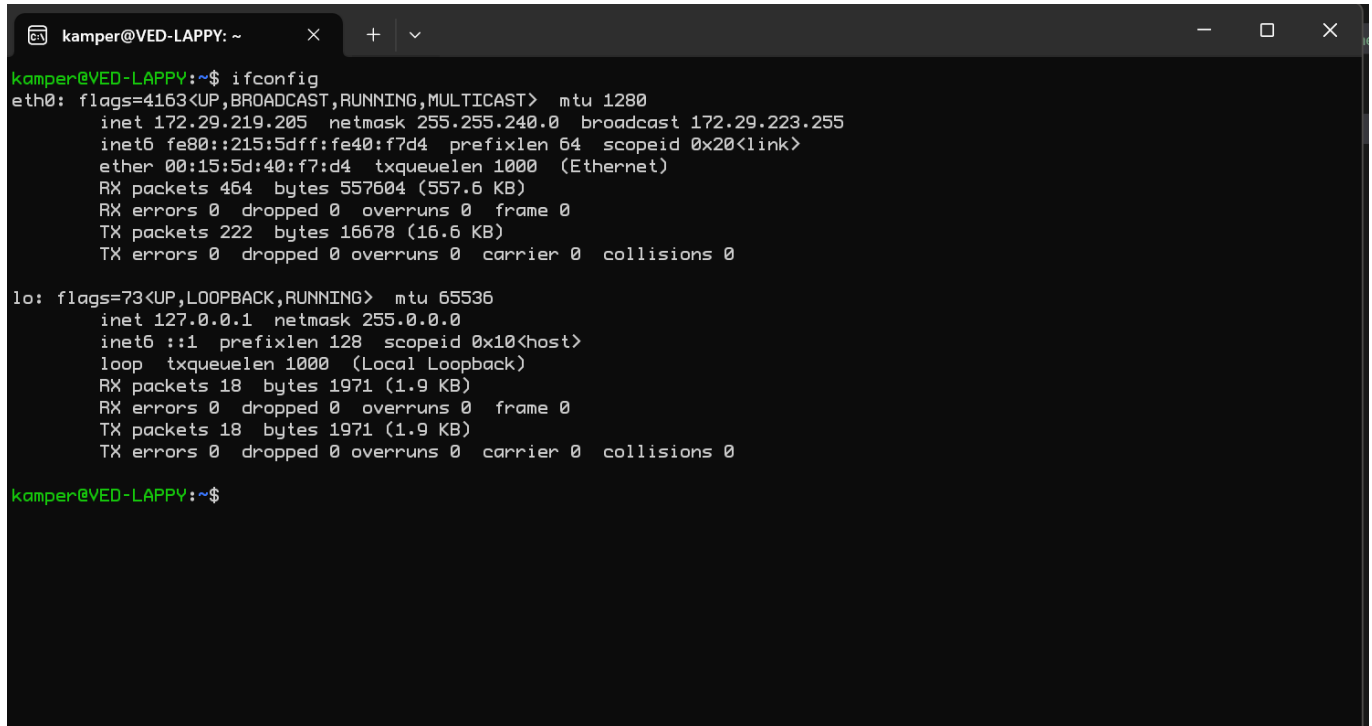


# Using command-line utilities for network debugging

## Question 1

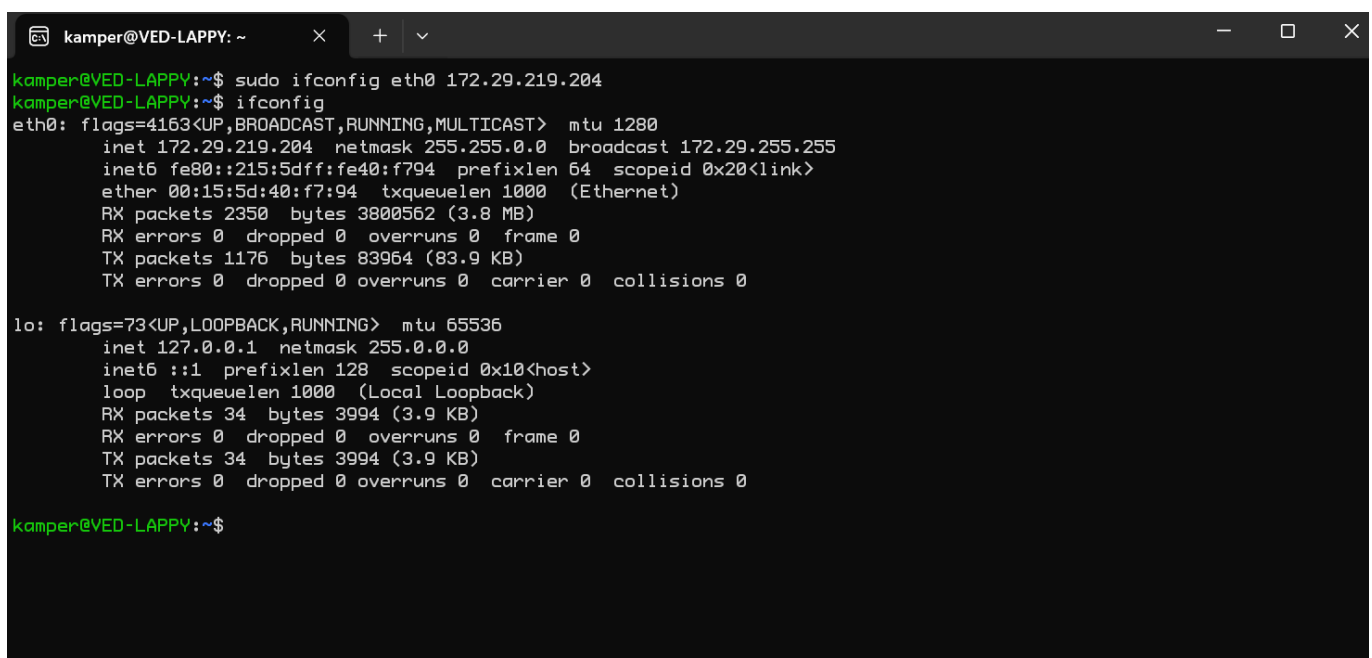
a.



```
kamper@VED-LAPPY: ~  
kamper@VED-LAPPY:~$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1280  
    inet 172.29.219.205 netmask 255.255.240.0 broadcast 172.29.223.255  
    inet6 fe80::215:5dff:fe40:f7d4 prefixlen 64 scopeid 0x20<link>  
    ether 00:15:5d:40:f7:d4 txqueuelen 1000 (Ethernet)  
    RX packets 464 bytes 557604 (557.6 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 222 bytes 16678 (16.6 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 18 bytes 1971 (1.9 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 18 bytes 1971 (1.9 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
kamper@VED-LAPPY:~$
```

b. The IP address on the website <https://whatismyip.com> is different. This is because the IP address shown in ifconfig is the private IP address provided by LAN and the IP address on the website is the public IP address that is used to identify the device on the internet.

## Question 2



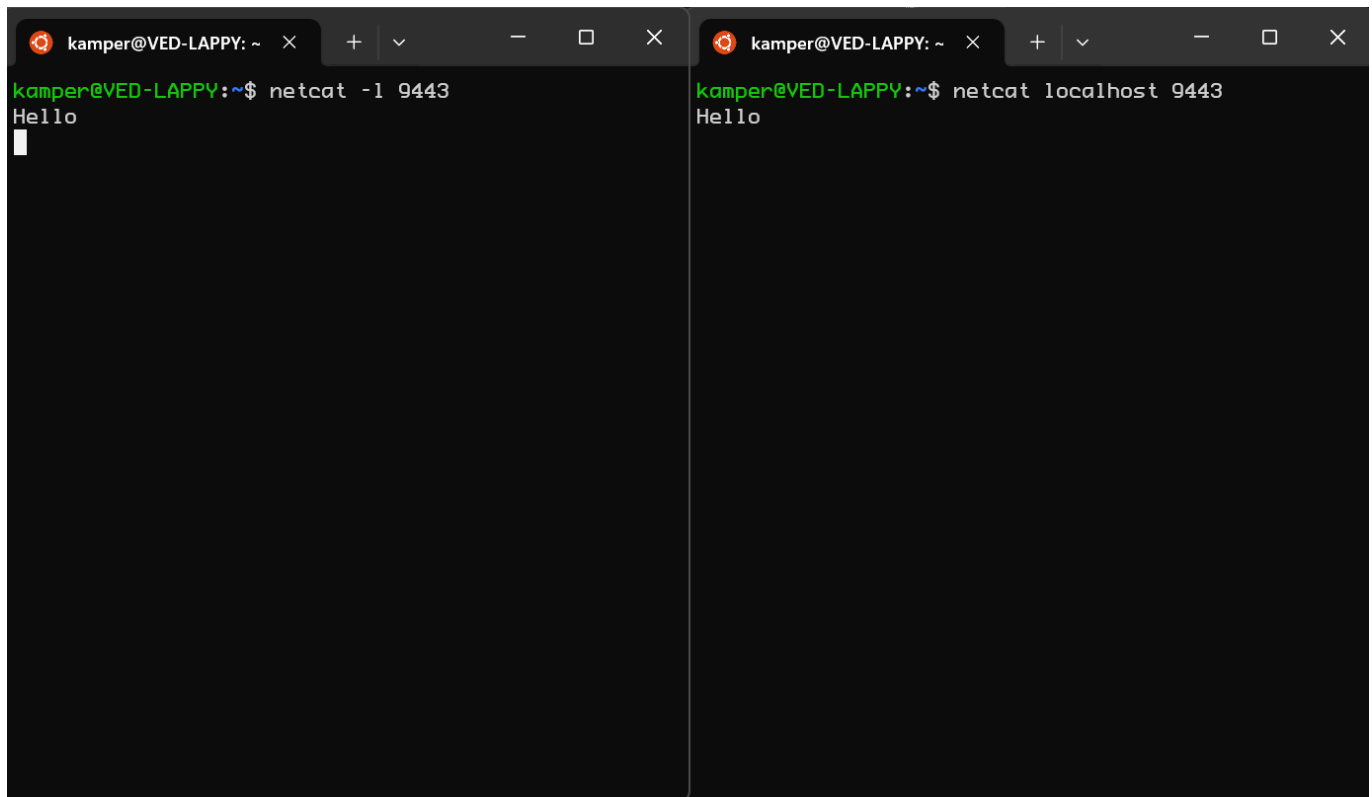
```
kamper@VED-LAPPY: ~  
kamper@VED-LAPPY:~$ sudo ifconfig eth0 172.29.219.204  
kamper@VED-LAPPY:~$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1280  
    inet 172.29.219.204 netmask 255.255.0.0 broadcast 172.29.255.255  
    inet6 fe80::215:5dff:fe40:f794 prefixlen 64 scopeid 0x20<link>  
    ether 00:15:5d:40:f7:94 txqueuelen 1000 (Ethernet)  
    RX packets 2350 bytes 3800562 (3.8 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 1176 bytes 83964 (83.9 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 34 bytes 3994 (3.9 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 34 bytes 3994 (3.9 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
kamper@VED-LAPPY:~$
```

you can revert back to the IP address by using the same command and use the original IP address.

Alternatively, if you don't know the original IP address, you can reboot the system to revert to the original IP address.

## Question 3

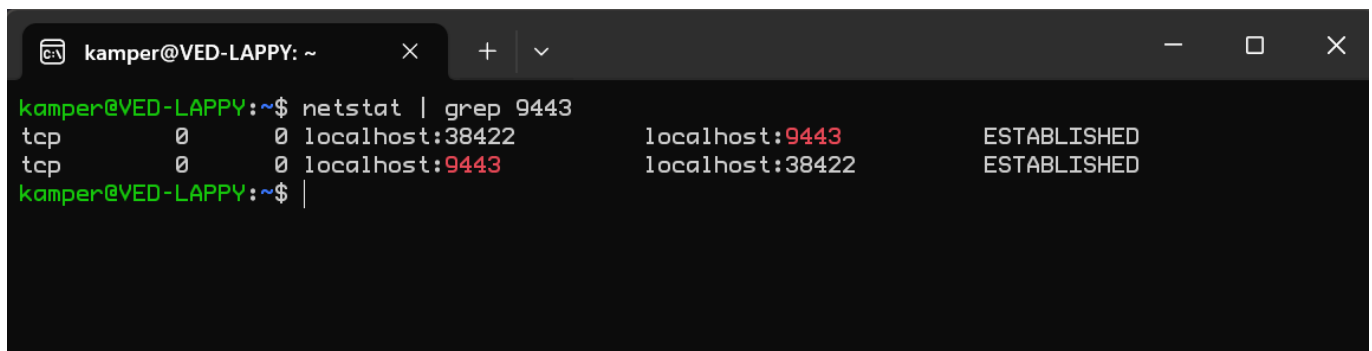
a.



Two terminal windows are shown side-by-side. Both windows have a title bar that reads 'kamper@VED-LAPPY: ~'. The left window shows the command 'netcat -l 9443' being executed, followed by the output 'Hello' and a cursor. The right window shows the command 'netcat localhost 9443' being executed, followed by the output 'Hello'.

```
kamper@VED-LAPPY: ~$ netcat -l 9443
Hello
kamper@VED-LAPPY: ~$ netcat localhost 9443
Hello
```

b.



A terminal window with a title bar that reads 'kamper@VED-LAPPY: ~'. The command 'netstat | grep 9443' is executed, resulting in two lines of output. The first line shows a TCP connection from localhost:38422 to localhost:9443 in an ESTABLISHED state. The second line shows a TCP connection from localhost:9443 to localhost:38422 in an ESTABLISHED state.

```
kamper@VED-LAPPY: ~$ netstat | grep 9443
tcp        0      0 localhost:38422    localhost:9443    ESTABLISHED
tcp        0      0 localhost:9443     localhost:38422    ESTABLISHED
kamper@VED-LAPPY: ~$
```

## Question 4

a.

```
pwsh in kamper x kamper@VED-LAPPY: ~ x + v
kamper@VED-LAPPY:~$ nslookup
> set querytype=soa
> google.in
Server:      10.255.255.254
Address:     10.255.255.254#53

Non-authoritative answer:
google.in
    origin = ns1.google.com
    mail addr = dns-admin.google.com
    serial = 668858537
    refresh = 900
    retry = 900
    expire = 1800
    minimum = 60


Authoritative answers can be found from:
ns1.google.com internet address = 216.239.32.10
ns1.google.com has AAAA address 2001:4860:4802:32::a
> exit

kamper@VED-LAPPY:~$ nslookup google.in ns1.google.com
Server:      ns1.google.com
Address:     216.239.32.10#53

Name:   google.in
Address: 142.250.207.196
Name:   google.in
Address: 2404:6800:4002:82e::2004

kamper@VED-LAPPY:~$
```

The query type soa shows where the authoritative answers can be found from.

b.  alt text This entry would expire from the local DNS server in 3600 seconds which means the cache for this will be cleared from the server every 184 seconds.

## Question 5

a.

```
pwsh in kamper x kamper@VED-LAPPY: ~ + v
kamper@VED-LAPPY:~$ traceroute google.in
traceroute to google.in (142.250.193.4), 30 hops max, 60 byte packets
 1 VED-LAPPY.mshome.net (172.29.208.1) 0.289 ms 0.257 ms 0.246 ms
 2 192.168.224.254 (192.168.224.254) 1.323 ms 1.631 ms 1.513 ms
 3 auth.iiitd.edu.in (192.168.1.99) 0.329 ms 0.320 ms 0.520 ms
 4 103.25.231.1 (103.25.231.1) 0.644 ms 0.634 ms 0.623 ms
 5 * * *
 6 10.119.234.162 (10.119.234.162) 5.213 ms * 5.719 ms
 7 72.14.195.56 (72.14.195.56) 5.582 ms 72.14.194.160 (72.14.194.160) 3.415 ms 3.401 ms
 8 192.178.80.159 (192.178.80.159) 26.744 ms 142.251.54.111 (142.251.54.111) 27.557 ms 192.178.80.159 (192.178.80.159) 27.024 ms
 9 142.251.54.87 (142.251.54.87) 24.374 ms 142.251.54.89 (142.251.54.89) 33.143 ms 33.136 ms
10 del11s14-in-f4.1e100.net (142.250.193.4) 29.794 ms 29.848 ms 29.610 ms
kamper@VED-LAPPY:~$
```

average latency

- 1 0.264ms
- 2 1.489ms
- 3 0.390ms
- 4 0.634ms
- 5 NA
- 6 5.466ms
- 7 4.132ms
- 8 27.115ms
- 9 30.218ms
- 10 29.751ms

b.

```
kamper@VED-LAPPY: ~ + v
kamper@VED-LAPPY:~$ ping google.in -c 50 > ping.txt
kamper@VED-LAPPY:~$
```

```
PING google.in (142.250.193.4) 56(84) bytes of data.
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=1 ttl=54
```

```
time=30.1 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=2 ttl=54
time=30.1 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=3 ttl=54
time=30.0 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=4 ttl=54
time=30.8 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=5 ttl=54
time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=6 ttl=54
time=30.1 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=7 ttl=54
time=30.3 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=8 ttl=54
time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=9 ttl=54
time=30.3 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=10 ttl=54
time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=11 ttl=54
time=30.6 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=12 ttl=54
time=30.1 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=13 ttl=54
time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=14 ttl=54
time=30.6 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=15 ttl=54
time=30.6 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=16 ttl=54
time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=17 ttl=54
time=30.1 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=18 ttl=54
time=30.4 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=19 ttl=54
time=30.8 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=20 ttl=54
time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=21 ttl=54
time=30.0 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=22 ttl=54
time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=23 ttl=54
time=30.6 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=24 ttl=54
time=30.1 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=25 ttl=54
time=30.4 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=26 ttl=54
time=31.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=27 ttl=54
time=30.7 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=28 ttl=54
```

```
time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=29 ttl=54
time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=30 ttl=54
time=30.3 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=31 ttl=54
time=30.1 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=32 ttl=54
time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=33 ttl=54
time=31.3 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=34 ttl=54
time=30.3 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=35 ttl=54
time=30.4 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=36 ttl=54
time=30.0 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=37 ttl=54
time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=38 ttl=54
time=30.3 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=39 ttl=54
time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=40 ttl=54
time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=41 ttl=54
time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=42 ttl=54
time=30.1 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=43 ttl=54
time=31.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=44 ttl=54
time=31.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=45 ttl=54
time=30.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=46 ttl=54
time=30.1 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=47 ttl=54
time=30.0 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=48 ttl=54
time=30.4 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=49 ttl=54
time=30.3 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=50 ttl=54
time=30.1 ms

--- google.in ping statistics ---
50 packets transmitted, 50 received, 0% packet loss, time 49089ms
rtt min/avg/max/mdev = 30.003/30.338/31.261/0.327 ms
```

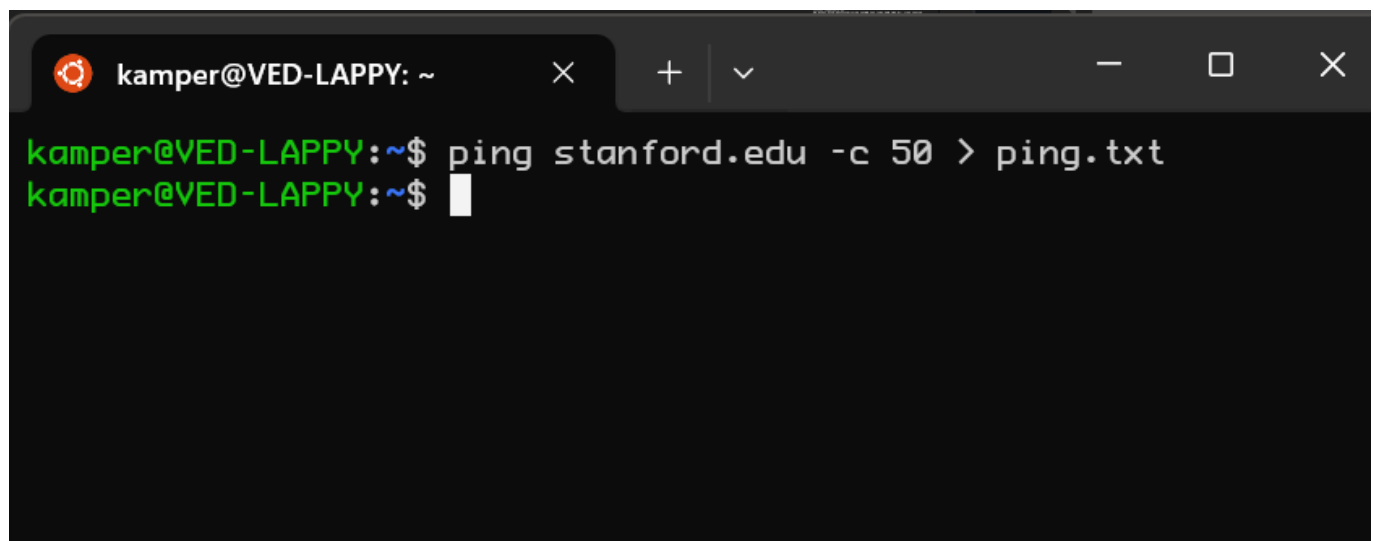
the average ping is 30.338ms. (NOTE: I decided to take text output because screenshot wouldn't fit the entire contents)

c. The total traceroute latency is 99.459ms which doesn't much the latency of 30.338ms from ping. Traceroute sends packets to each node and waits for the timeout response on each node. The traceroute shows the time it takes for each of those nodes to respond.

d. The maximum latency in (a) is very close to the average ping latency in (b). This is because the latency to get to the final destination should be the same.

e. There are more than one entries in intermediate hosts because there is more than one path from the machine to the final destination.

f.

A terminal window with a dark background. The title bar shows 'kamper@VED-LAPPY: ~' and standard window controls. The prompt is 'kamper@VED-LAPPY:~\$'. The command 'ping stanford.edu -c 50 > ping.txt' has been entered. The prompt is now 'kamper@VED-LAPPY:~\$' with a cursor.

```
PING stanford.edu (171.67.215.200) 56(84) bytes of data.  
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=1 ttl=235 time=271 ms  
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=2 ttl=235 time=271 ms  
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=3 ttl=235 time=271 ms  
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=4 ttl=235 time=271 ms  
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=5 ttl=235 time=271 ms  
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=6 ttl=235 time=271 ms  
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=7 ttl=235 time=271 ms  
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=8 ttl=235 time=271 ms  
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=9 ttl=235 time=271 ms  
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=10 ttl=235 time=270 ms  
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=11 ttl=235 time=271 ms  
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=12 ttl=235 time=271 ms  
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=13 ttl=235 time=271 ms  
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=14 ttl=235 time=272 ms  
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=15 ttl=235 time=271 ms  
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=16 ttl=235 time=271 ms  
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=17 ttl=235 time=271 ms  
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=18 ttl=235 time=271 ms  
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=19 ttl=235 time=271 ms  
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=20 ttl=235 time=271 ms  
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=21 ttl=235 time=271 ms  
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=22 ttl=235 time=271 ms
```

```
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=23 ttl=235 time=274 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=24 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=25 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=26 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=27 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=28 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=29 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=30 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=31 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=32 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=33 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=34 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=35 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=36 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=37 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=38 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=39 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=40 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=41 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=42 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=43 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=44 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=45 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=46 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=47 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=48 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=49 ttl=235 time=271 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=50 ttl=235 time=271 ms
```

```
--- stanford.edu ping statistics ---
```

```
50 packets transmitted, 50 received, 0% packet loss, time 49063ms
```

```
rtt min/avg/max/mdev = 270.380/270.999/274.375/0.556 ms
```

The average latency for stanford.edu is 270.999ms

9.



```

kamper@VED-LAPPY: ~$ traceroute stanford.edu
traceroute to stanford.edu (171.67.215.200), 30 hops max, 60 byte packets
 1 VED-LAPPY.mshome.net (172.29.208.1) 0.246 ms 0.215 ms 0.328 ms
 2 192.168.224.254 (192.168.224.254) 2.356 ms 2.488 ms 2.600 ms
 3 vpn.iiitd.edu.in (192.168.1.99) 0.231 ms 0.208 ms 0.201 ms
 4 103.25.231.1 (103.25.231.1) 0.587 ms 0.476 ms 0.574 ms
 5 10.1.209.201 (10.1.209.201) 23.704 ms 23.511 ms 23.678 ms
 6 10.1.200.137 (10.1.200.137) 44.162 ms 44.045 ms 43.729 ms
 7 10.255.238.254 (10.255.238.254) 24.943 ms 24.919 ms 10.255.238.122 (10.255.238.122) 23.407 ms
 8 180.149.48.18 (180.149.48.18) 27.456 ms 27.713 ms 27.809 ms
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 campus-ial-nets-b-v11104.SUNet (171.66.255.200) 273.401 ms campus-east-rtr-v11120.SUNet (171.66.255.232) 278.63
1 ms campus-east-rtr-v11020.SUNet (171.64.255.232) 269.697 ms
25 campus-ial-nets-b-v11120.SUNet (171.66.255.232) 278.831 ms * 278.723 ms
26 web.stanford.edu (171.67.215.200) 270.727 ms 270.580 ms *
kamper@VED-LAPPY:~$

```

there are 26 intermediate hosts in stanford.edu compared to 10 intermediate hosts in google.in

h. The main reason for higher latency in stanford.edu compared to google.in is due to the distance of the machines being different. stanford.edu probably has its node in america while google.in is probably in India. Latency of communication increases as distance increases.

## Question 6

```

kamper@VED-LAPPY: ~$ sudo ifconfig lo down
kamper@VED-LAPPY:~$ 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 ---
2 packets transmitted, 0 received, 100% packet loss, time 1034ms
kamper@VED-LAPPY:~$

```

Just remove the loopback and you can have 100% packet loss.