACC ]     SEQPACKET  LISTENING     15962    /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     1269080  @/tmp/dbus-JxVRX1y3
unix  2      [ ACC ]     STREAM     LISTENING     43093    /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     43200    /run/user/1000/bus
unix  2      [ ACC ]     STREAM     LISTENING     43201    /run/user/1000/gnupg/S.dirmngr
```

Figure 7: **Listening TCP ports**



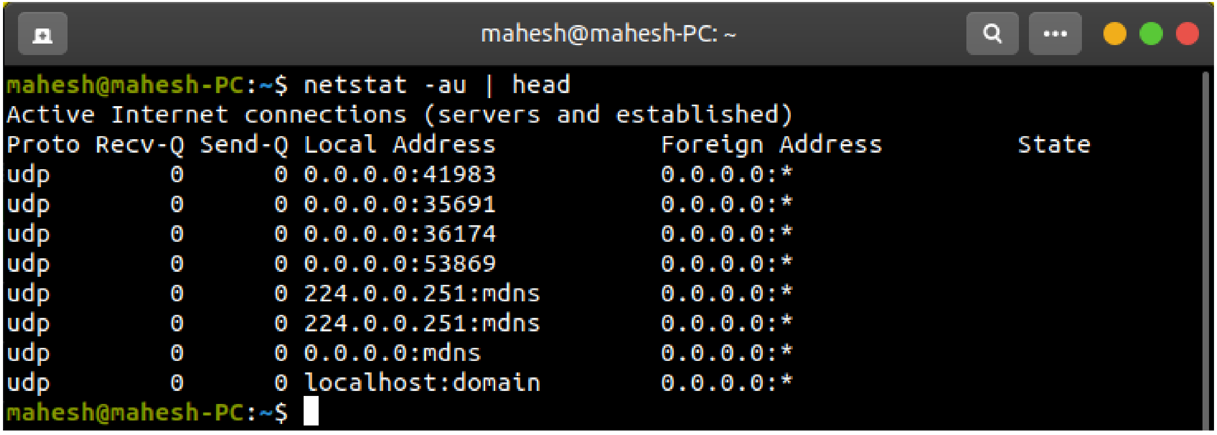
```
mahesh@mahesh-PC:~$ netstat -lt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:5939          0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
mahesh@mahesh-PC:~$
```

Figure 8: **Listening UDP ports**



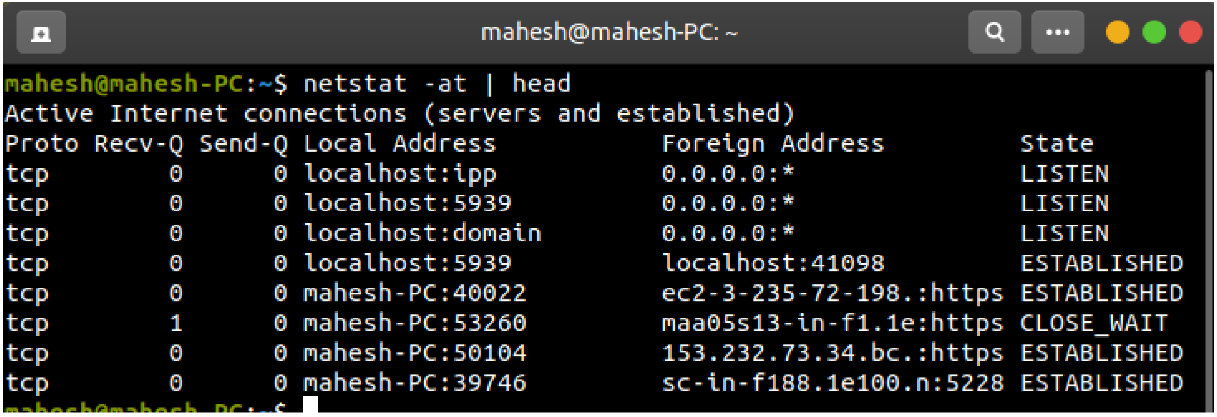
```
mahesh@mahesh-PC:~$ netstat -lu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 0.0.0.0:mdns            0.0.0.0:*
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp        0      0 0.0.0.0:59936           0.0.0.0:*
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 mahesh-PC:dhcpv6-client [::]:*
udp6       0      0 [::]:37698              [::]:*
mahesh@mahesh-PC:~$
```

Figure 9: **All UDP ports**



```
mahesh@mahesh-PC:~$ netstat -au | head
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 0.0.0.0:41983           0.0.0.0:*
udp        0      0 0.0.0.0:35691           0.0.0.0:*
udp        0      0 0.0.0.0:36174           0.0.0.0:*
udp        0      0 0.0.0.0:53869           0.0.0.0:*
udp        0      0 224.0.0.251:mdns        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 localhost:domain        0.0.0.0:*
mahesh@mahesh-PC:~$ 
```

Figure 10: **All TCP ports**



```
mahesh@mahesh-PC:~$ netstat -at | head
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 localhost:5939          0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:5939          localhost:41098         ESTABLISHED
tcp        0      0 mahesh-PC:40022         ec2-3-235-72-198.:https ESTABLISHED
tcp        1      0 mahesh-PC:53260         maa05s13-in-f1.1e:https CLOSE_WAIT
tcp        0      0 mahesh-PC:50104         153.232.73.34.bc.:https ESTABLISHED
tcp        0      0 mahesh-PC:39746         sc-in-f188.1e100.n:5228 ESTABLISHED
mahesh@mahesh-PC:~$ 
```

3. ifconfig

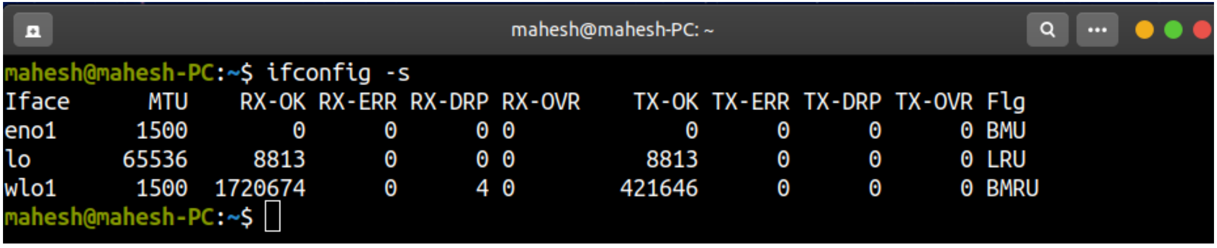
- **Description:**
  Command to configure network interfaces present in the system.
- **Syntax:** ifconfig [-options]

Table 3: Option and their meanings

Option	Meaning
-a	All interfaces available, even if they are not running.
-s	display a short list output

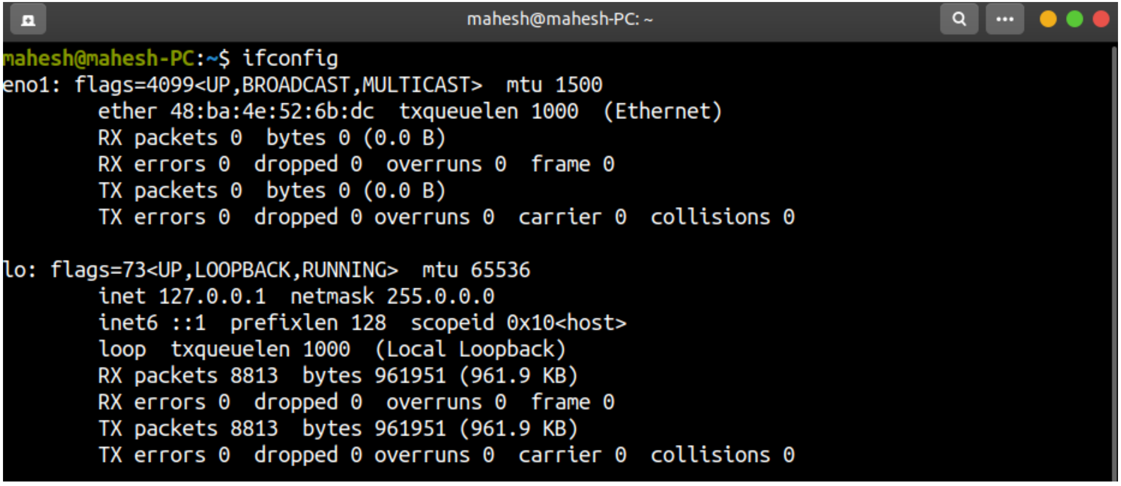
- **Output:**

Figure 11: **Short form output**



```
mahesh@mahesh-PC:~$ ifconfig -s
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eno1      1500        0      0      0 0             0      0      0      0 BMU
lo       65536     8813      0      0 0          8813      0      0      0 LRU
wlo1      1500  1720674      0      4 0        421646      0      0      0 BMRU
mahesh@mahesh-PC:~$ 
```

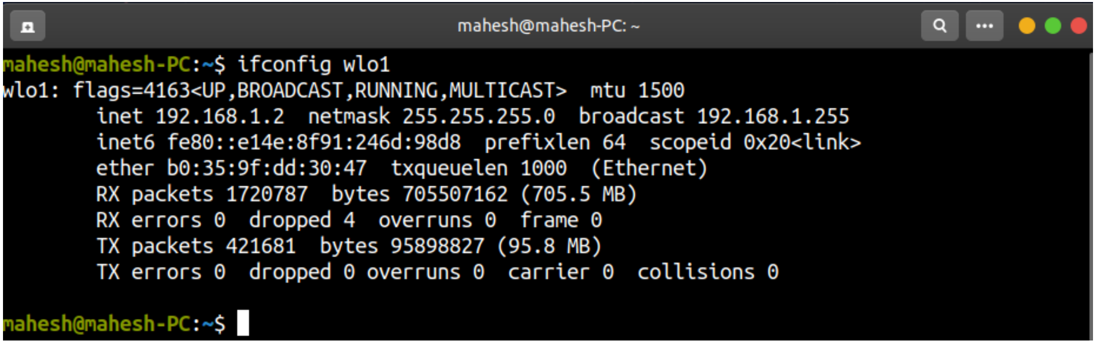
Figure 12: **Output of ifconfig**



```
mahesh@mahesh-PC:~$ ifconfig
eno1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 48:ba:4e:52:6b:dc  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 8813  bytes 961951 (961.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8813  bytes 961951 (961.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 13: **ifconfig of a particular interface**



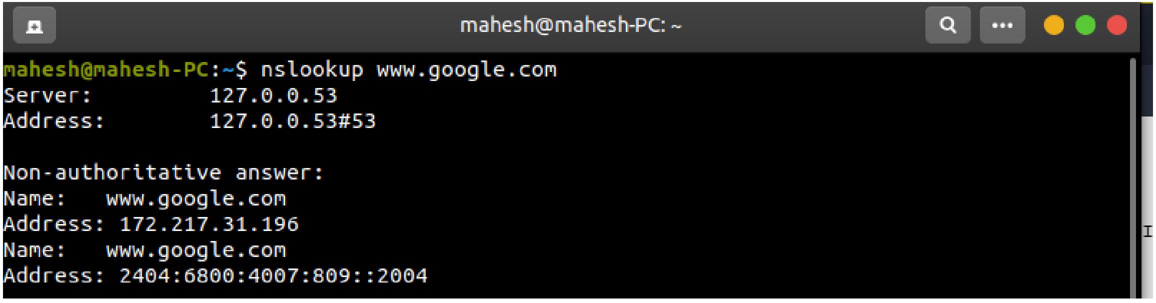
```
mahesh@mahesh-PC:~$ ifconfig wlo1
wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.2  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::e14e:8f91:246d:98d8  prefixlen 64  scopeid 0x20<link>
        ether b0:35:9f:dd:30:47  txqueuelen 1000  (Ethernet)
        RX packets 1720787  bytes 705507162 (705.5 MB)
        RX errors 0  dropped 4  overruns 0  frame 0
        TX packets 421681  bytes 95898827 (95.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

mahesh@mahesh-PC:~$ 
```

4. nslookup

- **Description:**
  Nslookup is a program to query Internet domain name servers for finding IP address given a URL or vice-versa.
- **Syntax:** nslookup [-option] [name | -] [server]
- **Output:**

Figure 14: **nslookup given URL**



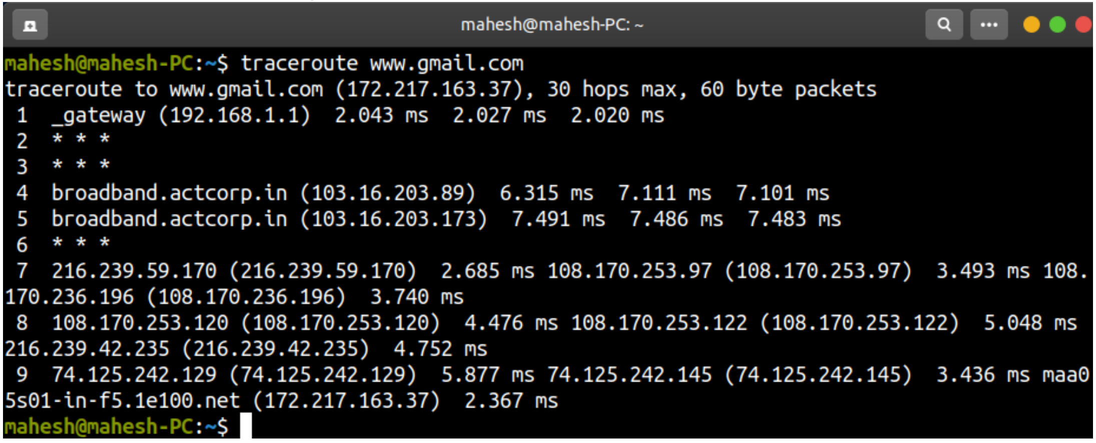
```
mahesh@mahesh-PC:~$ nslookup www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 172.217.31.196
Name:   www.google.com
Address: 2404:6800:4007:809::2004
```

5. traceroute

- **Description:**
  This command traces the route that packets takes to reach the host. It will show how many hops it takes to reach the host and time between each hop
- **Syntax:** traceroute [-option] ⟨*host*⟩.
- **Output:**

Figure 15: **traceroute of www.google.com**

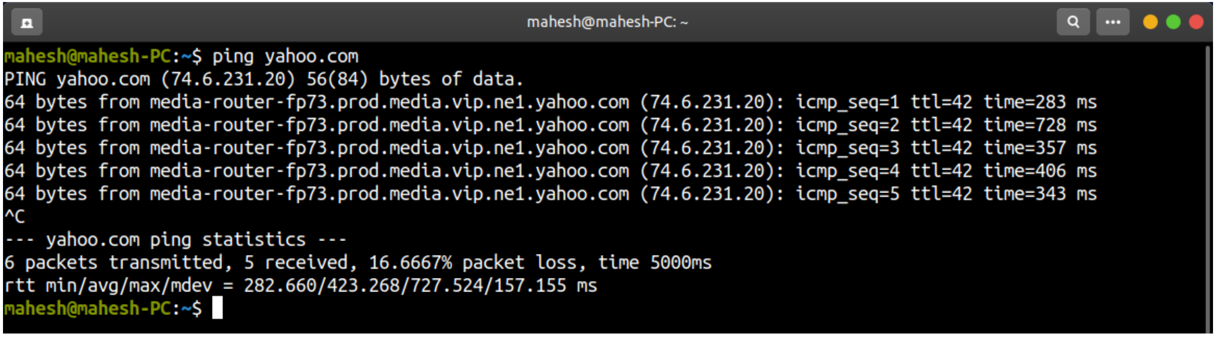


```
mahesh@mahesh-PC:~$ traceroute www.gmail.com
traceroute to www.gmail.com (172.217.163.37), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.1)  2.043 ms  2.027 ms  2.020 ms
 2  * * *
 3  * * *
 4  broadband.actcorp.in (103.16.203.89)  6.315 ms  7.111 ms  7.101 ms
 5  broadband.actcorp.in (103.16.203.173)  7.491 ms  7.486 ms  7.483 ms
 6  * * *
 7  216.239.59.170 (216.239.59.170)  2.685 ms 108.170.253.97 (108.170.253.97)  3.493 ms 108.
170.236.196 (108.170.236.196)  3.740 ms
 8  108.170.253.120 (108.170.253.120)  4.476 ms 108.170.253.122 (108.170.253.122)  5.048 ms
216.239.42.235 (216.239.42.235)  4.752 ms
 9  74.125.242.129 (74.125.242.129)  5.877 ms 74.125.242.145 (74.125.242.145)  3.436 ms maa0
5s01-in-f5.1e100.net (172.217.163.37)  2.367 ms
mahesh@mahesh-PC:~$ 
```

6. ping

- **Description:**
  Ping is a computer network administration software utility used to test the reachability of a host on an Internet Protocol network.
- **Syntax:** ping [-options] ⟨*destination*⟩
- **Output:**

Figure 16: ping request www.yahoo.com



```
mahesh@mahesh-PC:~$ ping yahoo.com
PING yahoo.com (74.6.231.20) 56(84) bytes of data.
64 bytes from media-router-fp73.prod.media.vip.ne1.yahoo.com (74.6.231.20): icmp_seq=1 ttl=42 time=283 ms
64 bytes from media-router-fp73.prod.media.vip.ne1.yahoo.com (74.6.231.20): icmp_seq=2 ttl=42 time=728 ms
64 bytes from media-router-fp73.prod.media.vip.ne1.yahoo.com (74.6.231.20): icmp_seq=3 ttl=42 time=357 ms
64 bytes from media-router-fp73.prod.media.vip.ne1.yahoo.com (74.6.231.20): icmp_seq=4 ttl=42 time=406 ms
64 bytes from media-router-fp73.prod.media.vip.ne1.yahoo.com (74.6.231.20): icmp_seq=5 ttl=42 time=343 ms
^C
--- yahoo.com ping statistics ---
6 packets transmitted, 5 received, 16.6667% packet loss, time 5000ms
rtt min/avg/max/mdev = 282.660/423.268/727.524/157.155 ms
mahesh@mahesh-PC:~$ 
```