Anket Sanjay Kotkar
Roll no.: 180101037

Question 1

(a) -c number_of_echo_requests

(b) -i interval_of_time
Only superuser can set values less than 0.2

(c) -l number_of_packets_to_be_sent
Only superuser can set the value of packets or specifically preload more than 3

(d) -s payload_size
If the payload size is set to 32 bytes the total packate size will be 40 (32 of payload + 8 bytes of ICMP header data)

Question 2

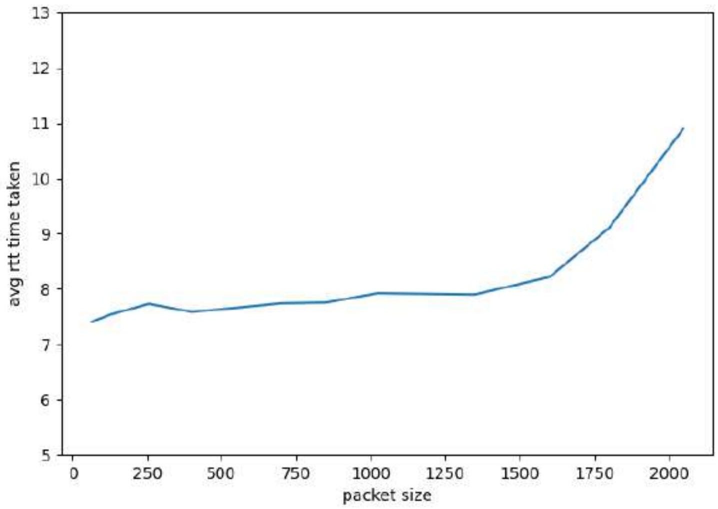
(a)

Hotstar	Google	Facebook	Amazon	LinkedIn	Stackoverflow
8.019	12.719	12.045	8.296	12.451	9.571

RTT does have a corelation with the grographical distance between the source and destination as the signal has to cover that much distance.

(b) Some **sites seems to hae blocked ICMP protocol**, that is why 100% loss of packates were seen in those cases like netflix. Also **some sites doesn't respond well to packet sizes greater than a specific limit** for them like google which was showing packate data loss when packet size crossed 1500.

(c) Host used is Hotstar.com for this subpart.



(d) According to general observation, the average rtt time increases as the packate size increases. Similarly at the time of the day when there is high traffic on the ip we are using for ping can cause increased RTT. Higher the traffic, higher the RTT.

Question 3

The IPAddress used for this question is Facebook.com (31.13.79.35).

(a) Packate loss rate for first command (ping -n <IPAddress>) is 0.6%. Packate loss rate for second command (ping -p ff00 <IPAddress>) is 0.4%.

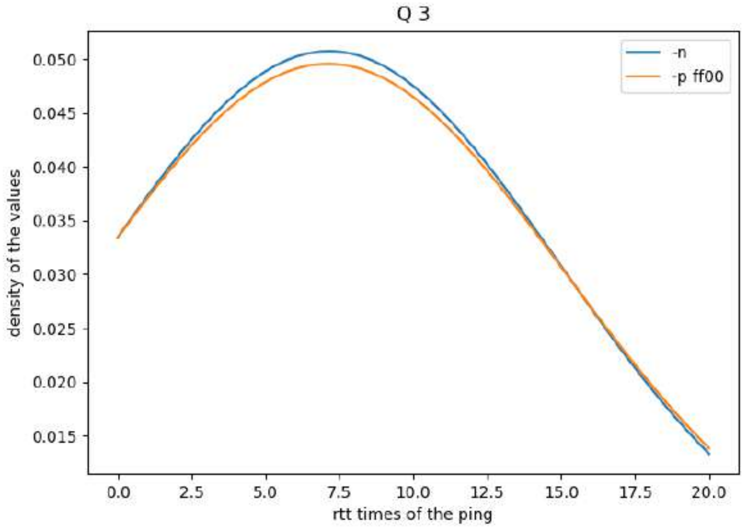
(b) First command:

Minimum	Maximum	Mean	Median latency
5.596	741.628	8.589	7.02

Second command:

Minimum	Maximum	Mean	Median latency
5.042	1002.548	8.172	6.96

(c)



(d) The mean deviation higher and the average RTT is lower in case of the command (ping -p ff00 <IPAddress>) comparing to the same data on command (ping -n <IPAddress>). The graph of 2nd instruction is wider and more spread than the 1st one.

Question 4

(a) ifconfig is a system administration utility in Unix-like operating systems for network interface configuration. On running the ifconfig command, 2 sections are shown in the terminal: enp0s3 and lo. These are the network interfaces configured on the system and are up.

enp0s3: Flags shown in this interface are broadcast (supports broadcast packates), running (the driver has allocated resources for it and ready to transmit and recieve the packets) and multicast (supports multicast packets). The inet, netmask and broadcast line can beexplained as: the inet shows the ip address of the host machine. the subnet mask can be set to subnet mask we are using or can be set it to default and broadcast is the broadcast address of the network. MTU limits the largest datagram that a given layer of a communications protocol can pass at a time.

lo: Flags are running and loopback (packets transfered on this network will not be transferred and will be looped back on the driver).

(b) -a : displays all the interfaces even if the network is down.

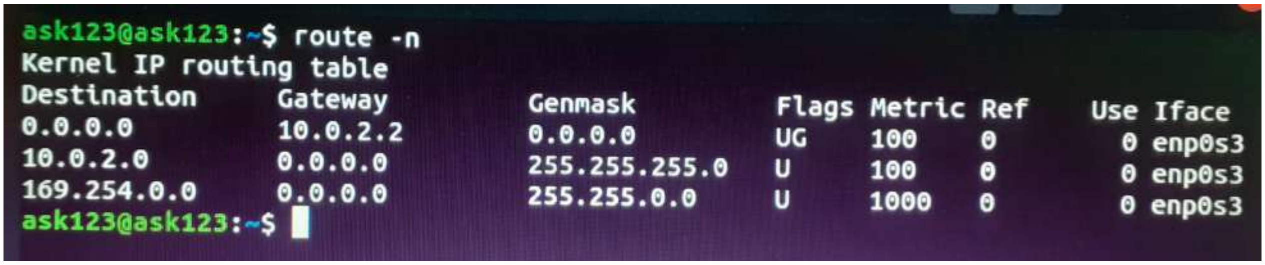
up : This flag causes the interface to get activated.

down: This flag causes the interface to get deactivated.

mtu N: this sets the mtu limit on the interface.

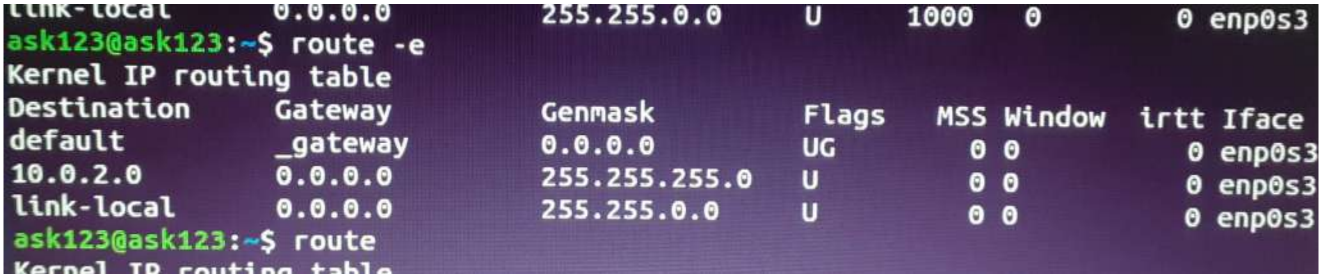
(c) It shows the computer’s routing table. It has the destination IP address which is the address of the destination subnet, and must be interpreted in the context of the subnet mask, interface on which it is configured, gateway and genmask. Genmask is the netmask for the destination net; ’255.255.255.255’ for a host destination and ’0.0.0.0’ for the default route.

(d) -n : shows numeric addresses instead of figuring out the symbolic host names.



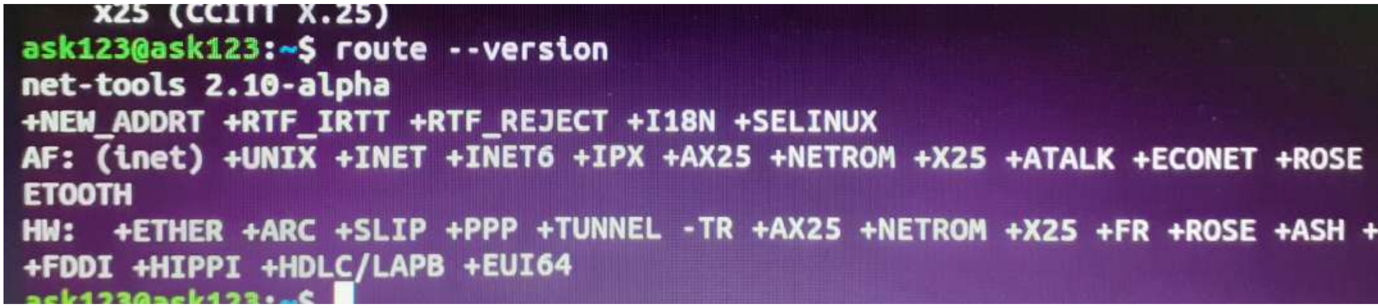
```
ask123@ask123:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.2.2        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
ask123@ask123:~$
```

-e : use netstat format for displaying the routing table.



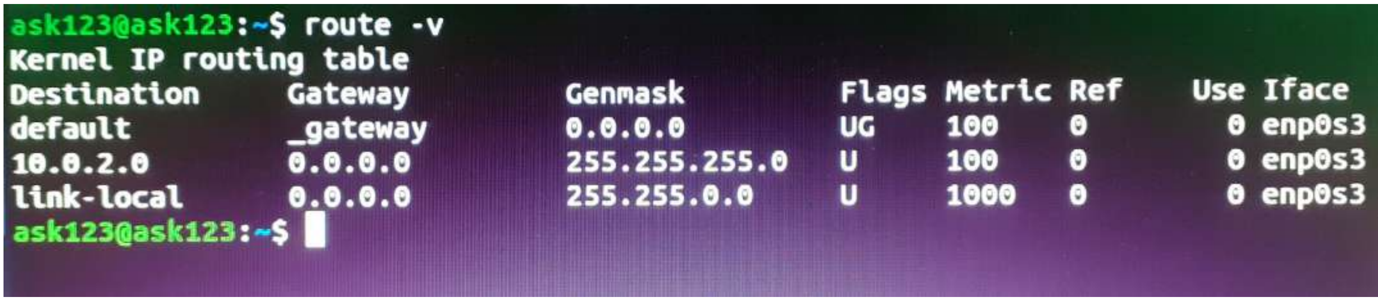
```
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
ask123@ask123:~$ route -e
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 enp0s3
link-local      0.0.0.0         255.255.0.0     U         0 0          0 enp0s3
ask123@ask123:~$ route
Kernel IP routing table
```

–version : version of the route



```
    x25 (CCITT X.25)
ask123@ask123:~$ route --version
net-tools 2.10-alpha
+NEW_ADDRT +RTF_IRTT +RTF_REJECT +I18N +SELINUX
AF: (inet) +UNIX +INET +INET6 +IPX +AX25 +NETROM +X25 +ATALK +ECONET +ROSE
ETOOTH
HW:  +ETHER +ARC +SLIP +PPP +TUNNEL -TR +AX25 +NETROM +X25 +FR +ROSE +ASH +
+FDDI +HIPPI +HDLC/LAPB +EUI64
ask123@ask123:~$
```

-v : select verbose operation

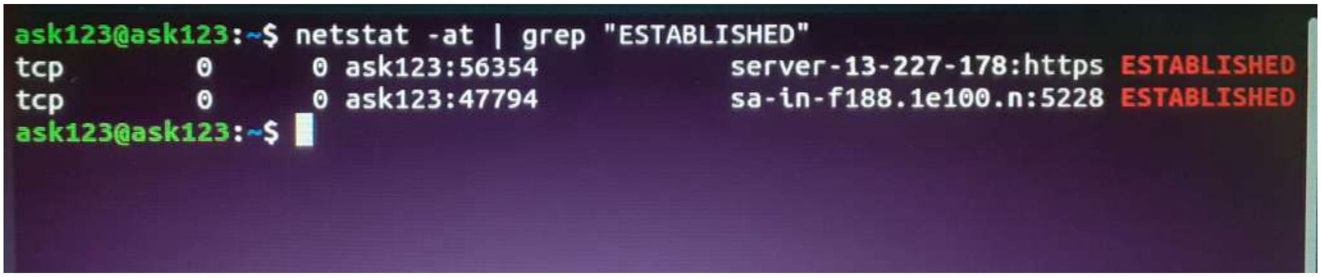


```
ask123@ask123:~$ route -v
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
ask123@ask123:~$
```

Question 5

(a) The netstat command generates displays that show network status and protocol statistics. We can display the status of TCP and UDP endpoints in table format, routing table information, and interface information.

(b) netstat -at — grep ”ESTABLISHED”



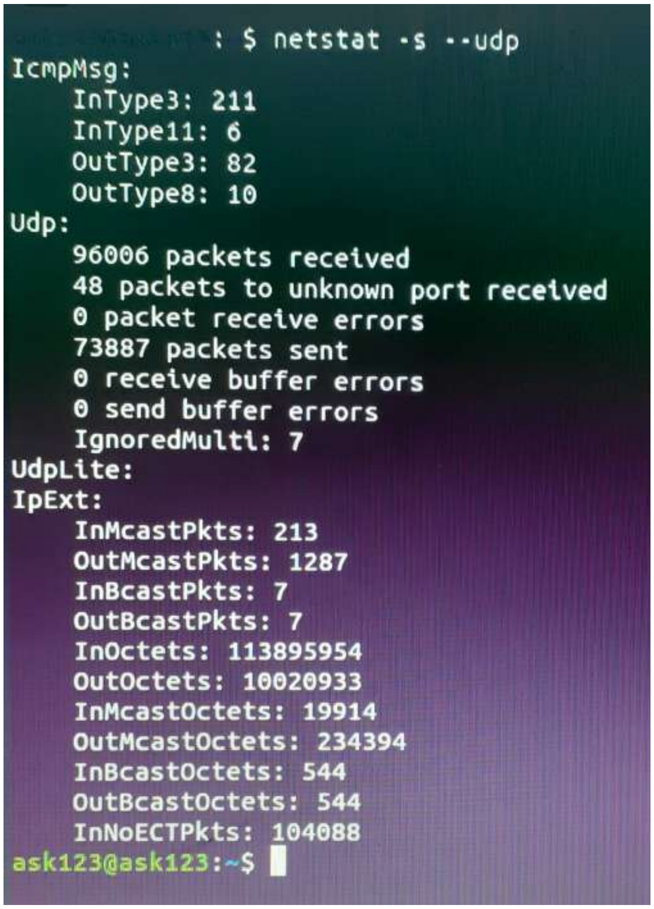
```
ask123@ask123:~$ netstat -at | grep "ESTABLISHED"
tcp        0      0 ask123:56354            server-13-227-178:https ESTABLISHED
tcp        0      0 ask123:47794            sa-in-f188.1e100.n:5228 ESTABLISHED
ask123@ask123:~$
```

(c) It displays the kernel routing table. The commands netstat -r and route -e are equivallent.
The routing table consists of destination ip address which is the address of the destination subnet, and must be interpreted in the context of the subnet mask, interface on which it is configured, gateway and genmask. Genmask is the netmask for the destination net; '255.255.255.255' for a host destination and '0.0.0.0' for the default route. MSS denoted the packet of data can be transmitted. Iface is the interface on which it is configured. "U" means the host is Up, "UG" means "Up and a route to a Gateway (which may pass the packet on)", "G" doesn't need to know if there is, or what its netmask is. It just sends the packet to the router, which deals with the request.

(d) netstar -i : This is the command to get all network interface status

I have 2 interfaces configured on my system.

(e) netstat -s –udp



```
[redacted]: $ netstat -s --udp
IcmpMsg:
    InType3: 211
    InType11: 6
    OutType3: 82
    OutType8: 10
Udp:
    96006 packets received
    48 packets to unknown port received
    0 packet receive errors
    73887 packets sent
    0 receive buffer errors
    0 send buffer errors
    IgnoredMulti: 7
UdpLite:
IpExt:
    InMcastPkts: 213
    OutMcastPkts: 1287
    InBcastPkts: 7
    OutBcastPkts: 7
    InOctets: 113895954
    OutOctets: 10020933
    InMcastOctets: 19914
    OutMcastOctets: 234394
    InBcastOctets: 544
    OutBcastOctets: 544
    InNoECTPkts: 104088
ask123@ask123:~$
```

(f) A loopback interface is a logical, virtual interface. Any traffic that a computer program sends on the loopback network is addressed to the same computer. The most commonly used IP address on the loopback network is 127.0.0.1 for IPv4 and ::1 for IPv6. A loopback interface is always up and allows Border Gateway Protocol (BGP) neighborship between two routers to stay up even if one of the outbound physical interface connected between the routers is down.As the loopback address never changes, it is the best way to identify a device in the network. While any interface address can be used to determine if the device is online, the loopback address is the preferred method.

Question 6

(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.

(b)

Hotstar	Google	Facebook	Amazon	LinkedIn	Stackoverflow
4	6	4	not reachable	not reachable	not reachable
not reachable	not reachable	6	not reachable	not reachable	not reachable
10	12	9	17	not reachable	not reachable

I went through the traceroutes but didn't found any common hops between 2 routes.

(c) According to me the route to the host changes according to the time when we trying for traceroute. It changes according to the network traffic on the IP through which it is going. As different time of the day experiences different network traffic, traceroute changes.

(d) Like as can be seen in the the table, traceroute for the sites LinkedIn and Stackoverflow was unable to find at all 3 times. The error shown by the tools were like timeout error and firewall reached. Mostly the reason behind this might be **because firewall of the IP being blocked through which the system was trying to reach the host**. This was the same reason shown by online tools described in the assignment.

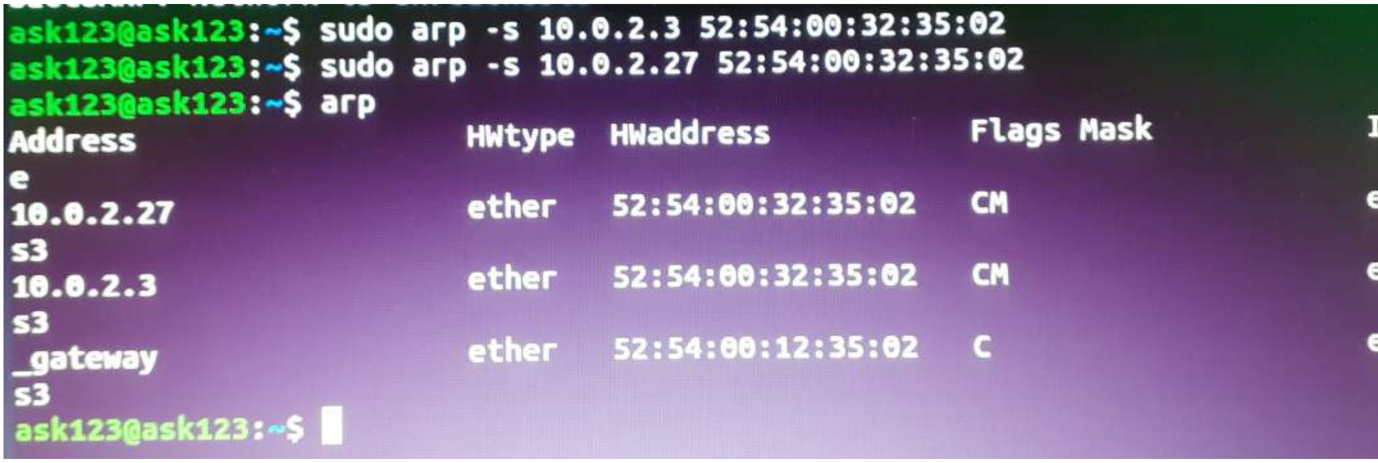
(e) The protocols on which the ping and traceroute commands work are different. Ping uses the ICMP protocol for the execution while the execution of traceroute uses the UDP packets with changing TTL field to map the hops to final destination. As the ICMP protocol may be blocked for some sites but it may not be the case otherwise. So traceroute may work and ping may not in some case.

Question 7

(a) The command to see the full arp table is: arp -a

The column HWType is the network link protocol type. HWaddress is the conversion of IP address of the system into hardware address. Each complete entry in the ARP cache will be marked with the C flag. Permanent entries are marked with M and published entries have the P flag.

(b) The command to add an entry to the ARP entry: sudo arp -s Address HWaddress



```
ask123@ask123:~$ sudo arp -s 10.0.2.3 52:54:00:32:35:02
ask123@ask123:~$ sudo arp -s 10.0.2.27 52:54:00:32:35:02
ask123@ask123:~$ arp
Address                  HWtype  HWaddress           Flags Mask            I
e
10.0.2.27                ether   52:54:00:32:35:02   CM                    e
s3
10.0.2.3                 ether   52:54:00:32:35:02   CM                    e
s3
_gateway                 ether   52:54:00:12:35:02   C                     e
s3
ask123@ask123:~$
```

(c) To send the packets ARP checks whether the IP we are trying to reach and our system IP are in same subnet. If they are in same subnet, then packate is directly sent to the destination IP. If this is not the case, then system tries to find the entry in routing table of the system through which it can directly send the packate and expects the router to take care of of next process of sending the packet and if it does not find any such entry then it sends the packet to the default entry of routing table.

(d) Those entries in the table who are not change show 0% packet loss. But we see a packet loss of 100% in the case of change in ethernet address of the IP address as it fails to establish the connection since the port is already occupied. This causes the all the ping data requests to failed giving the complete data loss.

Question 8

(a) nmap -sn 172.16.114.172/25

(b) sudo nmap -sA 172.16.114.172