Name: Ankit Kumar Singh
Roll No. 150101086

Networks Lab Assignment 1
Date : 28/01/2018

Sol.1. After Exploring enough on Ping command. Following can be said:

a) '**-c <count>**' option is required to specify the number of echo requests to send with ping. This option stop after sending count ECHO_REQUEST packets.

b) '**-i <interval_length(in secs)>**' is used to set time interval between two successive ping ECHO_REQUESTs. The default is to wait for one second between each packet normally, or not to wait in flood mode. Only super-user may set interval to values less than 0.2 seconds.

c) '**-l <no_of_packets_to_send>**' is used to send ECHO_REQUEST packets to the destination one after another without waiting for a reply. A Normal User can send at most 3 such packets. Super user can set this value to more than 3.

d) '**-s <packet_Size(in bytes)>**' is command to set ECHO_REQUEST packet size.
If Packet Size = 64 bytes

Then **Total Packet Size = 92** (20 bytes IP header + 8 bytes ICMP header + 64 byte data(Packet Size)).

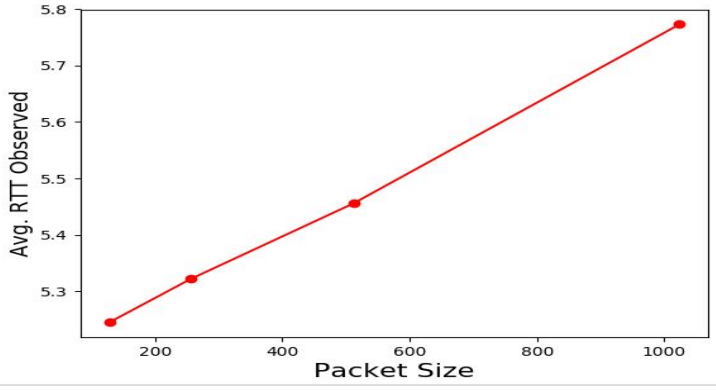
Sol. 2. a) Following tool was used to ping mentioned IP mentioned in table.
http://www.spfld.com/ping.html server located in **northern New Jersey.**

Host	RTT(5:46pm)	RTT(10.12pm)	RTT(9.26am)	Avg. RTT	Approx. Distance*
google.com	3.651	4.795	3.741	4.0623	2,886.3 mi
yahoo.com	76.307	23.512	41.516	47.1117	2,886.3 mi
facebook.com	12.640	13.457	12.743	12.947	2,886.3 mi
cloudfront.net	5.690	5.521	5.448	5.553	2,802.2 mi
reflux.in	31.623	31.300	31.582	31.5017	374.9 mi

*** From ping server. Also RTTs are in ms and are avg RTT observed. Col5 is avg of Col 4,2&3.**

Among the hosts chosen there is no case of packet loss. Even it there is some packet lost it may be because of network congestion or faulty server or firewall restrictions or number of hops on the route may be large compared to the ttl value thus the packet expires before it reaches designation.(**100% packet loss was observed on iitg.ernet.in**).

Also it can be observed that avg RTT is related to Geo. Distance. But the dependence is not strong(weakly correlated). It mainly depends on the route that the packet takes to reach the host, which is decided dynamically on each network establishment.



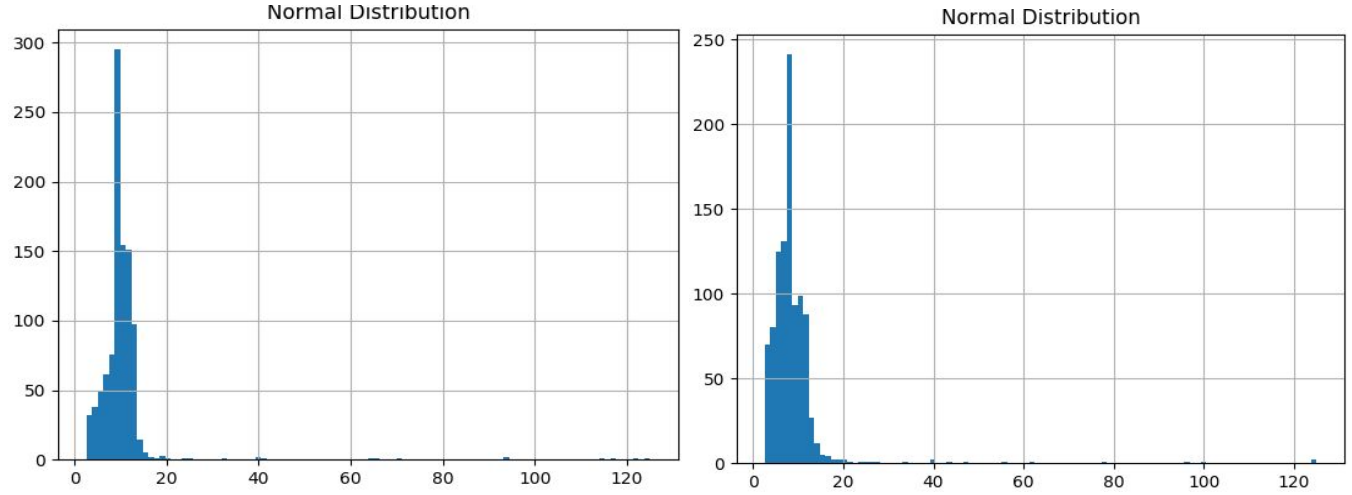
google.com was pinged for different file sizes and above graph was obtained(100% packet loss at packet size 2048 , same for facebook.com) . This shows that **more the packet size more is the RTT** given the other conditions remain almost identical. Also It **depends on the time of the day,** as during peak time when network is busy time taken will be more.

Sol. 3. IP chosen for the purpose: 202.141.80.36

Attributes	ping -n <IP Address>	ping -p ff00 <IP Address>
Packet Rate Loss	0.5%	0.2%
Minimum Latency	2.504 ms	2.486 ms

Maximum Latency	125.124 ms	125.474 ms
Mean Latency	9.348 ms	8.089 ms
Median Latency	9.350 ms	8.074128 ms

c) The normal distribution can be visualized as follows for **-n** and **-p ff00** respectively :



d) The major difference observed between 2 scenarios is that packet loss in case of **-n** is larger. Also the standard deviation for **-p ff00** is larger since same data pattern is send, hence chance to get same RTT increases(almost identical packets).

Sol 4.

```
enp7s0    Link encap:Ethernet  HWaddr 74:e6:e2:17:0b:06
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:446722 errors:0 dropped:390 overruns:0 frame:0
          TX packets:363160 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:178906777 (178.9 MB)  TX bytes:64816104 (64.8 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:154153 errors:0 dropped:0 overruns:0 frame:0
          TX packets:154153 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:13072078 (13.0 MB)  TX bytes:13072078 (13.0 MB)

wlp6s0    Link encap:Ethernet  HWaddr 4c:bb:58:2c:23:87
          inet addr:10.150.36.48  Bcast:10.150.39.255  Mask:255.255.248.0
          inet6 addr: fe80::6987:9ca0:4b64:44b6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:963944 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1213962 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:962600464 (962.6 MB)  TX bytes:257929717 (257.9 MB)
```

i. **Enp7s0 : Name of the interface device. Used for Wired Lan Connection**

Link encap:Ethernet : This denotes that it is a Ethernet Related Device.

HWaddr 74:e6:e2:17:0b:06: MAC address of the NIC responsible for wired connection.

The first half part of this address will contain the vendor id which is common for all the NICs manufactured by the same manufacturer and the rest will denote the device Id which should not be the same for any two devices manufactured at the same place.

UP : This flag causes the interface to be activated. It is implicitly specified if an address is assigned to the interface.

BROADCAST : This says that this interface supports broadcasting, which is required to get an IP address via DHCP.

MULTICAST : Interface supports multicast. That is it can packets send by the interface can be watched by all nodes listening to it.

MTU:1500 : Maximum Transmission Unit is the size of each packet received by the Ethernet card.Default value is 1500. Though you can change the value by passing the necessary option to the ifconfig command. Setting this to a higher value could hazard packet fragmentation or buffer overflows.for SLIP interfaces, this is 296.

Metric: 1 : This option may be used to assign a metric value to the routing table entry created for the interface. This metric is used by the Routing Information Protocol (RIP) to build routing tables for the network. The default metric used by ifconfig is a value of zero. If you don't run a RIP daemon, you don't need this option at all; if you do, you will rarely need to change the metric value.

RX packets:446722 errors:0 dropped:390 overruns:0 frame:0 : This shows the number of received packets , count of packets with errors, dropped packets etc. Since dropped packet is positive hence it may imply congestion in the network.

TX packets:363160 errors:0 dropped:0 overruns:0 carrier:0 : This shows the number of transmitted packets , count of packets with errors, dropped packets etc.

Collisions 0: It indicates the number of packets that are colliding while traversing the network. If it is greater than 0 it indicates network congestion.

txqueuelen :1 - This denotes the length of the transmit queue of the device. It is set to smaller values for slower devices with a high latency such as modem links and ISDN.

RX bytes:178906777 (178.9 MB) TX bytes:64816104 (64.8 MB) : It shows the received and transmitted bytes on interface.

2. **lo:** Loopback device interface used to virtually refer the machine itself. Used for various debugging purposes.

Link encap:Local Loopback : Indicates it is a loopback device.

inet addr:127.0.0.1 Mask:255.0.0.0 : This is the IP used by the machine to refer itself. And Mask value is the Subnet mask value used while referring

Scope: Host Indicates that the interface is a part of network and used to refer itself.

3. wlp6s0 : Link encap:Ethernet Ethernet Related Device.

HWaddr 4c:bb:58:2c:23:87 MAC address of the wireless hardware/ card.

inet addr:10.150.36.48 indicates the IPv4 address of the machine alloted in the network()

Bcast:10.150.39.255 - denotes the broadcast address of the subnet.

Mask:255.255.248.0: is the network mask which we passed using the netmask option

inet6 addr: fe80::6987:9ca0:4b64:44b6/64 : denotes the ipv6 address allocated to the device in the network(as per IPv6 protocol)

Scope:Link: Indicates that the interface is connected to the local network**.**

b) Various Options available in *route* are:

-A family : use the specified address family (eg 'inet't).

-F operate on the kernel's FIB (Forwarding Information Base) routing table. This is the default.

-C operate on the kernel routing cache.

-v select verbose operation.

-n show numerical addresses instead of trying to determine symbolic host names. This is useful if you are trying to determine why the route to your nameserver has vanished.

-e use ***netstat****(8)*-format for displaying the routing table. **-ee** will generate a very long line with all parameters from the routing table.

del delete a route.

add add a new route.

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.

netmask NM when adding a network route, the netmask to be used.

gw GW route packets via a gateway. **NOTE:** The specified gateway must be reachable first. This usually means that you have to set up a static route to the gateway beforehand. If you specify the address of one of your local interfaces, it will be used to decide about the interface to which the packets should be routed to. This is a BSDism compatibility hack.

metric M set the metric field in the routing table (used by routing daemons) to M.

mss M sets MTU (Maximum Transmission Unit) of the route to M bytes. Note that the current implementation of the route command does not allow the option to set the Maximum Segment Size (MSS).

window W set the TCP window size for connections over this route to W bytes. This is typically only used on AX.25 networks and with drivers unable to handle back to back frames.

irtt I set the initial round trip time (irtt) for TCP connections over this route to I milliseconds (1-12000). This is typically only used on AX.25 networks. If omitted the RFC 1122 default of 300ms is used.

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.

mod, dyn, reinstate

install a dynamic or modified route. These flags are for diagnostic purposes, and are generally only set by routing daemons.

dev If force the route to be associated with the specified device, as the kernel will otherwise try to determine the device on its own (by checking already existing routes and device specifications, and where the route is added to). In most normal networks you won't need this.

If **dev If** is the last option on the command line, the word **dev** may be omitted, as it's the default. Otherwise the order of the route modifiers (metric - netmask - gw - dev) doesn't matter.

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         172.16.112.1    0.0.0.0         UG    100    0        0 eno1
link-local      *               255.255.0.0     U     1000   0        0 eno1
172.16.112.1    *               255.255.255.255 UH    100    0        0 eno1
172.16.114.128  *               255.255.255.128 U     100    0        0 eno1
```

Fields in the above table are :

1. **Destination** The destination network or destination host.
2. **Gateway** The gateway address or '*' if none 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** 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. **Metric** The 'distance' to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.
6. **Ref** Number of references to this route. (Not used in the Linux kernel.)
7. **Use** Count of lookups for the route. Depending on the use of -F and -C this will be either route cache misses (-F) or hits (-C).
8. **Iface** Interface to which packets for this route will be sent.

Sol 5. netstat command, which stands for "network statistics", shows information about your network including statistics on connections to and from others on the network, used network interfaces, services, ports, and routing tables.

a) netstat -t or **--tcp** is used to show all the TCP connections established.

```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0    566 10.150.36.48:60980     172.16.115.94:3128      ESTABLISHED
tcp        0      0 10.150.36.48:34404     172.16.115.94:3128      ESTABLISHED
tcp        0  23528 10.150.36.48:33106     172.16.115.94:3128      ESTABLISHED
tcp        0      1 10.150.36.48:44772     10.3.3.64:http          SYN_SENT
tcp        0      0 10.150.36.48:37334     172.16.115.94:3128      TIME_WAIT
tcp        0      0 10.150.36.48:35874     172.16.115.94:3128      ESTABLISHED
tcp        0      1 10.150.36.48:52520     10.3.3.63:http          SYN_SENT
tcp        0      0 10.150.36.48:34042     172.16.115.94:3128      ESTABLISHED
tcp        0      1 10.150.36.48:53412     10.3.3.59:http          SYN_SENT
```

Various Fields in the Output are:

Proto : The protocol (tcp, udp, raw) used by the socket.

Recv-Q : The count of bytes not copied by the user program connected to this socket.

Send-Q: The count of bytes not acknowledged by the remote host.

Local Address: Address and port number of the local end of the socket. Unless the --numeric (-n) option is specified, the socket address is resolved to its canonical host name (FQDN), and the port number is translated into the corresponding service name.

Foreign Address: Address and port number of the remote end of the socket. Analogous to "Local Address."

State: The state of the socket. Since there are no states in raw mode and usually no states used in UDP, this column may be left blank. Normally this can be one of several values:

ESTABLISHED : The socket has an established connection.

SYN_SENT : The socket is actively attempting to establish a connection.

SYN_RECV : A connection request has been received from the network.

FIN_WAIT1 : The socket is closed, and the connection is shutting down.

FIN_WAIT2 : Connection is closed, and the socket is waiting for a shutdown from the remote end.

TIME_WAIT : The socket is waiting after close to handle packets still in the network.

CLOSE The socket is not being used.

CLOSE_WAIT: The remote end has shut down, waiting for the socket to close.

LAST_ACK : The remote end has shut down, and the socket is closed. Waiting for acknowledgement.

LISTEN : The socket is listening for incoming connections. Such sockets are not included in the output unless you specify the --listening (-l) or --all (-a) option.

CLOSING Both sockets are shut down but we still don't have all our data sent.

b) netstat -r Display the kernel routing tables. Output is same as the route command in Ques 4.b

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         172.16.112.1    0.0.0.0         UG        0 0          0 eno1
link-local      *               255.255.0.0     U         0 0          0 eno1
172.16.112.1    *               255.255.255.255 UH        0 0          0 eno1
172.16.114.128  *               255.255.255.128 U         0 0          0 eno1
```

Destination, Genmask, Gateway, Flags, Iface have same meaning and domain as for the **route** command. Other Fields are as follows:

MSS : TCP Maximum Segment Size (MSS) for connections over this route.The default is the device MTU minus headers, or a lower MTU when path mtu discovery occurred.

Window: TCP window size for connections over this route**.**

Irtt : initial round trip time (irtt) for TCP connections over this route.Typically only used on AX.25 networks.

c) netstat -ie shows the complete Kernel Interface table which can also be used to deduce which host is up. Also it shows the list of all network interfaces.

Number of interfaces : 3(enp7s0 , lo, wlp6s0)

d) The **loopback device** is a special, virtual network interface that your computer uses 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.

Sol. 6. a)

Host	HC(5:46pm)	HC(10.12pm)	HC(9.26am)
google.com	11	11	11
yahoo.com	10	10	10
facebook.com	8	8	8
d3373zkzjyplpu.cloudfront.net	12	12	12
reflux.in	18	18	18

***HC = Hops Count**

Yes common hops were observed in the facebook.com and cloudfront.net. Infact 4 hops were common.

Also they had one hop common with yahoo.com and reflux.in.

b) It was not observed any change in the routes taken. But the route can surely change with time, it depends on the circuit or path which is available for connection establishment.

c) When a different tool(ping.eu) was used, the tracert to reflux.in ended after 30 hops. It may be because it reached a firewall that does not respond to tracert requests.

d) It all has to do with how tracert works. Ping is straight ICMP from point A to point B, that traverses networks via routing rules. Tracert works very different, even though it uses ICMP. Tracert 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.

Sol.7. ARP

a) **arp -e** is used to show full ARP table of the machine in linux style. And **arp -a** is used to show it in BSD style.

Columns in arp table(linux style) are :

i. **Address :** Shows the IP address of the machines recently connected.

ii. **HWtype :** This shows the type of hardware generally it is ether, but it can also be ARCnet (arcnet) , PROnet (pronet) , AX.25 (ax25) and NET/ROM (netrom)

iii. **HWaddress :** MAC address corresponding to the IP address. Thus maintaining the IP and MAC mapping useful for routing protocol.

iv. **Flags Mask :** It can have one of the following value: C (complete), M (permanent), and P (publish).

v. **Iface :** Denotes the interface name of the interface to which the connection was made.

b) If you try to add/delete an entry from ARP table, you need to have the Root or netadmin privilege. Normal users can't do this.

ADD : arp -s address hw_addr is used to set up a new table entry.

DELETE : arp -d <address> will delete a ARP table entry. The entry is found by IP address. But the entry would not be removed from the arp table after this. This will change its hardware address to a sign of <incomplete> instead.

MODIFY : delete , wait for the cache to get clear and then add with the changed value.

After entering entries in ARP table.

Address	HWtype	HWaddress	Flags Mask	Iface
10.150.32.12	ether	aa:dd:dd:ee:dd:00	CM	wlp6s0
10.150.32.1	ether	00:25:b4:d9:f7:c0	C	wlp6s0
10.150.33.214	ether	d4:61:9d:28:0d:ee	C	wlp6s0
10.150.32.24	ether	aa:dd:dd:ee:dd:01	CM	wlp6s0

c) Entries stay cached in the ARP table for 60 sec(for my PC).This time may vary for different machines. This value can be changed.

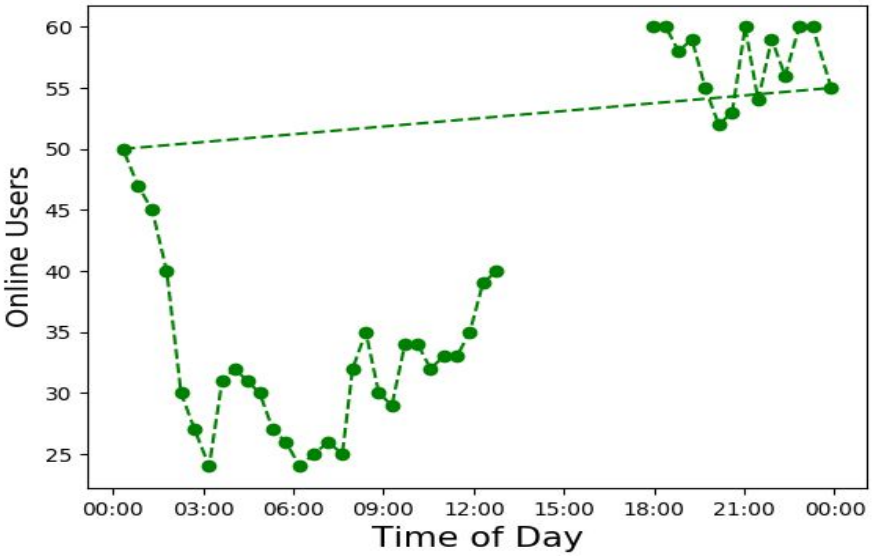
Method to approximately get this value : Guess any value for timeout say 30min. Now connect to any ip address and then increase the system time by 30 mins. If the entry is deleted ,try with half the value else try with double value.(Binary searching the value and thus minimizing the range.)

If same entry are given with different MAC address then the behaviour will be ambiguous. It can send to either of the device but packets will be sent to one device only.Or No machine can receive the packet(Packet Loss)

Sol. 8. Local network analysis

Subnet Range Used : 10.3.1.11/22

Data from Siang Hostel was collected from 5:45 pm to 1pm day at 30 min interval. Following plot is observed:



* Last and the first point are joined because of the continuity in time. To be viewed starting from 6:00 pm.

Following can be observed from the plot:

1. At evening after academic hours i.e 5-12 the number of users is maximum.
2. Online users decreases from 12 midnight to 3am(reason may be sleep).
3. Again it increases from 3 till 12 (as and when people start waking up).