

COMPUTER NETWORKS

ASSIGNMENT NO-1

Q 1)

Ans a) The output on running ifconfig on my device is as follows:-

```
farhan ➜ ~ ➜ 9.014s ➜ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
        ether a2:b2:c7:e3:d4:46 txqueuelen 0 (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 39 overruns 0 carrier 0 collisions 0

enp0s31f6: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 08:8f:c3:d5:24:8c 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
    device interrupt 16 memory 0x5e500000-5e520000

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 17645 bytes 2129757 (2.1 MB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 17645 bytes 2129757 (2.1 MB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 192.168.122.1 netmask 255.255.255.0 broadcast 192.168.122.255
        ether 52:54:00:ab:46:bf 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 50 overruns 0 carrier 0 collisions 0

wlp43s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.248.166.148 netmask 255.255.255.0 broadcast 10.248.166.255
        inet6 fe80::ee9e:334b:da90:f46e prefixlen 64 scopeid 0x20<link>
            ether f4:6a:dd:8c:d6:f7 txqueuelen 1000 (Ethernet)
            RX packets 522565 bytes 675780798 (675.7 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 130867 bytes 37278696 (37.2 MB)
            TX errors 0 dropped 57 overruns 0 carrier 0 collisions 0
```

As seen the image the ifconfig command describes various network interfaces of the device such as wlp43s0 which is the WiFi network interface and on top of that it also gives us information about the activities of the network interfaces for example the no. of packets shared . As we can see my device has a wireless connection , Ethernet connection , a connection created by docker so as to connect the docker application to the internet. We can also see that except wlp43s0 no other interface is receiving any kind of data so we can say sat only wlp43s0 is active at the moment.

Ans b) Some of the options of ifconfig are as follows:-

1)txqueuelen – It is used to decide the queue length before processing it further and sending to the next routers it decides how many maximum packets can stay in the queue at a given point of time .

2)up and down- It is used to switch off/on a network manually as per the requirement .The commands used are as follows - sudo ifconfig wlp43s0 down,sudo ifconfig wlp43s0 up.

3)mtu-MTU stands for maximum transmission unit which describes the maximum size of a packet .It can help in stablizing a connection or improving it in case of high-latency scenarios.

4)-s – It stands for short list and summarises each network removing residual information from each of them . It gives output as shown below .

| Iface | MTU | RX-OK | RX-ERR | RX-DRP | RX-OVR | TX-OK | TX-ERR | TX-DRP | TX-OVR | Flg |
|-----------|-------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| docker0 | 1500 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 40 | 0 BMU |
| enp0s31f6 | 1500 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 BMU |
| lo | 65536 | 19172 | 0 | 0 | 0 | 19172 | 0 | 0 | 0 | 0 LRU |
| virbr0 | 1500 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 51 | 0 BMU |
| wlp43s0 | 1500 | 544925 | 0 | 0 | 0 | 145738 | 0 | 0 | 66 | 0 BMRU |

Q2)

Ans a) The netstat stands for network statistics .It is used to display network connections, routing tables, interface statistics, and other network-related information on a system. It gives information about active servers and domain sockets.

Ans b) The active ports on my system are as follows:-

| Place your right thumb on the fingerprint reader | | | | | | |
|-------------------------------------------------------|--------|--------|---------------------|---------------------|-------------|---------------------|
| Active Internet connections (servers and established) | | | | | | |
| Proto | Recv-Q | Send-Q | Local Address | Foreign Address | State | PID/Program name |
| tcp | 0 | 0 | 127.0.0.1:6463 | 0.0.0.0:* | LISTEN | 6819/exe |
| tcp | 0 | 0 | 127.0.0.1:3306 | 0.0.0.0:* | LISTEN | 1590/mysql |
| tcp | 0 | 0 | 127.0.0.1:33060 | 0.0.0.0:* | LISTEN | 1590/mysql |
| tcp | 0 | 0 | 192.168.122.1:53 | 0.0.0.0:* | LISTEN | 1667/dnsmasq |
| tcp | 0 | 0 | 127.0.0.54:53 | 0.0.0.0:* | LISTEN | 854/systemd-resolve |
| tcp | 0 | 0 | 127.0.0.1:631 | 0.0.0.0:* | LISTEN | 1491/cupsd |
| tcp | 0 | 0 | 127.0.0.53:53 | 0.0.0.0:* | LISTEN | 854/systemd-resolve |
| tcp | 0 | 0 | 127.0.0.1:5432 | 0.0.0.0:* | LISTEN | 1569/postgres |
| tcp | 0 | 0 | 10.10.213.100:47210 | 35.186.224.39:443 | ESTABLISHED | 6758/exe |
| tcp | 0 | 0 | 10.10.213.100:48762 | 57.144.125.32:5222 | ESTABLISHED | 4653/brave --type=u |
| tcp | 0 | 0 | 10.10.213.100:58974 | 35.186.224.35:443 | ESTABLISHED | 4653/brave --type=u |
| tcp | 0 | 0 | 10.10.213.100:37992 | 162.159.136.234:443 | ESTABLISHED | 6758/exe |
| tcp6 | 0 | 0 | ::1716 | ::* | LISTEN | 3134/kdeconnectd |
| tcp6 | 0 | 0 | ::1:631 | ::* | LISTEN | 1491/cupsd |
| udp | 0 | 0 | 0.0.0.0:43193 | 0.0.0.0:* | | 936/avahi-daemon: r |
| udp | 0 | 0 | 192.168.122.1:53 | 0.0.0.0:* | | 1667/dnsmasq |
| udp | 0 | 0 | 127.0.0.54:53 | 0.0.0.0:* | | 854/systemd-resolve |
| udp | 0 | 0 | 127.0.0.53:53 | 0.0.0.0:* | | 854/systemd-resolve |
| udp | 0 | 0 | 0.0.0.0:67 | 0.0.0.0:* | | 1667/dnsmasq |
| udp | 0 | 0 | 10.10.213.100:68 | 10.200.10.250:67 | ESTABLISHED | 1193/NetworkManager |
| udp | 0 | 0 | 224.0.0.251:5353 | 0.0.0.0:* | | 4574/brave |
| udp | 0 | 0 | 0.0.0.0:5353 | 0.0.0.0:* | | 936/avahi-daemon: r |
| udp | 0 | 0 | 10.10.213.100:46777 | 142.250.192.106:443 | ESTABLISHED | 4653/brave --type=u |
| udp6 | 0 | 0 | :::49818 | ::* | | 936/avahi-daemon: r |
| udp6 | 0 | 0 | ::5353 | ::* | | 936/avahi-daemon: r |
| udp6 | 0 | 0 | ::1716 | ::* | | 3134/kdeconnectd |

The port for my browser(brave) is 5353 and pid is 4574. Only tcp udp ports are found in my pc.

Ans c) The command for it is netstat -su where s is for the statistics and u limits it to only udp. The output which I got by running it was follows:-

```
farhan ➜ ~/..../12340740 ✘ main ✘ 3.13.5 ➜ 2.766s sudo netstat -su
IcmpMsg:
  InType0: 24
  InType3: 874
  InType8: 2
  InType11: 57
  OutType0: 2
  OutType3: 1204
  OutType5: 3
  OutType8: 24
Udp:
  246046 packets received
  1147 packets to unknown port received
  3120 packet receive errors
  126537 packets sent
  3120 receive buffer errors
  79 send buffer errors
UdpLite:
IpExt:
  InNoRoutes: 62
  InMcastPkts: 601
  OutMcastPkts: 1233
  InBcastPkts: 2
  OutBcastPkts: 4
  InOctets: 1167541919
  OutOctets: 60496825
  InMcastOctets: 61720
  OutMcastOctets: 182851
  InBcastOctets: 4576
  OutBcastOctets: 4616
  InNoECTPkts: 913873
  InECT1Pkts: 109188
  InECT0Pkts: 4160
  InCEPkts: 23
MPTcpExt:
```

Q3)

Ans a) Ping is a network utility command used to test the rechablity of a host of an IP network by sending ICMP echo request packets and measuring time taken to receive those replies.

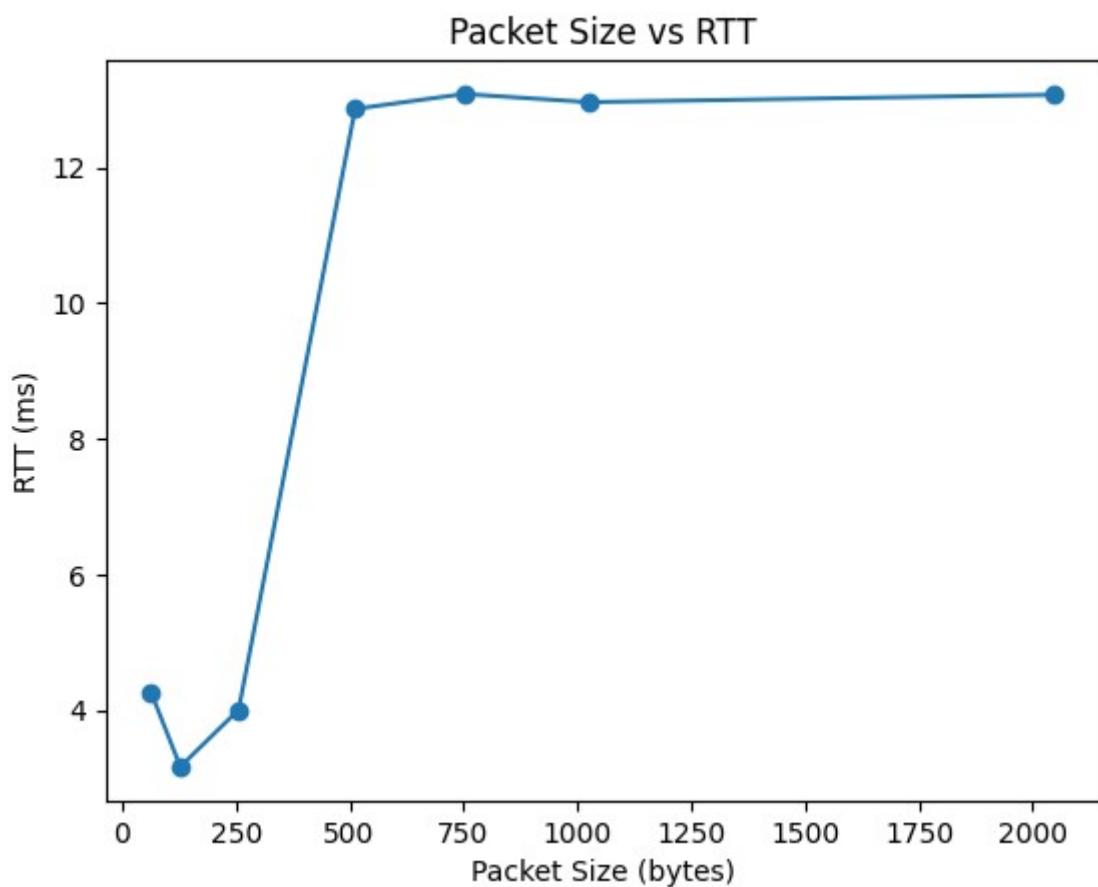
Ans b)

| Site | ip | distance | RTT | Time |
|------------|---------------|----------|---------|-------------|
| reddit.com | 151.101.1.140 | 15470 | 18.32 | 07:07:00 PM |
| openai.com | 104.18.33.45 | 15470 | 7.405 | 07:18:00 PM |
| lenovo.com | 104.69.42.39 | 3299 | 243.699 | 07:20:00 PM |
| reddit.com | 151.101.1.140 | 15470 | 18.54 | 01:18:00 AM |
| openai.com | 104.18.33.45 | 15470 | 7.388 | 01:18:00 AM |
| lenovo.com | 104.69.42.39 | 3299 | 268.065 | 01:18:00 AM |
| reddit.com | 151.101.1.140 | 15470 | 18.571 | 10:38:00 AM |
| openai.com | 104.18.33.45 | 15470 | 7.93 | 10:41:00 AM |
| lenovo.com | 104.69.42.39 | 3299 | 241.915 | 10:43:00 AM |
| reddit.com | 151.101.1.140 | 15470 | 19.85 | 07:08:00 PM |
| openai.com | 104.18.33.45 | 15470 | 7.343 | 07:09:00 PM |
| lenovo.com | 104.69.42.39 | 3299 | 250.783 | 07:09:00 PM |

We can see that for companies like reddit and open ai the rtt is quite stable irrespective of time because of global cdn and lenovo.com has a change of 18-20 ms wrt time we can see that in afternoon the time increases due to more traffic compared to night time.

Ans c) The site used was 8.8.8.8 (google) the data recorded was as follows:-

| ip | package size | RTT Time |
|---------|--------------|--------------------|
| 8.8.8.8 | 64 | 4.254 06:11:00 PM |
| 8.8.8.8 | 128 | 3.161 06:11:00 PM |
| 8.8.8.8 | 256 | 4 06:11:00 PM |
| 8.8.8.8 | 512 | 12.865 06:11:00 PM |
| 8.8.8.8 | 751 | 13.085 06:11:00 PM |
| 8.8.8.8 | 1024 | 12.964 06:11:00 PM |
| 8.8.8.8 | 1300 | 13.073 06:11:00 PM |

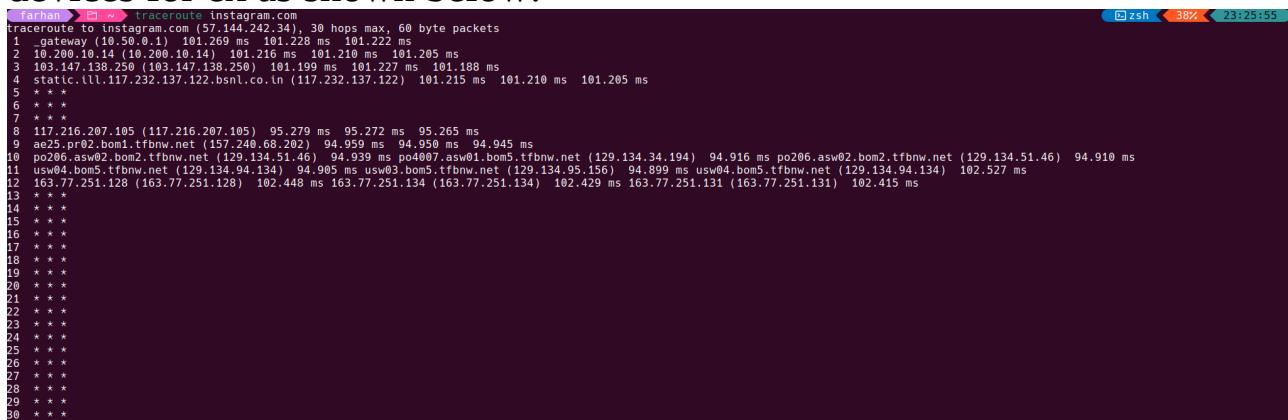


Ans d) From our observations we get that as we increase packet size rtt increase and during the afternoon hours the rtt increase where rtt is low during midnight.

Q4)

Ans a) Traceroute provides data about how a packet travels from source to destination .It lists each intermediate device between the source and destination , it also displays transit delays of packets across these devices.It also provides various other things like time to live ,round trip time,hostname .

Ans b) Many times traceroute shows * * * as the output for some of the devices for ex as shown below: -



```
farhan@farhan-OptiPlex-5070: ~ % traceroute to instagram.com (57.144.242.34), 30 hops max, 60 byte packets
1 gateway (10.50.8.1) 101.269 ms 101.228 ms 101.222 ms
2 10.200.19.14 (10.200.19.14) 101.216 ms 101.210 ms 101.205 ms
3 103.147.138.250 (103.147.138.250) 101.199 ms 101.227 ms 101.188 ms
4 static.ctl.117.232.137.122.bsnl.co.in (117.232.137.122) 101.215 ms 101.210 ms 101.205 ms
5 * * *
6 * * *
7 * * *
8 117.216.207.105 (117.216.207.105) 95.279 ms 95.272 ms 95.265 ms
9 ae25.pr02.bom1.tfbnw.net (157.240.68.202) 94.959 ms 94.950 ms 94.945 ms
10 po206.asw02.bom2.tfbnw.net (129.134.51.46) 94.939 ms po4007.asw01.bom5.tfbnw.net (129.134.34.194) 94.916 ms po206.asw02.bom2.tfbnw.net (129.134.51.46) 94.910 ms
11 usw04.bom5.tfbnw.net (129.134.94.134) 94.905 ms usw03.bom5.tfbnw.net (129.134.95.156) 94.899 ms usw04.bom5.tfbnw.net (129.134.94.134) 102.527 ms
12 163.77.251.128 (163.77.251.128) 102.448 ms 163.77.251.134 (163.77.251.134) 102.429 ms 163.77.251.131 (163.77.251.131) 102.415 ms
13
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
```

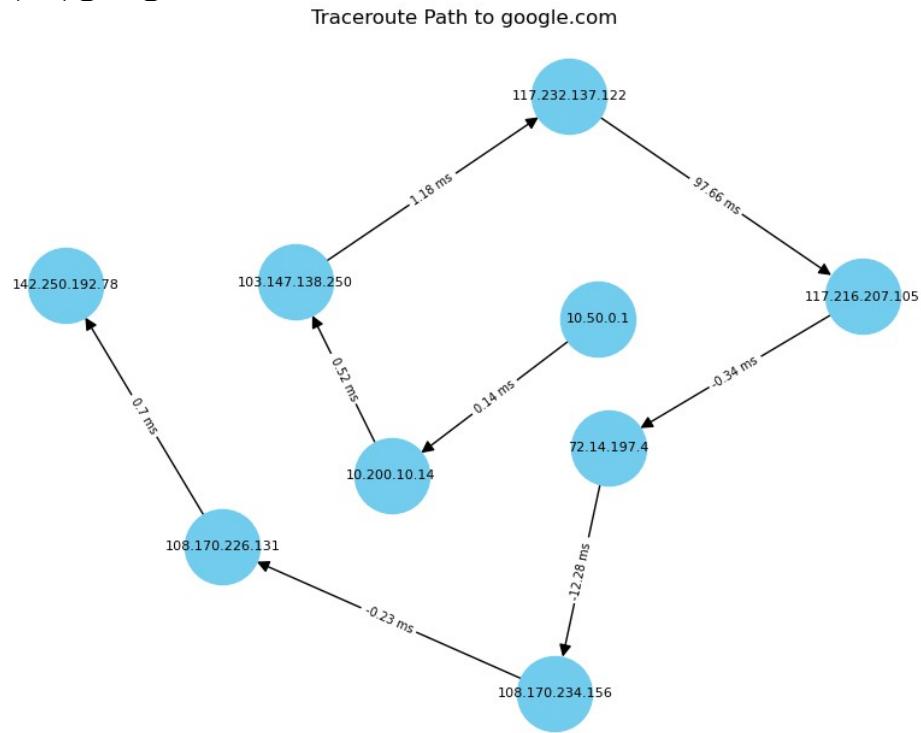
This sometimes depicts that the network is down but thats not the case generally this done deliberately by the provider with the reasons being as follows:-

- 1)Many routers are configured to not send ICMP responses for security or load reasons.It helps in avoiding ddos attacks and reduces cpu usage .
- 2)Many enterprise firewalls treat traceroute packets (Ucp,tcp etc based) as suspicious and drop them.
- 3)Routers prioritize forwarding over tasks like sending ICMP responses .Thus resulting in the asteriks.

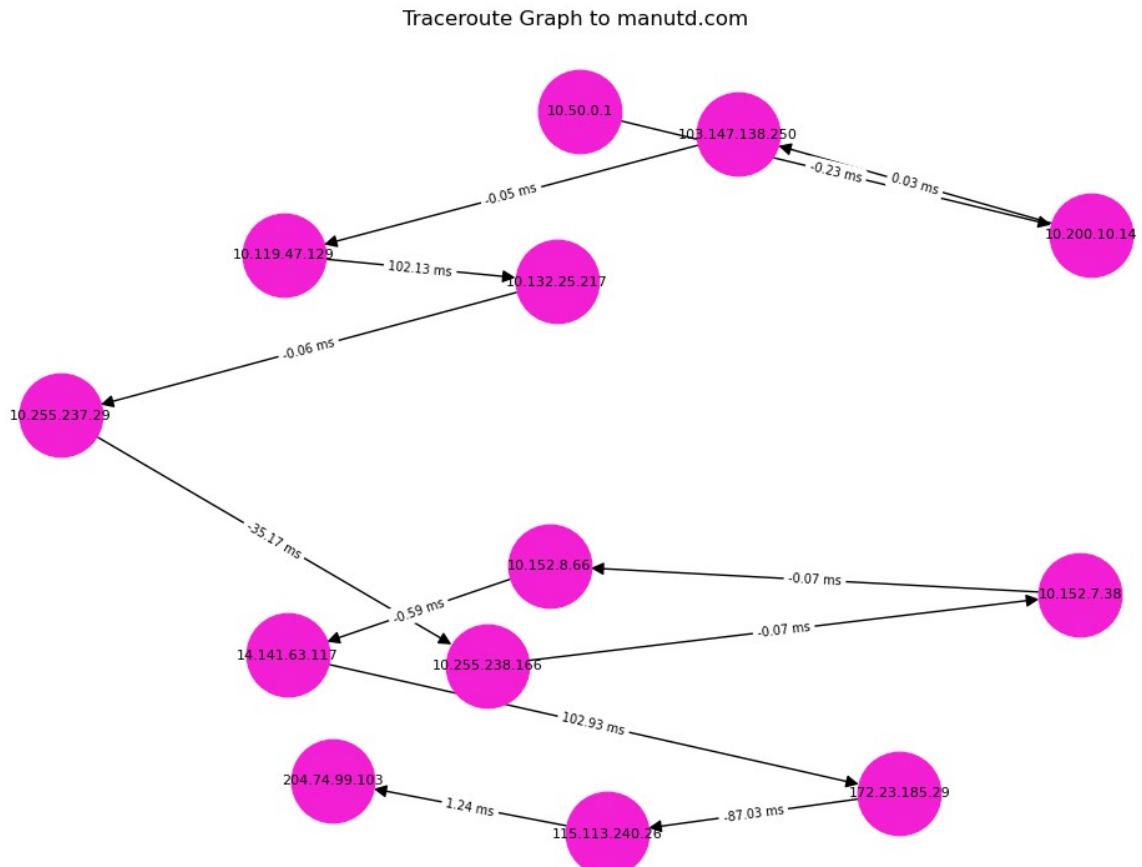
Ans c)Yes it is possible to find the route to specific hosts which fail to respond to the ping experiment.

The reason being that the ping only tests reachability of the end host I.e the destination whereas the traceroute provides info about the path being followed to reach the end host so if there is a case whereas the traceroute gives information about each router / device in between the client and the end host so if only the end host is not reachable by the ping I.e it blocks the icmp echo then we would be able to idnetify path using traceroute another scenariow would be if ICMP time limit is exceeded (ping fails in this case) then also trace route would work.

Ans d) 1)google.com

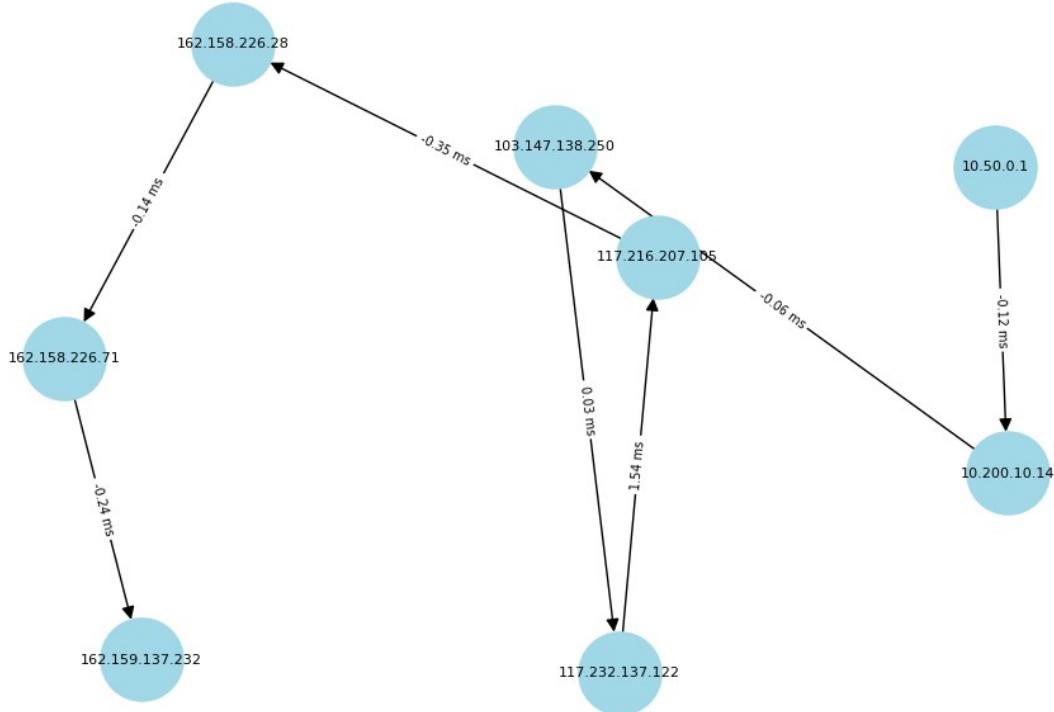


b)manutd.com



c)discord.com

Traceroute to discord.com (162.159.137.232)



Q5)

Ans a) Nmap is a network scanner used to discover hosts services provided by them their activity status on a network . This is done by sending packets and analising the responses.

Ans b) The open ports of iitbihilai.ac.in are as follows:-

```

farhan ➜ 44.431s nmap -sV iitbihilai.ac.in
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-10 12:20 IST
Nmap scan report for iitbihilai.ac.in (192.168.10.115)
Host is up (0.021s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.4 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16)
443/tcp   open  ssl/http    Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16)
5666/tcp  open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.93 seconds
  
```

The open ports are as follows:-

| PORT | SERVICE | VERSION |
|----------|----------|----------------------------|
| 22/tcp | ssh | OpenSSH 7.4 (protocol 2.0) |
| 80/tcp | http | Apache httpd 2.4.6 |
| 443/tcp | ssl/http | Apache httpd 2.4.6 |
| 5666/tcp | open | tcpwrapped |

The services are as follows:-

- 1) ssh- SSH stands for secure shell protocol which as the name suggests is a security protocol for operating network services over an unsecured

network. It is generally used to access a device remotely and execute commands in its terminal.22/tcp provides ssh service.

2)http-HTTP stands for hypertext transfer protocol which is an application layer protocol and is used to request and deliver web content over the Internet.80/tcp provides this service.

3)https-HTTPS stands for HyperText Transfer Protocol Secure .It is the same as HTTP but provides security /encryption over the http protocol.443/tcp follows this.

4)nrpe-NRPE stands for nagois remote plugin executor .It offers remote alerting and monitoring of system and alerts when things go wrong and again when they are resolved.

Ans c) The os of iitbihilai.ac.in could be found using the following command:- sudo nmap -O iitbihilai.ac.in

The output is as follows:-

```
farhan@farhan:~$ sudo nmap -O iitbihilai.ac.in
[sudo] password for farhan:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-10 12:08 IST
Nmap scan report for iitbihilai.ac.in (192.168.10.115)
Host is up (0.015s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
5666/tcp  open  nrpe
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

TCP/IP fingerprint:

```
OS:SCAN(V=7.94SVN%E=4%D=1/10%OT=22%CT=1%CU=43732%PV=Y%DS=3%DC=I%G=Y%TM=6961
OS:F3FE%P=x86_64-pc-linux-gnu)SEQ(SP=107%CD=1%ISR=106%TI=Z%II=I%TS=A)SEQ(S
OS:P=107%CD=3%ISR=106%TI=Z%II=I%TS=A)OPS(01=M4E2ST11NW7%02=M4E2ST11NW7%03=
05:M4E2NT11NW7%04=M4E2ST11NW7%05=M4E2ST11NW7%06=M4E2ST11)WINT(W1=7120%W2=71
0%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%0=M4E2NNSNW7
OS:%C=C=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=5+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(
OS=R=Y%DF=Y%T=40%W=0%S=Z%A=5+%F=AR%=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=4
OS:0%PL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

Network Distance: 3 hops

```
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.54 seconds
```

although the output says no exact os matches found we do have something in the output P=x86_64-pc-linux-gnu from which we can conclude that the os is linux.

Ans d) 1)lenovo.com

a)services and version

```

Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-10 12:46 IST
Nmap scan report for lenovo.com (23.47.239.18)
Host is up (0.036s latency).
rDNS record for 23.47.239.18: a23-47-239-18.deploy.static.akamaitechnologies.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): OpenBSD 4.X (86%)
OS CPE: cpe:/o:openbsd:openbsd4.0
Aggressive OS guesses: OpenBSD 4.0 (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.88 seconds

```

b) Operating system

```

farhan@farhan: ~ % sudo nmap -O lenovo.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-10 23:20 IST
Nmap scan report for lenovo.com (23.47.239.18)
Host is up (0.095s latency).
rDNS record for 23.47.239.18: a23-47-239-18.deploy.static.akamaitechnologies.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.69 seconds

```

2) openai.com

a) services and version

```

farhan@farhan: ~ % 27.741s nmap -sV openai.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-10 12:39 IST
Nmap scan report for openai.com (104.18.33.45)
Host is up (0.064s latency).
Other addresses for openai.com (not scanned): 172.64.154.211
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Cloudflare http proxy
443/tcp   open  ssl/http Cloudflare http proxy
8080/tcp  open  http    Cloudflare http proxy
8443/tcp  open  ssl/http Cloudflare http proxy

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.93 seconds

```

b) Operating system

```

[sudo] password for farhan:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-10 12:42 IST
Nmap scan report for openai.com (104.18.33.45)
Host is up (0.053s latency).
Other addresses for openai.com (not scanned): 172.64.154.211
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.48 seconds

```