Assignment 1

- **Name:** Arnab Sen
- **Roll:** 510519006
- **Gsuite:** 510519006.arnab@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.

Answer 1

`ifconfig`

- used to configure kernel-resident network interfaces.
- displays detailed information about the active interfaces.

`ping`

- checks if the internet connection to the destination host is available or not.
- gives information about the round-trip delay in communicating with the host.
- tells us the percentage of packet losss.

`traceroute`

- helps figure out the routing hops data has to go through, as well as response delays as it travels across nodes.
- enables you to locate where the data was unable to be sent along, known as points of failure.

`arp`

- viewing and modifying the local Address Resolution Protocol (ARP) cache, which contains recently resolved MAC addresses of Internet Protocol (IP) hosts on the network.

`dig`

- query information about various DNS records.

`nslookup`

- use to diagnose Domain Name System (DNS) infrastructure.
- If the host is an Internet address and the query type is A or PTR, the nslookup command returns the name of the host.
- If the host is a name and does not have a trailing period, the search list is used to qualify the name.

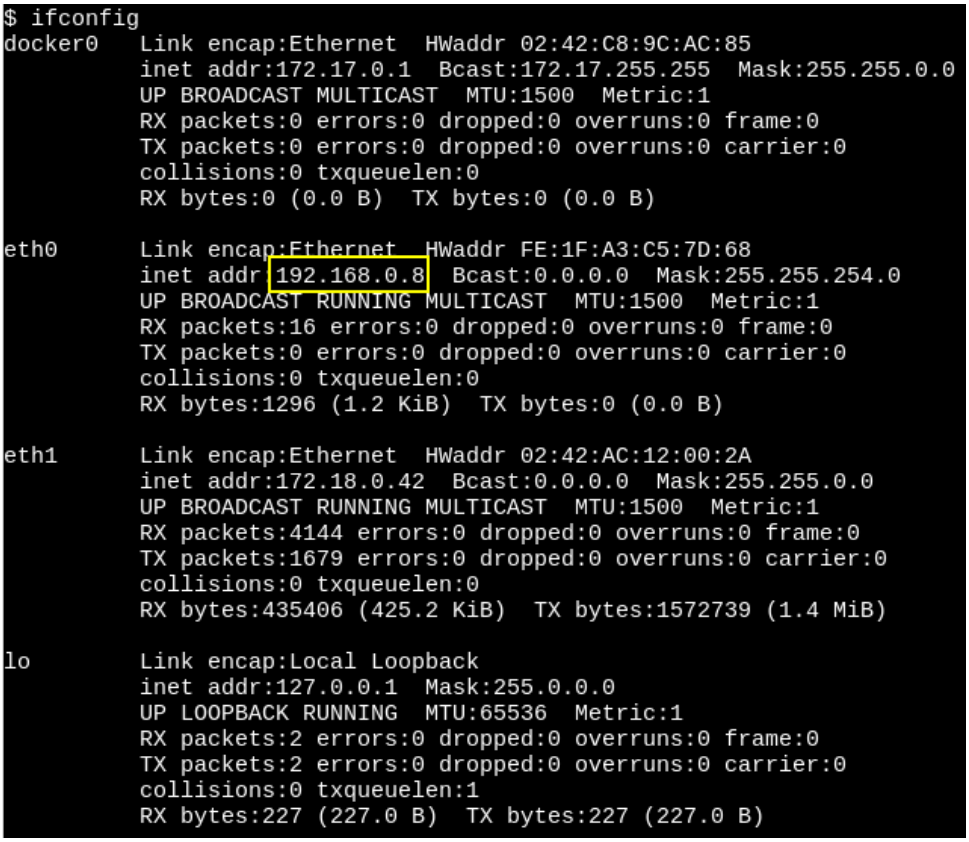
`netstat`

- Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols).

Question 2

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

Answer 2



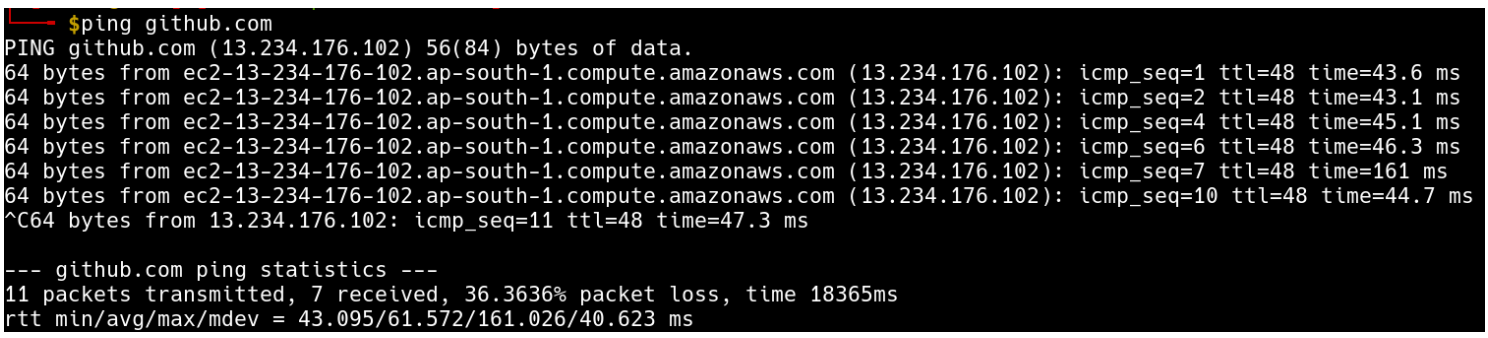
```
$ ifconfig
docker0   Link encap:Ethernet  HWaddr 02:42:C8:9C:AC:85
          inet addr:172.17.0.1  Bcast:172.17.255.255  Mask:255.255.0.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth0      Link encap:Ethernet  HWaddr FE:1F:A3:C5:7D:68
          inet addr:192.168.0.8  Bcast:0.0.0.0  Mask:255.255.254.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1296 (1.2 KiB)  TX bytes:0 (0.0 B)

eth1      Link encap:Ethernet  HWaddr 02:42:AC:12:00:2A
          inet addr:172.18.0.42  Bcast:0.0.0.0  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4144 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1679 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:435406 (425.2 KiB)  TX bytes:1572739 (1.4 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:227 (227.0 B)  TX bytes:227 (227.0 B)
```

- IP address is: `192.168.0.8`.
- HW address is: `FE:1F:A3:C5:7D:68`.

Question 3

Use `ping <AnyURL>` command and find out i. the average RTT (round trip time). ii. the %packet loss. iii. size of packet that is sent to `<AnyURL>` server. iv. size of packet that is received by your machine.

Answer 3



```
└──╼ $ping github.com
PING github.com (13.234.176.102) 56(84) bytes of data.
64 bytes from ec2-13-234-176-102.ap-south-1.compute.amazonaws.com (13.234.176.102): icmp_seq=1 ttl=48 time=43.6 ms
64 bytes from ec2-13-234-176-102.ap-south-1.compute.amazonaws.com (13.234.176.102): icmp_seq=2 ttl=48 time=43.1 ms
64 bytes from ec2-13-234-176-102.ap-south-1.compute.amazonaws.com (13.234.176.102): icmp_seq=4 ttl=48 time=45.1 ms
64 bytes from ec2-13-234-176-102.ap-south-1.compute.amazonaws.com (13.234.176.102): icmp_seq=6 ttl=48 time=46.3 ms
64 bytes from ec2-13-234-176-102.ap-south-1.compute.amazonaws.com (13.234.176.102): icmp_seq=7 ttl=48 time=161 ms
64 bytes from ec2-13-234-176-102.ap-south-1.compute.amazonaws.com (13.234.176.102): icmp_seq=10 ttl=48 time=44.7 ms
^C64 bytes from 13.234.176.102: icmp_seq=11 ttl=48 time=47.3 ms

--- github.com ping statistics ---
11 packets transmitted, 7 received, 36.3636% packet loss, time 18365ms
rtt min/avg/max/mdev = 43.095/61.572/161.026/40.623 ms
```

1. Average RTT is: `61.572 ms`.

2. Packet Loss is: `36.3636%` .
3. Size of packet sent ot `github.com` is: `56 bytes` .
4. Size of packet received is: `64 bytes` .

Question 4

Use `dig <AnyURL>` command and find out i. the IP address of `<AnyURL>` . ii. the IP addresses of DNS servers.

Answer 4

```
└── $dig github.com

; <<>> DiG 9.16.15-Debian <<>> github.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33940
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;github.com.                    IN      A

;; ANSWER SECTION:
github.com.             60      IN      A       13.234.210.38

;; Query time: 51 msec
;; SERVER: 10.10.0.1#53(10.10.0.1)
;; WHEN: Wed Jan 12 20:59:48 IST 2022
;; MSG SIZE  rcvd: 55
```

1. IP Address of `github.com` is: `13.234.210.38` .
2. IP Address of DNS server is: `10.10.0.1` .

Question 5

Use `traceroute <AnyURL>` and find out i. number of hops in between your machine and `<AnyURL>` server. ii. the IP address of your network gateway of your subnet.

Answer 5

```
└─── $sudo traceroute github.com -I
[sudo] password for arnab:
traceroute to github.com (13.234.210.38), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.1)  4.927 ms  4.855 ms  4.838 ms
 2  * 172.29.30.1 (172.29.30.1)  7.314 ms *
 3  10.10.0.5 (10.10.0.5)  4.786 ms * *
 4  * * 103.10.208.13 (103.10.208.13)  7.186 ms
 5  * * *
 6  103.27.170.190 (103.27.170.190)  44.875 ms * *
 7  52.95.66.156 (52.95.66.156)  42.071 ms * *
 8  52.95.64.186 (52.95.64.186)  38.456 ms *  38.424 ms
 9  * * *
10  99.83.76.135 (99.83.76.135)  44.625 ms * *
11  99.83.76.142 (99.83.76.142)  39.279 ms * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  ec2-13-234-210-38.ap-south-1.compute.amazonaws.com (13.234.210.38)  43.705 ms * *
```

1. Number of hops between my machine and `github.com` is: `18` .
2. IP address of my network gateway is: `192.168.1.1` .

Question 6

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

Answer 6

```
└─── $arp
_gateway (192.168.1.1) at 7d:b9:6c:44:d3:e6 [ether] on wlan0
```

MAC address of the device that is performing as my network gateway is: `7d:b9:6c:44:d3:e6` .

Question 7

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

Answer 7

```
└──╼ $nslookup github.com
Server:         10.10.0.1
Address:        10.10.0.1#53

Non-authoritative answer:
Name:   github.com
Address: 13.234.210.38

┌─[arnab@kali]─[~/Desktop/Networks-Lab]
└──╼ $nslookup 13.234.210.38
38.210.234.13.in-addr.arpa      name = ec2-13-234-210-38.ap-south-1.compute.amazonaws.com.

Authoritative answers can be found from:
```

- IP address of `github.com` is: `13.234.210.38` .
- Doing a reversse domain lookup I got: `ec2-13-234-210-38.ap-south-1.compute.amazonaws.com`

Question 8

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

Answer 8

```
└──╼ $netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:sunrpc          0.0.0.0:*               LISTEN
tcp        0      0 kali:40016              143.244.210.202:https   TIME_WAIT
tcp        0      0 kali:51810              ec2-3-108-30-176.:https ESTABLISHED
tcp        0      0 kali:58540              199.232.22.208:https    ESTABLISHED
tcp        0      0 kali:51676              a104-108-159-104.:https ESTABLISHED
tcp        0      0 kali:53862              13.67.9.5:https         ESTABLISHED
tcp        0      0 kali:45976              ec2-54-235-48-238:https ESTABLISHED
tcp        0      0 kali:56778              104.16.148.64:https     ESTABLISHED
tcp        0      0 kali:47262              server-54-230-237:https ESTABLISHED
tcp        0      0 kali:58200              69.173.158.64:https     ESTABLISHED
tcp        0      0 kali:42474              ec2-54-95-144-31.:https ESTABLISHED
tcp        0      0 kali:44368              104.20.184.68:https     ESTABLISHED
tcp        0      0 kali:60908              52.170.92.73:https      ESTABLISHED
tcp        0      0 kali:51812              ec2-3-108-30-176.:https ESTABLISHED
tcp        0      0 kali:51682              a104-108-159-104.:https ESTABLISHED
tcp        0      0 kali:56076              server-52-85-236-:https ESTABLISHED
^C
```