Computer Networks Lab 2

CS F303

Susmit Wani 2018A7PS0116G

Lab 2 Use of Network Commands

Vinayak Naik • Jan 30

Labs • 14 points **Due 7:00 PM**

Find network commands to do the following.

1. See the statistics of TCP and UDP ports on Linux machine
2. Enlist the listening ports on your machine
3. See the mail xchange (MX) record for www.gmail.com
4. Display the all network interfaces on your machine
5. A list of intermediate routers to reach 8.8.8.8 from your machine, with latency
6. Send 10 echo requests to 8.8.8.8 server from your machine
7. Get the IP address of www.bits-pilani.ac.in domain.

For each command, put up a screenshot of the output with the explanation in a PDF file. Submit the file.

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

```
lenovo@susmits-lenovo:~$ netstat -t -u
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 susmits-lenovo:41204    bom05s10-in-f142.:https ESTABLISHED
tcp        0      0 susmits-lenovo:41202    bom05s10-in-f142.:https TIME_WAIT
tcp        0      0 susmits-lenovo:54456    whatsapp-cdn-shv-:https ESTABLISHED
tcp        0      0 susmits-lenovo:52462    a104-71-100-96.de:https ESTABLISHED
tcp        0      0 susmits-lenovo:34986    104.18.9.154:https      ESTABLISHED
tcp        0      0 susmits-lenovo:46270    172.217.194.188:5228    ESTABLISHED
udp        0      0 susmits-lenovo:38080    sc-in-f189.1e100.ne:443 ESTABLISHED
udp        0      0 susmits-lenovo:47565    bom05s10-in-f142.1e:443 ESTABLISHED
udp        0      0 susmits-lenovo:55810    bom12s03-in-f14.1e1:443 ESTABLISHED
```

Used the netstat command with -t and -u flags.

These flags list the ports which have their protocols as tcp and udp

2. Enlist the listening ports on your machine

```
lenovo@susmits-lenovo:~$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:mysql         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:ipp             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 0.0.0.0:34939           0.0.0.0:*
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 0.0.0.0:bootpc          0.0.0.0:*
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 [::]:52028              [::]:*
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     SEQPACKET  LISTENING     13754    /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     38968    /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     26421    /run/user/120/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     32146    @/tmp/.ICE-unix/1992
unix  2      [ ACC ]     STREAM     LISTENING     38972    /run/user/1000/snapd-session-agent.socket
unix  2      [ ACC ]     STREAM     LISTENING     26425    /run/user/120/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     38973    /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     26426    /run/user/120/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     38974    /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     26427    /run/user/120/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     38975    /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     26428    /run/user/120/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     38976    /run/user/1000/bus
unix  2      [ ACC ]     STREAM     LISTENING     26429    /run/user/120/snapd-session-agent.socket
unix  2      [ ACC ]     STREAM     LISTENING     38977    /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     38978    /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     26430    /run/user/120/pulse/native
unix  2      [ ACC ]     STREAM     LISTENING     26431    /run/user/120/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     35292    /run/user/1000/keyring/control
unix  2      [ ACC ]     STREAM     LISTENING     26432    /run/user/120/bus
unix  2      [ ACC ]     STREAM     LISTENING     33724    /run/user/1000/keyring/pkcs11
unix  2      [ ACC ]     STREAM     LISTENING     31813    /run/user/120/wayland-0
unix  2      [ ACC ]     STREAM     LISTENING     33727    /run/user/1000/keyring/ssh
unix  2      [ ACC ]     STREAM     LISTENING     46578    /tmp/.com.google.Chrome.Fr9MJd/SingletonSocket
unix  2      [ ACC ]     STREAM     LISTENING     25547    @/tmp/dbus-pTmUCLK2
unix  2      [ ACC ]     STREAM     LISTENING     26026    @irqbalance859.sock
unix  2      [ ACC ]     STREAM     LISTENING     21491    @/tmp/.ICE-unix/1107
```

Used the ‘netstat -l’ command.

The -l flag lists the listening ports on the machine

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

```
lenovo@susmits-lenovo:~$ dig www.gmail.com MX

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> www.gmail.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17529
;; 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.          24703   IN      CNAME   mail.google.com.
mail.google.com.        7199    IN      CNAME   googlemail.l.google.com.

;; Query time: 92 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Feb 01 09:38:25 IST 2021
;; MSG SIZE  rcvd: 95
```

```
lenovo@susmits-lenovo:~$ nslookup
> set 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:
> 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 = 20 alt2.gmail-smtp-in.l.google.com.
gmail.com       mail exchanger = 30 alt3.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.

Authoritative answers can be found from:
>
```

To find the mail xchange record, we use the dig command followed by the domain name and the MX option.
We can also do it using the nslookup command and setting the type to mx

4. Display the all network interfaces on your machine

```
lenovo@susmits-lenovo:~$ ifconfig -a
enp2s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 8c:16:45:32:5b:bc  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 1336  bytes 131190 (131.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1336  bytes 131190 (131.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.6  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::d911:c386:bbac:a085  prefixlen 64  scopeid 0x20<link>
        ether 70:c9:4e:d2:91:d7  txqueuelen 1000  (Ethernet)
        RX packets 220755  bytes 271133427 (271.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 61229  bytes 16154545 (16.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

To list all the network interfaces on the system, we use the ifconfig command with the -a flag.

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

```
lenovo@susmits-lenovo:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  6.830 ms  4.749 ms  5.299 ms
 2  10.110.0.1 (10.110.0.1)  25.340 ms  25.338 ms  25.308 ms
 3  * * *
 4  202.88.186.66 (202.88.186.66)  27.930 ms  36.227 ms  36.224 ms
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  dns.google (8.8.8.8) 18.831 ms  19.360 ms  18.271 ms
```

Simply used the traceroute [ip] to find the list of intermediate routers along with the delays.

When a smaller packet is sent(28 byte), it seems to return a more comprehensive list of intermediate routers.

```
lenovo@susmits-lenovo:~$ traceroute 8.8.8.8 1
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 28 byte packets
 1  _gateway (192.168.0.1)  6.389 ms  7.047 ms  7.000 ms
 2  10.110.0.1 (10.110.0.1)  16.411 ms  20.119 ms  22.670 ms
 3  202.88.186.25 (202.88.186.25)  24.763 ms  29.715 ms  26.785 ms
 4  202.88.186.66 (202.88.186.66)  31.795 ms  34.640 ms  36.619 ms
 5  202.88.186.61 (202.88.186.61)  39.394 ms  41.461 ms  46.113 ms
 6  125.99.43.254 (125.99.43.254)  44.042 ms  44.208 ms  43.932 ms
 7  125.99.43.253 (125.99.43.253)  49.283 ms  36.108 ms  38.262 ms
 8  136.232.32.29.static.jio.com (136.232.32.29)  38.185 ms  37.036 ms  38.898 ms
 9  74.125.32.0 (74.125.32.0)  37.957 ms 74.125.51.62 (74.125.51.62)  40.973 ms 72.14.243.188 (72.14.243.188)  35.693 ms
10  * * *
11  dns.google (8.8.8.8) 41.114 ms  35.556 ms  38.611 ms
```

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

```
lenovo@susmits-lenovo:~$ 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=116 time=21.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=15.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=20.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=27.1 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=116 time=19.3 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=116 time=24.3 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=116 time=13.9 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=116 time=25.7 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=116 time=16.2 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=116 time=23.8 ms

--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9016ms
rtt min/avg/max/mdev = 13.963/20.810/27.192/4.358 ms
```

To send echo requests, we use the ping command

To send 10 requests, we use the -c or the count flag and give argument as 10 for the flag.

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

```
lenovo@susmits-lenovo:~$ 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: 14.139.243.20
Name:   universe.bits-pilani.ac.in
Address: 103.144.92.33
```

The IP website www.bits-pilani.ac.in is hosted on both IPs as seen in the screenshots
14.139.243.20
103.144.92.33

```
lenovo@susmits-lenovo:~$ dig www.bits-pilani.ac.in

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> www.bits-pilani.ac.in
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18398
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.bits-pilani.ac.in.         IN      A

;; ANSWER SECTION:
www.bits-pilani.ac.in.  6946    IN      CNAME   universe.bits-pilani.ac.in.
universe.bits-pilani.ac.in. 6946 IN     A       14.139.243.20
universe.bits-pilani.ac.in. 6946 IN     A       103.144.92.33

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Feb 01 09:59:05 IST 2021
;; MSG SIZE  rcvd: 105
```

We can also use ‘dig www.bits-pilani.ac.in’ to find IPs. Returns the same IP addresses. Could find it using the ‘ping www.bits-pilani.ac.in’ and ‘traceroute www.bits-pilani.ac.in’ commands as well

Typed the IPs in the web browser and could open the BITS website