Name : Gourav Kumar Shaw
Enrollment Id. : 2020CSB010
Section: Gx
Subject : Computer Network Lab (CS 3272)

Assignment – 1

Q1. Read the man pages of ifconfig, ping, traceroute, arp, dig, nslookup, and netstat and write their utilities in brief.

Answer:

1. ifconfig

- Ifconfig is used to configure the kernel-resident network interfaces. It is used at boot time to set up interfaces as necessary. After that, it is usually only needed when debugging or when system tuning is needed.

- If no arguments are given, ifconfig displays the status of the currently active interfaces. If a single interface argument is given, it displays the status of the given interface only.

- If a single -a argument is given, it displays the status of all interfaces, even those that are down. Otherwise, it configures an interface.

2. 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 losses.
- Ping sends out an ICMP echo request to which it expects an ICMP echo reply response.

3. traceroute

- Helps figure out the routing hops data has to go through, as well as response delays as it travels across nodes.
- Enables us to locate where the data was unable to be sent along, known as points of failure.
- Print the route packets trace to network host.

4. arp

- Address Resolution Protocol (ARP) is a communication protocol used for **discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address**.

5. dig

- Query information about various DNS records.
- Dig (Domain Information Groper) is **a Linux command line utility that performs DNS lookup by querying name servers and displaying the result**

6. nslookup

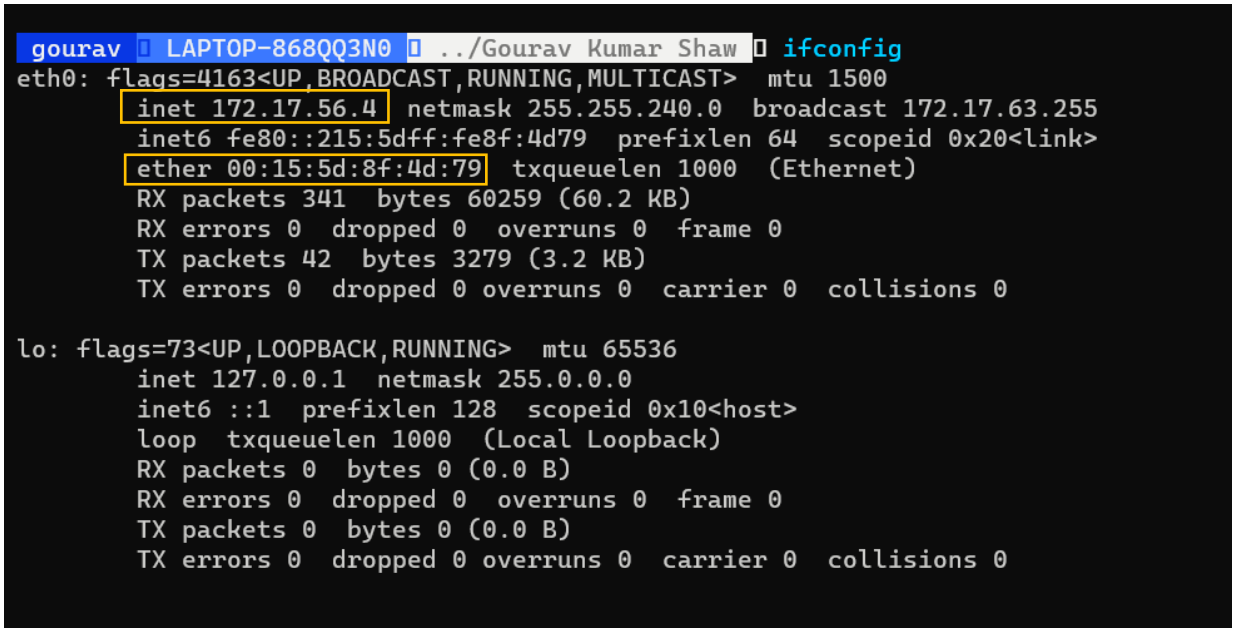
- use to diagnose Domain Name System (DNS) infrastructure.
- If the host is an Internet address and the query type is A or PTR, the nslookup command returns the name of the host.
- If the host is a name and does not have a trailing period, the search list is used to qualify the name.

7. netstat

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

Q2. Find the IP and hardware addresses of your machine using ifconfig command.

Answer:



- IP address is: 172.17.56.4
- HW address is: 00:15:5d:8f:4d:79

Q3. 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:

```
gourav@hamsa:~$ ping google.com
PING google.com (142.251.42.14) 56(84) bytes of data.
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=1 ttl=56 time=41.4 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=2 ttl=56 time=41.0 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=3 ttl=56 time=43.7 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=4 ttl=56 time=40.9 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=5 ttl=56 time=41.0 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=6 ttl=56 time=43.8 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=7 ttl=56 time=43.3 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=8 ttl=56 time=41.0 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=9 ttl=56 time=43.1 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=10 ttl=56 time=45.6 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=11 ttl=56 time=41.0 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=12 ttl=56 time=43.3 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=13 ttl=56 time=70.1 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=14 ttl=56 time=41.5 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=15 ttl=56 time=41.1 ms
64 bytes from bom12s19-in-f14.1e100.net (142.251.42.14): icmp_seq=16 ttl=56 time=47.8 ms
^C
--- google.com ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15020ms
rtt min/avg/max/mdev = 40.996/44.396/70.110/6.907 ms
gourav@hamsa:~$
```

i. Average RTT is: 44.396 ms .

ii. Packet Loss is: 0%.
iii. Size of packet sent of google.com is: 56 bytes.
iv. Size of packet received is: 64 bytes.

Q4. Use “dig <AnyURL>” command and find out

i. the IP address of <AnyURL>.

ii. the IP addresses of local DNS servers of IIEST.

Answer:

```
gourav@hamsa:~$ dig github.com

; <<>> DiG 9.11.3-1ubuntu1.18-Ubuntu <<>> github.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27685
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;github.com.                    IN      A

;; ANSWER SECTION:
github.com.             28      IN      A       20.207.73.82

;; Query time: 23 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Wed Jan 18 21:20:40 IST 2023
;; MSG SIZE  rcvd: 55
```

i. IP Address of github.com is 20.207.73.82

```
gourav@hamsa:~$ dig cs.iiests.ac.in

; <<>> DiG 9.11.3-1ubuntu1.18-Ubuntu <<>> cs.iiests.ac.in
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17353
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;cs.iiests.ac.in.               IN      A

;; ANSWER SECTION:
cs.iiests.ac.in.        3600    IN      A       14.139.223.166

;; Query time: 44 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Wed Jan 18 21:22:52 IST 2023
;; MSG SIZE  rcvd: 60
```

ii. IP addresses of local DNS servers of IIEST is 14.139.223.166

Q5. 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:

```
gourav@hamsa:~$ traceroute google.com
traceroute to google.com (142.251.42.14), 30 hops max, 60 byte packets
 1  _gateway (10.2.0.1)  0.487 ms  0.430 ms  0.382 ms
 2  * * *
 3  10.119.235.13 (10.119.235.13)  4.899 ms  4.889 ms  4.857 ms
 4  * * *
 5  * * *
 6  * * *
 7  10.119.234.162 (10.119.234.162)  24.013 ms  25.641 ms  26.635 ms
 8  72.14.195.56 (72.14.195.56)  28.320 ms  26.652 ms  26.031 ms
 9  74.125.244.195 (74.125.244.195)  38.718 ms 108.170.251.108 (108.170.251.108)  37.318 ms 74.125.244.195 (74.125.244.195)  32.598 ms
10  172.253.69.58 (172.253.69.58)  40.267 ms 72.14.233.107 (72.14.233.107)  31.618 ms 172.253.69.58 (172.253.69.58)  45.261 ms
11  216.239.48.65 (216.239.48.65)  41.688 ms 216.239.54.93 (216.239.54.93)  72.742 ms 216.239.48.65 (216.239.48.65)  47.876 ms
12  108.170.248.161 (108.170.248.161)  46.201 ms  41.317 ms 209.85.250.139 (209.85.250.139)  48.862 ms
13  209.85.250.139 (209.85.250.139)  45.920 ms 209.85.248.61 (209.85.248.61)  46.958 ms  49.710 ms
14  bom12s19-in-f14.1e100.net (142.251.42.14)  41.090 ms  41.754 ms  44.402 ms
```

i. Number of hops between my machine and google.com is:14
ii. IP address of my network gateway is : 10.2.0.1

Q6. Use “arp” command to find out the MAC address of the device that is performing as your network gateway.

Answer:

```
gourav  LAPTOP-868QQ3N0  ../Gourav Kumar Shaw  arp
Address                  HWtype  HWaddress           Flags Mask            Iface
LAPTOP-868QQ3N0.mshome.  ether   00:15:5d:06:01:0d   C                     eth0
```

MAC address of the device that is performing as my network gateway is: 00:15:5d:06:01:0d

Q7. Use nslookup <AnyURL> command and find out the IP address of <AnyURL>. Use nslookup <IP address> command and perform reverse domain lookup.

Answer:

```
gourav@hamsa:~$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.251.42.14
Name:   google.com
Address: 2404:6800:4009:82f::200e

gourav@hamsa:~$ nslookup 142.251.42.14
14.42.251.142.in-addr.arpa      name = bom12s19-in-f14.1e100.net.

Authoritative answers can be found from:
```

- IP address of google.com is (IPv4) : 142.251.42.14
  and (IPv6): 2404:6800:4009:82f: :200e
- Doing a reverse domain lookup I got:
  bom12s19-in-f14.1e100.net

Q8. Use netstat command and find out the active connections of your machine.

Answer:

```
gourav@hamsa:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State

tcp        0      0 hamsa.cs.iiests.a:55060 10.1.76.105:8181        TIME_WAIT
tcp        0      0 hamsa.cs.iiests.a:34752 10.1.76.113:3000        TIME_WAIT
tcp        0      0 hamsa.cs.iiests.a:35496 10.1.76.113:3000        TIME_WAIT
tcp        0      0 localhost:43288         localhost:9099          TIME_WAIT
tcp        0      0 hamsa.cs.iiests.a:47612 10.152.183.1:https      ESTABLISHED
tcp        0      0 localhost:40910         localhost:9099          TIME_WAIT
tcp        0      0 localhost:55332         localhost:19001         ESTABLISHED
tcp        0      0 hamsa.cs.iiests.a:35490 10.1.76.113:3000        TIME_WAIT
tcp        0      0 localhost:58682         localhost:19001         ESTABLISHED
tcp        0      0 hamsa.cs.iiests.a:59566 10.1.76.113:3000        TIME_WAIT
tcp        0      0 localhost:50678         localhost:9099          TIME_WAIT
tcp        0    200 hamsa.cs.iiests.ac.:ssh kaveri.cs.iiests.:44250 ESTABLISHED
tcp        0     35 localhost:56184         localhost:16443         ESTABLISHED
tcp        0      0 hamsa.cs.iiests.a:59550 10.1.76.113:3000        TIME_WAIT
tcp        0      0 hamsa.cs.iiests.a:36200 10.1.76.113:3000        TIME_WAIT
tcp        0      0 hamsa.cs.iiests.a:53412 10.1.76.126:8000        ESTABLISHED
tcp        0      0 hamsa.cs.iiests.a:59574 10.1.76.113:3000        TIME_WAIT
tcp        0      0 hamsa.cs.iiests.a:47332 10.1.76.103:tproxy      TIME_WAIT
tcp        0      0 hamsa.cs.iiests.a:49016 ec2-3-136-132-147:https ESTABLISHED
tcp        0      0 hamsa.cs.iiests.ac.:nfs olinux76.cs.iiests.:780 ESTABLISHED
tcp        0      0 localhost:52692         localhost:9099          TIME_WAIT
tcp        0      0 localhost:50688         localhost:9099          TIME_WAIT
tcp        0      0 hamsa.cs.iiests.a:43198 10.1.76.113:3000        TIME_WAIT
tcp        0      0 hamsa.cs.iiests.a:50932 10.1.76.113:3000        TIME_WAIT
tcp        0      0 hamsa.cs.iiests.a:36214 10.1.76.113:3000        TIME_WAIT
tcp        0      0 localhost:53672         localhost:9099          TIME_WAIT
tcp        0      0 localhost:19001         localhost:58682         ESTABLISHED
tcp        0      0 localhost:35922         localhost:9099          TIME_WAIT
tcp        0      0 hamsa.cs.iiests.a:38850 10.1.76.113:3000        TIME_WAIT
tcp        0      0 localhost:52688         localhost:9099          TIME_WAIT
tcp        0      0 hamsa.cs.iiests.a:50936 10.1.76.113:3000        TIME_WAIT
tcp        0      0 hamsa.cs.iiests.a:36208 10.1.76.113:3000        TIME_WAIT
```