Assignment 1

Task 1

(i) ping www.google.com - Ping is used to verify the connectivity & reachability to the particular domain (www.google.com here) or IP Address of the system hosting this domain. It gives the round-trip time(rtt) for messages sent from the originating host to a destination computer that are echoed back to the source. It also gives min,average and max rtt. The output is as follows :

```
paru04@LAPTOP-NVGR5VB8:~$ ping www.google.com
PING www.google.com (142.250.182.132) 56(84) bytes of data.
64 bytes from maa05s22-in-f4.1e100.net (142.250.182.132): icmp_seq=1 ttl=117 time=15.5 ms
64 bytes from maa05s22-in-f4.1e100.net (142.250.182.132): icmp_seq=2 ttl=117 time=16.4 ms
64 bytes from maa05s22-in-f4.1e100.net (142.250.182.132): icmp_seq=3 ttl=117 time=21.8 ms
64 bytes from maa05s22-in-f4.1e100.net (142.250.182.132): icmp_seq=4 ttl=117 time=35.2 ms
64 bytes from maa05s22-in-f4.1e100.net (142.250.182.132): icmp_seq=5 ttl=117 time=18.1 ms
64 bytes from maa05s22-in-f4.1e100.net (142.250.182.132): icmp_seq=6 ttl=117 time=18.3 ms
64 bytes from maa05s22-in-f4.1e100.net (142.250.182.132): icmp_seq=7 ttl=117 time=15.8 ms
64 bytes from maa05s22-in-f4.1e100.net (142.250.182.132): icmp_seq=8 ttl=117 time=15.7 ms
64 bytes from maa05s22-in-f4.1e100.net (142.250.182.132): icmp_seq=9 ttl=117 time=15.1 ms
64 bytes from maa05s22-in-f4.1e100.net (142.250.182.132): icmp_seq=10 ttl=117 time=20.6 ms
64 bytes from maa05s22-in-f4.1e100.net (142.250.182.132): icmp_seq=11 ttl=117 time=18.0 ms
64 bytes from maa05s22-in-f4.1e100.net (142.250.182.132): icmp_seq=12 ttl=117 time=16.5 ms
64 bytes from maa05s22-in-f4.1e100.net (142.250.182.132): icmp_seq=13 ttl=117 time=20.8 ms
64 bytes from maa05s22-in-f4.1e100.net (142.250.182.132): icmp_seq=14 ttl=117 time=22.4 ms
64 bytes from maa05s22-in-f4.1e100.net (142.250.182.132): icmp_seq=15 ttl=117 time=16.0 ms
^C
--- www.google.com ping statistics ---
15 packets transmitted, 15 received, 0% packet loss, time 14025ms
rtt min/avg/max/mdev = 15.070/19.092/35.182/4.895 ms
```

(ii) traceroute www.google.com - It prints the route that a packet takes to reach the host (host for the domain "www.google.com" here). The output is as follows :

```
paru04@LAPTOP-NVGR5VB8: $ traceroute www.google.com
traceroute to www.google.com (142.250.70.68), 30 hops max, 60 byte packets
 1  LAPTOP-NVGR5VB8.mshome.net (172.23.208.1)  1.021 ms  0.931 ms  1.268 ms
 2  10.240.122.2 (10.240.122.2)  3.425 ms  3.410 ms  3.392 ms
 3  10.240.0.1 (10.240.0.1)  3.376 ms  3.366 ms  3.354 ms
 4  10.240.240.1 (10.240.240.1)  7.410 ms  6.370 ms  7.390 ms
 5  103.120.31.121.static-chennai.powertel.in (103.120.31.121)  16.347 ms  16.337 ms  16.322 ms
 6  103.120.29.73.static-delhi.powertel.in (103.120.29.73)  17.763 ms  16.529 ms  16.506 ms
 7  103.120.29.72.static-delhi.powertel.in (103.120.29.72)  28.171 ms  16.300 ms  16.268 ms
 8  72.14.209.113 (72.14.209.113)  15.133 ms  15.123 ms  15.114 ms
 9  108.170.253.119 (108.170.253.119)  16.314 ms 108.170.253.105 (108.170.253.105)  27.547 ms 74.125.242.130 (74.125.242.130
)  15.834 ms
10  142.250.238.182 (142.250.238.182)  33.758 ms 142.250.56.38 (142.250.56.38)  40.223 ms  37.625 ms
11  142.250.226.135 (142.250.226.135)  34.733 ms 72.14.232.50 (72.14.232.50)  32.662 ms 108.170.248.193 (108.170.248.193)  3
2.656 ms
12  192.178.86.203 (192.178.86.203)  37.597 ms  38.857 ms  50.366 ms
13  pnbomb-ab-in-f4.1e100.net (142.250.70.68)  32.236 ms 192.178.86.201 (192.178.86.201)  37.694 ms pnbomb-ab-in-f4.1e100.ne
t (142.250.70.68)  43.844 ms
```

(iii) arp - It contains recently resolved MAC addresses of Internet Protocol (IP) hosts on the network. It displays and modifies the Internet-to-adapter address translation tables used by the Address in Networks and communication management. The output is as follows :

```
paru04@LAPTOP-NVGR5VB8:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
LAPTOP-NVGR5VB8.mshome.  ether   00:15:5d:0f:c1:7e   C                     eth0
```

(iv) ifconfig - It is used from the command line either to assign an address to a network interface or to configure or display the current network interface configuration information i.e. to view IP Address and Hardware / MAC address assigned to the interface. The output is as follows :

```
paru04@LAPTOP-NVGR5VB8:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.23.209.143  netmask 255.255.240.0  broadcast 172.23.223.255
        inet6 fe80::215:5dff:fe95:454e  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:95:45:4e  txqueuelen 1000  (Ethernet)
        RX packets 27964  bytes 35743281 (35.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3517  bytes 263751 (263.7 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 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
```

(v) hostname - It displays the name of the current host system. The output is as follows :

```
paru04@LAPTOP-NVGR5VB8:~$ hostname
LAPTOP-NVGR5VB8
```

(vi) /etc/hostname - This file configures/stores the name of the local Linux system(hostname) that is set during boot using the Linux kernel system call.

/etc/hosts - This file is an operating system file that matches a fully qualified domain name or hostname with the server IP hosting a specific domain i.e. translates them to an IP address.

/etc/resolv.conf - Lists nameservers that are used by your host for DNS resolution. If you are using DHCP, this file is automatically populated with the DNS record issued by the DHCP server.

/etc/protocols - This file contains information regarding the known protocol. It provides a name for a protocol seen in use or determines the protocol number for a user-specified protocol name.

/etc/services - This file contains a list of network services and ports mapped to them.

Task 2

(i) hostname - LAPTOP-NVGR5VB8, IP Address - 172.23.209.143
The above are obtained by using commands:
"$ hostname" to get hostname and "$ ifconfig" to get IP Address respectively

(ii) next hop router's IP address - 172.23.208.0 - using command "route"
MAC address - 00:15:5d:f9:97:81 - using command "arp"

(iii) DNS server's IP address - nameserver 172.23.208.1 - opening the file etc/resolv.conf

(iv) The numbers in the file /etc/protocols represent protocol numbers that identify the protocol in the layer above IP to which the data should be passed.

(v) The port number associated with applications:
ssh is 22
ftp is 20 / 21
nfs is 2049
smtp is 25 / 465
It is obtained using the command “grep <applicationname> /etc/services”
grep ssh /etc/services
grep ftp /etc/services
grep nfs /etc/services
grep smtp /etc/services respectively

(vi) The phone running on android/ios has hostname, IP address, MAC address, local DNS server's IP address, and ports for ssh, ftp, nfs(third-party app), smtp(third-party email apps) that are accessible to user, but doesn’t have next hop router's IP address and file /etc/protocols available.
So, we can answer only 3.5 of the above questions(i, iii, v and MAC address in ii) for a phone running on android/ios.

Task 3

(i)

(a) Output for “ping www.amazon.in” is as follows :

```
paru04@LAPTOP-NVGR5VB8:~$ ping www.amazon.in
PING www-amazon-in.customer.fastly.net (162.219.225.220) 56(84) bytes of data.
64 bytes from 162.219.225.220 (162.219.225.220): icmp_seq=1 ttl=54 time=16.6 ms
64 bytes from 162.219.225.220 (162.219.225.220): icmp_seq=2 ttl=54 time=19.0 ms
64 bytes from 162.219.225.220 (162.219.225.220): icmp_seq=3 ttl=54 time=17.8 ms
64 bytes from 162.219.225.220 (162.219.225.220): icmp_seq=4 ttl=54 time=17.8 ms
64 bytes from 162.219.225.220 (162.219.225.220): icmp_seq=5 ttl=54 time=17.3 ms
64 bytes from 162.219.225.220 (162.219.225.220): icmp_seq=6 ttl=54 time=18.9 ms
64 bytes from 162.219.225.220 (162.219.225.220): icmp_seq=7 ttl=54 time=18.1 ms
64 bytes from 162.219.225.220 (162.219.225.220): icmp_seq=8 ttl=54 time=17.2 ms
^C64 bytes from 162.219.225.220: icmp_seq=9 ttl=54 time=17.3 ms

--- www-amazon-in.customer.fastly.net ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8343ms
rtt min/avg/max/mdev = 16.633/17.780/19.013/0.757 ms
```

Here the ping command is executed successfully, that is, the system can reach the specified host(“www.amazon.in” here).

Output for “ping www.iitb.ac.in” is as follows :

Here the ping command failed to execute. In general the reasons can be various like network issues, firewalls, or the target server not responding. But here it is due to denial of service by the host (“www.iitb.ac.in” here)

```
paru04@LAPTOP-NVGR5VB8:~$ ping www.iitb.ac.in
PING www.iitb.ac.in (103.21.124.10) 56(84) bytes of data.
^C
--- www.iitb.ac.in ping statistics ---
34 packets transmitted, 0 received, 100% packet loss, time 34358ms
```

(b) The reasons for the values of RTTs
RTT (Round-Trip Time) values depend on the network distance and the responsiveness of the target server.
Short RTTs indicate a fast and responsive connection, while longer RTTs may suggest network congestion or server load.

(ii)
(a) The output obtained for the command “traceroute www.amazon.in“ is :

```
paru04@LAPTOP-NVGR5VB8: $ traceroute www.amazon.in
traceroute to www.amazon.in (23.50.253.98), 30 hops max, 60 byte packets
 1  LAPTOP-NVGR5VB8.mshome.net (172.23.208.1)  0.684 ms  0.637 ms  0.623 ms
 2  10.240.200.1 (10.240.200.1)  3.449 ms  3.438 ms  3.425 ms
 3  10.240.240.1 (10.240.240.1)  3.347 ms  3.337 ms  3.317 ms
 4  103.120.31.121.static-chennai.powertel.in (103.120.31.121)  21.202 ms  21.194 ms  21.184 ms
 5  103.120.29.73.static-delhi.powertel.in (103.120.29.73)  17.713 ms  17.701 ms  17.682 ms
 6  103.120.29.72.static-delhi.powertel.in (103.120.29.72)  17.920 ms  19.873 ms  19.852 ms
 7  115.247.148.69 (115.247.148.69)  19.820 ms  23.782 ms  23.760 ms
 8  172.16.92.147 (172.16.92.147)  56.279 ms  50.983 ms  56.269 ms
 9  172.16.92.147 (172.16.92.147)  50.974 ms 49.44.188.14 (49.44.188.14)  59.048 ms 172.16.92.147 (172.16.92.147)  73.599 ms10  * 49.
44.188.14 (49.44.188.14)  45.239 ms *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

Here it is executed successfully.
Hop 1 to 9:
The initial hops indicate the route from my local machine (LAPTOP-NVGR5VB8) through the local network and internet service provider (ISP). The RTT values show the time it takes for the packets to reach each hop.
Hops 10 to 30:
The subsequent hops show a series of asterisks, indicating that the traceroute is unable to reach the destination or receive responses beyond hop 10(i.e. the router at that hop doesn't

respond to the type of packet used for the traceroute here). This could be due to network configurations, firewalls, or other reasons.

Network Map:
My Machine (LAPTOP-NVGR5VB8) -> Local Network (172.23.208.1) -> ISP Network (10.240.200.1) -> ISP Network (10.240.240.1) -> ISP Network (103.120.31.121) -> ISP Network (103.120.29.73) -> ISP Network (103.120.29.72) -> ISP Network (115.247.148.69) -> ISP Network (172.16.92.147) -> ISP Network (49.44.188.14) -> …

(b) To change the maximum hop number we can use the command “traceroute -m <number> www.amazon.in” (<number> can be any natural number we wish to set the limit as).
Ex:

```
paru04@LAPTOP-NVGR5VB8: $ traceroute -m 25 www.amazon.in
traceroute to www.amazon.in (18.239.152.68), 25 hops max, 60 byte packets
 1  LAPTOP-NVGR5VB8.mshome.net (172.23.208.1)  0.595 ms  0.995 ms  0.596 ms
 2  10.240.200.1 (10.240.200.1)  3.735 ms  3.723 ms  3.716 ms
 3  10.240.240.1 (10.240.240.1)  3.750 ms  3.042 ms  3.732 ms
 4  103.120.31.121.static-chennai.powertel.in (103.120.31.121)  14.629 ms  14.622 ms  14.614 ms
 5  103.120.29.73.static-delhi.powertel.in (103.120.29.73)  18.277 ms  18.270 ms  18.262 ms
 6  103.120.29.72.static-delhi.powertel.in (103.120.29.72)  17.354 ms  33.516 ms  30.472 ms
 7  115.247.148.69 (115.247.148.69)  28.573 ms  28.016 ms  21.225 ms
 8  172.26.40.7 (172.26.40.7)  44.005 ms  43.976 ms  43.960 ms
 9  172.26.40.7 (172.26.40.7)  43.942 ms 99.83.67.30 (99.83.67.30)  45.743 ms  45.707 ms
10  52.95.64.121 (52.95.64.121)  53.855 ms 52.95.64.127 (52.95.64.127)  38.963 ms 52.95.67.249 (52.95.67.249)  38.957 ms
11  52.95.67.249 (52.95.67.249)  38.947 ms 52.95.64.125 (52.95.64.125)  40.997 ms 52.95.67.249 (52.95.67.249)  38.930 ms
12  52.95.66.53 (52.95.66.53)  38.921 ms 52.95.66.55 (52.95.66.55)  52.906 ms 52.95.66.187 (52.95.66.187)  38.102 ms
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
```

(c) The three timestamps represent the following :
First Timestamp: The time it takes for the probe packet to reach the destination hop (forward trip).
Second Timestamp: The time it takes for the probe packet to return from the destination hop to the machine (backward trip).
Third Timestamp: The total round-trip time (RTT), which is the sum of the forward and backward trip times.

(d) TTL is a field in ICMP packets used by traceroute.
It limits the lifespan of a packet. Each router decrements the TTL, and when it reaches zero, the router sends an ICMP Time Exceeded message back.
Packet TTL can also be useful in determining how long a packet has been in circulation, and allow the sender to receive information about a packet's path through the Internet. Each packet has a place where it stores a numerical value determining how much longer it should continue to move through the network.