CS 315 : Computer Networks Lab
Assignment - 1
Introduction to Networking Tools

Ayush Mallick
CS22BT008

Q1.i $ *ping www.google.com*

Sends packets to www.google.com to check connectivity and measure round trip time.
It displays the IP address of the server, measures the time taken by the packet to travel to and from the host, and summarizes the packet loss and latency information.

```
ayushm@ayushm-HP-Pavilion-x360-Convertible-14-cd0xxx:~$ ping www.google.com
PING www.google.com (142.250.193.164) 56(84) bytes of data.
64 bytes from maa05s26-in-f4.1e100.net (142.250.193.164): icmp_seq=1 ttl=116 time=145 ms
64 bytes from maa05s26-in-f4.1e100.net (142.250.193.164): icmp_seq=2 ttl=116 time=63.7 ms
64 bytes from maa05s26-in-f4.1e100.net (142.250.193.164): icmp_seq=3 ttl=116 time=210 ms
64 bytes from maa05s26-in-f4.1e100.net (142.250.193.164): icmp_seq=4 ttl=116 time=210 ms
64 bytes from maa05s26-in-f4.1e100.net (142.250.193.164): icmp_seq=5 ttl=116 time=130 ms
64 bytes from maa05s26-in-f4.1e100.net (142.250.193.164): icmp_seq=6 ttl=116 time=356 ms
64 bytes from maa05s26-in-f4.1e100.net (142.250.193.164): icmp_seq=7 ttl=116 time=235 ms
^C
--- www.google.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6011ms
rtt min/avg/max/mdev = 63.704/192.773/356.421/86.168 ms
```

Q1.ii $ *traceroute www.google.com*

Traces the route taken by packets to reach www.google.com, displaying the intermediate hops.
It lists all the IP addresses or hostnames of the routers between the system and www.google.com, along with the latency for each hop.

```
ayushm@ayushm-HP-Pavilion-x360-Convertible-14-cd0xxx:~$ traceroute www.google.com
traceroute to www.google.com (142.250.196.36), 30 hops max, 60 byte packets
 1  _gateway (10.200.240.2)  1.744 ms  1.966 ms  1.867 ms
 2  10.240.0.1 (10.240.0.1)  1.789 ms  1.717 ms  1.649 ms
 3  internet.iitdh.ac.in (10.240.240.1)  3.657 ms  3.574 ms  3.513 ms
 4  * * *
 5  * * *
 6  103.120.29.72.static-delhi.powertel.in (103.120.29.72)  30.987 ms  30.774 ms  30.530 ms
 7  72.14.209.113 (72.14.209.113)  30.640 ms  30.556 ms  30.481 ms
 8  142.251.54.79 (142.251.54.79)  32.730 ms  33.019 ms  32.937 ms
 9  142.251.55.29 (142.251.55.29)  32.298 ms 142.251.55.31 (142.251.55.31)  31.120 ms 142.251.55.29 (142.251.55.29)  32.883 ms
10  maa03s45-in-f4.1e100.net (142.250.196.36)  31.264 ms  31.372 ms  31.345 ms
```

Q1.iii $ *arp*

Displays the system's neighbour network cache in the form of an ARP(Address Resolution Protocol) table, which maps IP addresses to MAC addresses.
It lists all the active entries of devices on the network in the ARP table.

```
ayushm@ayushm-HP-Pavilion-x360-Convertible-14-cd0xxx:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   44:b6:be:0a:9a:f3   C                     wlo1
```

Q1.iv $ *ifconfig*

Displays the status of all the currently active network interfaces.

It lists the details about each network interface like IP address, subnet mask, broadcast address, MAC address, RX/TX packets, etc.

```
ayushm@ayushm-HP-Pavilion-x360-Convertible-14-cd0xxx:~$ ifconfig
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 5151  bytes 515036 (515.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5151  bytes 515036 (515.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.200.255.153  netmask 255.255.240.0  broadcast 10.200.255.255
        inet6 fe80::ffd0:a85f:6677:d0b  prefixlen 64  scopeid 0x20<link>
        ether 28:3a:4d:63:21:71  txqueuelen 1000  (Ethernet)
        RX packets 1844932  bytes 2645847537 (2.6 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 940311  bytes 121119394 (121.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Q1.v $ *hostname*

It displays the current hostname of the system.

```
ayushm@ayushm-HP-Pavilion-x360-Convertible-14-cd0xxx:~$ hostname
ayushm-HP-Pavilion-x360-Convertible-14-cd0xxx
```

Q1.vi

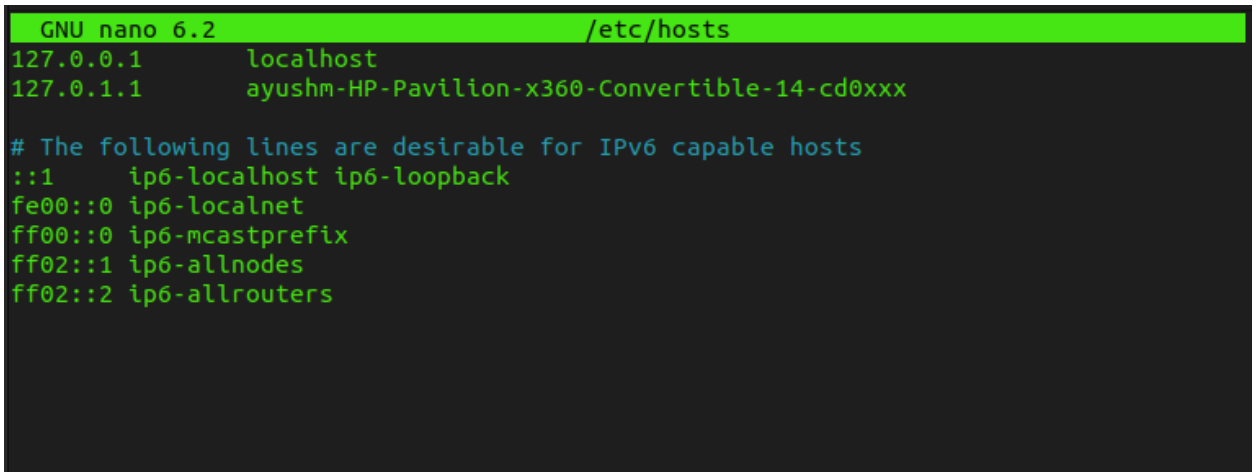
/etc/hostname

This file has a single line containing the system's hostname.

```
  GNU nano 6.2                  /etc/hostname
ayushm-HP-Pavilion-x360-Convertible-14-cd0xxx
```

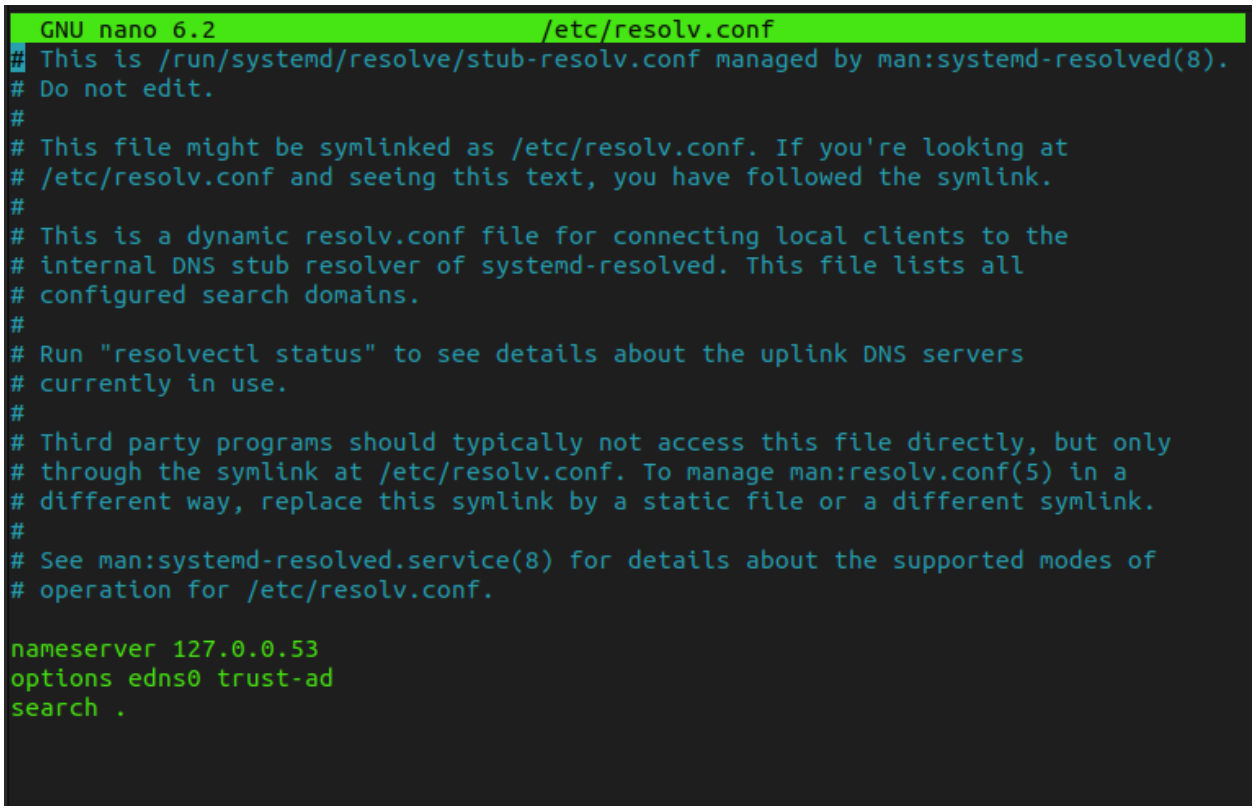
/etc/hosts

This file maps hostnames to IP addresses for local name resolution.



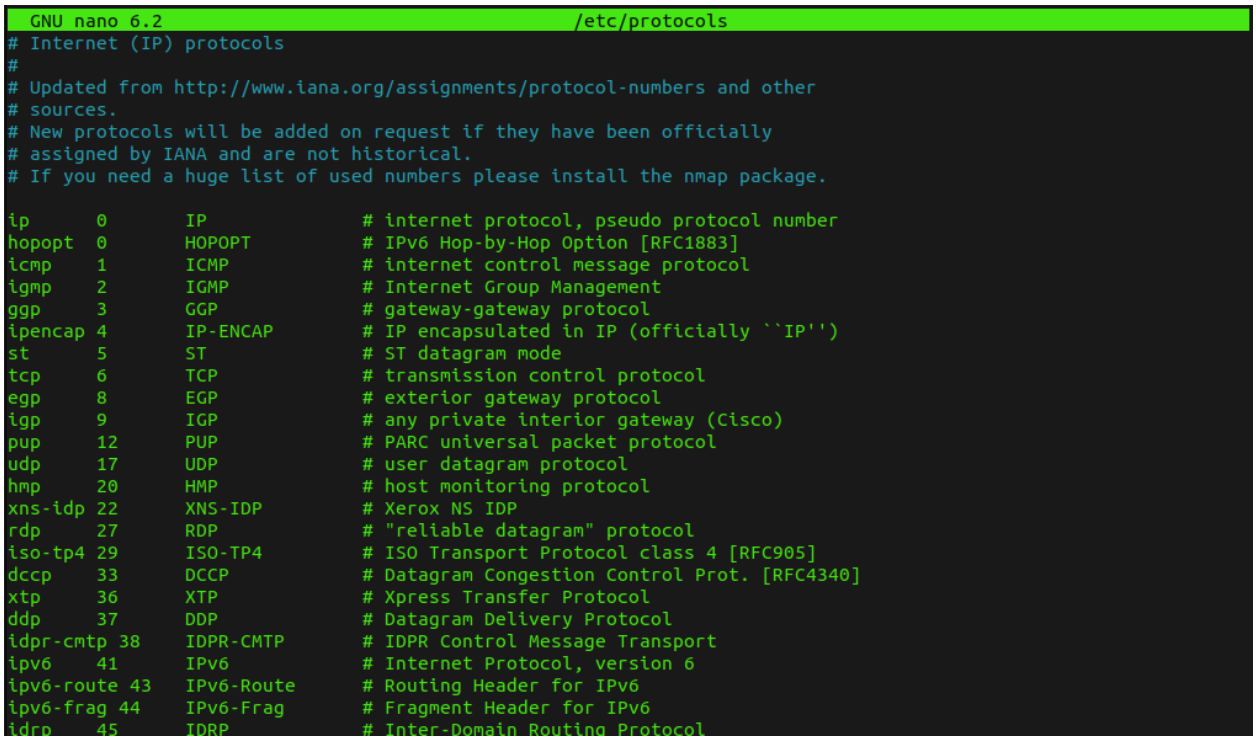
/etc/resolv.conf

This file configures DNS servers for domain name resolution.



/etc/protocols

This file lists network protocols with their respective numbers used by the operating system.

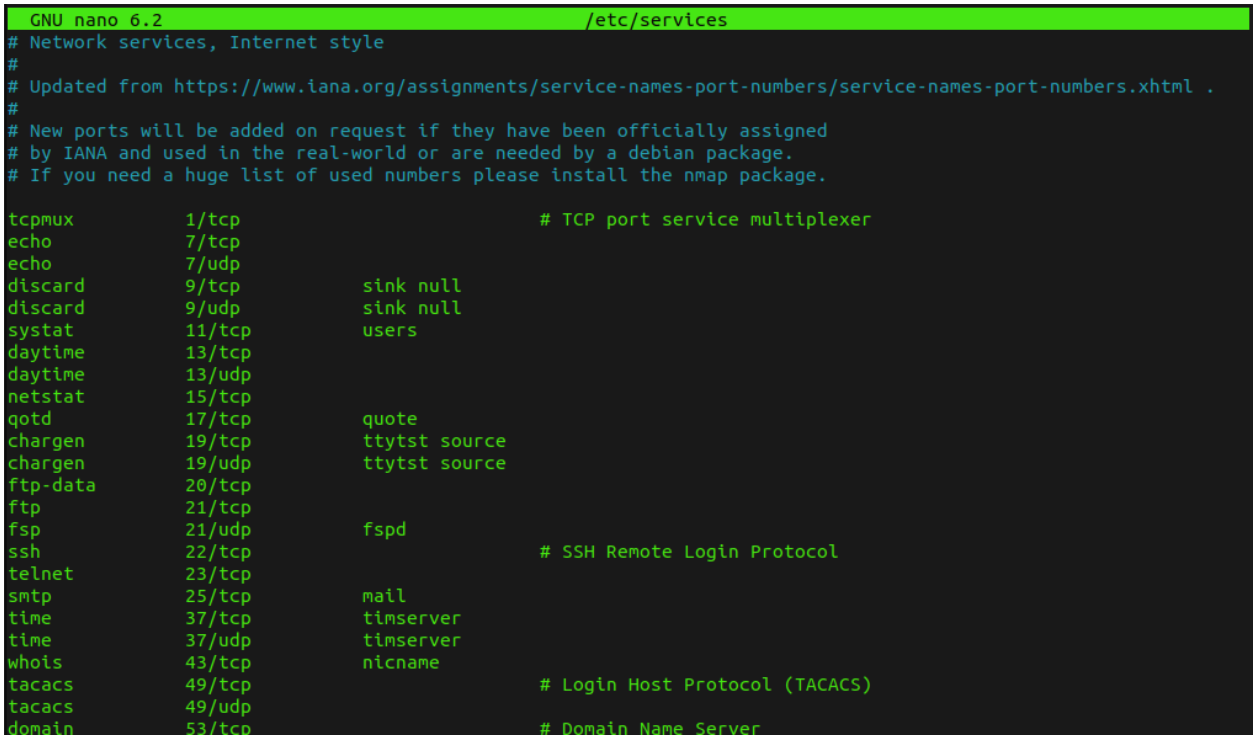


```
  GNU nano 6.2                                  /etc/protocols
# Internet (IP) protocols
#
# Updated from http://www.iana.org/assignments/protocol-numbers and other
# sources.
# New protocols will be added on request if they have been officially
# assigned by IANA and are not historical.
# If you need a huge list of used numbers please install the nmap package.

ip      0       IP              # internet protocol, pseudo protocol number
hopopt  0       HOPOPT          # IPv6 Hop-by-Hop Option [RFC1883]
icmp    1       ICMP            # internet control message protocol
igmp    2       IGMP            # Internet Group Management
ggp     3       GGP             # gateway-gateway protocol
ipencap 4       IP-ENCAP        # IP encapsulated in IP (officially ``IP'')
st      5       ST              # ST datagram mode
tcp     6       TCP             # transmission control protocol
egp     8       EGP             # exterior gateway protocol
igp     9       IGP             # any private interior gateway (Cisco)
pup     12      PUP             # PARC universal packet protocol
udp     17      UDP             # user datagram protocol
hmp     20      HMP             # host monitoring protocol
xns-idp 22      XNS-IDP         # Xerox NS IDP
rdp     27      RDP             # "reliable datagram" protocol
iso-tp4 29      ISO-TP4         # ISO Transport Protocol class 4 [RFC905]
dccp    33      DCCP            # Datagram Congestion Control Prot. [RFC4340]
xtp     36      XTP             # Xpress Transfer Protocol
ddp     37      DDP             # Datagram Delivery Protocol
idpr-cmtp 38    IDPR-CMTP       # IDPR Control Message Transport
ipv6    41      IPv6            # Internet Protocol, version 6
ipv6-route 43   IPv6-Route       # Routing Header for IPv6
ipv6-frag 44    IPv6-Frag       # Fragment Header for IPv6
idrp    45      IDRP            # Inter-Domain Routing Protocol
```

/etc/services

This file maps service names to their corresponding port numbers and protocols.



```
  GNU nano 6.2                                  /etc/services
# Network services, Internet style
#
# Updated from https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml .
#
# New ports will be added on request if they have been officially assigned
# by IANA and used in the real-world or are needed by a debian package.
# If you need a huge list of used numbers please install the nmap package.

tcpmux          1/tcp                           # TCP port service multiplexer
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp             21/tcp
fsp             21/udp          fspd
ssh             22/tcp                          # SSH Remote Login Protocol
telnet          23/tcp
smtp            25/tcp          mail
time            37/tcp          timserver
time            37/udp          timserver
whois           43/tcp          nicname
tacacs          49/tcp                          # Login Host Protocol (TACACS)
tacacs          49/udp
domain          53/tcp                          # Domain Name Server
```

Q2.i

Machine Hostname : *ayushm-HP-Pavilion-x360-Convertible-14-cd0xxx*
Machine IP address : *10.200.255.153*

The commands *hostname* and *ifconfig* were used to obtain the aforementioned information.

```
ayushm@ayushm-HP-Pavilion-x360-Convertible-14-cd0xxx:~$ hostname
ayushm-HP-Pavilion-x360-Convertible-14-cd0xxx
ayushm@ayushm-HP-Pavilion-x360-Convertible-14-cd0xxx:~$ ifconfig
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 5285  bytes 527378 (527.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5285  bytes 527378 (527.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.200.255.153  netmask 255.255.240.0  broadcast 10.200.255.255
        inet6 fe80::ffd0:a85f:6677:d0b  prefixlen 64  scopeid 0x20<link>
        ether 28:3a:4d:63:21:71  txqueuelen 1000  (Ethernet)
        RX packets 1848235  bytes 2646781405 (2.6 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 943841  bytes 124358559 (124.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Q2.ii

Next hop router IP address : *10.200.240.2*
Next hop router MAC address : *44:b6:be:0a:9a:f3*

The command *traceroute www.google.com* was used to find the IP address of the next hop router, then the MAC address of the router is obtained using the command *arp -a 10.200.240.2*.

```
ayushm@ayushm-HP-Pavilion-x360-Convertible-14-cd0xxx:~$ traceroute www.google.com
traceroute to www.google.com (142.250.195.100), 30 hops max, 60 byte packets
 1  _gateway (10.200.240.2)  1.922 ms  1.811 ms  1.753 ms
 2  10.240.0.1 (10.240.0.1)  1.458 ms  1.645 ms  1.589 ms
 3  internet.iitdh.ac.in (10.240.240.1)  3.356 ms  3.303 ms  3.075 ms
 4  * * *
 5  * * *
 6  103.120.29.72.static-delhi.powertel.in (103.120.29.72)  31.338 ms  30.836 ms  31.776 ms
 7  72.14.209.113 (72.14.209.113)  30.756 ms  30.406 ms  30.637 ms
 8  142.250.209.75 (142.250.209.75)  32.251 ms 142.251.54.79 (142.251.54.79)  31.397 ms  31.324 ms
 9  142.251.55.71 (142.251.55.71)  30.916 ms 142.251.55.69 (142.251.55.69)  43.788 ms  43.412 ms
10  maa03s39-in-f4.1e100.net (142.250.195.100)  37.037 ms  36.704 ms  36.798 ms
ayushm@ayushm-HP-Pavilion-x360-Convertible-14-cd0xxx:~$ arp -a 10.200.240.2
_gateway (10.200.240.2) at 44:b6:be:0a:9a:f3 [ether] on wlo1
```

Q2.iii

Local DNS server IP address : *127.0.0.53*

This information is present in the *resolv.conf* file, which can be accessed using the command *cat /etc/resolv.conf* or *nano /etc/resolv.conf*.

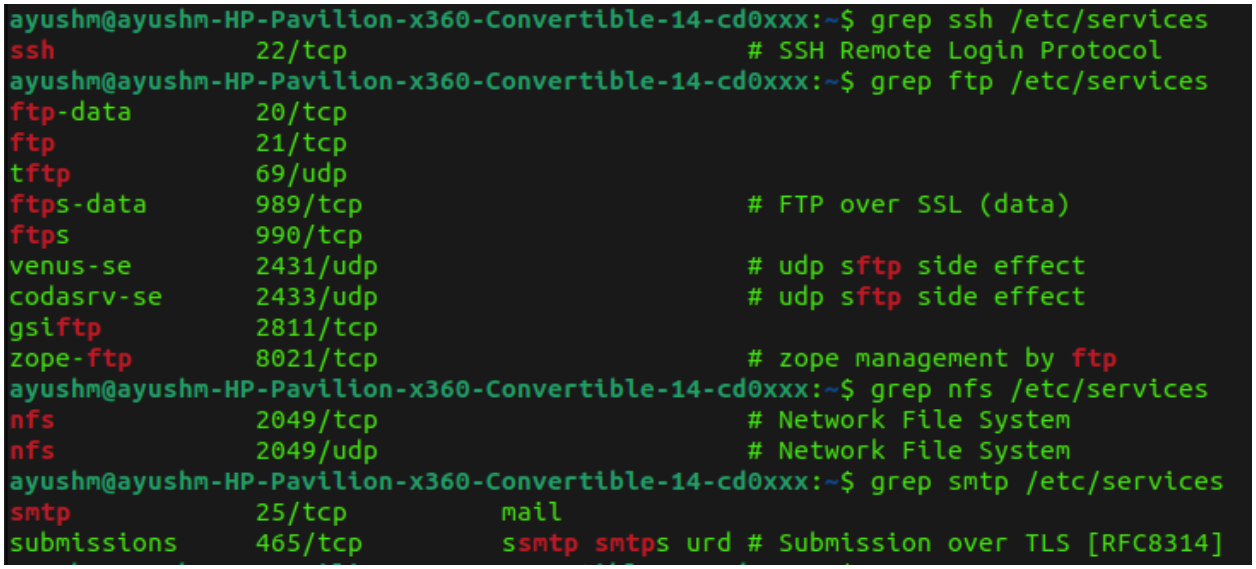
Q2.iv

Each number in the */etc/protocols* file represents a protocol's identification number used in the IP header's protocol field.

Q2.v

Port number for ssh : *22*
Port number for ftp : *21*
Port number for nfs : *2049*
Port number for smtp : *25*

This information can be obtained using the commands *grep ssh /etc/services*, *grep ftp /etc/services*, *grep nfs /etc/services*, and *grep smtp /etc/services* respectively.



Q2.vi

3 questions can be answered for the phone running on Android/iOS.
The client's IP address, MAC address, and local DNS server's IP address can be obtained.

Q3.i.a

www.amazon.in

Ping successful, with *0%* packet loss, and an average RTT of *89.498 ms*.

```
ayushm@ayushm-HP-Pavilion-x360-Convertible-14-cd0xxx:~$ ping www.amazon.in -c 7
PING d1elgm1ww0d6wo.cloudfront.net (52.84.204.232) 56(84) bytes of data.
64 bytes from server-52-84-204-232.blr50.r.cloudfront.net (52.84.204.232): icmp_seq=1 ttl=248 time=100 ms
64 bytes from server-52-84-204-232.blr50.r.cloudfront.net (52.84.204.232): icmp_seq=2 ttl=248 time=41.3 ms
64 bytes from server-52-84-204-232.blr50.r.cloudfront.net (52.84.204.232): icmp_seq=3 ttl=248 time=46.8 ms
64 bytes from server-52-84-204-232.blr50.r.cloudfront.net (52.84.204.232): icmp_seq=4 ttl=248 time=97.0 ms
64 bytes from server-52-84-204-232.blr50.r.cloudfront.net (52.84.204.232): icmp_seq=5 ttl=248 time=139 ms
64 bytes from server-52-84-204-232.blr50.r.cloudfront.net (52.84.204.232): icmp_seq=6 ttl=248 time=157 ms
64 bytes from server-52-84-204-232.blr50.r.cloudfront.net (52.84.204.232): icmp_seq=7 ttl=248 time=45.2 ms

--- d1elgm1ww0d6wo.cloudfront.net ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 8154ms
rtt min/avg/max/mdev = 41.339/89.498/156.863/43.508 ms
```

www.iitb.ac.in

Ping failed, probably due to firewall restrictions, or the target host blocking ICMP packets.

```
ayushm@ayushm-HP-Pavilion-x360-Convertible-14-cd0xxx:~$ ping www.iitb.ac.in -c 7
PING www.iitb.ac.in (103.21.124.133) 56(84) bytes of data.

--- www.iitb.ac.in ping statistics ---
7 packets transmitted, 0 received, 100% packet loss, time 6174ms
```

Q3.i.b

There can be multiple reasons for the different values of the round trip time (RTT) observed :

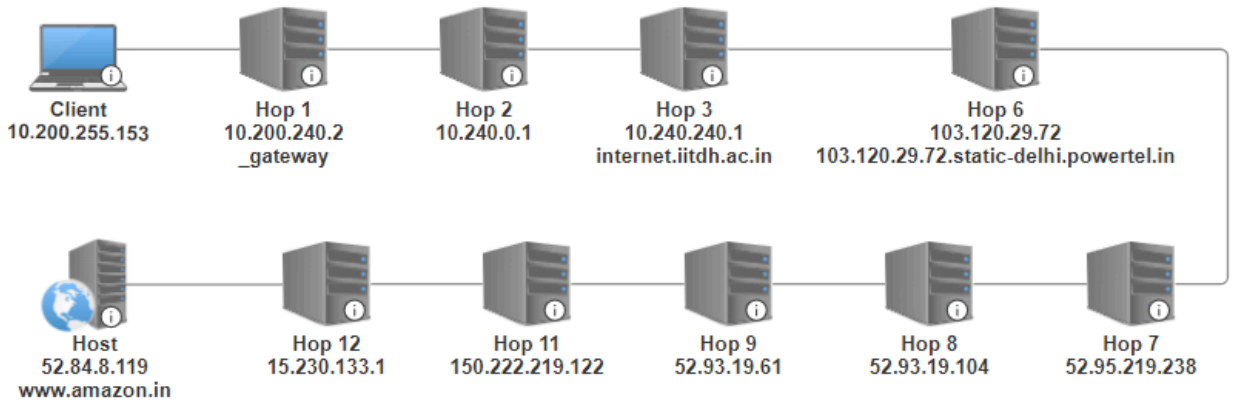
- Firewall policies of some servers deprioritize or block ICMP packets, causing timeouts.
- Busy servers with high loads may respond more slowly, increasing RTT.
- Servers geographically farther from the client location have higher RTT.
- The number of hops and quality of intermediate routers impact RTT.
- Increased network traffic and congestion can lead to higher RTT.

Q3.ii.a

Traceroute on www.amazon.in successfully completed in 18 hops.

```
ayushm@ayushm-HP-Pavilion-x360-Convertible-14-cd0xxx:~$ traceroute www.amazon.in
traceroute to www.amazon.in (52.84.8.199), 30 hops max, 60 byte packets
 1  _gateway (10.200.240.2)  2.137 ms  2.105 ms  2.070 ms
 2  10.240.0.1 (10.240.0.1)  1.542 ms  1.869 ms  1.835 ms
 3  internet.iitdh.ac.in (10.240.240.1)  9.908 ms  10.149 ms *
 4  * * *
 5  * * *
 6  * 103.120.29.72.static-delhi.powertel.in (103.120.29.72)  39.195 ms  44.702 ms
 7  52.95.219.238 (52.95.219.238)  40.840 ms  40.799 ms  40.385 ms
 8  52.93.19.104 (52.93.19.104)  39.441 ms 52.93.19.24 (52.93.19.24)  38.753 ms 52.93.19.56 (52.93.19.56)  39.658 ms
 9  52.93.19.61 (52.93.19.61)  67.323 ms 52.93.19.115 (52.93.19.115)  59.960 ms 52.93.19.99 (52.93.19.99)  53.270 ms
10  * * *
11  150.222.219.122 (150.222.219.122)  48.927 ms * *
12  15.230.133.1 (15.230.133.1)  101.557 ms 15.230.133.15 (15.230.133.15)  101.481 ms 15.230.133.9 (15.230.133.9)  101.433 ms
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  server-52-84-8-199.maa51.r.cloudfront.net (52.84.8.199)  100.880 ms  100.820 ms  100.771 ms
```

The network map, indicating the intermediate hops with sequential connections, is shown below. Only the responding routers are indicated in the map.



Q3.ii.b

The maximum hop number can be changed using the *-m* or *–max-hops* flag in the command.
Example : $ *traceroute -m 50 www.amazon.in*

Q3.ii.c

Each of the three timestamps in traceroute represents the time (in milliseconds) for three ICMP packets sent to the same hop, to measure variability in response times and detect delays.

Q3.ii.d

TTL (Time To Live) field in ICMP packets specifies the maximum number of hops a packet can traverse before being discarded, done to prevent infinite loops in routing.