Assignment - 1
CS 342: Networks Lab (September – November2020)
Name: Annapurne Krishna
Roll No: 180101009

Q1.

a) "**-c count**" where count is the number of echo requests to be sent
b) "**-i sec**" where sec is the time interval(in seconds) between two successive ping ECHO_REQUESTs.
c) We can use the **'–l'** option to send packets to the destination without waiting for a reply. The limit for normal users is **3** packets for sending such ECHO_REQUEST packets. **'-f**' option can be used to send requests without any gap or we can set the time interval to 0 using -i option.
d) "-**s packetSize**" where packetSize is the size of packet to be sent in bytes. If the payload size is set to 32 bytes, total packet size was found to be **40 bytes**.

Q2.

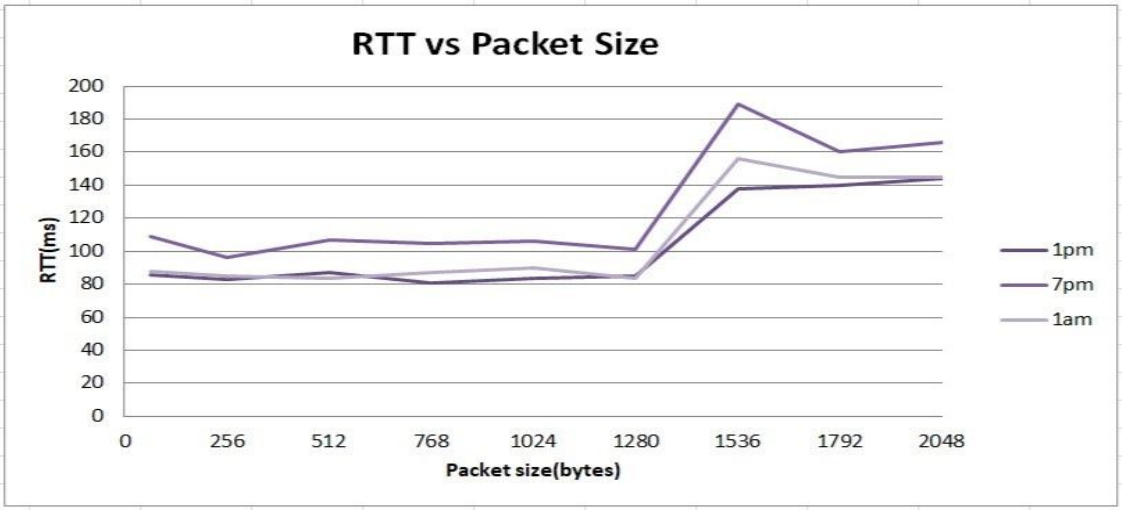
a) The readings are taken at 1pm, 1am and 7pm.

Destination Host IP	Destination host name	Geographical location of host	Avg. RTT 1 (ms)	Avg. RTT 2 (ms)	Avg. RTT 3 (ms)	Total avg. RTT(ms)
81.27.240.126	www.codeforces.com	Russia	392	284	242	306
184.168.131.241	www.grammerly.com	US	510	433	352	431.66
35.160.83.36	www.interviewbit.com	US	408	390	305	367.66
13.35.130.68	www.amazon.com	US	92	79	91	87.33
163.53.78.110	www.flipkart.com	India	101	129	85	105
8.8.8.8	www.google.com	US	71	71	62	68

From the experiment we can say that geographical distance affects RTT. The reason for which is as the distance of destination from the source increases the packet has to travel a longer distance and hence has to go through more number of routers, each router adds a delay to the propagation of the packet. So as the distance increases the number of hops packet has to take increases.

b) Host 81.27.240.126(www.codeforces.com) gave 12% packet loss. Packet loss generally occurs due to network conjunction and the traffic. ICMP packets take more time to process because of lesser priority. Sometimes all the packets can be dropped by the server and result in 100% packet loss.

c) Host used: 13.35.130.68 (www.amazon.com)



d) From the above table, we can see that initially the RTT does not change much then it takes a sudden jump. The reason for this is that the mtu is 1500 bytes which means that for packets with size

lesser than mtu, data is padded to make the size 1500 and for packets with greater size than mtu the packet is broken into two frames of 1500. That's why we observe a sharp change in the RTT.
From both the above tables, we observe that RTT's vary with time of the day. At different times, the congestion in the network is different. Since late night in some regions can be peak business hours in some other regions, often the average RTT at late night is greater than during the day time. Order of RTT in decreasing order would be late night, morning, evening, afternoon.

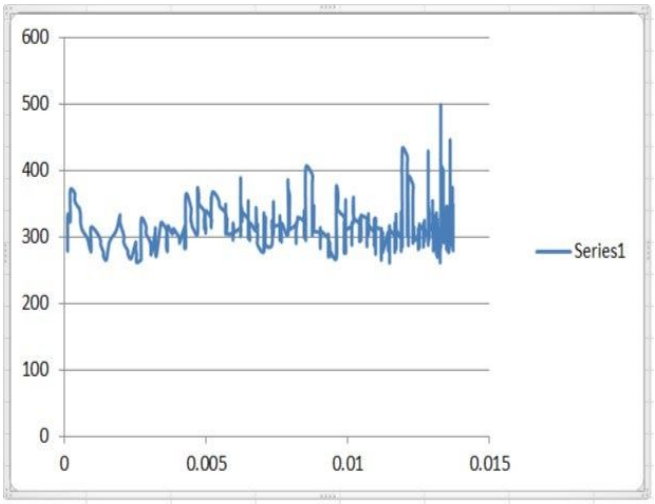
Q3. Host used: 13.35.130.68 (www.amazon.com)

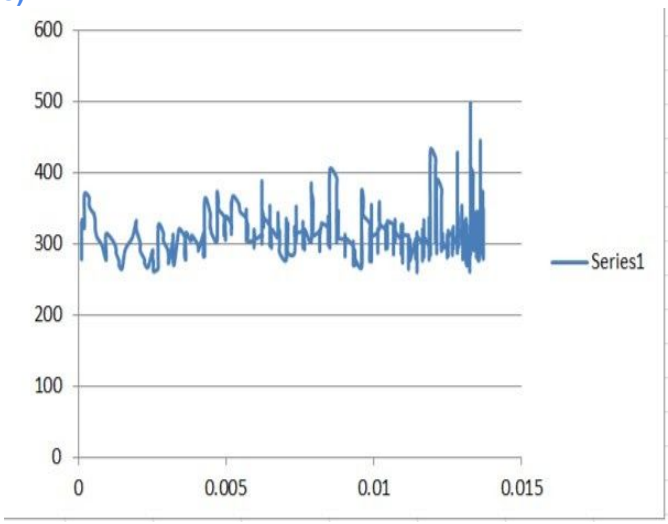
a) Packet loss rate was found 0% for both the commands.

b)c) For first command: minimum=260.874ms, maximum=497.669ms, mean=315.608ms, median=313ms

For second command:minimum=261.632ms, maximum=381.031, mean=305.144ms, median=305ms

c)





d) For the first experiment host names for host addresses will not be looked up . In the second command,the sent packet will be filled with the pattern 11111100000000 which will be useful for solving data-dependent problems.

Q4.

a) **eth0/wifi0**- indicates that I am connected to a wired/wireless network. In this 0 stands for first internet interface.
inet address- internet address assigned to particular interface
netmask- mask that shows how much of address is routable, which determines whether the computer can connect directly to a device on the LAN or whether it needs to send the packet to a router
broadcast address
Lo - Loopback interface.It is a special network interface that the system uses to communicate with itself. Inet, netmask,scopeid and prefixlen are shown along with it.

b) Options with ifconfig command-
-a : This option is used to display all the interfaces available, even if they are down
-v : Run the command in verbose mode log more details about execution
-s : Display a short list, instead of details.
mtu N : The user uses this parameter to set the mtu.
up : This option is used to activate the driver for the given interface
down : This option is used to deactivate the driver for the given interface

c) route command without any options gives Kernel IP routing table. Table contains Destination, Getaway, Genmask, Flags, Metric, Ref, Use, Iface.
Destination : The destination network or destination host.
Getaway: The gateway address or '*' if none set.

Genmask : The netmask for the destination net; 255.255.255.255 for a host destination and 0.0.0.0 for the default route.
Metric : The distance to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.
Ref : Number of references to this route. (Not used in the Linux kernel.)
Use : Count of lookups for the route. Depending on the use of -F and -C this will be either route cache misses (-F) or hits (-C).
Iface : Interface to which packets for this route will be sent
d) **route -n** : to display routing table in full numeric form;**ip route**:to get details of the kernel/IP routing table using ip command;**route -v**: selects verbose operation;**route -e** : displays additional information

```
krishna0312@DESKTOP-RIT0GFP: $ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
127.0.0.0       0.0.0.0         255.0.0.0       U     256    0        0 lo
127.0.0.1       0.0.0.0         255.255.255.255 U     256    0        0 lo
127.255.255.255 0.0.0.0         255.255.255.255 U     256    0        0 lo
224.0.0.0       0.0.0.0         240.0.0.0       U     256    0        0 lo
255.255.255.255 0.0.0.0         255.255.255.255 U     256    0        0 lo
0.0.0.0         192.168.43.1    255.255.255.255 U     0      0        0 wifi0
192.168.43.0    0.0.0.0         255.255.255.0   U     256    0        0 wifi0
192.168.43.33   0.0.0.0         255.255.255.255 U     256    0        0 wifi0
192.168.43.255  0.0.0.0         255.255.255.255 U     256    0        0 wifi0
224.0.0.0       0.0.0.0         240.0.0.0       U     256    0        0 wifi0
255.255.255.255 0.0.0.0         255.255.255.255 U     256    0        0 wifi0
krishna0312@DESKTOP-RIT0GFP: $ ip route
none 224.0.0.0/4 dev eth0 proto unspec metric 256
none 255.255.255.255 dev eth0 proto unspec metric 256
none 224.0.0.0/4 dev eth1 proto unspec metric 256
none 255.255.255.255 dev eth1 proto unspec metric 256
none 127.0.0.0/8 dev lo proto unspec metric 256
none 127.0.0.1 dev lo proto unspec metric 256
none 127.255.255.255 dev lo proto unspec metric 256
none 224.0.0.0/4 dev lo proto unspec metric 256
none 255.255.255.255 dev lo proto unspec metric 256
none default via 192.168.43.1 dev wifi0 proto unspec metric 0
none 192.168.43.0/24 dev wifi0 proto unspec metric 256
none 192.168.43.33 dev wifi0 proto unspec metric 256
none 192.168.43.255 dev wifi0 proto unspec metric 256
none 224.0.0.0/4 dev wifi0 proto unspec metric 256
none 255.255.255.255 dev wifi0 proto unspec metric 256
none 224.0.0.0/4 dev wifi1 proto unspec metric 256
none 255.255.255.255 dev wifi1 proto unspec metric 256
none 224.0.0.0/4 dev wifi2 proto unspec metric 256
none 255.255.255.255 dev wifi2 proto unspec metric 256
krishna0312@DESKTOP-RIT0GFP: $ route -v
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
127.0.0.0       0.0.0.0         255.0.0.0       U     256    0        0 lo
127.0.0.1       0.0.0.0         255.255.255.255 U     256    0        0 lo
127.255.255.255 0.0.0.0         255.255.255.255 U     256    0        0 lo
224.0.0.0       0.0.0.0         240.0.0.0       U     256    0        0 lo
255.255.255.255 0.0.0.0         255.255.255.255 U     256    0        0 lo
0.0.0.0         192.168.43.1    255.255.255.255 U     0      0        0 wifi0
192.168.43.0    0.0.0.0         255.255.255.0   U     256    0        0 wifi0
192.168.43.33   0.0.0.0         255.255.255.255 U     256    0        0 wifi0
192.168.43.255  0.0.0.0         255.255.255.255 U     256    0        0 wifi0
224.0.0.0       0.0.0.0         240.0.0.0       U     256    0        0 wifi0
255.255.255.255 0.0.0.0         255.255.255.255 U     256    0        0 wifi0
krishna0312@DESKTOP-RIT0GFP: $ route -e
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
127.0.0.0       0.0.0.0         255.0.0.0       U         0 0          0 lo
127.0.0.1       0.0.0.0         255.255.255.255 U         0 0          0 lo
127.255.255.255 0.0.0.0         255.255.255.255 U         0 0          0 lo
224.0.0.0       0.0.0.0         240.0.0.0       U         0 0          0 lo
255.255.255.255 0.0.0.0         255.255.255.255 U         0 0          0 lo
0.0.0.0         192.168.43.1    255.255.255.255 U         0 0          0 wifi0
192.168.43.0    0.0.0.0         255.255.255.0   U         0 0          0 wifi0
192.168.43.33   0.0.0.0         255.255.255.255 U         0 0          0 wifi0
192.168.43.255  0.0.0.0         255.255.255.255 U         0 0          0 wifi0
224.0.0.0       0.0.0.0         240.0.0.0       U         0 0          0 wifi0
255.255.255.255 0.0.0.0         255.255.255.255 U         0 0          0 wifi0
```

Q5.

a) The netstat command generates displays that show network status and protocol statistics. You can display the status of TCP and UDP endpoints in table format, routing table information, and interface information. It can be used to troubleshoot network-related issues and verify connection statistics.

b) -t flag should be used with netstat command to show the established tcp connections.

```
C:\Users\Admin>netstat -t

Active Connections

  Proto  Local Address          Foreign Address        State           Offload State

  TCP    192.168.225.31:58671   aerodent:http          CLOSE_WAIT      InHost
  TCP    192.168.225.31:58673   aerodent:http          CLOSE_WAIT      InHost
  TCP    192.168.225.31:58752   relay-57634b9d:http    ESTABLISHED     InHost
  TCP    192.168.225.31:58802   40.119.211.203:https   ESTABLISHED     InHost
  TCP    192.168.225.31:58805   40.90.189.152:https    ESTABLISHED     InHost
  TCP    192.168.225.31:58806   aeab55d76dd13c9bb:https  ESTABLISHED     InHost
  TCP    192.168.225.31:58808   server-13-227-141-14:https  ESTABLISHED     InHost
  TCP    192.168.225.31:58816   ec2-34-206-249-113:https  CLOSE_WAIT      InHost
  TCP    192.168.225.31:58817   ec2-34-206-249-113:https  CLOSE_WAIT      InHost
  TCP    192.168.225.31:58818   ec2-34-252-134-45:https  ESTABLISHED     InHost
  TCP    192.168.225.31:58819   151.101.1.69:https     ESTABLISHED     InHost
  TCP    192.168.225.31:58821   151.101.1.69:https     ESTABLISHED     InHost
  TCP    192.168.225.31:58823   151.101.129.69:https   ESTABLISHED     InHost
  TCP    192.168.225.31:58824   ec2-34-252-134-45:https  ESTABLISHED     InHost
  TCP    192.168.225.31:58826   104.16.1.35:https      ESTABLISHED     InHost
  TCP    192.168.225.31:58829   stackoverflow:https    ESTABLISHED     InHost
  TCP    192.168.225.31:58830   a23-61-85-253:https    ESTABLISHED     InHost
  TCP    192.168.225.31:58834   aeab55d76dd13c9bb:https  ESTABLISHED     InHost
  TCP    [2409:4042:599:b2af:60ed:a5b6:4c28:b994]:56280  [2620:1ec:c::11]:https  ESTABLISHED     InHost
  TCP    [2409:4042:599:b2af:60ed:a5b6:4c28:b994]:58765  [2404:6800:4003:c03::bc]:5228  ESTABLISHED     InHost
  TCP    [2409:4042:599:b2af:60ed:a5b6:4c28:b994]:58769  whatsapp-cdn6-shv-02-bom1:https  ESTABLISHED     InHost
  TCP    [2409:4042:599:b2af:60ed:a5b6:4c28:b994]:58770  [2603:1046:900:19::2]:https  ESTABLISHED     InHost
  TCP    [2409:4042:599:b2af:60ed:a5b6:4c28:b994]:58793  [2603:1046:900:19::2]:https  ESTABLISHED     InHost
  TCP    [2409:4042:599:b2af:60ed:a5b6:4c28:b994]:58822  bom05s11-in-x0a:https  ESTABLISHED     InHost
  TCP    [2409:4042:599:b2af:60ed:a5b6:4c28:b994]:58828  [2a04:fa87:fffe::c000:4902]:https  ESTABLISHED     InHost
  TCP    [2409:4042:599:b2af:60ed:a5b6:4c28:b994]:58831  [2620:116:800e:21:e81a:f5c1:48e5:3dca]:https  ESTABLISHED     InHost
  TCP    [2409:4042:599:b2af:60ed:a5b6:4c28:b994]:58832  bom07s25-in-x01:https  ESTABLISHED     InHost
  TCP    [2409:4042:599:b2af:60ed:a5b6:4c28:b994]:58833  bom07s24-in-x0e:https  ESTABLISHED     InHost
```

c) netstat -r shows kernel routing information. It contains columns Destination, Gateway, Genmask, Flags, MSS, Window, irtt, Iface.

Destination - indicates the pattern to which the destination of a packet is compared.

Gateway - It tells the computer where to send a packet that matches the destination of the same line.

Genmask -It tells how many bits from the start of the ip address are used to identify the subnet.

Flags - It displays the flags that describe the route. Following are the flags

G- implies that the route uses a gateway;U-implies that the interface is up;H-implies that the only a single host can be reached through the route;D-implies that the route is dynamically created;M-implies that the route is set if the table entry was modified by an ICMP redirect message;!-implies that the route is a rejected route and datagrams will be dropped

MSS- stands for Maximum Segment Size and it is the size of the largest datagram the kernel will construct for transmission via this route

Window - It is the maximum amount of data the system will accept in a single burst from a remote host.

irtt -It stands for initial round trip time.

Iface -column tells which network interface should be used for sending packets that match destination.

d) i flag can be used with netstat command to display the status of all network interfaces. My device has 2 interfaces, which are lo(loopback device) and wifi0(wireless network).

e) s flag along with the u flag should be used to display the statistics of all UDP connections on linux. While s flag displays UDP connections along with other connections on windows.

```
UDP Statistics for IPv4

  Datagrams Received    = 305367
  No Ports              = 18103
  Receive Errors        = 1754
  Datagrams Sent        = 156242

UDP Statistics for IPv6

  Datagrams Received    = 209191
  No Ports              = 10297
  Receive Errors        = 11
  Datagrams Sent        = 128838
```

f) The loopback interface is used to identify the device. While any interface address can be used to determine if the device is online, the loopback address is the preferred method. Whereas interfaces might be removed or addresses changed based on network topology changes, the loopback address never changes. The loopback interface is always up and it is reachable as long as the route to that IP address is available in the IP routing table. Hence you can use the loopback interface for diagnostics and troubleshooting purposes. As the loopback address never changes, it is the best way to identify a device in the network. ping command requires a loopback address to function correctly.

Q6.

a) traceroute is a network diagnostic tool used to track in real-time the pathway taken by a packet on an IP network from source to destination, reporting the IP addresses of all the routers it pinged in between. Traceroute also records the time taken for each hop the packet makes during its route to the destination.Traceroute is a useful tool for determining the response delays and routing loops present in a network pathway across packet switched nodes. It also helps to locate any points of failure encountered while en route to a certain destination.

b)

Destination Host IP	Destination Host name	hop count1	hop count2	hop count3
81.27.240.126	www.codeforces.com	18	20	17
184.168.131.241	www.grammerly.com	23	29	18
35.160.83.36	www.interviewbit.com	25	27	22
13.35.130.68	www.amazon.com	22	27	25
163.53.78.110	www.flipkart.com	15	19	24
8.8.8.8	www.google.com	13	22	11

Some common hops included my machine ip(172.25.9.85) and my service provider(jiofi.local.html [192.168.225.1]) which were common in all the experiments. 10.71.235.35 was also a common hop in *grammerly.com* and *amazon.com* and 10.71.235.34 was common in *flipkart.com* and *interviewbit.com* Hops are common because of the reason that routes to these destinations pass through the same internet circles and hence overlap.

c) Due to network traffic the route of the packets change when experiment is done at different times of the day.The packets take the route having minimum traffic which may differ every time so the route may change even if the destination host is the same.

d) Yes, it is possible to find the route to certain hosts which fail to respond with a ping experiment. Ping uses ICMP which is blocked by the system you are trying to reach and traceroute uses UDP packets with an incrementation method of TTL field which is not blocked at the system we are trying to reach. Routers decrement TTL values of packets by one and discard packets whose TTL value has reached zero, which result in ICMP time exceeded. Traceroute looks for the ICMP Time exceeded packet and not the ICMP reply packet, and hence it should be possible.

Q7.

a) ARP is an acronym Address Resolution Protocol which gives mapping of IP addresses to MAC addresses. arp –a shows the complete ARP Table of the machine. It shows the *IP-Address* which is the address of the system, the corresponding *physical address* (also known as mac address) of the system and the type of arp entry (static or dynamic).

```
Interface: 192.168.225.31 --- 0x5
  Internet Address      Physical Address      Type
  192.168.225.1         ee-3c-62-b3-5d-70     dynamic
  192.168.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

b) -s flag is used to add an entry to the ARP table and -d flag is used to delete an entry.

```
C:\WINDOWS\system32>arp -a

Interface: 192.168.225.31 --- 0x5
  Internet Address      Physical Address      Type
  192.168.225.1         ee-3c-62-b3-5d-70     dynamic
  192.168.225.3         00-00-00-00-00-00     static
  192.168.225.31        d0-c5-d3-1e-b5-81     static
  192.168.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\WINDOWS\system32>arp -s 192.168.225.5 00-00-00-00-00-00

C:\WINDOWS\system32>arp -s 192.168.225.7 00-00-00-00-00-00

C:\WINDOWS\system32>arp -a

Interface: 192.168.225.31 --- 0x5
  Internet Address      Physical Address      Type
  192.168.225.1         ee-3c-62-b3-5d-70     dynamic
  192.168.225.3         00-00-00-00-00-00     static
  192.168.225.5         00-00-00-00-00-00     static
  192.168.225.7         00-00-00-00-00-00     static
  192.168.225.31        d0-c5-d3-1e-b5-81     static
  192.168.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

c)No. ARP only works between devices in the same IP subnet. If the two IP Addresses are on different subnets, the device will look in its routing table for a route to the destination network, and then it will send its packet to the appropriate router or to its default gateway. If no more specific route is present in this scenario, ARP will be used to find the hardware address of the router, because the destination IP address has already be deemed to not be directly reachable, so the packet must be delivered to a router which can take care of it.The entries in the table have the same network which means they have the same subnet and hence cannot be connected with other subnet.

d) The ping requests failed. When a router connects to two or more subnet ranges, two IPs can map to the same ethernet address. The mac address is required for directing the packages when communicating with machines having the same subnet. In the arp table, the IPs of the devices which are connected in the other subnet range have a mac address same as that of the router which connects the two subnet ranges. ARP table is looked at when converting these IP addresses to MAC addresses and packets are sent to it. The router then uses its routing table and sends packets further to the right device.

Q8.

a) sudo nmap 172.16.114.222/24

b) using the command “sudo nmap -sA target_ip_address”

c) Number of hosts online in order of time were 43, 52, 61, 54, 59, 51.