Roll number: 214101020
Name: Harsh Bijwe

Question-1 Solution:

a) **The '-c' option** helps specify the number of echo requests to send with the ping command. Example: ping -c 5 www.google.com, defines 5 echo requests to send to the server.
b) **The '-i' option** helps to set the time interval rather than default 1 second. Example: ping -i 2 www.google.com, sets time interval to 2 seconds.
c) **The '-l' option** used in command sends ECHO_REQUEST packets to the destination one after another without waiting for a reply. Example: ping -l 3 www.google.com, sends 3 ECHO_REQUEST packets at same time without waiting for a reply. **Normal users can send at-most 3 such requests.**
d) **The '-s' option** is used to set ECHO_REQUEST packet size (in bytes). Example: ping -s 32 www.google.com, specify packet size of 32 Bytes. **Total size in Bytes = Packet-Size + Header-Size(Considering IPv4 and ICMP header) = 32+20+8 = 60 Bytes.**

Question-2 Solution:

Following are the hosts and their respective details:-

HOST_NAME	Region Of IP Address	Avg_RTT Morning	Packet Loss Morning	Avg_RTT Afternoon	Packet Loss Afternoon	Avg_RTT Evening	Packet Loss Evening
www.google.com	US, California	34.10	0%	33.65	0%	34.04	0%
www.amazon.com	Canada, Toronto	23.96	0%	23.57	0%	23.22	0%
www.flipkart.com	India, Banglore	206.585	0%	226.59	2%	225.87	0%
www.irctc.com	India, Delhi	NA	100%	NA	100%	NA	100%
www.onlinesbi.com	India, Mumbai	NA	100%	NA	100%	NA	100%
www.bbc.com	US, California	17.09	0%	17.91	0%	17.96	0%

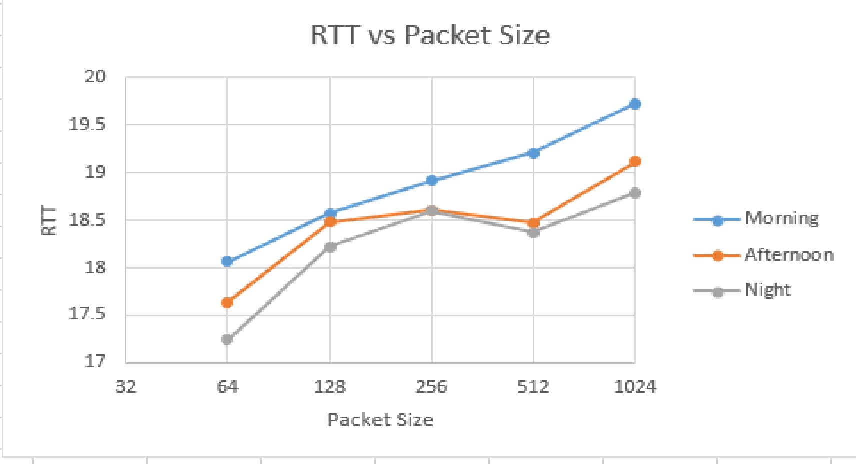
There are some cases where the packet loss is greater than 0%, even 100%. **The reason is:**

- **Firewall or the security devices at the destination is blocking the incoming ICMP Packets.**
- **The congestion in the network is very high due to which the buffer gets full and it discard some incoming packets.**

The measured RTTs are weakly correlated with the geographical distance of the hosts because we can see that the servers of google.com/amazon.com are located in the US but still we are getting less average RTT as compared to the host (www.flipkart.com) located in india.

For host, www.bbc.com following is the plot:-

Packet size	Morning	Noon	Night
64	18.06	17.64	17.24
128	18.57	18.48	18.22
256	18.92	18.61	18.6
512	19.21	18.47	18.37
1024	19.73	19.12	18.79



For packet size 2048 Bytes the packets were getting blocked at destination, so no RTT values. In Morning RTT values are higher than other times, reason being traffic on websites is generally more in morning.

Question-3 Solution:

a) **Ifconfig** command is used to configure the kernel-resident network interfaces. Also, this command is used to assign the IP address and netmask to an interface or to enable or disable a given interface. When I ran ifconfig on my pc, it showed:

   i. **enp0s3**
   ii. **lo**

enp0s3: The network interface name as a string. The “en” stands for ethernet, “p0” is the bus number of the ethernet card, and “s3” is the slot number. It has flag values <UP,BROADCAST,RUNNING,MULTICAST>. This interface supports broad- and multicasting, and the interface is UP (operational and connected). It also shows mtu(the maximum transfer unit this interface supports). netmask address, number of received packets, transmitted packets, dropped packets count. In my case, I’m connected to ethernet so that interface is being shown.

lo(loopback interface): It is used by the system to communicate with itself, hence its assigned ip addresses are loopback addresses where for ipv4 address is 127.0.0.1 and for ipv6. The address is : : 1.

b) Following are the options of ifconfig:

   i) **-a :** This option is used to display all the interfaces available, even if they are down.
   Syntax: **ifconfig -a**

   ii) **-v :** Run the command in verbose mode – log more details about execution.
   Syntax: **ifconfig -v**

iii) **add addr/prefixlen :** This option is used to add an IPv6 address to an interface.
Syntax: **ifconfig interface add addr/prefixlen**

iv) **del addr/prefixlen :** This option is used to remove an IPv6 address to an interface.
Syntax: **ifconfig interface del addr/prefixlen**

c) On typing **'route'** command we get:-

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref        Use Iface
default         _gateway        0.0.0.0         UG      100    0          0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U       100    0          0 enp0s3
link-local      0.0.0.0         255.255.0.0     U       1000  0           0 enp0s3
```

Destination: IP address of the destination network/host.
Gateway: Specifies the forwarding or next hop IP address over which the set of addresses defined by the network destination and subnet mask are reachable.
Genmask: This mask helps in finding the next hop or gateway by anding given ip address with genmask and if it matches with destination address in the table, it will forwarded to gateway accordingly which has a longest prefix match.
Flag: The U flag indicates that the route is up. The G flag indicates that the route is to a gateway.
Metric: A metric is a value that's assigned to an IP route for a particular network interface. It identifies the cost that's associated with using that route.
Ref: Number of references to this route.
Use: Count of the lookups.
Iface: Determines the next interface to where this packet is forwarding.

d) Following are the options in route command:

i) To add a default gateway.
Syntax: **sudo route add default gw 169.254.0.0**

Output:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref        Use Iface
default         169.254.0.0     0.0.0.0         UG      0      0          0 enp0s3
default         10.0.2.2        0.0.0.0         UG      100    0          0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U       100    0          0 enp0s3
link-local      0.0.0.0         255.255.0.0     U       1000  0           0 enp0s3
```

ii) To get details of the kernel/IP routing table using ip command.
Syntax: **ip route**

Output:

```
default via 169.254.0.0 dev enp0s3
default via 10.0.2.2 dev enp0s3 proto dhcp metric 20100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
169.254.0.0/16 dev enp0s3 scope link metric 1000
```

iii) To display a routing table in full numeric form.

Syntax: **route -n**

Output:

```
Kernel IP routing table
Destination    Gateway        Genmask        Flags Metric Ref       Use Iface
0.0.0.0        192.168.0.1    0.0.0.0        UG      0       0      0 enp0s3
0.0.0.0        10.0.2.2       0.0.0.0        UG      20100  0       0 enp0s3
10.0.2.0       0.0.0.0        255.255.255.0  U       100      0     0 enp0s3
169.254.0.0    0.0.0.0        255.255.0.0    U       1000   0       0 enp0s3
```

iv) To reject routing to a particular host or network.

Syntax: sudo route add -host 192.168.1.51 reject.

Now if you ping to the above-mentioned IP it will display:

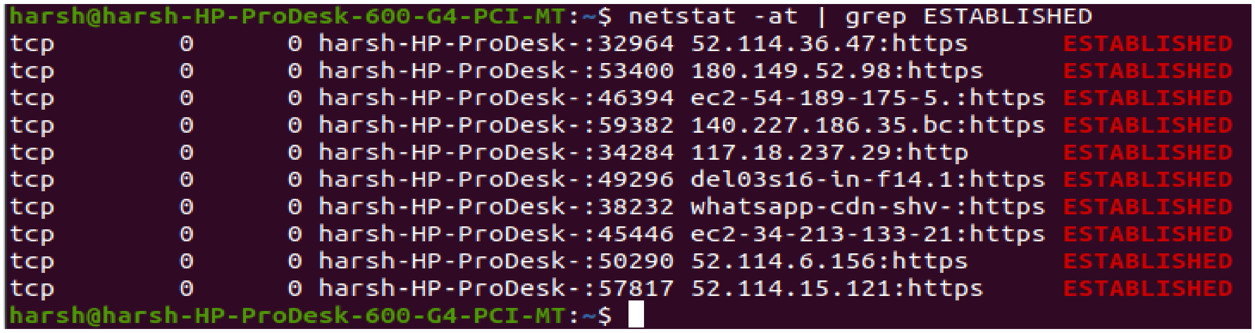
ping 192.168.1.51

ping: connect: No route to host.

Question-4 Solution:

a) **Netstat command** displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.

b) The command '**netstat -at | grep ESTABLISHED**' is used to show all the established TCP connections and the image of the output of this command is attached below-



```
harsh@harsh-HP-ProDesk-600-G4-PCI-MT:~$ netstat -at | grep ESTABLISHED
tcp        0      0 harsh-HP-ProDesk-:32964 52.114.36.47:https      ESTABLISHED
tcp        0      0 harsh-HP-ProDesk-:53400 180.149.52.98:https     ESTABLISHED
tcp        0      0 harsh-HP-ProDesk-:46394 ec2-54-189-175-5.:https ESTABLISHED
tcp        0      0 harsh-HP-ProDesk-:59382 140.227.186.35.bc:https ESTABLISHED
tcp        0      0 harsh-HP-ProDesk-:34284 117.18.237.29:http      ESTABLISHED
tcp        0      0 harsh-HP-ProDesk-:49296 del03s16-in-f14.1:https ESTABLISHED
tcp        0      0 harsh-HP-ProDesk-:38232 whatsapp-cdn-shv-:https ESTABLISHED
tcp        0      0 harsh-HP-ProDesk-:45446 ec2-34-213-133-21:https ESTABLISHED
tcp        0      0 harsh-HP-ProDesk-:50290 52.114.6.156:https      ESTABLISHED
tcp        0      0 harsh-HP-ProDesk-:57817 52.114.15.121:https     ESTABLISHED
harsh@harsh-HP-ProDesk-600-G4-PCI-MT:~$
```

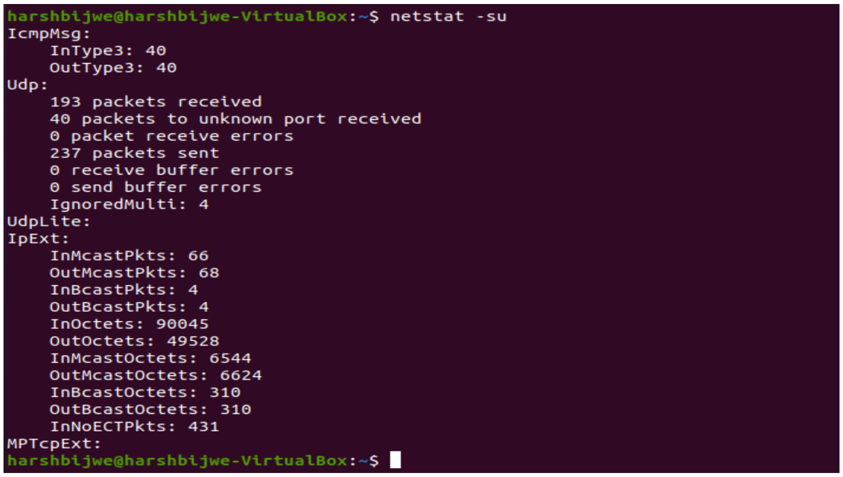
c) The command '**netstat -r**' is used to **get the kernel routing table information**. Some Important information provided by this command includes:-

- **Destination**: Identifies the destination network.
- **Gateway**: It shows the gateway to which the routing entry points. If no gateway is used, an asterisk is printed.
- **Genmask**: It represents the network mask for this route. When given an IP address to find a suitable route, the kernel steps through each of the routing table entries, taking the bitwise AND of the address and the genmask before comparing it to the target of the route.
- **Flags**: They describe the route ('G' means the route uses a gateway,'U' means the interface to be used is up,'H' means only a single host can be reached through the route).
- **MSS**:The MSS is the Maximum Segment Size, it is the size of the largest datagram the kernel will construct for transmission via this route.
- **Window**: The Window is the maximum amount of data the system will accept in a single burst from a remote host.

- **Irtt**: irtt stands for “initial round trip time”.The initial round-trip time is the value that the TCP protocol will use when a connection is first established.
- **Iface**: This field displays the network interface that this route will use.

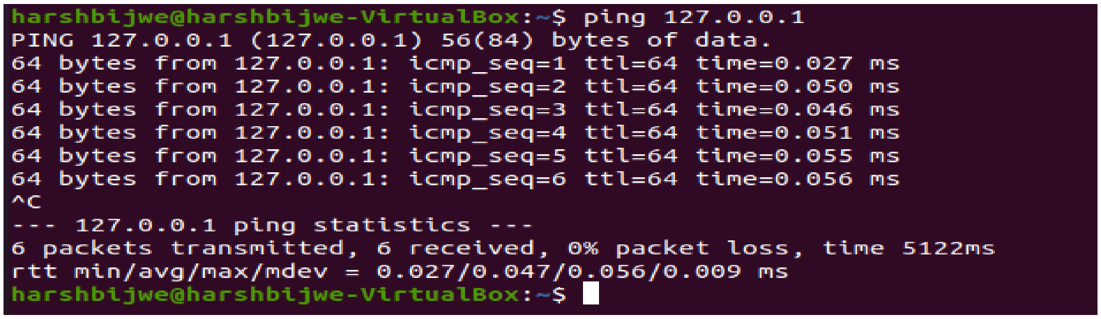
d) **Option ‘-i’** is used to display the status of all network interfaces.
Syntax: **netstat -i**
Using this command on my machine shows 2 Interfaces: Enp0s3 and lo.

e) **Option ‘-su’** is used to show the statistics of all UDP connections and the output of the this command is mentioned below-



```
harshbijwe@harshbijwe-VirtualBox:~$ netstat -su
IcmpMsg:
    InType3: 40
    OutType3: 40
Udp:
    193 packets received
    40 packets to unknown port received
    0 packet receive errors
    237 packets sent
    0 receive buffer errors
    0 send buffer errors
    IgnoredMulti: 4
UdpLite:
IpExt:
    InMcastPkts: 66
    OutMcastPkts: 68
    InBcastPkts: 4
    OutBcastPkts: 4
    InOctets: 90045
    OutOctets: 49528
    InMcastOctets: 6544
    OutMcastOctets: 6624
    InBcastOctets: 310
    OutBcastOctets: 310
    InNoECTPkts: 431
MPTcpExt:
harshbijwe@harshbijwe-VirtualBox:~$
```

f) The loopback device is a special, virtual network interface that your computer uses to **communicate with itself**. It is **used mainly for diagnostics and troubleshooting, and to connect to servers** running on the local machine.



```
harshbijwe@harshbijwe-VirtualBox:~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.027 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.050 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.046 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.051 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.055 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.056 ms
^C
--- 127.0.0.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5122ms
rtt min/avg/max/mdev = 0.027/0.047/0.056/0.009 ms
harshbijwe@harshbijwe-VirtualBox:~$
```

Question-5 Solution:

The 'traceroute’ command in Linux prints the route that a packet takes to reach the host. This command is useful when we want to know about the route and about all the hops that a packet takes.

a)

Host_name	Hop Count Morning	Hop Count Afternoon	Hop Count Evening
www.google.com	7	6	6

www.amazon.com	4	4	4
www.flipkart.com	10	10	10
www.irctc.com	10	10	10
www.onlinesbi.com	10	10	10
www.bbc.com	3	2	3

Common hops between routers observed: 45.79.12.201, 103.137.84.20, 95.2.3.53,103.68.221.190.

b) **Yes, in my case the route to some hosts changes at different times of the day** and the reason is, **some routers forward the data in different paths at different times due to the congestion/unavailability in one path** and this may cause the different route to any host.

c) **In my case (irctc.com/onlinesbi.com) does not provide the complete path at any time in a day.** The reason behind this is, **the firewall or other security component at the destination is blocking the UDP packets coming from the internet** and we do not get a response.

d) **Yes, it is possible to find the route to certain hosts which fail to respond** with the ping experiment. Since ping command use ICMP & 'traceroute' does not use ICMP on the unix based machine instead they use UDP packets with an incrementing TTL field to map the hops to the final destination. So if we try to "ping" a certain host there is a possibility that the system has blocked ICMP packets and in the case of the 'traceroute' system has not blocked UDP packets,so here ping fails but traceroute succeeds.

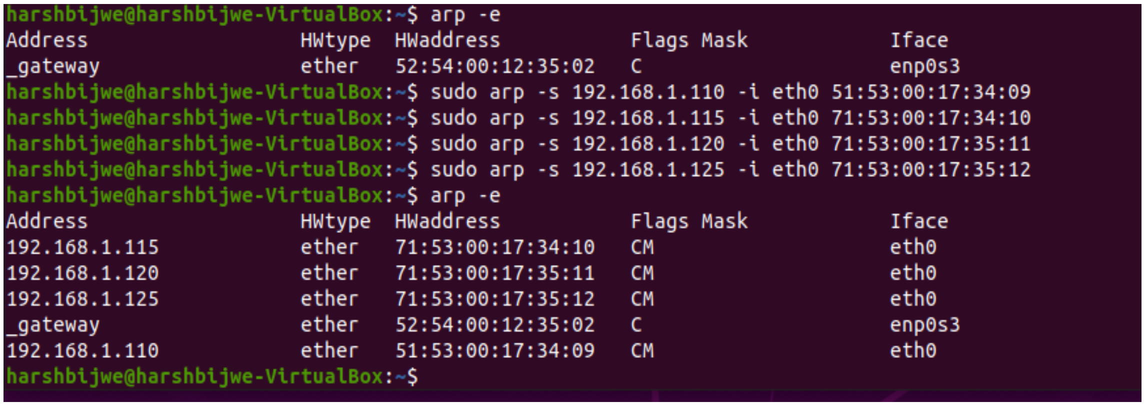
Question-6 Solution:

a) The command '**arp -e**' shows the full ARP table for our machine. And the output of this command consists of following-

- **Address** shows IP address which is associated with the MAC-address.
- **Hwtype** shows the type of hardware with which the MAC address is associated.
- **HWaddress** shows the MAC address of the hardware.
- **Flags** show the interface is UP or down.
- **Iface** shows interface on the router on which the corresponding host is connected.

b) Adding or deleting an entry in the ARP table updates ARP table/cache with the new entries.
Syntax for adding: sudo arp -s <ip-address> -i <interface-name> <mac-address>
Syntax for deleting: sudo arp -d <ip-address>

Note: I created a virtual network interface named eth0 to query the arp table.



```
harshbijwe@harshbijwe-VirtualBox:~$ arp -e
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   52:54:00:12:35:02   C                     enp0s3
harshbijwe@harshbijwe-VirtualBox:~$ sudo arp -s 192.168.1.110 -i eth0 51:53:00:17:34:09
harshbijwe@harshbijwe-VirtualBox:~$ sudo arp -s 192.168.1.115 -i eth0 71:53:00:17:34:10
harshbijwe@harshbijwe-VirtualBox:~$ sudo arp -s 192.168.1.120 -i eth0 71:53:00:17:35:11
harshbijwe@harshbijwe-VirtualBox:~$ sudo arp -s 192.168.1.125 -i eth0 71:53:00:17:35:12
harshbijwe@harshbijwe-VirtualBox:~$ arp -e
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.115            ether   71:53:00:17:34:10   CM                    eth0
192.168.1.120            ether   71:53:00:17:35:11   CM                    eth0
192.168.1.125            ether   71:53:00:17:35:12   CM                    eth0
_gateway                 ether   52:54:00:12:35:02   C                     enp0s3
192.168.1.110            ether   51:53:00:17:34:09   CM                    eth0
harshbijwe@harshbijwe-VirtualBox:~$
```

c) The parameter '**Timeout**' is used to determine how long the entries in the cache of the ARP module of the kernel remain valid, the command to check the timeout value is '**cat/proc/sys/net/ipv4/neigh/ethX/gc_stale_time**' and it gets deleted from the cache if the timeout value gets over.
The default value for timeout is 21600 seconds(6 hours). After 6 hours the entry will be automatically deleted from the cache. Consider, we guess the timeout value of 60 mins and then make the system clock 60 mins faster and see what happens. Try 30 mins if the arp cache has been cleared or some value bigger if it hasn't.This is how trial and error method will work for arp.

d) There are two possible cases which if two IP-address map to the same Ethernet(MAC) address-

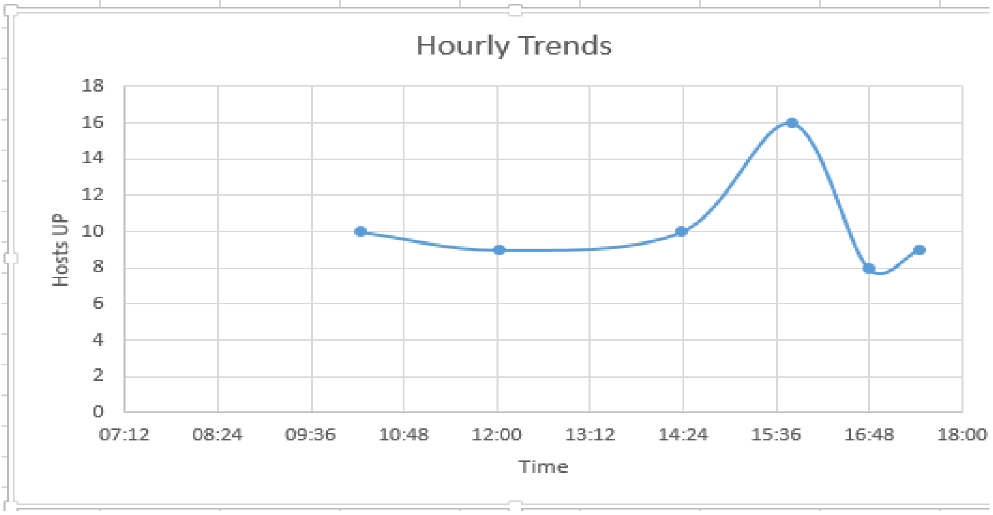
• **The first one is when both the IP addresses are in different networks** in this case there **won't be any bad effect on the system** as the Ethernet address does not leave the network which the NIC is immediately connected to.

• **The second one is when both the IP addresses are present in the same network then in this case there will be a confusion in the network** and packets may travel to any of the machines it encountered first through switches.

Question-7 Solution:

I queried my LAN using **'nmap –n –sP 172.16.112.0/26'**.Following are results.

Time	Hosts UP
10:14	10
12:02	9
14:23	10
15:48	16
16:47	8
17:26	9


Hourly Trends
Hosts UP
07:12
08:24
09:36
10:48
12:00
13:12
14:24
15:36
16:48
18:00
Time