Assignment-1 Report
Arpit Gupta(160101015)

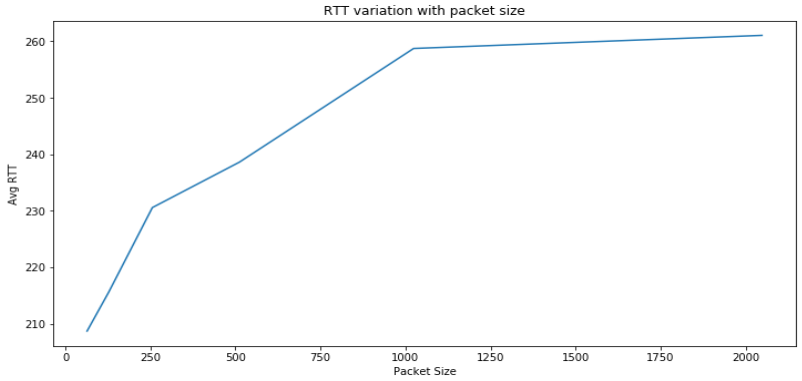
1.Ping command

1. The option required to specify the number of echo requests to send with ping is **'-c'**.
2. The option to set the time interval between two successive ping requests is **'-i'.**
3. The command to send ECHO_REQUEST packets to the destination one after another without waiting for a reply is **'-l'.**The normal users can send at max **3** packets using this.Additionally, there is also a provision for flooding the destination with ping requests without waiting using **'-f'** option.And the time interval can also be set 0 seconds using **'-i'** option.Also normal users have a limit of **200ms.**
4. The command to set the size of ECHO_REQUEST packet size(in bytes) is **'-s'.**The actual packet size will be slightly larger than what we enter due to the addition of the ICMP header(8 Bytes) and IP header(20 bytes). Hence, total packet size will be 92 bytes if size is set as 64 bytes.

2.Ping experiment

Host	ip-address	loss1	loss2	loss3	RTT1	RTT2	RTT3	avg_RTT	location
iitg.ac.in	14.139.196.22	0%	0%	0%	358.816	223.538	272.256	284.87	guwahati
cricbuzz.com	161.202.24.162	5%	5%	5%	185.029	286.571	212.022	227.874	singapore
amazon.com	176.32.98.166	0%	10%	0%	365.861	429.101	359.807	384.923	USA
netflix.com	52.88.70.220	100%	100%	100%	NO_RTT	NO_RTT	NO_RTT	NO_RTT	USA
github.com	192.30.253.113	0%	40%	0%	411.305	410.717	430.227	417.46	california

Observation: There seems to be a correlation between the geographical distance and the latencies.Lower latencies are close servers.**But** as an examp1le in the table above singapore's latency is lower than the indian server, **meaning that the correlation is not very strict.(**Observations taken at times 5 pm,9 pm and 1am)
The packet losses do take place occasionally.It is most probably due to **link congestion,** though it can also happen due to fault in cables, or failing of intermediate routers or even firewalls.e.g., in the table netflix shows 100% packet losses at all times.
I picked **cricbuzz.com** and experimented with different packet sizes as can be seen in the graph below for RTT variation visualisation.



Observation from the graph above: The average RTT consistently increases with increasing packet size.Variation with time - The latencies varied by about +-20% for each observation.

3. Ping -n vs -p

Chosen IP: 202.141.80.14

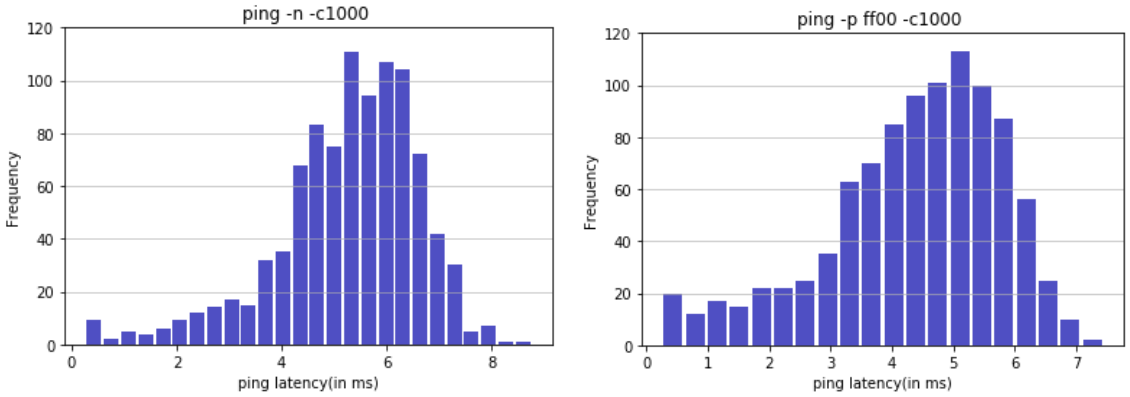
a.) Packet loss rates:

- No lookup option(-n): 1000 packets transmitted, 960 received, 4% packet loss, time 1001111ms
- Data pattern option(-p): 1000 packets transmitted, 976 received, 2% packet loss, time 1001358ms

b.)

Type of command	Min RTT	Max RTT	Mean RTT	Median RTT
ping -n	0.265	8.762	5.266	5.450
Ping -p ff00	0.262	7.447	4.360	4.580

c.)plots of the pings



d.) All the statistical values of latency for No-lookup option are higher than those for the other.The difference in average is about 12%.
The no-lookup option will not attempt to lookup symbolic names for host addresses.This reflects in the ping output as the symbolic name of the IP is no longer visible.
The pattern option will fill the data field with given pattern.Ideally the packets should not be differentiated by the contents of data.But some data-dependent problems have been known to appear. A particular file that either can't be sent or that takes much longer to transfer than expected indicates a data-dependent problem.

4. Ifconfig and Route

The command **'ifconfig'** shows details of the network interfaces that are up and running in the computer.My machine has a wired ethernet interface (**enp2s0**), a loopback interface (**lo**) and a wireless ethernet interface (**wlo1**).**Link encap:Ethernet** denotes that the interface is an Ethernet related device.**Hwaddr** is the hardware address or the MAC address, which is unique to each Ethernet card which is manufactured.**Inet addr & inet6 addr** indicates the machine IPv4 and IPv6 address associated with that network interface respectively.

```
arpitgupta@arpitgupta-HP-Notebook:~$ ifconfig -a -v
enp2s0    Link encap:Ethernet  HWaddr a0:8c:fd:4c:86:ef
          inet addr:10.3.1.35  Bcast:10.3.3.255  Mask:255.255.252.0
          inet6 addr: fe80::329d:1447:8b7e:3aa6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:196142 errors:0 dropped:103 overruns:0 frame:0
          TX packets:112832 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:211873740 (211.8 MB)  TX bytes:14912475 (14.9 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:409424 errors:0 dropped:0 overruns:0 frame:0
          TX packets:409424 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:24595189 (24.5 MB)  TX bytes:24595189 (24.5 MB)

wlo1      Link encap:Ethernet  HWaddr 74:df:bf:7f:94:df
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:1717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1942 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2040126 (2.0 MB)  TX bytes:248560 (248.5 KB)
```

Bcast denotes the broadcast address (The address required to broadcast on the network connected through that interface of the machine). **Mask** is the network mask which decides the potential size of the network. **Scope** is the scope of the area where the address is valid.Link means valid only on this device and host means valid only inside the host(my machine)**.UP** flag indicates that the kernel modules related to the Ethernet interface has been loaded.**BROADCAST & MULTICAST** denotes that the Ethernet device supports broadcasting and multicasting respectively. **RUNNING** means that the interface is ready to accept data. **MTU(Maximum Transmission Unit)** is the size of each packet received by the Ethernet card. **Metric** take a value of 0,1,2... It decides the priority of the device. Lower the value the more leverage it has. **RX Packets, TX Packets** show the total number of packets received and transmitted respectively. It also shows the number of packets dropped and the overruns. **Collision** shows the number of packets that are colliding while traversing the network due to network congestion. **RX bytes, TX bytes** indicates the total amount of data that has passed through the interface either way. **Txqueuelen** denotes the length of the transmit queue of the device.

```
arpitgupta@arpitgupta-HP-Notebook:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.3.0.254      0.0.0.0         UG    100    0        0 enp2s0
10.3.0.0        0.0.0.0         255.255.252.0   U     100    0        0 enp2s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp2s0
```

The **'route'** command shows the routing table of the device.The **Destination** column identifies the destination network or destination host. The **Gateway** column identifies the defined gateway for the specified network. An asterisk (*) appears in this column if no forwarding gateway is needed for the network. The **Genmask** column shows the netmask for the network. The **Iface** column shows the network interface.**'enp2s0'** is for the Ethernet device.Under the Flags section, the **U flag** means the route is up, and the **G flag** means that specified gateway should be used for this route. Metric is the distance to the target (usually counted in hops). **Ref** is the number of references to this route. **Route** command has many options – **'-n'** is used to display the numerical IP address, list the kernel's routing cache information by using **'-C'**, **'-v'** to select verbose operation, **'del'** to delete a route and '**add'** to add a route, **'-net'** specifies that the target is a network and **'-host'** specifies that the target is a host.

5. Netstat

Netstat command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.
$ netstat -at is used to show all established tcp connections.The **proto** column shows the protocol (tcp, udp, raw) used by the socket.The **Recv-Q and Send-Q** columns tell us how much data is in the queue for that socket, waiting to be read or sent.

```
arpitgupta@arpitgupta-HP-Notebook:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 arpitgupta-HP-No:domain *:*                     LISTEN
tcp        0      0 localhost:ipp           *:*                     LISTEN
tcp        0      0 localhost:8888          *:*                     LISTEN
tcp        0      0 localhost:6341          *:*                     LISTEN
tcp        0      0 localhost:6342          *:*                     LISTEN
tcp        0      0 10.3.1.35:51430         bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 10.3.1.35:53374         bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 10.3.1.35:54120         bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 10.3.1.35:53786         bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 10.3.1.35:54114         bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 10.3.1.35:51710         bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 10.3.1.35:51072         bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 10.3.1.35:54116         bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 10.3.1.35:54102         bichitra.iitg.erne:3128 TIME_WAIT
tcp        0      0 10.3.1.35:49858         bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 10.3.1.35:54082         bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 10.3.1.35:52014         bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 10.3.1.35:53456         bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 10.3.1.35:53788         bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 10.3.1.35:51966         bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 10.3.1.35:54118         bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 10.3.1.35:54122         bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 10.3.1.35:54104         bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 10.3.1.35:51054         bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 10.3.1.35:49856         bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 10.3.1.35:52432         bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 10.3.1.35:52426         bichitra.iitg.erne:3128 ESTABLISHED
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
```

The Local Address and Foreign Address columns tell to which hosts and ports the listed sockets are connected.The local end is my machine on which we run netstat, and the foreign end is the other computer (could be somewhere in the local network or on the internet). The **state** of the socket can be listen (waiting for an incoming connection), established (connections which are established), and time wait (the foreign or remote machine has already closed the connection, but that the local program somehow hasn't followed suit).suit). If the Foreign Address is *:* (with **TCP sockets & LISTEN state**), a socket is usually waiting for some remote host to send the first data. When connecting to a foreign host, a program on the computer usually doesn't care which local port is used for the connection. That's why the port on the local side isn't usually recognized and translated to a protocol like "https" or "www".

$ netstat -r shows the kernel routing table of machine.

```
arpitgupta@arpitgupta-HP-Notebook:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         10.3.0.254      0.0.0.0         UG        0 0          0 enp2s0
10.3.0.0        *               255.255.252.0   U         0 0          0 enp2s0
link-local      *               255.255.0.0     U         0 0          0 enp2s0
```

The **Destination** column indicates the pattern that the destination of a packet is compared to. The **Gateway** column tells the computer where to send a packet that matches the destination of the same line. An asterisk (*) here means send locally.locally.The **Genmask** column tells how many bits from the start of the ip address are used to identify the subnet. As a rule of thumb, it is 255 for non-zero part and 0 for other parts of the destination.The **Flags** column displays the flags that describe the route - **G**(route uses a gateway), **U**(interface is up), **H**(Only a single host can be reached through the route), **D**(route is dynamically created), **M**(route is set if the table entry was modified by an ICMP redirect message), **!**(route is a reject route and datagrams will be dropped).The next three columns show the **MSS**, **Window** and **irtt** that will be applied to TCP connections established via this route. The **MSS(Maximum Segment Size)** is the size of the largest datagram the kernel will construct for transmission via this route. The **Window** is the maximum amount of data the system will accept in a single burst from a remote host. The acronym **irtt** is the initial round trip time. The **Iface** column tells which network interface should be used for sending packets that match the destination.

$ netstat -i shows the status of network interfaces.The three interfaces ethernet(enp2s0),loopback(lo), and wireless(wlo1).The **RX and TX** columns show how many packets have been received or transmitted error-free(RX-OK/TX-OK), damaged(RX-ERR/TX-ERR), dropped(RX-DRP/TX-DRP) and lost because of an overrun (RX-OVR/TX-OVR).

```
arpitgupta@arpitgupta-HP-Notebook:~$ netstat -i
Kernel Interface table
Iface   MTU Met   RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp2s0     1500 0    1549911      0    584 0       1061904      0      0      0 BMRU
lo        65536 0     495090      0      0 0        495090      0      0      0 LRU
wlo1       1500 0       1720      0      0 0          1969      0      0      0 BMU
```

The last column shows the flags that have been set for this interface- **B**(broadcast address has been set), **L**(it is a loopback device), **M**(all packets are received, i.e.promiscuous mode), **O**(ARP is turned off for this interface), **P**(This is a point-to-point connection), **R**(Interface is running), **U**(Interface is up).
The **loopback** device is a special, virtual network interface that the computer uses to communicate with itself. It is used mainly for diagnostics and troubleshooting, and to connect to servers running on the local machine. When a network interface is disconnected, no communication on that interface is possible, not even communication between the computer and itself. The loopback interface does not represent any actual hardware, but exists so applications running on the computer can always connect to servers on the same machine. For example, if you run a web server, you have all your web documents and could examine them file by file on the local machine. For IPv4, the loopback interface is assigned all the IPs in the 127.0.0.0/8 address block (i.e.127.0.0.1 through 127.255.255.254).

6.TRACEROUTE

I used **http://www.cogentco.com/en/network/looking-glass** for this experiment at the starting router location at washington(DC).

	iitg.ac.in	amazon.com	netflix.com	cricbuzz.com	github.com
Hop count1	12	30	30	13	30
Hop count2	12	30	30	12	30
Hop count3	12	30	30	7	30

a.) Common route observed:- All the routes contained the same first hop - from **atlas.cogneto.com(66.250.250.121) to 154.54.81.141**.
b.) Change of route was observed for **cricbuzz.com,** which was different for all the three times of a day.The reasons mainly involve two things - **process switching** and **load balancing.**At each hop, the router may do process switching and decide a different intermediate router for the next hop, resulting in a changed route.Also, when the destination router has two or more connections to different ISPs, to avoid a single connection getting overloaded, the router uses the next free connection to do load balancing, again changing the route.
c.) Such cases, in my experiment, occur with github.com,netflix.com and amazon.com.One of the reasons for the traceroute to not work is if one of the intermediate routers are **limiting ICMP responses to prevent DDoS attacks.**As a side effect, the router may not send back any response for traceroute on the machine.
d.) It is possible when the host has blocked ICMP ECHO REQUESTs.Traceroute, although it(in Windows) uses ICMP protocol, relies on **ICMP TTL EXCEEDED** messages, which might be allowed.

7. ARP

ARP stands for **Address Resolution Protocol**, which is used to find the address of a network neighbor for a given IPv4 address.**$ arp -a** shows the complete ARP Table of the machine.It shows the **IP-address,**the corresponding **MAC-address,**and the **Network interface**.When we try to ping an IP address on our local network, say 10.0.0.1, the system has to turn the IP address 10.0.0.1 into a MAC address. This involves using ARP Table to resolve it. An entry for the IP address can be deleted from the ARP table using the command "**$ arp –d <address>**". If you want to make a specific MAC address be used for an IP, use the command: "**$ arp -s <ip_addr> <MAC_addr>**". You need to run it as a root user(use sudo).Entries stay cached in the ARP table for **60 seconds**.Adding new hosts to the ARP table can be

done by just pinging another IP address in the same intranet.Then a new pair of **(host_ip,hw_addr)** will be added to the ARP table.Below picture shows two IP addresses **10.3.1.36 and 10.3.1.37** are added in this way to the ARP table.

```
arpitgupta@arpitgupta-HP-Notebook:~$ arp -v
Address                  HWtype  HWaddress           Flags Mask            Iface
10.3.0.20                ether   8c:ec:4b:0e:15:5f   C                     enp2s0
10.3.1.38                ether   dc:4a:3e:aa:e0:0c   C                     enp2s0
10.3.0.254               ether   4c:4e:35:97:1e:ef   C                     enp2s0
Entries: 3      Skipped: 0      Found: 3
arpitgupta@arpitgupta-HP-Notebook:~$ ping -c1 10.3.1.36
PING 10.3.1.36 (10.3.1.36) 56(84) bytes of data.
64 bytes from 10.3.1.36: icmp_seq=1 ttl=64 time=0.748 ms

--- 10.3.1.36 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.748/0.748/0.748/0.000 ms
arpitgupta@arpitgupta-HP-Notebook:~$ ping -c1 10.3.1.37
PING 10.3.1.37 (10.3.1.37) 56(84) bytes of data.
64 bytes from 10.3.1.37: icmp_seq=1 ttl=64 time=0.984 ms

--- 10.3.1.37 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.984/0.984/0.984/0.000 ms
arpitgupta@arpitgupta-HP-Notebook:~$ arp -v
Address                  HWtype  HWaddress           Flags Mask            Iface
10.3.1.37                ether   a0:8c:fd:22:4b:89   C                     enp2s0
10.3.1.36                ether   34:ce:00:23:3a:ab   C                     enp2s0
10.3.0.20                ether   8c:ec:4b:0e:15:5f   C                     enp2s0
10.3.1.38                ether   dc:4a:3e:aa:e0:0c   C                     enp2s0
10.3.0.254               ether   4c:4e:35:97:1e:ef   C                     enp2s0
Entries: 5      Skipped: 0      Found: 5
```

We can use **$ cat /proc/sys/net/ipv4/neigh/default/gc_stale_time** to know the entries cached time in the ARP table.A **trial & error method** to discover the timeout value is to add a temporary entry in the arp table and keep on checking the arp table after fixed intervals of time (say 5 seconds). The time after which it dissapears is approximately the required cache timeout. For a better appproximation, decrease the interval length. Alternatively, one can use **binary search** also for finding the cache time, for e.g. – Add a temporary entry in ARP and check after 5000ms. If then entry has been deleted, then add the entry again and check after 2500ms. Continue in Binary sense to find the cache time. **The scenario where two IP's can map to same Ethernet Address is when a router or a gateway connects two or more subnet ranges**. When communicating with machines on the same subnet range, MAC address is used for directing the packages. In the ARP Table, the IP's of the devices which are connected in the other subnet range have the ethernet address/MAC address as that of the Router or Gateway which connects the two subnet ranges. ARP table is referred to convert these IP addresses to the MAC address and packets are sent to it(router/gateway). The router then uses it's routing table and sends the packet further to the correct device.

8. NMAP

The IP's analysed are of **siang hostel** using **$ nmap -n -sP 10.3.0.254/22.**From below,one can easily notice that the number of hosts are low in the early morning around 11.00 AM and steadily increase till the afternoon (around 5.00PM). After that there is a slight decrease till 8 pm and then increases till night around 12:00AM. The number of hosts online starts to decrease after that.