Name Deshmukh Udayraj
Roll No 150101021

Q1 Ping basics

a) The '-c' option : `ping -c 5 202.141.80.14`
b) The '-i' option : `ping -i 2 202.141.80.14`
c) Setting -i interval very low will send next ECHO_REQUEST packet regardless of receiving previous ECHO_REPLY. The interval limit for non-sudo users is **0.2s**.
   `sudo ping -i 0.0001`
d) The '-s' option : `ping -s 64 202.141.80.14`
   The actual packet size will be slightly larger than PacketSize due to the addition of the ICMP header information attached to the ping (here 8 bytes). So total packet size for a 64 bit packet will be **72 bytes**.

Q2 Ping latencies and RTT

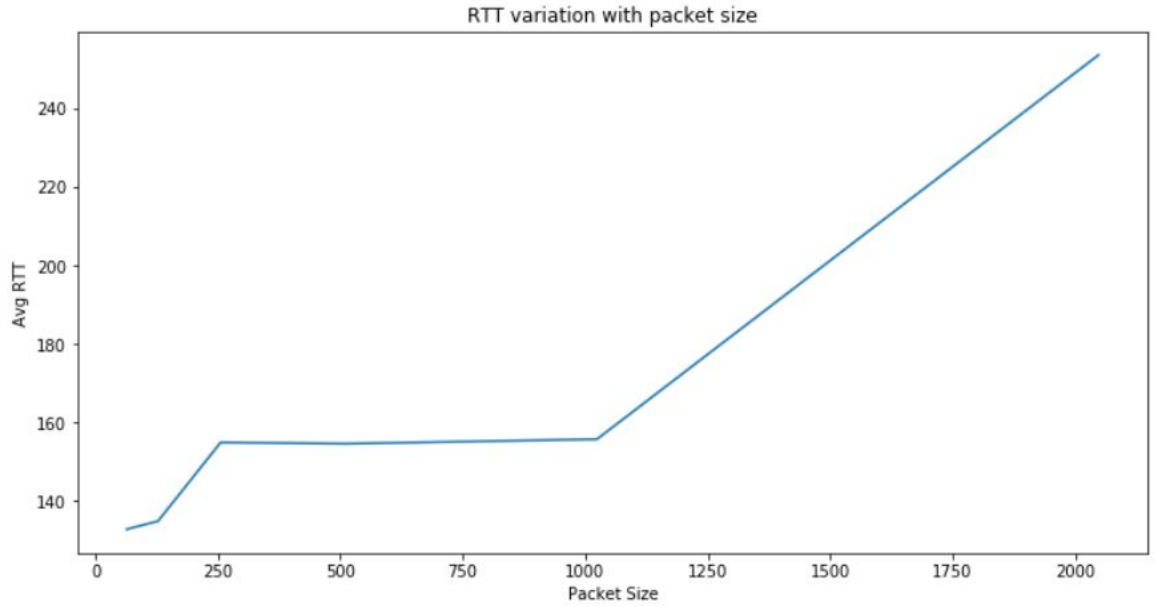
Chosen 5 hosts from the internet -

host	IP	Location
techniche.org	43.255.154.56	Singapore
techfest.org	103.50.163.52	India
supercell.com	52.216.99.42	United States
github.com	192.30.253.113	United states
codeforces.com	212.193.33.27	Russian federation

Collected Data (Packet loss and RTT)-

host	pkt loss1	pkt loss2	pkt loss3	RTT1	RTT2	RTT3	Avg RTT	Location
techniche	0	0	0	148.065	145.025	133.644	142.244	Singapore
techfest	5	0	5	174.888	173.331	189.217	179.145	India
supercell	5	0	10	397.669	381.348	438.307	405.774	United States
github	15	0	15	408.595	393.653	469.321	423.856	United states
codeforces	0	0	0	316.335	305.356	308.571	310.087	Russia

Observation : There seems to be a correlation between the geographical distance and the latencies. Lower latencies for closer servers. But still, the Singapore's latency is even lower than the indian server, meaning the correlation is not very strict.
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.



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

Q3 Ping -n and -p

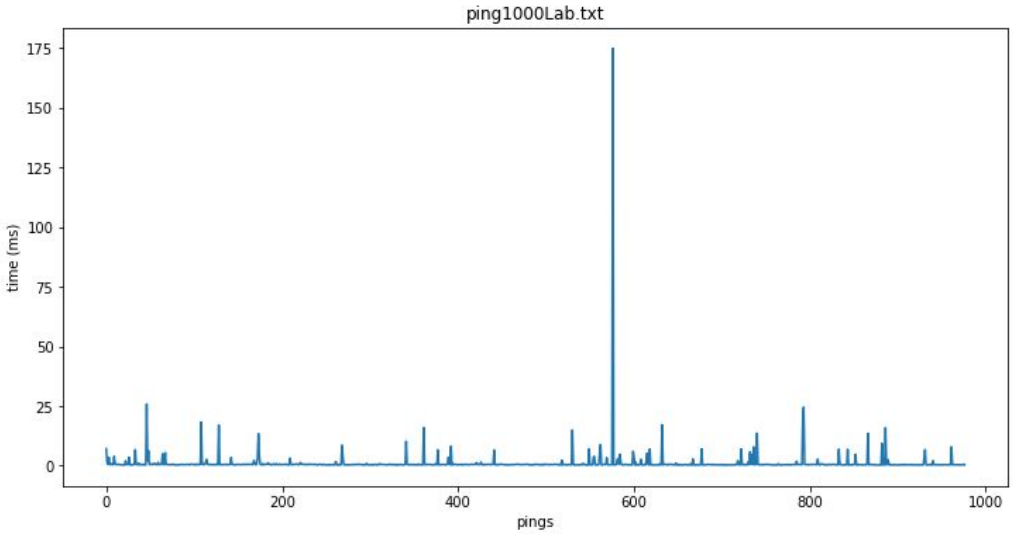
Chosen IP : 202.141.80.14 (Both the commands were run simultaneously in separate terminals.)

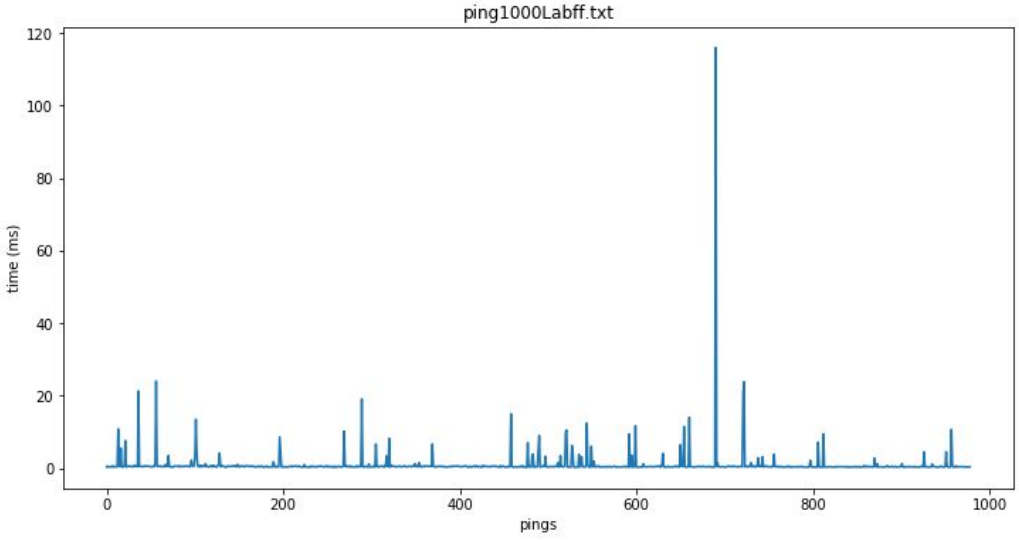
a) Packet Loss rates -
   No lookup option => 1000 packets transmitted, 977 received, **2% packet loss**, time 1015303ms
   Data pattern option => 1000 packets transmitted, 979 received, **2% packet loss**, time 1015471ms

b) ping1000Lab.txt ping1000Labff.txt

min	0.244000	min	0.229000
max	175.000000	max	116.000000
mean	1.081548	mean	0.964655
Median	**0.425000**	**Median**	**0.388000**

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 10%.
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.

Q4 The ifconfig command

Term	Explanation
eno1, lo, wlo1	These identify the network cards present on the device. eno1 is the onboard Ethernet (wired) adapter. lo is a loopback device. the prefix ‘w’ stands for wireless.
UP/DOWN	Indicates whether kernel modules related to the Ethernet interface has been loaded.
RUNNING	Means the interface is ready to accept data

BROADCAST/ MULTICAST	Denotes what the ethernet device is supporting. BROADCAST- device can send traffic to all hosts on the link MULTICAST - allows a source to send packets to multiple machines ALLMULTI - device receives all multicast packets on the link PROMISC - device receives all traffic on the link
mtu	short for Maximum Transmission Unit. It is the size of each packet received by the Ethernet card. The default value is 1500.
inet,inet6	inet addr - indicates the machine IP address inet6 addr - indicates the machine IPv6 address
netmask	Shows the configured value of Netmask
txqueuelen	It denotes the length of the transmit queue of the device.
ether HWaddr	It's a MAC address which is unique to each Ethernet card.
RX/TX packets	total number of packets received and transmitted respectively.
RX bytes/TX bytes	total number of bytes received and transmitted respectively.
dropped	total number of packets dropped by receiver/transmitter.
errors	total number of errors detected by receiver/transmitter.
overruns	total number of overruns detected by receiver/transmitter.
carrier	total number of carrier wave loss detected by receiver/transmitter.
collisions	total number of collisions detected by receiver/transmitter. It is positive when congestion occurs in the medium.

Q4 The route command

Output (the -n option shows ip addresses instead of hostnames) -

```
udayraj@aardvark:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.1.0.254      0.0.0.0         UG    100    0        0 eno1
10.1.0.254      0.0.0.0         255.255.255.255 UH    100    0        0 eno1
10.1.2.0        0.0.0.0         255.255.255.0   U     100    0        0 eno1
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 eno1
```

It shows the kernel routing table entries.
According to this routing table, any packets with a destination address in the 10.1.2.0/24 network will be routed to the gateway 0.0.0.0 instead of the default gateway. This will prevent unnecessary ICMP redirect messages.
The column after the netmask column (Flags) should always contain a **G** for destination not locally connected to the linux machine. U flag means UP.
The fields Metric, Ref and Use are not generally used in simple or even moderately complex routing tables
The other entries can be read in a similar way.

Route options -

-v, --verbose	be verbose
-n, --numeric	don't resolve names
-e, --extend	display other/more information
-F, --fib	display Forwarding Information Base (default)
-C, --cache	display routing cache instead of FIB

Q5 The netstat command

Command to show all tcp connections established `netstat --tcp` (The --numeric is optional as it only suppresses hostname,etc lookups)-

```
udayraj@aardvark:~$ netstat --tcp --numeric
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:49030         127.0.0.1:3128          ESTABLISHED
tcp        0      0 10.1.2.22:37482         202.141.80.24:3128      ESTABLISHED
tcp        0      0 127.0.0.1:49158         127.0.0.1:3128          ESTABLISHED
tcp        0      0 10.1.2.22:37432         202.141.80.24:3128      ESTABLISHED
tcp        0      0 127.0.0.1:48980         127.0.0.1:3128          ESTABLISHED
tcp        0      0 127.0.0.1:49002         127.0.0.1:3128          ESTABLISHED
tcp        0      1 10.1.2.22:49994         202.141.80.9:53         SYN_SENT
tcp        0      1 10.1.2.22:52118         8.8.4.4:53              SYN_SENT
```

`netstat -r` shows the routing table

`netstat -i` displays the interface statistics. There are **3 network interfaces** on my system

Loopback interface functions -

- Device Identification - pinging machine itself. Also verifies the network is configured correctly
- Routing information—The loopback address is used by protocols such as OSPF to determine protocol-specific properties for the device or network. Further, some commands such as ping mpls require a loopback address to function correctly.
- Packet filtering—Stateless firewall filters can be applied to the loopback address to filter packets originating from, or destined for, the Routing Engine.

Q6 traceroute

1) No of hops per host per time-slot -

Host \ Time	18:07:27	19:37:22	21:07:26
github.com	18	17	17
techniche.org	30	11	30
techfest.org	7	7	7
codeforces.com	18	18	17
supercell.com	25	26	26

Common route observed: ALL the routes contained same first hop - from gateway (10.8.0.1) to 139.59.80.254

2) Change of route was observed for techniche.org (when hops dropped to 11). 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 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.
3) One of the reasons for 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.
4) It is possible in the case 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.

Q7 The arp command

Commands : arp will show the full arp table, arp -s *IP HWaddr* will add/modify entry, arp -d *IP* will delete an entry.
Each entry in arp cache represents a mapping between an IP address and a device's MAC address.
Explanation of columns -
Address = IP address of the device,
HWtype = type of connection by the device
HWaddress = MAC address of device,
Iface = interface used by device.

ARP timeout : By default the arp cache is flushed every 60 seconds on ubuntu 17.10
(command used to find - cat /proc/sys/net/ipv4/neigh/eno1/gc_stale_time).
Trial and error method to find arp timeout - Interval halving method -

1. Firstly to check if cache is refreshed : we watch arp table
   Run following in **tab1** of terminal- which would highlight changes in arp table
   while true; do p1=$p2; p2=$(clear; arp -ne); dwdiff -y "\010" -1 -c <(echo "$p1") <(echo "$p2"); sleep 2; done
2. Populate the arp table. we can use nmap on local network.
3. Note: In the current system, the arp cache is never cleaned fully. It is "marked as stale" after the cache timeout (gc_stale_time), then the garbage collector clears them. But it also maintains a minimum number of entries in the table (gc_thresh1, source) which defaults to 128. Run the following in **tab2 -**
   sudo ip -s -s neigh flush all
   sudo sysctl -w net.ipv4.neigh.default.gc_thresh1=1
4. The timer is now started, all entries except one will be flushed at timeout. Now, assume the timeout is 60 minutes, change system time to 60 minutes ahead, if cache is refreshed, it means the timeout is within 60 minutes, then try 30 minutes ahead, if it did not refresh this time, we narrowed down the window to between 30-60 minutes. And continue in similar fashion.

If two IP addresses map to the same Ethernet address, pinging to any of the IP address will give us a reply from the correct IP address (stored on the device at Ethernet address)
This can be tested by adding a false entry to existing IP -
For the entry 10.1.2.24 - 14:58:d0:ca:4b:89, we add the following entry
sudo arp -s 10.1.2.99 14:58:d0:ca:4b:89
Now, if we ping to 10.1.2.99, it gives a **reply from 10.1.2.24**, but it gives 100% packet loss.

Q8 The nmap command

nmap -n -sP 10.1.2.0/24 was run every half an hour using cron job, plot -