CS349 Network Lab Assignment -1

PHOOL CHANDRA (160101051)

ANS 1. (a) '-c' option is required to specify the number of echo request to send with the ping command.
(b) '-i' option is required to set the time interval (in seconds) between two successive ping ECHO_REQUESTs.
(c) 'ping -f <destination IP/URL>' command is used to send **ECHO_REQUEST** packets to the destination one after another without waiting for a reply. A normal user can send only 3 such request, otherwise destination can be flooded with ping requests without waiting any time using **'-f'** option. Alternatively, we can set interval zero with **'-I'** option. A normal user has limit of 200ms.
(d) The command **'ping -s <Packet_Size> <destination IP/URL>'** is used to set the **ECHO_REQUEST** packet size. If packet size is 64 bytes then in actual packet ICMP header will be added of 8 byte and IP header will be added of 20 bytes. So actual size of packet become 92 bytes.

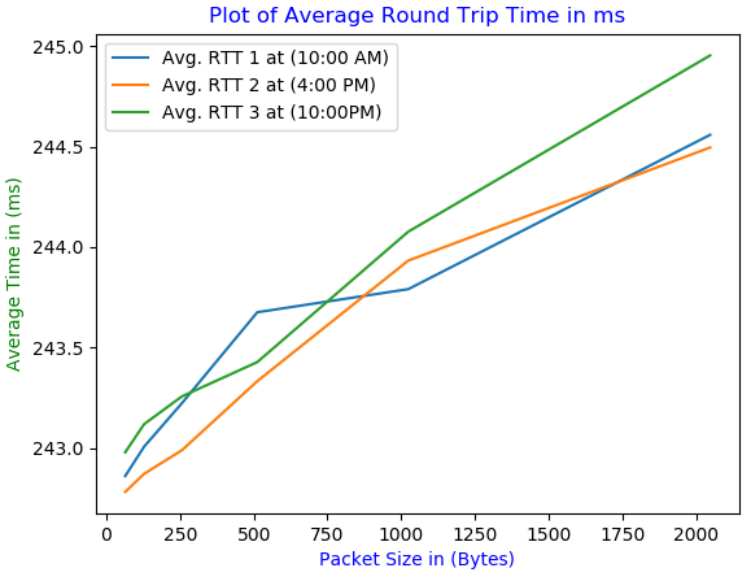
ANS 2: I have taken below data on **21st JAN,** 2018 at **10:00 AM**, **4:00 PM**, **10:00 PM** using http://www.spfld.com/ping.html (**USA server**). I have chosen **flipkart.com** for experiment with packet size from 64 bytes to 2048 bytes. RTT is in milliseconds (ms) and packet size is in bytes.

Destination Host Address	Ip Address	Geographic Location	Avg. RTT1 (ms)	Avg. RTT2 (ms)	Avg. RTT3 (ms)	Total Avg. RTT (ms)
www.iitg.ac.in	14.139.196.22	Guwahati, India	259.786	265.205	273.786	266.259
www.cam.ac.uk	128.232.132.8	Cambridge, UK	99.905	98.305	100.872	99.695
www.flipkart.com	163.53.78.128	Banglore, India	242.867	242.782	242.979	242.876
www.facebook.com	157.240.2.35	Chicago, US	30.162	29.007	30.287	29.819
www.nus.edu.sg	137.132.21.27	Singapore	242.937	241.535	243.117	242.396
		Avg. Round trip times of 5 hosts				

RTT VS DISTANCE : from above table, we can conclude that there exist a strongly positive correlation between the distance and round trip because the server of spfld.com is hosted in USA and the server which are nearby it have smaller Avg. RTT and the hosts which away have larger Avg. RTT . As distance increases, propagation delay increases. The packets have taken large number of hops and have to pass more number of nodes and routers as distance increase. Every node and routers have own processing time so as distance increased significantly resultant processing time of every nodes increases significantly. So, we can say that the

Size (bytes)	64	128	256	512	1024	2048
Avg. RTT1 (ms)	242.867	243.007	243.223	243.676	243.791	244.558
Avg. RTT2 (ms)	242.782	242.872	242.989	243.333	243.933	244.496
Avg. RTT3 (ms)	242.979	243.119	243.257	243.428	244.077	244.954
	Round Trip Time(RTT) vs packet size(bytes)					

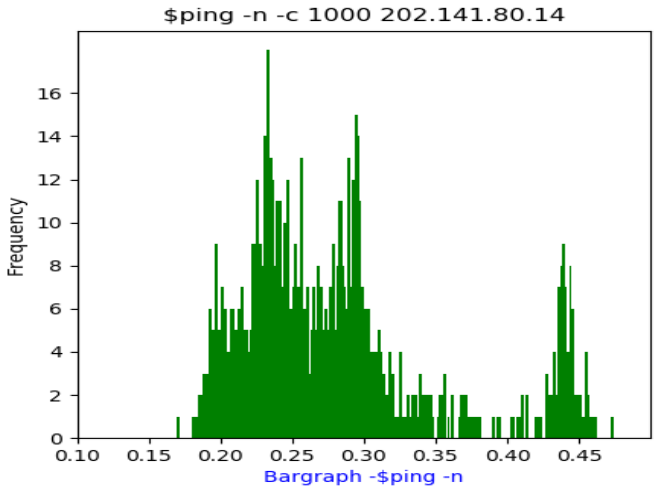
Round Trip Time (RTT) is directly proportional to number of routers and distance of destination host because resultant sum of propagation time and processing time increased. In my experiment, there were no cases of packet loss greater than 0%. But in general packets loss can be greater than 0% because of network congestion and traffic. There may be packets loss due to collision of one packet with other packets in the network. There may be some server can be overloaded in particular time of the day that causes dropping the further packets.There be chance of 100% packet loss sometime because in that case destination drop all the ping ICMP packets because buffer at the intermediate router gets filled up quickly hence losing packets.
RTT VS DAY OF TIME: from second table we can say that RTT is vary in time. In my case at 10:00 PM, Avg, RTT is greater than RTT of another two time. It may be due to increase traffic at that time. At 10:00 PM may be the number of India users increased and USA servers may have heavy loaded at this time due to more uses of internet by users. RTT at 4 PM is lowest.
RTT VS PACKET SIZE: as size of packets increases RTT also increases. The probable reason for could be due to

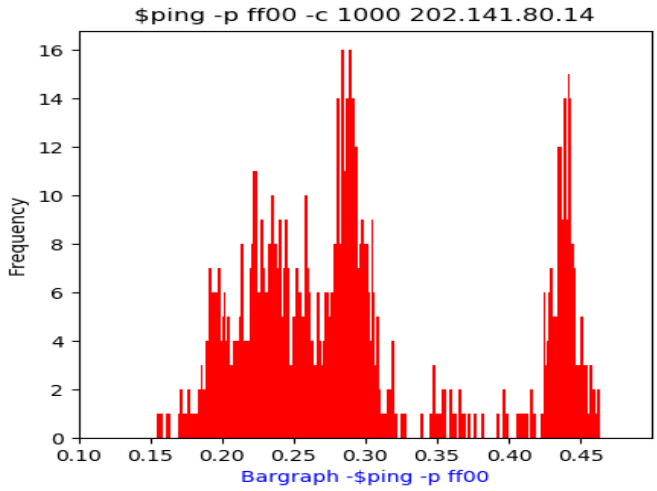


larger packet size, it takes more time for transmission but the measure part of RTT is composed of connection establishment time and transmission time, it depend very less on the packet size though we can see a slight positive correlation . From observation we see that RTT changes for different time of day it may due to the network's high usage and congestion.

ANS 3. (a),(b),(c) Latency in (ms)

Command	Packets sent	Packets Received	Packet Loss Rate	Minimum Latency	Maximum Latency	Mean Latency	Median Latency
$ping –n –c 1000 202.141.80.14	1000	994	0.6%	0.170	0.473	0.279	0.272
$ping –p ff00 –c 1000 202.141.80.14	1000	976	2.4%	0.793	0.492	0.295	0.319



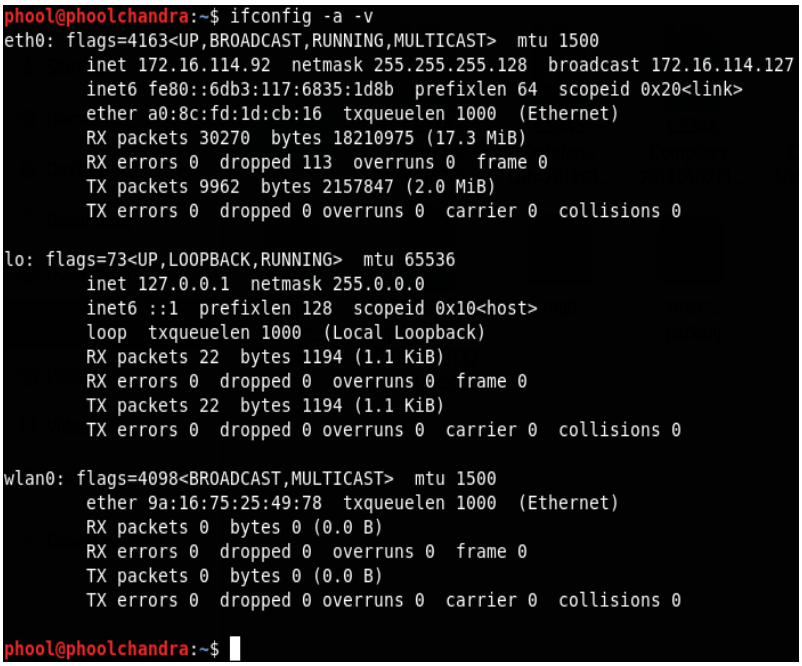


(d) I observed following difference in output of both the commands. First command does not attempt to lookup symbolic names of host addresses when using with **'-n'** , where second command does when using ping with option **'-p ff00'**. First command does not show full hostname while the second command does.So, the mean latency of output of second command is higher than the mean latency of first case.

2. **'-p ff00'** filled the sent package with the pattern 11111100000000 which is useful for diagnosing data-dependent problem in a network. This will cause the problems with clock synchronization of the clocks because

only one transition is present in the padding from 1 or 0. Hence, the clocks are more likely to go out of synchronization. So, in second case we observed that the packets loss is higher in the second case. Due to the data put up in packets in second command Avg. Latency increases as time increases. Latency is weakly positive correlated to packet size.

ANS (4). When I apply the command 'ifconfig -a –v'. I have got the output, which is in image just below.



My Laptop is connected with ethernet wire. In above image ***eth0*** show the connection of ethernet interface ***lo*** show the loopback interface, it is a virtual network device tha is on all system. It is used to access service locally. ***wlan0*** shows the wireless ethernet interface. Local Loopback indicates the interface is local network related. ***BROADCAST***- denotes that the device supports broadcasting which is a necessary characteristic to obtain IP address via DHCP. ***RUNNING*** – denotes the interface is ready to accept data. **MULTICAST** – indicates that the Ethernet interface is support the multicasting which allow a source to send a packet(s) to multiple machines as long as the machine are watching out for that packet. **Inet** – indicate the machine IP4 address. **Inet6**- is the IP6 address and **prefixlen 64** - indicates the subnet size. **ether a0:8c:fd:1d:cb:16** is the MAC address of your PC/Laptop which is unique to each ethernet card. **UP**- this is a flag which indicates that the kernel module related to the ethernet interface has been loaded. **Mtu** is a short form of maximum transmission unit is the size of each packet transferred by the Ethernet card. The value of **mtu** for all ethernet devices by default is set to 1500. **Scopeid**-indicate type of addressing in **inet5**. **RX packets** and **TX packets** denote the total number of packets received and transmitted respectfully. **Rx error** and **TX error** denotes the number of damaged packets received and transferred respectively. **Dropped** denotes the dropped packets it may due to reception or transfer error. **Overruns** this denotes the number of received or transferred packets that experienced data overruns. **Frame :** the number of received or transferred packets that experience frame errors. **Carrier :** the number of transferred packets that experienced loss of carriers. **Collision:** if it has value greater than 0, it means that the packets are colliding while traversing your network. **Txqueuelen:** this denotes the length of the transmit queue of the device. **RX Bytes** denotes the total amount of data has been transferred and **Tx Bytes** - indicates that total amount of data received. In ifconfig command option '**–a'** displays all interface available(both active and inactive), **'-s'** : displays a short list, '**-V':** displays more verbose for error conditions. **'flags=' indicates different types of flags.**

The **'route'** command shows the routing table of the device. **Destination** column identifies the destination network or destination host. The **Gateway** column shows the defined gateway for the specified network. If there is no need of gateway for the network then asterisk(*) appears. **Genmask** column shows the netmask of the destination net. **Flags: U** (route is **UP**) **G** (use gateway). **Metric** is the distance to the target (generally counted in hops). **Ref** is the number of references to this route. **Use:** count of lookups for the route. **Iface** : interface to which packets for this route will be sent. Some of the relevant options of route used are: **'-n'**: show numerical address instead of trying to determine the symbolic host names. **'Del'** : delete a route, **'-v'**: verbose operation, **'add'**: add new route.

```
phool@phoolchandra:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.16.112.1    0.0.0.0         UG    100    0        0 eth0
172.16.112.1    0.0.0.0         255.255.255.255 UH    100    0        0 eth0
172.16.114.0    0.0.0.0         255.255.255.128 U     100    0        0 eth0
phool@phoolchandra:~$
```

ANS 5:

```
phool@phoolchandra:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 phoolchandra:42596      bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 phoolchandra:42620      bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 phoolchandra:42638      bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 phoolchandra:42480      bichitra.iitg.erne:3128 ESTABLISHED
tcp       32      0 phoolchandra:42636      bichitra.iitg.erne:3128 CLOSE_WAIT
```

netstat 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 statics. It is used for finding problems in the network and to determine the amount of traffic on the network as a performance measurement.The **Proto** column tells us if the socket listed is TCP or UPD (protocol). The **Recv-Q** and **Send-Q** columns tell us how much data is in the queue for the socket, waiting to be read(Recv-Q) or sent (Send-Q). The **"Local Address**" and **"Foreign Address"** columns tell us to which host and ports the listed sockets are connected. The local address is the address of the machine on which netstat is running and the foreign address is the target computer. **"State"** column tells the states of the listed sockets.

```
phool@phoolchandra:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 eth0
_gateway        0.0.0.0         255.255.255.255 UH        0 0          0 eth0
172.16.114.0    0.0.0.0         255.255.255.128 U         0 0          0 eth0
phool@phoolchandra:~$
```

in output of the command **$netstat -r. the "Destination"** column indicates the pattern that the destination of a packet is compared to. the " **Gateway**" column tell the computer where to send a packets that matches the destination of the same line. An asterisk (*) here means "send data locally", because the destination is supposed to be the same network. the "**Genmask"** column show the subnet mask of connected hosts. the **" Flags"** column show the flags apply to current line **"U"** means Up (active line), **"G"** means line uses a Gateway. The **"MSS**" column list the value of the maximum segment size for this line. The **"window"** column gives the option of altering a TCP parameter. The **"irtt"** column is used by the kernel to guess about the best TCP parameters without waiting for slow replies. The **"Iface"** column tells which network interface should be used for sending packets that match the destination

```
phool@phoolchandra:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0      1500  1405461      0   2123 0        266956      0      0      0 BMRU
lo       65536      140      0      0 0           140      0      0      0 LRU
phool@phoolchandra:~$
```

'netstat -I' command is used to display network interface status. The loopback device is a virtual network interface that computer uses to communicate with itself it is used for diagnostics and troubleshooting, and to connect to server running on local machine. The loopback interface is assigned all the IPs in the 127.0.0.1/8 address block.

ANS6. I have taken the reading at 8:00 AM, 4:00 PM, and 10:PM respectively. All these reading using JIO network.

Hosts	Hopcount 1	Hopcount 2	Hop count3	Common host
Iitg.ac.in	15	16	14	192.168.43.1, 14.142.139.81, 14.140.113.30

Cam.ac.uk	30	30	30	192.168.41.1, 10.72.163.3, 103.198.140.62, 49.45.4.251, 38.104 .85, 62.115.137.38, 146.97.35.193, 193.60.88.6
Flipkart.com	10	10	10	192.168.43.1, 10.72.163.19, 10.72.163.2, 49.44.18.38
Faceboook.com	25	25	24	192.168.43.1, 10.72.163.18, 49.45.4.85, 154.54.42.66, 38.104.65.234, 31.13.24.88, 173.252.67.25, 157.240.2.35
Nus.edu.sg	30	30	30	192.168.43.1, 10.72.163.18, 103.198.140.62, 49.45.4.251, 103.16.102.57, 202..51.240.34, 137.132.21.27

(II) Rout to same host changes at different time of the day due to differening traffic pattern. Routing may change due to consideration of diffrerent servers along the way,such as server load and availablity. if the routing is not dynamic and let's say server is down, it will lead to undelivered requests. Some servers are extremely busy during day time due to heavy computations or too many request while during night, they may be ideal so in such case we may route the requests to these servers at night and change during day time.

(III) Its primary reason could be existence of firewall which is configured to block these packets or a secondary reason may be that router is dropping packets going through it. This is usually caused by three reason either the router is overloaded, the router having a software or physical failure or the router is configured to do so (null route/ black holes).**(iv)** yes. The ping and traceroute both use the ICMP packets but their working is different. Ping is straight ICMP from point A to B, that traverses the network via routing rules and expects an ICMP reply from the host. Most probably the server is blocking the reply. On the other hand, traceroute sends packets with TTL values that gradually increase from packet to packet. Routers decrement TTL values of packets by one and discard packets whose TTL value reached zero, returning the ICMP error (ICMP time Exceeded). Traceroute looks for the ICMP time exceeded packet and not the ICMP reply packet, and that is why it might be possible.

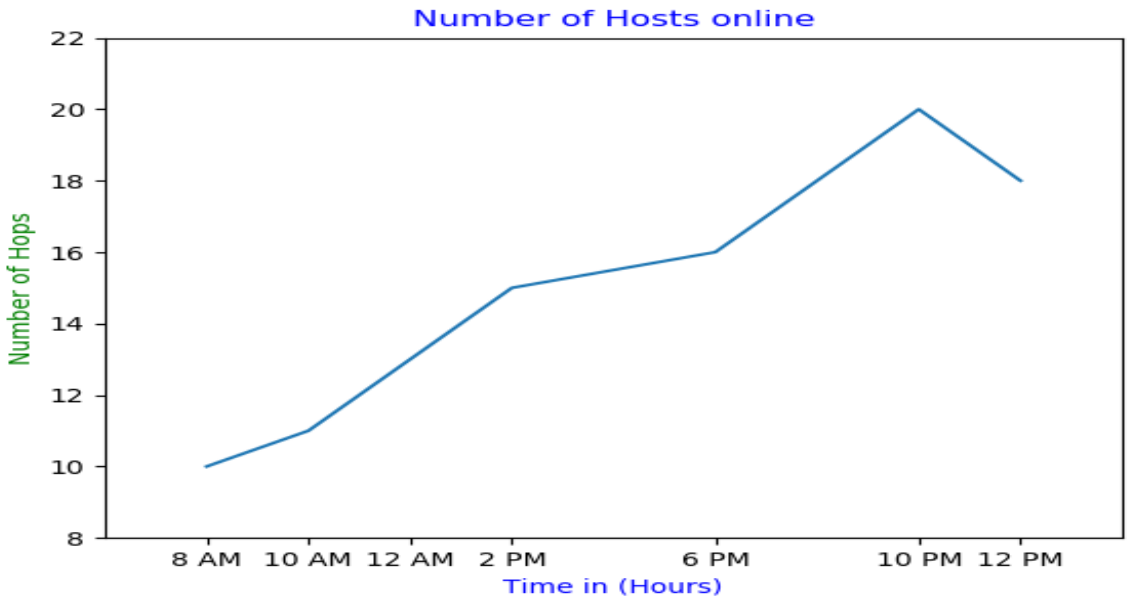
ANS 7.

```
phool@phoolchandra:~$ sudo arp -v
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   ec:44:76:74:60:41   C                     eth0
10.19.1.20               ether   f8:ca:b8:5f:7f:e4   C                     eth0
10.19.0.81               ether   f8:ca:b8:53:11:31   C                     eth0
10.19.1.48               ether   cc:2f:71:28:58:d9   C                     eth0
Entries: 4      Skipped: 0      Found: 4
phool@phoolchandra:~$ sudo arp -i eth0 -s 172.16.114.93 B0:83:FE:8D:92:DE
phool@phoolchandra:~$ sudo arp -i eth0 -s 172.16.114.90 B0:83:FE:8D:92:68
phool@phoolchandra:~$ sudo arp -v
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.114.93            ether   b0:83:fe:8d:92:de   CM                    eth0
_gateway                 ether   ec:44:76:74:60:41   C                     eth0
10.19.1.20               ether   f8:ca:b8:5f:7f:e4   C                     eth0
10.19.0.81               ether   f8:ca:b8:53:11:31   C                     eth0
172.16.114.90            ether   b0:83:fe:8d:92:68   CM                    eth0
10.19.1.48               ether   cc:2f:71:28:58:d9   C                     eth0
Entries: 6      Skipped: 0      Found: 6
phool@phoolchandra:~$
```

Using command "sudo arp -v", we can show the full ARP table. **Address** column show the IP4 of target pc connected to this pc. **HWtype** specifies the type of hardware. **HWaddress** shows the Mac address corresponding the particular entry in the table . ARP cache entries may be marked the flags C(complete), M(permanent). **Iface** column shows the network interface type for the corresponding entry. Using command **"sudo arp –s <ip4> <mac_address>"**, or **"sudo arp -I <Iface type> –s <ip4> <mac_address>"**, we can add the entries. We can delete the entry by command **"sudo -arp –d <ip4>"**. Dynamic entries stay cached 60 seconds and static entries stay cached for about 4 hours. A trial and error method is similar to binary search approach to get the desired value. Connect the machine to another network and check the ARP table after every t minutes. let the table is updated after k times then its mean that entry is updated between (k-1)*t and (k)*t minutes. Now check after (k-1)*t +(t/2) minutes. if the entry still exist at this time that means the cache is cleared after this time and before k*t minutes. Continue this approach until the result got. It can be two IP address can be mapped to same MAC address, this is known as IP aliasing. It happens when we use two operating system simultaneously one background and another as virtual machine. We use two different IP address to communicate among them, even though mac adderess is same. If IP's with same mac address are on different subnet then there is no

problem in packet routing each router's table contain single IP with a specific mac. But if IP's with same mac are on same subnet, there will be conflict as router will not know to which IP it has to route as ARP table contains many IPS with same mac, hence less correct transmission.

ANS 8 I have used the Ip address 172.16.114.93/26 from Lab pc. I have used the command $nmap –n -sP 172.16.114.93/26. Its outputs at different times are plotted in just below plot.



From figure We from plot we know that at morning there are lesser number of active hosts as time passes number of active hosts increase. But the number of active hosts at evening time are more than morning time because most of the students go to class at morning time and got free after 6:00 PM. Above number of active hosts are out of 64.

Time	8:00 AM,	10:00 AM,	12:01 PM	14:00 PM	18:00 PM	22:00 PM	24:00 PM
Host #	10	11	13	15	16	20	18