NAME: MAYANK KUMAR AGRAWAL
ROLL NO.: 150101033

1)

a) ping -c count, count echo requests sent
b) ping -i t, t second wait between two consecutive ping requests
c) ping -l ,maximum 3 packets can be sent
d) ping -s x, ping request of size x, for packet of size 64kb total sent is 64+8=72byte

2)
using my own cellular network i have pinged following servers:

SERVER NAME	PING TIME	RTT	PACKET LOSS %
COINDELTA.COM (SERVER IN INDIA)	11:00AM	83.22	0
	5:00 PM	81.567	0
	10:00 PM	90.12	0
13.112.63.251 (TOKYO)	11:00AM	119.712	0
	5:00 PM	130.213	0
	10:00 PM	145.214	0
WIKIPEDIA.ORG (SERVER IN FLORIDA.U.S.)	11:00AM	229.276	0
	5:00 PM	235.541	0
	10:00 PM	240.524	0
209.85.202.138 GOOGLE.COM (CALIFORNIA,US)	11:00AM	430.637	0
	5:00 PM	447.909	0
	10:00 PM	480.366	0
TINDER.COM (US)	11:00AM	137.811	0
	5:00 PM	126.16	0
	10:00 PM	150.15	0

Packet Loss: There was packet loss in some of the cases , it is caused due to:

i) Network congestion

ii) A TCP connection may uses packet loss to reduce throughput.

iii) Packet loss can be caused by weak signals due to distance or multi-path fading , faulty networking hardware.

RTT and Geographic Distance: RTT is posttively related to geographical distance, but it is less as compared to linearized distance.For a given range of linearized distance of a path the RTT variation is much smaller than its variation for the same range of geographic distance between end hosts. So RTTs are weakly correlated to geographic distance

Relation of RTT and packet size:

Host used is 209.85.202.138 GOOGLE.COM server in (CALIFORNIA,US).

Varying packet size from 64bytes to 1500 bytes as above 1500 bytes the ISP itself was rejecting the requests. I couldn’t generalize any trend from it but we can see some increase in time taken (see the table below). Thus packet size and ping latency are weakly related.

SIZE	64	256	448	640	832	1024	1216	1408	1600
AVG RTT	452.725	487.954	475.996	477.170	488.163	483.460	502.327	481.470	rejected

3)

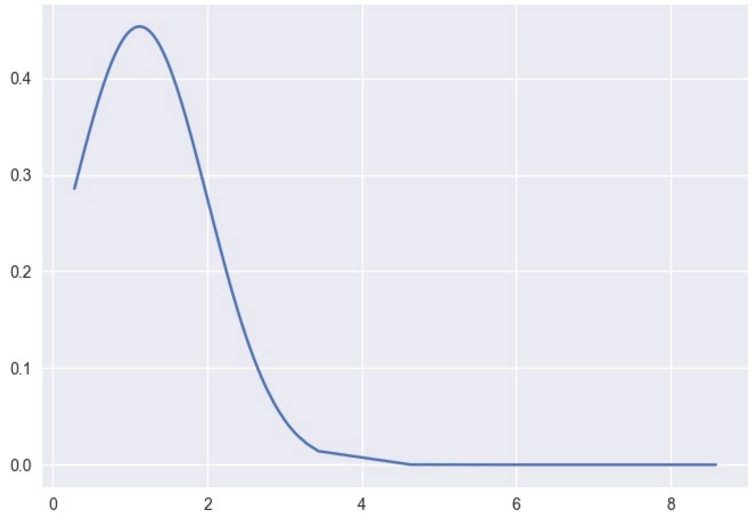
The ip address i have used is 202.141.80.14

command: = ping -n 202.141.80.14 -c 1000 (stored all the rtt’s in a file and used a python script to plot the normal distribution)

packet loss rate =0

rtt min/avg/max/mdev = 0.276/1.118/8.598/0.879 ms

The normal distribution is as follows (x-axis dentoes the acg RTT’s)

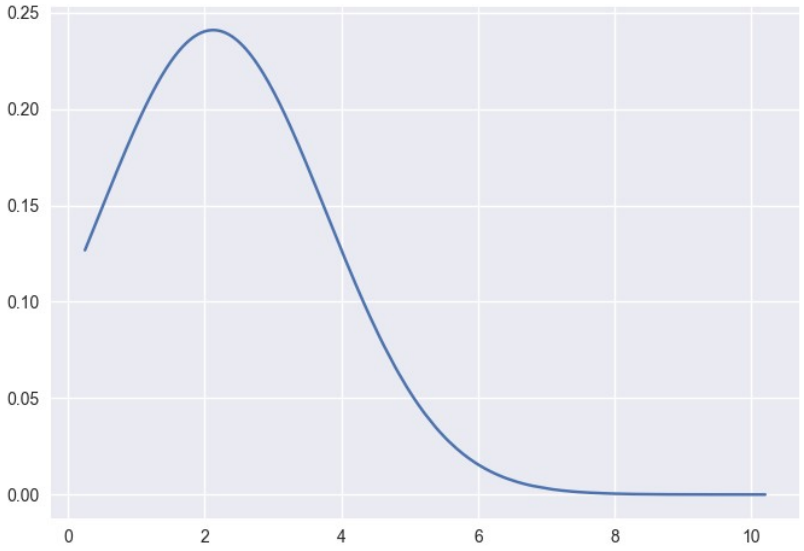


command: = ping -p ff00 202.141.80.14 -c 1000 (stored all the rtt’s in a file and used a python script to plot the normal distribution)

packet loss rate =0

rtt min/avg/max/mdev = 0.247/2.127/10.273/1.661 ms

The normal distribution is as follows (x-axis dentoes the acg RTT's)



Reason of difference:

ping -n does the DNS look up happens for the first time only and saves it for next requests thus saving some time in DNS resolution, hence the ping latency is reduced. But in the case of ping -p case the packets are over-written with ff00 and it takes more time as every time the DNS is resolved to get the ip address. We can see this from the shifted peak of the distribution in second case as compared to the first one.

4) **IFCONFIG:** It is used to configure, or view the configuration of, a network interface. ifconfig stands for "interface configuration". The "ifconfig" command is used for displaying current network configuration information, setting up an ip address, netmask or broadcast address to an network interface, creating an alias for network interface, setting up hardware address and enable or disable network interfaces. It is used to view and change the configuration of the network interfaces on your system. Running the command displays information about all network interfaces currently in operation. When a network interface is active, it can send and receive data; when it is inactive, it is not able to transmit or receive. You can use ifconfig to change the status of a network interface from inactive to active, or vice-versa.

To enable an inactive interface, provide ifconfig with the interface name followed by the keyword up. Terms in ouput of ifconfig commands are following:

- Link Encap: This represents the frame type associated with this interface. Ex. Ethernet,wifi etc.
- Hwadd: This represents the hardware address of the interface commonly known as 'MAC address'.

- inet addr: IPv4 address assigned to the interface.
- Bcast: Broadcast address of the network associated with the interface.
- Mask: Network mask associated with the interface.
- UP: This flag indicates that the network interface is configured to be enabled.
- BROADCAST: can to handle broadcast packets, important for obtaining the IP address via DHCP server.
- RUNNING: network interface is running or operational.
- MULTICAST: handle multicast packets.
- Interrupt: Information about the Interface Request (IRQ) value assigned to this interface.
- Base address: The I/O base address associated with this interface.
- RX: Related to received packets.
- TX: Related to transmitted packets

ROUTE: Route manipulates the kernel's IP routing tables. Its primary use is to set up static routes to specific hosts or networks via an interface after it has been configured with the ifconfig program. When the add or del options are used, route modifies the routing tables. Without these options, route displays the current contents of the routing tables.Options:

-target - the destination network or host. You can provide IP addresses in dotted decimal or host/network names**.**

-net - the target is a network.

-host - the target is a host.

-**reject -** install a blocking route, which will force a route lookup to fail. This is for example used to mask out networks before using the default route. This is NOT for firewalling.

OUTPUT:

Destination : The destination network or destination host.

Gateway : 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.

Flags: Possible flags include

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) **NETSTAT (*NETWORK STATISTICS*):**

It is a command-line network utility tool that displays network connections for the Transmission Control Protocol (both incoming and outgoing), routing tables, and a number of network interface (network interface controller or software-defined network interface) and network protocol statistics. It is used for finding problems in the network and to determine the amount of traffic on the network as a performance measurement. Displays *very* detailed information about how your computer is communicating with other computers or network devices. Netstat provides statistics for the following:

- The name of the protocol (TCP or UDP).
- Local Address: The IP address of the local computer and the port number being used.

- Foreign Address: The IP address and port number of the remote computer to which the socket is connected.
- Indicates the state of a TCP connection. Example: CLOSE_WAIT, CLOSED, ESTABLISHED, FIN_WAIT_1, FIN_WAIT_2, LAST_ACK, etc.

Execute the netstat command alone to show a relatively simple list of all active TCP connections which, for each one, will show the local IP address (your computer), the foreign IP address (the other computer or network device), along with their respective port numbers, as well as the TCP state.

netstat -t: for all tcp connections or **netstat -anp -tcp** to show currently active tcp connections or **netstat -t -p** with name of process uisng the connection.

netstat -r : Execute netstat with -r to show the IP routing table. This is the same as using the route command to execute route print. Output attributes Destination (Destination address of the connection) , Gateway , Genmask , Flags**,** MSS **(**Default maximum segment size for TCP connections over this route.), Window (Default window size for TCP connections over this route.)**,** Irtt (Initial RTT (Round Trip Time).

netstat -i : This option is used to check network interface status.
LoopBack Interface : The loopback address (lo0) has several uses, depending on the particular Junos feature being configured. It can perform the following functions:

- Device identification—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.

<u>6) HOP-COUNT:</u>

1) A hop is a computer networking term that refers to the number of routers that a packet (a portion of data) passes through from its source to its destination.

Sometimes a hop is counted when a packet passes through other hardware on a network, like switches, access points, and repeaters. This isn't always the case and it depends on what role those devices are playing on the network and how they're configured.

	COINDELTA.COM	13.112.63.251	WIKIPEDIA.ORG	209.85.202.138	TINDER.COM
03:00 AM	8	21	NO PATH	19	17 then firewall reached
07:00 PM	9	21	NO PATH	17	17 then firewall reached

12:00 PM	8	21	NO PATH	NO PATH	NO PATH

Initial 4 hops to most of the servers were same as it depends on the service i used and The ISP service i used was constant through out the experiment.

Example output of first 4 hops, command: traceroute coindelta.com was

```
HOP1:  192.168.43.1 (192.168.43.1)  5.452 ms  4.813 ms  4.803 ms

HOP2:  10.50.46.49 (10.50.46.49)  49.095 ms  49.076 ms  49.071 ms

HOP3:  10.206.254.129 (10.206.254.129)  45.133 ms *

HOP4:  10.206.252.213 (10.206.252.213)  48.848 ms * *
```

these 4 hops were constantly same.

2) yes the route to same hop may change at different times of day (we can also this in the case of coindelta.com). The trace hops are not just different "hops" but indeed totally different events, at different times, and possibly under different conditions.Traceroute sends a packet with at TTL of 1 and sees how long it takes for an answer to arrive. The program repeats this three times to account for some variation that is possible. Then, traceroute sends a packet with a TTL of 2 (and then 3, and 4, etc.) and sees how long it takes for an answer to arrive. In the mean time, the load on the first router may have lowered, so your packets are actually forwarded faster.There is no way of going back in time, so you can't change the fact that a second ago it took a bit longer for your packets to make it through. You're probing at two different times, so all you can get is a reasonable estimate. Yes, generally, the time from hop to hop should gradually increase, but it need not.

3) Some cases in which hop was unresponsive(*) and unreachable(!H) pointed to no path route. * means that your machine received no response. And !H means that your machine received ICMP message "destination host unreachable" from the host indicated in the traceroute output. A machine normally sends "destination host unreachable" when it cannot send the IP packet to the network. This could happen when there is no route to the destination or The next hop IP address cannot be resolved.

4) Yes we can find a route to a host if ping isn’t working. Ping is straight ICMP from point A to point B, that traverses networks via routing rules. Traceroute works very different, even though it uses ICMP.Traceroute works by targeting the final hop, but limiting the TTL and waiting for a time exceeded message, and then increasing it by one for the next iteration. Therefore, the response it gets is not an ICMP echo reply to the ICMP echo request from the host along the way, but a time exceeded message from that host - so even though it is using ICMP, it is using it in a very different way.

7)

The command **arp**: arp with no mode specifier will print the current content of the table. It is possible to limit the number of entries printed, by specifying an hardware address type, interface name or host address. First col. ‘Address’ and ‘Hwaddr’ shows the IP address mapped to the MAC address by the machine. The ‘Iface’ col shows the interface name(alias) whose IP/MAC address is mapped. Flag coloumn shows the flags used.

The command: **arp -d *ip* / arp -s *ip mac*** ,command is used to delete/add entry with *ip* specified , with root previliges. I*f an ARP entry is not used a specific amount of time called the ARP timeout the entry is removed from the caching table.*

The command: **arp -s address hw_addr**, Manually create an ARP address mapping entry for host hostname with hardware address set to hw_addr class, but for most classes one can assume that the usual presentation can be used.

Time out: In my case it's 60. That means 60 seconds until the entry is removed. Every time the entry is used in the table, the timer for this entry resets to 60 seconds.

We can find out **timeout** using **binary search**. Like we can take max 1000 seconds and advance the system by that value, we can do that by this command

```
use sudo cat /proc/sys/net/ipv4/neigh/default/gc_stale_time
```

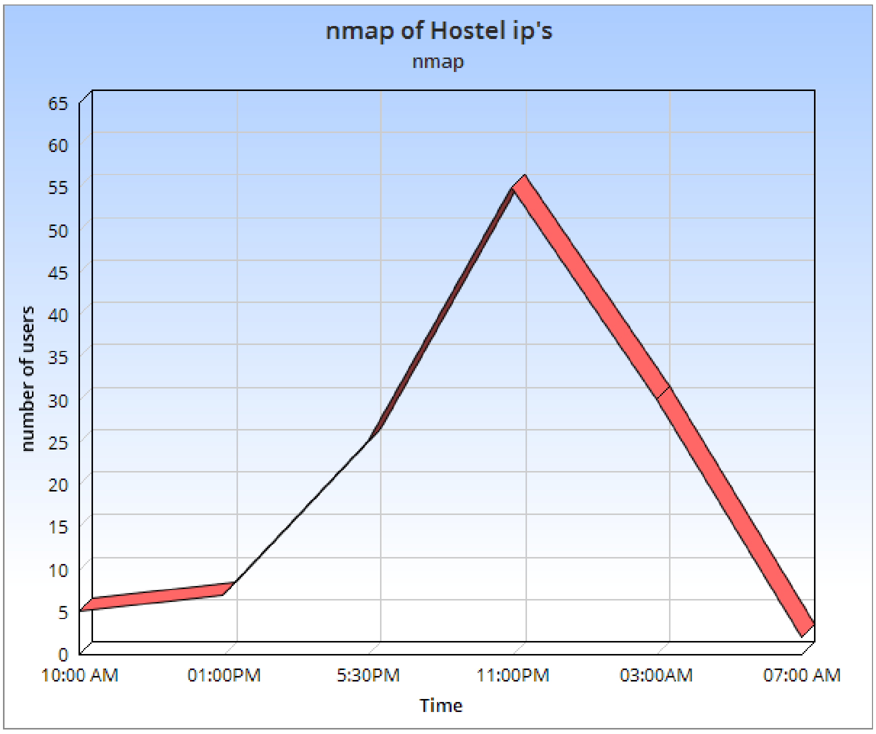
and change timeout values by hit and trial using binary search.The dynamic hops will be affected by this file.

Two IP having same MAC : It depend on how the routers and systems on the network are configured. Sometimes you get into "races" where each computer attempts to register itself with the router, and any traffic coming to the machine can get lost since packet A will go to your machine, the other machine will register, so packet B will go there. Things can start bouncing back and forth. You can start seeing unreachable host errors due to the collisions as well. The results really do vary depending on when the duplicate machine is coming online and how the current infrastructure is setup to handle such items.

8)

doing nmap for my hostel lobby using command :

nmap -n -sP 10.3.3.0/70


nmap of Hostel ip's
nmap
number of users
10:00 AM
01:00PM
5:30PM
11:00PM
03:00AM
07:00 AM
Time