CN Homework -2

Setu Gupta (2018190)

1.

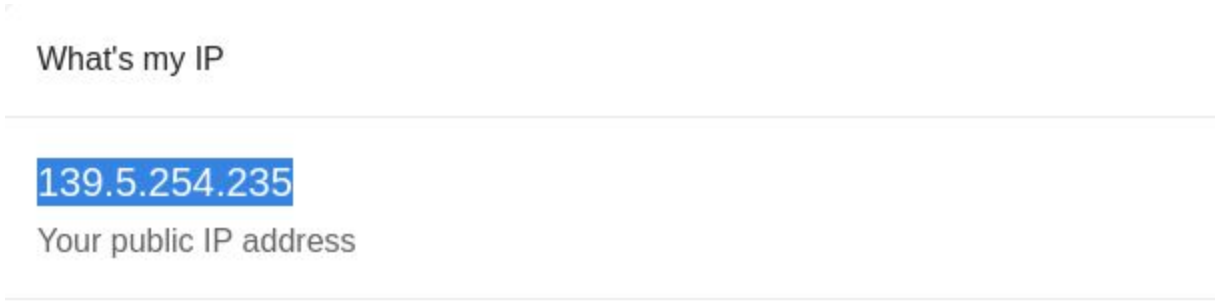
a. 192.168.0.180 (Private IP). I confirm it from my router's configuration page.

```
ifconfig
enp8s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether ec:b1:d7:de:c5:17  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 12  bytes 856 (856.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 856 (856.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp9s0f0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.180  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::4ad7:769c:e432:f62a  prefixlen 64  scopeid 0x20<link>
        ether 74:29:af:5d:8d:4d  txqueuelen 1000  (Ethernet)
        RX packets 12121  bytes 12042323 (11.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8991  bytes 1514630 (1.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

b. 139.5.254.235 (Public IP at the time of measurement. My ISP shuffles through a list of public IPs. Both IPs are different as ifconfig gives private IP whereas whatsmyIP gives public IP.



2.

a. Avg = 3.688ms to 8.8.8.8 (Google's DNS)

```
ping -c 10 8.8.8.8
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=118 time=4.01 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=3.44 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=5.28 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=3.57 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=118 time=4.12 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=118 time=3.39 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=118 time=2.72 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=118 time=3.87 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=118 time=3.52 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=118 time=2.96 ms

--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 2.721/3.688/5.279/0.671 ms
```

b. I found out the IP address using nmap.

```
~/De/CN/hw2/helper_scripts  master ?1  nmap 192.168.0.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-20 19:58 IST
Nmap scan report for dlinkrouter (192.168.0.1)
Host is up (0.0043s latency).
Not shown: 993 closed ports
PORT     STATE    SERVICE
1/tcp    filtered tcpmux
53/tcp   open     domain
80/tcp   open     http
443/tcp  open     https
2601/tcp open     zebra
2602/tcp open     ripd
8888/tcp open     sun-answerbook

Nmap scan report for 192.168.0.11
Host is up (0.0044s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
1900/tcp  open  upnp
49152/tcp open  unknown
```

I have used a custom script to calculate the statistics. This script can be found under helper_scripts
IP -> 192.168.0.11
Median: 1.47ms
90th percentile: 3.72ms
99th percentile: 87.4ms

```
~/Desktop/CN/hw2/helper_scripts  master ?1  ping -c 100 192.168.0.11 | python3 percentile.py
Got 100 samples
50th percentile: 1.47
90th percentile: 3.72
99th percentile: 87.4
Average: 2.7480600000000006
0% packet loss
```

c. Median: 4.16ms
90th percentile: 6.09ms
99th percentile: 12.1ms

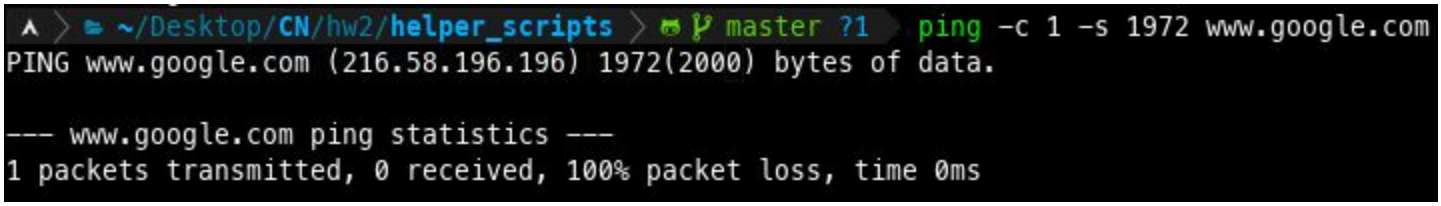
```
~/De/CN/hw2/helper_scripts  master ?1  ping -c 100 www.amazon.com | python3 percentile.py
Got 100 samples
50th percentile: 4.16
90th percentile: 6.09
99th percentile: 12.1
Average: 4.539199999999999
0% packet loss
```

d. Packet loss for 192.168.0.11 -> 0%
Average latency for 192.168.0.11 -> 2.74806ms
Packet loss for www.amazon.com -> 0%

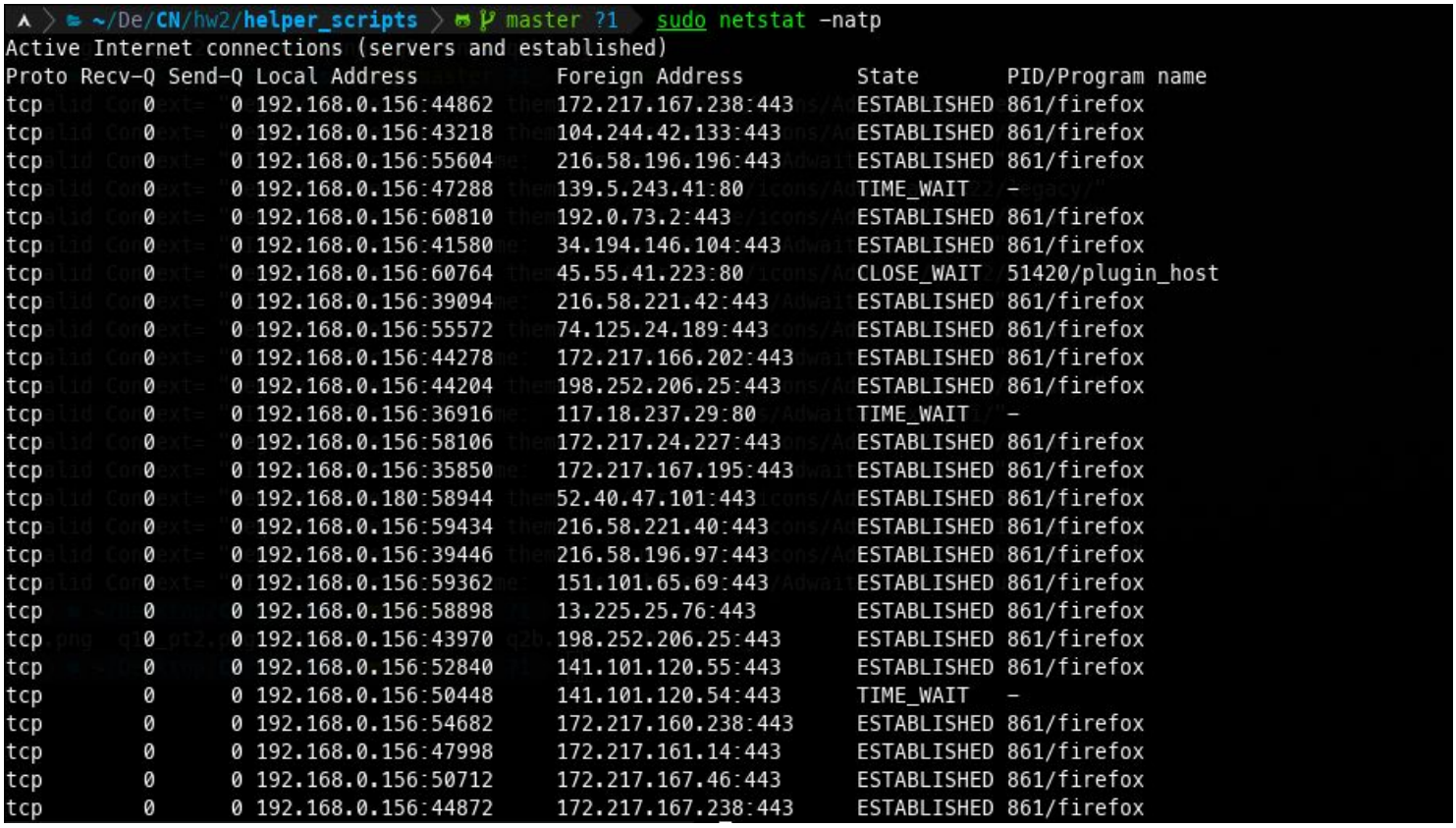
Average latency for www.amazon.com -> 4.5392ms
Both have the same (0%) packet loss.
www.amazon.com has higher average latency. This is because we have to travel a longer distance to reach amazon's server that 192.168.0.11

3.

a. Source: https://access.redhat.com/solutions/2440411
Command: `ping -c 1 -s 1972 www.google.com`
Explanation: ping with 1 packet (-c 1) of size 1972 bytes (-s 1972) to www.google.com. We send 1972 bytes as there is an overhead of 28 bytes (8 bytes for ICMP and 20 bytes for ethernet) making the total 2000 bytes.
Failure is indicated by packet loss.
The reason the test failed is because the connection from my laptop to www.google.com didn't support MTU of 2000. The reason might be that some of the routers may not be able to support higher bandwidths required for larger MTUs.



b. Command: `netstat -atp`
Explanation: -p to show process info (pid, etc.), -t to only show TCP sockets and -a to show all (listening and non listening).



```
~/De/CN/hw2/helper_scripts  master ?1  sudo netstat -natp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 192.168.0.156:44862     172.217.167.238:443     ESTABLISHED 861/firefox
tcp        0      0 192.168.0.156:43218     104.244.42.133:443      ESTABLISHED 861/firefox
tcp        0      0 192.168.0.156:55604     216.58.196.196:443      ESTABLISHED 861/firefox
tcp        0      0 192.168.0.156:47288     139.5.243.41:80         TIME_WAIT   -
tcp        0      0 192.168.0.156:60810     192.0.73.2:443          ESTABLISHED 861/firefox
tcp        0      0 192.168.0.156:41580     34.194.146.104:443      ESTABLISHED 861/firefox
tcp        0      0 192.168.0.156:60764     45.55.41.223:80         CLOSE_WAIT  51420/plugin_host
tcp        0      0 192.168.0.156:39094     216.58.221.42:443       ESTABLISHED 861/firefox
tcp        0      0 192.168.0.156:55572     74.125.24.189:443       ESTABLISHED 861/firefox
tcp        0      0 192.168.0.156:44278     172.217.166.202:443     ESTABLISHED 861/firefox
tcp        0      0 192.168.0.156:44204     198.252.206.25:443      ESTABLISHED 861/firefox
tcp        0      0 192.168.0.156:36916     117.18.237.29:80        TIME_WAIT   -
tcp        0      0 192.168.0.156:58106     172.217.24.227:443      ESTABLISHED 861/firefox
tcp        0      0 192.168.0.156:35850     172.217.167.195:443     ESTABLISHED 861/firefox
tcp        0      0 192.168.0.180:58944     52.40.47.101:443        ESTABLISHED 861/firefox
tcp        0      0 192.168.0.156:59434     216.58.221.40:443       ESTABLISHED 861/firefox
tcp        0      0 192.168.0.156:39446     216.58.196.97:443       ESTABLISHED 861/firefox
tcp        0      0 192.168.0.156:59362     151.101.65.69:443       ESTABLISHED 861/firefox
tcp        0      0 192.168.0.156:58898     13.225.25.76:443        ESTABLISHED 861/firefox
tcp        0      0 192.168.0.156:43970     198.252.206.25:443      ESTABLISHED 861/firefox
tcp        0      0 192.168.0.156:52840     141.101.120.55:443      ESTABLISHED 861/firefox
tcp        0      0 192.168.0.156:50448     141.101.120.54:443      TIME_WAIT   -
tcp        0      0 192.168.0.156:54682     172.217.160.238:443     ESTABLISHED 861/firefox
tcp        0      0 192.168.0.156:47998     172.217.161.14:443      ESTABLISHED 861/firefox
tcp        0      0 192.168.0.156:50712     172.217.167.46:443      ESTABLISHED 861/firefox
tcp        0      0 192.168.0.156:44872     172.217.167.238:443     ESTABLISHED 861/firefox
```

4.

a. I used ns type query to find the authoritative name servers. Then I used one of these nameservers for the DNS query. However, for some reason, I still got a non-authoritative answer. This is probably because the authoritative server itself fulfilled the query from its own cache.
Source: https://serverfault.com/questions/647974/how-to-get-authoritative-answers-from-nslookup

```
~/Desktop/CN/hw2/helper_scripts  master ?1  nslookup -type=ns google.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns1.google.com.

Authoritative answers can be found from:
ns4.google.com  internet address = 216.239.38.10
ns3.google.com  internet address = 216.239.36.10
ns2.google.com  internet address = 216.239.34.10
ns1.google.com  internet address = 216.239.32.10
ns4.google.com  has AAAA address 2001:4860:4802:38::a
ns3.google.com  has AAAA address 2001:4860:4802:36::a
ns2.google.com  has AAAA address 2001:4860:4802:34::a
ns1.google.com  has AAAA address 2001:4860:4802:32::a

~/Desktop/CN/hw2/helper_scripts  master ?1  nslookup google.com ns4.google.com
Server:         ns4.google.com
Address:        216.239.38.10#53

Non-authoritative answer:
Name:   google.com
Address: 172.217.166.14
```

b. Source: https://en.wikipedia.org/wiki/SOA_record
TTL = 60s = 1 minute
SOA query has a field for TTL (a.k.a minimum)

```
~/Desktop/CN/hw2/helper_scripts  master ?1  nslookup -type=soa google.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
google.com
        origin = ns1.google.com
        mail addr = dns-admin.google.com
        serial = 332629538
        refresh = 900
        retry = 900
        expire = 1800
        minimum = 60

Authoritative answers can be found from:
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns1.google.com.
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns4.google.com.
ns4.google.com  internet address = 216.239.38.10
ns3.google.com  internet address = 216.239.36.10
ns2.google.com  internet address = 216.239.34.10
ns1.google.com  internet address = 216.239.32.10
ns4.google.com  has AAAA address 2001:4860:4802:38::a
ns3.google.com  has AAAA address 2001:4860:4802:36::a
ns2.google.com  has AAAA address 2001:4860:4802:34::a
ns1.google.com  has AAAA address 2001:4860:4802:32::a
```

5. `traceroute google.com -q 5 -z 12345 -f 5 -m 7`
    a. -z is used to set minimum probe interval
    b. -q is used to specify number of probing packets
    c. -f is used to specify minimum TTL i.e. minimum hop and -m is used to specify maximum TTL i.e. maximum hop.

```
~/Desktop/CN/hw2/helper_scripts  master ?1  traceroute google.com -q 5 -z 12345 -f 5 -m 7                    INT ✘  10:27:20 PM
traceroute to google.com (172.217.167.238), 7 hops max, 60 byte packets
 5  209.85.172.217 (209.85.172.217)  6.702 ms  7.337 ms  11.456 ms  5.574 ms  5.182 ms
 6  74.125.244.193 (74.125.244.193)  3.316 ms 74.125.243.97 (74.125.243.97)  3.572 ms  3.370 ms  5.219 ms  6.175 ms
 7  172.253.67.91 (172.253.67.91)  24.451 ms 172.253.67.89 (172.253.67.89)  9.301 ms  41.618 ms 172.253.67.91 (172.253.67.91)  3.864 ms 172.253.67.89 (172.253.67.89)  3
.339 ms
```

6. I took the lo interface down using ifconfig. As a result all the packets sent to 127.0.0.1 were lost.

```
~/Desktop/CN/hw2/helper_scripts  master ?1  ping -c 3 127.0.0.1                                    10:32:00 PM
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.026 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.033 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.057 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2017ms
rtt min/avg/max/mdev = 0.026/0.038/0.057/0.013 ms
~/Desktop/CN/hw2/helper_scripts  master ?1  sudo ifconfig lo down                                   10:32:12 PM
~/Desktop/CN/hw2/helper_scripts  master ?1  ping -c 3 127.0.0.1                                     10:32:17 PM
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2036ms
~/De/CN/hw2/helper_scripts  master ?1                                                  1 ✘  12s  10:32:32 PM
```

7. I used the -x option in dig to perform reverse DNS search. Other options used are +noall which removes all the output and +answer which adds back only the answer portion.
   Source: https://linuxcommando.blogspot.com/2008/07/how-to-do-reverse-dns-lookup.html

```
~/Desktop/CN/hw2/helper_scripts  master ?1  dig +noall +answer google.com
google.com.             106     IN      A       172.217.167.238
~/Desktop/CN/hw2/helper_scripts  master ?1  dig +noall +answer -x 172.217.167.238
238.167.217.172.in-addr.arpa. 7079 IN   PTR     del11s04-in-f14.1e100.net.
```
