Name: Pulkit Changoiwala Roll No: 180101093

CS342 Assignment1

Ans 1)

No	Option	Example	Comments
A	“-c”	ping -c 25 google.com	This ping 25 packets.
B	“-i”	ping -i 2 www.youtube.com	This changes the ping interval to 2 seconds.
C	“-l”	ping -l www.google.com	Only, the superuser is allowed to send more than 3 packets
D	“-s”	ping -s 32 www.google.com	If payload size is set to 32 bytes actual size will be 60 bytes. (28 bytes for header packet)

Ans 2)

a)

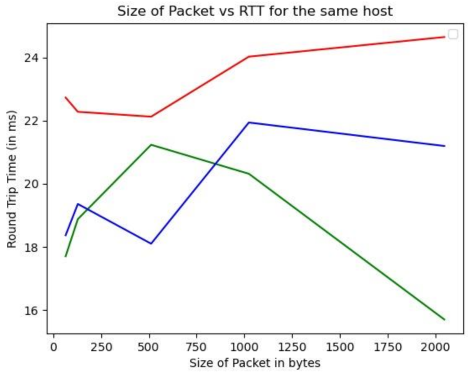
Host IP Address	IP-Address	Time1 12:30 pm	Time 2 6:00pm	Time 3 12:05am	Geographical Location
www.google.com	172.217.167.196	25.06	60.96	35.29	California, US
www.olacabs.com	99.86.42.75	28.197	51.63	16.65	US
www.codeforces.com	81.27.240.126	200.7	194.713	194.58	Russia (St. Petersburg)
www.facebook.com	157.240.218.35	102.67	172.705	99.001	US, NY
www.twitter.com	104.244.42.129	180	185.49	86.80	US
www.interviewbit.com	35.160.83.36	309.33	311.095	306.64	US, Portland

Destination having a larger distance with source has higher RTT compared to one with shorter distance. But RTT also depends on other factors like traffic, firewalls, router configurations etc.

b) Here packet loss is zero for all cases. But packet loss can be more than 0 owing to large traffic. For eg: If a particular IP address is used by lots of people at the same time then it may lead to dropping of some packets.

c) www.olacabs.com (99.86.42.75)

Packet Size (in bytes)	Time 1 in ms 9:00 am	Time 2 in ms 6:00 pm	Time 3 in ms 12:05 am
64	22.73	17.706	18.370
128	22.279	18.882	19.362
512	22.125	21.235	18.105
1024	24.024	20.318	21.94
2048	24.645	15.706	21.197



In Graph:
Redline – Time 1
Greenline – Time 2
Blueline – Time3

d) No drastic changes occur in ping after changing the size of the packet. RTT fluctuates with change in time of the day because of change in traffic on the network throughout the day.

Ans 3) **Command 1**: ping -c 1000 www.facebook.com > op3_1.txt

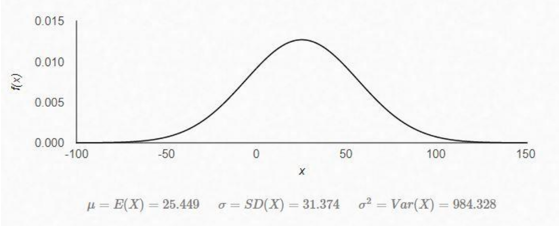
Command 2: ping -c 1000 -p ff00 www.facebook.com > op3_2.txt

a) For Command1: 0.5 % loss For Command 2: 0.1 % loss

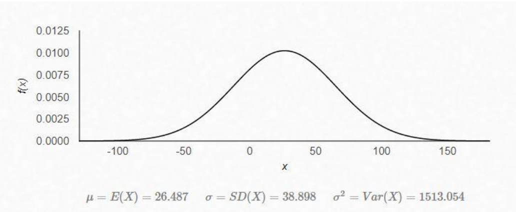
b)

Command	Minimum	Maximum	Mean	Median	Dev.
1	18.202	714.734	25.449	5.8	31.374
2	18.425	765.984	26.487	4.1	38.898

c) Command 1



Command 2



d) "-p" is useful for diagnosing data-dependent problems in a network. 16 pad bits can be sent. In our Eg we sent MS 8 bits as 1 and last 8 bits as 0. As our given commands were simple "ping" so no significant difference was observed. With "-n" no lookup of destination names. Used when no Domain Name Server is available.

Ans 4)

a) **ifconfig** stands for interface configuration.

- It is used to view and change the network interface configuration on a PC.
- It is used at the boot time to set up the interfaces as necessary.

Output:

inet addr: IPv4 address assigned to the interface	**inet6 addr**: IPv6 address assigned to the interface
Bcast: Broadcast address of the network associated with the interface.	**Mask:** Network mask associated with the interface.
UP: Indicates network interface is configured to be enabled	**RUNNING:** Indicates that interface is operational and ready
RX packets: Number of packets received	**TX packets**: Number of packets transmitted
Left margin displays the name of the interface.	

b)

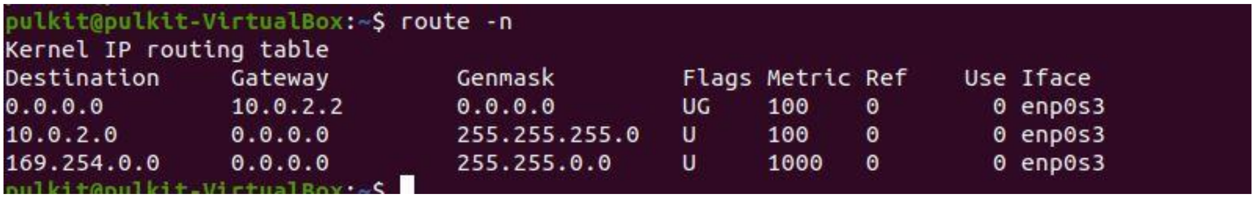
S.No	Option	Explanation
1	-a	Display all the interfaces even if they are down
2	-s	Display a short list, instead of details
3	up	Used to activate the driver for the given interface
4	down	Used to deactivate the driver for the given interface
5	add	This is used to add an IPv6 address to an interface
6	del	This is used to remove an IPv6 address to an interface

c) Route command in Linux is used when you want to work with the IP/kernel routing table. It is mainly used to set up static routes to specific hosts or networks via an interface. It is used for showing or update the IP/kernel routing table

- Destination: Destination network or destination host
- Gateway: The address of the gateway through which packets should pass through
- Genmask: The netmask for the destination net; '255.255.255.255' for a host destination and '0.0.0.0' for the default route.

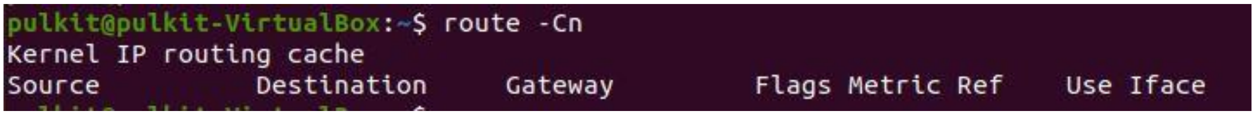
d)

1) "**-n**" It displays a routing table in full numeric form. **Syntax**: route -n



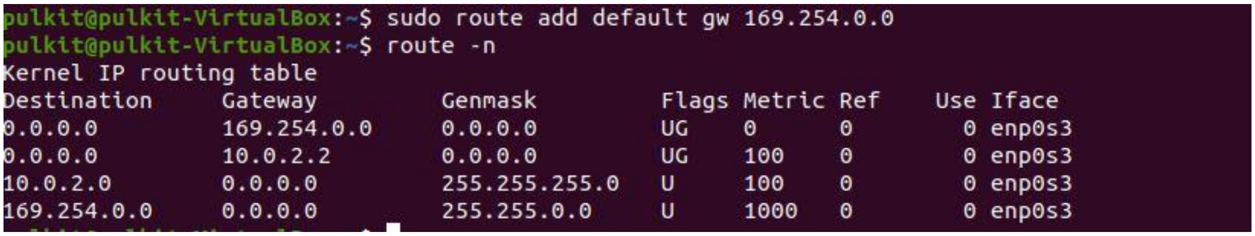
```
pulkit@pulkit-VirtualBox:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.2.2        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
pulkit@pulkit-VirtualBox:~$
```

2) "**-Cn**" To route the packets faster the kernel maintains the routing cache. This option prints those cache information. **Syntax**: route -Cn



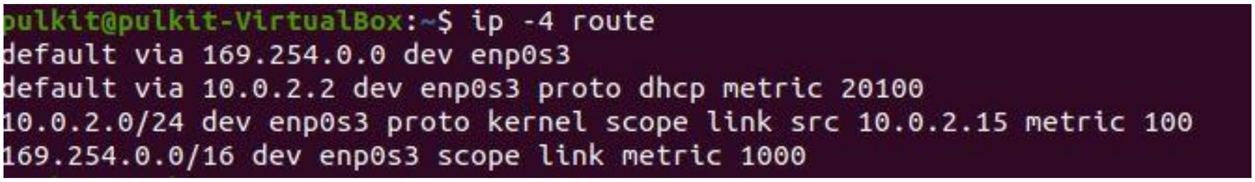
```
pulkit@pulkit-VirtualBox:~$ route -Cn
Kernel IP routing cache
Source          Destination     Gateway         Flags Metric Ref    Use Iface
```

3) To add default gateway: **sudo route add default gw 169.254.0.0**



```
pulkit@pulkit-VirtualBox:~$ sudo route add default gw 169.254.0.0
pulkit@pulkit-VirtualBox:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         169.254.0.0     0.0.0.0         UG    0      0        0 enp0s3
0.0.0.0         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
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
```

4) To get output related to IPv4: “ **ip -4 route** ”

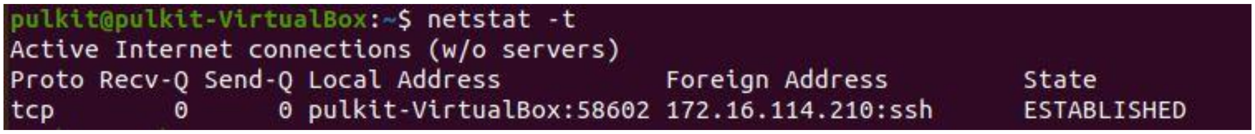


```
pulkit@pulkit-VirtualBox:~$ ip -4 route
default via 169.254.0.0 dev enp0s3
default via 10.0.2.2 dev enp0s3 proto dhcp metric 20100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
169.254.0.0/16 dev enp0s3 scope link metric 1000
```

Ans 5)

a) To see various network related information netstat command is used. Information pertaining to network connections, routing tables, interface statistics

b) “-t”



```
pulkit@pulkit-VirtualBox:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 pulkit-VirtualBox:58602 172.16.114.210:ssh      ESTABLISHED
```

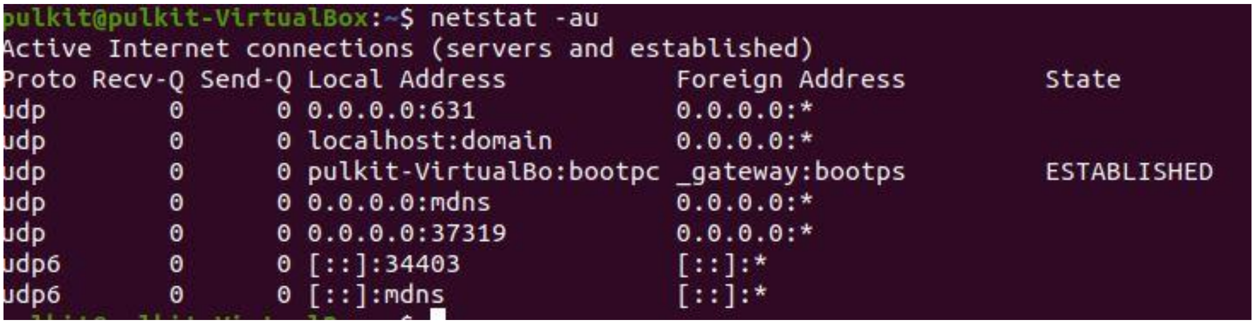
c) “netstat -r” shows kernel routing information.

Output Fields:

Destination:	The destination address of the packet
Gateway:	The address of the gateway
Genmask:	The netmask for the destination net
Flags:	The U flag indicates that the route is up. The G flag indicates that the route is to a gateway
MSS:	The MSS column indicates the default Maximum Segment Size for TCP connections over this route
Window:	The Window column indicates the default window size for TCP connections over this route
IRTT:	Initial Round Trip Time for this route.
Iface:	Interface name

d) **“-i”** It lists down all the interfaces.
My PC has two interfaces one is enp0s3(Ethernet Network Peripheral) and another one is “lo”(loopback interface)

e) “-au”



```
pulkit@pulkit-VirtualBox:~$ netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 pulkit-VirtualBo:bootpc _gateway:bootps         ESTABLISHED
udp        0      0 0.0.0.0:mdns            0.0.0.0:*
udp        0      0 0.0.0.0:37319           0.0.0.0:*
udp6       0      0 [::]:34403              [::]:*
udp6       0      0 [::]:mdns               [::]:*
```

f) Loopback Interfaces is a virtual network interface which is used by a computer to communicate with itself. It is used mainly for diagnostics and troubleshooting, and to connect to servers running on the local machine. The loopback interface does not represent any actual hardware but exists so applications running on your computer can always connect to servers on the same machine.

For IPv4, the loopback interface is assigned all the IPs in the 127.0.0.0/8 address block. That is, 127.0.0.1 through 127.255.255.254 all represent our computer. For most purposes, though, it is only necessary to use one IP address, and that is 127.0.0.1. This IP has the hostname of localhost mapped to it.

Ans 6)

a) Traceroute in Linux prints the route which packets take to reach the host.
Syntax: traceroute ipAddress
Output: First column- Hop Count || Second column: Address of the hop || then three space generated time in ms
traceroute command sends three packets to the hop and each of the time refers to the time taken by the packet to reach the hop.

b)

Host IP Address	IP-Address	Time1 9:00 am	Time 2 13:00pm	Time 3 1:00am	Geographical Location
www.google.com	172.217.167.196	8	8	8	India
www.olacabs.com	99.86.42.75	11	17	17	India, Delhi
www.codeforces.com	81.27.240.126	9	9	9	Russia(St. Petersburg)
www.facebook.com	157.240.218.35	14	14	14	US, NY
www.twitter.com	104.244.42.129	5	5	5	US
www.interviewbit.com	35.160.83.36	14	14	14	US, Portland

Most Common Hops:
core4.fra.hetzner.com, core23.fsn1.hetzner.com, juniper5.nbg1.hetzner.com, a100row-ic-300117-sjo-b21.c.telia.net

c) A route to the same host changes due to change in traffic over the network during the course of time. **In intermediate nodes(switches) fast switching occurs which checks the address to the next hop from cache and cache entries might change due to change in traffic**.

d) Some hops are missing in various route, reasons can be:

- ICMP transfers to the next-hop without decreasing TTL value(from the current hop, **usually firewall**) so it prevents the node from sending "TTL expired in transit" message to the source. Hence corresponding entry is missing from hops.
- **A traceroute shows only layer 3 hops**, so layer 2 hops can be missing.
  For eg: We are going through say 10 ISP routers running a layer 2 VPN which appears as a single hop.

e) **"traceroute" can still work even if the ping isn't. Reason:** Traceroute is an application, not a protocol, the protocol used depends on implementation in use.
LINUX traceroute uses UDP, while echo requests are ICMP. So some networks now block ICMP by default, so PING command won't work but traceroute does.

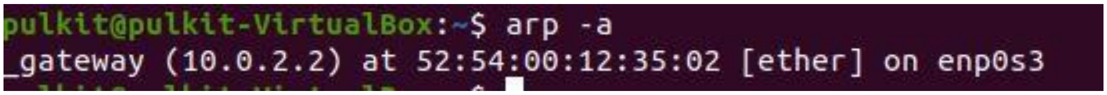
Moreover, it can be the case that ICMP "echo-reply"(ping) is blocked but ICMP "time exceeded" isn't.

Ans 7)

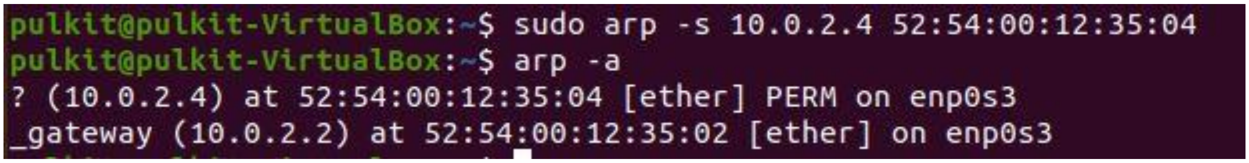
a) ARP(Address Resolution Protocol) table is a mapping from IP address to MAC that a system uses to communicate over the network effectively.

Table Column	Description
Address	IPv4 (network layer) address for which a permanent entry is added to the ARP cache.
HWtype	Hardware type
HWaddress	MAC address of a hardware
Flags Mask	Describes on or off
Iface	Interface type

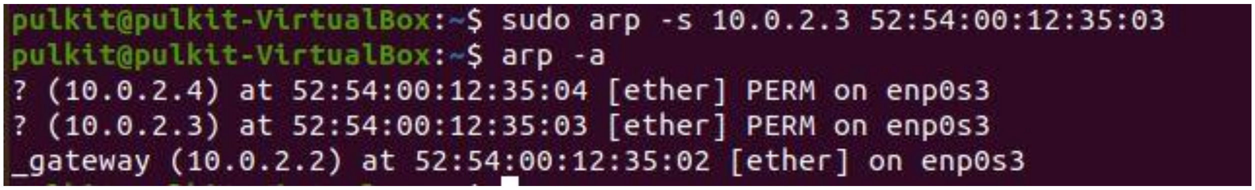
b) For deleting an entry. Syntax: **sudo arp -d hostname**
For adding an entry to ARP. Syntax: **sudo arp -s IPAddr MACAddr**



```
pulkit@pulkit-VirtualBox:~$ arp -a
_gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3
```



```
pulkit@pulkit-VirtualBox:~$ sudo arp -s 10.0.2.4 52:54:00:12:35:04
pulkit@pulkit-VirtualBox:~$ arp -a
? (10.0.2.4) at 52:54:00:12:35:04 [ether] PERM on enp0s3
_gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3
```



```
pulkit@pulkit-VirtualBox:~$ sudo arp -s 10.0.2.3 52:54:00:12:35:03
pulkit@pulkit-VirtualBox:~$ arp -a
? (10.0.2.4) at 52:54:00:12:35:04 [ether] PERM on enp0s3
? (10.0.2.3) at 52:54:00:12:35:03 [ether] PERM on enp0s3
_gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3
```

c) ARP works only on the IP in the same subnet.
If two IP addresses. are on different subnets then packets follow a diff. logic. It will look at the routing table for the destination network and send the packet to the router or default gateway. In this case, the ARP table is used to find the hardware address of that router. because the destination IP address has already been deemed to not be directly reachable, so the packet must be delivered to a router which can take care of it.

d) Ping command didn't run on the modified node.
Two types of conflict may occur
1) **IP Address conflict**: In this case traffic will be forwarded based on ARP cache.
2) **MAC address** (two nodes have the same MAC address):

- Two nodes won't be able to communicate, as ARP broadcast will fail as source node will have the same MAC address as the destination node.
- Other nodes trying to send data to any one of these nodes with the same MAC address; these nodes will be contacted through the switch. These two nodes will send data continuously thus the switch will continuously update the table for this MAC address. This results in MAC address flapping and communication disruption occurs

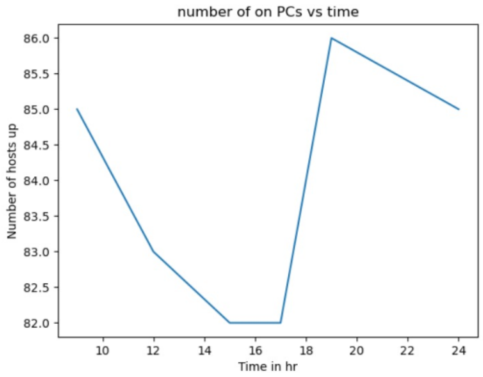
Ans 8)

a) To get PCs which are up in subnet we use "*" in IP address.
Eg: **nmap -sP 192.168.1.***

b) To scan the firewall setting of my own pc:- **sudo nmap -sA 192.168.1.***

c) Command used "**nmap -sP 172.16.114.*** "
(CSE Department Lab PCs) 256 IP addresses were scanned each time.

Time	9:00	12 00	15:00	17:00	19:00	24:00
Host Up	85	83	82	82	86	85


number of on PCs vs time
Number of hosts up
Time in hr