Parth Bakare
180101056

CS342 : Networks Lab, Assignment-1

Question 1.

(a) *ping -c* <number of packets>
(b) *ping -i* <time interval>
(c) *ping -l* <number of packets>
Maximum 3 packets can be sent (one after another without waiting for a reply) by a normal user.
(d) *ping -s* <packet size in bytes>
If the payload size is 32 bytes, then the total packet size will be 60 bytes.

Question 2.

(a)

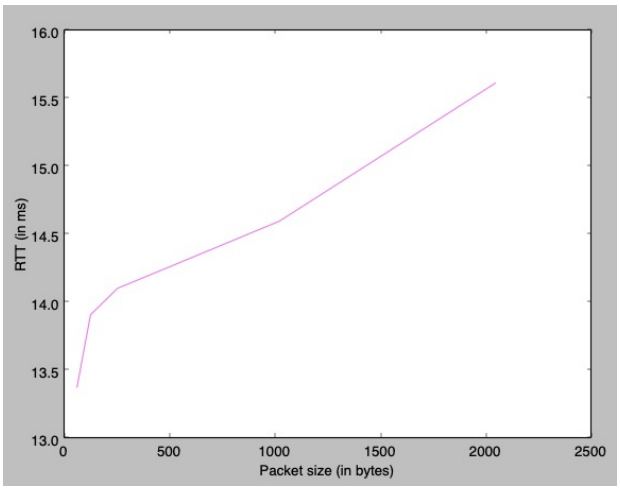
	3:00 PM	4:00 PM	12 noon	Average
youtube.com	34.409 ms	36.349 ms	33.733 ms	34.830 ms
atcoder.jp	N/A	N/A	N/A	N/A
nutanix.com	71.602 ms	68.616 ms	13.898 ms	51.372 ms
manutd.com	13.207 ms	14.582 ms	36.653 ms	21.481 ms
timesnownews.com	258.541 ms	260.568 ms	14.252 ms	177.787 ms
hotstar.com	5.161 ms	4.572 ms	13.459 ms	7.731 ms

→ 100% packet loss

RTT increases with increase in geographical distance. When a packet has to travel a larger distance, it needs to travel through more routers and perform more hops, resulting in an increased amount of time for the ping.

(b) The packet loss was 100% for atocder.jp, because it blocked IMCP packets.

(c) Measuring RTT with change in packet size for hotstar.com,



Packet size	RTT
64 bytes	13.376 ms
128 bytes	13.908 ms
256 bytes	14.103 ms
512 bytes	14.267 ms
1024 bytes	14.597 ms
2048 bytes	15.612 ms

(d) RTT increases with increase in packet size, as shown in the above graph. RTT increases because processing larger packets takes more time which leads to delays.
RTT varies across the time of the day. This occurs because of different network traffic situations at different hours of the day. The network is more congested at certain hours and less congested at other hours.

Question 3.

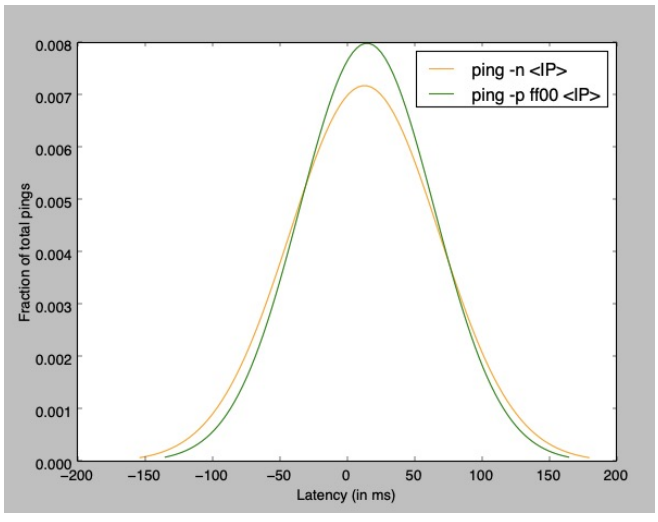
(a)

	ping -n <IP>	ping -p ff00 <IP>
Packet loss	3.3%	2.8%

(b)

Minimum latency	5.326 ms	5.425 ms
Maximum latency	1282.310 ms	1112.820 ms
Median latency	7.956 ms	7.950 ms
Mean latency	13.465 ms	15.308 ms

(c)



(d) *ping -p ff00* <IP> sends packets where the first 8 bits are 1s and the next 8 bits are 0s. This operation is used to diagnose data-dependent problems in a network ie. whether a network is susceptible to packets of specific data configurations. *ping -n* <IP> does not do any such thing, and the difference in the two curves shows the behaviour of the network towards a certain type of data. In this case, the latency values over the two experiments are very similar, and thus the two curves are almost identical in shape.

Question 4.

(a) *ifconfig* (interface configuration) is used to configure network-interfaces, and to diagnose them. Running *ifconfig* in the terminal prints the following fields as output -
- inet : IPv4 address of the interface
- netmask : network mask of the interface (that divides the IP into subnets and specifies the hosts)
- broadcast : interface broadcast address
- inet6 : IPv6 address of the interface
- RX packets : Number of received packets
- RX errors : Number of received packets (with an error)
- TX packets : Number of transmitted packets
- TX errors : Number of transmitted packets (with an error)

(b) Some options provided with *ifconfig* are -
- *-a* : displays all available interfaces (even those which are down)
- *-s* : displays a short list (concise summary of interfaces and their attributes)
- *mtu N* : sets the MTU (maximum transfer unit) of the interface
- *[-] arp* : enables/disables the use of ARP for this interface

Apart from these, some other options provided by *ifconfig* are *-v*, *up*, *down*, *add addr*, *del addr* etc.

(c) *route* displays the kernel IP routing table, with the following fields in the table :
- Destination : Destination network (or destination host) of the route
- Gateway : Gateway address
- Genmask : Network mask of the destination
- Flags : Additional attributes describing the route, such as U (route is up), G (use gateway) etc
- Metric : Target distance (in number of hops)
- Ref : Number of route references
- Use : Number of route lookups
- Iface : Reachable interface (to which packets will be sent)

(d)

```
(base) lelouch_666@Lancelot-Albion:~$ 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    20100  0        0 eno1
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 eno1
172.16.112.1    0.0.0.0         255.255.255.255 UH    20100  0        0 eno1
172.16.114.128  0.0.0.0         255.255.255.128 U     100    0        0 eno1
(base) lelouch_666@Lancelot-Albion:~$ route -v
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    20100  0        0 eno1
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 eno1
_gateway        0.0.0.0         255.255.255.255 UH    20100  0        0 eno1
172.16.114.128  0.0.0.0         255.255.255.128 U     100    0        0 eno1
(base) lelouch_666@Lancelot-Albion:~$ route -F
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    20100  0        0 eno1
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 eno1
_gateway        0.0.0.0         255.255.255.255 UH    20100  0        0 eno1
172.16.114.128  0.0.0.0         255.255.255.128 U     100    0        0 eno1
(base) lelouch_666@Lancelot-Albion:~$ route -C
Kernel IP routing cache
Source          Destination     Gateway         Flags Metric Ref    Use Iface
```

- *-n* : shows all the data in full numeric form
- *-v* : selects verbose operation
- *-F* : displays Forwarding Info Base
- *-C* : displays routing cache

Question 5.

(a) *netstat* (network statistics) is a tool used to debug networks by monitoring connections (both incoming and outgoing), viewing interface statistics, viewing routing tables etc.

(b)
```
(base) lelouch_666@Lancelot-Albion:~$ netstat -at | grep 'ESTABLISHED'
tcp        0      0 Lancelot-Albion:ssh     172.18.16.41:55928      ESTABLISHED
tcp        0      0 Lancelot-Albion:ssh     172.18.16.41:56623      ESTABLISHED
tcp        0     36 Lancelot-Albion:ssh     172.18.16.41:56626      ESTABLISHED
```
netstat -at displays all the tcp connections (both established and listen). Using *grep 'ESTABLISHED'* shows only the established connections.

(c) *netstat -r* displays the kernel IP routing table, similar to the route command (**Question 4.**), with a different column MSS instead of metric. MSS is the maximum segment size for TCP connections in this route.

(d) *netstat -ai* shows the status of all network interfaces. Number of interfaces can be printed using *expr $(netstat -ai | wc -l) - 2* (*wc -l* shows number of lines in the output, *expr* is used for math operations in the terminal (subtracting 2 because the first two lines displayed by *netstat -ai* are not interfaces)).

(e) *netstat -su* shows statistics of all UDP connections.
```
(base) lelouch_666@Lancelot-Albion:~$ netstat -su
IcmpMsg:
    InType0: 532
    InType3: 182
    InType8: 245
    InType13: 2
    OutType0: 152
    OutType3: 181
    OutType8: 691
    OutType14: 2
Udp:
    23636 packets received
    72 packets to unknown port received
    0 packet receive errors
    27841 packets sent
    0 receive buffer errors
    0 send buffer errors
    IgnoredMulti: 649615
UdpLite:
IpExt:
    InMcastPkts: 1101
    OutMcastPkts: 616
    InBcastPkts: 649708
    OutBcastPkts: 7
    InOctets: 90183611
    OutOctets: 11448341
    InMcastOctets: 107523
    OutMcastOctets: 46656
    InBcastOctets: 44127854
    OutBcastOctets: 327
    InNoECTPkts: 809817
    InECT0Pkts: 5623
```

(f) A machine uses the loopback interface, a virtual interface, to communicate with itself. The loopback interface is not dedicated to any hardware and never goes down, unless it is forcibly shut, and can be used for diagnosing a network. Loopback interface provides a reliable option for interfaces on the same machine to communicate efficiently, and without an interface which never goes down, interfaces would fail to access applications in the same machine after going down.

Question 6.

(a) *traceroute* is a network diagnosis tool used to track the route a packet takes when traveling from a source to a destination over a network. *traceroute* displays the details of every hop made by the packet in its path, and also reveals the IP it reached at every hop and can be used to determine at which router a packet goes missing incase of a packet loss.

(b)

	1:00 PM	2:00 PM	3:00 PM
youtube.com	9	9	9
atcoder.jp	20	20	20
nutanix.com	timed out	timed out	timed out
manutd.com	timed out	timed out	timed out
timesnownews.com	18	18	18
hotstar.com	24	24	24

No common hops
between 2 different routes.

(c) Route to youtube.com was different at every hour. This happens because there could be several intermediate routers between the source and the destination belonging to the same network, and the preceding router is free to choose any of the routers to send the packet.

(d) *traceroute* could not find paths to nutanix.com and manutd.com because of firewall protection somewhere in the path which guards against such activities.

(e) Some hosts do not respond to *ping* because they block ICMP packets. *traceroute* uses UDP packets to map hops to the destination, and can perform its operation if the host does not guard against this, even if it blocks ICMP packets.

Question 7.

(a) The *arp -a* command shows the full ARP table. The ARP table has the following columns -
Hostname : name of the host device
IP Address : IP address of the host
Hardware Address : MAC address of the host
Hardware Type : type of hardware used for the connection
Iface : network interface

(b) *sudo arp -d* <IP> : delete an entry
sudo arp -s <IP> <HW address> : add an entry

```
(base) lelouch_666@Lancelot-Albion:~$ sudo arp -s 172.16.114.240 a0:8c:fd:de:50:39
(base) lelouch_666@Lancelot-Albion:~$ sudo arp -s 172.16.114.246 a0:8c:fd:e3:d9:31
(base) lelouch_666@Lancelot-Albion:~$ arp -n | grep '172.16.114.240\|172.16.114.246'
172.16.114.246           ether   a0:8c:fd:e3:d9:31   CM                    eno1
172.16.114.240           ether   a0:8c:fd:de:50:39   CM                    eno1
```

(c) ARP works only between devices in the same subnet, and there cannot be an IP from a different subnet in the ARP table of a PC. When a device needs to send a packet to an IP address, it looks if the IP address belongs to a subnet reachable from it through one of its network interfaces. If such an interface is found, this search is complete and the packet is sent. Otherwise, the source sends the packet to a router which can take care of this.

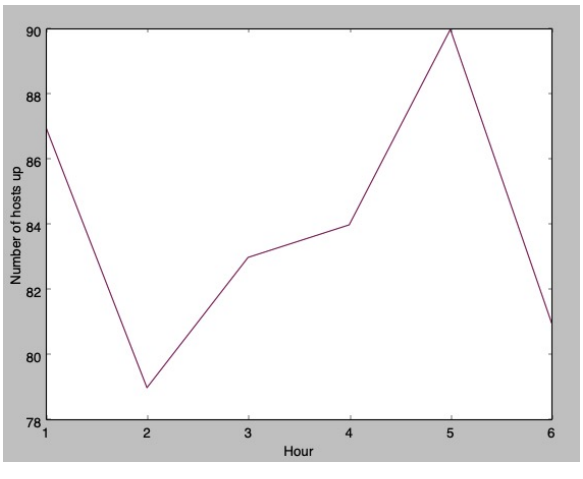
(d) Assuming IPs A and B have the same ethernet address after B's entry was deleted and then added, then we get a 100% packet loss if we ping B. This happens because B tries to connect through a port which is already occupied, and is unable to establish a connection. This results in B being unreachable from other devices in the subnet and hence the ping fails.

Question 8.

(a) *sudo nmap -sn 172.16.114.0/24*

(b) *sudo nmap -sA 172.16.114.203*

(c)



Hour	Number of hosts up
1	87
2	79
3	83
4	84
5	90
6	81