Computer Networks Lab 2

Name: Vaibhav Chaudhari

ID: 2017B5A70834G

Find network commands to do the following.

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

```
vaibhav@Jarvis:~$ netstat -stu
IcmpMsg:
    InType3: 40
    OutType3: 42
Tcp:
    499 active connection openings
    0 passive connection openings
    8 failed connection attempts
    138 connection resets received
    77 connections established
    8311 segments received
    8717 segments sent out
    0 segments retransmitted
    0 bad segments received
    174 resets sent
Udp:
    12915 packets received
    42 packets to unknown port received
    0 packet receive errors
    7899 packets sent
    0 receive buffer errors
    0 send buffer errors
    IgnoredMulti: 4
UdpLite:
TcpExt:
    105 TCP sockets finished time wait in fast timer
    233 delayed acks sent
    2857 packet headers predicted
    1214 acknowledgments not containing data payload received
    2618 predicted acknowledgments
    131 connections reset due to early user close
    TCPRcvCoalesce: 40
    TCPAutoCorking: 92
    TCPOrigDataSent: 3096
    TCPHystartTrainDetect: 2
    TCPHystartTrainCwnd: 36
    TCPWinProbe: 2
    TCPKeepAlive: 747
    TCPDelivered: 3585
IpExt:
    InMcastPkts: 66
    OutMcastPkts: 96
    InBcastPkts: 4
    OutBcastPkts: 4
    InOctets: 17980507
    OutOctets: 3468213
    InMcastOctets: 6384
    OutMcastOctets: 12036
    InBcastOctets: 310
    OutBcastOctets: 310
    InNoECTPkts: 24713
MPTcpExt:
```

netstat is used to display network related information like network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.
To view the Network statistics we can use the **-s** flag along with **-u** flag for all UDP ports and **-t** flag for all TCP ports.

2. Enlist the listening ports on your machine

```
vaibhav@Jarvis:~$ 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 0.0.0.0:ssh             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:telnet          0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
udp        0      0 0.0.0.0:32797           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      0 224.0.0.251: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:*
udp6       0      0 [::]:53261              [::]:*
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     38360    @/tmp/.ICE-unix/2212
unix  2      [ ACC ]     SEQPACKET  LISTENING     17703    /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     44299    /tmp/.com.google.Chrome.Hx92GW/SingletonSocket
unix  2      [ ACC ]     STREAM     LISTENING     27414    @/tmp/dbus-1tv8y5eT
unix  2      [ ACC ]     STREAM     LISTENING     17676    /run/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     17678    /run/systemd/userdb/io.systemd.DynamicUser
unix  2      [ ACC ]     STREAM     LISTENING     33539    /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     33544    /run/user/1000/bus
unix  2      [ ACC ]     STREAM     LISTENING     17689    /run/systemd/fsck.progress
unix  2      [ ACC ]     STREAM     LISTENING     33545    /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     33546    /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     33547    /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     17699    /run/systemd/journal/stdout
unix  2      [ ACC ]     STREAM     LISTENING     33548    /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     33549    /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     33550    /run/user/1000/pk-debconf-socket
unix  2      [ ACC ]     STREAM     LISTENING     33551    /run/user/1000/pulse/native
unix  2      [ ACC ]     STREAM     LISTENING     33552    /run/user/1000/snapd-session-agent.socket
unix  2      [ ACC ]     STREAM     LISTENING     34732    /run/user/1000/keyring/control
unix  2      [ ACC ]     STREAM     LISTENING     35179    @/tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     16779    /run/systemd/journal/io.systemd.journal
unix  2      [ ACC ]     STREAM     LISTENING     36143    /run/user/1000/keyring/pkcs11
unix  2      [ ACC ]     STREAM     LISTENING     36173    /run/user/1000/keyring/ssh
unix  2      [ ACC ]     STREAM     LISTENING     23783    /run/acpid.socket
unix  2      [ ACC ]     STREAM     LISTENING     35871    @/tmp/dbus-5cDrutvM
unix  2      [ ACC ]     STREAM     LISTENING     35180    /tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     35870    @/tmp/dbus-cVraGU8m
unix  2      [ ACC ]     STREAM     LISTENING     23785    /run/avahi-daemon/socket
unix  2      [ ACC ]     STREAM     LISTENING     23787    /run/cups/cups.sock
unix  2      [ ACC ]     STREAM     LISTENING     23789    /run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     23791    /run/snapd.socket
unix  2      [ ACC ]     STREAM     LISTENING     23793    /run/snapd-snap.socket
unix  2      [ ACC ]     STREAM     LISTENING     23795    /run/uuidd/request
unix  2      [ ACC ]     STREAM     LISTENING     38293    @/tmp/dbus-YSLNv47q1Y
unix  2      [ ACC ]     STREAM     LISTENING     25813    /run/irqbalance//irqbalance661.sock
unix  2      [ ACC ]     STREAM     LISTENING     37104    /tmp/ssh-oZDWNKZ9paI6/agent.2024
unix  2      [ ACC ]     STREAM     LISTENING     27413    @/tmp/dbus-243cToTQ
unix  2      [ ACC ]     STREAM     LISTENING     35469    @/home/vaibhav/.cache/ibus/dbus-8wPmrBFd
unix  2      [ ACC ]     STREAM     LISTENING     38361    /tmp/.ICE-unix/2212
```

We can use the **netstat** command with **-l** flag which is basically used to list all actively listening ports including both the UDP and the TCP port.

3. See the mail xchange (MX) record for www.gmail.com

```
vaibhav@Jarvis:~$ nslookup -type=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:
```

MX maps a domain name to a list of mail exchange servers for that domain. All the mail sent to gmail.com should be routed to mail server in that domain

```
vaibhav@Jarvis:~$ dig www.gmail.com MX

; <<>> DiG 9.16.1-Ubuntu <<>> www.gmail.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62747
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.gmail.com.          6923    IN      CNAME   mail.google.com.
mail.google.com.        6923    IN      CNAME   googlemail.l.google.com.

;; Query time: 128 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Feb 01 15:35:16 IST 2021
;; MSG SIZE  rcvd: 95

vaibhav@Jarvis:~$ dig www.gmail.com MX +short
mail.google.com.
googlemail.l.google.com.
```

dig command can be used with the **MX** option to get the mail xchange records for a site.

We can use any of the above two methods

4. Display the all network interfaces on your machine

```
vaibhav@Jarvis:~$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 08:00:27:fd:57:df brd ff:ff:ff:ff:ff:ff
```

ip link show displays the state of all network interfaces on the machi

```
vaibhav@Jarvis:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp0s3    1500    48221      0      0 0         33529      0      0      0 BMRU
lo       65536     2122      0      0 0          2122      0      0      0 LRU
```

netstat command with **-i** flag for the interfaces can be used to show all the network interfaces on our machine too

Any of these can be used

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

```
vaibhav@Jarvis:~$ sudo traceroute -I 8.8.8.8
[sudo] password for vaibhav:
traceroute to 8.8.8.8 (8.8.8.8), 64 hops max
  1   10.0.2.2  0.409ms  0.229ms  0.224ms
  2   192.168.43.1  4.796ms  3.732ms  6.482ms
  3   *  *  *
  4   10.72.96.130  52.260ms  56.907ms  91.133ms
  5   192.168.50.13  70.598ms  59.400ms  59.923ms
  6   172.26.100.150  63.653ms  60.728ms  56.145ms
  7   172.26.100.167  64.456ms  55.779ms  60.172ms
  8   192.168.41.76  60.277ms  58.599ms  64.235ms
  9   192.168.41.77  56.519ms  60.699ms  59.317ms
 10   172.26.14.75  64.947ms  59.358ms  52.930ms
 11   172.16.28.6  66.038ms  60.226ms  59.104ms
 12   172.16.0.59  61.665ms  51.739ms  67.792ms
 13   108.170.232.227  62.007ms  56.871ms  59.602ms
 14   72.14.235.109  61.799ms  59.057ms  60.048ms
 15   8.8.8.8  60.134ms  58.964ms  84.880ms
```

traceroute command is used to get a list of all the intermediate routers used to reach 8.8.8.8 along with sudo and **-I** flag which is used to use ICMP ECHO as probe. The latency is given by the round trip time.

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

```
vaibhav@Jarvis:~$ ping 8.8.8.8 -c 10
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=111 time=101 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=79.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=111 time=64.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=111 time=57.1 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=111 time=47.6 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=111 time=212 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=111 time=71.7 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=111 time=67.8 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=111 time=135 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=111 time=57.0 ms

--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 47.637/89.264/211.561/47.412 ms
```

We use the ping command to send echo requests and the number of echo requests can be controlled with **-c** flag which represents the count of the echo requests we want to send.

7. **Get the IP address of www.bits-pilani.ac.in domain.**

```
vaibhav@Jarvis:~$ 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
```

We can get the IP Address using the **nslookup** command along with the name of the site.