Using Command Line Utilities for Network Debugging

Name: Aditya Jagadale **Roll Number: 2022032**

Q1.)

a)

```
jaags@LAPTOP-GR95AUF8:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.19.17.127  netmask 255.255.240.0  broadcast 172.19.31.255
        inet6 fe80::215:5dff:fe1c:4529  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:1c:45:29  txqueuelen 1000  (Ethernet)
        RX packets 14  bytes 10612 (10.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26  bytes 2680 (2.6 KB)
        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 1355 (1.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 1355 (1.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

IP Address: 172.19.17.127

b) IP Address: 103.25.231.125

The IP Address' are different from each other

Reason: IP Address is different in both the cases because ifconfig displays the ip address assigned to your device but whatsmyip gives you your public ip address. This address is assigned by the ISP.

Q2.)

a)

```
jaags@LAPTOP-GR95AUF8:~$ sudo ifconfig eth0 172.19.17.10 netmask 255.255.240.0
jaags@LAPTOP-GR95AUF8:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.19.17.10  netmask 255.255.240.0  broadcast 172.19.31.255
        inet6 fe80::215:5dff:fe1c:4529  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:1c:45:29  txqueuelen 1000  (Ethernet)
        RX packets 1487  bytes 4251897 (4.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 773  bytes 102973 (102.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
jaags@LAPTOP-GR95AUF8:~$ sudo ifconfig eth0 172.19.17.127 netmask 255.255.240.0
jaags@LAPTOP-GR95AUF8:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.19.17.127  netmask 255.255.240.0  broadcast 172.19.31.255
        inet6 fe80::215:5dff:fe1c:4529  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:1c:45:29  txqueuelen 1000  (Ethernet)
        RX packets 1487  bytes 4251897 (4.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 773  bytes 102973 (102.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Q3.)

a)

```
jaags@LAPTOP-GR95AUF8:~$ nc -l -p 8000
hi
connection established
bye
```

```
jaags@LAPTOP-GR95AUF8:~$ nc localhost 8000
hi
connection established
bye
```

b)

```
jaags@LAPTOP-GR95AUF8:~$ netstat -tn
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:8000          127.0.0.1:34718         ESTABLISHED
tcp        0      0 127.0.0.1:34718         127.0.0.1:8000          ESTABLISHED
jaags@LAPTOP-GR95AUF8:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:8000          localhost:34718         ESTABLISHED
tcp        0      0 localhost:34718         localhost:8000          ESTABLISHED
```

Q4.)

a)

```
jaags@LAPTOP-GR95AUF8:~$ nslookup -type=NS google.in
Server:         10.255.255.254
Address:        10.255.255.254#53

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

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

To get an authtoritative response from nslookup we add -type=NS. It is a query for Name Server records.

b)

```
jaags@LAPTOP-GR95AUF8:~$ dig x.com

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> x.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37869
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;x.com.                         IN      A

;; ANSWER SECTION:
x.com.                  498     IN      A       104.244.42.193
x.com.                  498     IN      A       104.244.42.129
x.com.                  498     IN      A       104.244.42.1
x.com.                  498     IN      A       104.244.42.65

;; Query time: 20 msec
;; SERVER: 10.255.255.254#53(10.255.255.254) (UDP)
;; WHEN: Fri Aug 30 02:22:20 IST 2024
;; MSG SIZE  rcvd: 98
```

TTL: 498 seconds
The DNS record for x.com will expire from local DNS server's cache after 498 seconds.

Q5.)
a)

```
jaags@LAPTOP-GR95AUF8:~$ traceroute google.in
traceroute to google.in (142.250.193.4), 30 hops max, 60 byte packets
 1  LAPTOP-GR95AUF8.mshome.net (172.19.16.1)  0.957 ms  1.151 ms  0.914 ms
 2  192.168.32.254 (192.168.32.254)  21.899 ms  21.263 ms  21.253 ms
 3  vpn.iiitd.edu.in (192.168.1.99)  11.786 ms  11.717 ms  11.708 ms
 4  103.25.231.1 (103.25.231.1)  9.192 ms  9.184 ms  9.177 ms
 5  * * *
 6  10.119.234.162 (10.119.234.162)  9.211 ms  9.554 ms  9.517 ms
 7  72.14.195.56 (72.14.195.56)  9.544 ms  11.934 ms 72.14.194.160 (72.14.194.160)  9.396 ms
 8  192.178.80.159 (192.178.80.159)  31.565 ms 142.251.54.111 (142.251.54.111)  27.963 ms  29.456 ms
 9  142.251.54.89 (142.251.54.89)  32.802 ms  30.286 ms 142.251.54.87 (142.251.54.87)  32.881 ms
10  del11s14-in-f4.1e100.net (142.250.193.4)  56.186 ms  56.176 ms  56.168 ms
```

There are 10 intermediate hosts.

Hop 1: 172.19.16.1
Hop 2: 192.168.32.254
Hop 3: 192.168.1.99
Hop 4: 103.25.231.1
Hop 6: 10.119.234.162
Hop 7: 72.14.195.56
Hop 8: 192.178.80.159
Hop 9: 142.251.54.89
Hop 10: 142.250.193.4

Avg latency

Host 1: 1.007
Host 2: 21.471
Host 3: 11.737
Host 4: 9.184
Host 6: 9.427
Host 7: 10.291
Host 8: 29.661
Host 9: 31.989
Host 10: 56.176

b)

```
--- google.in ping statistics ---
50 packets transmitted, 50 received, 0% packet loss, time 49083ms
rtt min/avg/max/mdev = 49.853/57.937/86.125/7.117 ms
jaags@LAPTOP-GR95AUF8:~$
```

Avg latency: 57.937

c) Total latency of intermediate hosts = 180.943 ms
Avg ping latency = 57.937

The latencies are not same as traceroute measures the latency to each intermediate hosts along a path. Ping measures the round trip time directly to the destination.

d) max latency = 56.176
Avg latency = 57.937

The latencies are different as traceroute may include paths with congested or slow routers and reflect the delay whereas Ping measures the round trip total which may not reflect the congestion. Both the values serve different purpose and are not expected to match

e) Multiple entries for single hop occur as traceroute sends 3 packets to each hop in the route. Each of these packets measure the RTT to that hop. Sending multiple packets helps to provide more accuracy and identify issues such as network congestion, packet loss.

f)

```
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=45 ttl=241 time=304 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=46 ttl=241 time=301 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=47 ttl=241 time=288 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=48 ttl=241 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=49 ttl=241 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=50 ttl=241 time=319 ms

--- stanford.edu ping statistics ---
50 packets transmitted, 50 received, 0% packet loss, time 49066ms
rtt min/avg/max/mdev = 287.661/342.788/437.441/46.765 ms
```

Avg latency = 342.788 ms

g)

```
jaags@LAPTOP-GR95AUF8:~$ traceroute stanford.edu
traceroute to stanford.edu (171.67.215.200), 30 hops max, 60 byte packets
 1  LAPTOP-GR95AUF8.mshome.net (172.19.16.1)  0.607 ms  0.586 ms  0.575 ms
 2  192.168.32.254 (192.168.32.254)  32.178 ms  32.169 ms  32.163 ms
 3  auth.iiitd.edu.in (192.168.1.99)  10.291 ms  10.286 ms  10.278 ms
 4  103.25.231.1 (103.25.231.1)  11.047 ms  11.042 ms  11.036 ms
 5  10.1.209.201 (10.1.209.201)  57.471 ms  56.619 ms  56.613 ms
 6  10.1.200.137 (10.1.200.137)  32.263 ms  33.678 ms  33.667 ms
 7  10.255.238.122 (10.255.238.122)  57.885 ms 10.255.238.254 (10.255.238.254)  31.253 ms  31.239 ms
 8  180.149.48.18 (180.149.48.18)  55.214 ms  88.606 ms  54.378 ms
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  campus-ial-nets-b-vl1120.SUNet (171.66.255.232)  414.434 ms campus-east-rtr-vl1020.SUNet (171.64.255.232)  414.510 m
s *
25  campus-ial-nets-a-vl1020.SUNet (171.64.255.232)  420.652 ms * campus-ial-nets-a-vl1004.SUNet (171.64.255.200)  290.4
81 ms
26  * * web.stanford.edu (171.67.215.200)  309.834 ms
```

The hops in this are 26 and 10 in google.in

h) There is a significant latency difference in google.in and stanford.edu as their servers are placed in different locations. google.in has a server in india and stanford.edu has in california USA. The greater the distance the longer it takes for data packets to travel between device and server.

Q6.)

```
jaags@LAPTOP-GR95AUF8:/$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
^C
--- 127.0.0.1 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9377ms
```

For ping to fail for 127.0.0.1 we have to first turn our lo down using sudo ifconfig lo down and then run the ping command which will keep running until we terminate it.
After termination it will show 100% packet loss. This disables the loopback network interface which is used by the system to communicate with itself.