Assignment 1

CS 342: Networks Lab

Name: Somya Khandelwal
Roll Number: 200123056

Question 1.

a -c followed by the count of ECHO_REQUESTs.
Example, $ ping -c 2 facebook.com

b -i followed by the time interval in seconds.
Example, $ ping -i 2 facebook.com

c -l followed by number of packets or preload.
Example, $ ping -l 2 facebook.com
The limit for sending such ECHO_REQUEST for a normal user is 3. Only super-user may preload more than 3.

d -s followed by data bytes to be sent.
Example, $ ping -s 32 facebook.com
If the payload size is set to 32 bytes then the packet size will be 60 including ICMP header and IPv4 header.

Question 2.

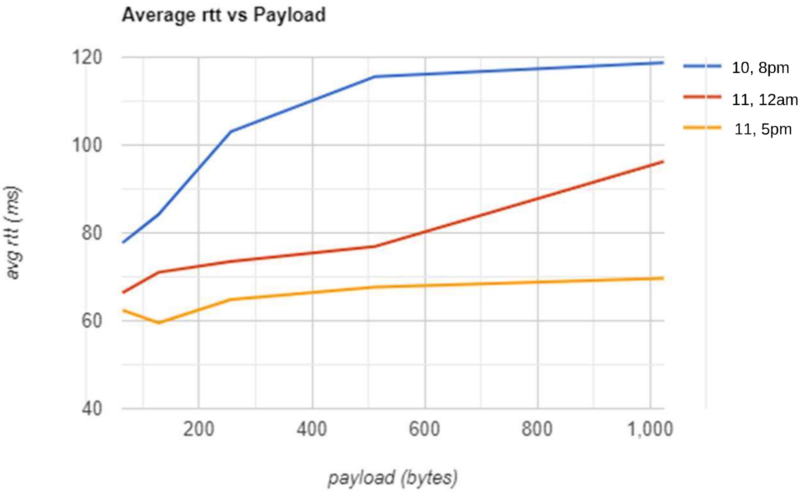
Hosts: facebook.com, google.com, youtube.com, bing.com, yahoo.com, instagram.com
Pinged the servers using command prompt.

Hostname	**10/08/2022 8pm**	**11/08/2022 12am**	**11/08/2022 5pm**
facebook.com	64.155	63.333	62.132
google.com	84.552	52.577	54.574
yahoo.com	414.835	400.602	352.924
bing.com	55.894	46.054	58.732
instagram.com	416.286	412.308	577.144
youtube.com	96.388	67.696	110.378

Round trip time and geographical distance have a positive correlation i.e. in general, rtt increases with increase in geographical distance, with the reason being, larger distance implies a greater number of hops and having to go through a greater number of routers and switches, which causes delay.

The packet loss was greater than 0% when pinging ‘instagram.com’. The possible reason for nonzero packet loss can be network congestion, which occurs when there is a lot of traffic on the route or poor internet connectivity which causes the ECHO_REQUEST to timeout and fail.
Also, some websites gave 100% packet loss because of certain host firewall settings blocking ICMP packet, sent by the ping command.

Hostname: facebook.com. Pings with payload size 2048 bytes gave 100% packet loss.



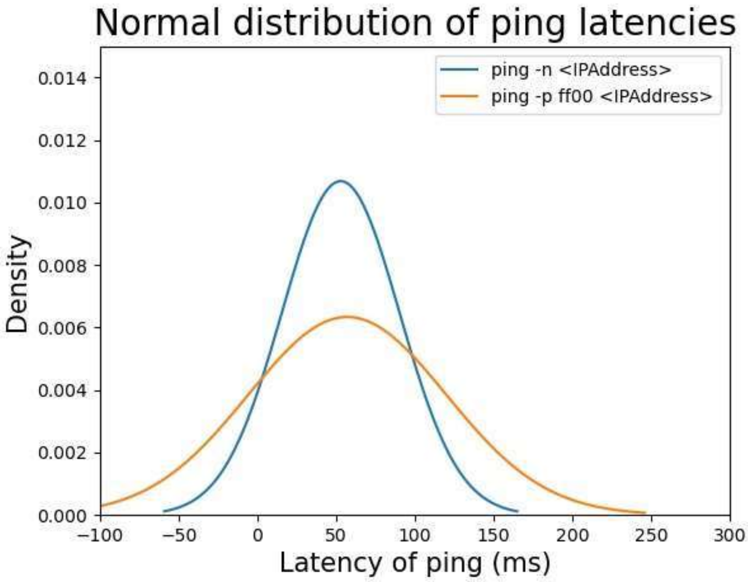
According to the data obtained in ` ` part of the question it is observed that the round-trip time increases when packet size is increased because processing larger packets takes more time.
RTT also changes with the time of day at which the ping is made subject to the network congestion. The traffic on a network is different at different hours of the day thus the rtt changes or simply rtt increases when there is more network congestion.

Question 3.

a The packet loss rate for each command was 0%.

b For $ ping -n <IPAddress>
Latency values:
Min: 28.1 max: 835.0 mean: 52.85 median: 47.7
For $ ping -p ff00 <IPAddress>
Latency values:
Min: 25.6 max: 989.0 mean: 57.05 median: 45.6

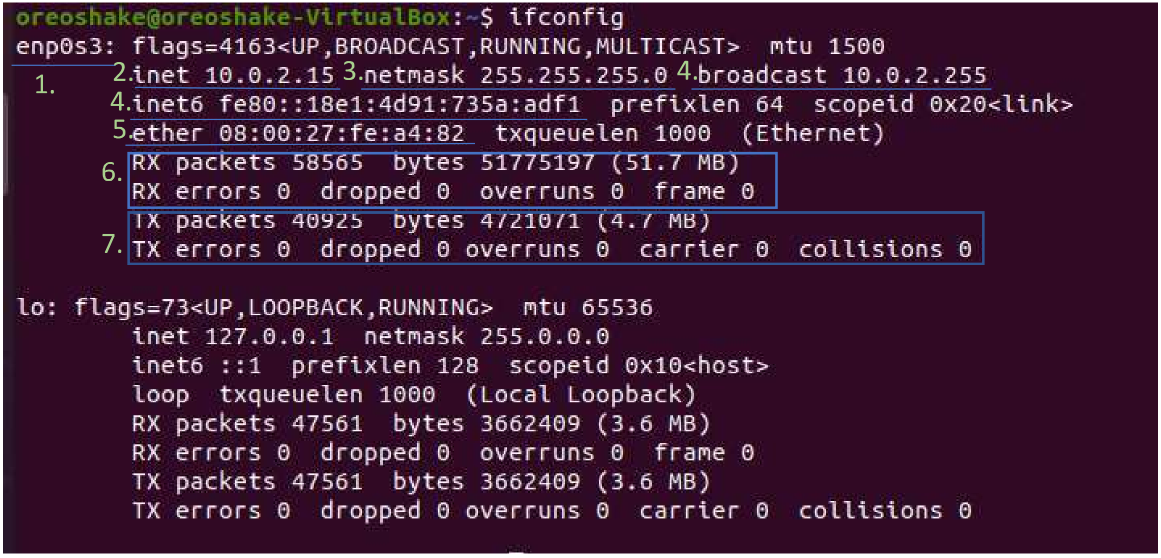
c



d The two distributions have almost same mean latency but variance value is different. [-p] option is useful for diagnosing data-dependent problems in a network and ping with [-n] option does not lookup for names of host addresses. The comparison of curves in the two cases shows the network behaviour towards certain data configuration. In this case the curves are almost similar implying similar network behaviour but the variance value for second command is higher.

Question 4.

a ifconfig command is used to configure network interfaces. If no arguments are given it displays currently active network interfaces. Ifconfig stands for "interface configuration".



```
oreoshake@oreoshake-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::18e1:4d91:735a:adf1  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:fe:a4:82  txqueuelen 1000  (Ethernet)
        RX packets 58565  bytes 51775197 (51.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 40925  bytes 4721071 (4.7 MB)
        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 47561  bytes 3662409 (3.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 47561  bytes 3662409 (3.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

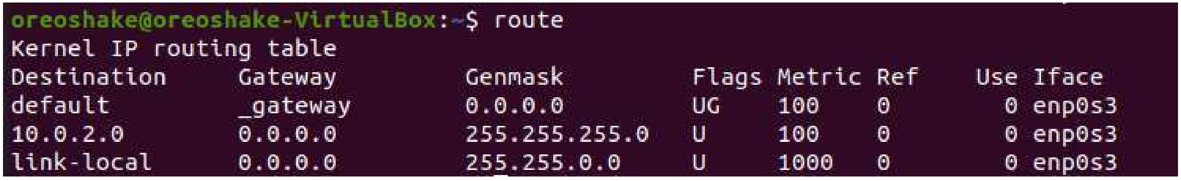
Looking at the first interface in the output, the first line states that the interface is up and running, supports broadcast message, and multicast message.

1. Iface: Name of interface.
2. Inet addr: IPv4 address assigned to the interface
3. Netmask: Network mask associated with the interface. A Netmask is a 32-bit "mask" used to divide an IP address into subnets and specify the network's available hosts
4. Broadcast: Broadcast address associated with network interface.
5. Hardware class followed by Hardware address also called the MAC address.
6. Details of packets received via interface
7. Details of packets transmitted via interface

b Options for ifconfig command:

1. [-a] : To display all the available network interfaces even if they are down.
2. [up/down] : Causes an interface to be activated or deactivated respectively. Syntax:
   $ ifconfig <interface> up/down
3. [[-]arp]: Enable or disable ARP protocol on an interface. Syntax:
   $ ifconfig <interface> arp (to enable)
   $ ifconfig <interface> -arp (to disable)
4. -v : Be more verbose or display additional information on errors.

c Route command is used to display and manipulate IP routing table. A routing table is a set of rules, that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed.

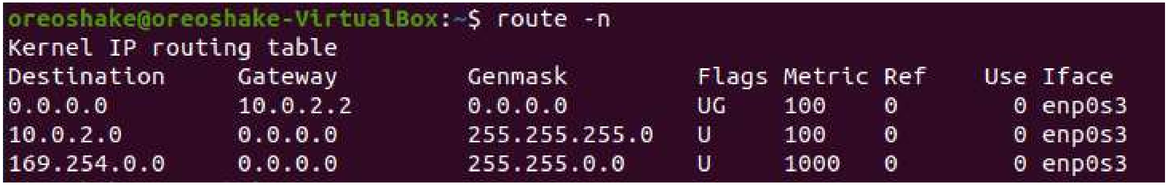


```
oreoshake@oreoshake-VirtualBox:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3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

1. Destination: The IP Address/name of the destination host
2. Gateway: The gateway address. Show '*' is no gateway address is set.
3. Genmask: The netmask for the destination net; 255.255.255.255 for a host destination and 0.0.0.0 for the default route.
4. Flags: May take any of the values (possibly more than one or zero),
   U (route is up), H (target is a host), G (use gateway), R (reinstate route for dynamic routing), D (dynamically installed by daemon or redirect), M (modified from routing daemon or redirect), A (installed by addrconf), C (cache entry), ! (reject route)
5. Metric: The distance to the target (usually counted in hops)
6. Ref: Number of references to this route.
7. Use: Count of lookups for the route.
8. Iface: Interface to which packets for this route will be sent.

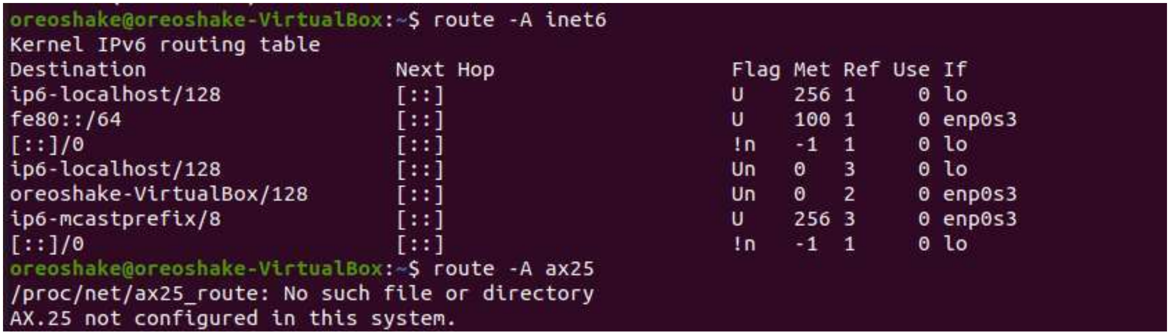
d

1. [-n]: show numerical addresses instead of trying to determine symbolic host names.



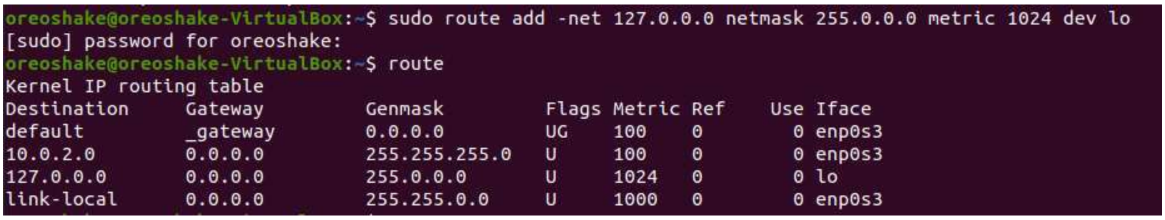
```
oreoshake@oreoshake-VirtualBox:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.2.2        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3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

2. [-A family]: To use the specified address family.
   Possible address families: inet(default), inet6, ax25, netrom, ipx, ddp, x25



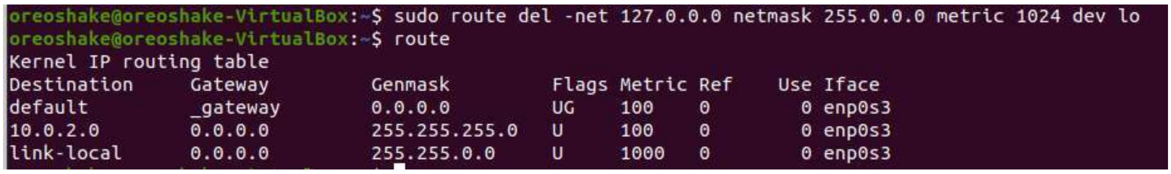
```
oreoshake@oreoshake-VirtualBox:~$ route -A inet6
Kernel IPv6 routing table
Destination                    Next Hop                   Flag Met Ref Use If
ip6-localhost/128              [::]                       U    256 1     0 lo
fe80::/64                      [::]                       U    100 1     0 enp0s3
[::]/0                         [::]                       !n   -1  1     0 lo
ip6-localhost/128              [::]                       Un   0   3     0 lo
oreoshake-VirtualBox/128       [::]                       Un   0   2     0 enp0s3
ip6-mcastprefix/8              [::]                       U    256 3     0 enp0s3
[::]/0                         [::]                       !n   -1  1     0 lo
oreoshake@oreoshake-VirtualBox:~$ route -A ax25
/proc/net/ax25_route: No such file or directory
AX.25 not configured in this system.
```

3. add: add a new route



```
oreoshake@oreoshake-VirtualBox:~$ sudo route add -net 127.0.0.0 netmask 255.0.0.0 metric 1024 dev lo
[sudo] password for oreoshake:
oreoshake@oreoshake-VirtualBox:~$ route
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
127.0.0.0       0.0.0.0         255.0.0.0       U     1024   0        0 lo
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
```

4. del: delete a route

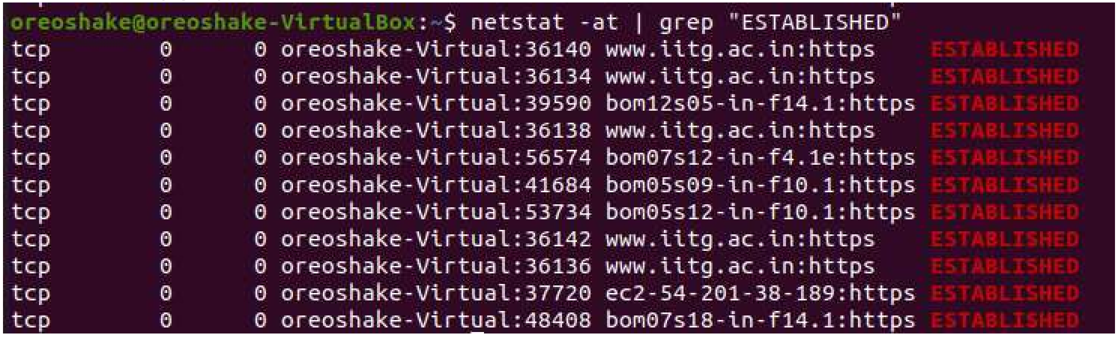


```
oreoshake@oreoshake-VirtualBox:~$ sudo route del -net 127.0.0.0 netmask 255.0.0.0 metric 1024 dev lo
oreoshake@oreoshake-VirtualBox:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    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
```

Question 5.

a The netstat (network statistics) command is used to print network connections, routing table, interface statistics, masquerade connections and multicast memberships.

b $ netstat -at | grep “ESTABLISHED”



```
oreoshake@oreoshake-VirtualBox:~$ netstat -at | grep "ESTABLISHED"
tcp        0      0 oreoshake-Virtual:36140 www.iitg.ac.in:https    ESTABLISHED
tcp        0      0 oreoshake-Virtual:36134 www.iitg.ac.in:https    ESTABLISHED
tcp        0      0 oreoshake-Virtual:39590 bom12s05-in-f14.1:https ESTABLISHED
tcp        0      0 oreoshake-Virtual:36138 www.iitg.ac.in:https    ESTABLISHED
tcp        0      0 oreoshake-Virtual:56574 bom07s12-in-f4.1e:https ESTABLISHED
tcp        0      0 oreoshake-Virtual:41684 bom05s09-in-f10.1:https ESTABLISHED
tcp        0      0 oreoshake-Virtual:53734 bom05s12-in-f10.1:https ESTABLISHED
tcp        0      0 oreoshake-Virtual:36142 www.iitg.ac.in:https    ESTABLISHED
tcp        0      0 oreoshake-Virtual:36136 www.iitg.ac.in:https    ESTABLISHED
tcp        0      0 oreoshake-Virtual:37720 ec2-54-201-38-189:https ESTABLISHED
tcp        0      0 oreoshake-Virtual:48408 bom07s18-in-f14.1:https ESTABLISHED
```

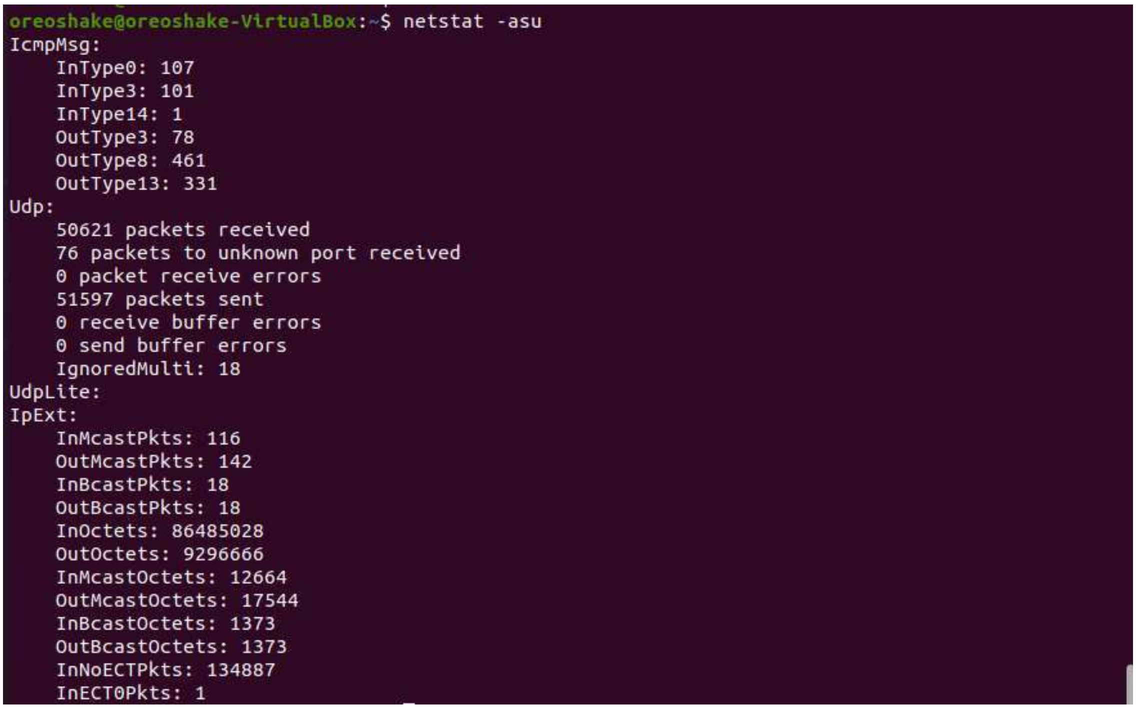
c $ netstat -r shows the Kernel IP routing table.

The following are the attributes of the table:

1. Destination: The IP Address of the destination host
2. Gateway: The gateway address. Show ‘*’ is no gateway address is set.
3. Genmask: The netmask for the destination net; 255.255.255.255 for a host destination and 0.0.0.0 for the default route.
4. Flags: May take any of the values (possibly more than one or zero),
   U (route is up), H (target is a host), G (use gateway), R (reinstate route for dynamic routing), D (dynamically installed by daemon or redirect), M (modified from routing daemon or redirect), A (installed by addrconf), C (cache entry), ! (reject route)
5. MSS : Default maximum segment size for TCP connections over this route.
6. Window : Default window size for TCP connections over this route.
7. irtt : Initial RTT (Round Trip Time). The kernel uses this to guess about the best TCP protocol parameters.
8. Iface: Interface to which packets for this route will be sent.

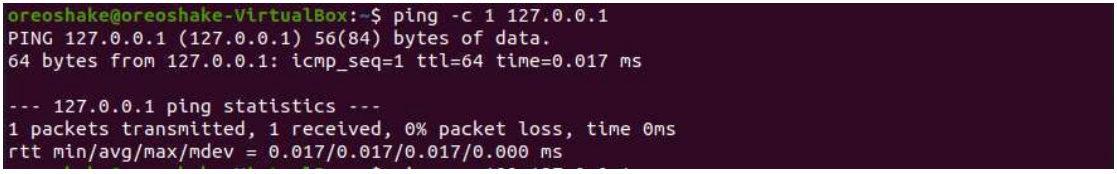
d -a and -i options of the netstat command can be used together to display status of all the network interfaces.
$ netstat -a –interfaces
To figure out the number of interfaces, the below command can be used:
$ netstat -ai | echo $(expr $(wc -l) - 2)

e $ netstat -asu



```
oreoshake@oreoshake-VirtualBox:~$ netstat -asu
IcmpMsg:
    InType0: 107
    InType3: 101
    InType14: 1
    OutType3: 78
    OutType8: 461
    OutType13: 331
Udp:
    50621 packets received
    76 packets to unknown port received
    0 packet receive errors
    51597 packets sent
    0 receive buffer errors
    0 send buffer errors
    IgnoredMulti: 18
UdpLite:
IpExt:
    InMcastPkts: 116
    OutMcastPkts: 142
    InBcastPkts: 18
    OutBcastPkts: 18
    InOctets: 86485028
    OutOctets: 9296666
    InMcastOctets: 12664
    OutMcastOctets: 17544
    InBcastOctets: 1373
    OutBcastOctets: 1373
    InNoECTPkts: 134887
    InECT0Pkts: 1
```

f A machine uses the loopback interface, to communicate with itself. Loopback interface is a virtual network interface that is always up and available after it has been configured. It is used for network diagnostics to check whether the device is up or not. We can configure a loopback interface for the router and ping it. A successful ping indicates that the router is up.



```
oreoshake@oreoshake-VirtualBox:~$ ping -c 1 127.0.0.1
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=0.017 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.017/0.017/0.017/0.000 ms
```

Question 6.

- Traceroute tool is used to track the path taken by a packet to go from one IP address to another and gives a log of all the routers pinged along the way with timestamp. It can be used to detect the cause of packet loss.

a

Host	Hopcount 1	Hopcount 2	Hopcount 3
Google.com	6	6	6
Facebook.com	6	6	6
Instagram.com	10	10	10
Yahoo.com	10	10	10
Bing.com	Timed out	Timed out	Timed out
Youtube.com	6	6	6

There exist common hops between two routes. The first hop in each route is going through one of the 2 specific routers as observed from the IP addresses.

b Route to the same host can vary. When a router receives a packet, to send it to next hop, it scans through the routing table uses process switching. To carryout efficient load balancing, it uses a round-robin mechanism to evenly distribute the traffic among all the connection as there can be multiple intermediate routers belonging to same network and hence gives different routes for the same host.

c The possible reasons for traceroute not finding a complete path can be:
1. The request getting timed out because of network congestion.
2. Firewall blocking the ICMP or UDP packets.
3. Malfunctioning router.

d For certain hosts, it is possible to find the route which fail to respond to ping experiment. This is because ping is sends ICMP ECHO_REQUESTs which can be blocked by the firewall whereas and traceroute supports ICMP, TCP SYN and UDP packets which may pass through some firewalls.

Question 7.

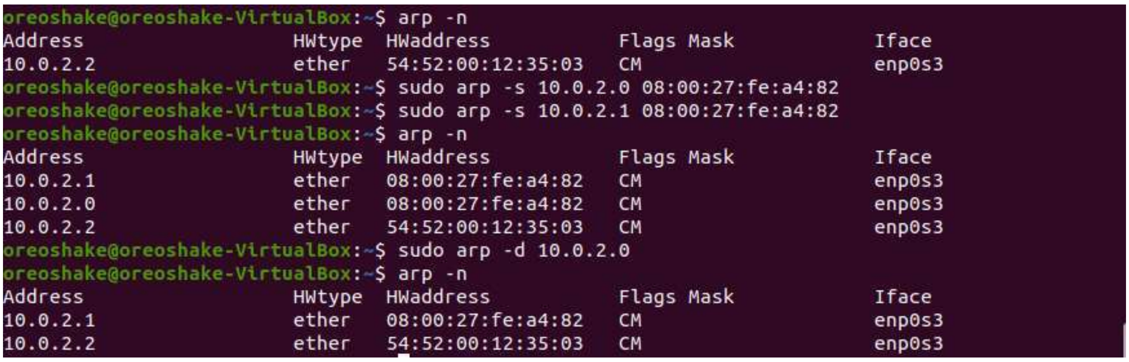
a Arp command is used to manipulate and display system's ARP cache. The following command can be used to view the full ARP table $ arp -a

Attributes of the ARP table

1. HostName: Name of the host.
2. Address: Displays the IPv4 address of the host.
3. HWtype: This field specifies the network link protocol type.
4. HWaddress: Displays the Hardware address or the MAC (Media Access Control) address
5. Iface: Gives the name of the interface

b To add an entry in the ARP table $ sudo arp -s Address HWaddress

To delete an entry from the ARP table $ sudo arp -d Address



```
oreoshake@oreoshake-VirtualBox:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.2                 ether   54:52:00:12:35:03   CM                    enp0s3
oreoshake@oreoshake-VirtualBox:~$ sudo arp -s 10.0.2.0 08:00:27:fe:a4:82
oreoshake@oreoshake-VirtualBox:~$ sudo arp -s 10.0.2.1 08:00:27:fe:a4:82
oreoshake@oreoshake-VirtualBox:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.1                 ether   08:00:27:fe:a4:82   CM                    enp0s3
10.0.2.0                 ether   08:00:27:fe:a4:82   CM                    enp0s3
10.0.2.2                 ether   54:52:00:12:35:03   CM                    enp0s3
oreoshake@oreoshake-VirtualBox:~$ sudo arp -d 10.0.2.0
oreoshake@oreoshake-VirtualBox:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.1                 ether   08:00:27:fe:a4:82   CM                    enp0s3
10.0.2.2                 ether   54:52:00:12:35:03   CM                    enp0s3
```

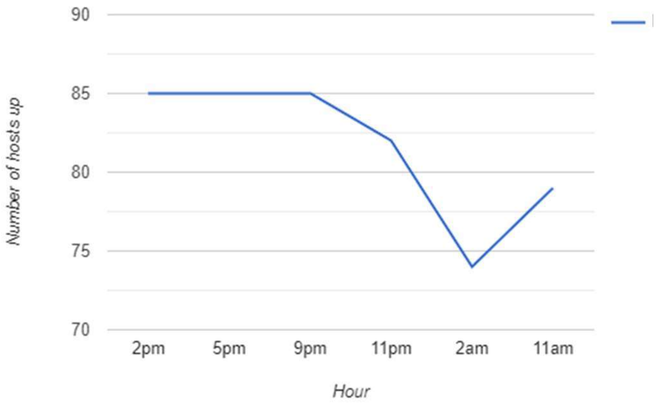
c The ARP table cannot contain an entry for any IP from different subnet from our PC. When sending a packet, the device first looks through the routing table to check if the destination IP belongs to the subnet it can directly reach. If it does, then it can directly send the packet through that interface. Otherwise, it looks for the appropriate router to handle the request in the routing table or sends it to the default router.

d The ping results in 100% packet loss. This occurs because the systems tries to connect to the host through a port which is already occupied by a different IP address. Thus, the attempt for connection fails, as the host is no longer reachable and the ping fails.

Question 8.

$ nmap -sn <IPRange> or $ nmap -sn 172.16.114.00/24

$ sudo nmap -sA <IPAddress>

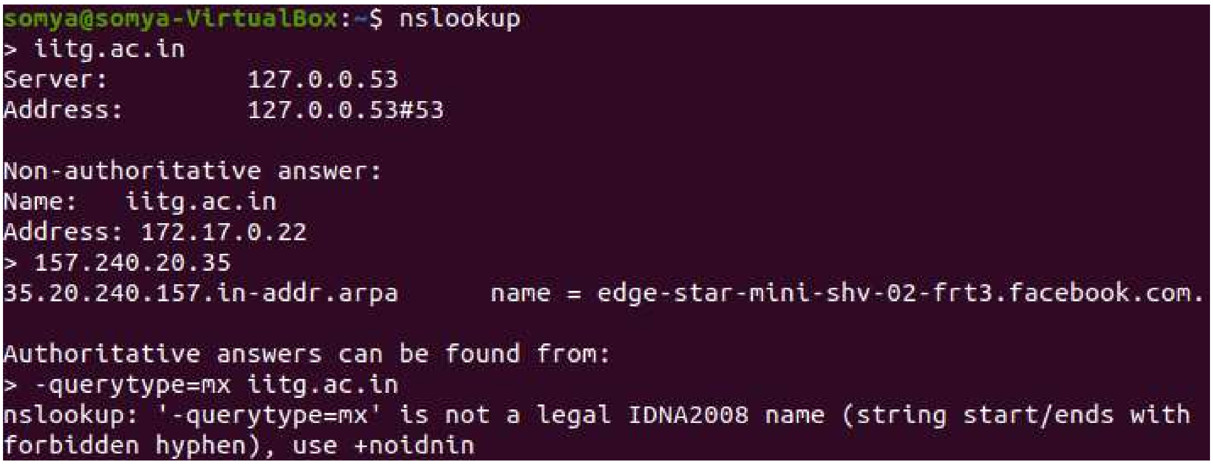


Hour	Active hosts
2pm	85
5pm	85
9pm	85
11pm	82
2am	74
11am	79

The number of active hosts lies between 70 and 85 and the number of active hosts goes down during the night.

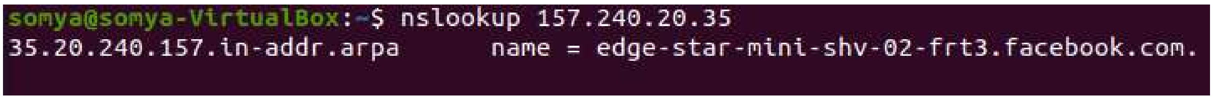
Question 9

a To find the ip address of a host e.g. iitg.ac.in type: nslookup iitg.ac.in



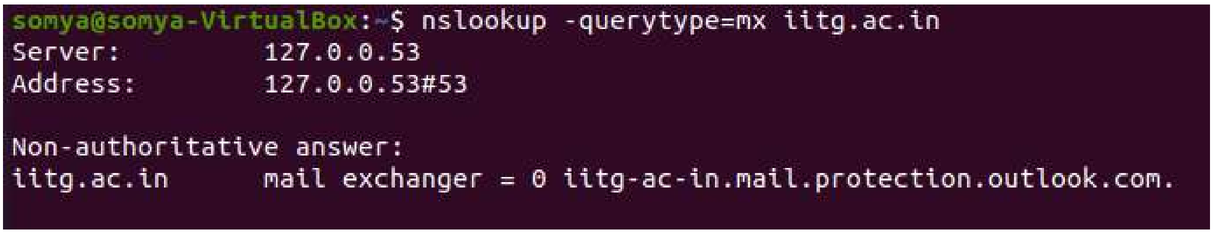
```
somya@somya-VirtualBox:~$ nslookup
> iitg.ac.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   iitg.ac.in
Address: 172.17.0.22
> 157.240.20.35
35.20.240.157.in-addr.arpa      name = edge-star-mini-shv-02-frt3.facebook.com.

Authoritative answers can be found from:
> -querytype=mx iitg.ac.in
nslookup: '-querytype=mx' is not a legal IDNA2008 name (string start/ends with
forbidden hyphen), use +noidnin
```

b. To find domain name of IP address type nslookup IP address



```
somya@somya-VirtualBox:~$ nslookup 157.240.20.35
35.20.240.157.in-addr.arpa      name = edge-star-mini-shv-02-frt3.facebook.com.
```

c. To find mail servers for a Domain type nslookup -querytype=mx domain name



```
somya@somya-VirtualBox:~$ nslookup -querytype=mx iitg.ac.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
iitg.ac.in      mail exchanger = 0 iitg-ac-in.mail.protection.outlook.com.
```