ASSIGNMENT -1

Name: Kartikeya Saxena

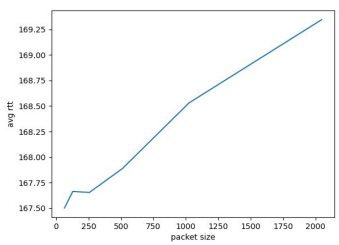
Roll Number: 180101034

Ans. 1 -
a) -c count option is required to specify the number of echo requests to send with ping command.
b) -i interval option is used to set time interval in sec.
c) -l preload command is used to send packets one after another without reply. Normal user limited to max 3 ECHO_REQUEST packets
d) -s packetsize is used to set payload/data size. If payload size is set to 32 bytes total packet size will be 40 because of the 8 bytes of ICMP header data.

Ans. 2 -
IP-1 - www.codeforces.com (81.27.240.126) **Russia**
IP-2 - www.facebook.com (157.240.198.35) **Germany**
IP-3 - www.geeksforgeeks.org (23.55.108.41) **United Kingdom**
IP-4 - 106.215.61.164 **New Delh**i
IP-5 - www.leetcode.com (172.67.138.83) **United States**
IP-6 - kissanime.ru (104.31.74.190) **Canada**

TIME OF EXECUTION	IP-1	IP-2	IP-3	IP-4	IP-5	IP-6
Sep 16 15:56:39 2020	218.602	10.130	12.871	5.418	198.580	72.650
Sep 16 19:49:43 2020	217.893	49.176	8.485	6.595	197.749	71.870
Sep 17 00:54:09 2020	262.872	20.315	10.571	3.542	189.349	71.824

a) In general, yes there is a relation between geo distance from source to destination to RTT. RTT should increases with increase in geo distance as there will be more hops required for packet to travel to the destination in general, hence transmission time and propagation time will be more. But this is not the only factor, network cross traffic, crappy routers and network congestion also play a role, which lead to inconsistencies.
b) Yes, in **IP-1**, probably due to faulty routers or network congestion or error in data transmission.
c) I chose **IP-4** for the experiment and increased packet size in a power of 2 from 32 to 2048

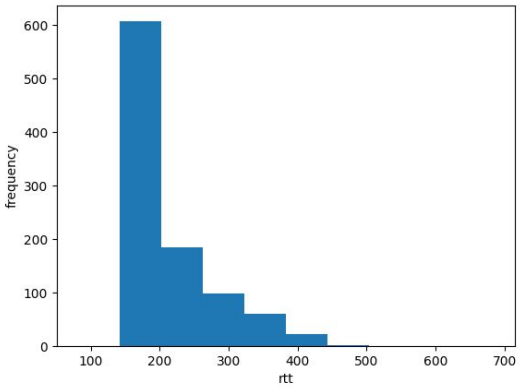


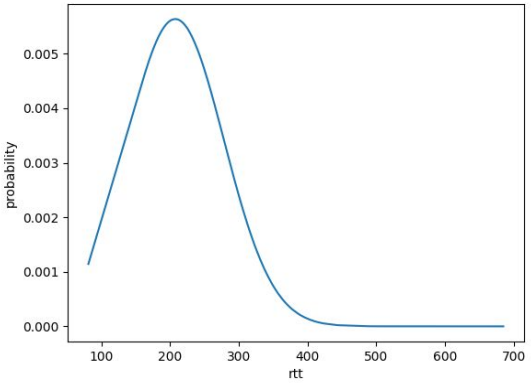
d) Yes there is an increase in RTT with increasing packet size but it is not that significant. The main factor which impacts RTT, among all, is source net connection which if unstable could lead to significant changes in the graph below. There are slight variations in RTT at different times of day due to variations in network congestion and traffic.

Ans.3 -

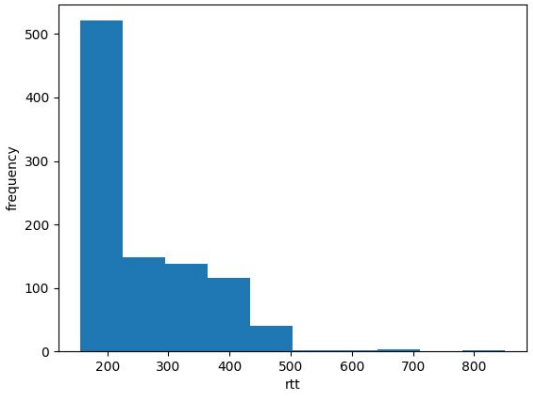
i) ping -c 1000 -p ff00 www.leetcode.com > pingff00.txt
ii) ping -c 1000 -n www.leetcode.com > pingn.txt

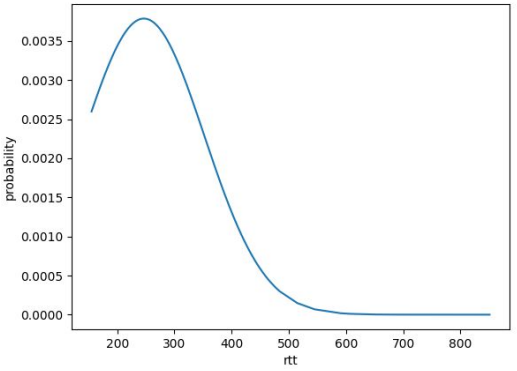
a) i) 980/1000, 2% packet loss ii) 972/1000, 2% packet loss
b) i) **min/max/mean/median** : 155.490/1081.342/208.859/163
ii) **min/max/mean/median** : 155.344/3195.700/250.039/202
c) i)





ii)





d) The standard deviation and mean of the normal distribution of (ii) is more than (i).
-p pattern : is used to fill out the packet with upto 16 bytes. This is useful for diagnosing data-dependent problems in a network.
-n: is used for numeric output only. No attempt will be made to lookup symbolic names for host addresses
The variations are mild only and the distribution is nearly the same.

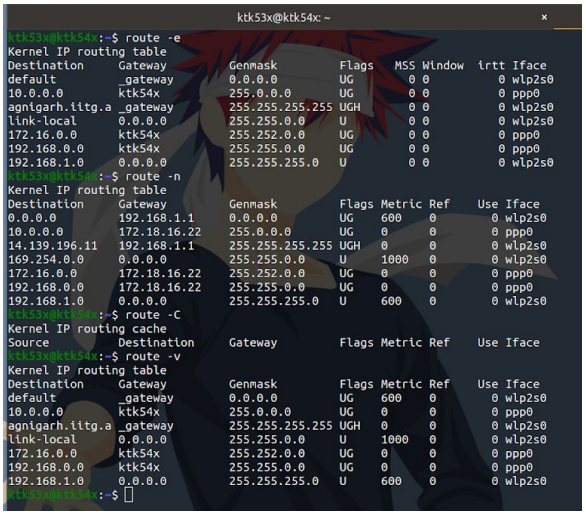
Ans.4 -

a) The important attributes of ifconfig command are as follows:
1- Network interface: A network interface is a software interface to networking hardware. Eg: lo (loopback interface), wlp2s0 (wireless connection), eth0 (ethernet), ppp0 etc
2- IP address both (IPv4 and IPv6), **netmask** and **broadcast** of the interface
3- RX = number of packets received and errors at the time of command execution
4- TX = number of packets transmitted and errors at the time of command execution
5- MTU = maximum transmission unit is the largest packet or frame size that can be sent in a packet- or frame-based network such as the internet

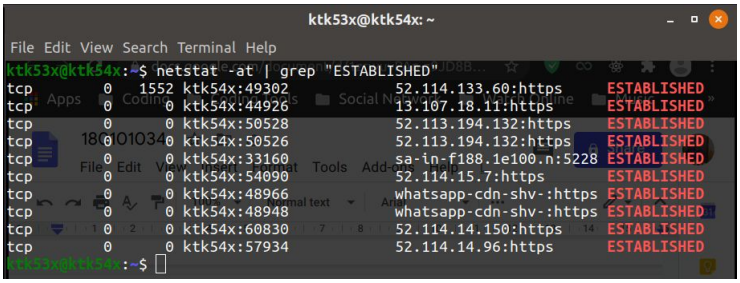
b) interface down: causes the interface to shut down
Interface up: causes the interface to be activated
mtu N: to set the mtu of an interface
-a: display all interface (even if down)

c) Route command is used to work with IP routing table. Which store the routing info of some static routes along with the **metric** (cost associated with that route).
We have some **destination routes** along with **genmask**, which are the netmask of destination network, **gateway**, which is the location of the next router one hop away, and **interface** of the network.
Each route has **flags** such as U (route is up), H (target is host) and G(use gateway) indicating the status of the routes

d) -e : this option is used to display all parameters of the routing table
-n : it shows numeric address instead of giving symbolic host names
-C : to operate on kernel's routing cache
-v : it gives more verbose description



Ans.5 -
a) Netstat prints information about the Linux networking subsystem. Netstat command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.
b) netstat -at | grep "ESTABLISHED"



c) netstat -r shows the kernels routing table. It has following fields in the output

1- **Destination**: destination ip address
2- **Genmask**: network mask of the destination
3- **Gateway**: next router where to hop
4- **Iface**: interface of the network
5- **MSS**: maximum segment size for the TCP connections
6- **Window**: default window size of TCP connection over this route

d) netstat -i | tail -n +3 | wc -l

e) netstat -aus

f) The loopback device is a special, virtual network interface that your computer uses to communicate with itself. It is mostly used as a diagnostic tool and troubleshooting. It helps to communicate with servers located in the same machine itself.

Ans.6 -

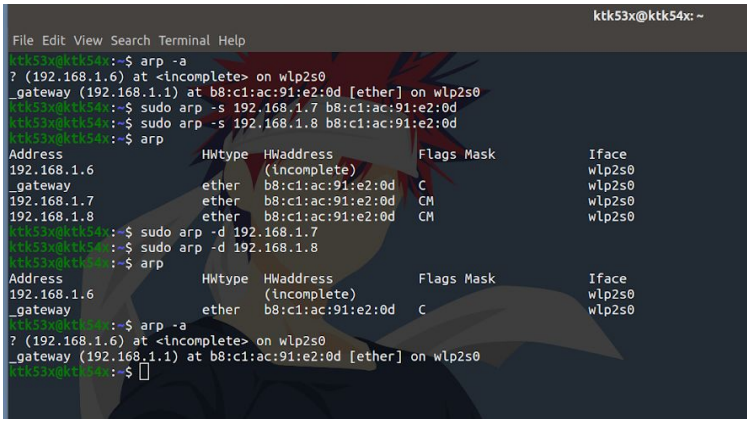
a) Traceroute tracks the route packets taken from an IP network on their way to given host. It is useful if you want to know about the route and about all the hops that a packet takes.
Command: sudo traceroute -I ip

IP-1 - www.codeforces.com (81.27.240.126) **Russia**
IP-2 - www.facebook.com (157.240.198.35) **Germany**
IP-3 - www.geeksforgeeks.org (23.55.108.41) **United Kingdom**
IP-4 - 106.215.61.164 **New Delh**i
IP-5 - www.leetcode.com (172.67.138.83) **United States**
IP-6 - kissanime.ru (104.31.74.190) **Canada**

TIME OF EXECUTION	IP-1	IP-2	IP-3	IP-4	IP-5	IP-6
Sep 17 20:58:52 2020	11	7	5	1	6	6
Sep 17 16:27:37 2020	11	7	4	1	5	5
Sep 17 13:39:19 2020	11	7	5	1	6	6

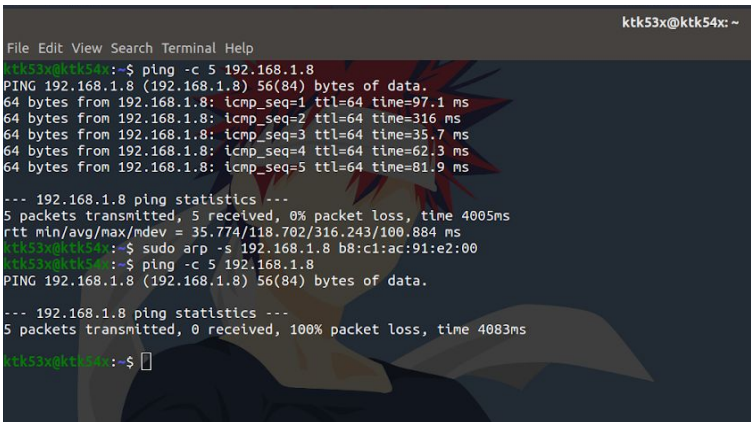
b) __gateway(192.168.1.1), abts-north-static-070.127.176.122.airtelbroadband.in (122.176.127.70) were common in all except **IP-4** and 125.19.38.109 (125.19.38.109) were common in **IP-1,IP-2,IP-3,IP-6**
c) Yes route to (172.67.138.83) changes at different times of the day probably due to change in cross traffic and congestion in different routes.
d) Yes the default tracerouting send udp datagrams to “unlikely” destination ports which normally reply with icmp unreach port as final response. Also in modern network environments firewalls filter these requests. When executing traceroute without -I at (81.27.240.126), it failed because its firewall didn’t allow those udp datagrams.
e) Traceroute sends udp datagram while ping uses icmp so if a router is configured to block icmp echo packets then ping will fail but traceroute might succeed.

Ans.7 -
a) ARP stands for Address Resolution Protocol. The primary function of this protocol is to resolve the IP address of a system to its mac address. Arp manipulates or displays the kernel's IPv4 network neighbour cache.
The command arp -e is used to see the full ARP table.
The ARP table contains the **host IP address, HardWareType**, **MAC address or HWaddress** which is a hardware identification number manufactured into each network card that uniquely identifies each device on a network, **Flags** such as C for complete and M for permanent entries and the **interface network**
b) To add and entry into the ARP table: arp -s address hw_addr
To delete an entry from the ARP table: arp -d address



c) No if the subnet is not connected, It will result in SIOCSARP: Network is unreachable
We can add only for connected reachable subnet.

d) Due to different MAC address in ARP table the requests are forwarded to wrong network hardware leading to loss of packets (which are rejected by routers on that network because of unexpected IP headers in the packets)



Ans.8 -

a) sudo nmap -sn 172.16.114.128/25 (ip_addr/mask)

b) sudo nmap -sA -T4 172.16.114.150

c) The following distribution occurred, the number of online hosts remained nearly the same.