CS301 Computer Networks Assignment 1

Ojus Goel

August 17, 2024

Answer 1

1. Ifconfig shows currently active interfaces and shows the 3 network interfaces on my system:

   (a) **docker0**: It is a virtual network interface for container communication. It has IPv4 address 172.17.0.1.

   (b) **Io**: It is used for internal communication within the system. It has the IPv4 address 127.0.0.1

   (c) **Wlp0s20f3**: It is the wifi network interface. This also shows my system's IP 10.10.2.98

   It also includes information about the received and transmitted packets, also about any errors for each of the above networks.

```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ 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 02:42:ee:8b:3f:09  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 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 51881  bytes 7459084 (7.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 51881  bytes 7459084 (7.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.2.98  netmask 255.255.252.0  broadcast 10.10.3.255
        inet6 fe80::22df:4cc6:8fa3:3cc6  prefixlen 64  scopeid 0x20<link>
        ether 38:7a:0e:01:30:47  txqueuelen 1000  (Ethernet)
        RX packets 1619239  bytes 1645830251 (1.6 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 766574  bytes 280742419 (280.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. We can use the following options with ifconfig command:

   (a) **ifconfig -a:** It displays all the currently available interfaces

   (b) **ifconfig -s:** It displays short list of interfaces

   (c) **ifconfig [interface] up:** This activates network interface, and make it available for use

   (d) **ifconfig [interface] mtu [size] :** With this we can set Maximum Transmission Unit (MTU) for a network interface.

```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ ifconfig -a
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:ee:8b:3f:09  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 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 54428  bytes 7834254 (7.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 54428  bytes 7834254 (7.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.2.41  netmask 255.255.252.0  broadcast 10.10.3.255
        inet6 fe80::22df:4cc6:8fa3:3cc6  prefixlen 64  scopeid 0x20<link>
        ether 38:7a:0e:01:30:47  txqueuelen 1000  (Ethernet)
        RX packets 1707000  bytes 1726182380 (1.7 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 816059  bytes 296866061 (296.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ ifconfig -s
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      0 BMU
lo       65536    54501      0      0 0         54501      0      0      0 LRU
wlp0s20f  1500  1709192      0      0 0        816801      0      0      0 BMRU
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ ifconfig lo up
SIOCSIFFLAGS: Operation not permitted
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ sudo ifconfig lo up
[sudo] password for ojusg:
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ ifconfig lo mtu 65000
SIOCSIFMTU: Operation not permitted
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ sudo ifconfig lo mtu 65000
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ ifconfig -s
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      0 BMU
lo       65000    54525      0      0 0         54525      0      0      0 LRU
wlp0s20f  1500  1709617      0      0 0        817196      0      0      0 BMRU
```

Answer 2

1. The ping command is a utility tool to test if a device is reachable and test connectivity between your computer and other devices (like server or another computer). We can diagnose networks with its help by sending a series of echo packets to the target device and waiting for echo reply packets.

   Uses:

   (a) Check network connectivity

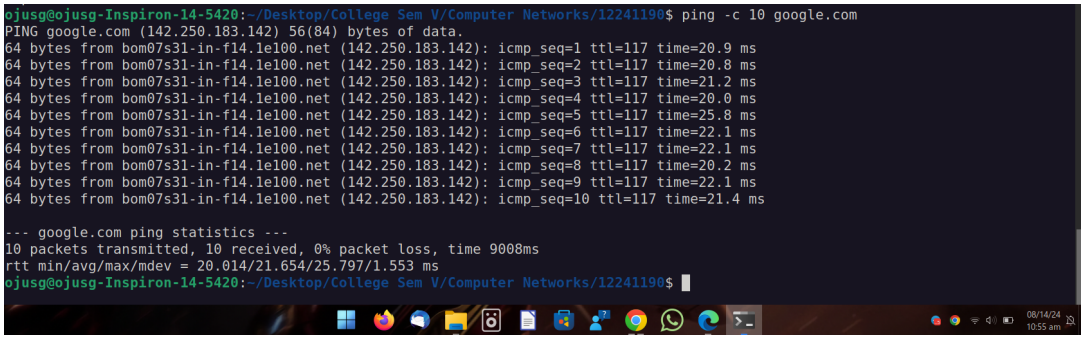
   (b) Measure latency

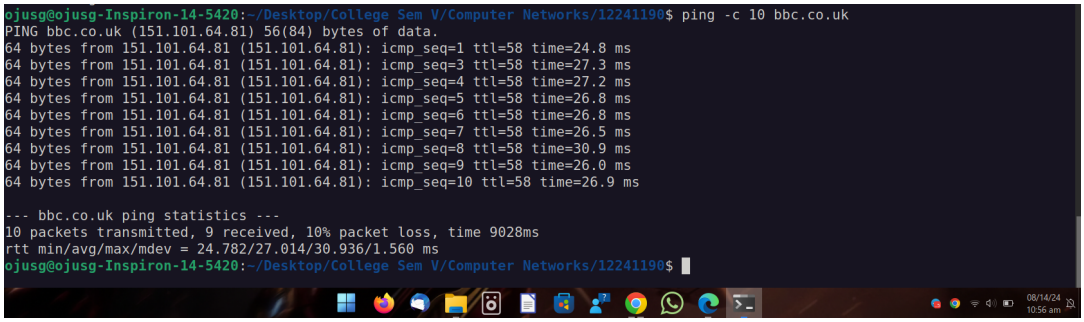
   (c) Detect packet loss

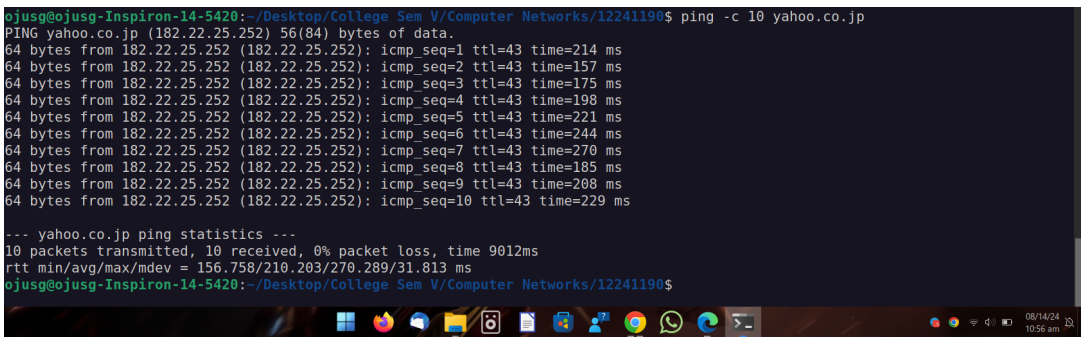
   (d) Determine Host Availability

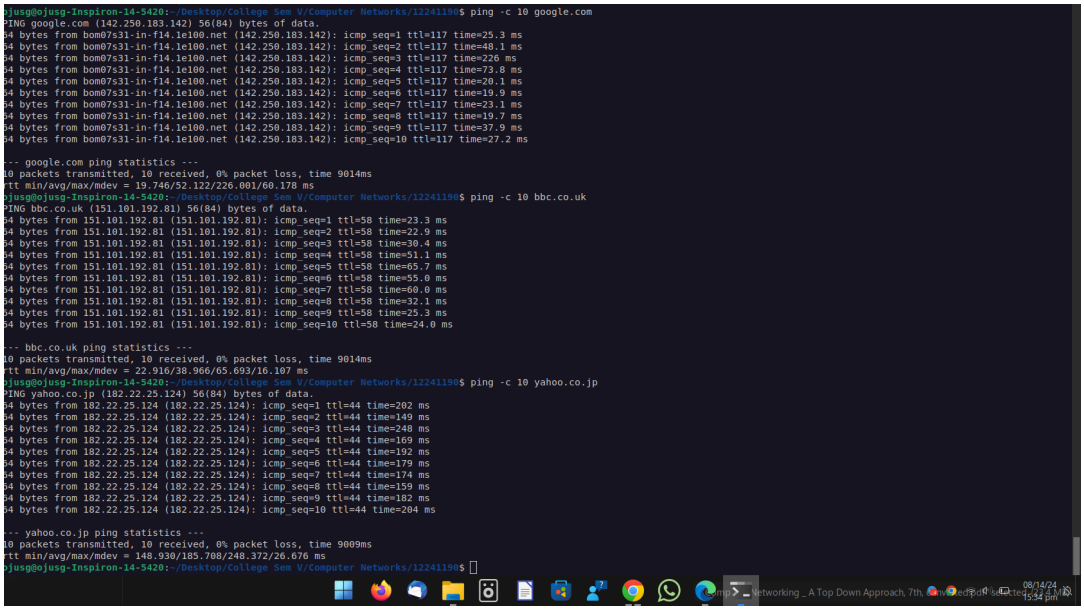
2. a) **Average RTT**

Time	google.com (142.250.183.142)	bbc.co.uk (151.101.64.81)	yahoo.co.jp (182.22.25.252)
10:55	21.654 ms	27.014 ms	210.203 ms
15:35	52.122 ms	38.966 ms	185.708 ms
22:35	21.583 ms	23.358 ms	175.069 ms





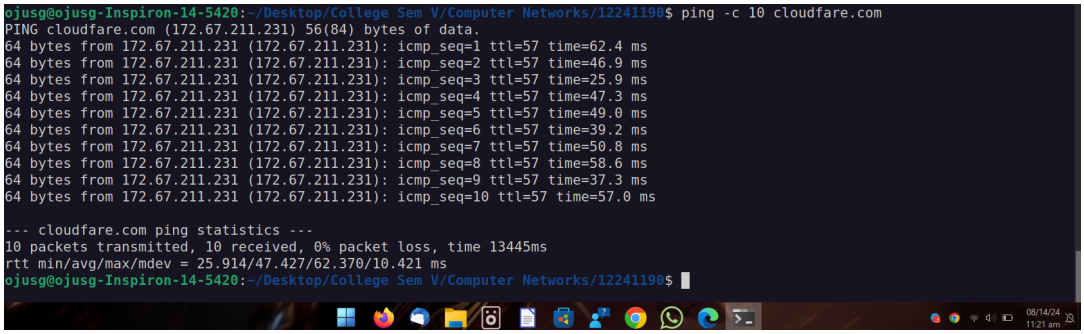


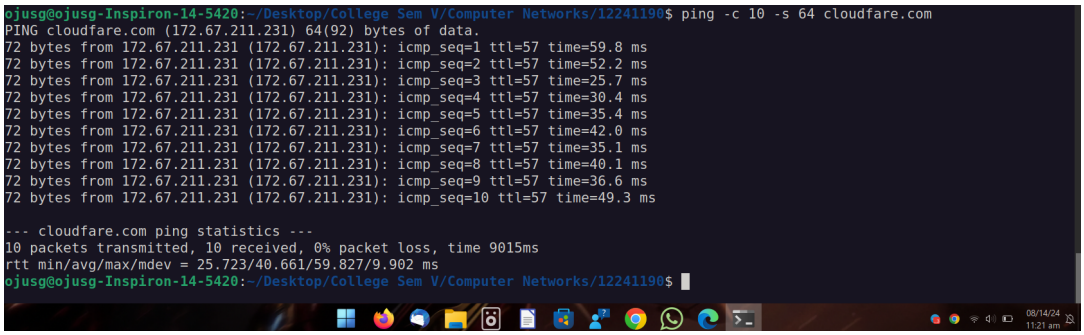


Yes, RTT has correlation with geographical distance of destinations from source. RTT is generally higher for farther away geographical locations due to internet propagation delay. Distance is a significant factor but we also need to consider the efficiency of the network path between source and destination.

b) Tried with google.com but the results were truncated because they exceeded the maximum packet size that could be handled. So tried with cloudflare.com because it has high mtu.

cloudflare.com (104.21.77.216)





Packet Size	Average RTT
64	40.661
128	50.204
256	61.379
384	54.311
512	53.635
640	55.053
768	59.940
896	49.286
1024	54.590
1152	50.996
1280	55.600
1408	52.975
1536	(100% packet loss)

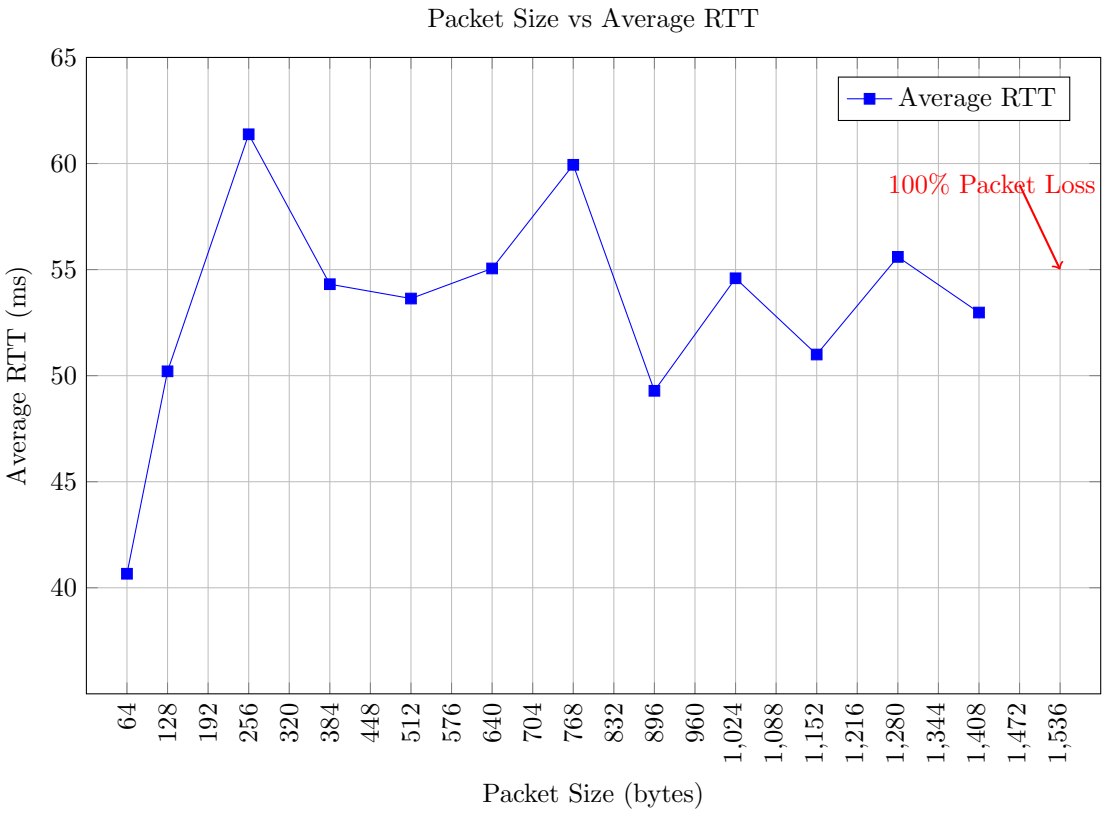


Figure 1: Graph of Packet Size vs Average RTT

c) **Impact of packet size on RTT:**

Larger packets take more time to transmit and receive leading to higher RTT.

If packets exceed MTU, they need to be fragmented, which adds to the processing time.

Larger packets may cause more delay due to buffering and queuing.

Impact of time of day on RTT:

Network congestion during peak hours can increase RTT because network traffic is higher due to more usage.

Answer 3

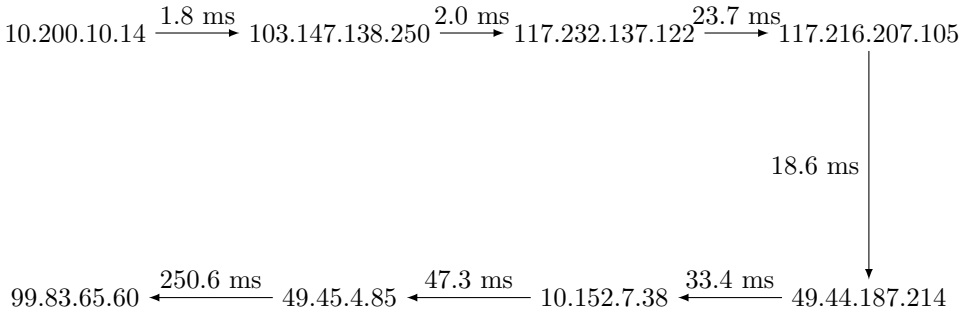
1. Traceroute is used to track the path taken by a packet from a source to the destination over an IP network. It shows the series of intermediate devices that packets pass through to reach the destination.

2. (a) **Traceroute does not find the complete paths in the following cases:**
   i. Firewall / Security configurations:Some network devices may be configured to block certain ICMP packets or traceroute probes as a security measure.
   ii. ICMP rate limiting: Some routers may limit the rate of ICMP packets to prevent denial of service attacks.
   iii. Network Congestion: High traffic can lead to packet drop.
   iv. Packet Fragmentation: If packages are too large then they are fragmented, and some routers might not handle fragmented packets correctly.

3. Yes, with traceroute it is possible to find a route to a specific host that does not respond to ping. Ping sends out an ICMP echo request message to the target host and has to wait for an echo reply. Some target hosts are configured to ignore ping requests, or due to network issues we may not get a response. Traceroute doesn't depend only on reply messages by hosts, it traces route to host, showing each hop along the way. Traceroute can hence be used to identify wherever failure occurs if a router is down, unreachable or misconfigured.

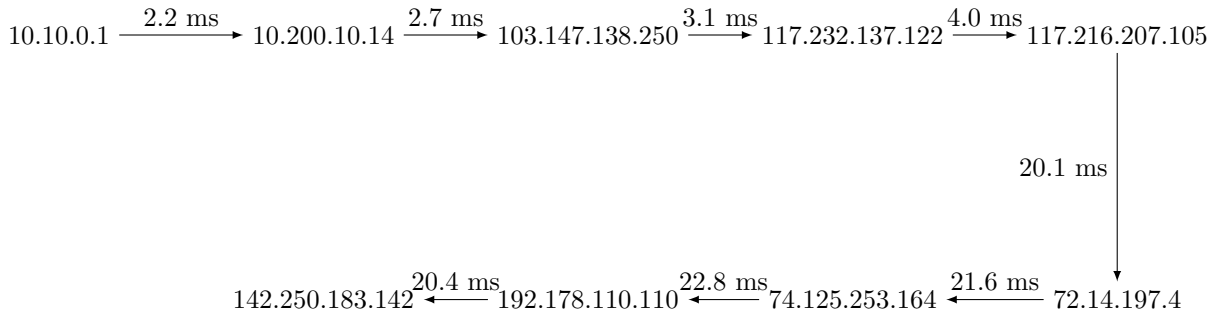
4.

Traceroute to netflix.com



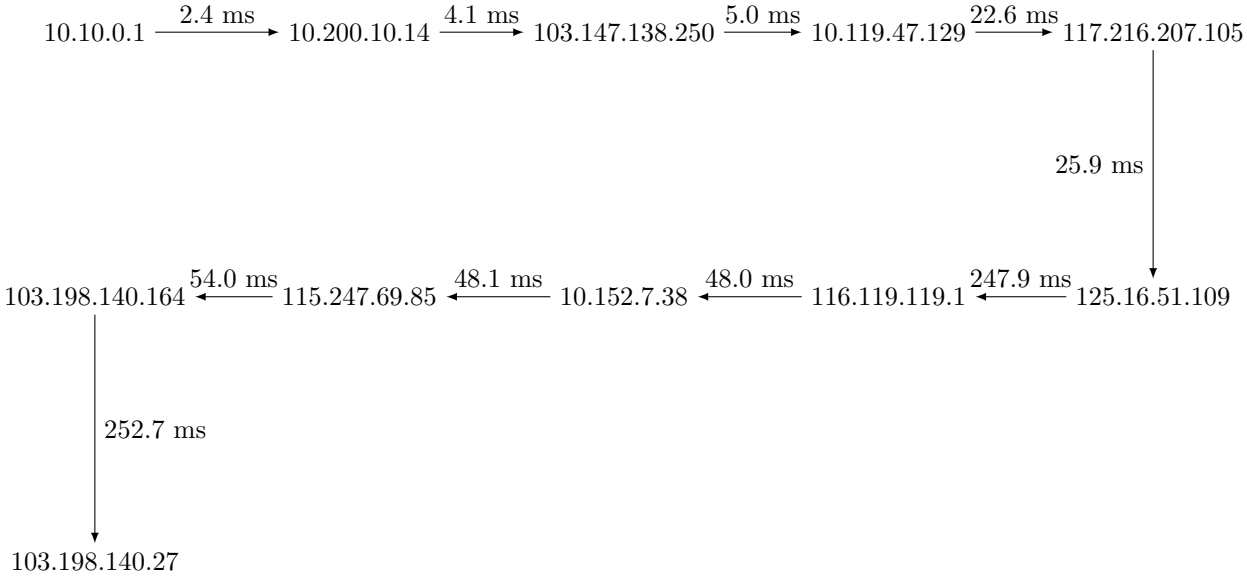

```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ traceroute netflix.com
traceroute to netflix.com (44.226.113.145), 30 hops max, 60 byte packets
 1  * * *
 2  10.200.10.14 (10.200.10.14)  1.832 ms  1.827 ms  1.822 ms
 3  103.147.138.250 (103.147.138.250)  1.998 ms  1.781 ms  1.775 ms
 4  static.ill.117.232.137.122.bsnl.co.in (117.232.137.122)  23.735 ms 10.119.47.129 (10.119.47.129)  2.063 ms  2.382 ms
 5  117.216.207.105 (117.216.207.105)  18.602 ms  18.824 ms  18.589 ms
 6  49.44.187.214 (49.44.187.214)  33.352 ms * *
 7  * * *
 8  10.152.7.38 (10.152.7.38)  47.294 ms 103.198.140.64 (103.198.140.64)  43.312 ms  43.502 ms
 9  49.45.4.85 (49.45.4.85)  250.586 ms  251.426 ms  253.966 ms
10  * * 99.83.65.60 (99.83.65.60)  253.025 ms
11  * 103.198.140.64 (103.198.140.64)  58.919 ms *
12  49.45.4.85 (49.45.4.85)  304.485 ms  304.480 ms  304.475 ms
13  * 49.45.4.85 (49.45.4.85)  304.466 ms  304.461 ms
14  99.83.65.60 (99.83.65.60)  304.444 ms * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$
```

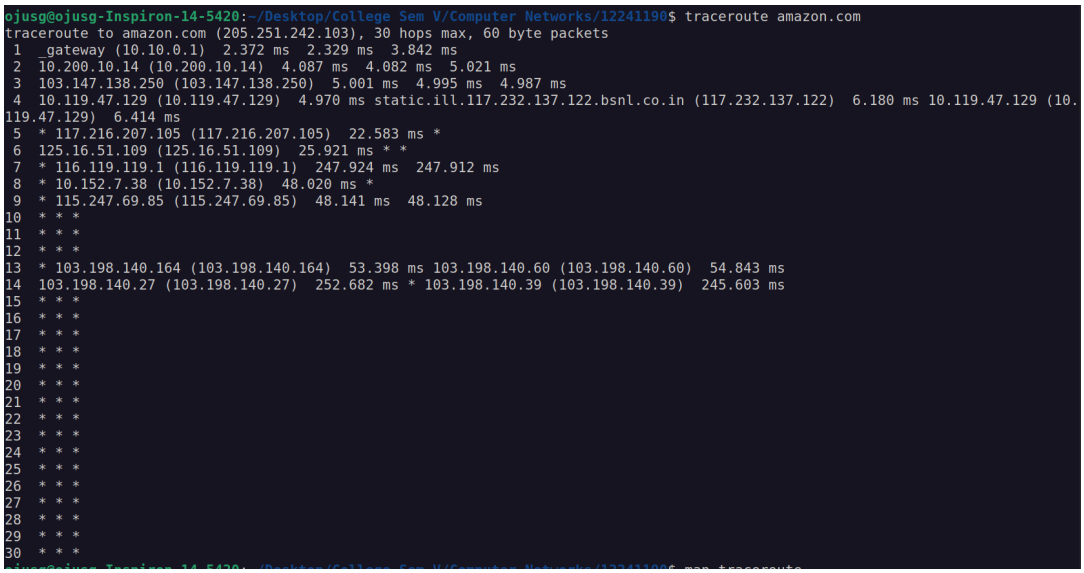
Traceroute to google.com




```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ traceroute google.com
traceroute to google.com (142.250.183.142), 30 hops max, 60 byte packets
 1  _gateway (10.10.0.1)  2.155 ms  2.338 ms  2.333 ms
 2  10.200.10.14 (10.200.10.14)  2.791 ms  2.786 ms  2.306 ms
 3  103.147.138.250 (103.147.138.250)  3.069 ms  2.269 ms  2.689 ms
 4  static.ill.117.232.137.122.bsnl.co.in (117.232.137.122)  4.020 ms  4.013 ms  4.008 ms
 5  117.216.207.105 (117.216.207.105)  22.225 ms  22.219 ms  20.123 ms
 6  72.14.197.4 (72.14.197.4)  21.571 ms  19.961 ms  22.894 ms
 7  * * *
 8  74.125.253.164 (74.125.253.164)  22.873 ms  22.854 ms 192.178.86.242 (192.178.86.242)  22.847 ms
 9  192.178.110.110 (192.178.110.110)  22.815 ms 142.250.214.113 (142.250.214.113)  22.811 ms 192.178.110.198 (192.178.110.198)
 25.992 ms
10  bom07s31-in-f14.1e100.net (142.250.183.142)  20.731 ms 142.250.209.71 (142.250.209.71)  20.376 ms bom07s31-in-f14.1e100.net
(142.250.183.142)  20.326 ms
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Network 241190$
```

Traceroute to amazon.com




ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ traceroute amazon.com
traceroute to amazon.com (205.251.242.103), 30 hops max, 60 byte packets
1 _gateway (10.10.0.1) 2.372 ms 2.329 ms 3.842 ms
2 10.200.10.14 (10.200.10.14) 4.087 ms 4.082 ms 5.021 ms
3 103.147.138.250 (103.147.138.250) 5.001 ms 4.995 ms 4.987 ms
4 10.119.47.129 (10.119.47.129) 4.970 ms static.ill.117.232.137.122.bsnl.co.in (117.232.137.122) 6.180 ms 10.119.47.129 (10.119.47.129) 6.414 ms
5 * 117.216.207.105 (117.216.207.105) 22.583 ms *
6 125.16.51.109 (125.16.51.109) 25.921 ms * *
7 * 116.119.119.1 (116.119.119.1) 247.924 ms 247.912 ms
8 * 10.152.7.38 (10.152.7.38) 48.020 ms *
9 * 115.247.69.85 (115.247.69.85) 48.141 ms 48.128 ms
10 * * *
11 * * *
12 * * *
13 * 103.198.140.164 (103.198.140.164) 53.398 ms 103.198.140.60 (103.198.140.60) 54.843 ms
14 103.198.140.27 (103.198.140.27) 252.682 ms * 103.198.140.39 (103.198.140.39) 245.603 ms
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *

Answer 4

1. (a) Nmap is Network Mapper. It is used to gather information about network hosts, services and potential vulnerabilities. It has following uses:
   i. **Host discovery**: It can identify hosts on a network by sending out packets.
   ii. **Security**: nmap can be used to detect known vulnerabilities in the network which can be done using nmap scripting engine (NSE).
   iii. **Port Scanning**: nmap can be used to detect open ports on a target host.
   iv. **Penetration testing**

2. (a) The following ports are open for iitbhilai.ac.in
   i. **Port 22/tcp** - It is used to provide ssh services. Ssh is a protocol used to securely log into systems and execute commands. Ssh encrypts communication between client and server.
   ii. **Port 80/tcp** - It is to provide http services. HTTP is a protocol used to provide web services and serve web pages over unencrypted connections.
   iii. **Port 443/tcp** - It is used to provide https services. Https is a secure version of http. It is used to provide secure connection and communication between web and server is encrypted using SSL/TLS.
   iv. **Port 5666/tcp** - It is used to provide nrpe(Nagios Remote Plugin Executor) services. It is used for monitoring services on remote hosts using Nagios monitoring system.

```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ nmap iitbhilai.ac.in
Starting Nmap 7.80 ( https://nmap.org ) at 2024-08-15 13:44 IST
Nmap scan report for iitbhilai.ac.in (192.168.10.115)
Host is up (0.0029s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
5666/tcp open  nrpe

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

Yes, we can identify the service version of services running on the host using nmap -sV.

```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ nmap -sV iitbhilai.ac.in
Starting Nmap 7.80 ( https://nmap.org ) at 2024-08-15 16:44 IST
Nmap scan report for iitbhilai.ac.in (192.168.10.115)
Host is up (0.0035s latency).
Not shown: 996 closed ports
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/ssl    Apache httpd (SSL-only mode)
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 15.45 seconds
```

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/ssl	Apache httpd (SSL-only mode)
5666/tcp	open	tcpwrapped	

Process for identifying service version of services: Nmap sends specially crafted packets to open ports and analyze responses. Nmap compares the responses with its database of service fingerprints. If a match is found, it identifies the service and its version. The results are displayed as output.

3. We can try to identify OS running on iitbhilai.ac.in using nmap. Nmap has a feature that uses TCP/IP stack fingerprinting to make educated guess about the OS.

   Steps to identify OS: We can try to identify the OS using the -O flag with nmap. When we use this option, nmap sends various probes with different flags and various TTL values to target hosts and analyze the responses. Different OS responds to these probes differently and nmap compares these responses against a database of known OS fingerprints. Based on the closest match, nmap guesses the OS.

We were not able to identify os for iitbhilai.ac.in. No exact OS matches for host: Nmap was not able to match TCP/IP fingerprint with any known operating system in its database. This might happen if the OS is customized, or if there are network security devices (like firewalls). Nmap could not definitely identify the OS, but it hints for a linux based OS.

```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ nmap -O iitbhilai.ac.in
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ sudo nmap -O iitbhilai.ac.in
[sudo] password for ojusg:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-08-15 16:57 IST
Nmap scan report for iitbhilai.ac.in (192.168.10.115)
Host is up (0.0034s latency).
Not shown: 996 closed ports
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=7.80%E=4%D=8/15%OT=22%CT=1%CU=42414%PV=Y%DS=3%DC=I%G=Y%TM=66BDE62
OS:6%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=10E%TI=Z%II=I%TS=A)SEQ(SP=1
OS:08%GCD=1%ISR=10E%TI=Z%TS=A)OPS(O1=M4E2ST11NW7%O2=M4E2ST11NW7%O3=M4E2NNT1
OS:1NW7%O4=M4E2ST11NW7%O5=M4E2ST11NW7%O6=M4E2ST11)WIN(W1=7120%W2=7120%W3=71
OS:20%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M4E2NNSNW7%CC=Y%Q=
OS:)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y
OS:%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=16
OS:4%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 13.29 seconds
```

4. **google.com**

```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ nmap google.com
Starting Nmap 7.80 ( https://nmap.org ) at 2024-08-15 17:15 IST
Nmap scan report for google.com (142.250.183.142)
Host is up (0.021s latency).
Other addresses for google.com (not scanned): 2404:6800:4009:824::200e
rDNS record for 142.250.183.142: bom07s31-in-f14.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 4.23 seconds
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ nmap -sV google.com
Starting Nmap 7.80 ( https://nmap.org ) at 2024-08-15 17:15 IST
Nmap scan report for google.com (142.250.183.142)
Host is up (0.022s latency).
Other addresses for google.com (not scanned): 2404:6800:4009:824::200e
rDNS record for 142.250.183.142: bom07s31-in-f14.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE   VERSION
80/tcp  open  http      gws
443/tcp open  ssl/https gws
```

```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ sudo nmap -O google.com
Starting Nmap 7.80 ( https://nmap.org ) at 2024-08-15 17:57 IST
Nmap scan report for google.com (142.250.183.142)
Host is up (0.021s latency).
Other addresses for google.com (not scanned): 2404:6800:4009:824::200e
rDNS record for 142.250.183.142: bom07s31-in-f14.1e100.net
Not shown: 998 filtered ports
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 8.73 seconds
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$
```

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	gws
443/tcp	open	ssl/ssl	gws

Usage for http and ssl/ssl is the same as above.

OS detection for google.com failed.To detect at least 1 open and 1 closed port are required. The output shows that we have 2 closed ports and 998 filtered ports. FIltered ports means that these ports are not accessible due to firewall rules that prevent nmap from determining their state.

bbc.co.uk

```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ nmap bbc.co.uk
Starting Nmap 7.80 ( https://nmap.org ) at 2024-08-15 18:27 IST
Nmap scan report for bbc.co.uk (151.101.192.81)
Host is up (0.022s latency).
Other addresses for bbc.co.uk (not scanned): 151.101.128.81 151.101.64.81 151.101.0.81 2a04:4e42:600::81 2a04:4e42::81 2a04:4e42
:400::81 2a04:4e42:200::81
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.09 seconds
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ nmap -sV bbc.co.uk
Starting Nmap 7.80 ( https://nmap.org ) at 2024-08-15 18:27 IST
Nmap scan report for bbc.co.uk (151.101.192.81)
Host is up (0.025s latency).
Other addresses for bbc.co.uk (not scanned): 151.101.128.81 151.101.64.81 151.101.0.81 2a04:4e42::81 2a04:4e42:200::81 2a04:4e42
:400::81 2a04:4e42:600::81
Not shown: 998 filtered ports
PORT    STATE SERVICE   VERSION
80/tcp  open  http      Varnish
443/tcp open  ssl/https Varnish
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at htt
ps://nmap.org/cgi-bin/submit.cgi?new-service :
```

```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ sudo nmap -O bbc.co.uk
[sudo] password for ojusg:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-08-15 18:29 IST
Nmap scan report for bbc.co.uk (151.101.128.81)
Host is up (0.023s latency).
Other addresses for bbc.co.uk (not scanned): 151.101.0.81 151.101.64.81 151.101.192.81 2a04:4e42:600::81 2a04:4e42:200::81 2a04:
4e42::81 2a04:4e42:400::81
Not shown: 998 filtered ports
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): FreeBSD 8.X|6.X (88%), Linux 2.6.X (86%), OpenBSD 4.X (86%)
OS CPE: cpe:/o:freebsd:freebsd:8.2 cpe:/o:linux:linux_kernel:2.6 cpe:/o:freebsd:freebsd:6.1 cpe:/o:openbsd:openbsd:4.0
Aggressive OS guesses: FreeBSD 8.2-RELEASE (88%), Linux 2.6.18 - 2.6.22 (86%), FreeBSD 6.1-RELEASE (86%), 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 8.67 seconds
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$
```

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Varnish
443/tcp	open	ssl/https	Varnish

Usage for http and ssl/https is the same as above.

The results suggest that bbc.co.uk might be running FreeBSD, Linux or OpenBSD with following probabilities.

FreeBSD 8.X—6.X (88%)

Linux 2.6.X (86%)

OpenBSD 4.X (86%)

Exact OS could not be predicted because nmap required at least 1 closed and 1 open port. Again we had 2 open ports and 998 filtered ports. For accurate OS fingerprinting, Nmap needs to compare behaviour of both open and closed ports.

Although both google.com and bbc.co.uk have the same number of open and filtered ports, still we got some idea of os used by bbc but not by google. This may be because of differences in security measures, server configuration, and level of customization in operating systems. Google's infrastructure may be more optimised to prevent such detections.

Answer 5

1. Netstat is a versatile networking utility used for troubleshooting, and configuration, that is also used as a monitoring tool for connections over the network. It also provides information about network connections, routing tables, interface statistics and more.

```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 ojusg-Inspiron-14:41712 20.198.119.143:https    ESTABLISHED
tcp        0      0 ojusg-Inspiron-14:47672 13.107.42.16:https      ESTABLISHED
tcp        0      0 ojusg-Inspiron-14:37602 91.108.23.100:https     ESTABLISHED
tcp        0      0 ojusg-Inspiron-14:44018 server-3-164-36-4:https TIME_WAIT
tcp        0      0 ojusg-Inspiron-14:50738 93.243.107.34.bc.:https ESTABLISHED
tcp        0      0 ojusg-Inspiron-14:37554 91.108.23.100:https     ESTABLISHED
tcp        0      0 ojusg-Inspiron-14:36628 104.18.32.47:https      TIME_WAIT
tcp        0      0 ojusg-Inspiron-14:58640 sh-in-f188.1e100.n:5228 ESTABLISHED
tcp        0      0 ojusg-Inspiron-14:37588 91.108.23.100:https     ESTABLISHED
tcp        0      0 ojusg-Inspiron-14:37562 91.108.23.100:https     ESTABLISHED
tcp        0      0 ojusg-Inspiron-14:55942 a184-27-197-74.de:https ESTABLISHED
tcp        0      0 ojusg-Inspiron-14:37580 91.108.23.100:https     ESTABLISHED
tcp        0      0 ojusg-Inspiron-14:37570 91.108.23.100:https     ESTABLISHED
tcp        0      0 ojusg-Inspiron-14:58630 sh-in-f188.1e100.n:5228 ESTABLISHED
tcp        0      0 ojusg-Inspiron-14:60586 91.108.56.153:https     ESTABLISHED
tcp        0      0 ojusg-Inspiron-14:42800 172.64.155.209:https    ESTABLISHED
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$
```

2. Trying to identify ports and PIDs of my web browser (Chrome):

```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ netstat -tnp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 10.10.3.24:46618        3.164.36.5:443          ESTABLISHED 3756/chrome --type=
tcp        0      0 10.10.3.24:37602        91.108.23.100:443       ESTABLISHED 9617/telegram-deskt
tcp        0      0 10.10.3.24:34834        172.64.155.209:443      ESTABLISHED 3756/chrome --type=
tcp        0      0 10.10.3.24:50738        34.107.243.93:443       ESTABLISHED 122233/firefox
tcp        0      0 10.10.3.24:37554        91.108.23.100:443       ESTABLISHED 9617/telegram-deskt
tcp        0      0 10.10.3.24:58640        142.251.175.188:5228    ESTABLISHED 3756/chrome --type=
tcp        0      0 10.10.3.24:37588        91.108.23.100:443       ESTABLISHED 9617/telegram-deskt
tcp        0      0 10.10.3.24:46124        172.217.167.166:443     ESTABLISHED 3756/chrome --type=
tcp        0      0 10.10.3.24:37580        91.108.23.100:443       ESTABLISHED 9617/telegram-deskt
tcp        0      0 10.10.3.24:37570        91.108.23.100:443       ESTABLISHED 9617/telegram-deskt
tcp        0      0 10.10.3.24:58630        142.251.175.188:5228    ESTABLISHED 3756/chrome --type=
tcp        0      0 10.10.3.24:32956        91.108.23.100:443       ESTABLISHED 9617/telegram-deskt
tcp        0      0 10.10.3.24:52190        20.198.118.190:443      ESTABLISHED 5894/msedge --type=
tcp        0      0 10.10.3.24:60586        91.108.56.153:443       ESTABLISHED 9617/telegram-deskt
tcp        0      0 10.10.3.24:42800        172.64.155.209:443      ESTABLISHED 3756/chrome --type=
```

```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ netstat -tnp | grep chrome
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 10.10.3.24:56488        3.164.36.58:443         ESTABLISHED 3756/chrome --type=
tcp        0      0 10.10.3.24:34834        172.64.155.209:443      ESTABLISHED 3756/chrome --type=
tcp        0      0 10.10.3.24:41634        172.67.6.190:443        ESTABLISHED 3756/chrome --type=
tcp        0      0 10.10.3.24:58640        142.251.175.188:5228    ESTABLISHED 3756/chrome --type=
tcp        0      0 10.10.3.24:55876        142.250.183.165:443     ESTABLISHED 3756/chrome --type=
tcp        0      0 10.10.3.24:58630        142.251.175.188:5228    ESTABLISHED 3756/chrome --type=
tcp       64      0 10.10.3.24:35500        52.1.16.29:443          CLOSE_WAIT  3756/chrome --type=
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$
```

Finding out if any of the services running in my system use the standard ports of HTTP, DHCP, DNS, SMTP, and FTP.

(a) HTTP: 80
(b) HTTPS: 443
(c) DHCP: 67 (server), 68 (client)
(d) DNS: 53
(e) SMTP: 25
(f) FTP: 21

```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ netstat -tuln | grep -E ':80|:443|:67|:68|:53|:
25|:21'
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
udp        0      0 224.0.0.251:5353        0.0.0.0:*
udp        0      0 224.0.0.251:5353        0.0.0.0:*
udp        0      0 224.0.0.251:5353        0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp        0      0 0.0.0.0:53680           0.0.0.0:*
udp6       0      0 :::5353                 :::*
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$
```

```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ netstat -n | grep -E ':80|:443|:67|:68|:53|:25|
:21'
tcp        0      0 10.10.3.24:35004        104.18.87.42:443        ESTABLISHED
tcp        0      0 10.10.3.24:44790        172.217.166.46:443      ESTABLISHED
tcp        0      0 10.10.3.24:43132        20.198.119.143:443      ESTABLISHED
tcp        0      0 10.10.3.24:46436        54.182.0.31:443         ESTABLISHED
tcp        0      0 10.10.3.24:44346        172.217.27.195:443      ESTABLISHED
tcp        0      0 10.10.3.24:37602        91.108.23.100:443       ESTABLISHED
tcp        0      0 10.10.3.24:57376        216.239.32.116:443      ESTABLISHED
tcp        0      0 10.10.3.24:42352        3.164.36.55:443         ESTABLISHED
tcp        0      0 10.10.3.24:35266        104.16.142.237:443      ESTABLISHED
tcp        0      0 10.10.3.24:50738        34.107.243.93:443       ESTABLISHED
tcp        0      0 10.10.3.24:37554        91.108.23.100:443       ESTABLISHED
tcp        0      0 10.10.3.24:55700        142.250.183.165:443     ESTABLISHED
tcp        0      0 10.10.3.24:54910        34.120.83.142:443       ESTABLISHED
tcp        0      0 10.10.3.24:37588        91.108.23.100:443       ESTABLISHED
tcp        0      0 10.10.3.24:37580        91.108.23.100:443       ESTABLISHED
tcp        0      0 10.10.3.24:37570        91.108.23.100:443       ESTABLISHED
tcp        0      0 10.10.3.24:48530        108.158.61.3:443        TIME_WAIT
tcp        0      0 10.10.3.24:32956        91.108.23.100:443       ESTABLISHED
tcp        0      0 10.10.3.24:53434        172.217.27.195:443      ESTABLISHED
tcp        0      0 10.10.3.24:60586        91.108.56.153:443       ESTABLISHED
tcp        0      0 10.10.3.24:60700        142.250.67.138:443      TIME_WAIT
udp        0      0 10.10.3.24:46033        34.120.83.142:443       ESTABLISHED
udp        0      0 10.10.3.24:46528        216.239.32.116:443      ESTABLISHED
udp        0      0 10.10.3.24:68           10.200.10.250:67        ESTABLISHED
udp        0      0 10.10.3.24:49490        142.250.70.67:443       ESTABLISHED
udp        0      0 10.10.3.24:41723        142.250.70.110:443      ESTABLISHED
udp        0      0 10.10.3.24:34505        172.217.27.195:443      ESTABLISHED
udp        0      0 10.10.3.24:52844        142.250.67.174:443      ESTABLISHED
udp        0      0 10.10.3.24:53304        216.239.32.116:443      ESTABLISHED
udp        0      0 10.10.3.24:36924        142.250.77.42:443       ESTABLISHED
udp        0      0 10.10.3.24:53714        142.250.183.170:443     ESTABLISHED
```

3. netstat -su

```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College Sem V/Computer Networks/12241190$ netstat -su
IcmpMsg:
    InType0: 306
    InType3: 2145
    InType8: 27
    InType11: 197
    InType14: 2
    OutType0: 27
    OutType3: 3142
    OutType5: 28
    OutType8: 678
    OutType13: 4
Udp:
    1074287 packets received
    2230 packets to unknown port received
    20316 packet receive errors
    681875 packets sent
    20316 receive buffer errors
    125 send buffer errors
    IgnoredMulti: 6
UdpLite:
IpExt:
    InNoRoutes: 43
    InMcastPkts: 2631
    OutMcastPkts: 9145
    InBcastPkts: 6
    OutBcastPkts: 6
    InOctets: 2914685704
    OutOctets: 413166931
    InMcastOctets: 343258
    OutMcastOctets: 1642121
    InBcastOctets: 468
    OutBcastOctets: 468
    InNoECTPkts: 2999236
    InECT0Pkts: 152
MPTcpExt:
```