Assignment 1

- Name: Abhiroop Mukherjee
- Roll No.: 510519109
- GSuite: 510519109.abhirup@students.iiests.ac.in

- Subject: Computer Networks Lab (CS 3272)

Question 1

Read the man pages of `ifconfig`, `ping`, `traceroute`, `arp`, `dig`, `nslookup`, and `netstat` and write their utilities in brief

`ifconfig`

- used to configure network interface controller (NIC)
- if no arguments are given, `ifconfig` displays active network interfaces.

`ping <IP>`

- send ICMP ECHO_REQUEST to `<IP>`
- generally used to check if we can access a URI/IP address or not
- `-s` flag is used to define the (amount + 8) bytes that will be sent
    - 8 extra bytes also added to the number as header
- `-c` flag can be used to define how much request to send to the IP, absence of this flag will make the command continuously send request to the IP until we forcefully stop it via Ctrl + C.

`traceroute <IP>`

- print route packets trace to network host
- sends multiple packets to IP incrementing TTL and listens for ICMP "Time Exceeded" reply from the network devices in the path between the the sender and the destination server.

`arp`

- manipulate the system ARP (Address Resolution Protocol) cache.
- if run without any specifier, it will print the current content of the table.

`dig <URL>`

- Domain Information Grouper
- DNS lookup utility
- performs DNS lookup of the `<URL>` using the DNS IP mentioned in `/etc/resolv.conf` and returns the IP

`nslookup`

- query Internet name server interactively
- same work as `dig` but runs interactively
- we can do `nslookup <IP>` to reverse domain search, i.e find URL from the IP.

`netstat`

- Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships
- running without any flags displays all active internet connections and connected sockets

Question 2

Find the IP and hardware addresses of your machine using `ifconfig` command.

- output of `ifconfig`

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.18.105.60  netmask 255.255.240.0  broadcast
172.18.111.255
        inet6 fe80::215:5dff:fef2:6475  prefixlen 64  scopeid
0x20<link>
        ether 00:15:5d:f2:64:75  txqueuelen 1000  (Ethernet)
        RX packets 714  bytes 169651 (169.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 265  bytes 46103 (46.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 59520  bytes 39758752 (39.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 59520  bytes 39758752 (39.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- hence my computer IP is `172.18.105.60` with physical address `00:15:5d:f2:64:75`

Question 3

Use `ping <AnyURL>` command and find out

1. the average RTT (round trip time).
2. the %packet loss
3. size of packet that is sent to `<AnyURL>` server.
4. size of packet that is received by your machine.

- output of `ping www.google.com -s 56 -c 5`

```
PING www.google.com (142.250.183.68) 56(84) bytes of data.
64 bytes from bom12s12-in-f4.1e100.net (142.250.183.68): icmp_seq=1
ttl=116 time=136 ms
64 bytes from bom12s12-in-f4.1e100.net (142.250.183.68): icmp_seq=2
ttl=116 time=12.1 ms
64 bytes from bom12s12-in-f4.1e100.net (142.250.183.68): icmp_seq=3
ttl=116 time=31.1 ms
64 bytes from bom12s12-in-f4.1e100.net (142.250.183.68): icmp_seq=4
ttl=116 time=17.5 ms
64 bytes from bom12s12-in-f4.1e100.net (142.250.183.68): icmp_seq=5
ttl=116 time=13.7 ms

--- www.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 12.090/41.986/135.676/47.318 ms
```

- hence
    - average rtt : 41.986 ms
    - %packet loss = 0%
    - size of packet sent: 56 + 8 = 64 bytes
    - size of packet received: 64 bytes

Question 4

Use `dig <AnyURL>` command and find out

1. the IP address of `<AnyURL>`.
2. the IP addresses of DNS servers.

- output of `dig www.google.com`

```
; <<>> DiG 9.16.1-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65227
;; flags: qr rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         0       IN      A       142.250.183.68

;; Query time: 20 msec
;; SERVER: 172.18.96.1#53(172.18.96.1)
;; WHEN: Fri Jan 14 21:42:10 IST 2022
;; MSG SIZE  rcvd: 62
```

- hence
    - ip address of www.google.com : 142.250.183.68
    - ip address of the DNS server(s) : 172.18.96.1#53

Question 5

Use `traceroute <AnyURL>` and find out

1. number of hops in between your machine and `<AnyURL>` server.
2. the IP address of your network gateway of your subnet.

- output of `traceroute www.google.com`

```
traceroute to www.google.com (142.250.183.68), 30 hops max, 60 byte
packets
1  LAPTOP-TNR28RHP.mshome.net (172.18.96.1)  0.392 ms  0.365 ms  0.356
ms
2  192.168.0.1 (192.168.0.1)  26.937 ms  9.214 ms  26.922 ms
3  192.168.1.251 (192.168.1.251)  26.919 ms  26.911 ms  26.906 ms
4  * * *
5  static-mum-59.185.210.201.mtnl.net.in (59.185.210.201)  26.792 ms *
39.136 ms
6  static-mum-59.185.210.210.mtnl.net.in (59.185.210.210)  38.828 ms
37.391 ms  37.365 ms
7  74.125.51.205 (74.125.51.205)  37.303 ms  29.599 ms *
8  * * *
9  72.14.237.10 (72.14.237.10)  9.516 ms 216.239.56.34 (216.239.56.34)
13.659 ms 142.250.210.182 (142.250.210.182)  71.803 ms
10  108.170.238.199 (108.170.238.199)  71.792 ms * *
11  bom12s12-in-f4.1e100.net (142.250.183.68)  73.007 ms  72.997 ms *
```

- Hence
    - No. of hops: 11
    - IP address of the network gateway of my subnet: the first traceroute ip address: 172.18.96.1

Question 6

Use `arp` command to find out the MAC address of the device that is performing as your network gateway.

- output of `arp`

```
Address                  HWtype  HWaddress           Flags Mask
Iface
LAPTOP-TNR28RHP.mshome.  ether   00:15:5d:f2:6c:b7   C
eth0
```

- Hence MAC address: 00:15:5d:f2:6c:b7

Question 7

Use `nslookup <AnyURL>` command and find out the IP address of `<AnyURL>`. Use `nslookup <IP address>` command and perform reverse domain lookup.

- output of `nslookup www.google.com`

```
Server:         172.18.96.1
Address:        172.18.96.1#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.183.68
Name:   www.google.com
Address: 2404:6800:4009:800::2004
```

- hence output IP address of www.google.com is 142.250.183.68
- output of `nslookup 142.250.183.68`

```
68.183.250.142.in-addr.arpa     name = bom12s12-in-f4.1e100.net.
```

- hence the name of the server is bom12s12-in-f4.1e100.net.

Question 8

Use `netstat` command and find out the active connections of your machine.

- output of `netstat`

```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address
State
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     17492
unix  3      [ ]         STREAM     CONNECTED     16532    @/tmp/dbus-
CZuKp0IpBo
unix  3      [ ]         STREAM     CONNECTED     21516
unix  3      [ ]         STREAM     CONNECTED     21515
unix  3      [ ]         STREAM     CONNECTED     17460
unix  3      [ ]         STREAM     CONNECTED     17461
unix  2      [ ]         SEQPACKET  CONNECTED     78
```