Nirbhay Sharma (B19CSE114)

Computer Network - Lab:2

To install the below commands in linux, do

> sudo apt install net-tools

1. **ifconfig**

    1. if config command is used to configure or display the current network interface information
    2. my system has 2 interface shown below

```
sharma406@LAPTOP-N4BIN1J0:/mnt/d/coding assn sem6/cn assn/assn2$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.31.130.176  netmask 255.255.240.0  broadcast 172.31.143.255
        inet6 fe80::215:5dff:fe85:6d90  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:85:6d:90  txqueuelen 1000  (Ethernet)
        RX packets 51563  bytes 75953706 (75.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19976  bytes 1506988 (1.5 MB)
        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 10216  bytes 13126108 (13.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10216  bytes 13126108 (13.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

    3. command to change ip -

        > sudo ifconfig eth0 172.31.130.177 netmask 255.255.240.0 up

```
sharma406@LAPTOP-N4BIN1J0:/mnt/d/coding assn sem6/cn assn/assn2$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.31.130.177  netmask 255.255.240.0  broadcast 172.31.143.255
        inet6 fe80::215:5dff:fe85:6d90  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:85:6d:90  txqueuelen 1000  (Ethernet)
        RX packets 51563  bytes 75953706 (75.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19976  bytes 1506988 (1.5 MB)
        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 11299  bytes 13231788 (13.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11299  bytes 13231788 (13.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

4. virtual ip address is an address that does not corresponds to the physical network interface

- command for adding a virtual ip address

> sudo ifconfig eth0:0 10.0.0.1

> sudo ifconfig eth0:1 10.0.0.2

> sudo ifconfig eth0:2 10.0.0.3

```
eth0:0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.1  netmask 255.0.0.0  broadcast 10.255.255.255
        ether 00:15:5d:85:6d:90  txqueuelen 1000  (Ethernet)

eth0:1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.2  netmask 255.0.0.0  broadcast 10.255.255.255
        ether 00:15:5d:85:6d:90  txqueuelen 1000  (Ethernet)

eth0:2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.3  netmask 255.0.0.0  broadcast 10.255.255.255
        ether 00:15:5d:85:6d:90  txqueuelen 1000  (Ethernet)
```

2. **route**

1. route command in Linux is used when you want to work with the network routing table. The command allows us to make manual entries into network routing tables using this command we can delete, change, get a partiuclar route
2. using the command

```
sharma406@LAPTOP-N4BIN1J0:/mnt/d/coding assn sem6/cn assn/assn2$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         LAPTOP-N4BIN1J0 0.0.0.0         UG    0      0        0 eth0
172.31.128.0    0.0.0.0         255.255.240.0   U     0      0        0 eth0
```

```
sharma406@LAPTOP-N4BIN1J0:/mnt/d/coding assn sem6/cn assn/assn2$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.31.128.1    0.0.0.0         UG    0      0        0 eth0
172.31.128.0    0.0.0.0         255.255.240.0   U     0      0        0 eth0
```

- from above output we can interpret that if the destination ip is between 172.31.128.0 till Genmask then gateway is * i.e. 0.0.0.0

3. from the above images we can see that thhe packets are forwarding to gateway 172.31.128.1

4. > sudo ip addr add 192.168.178.201/24 dev eth0

5. add route

```
sharma406@LAPTOP-N4BIN1J0:/mnt/d/coding assn sem6/cn assn/assn2$ sudo route add default gw 192.168.178.201
sharma406@LAPTOP-N4BIN1J0:/mnt/d/coding assn sem6/cn assn/assn2$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.178.201 0.0.0.0         UG    0      0        0 eth0
default         LAPTOP-N4BIN1J0 0.0.0.0         UG    0      0        0 eth0
172.24.144.0    0.0.0.0         255.255.240.0   U     0      0        0 eth0
192.168.178.0   0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

7. delete route

```
sharma406@LAPTOP-N4BIN1J0:/mnt/d/coding assn sem6/cn assn/assn2$ sudo route del default
sharma406@LAPTOP-N4BIN1J0:/mnt/d/coding assn sem6/cn assn/assn2$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         LAPTOP-N4BIN1J0 0.0.0.0         UG    0      0        0 eth0
172.24.144.0    0.0.0.0         255.255.240.0   U     0      0        0 eth0
192.168.178.0   0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

3. **arp**

    1. arp flags are as follows
        1. C flag - complete entries are marked with C flag
        2. M flag - permanant entries are marked with M flag
        3. P flag - published entries are marked with P flag
    - some of the flags are shown below

```
sharma406@LAPTOP-N4BIN1J0:/mnt/d/coding assn sem6/cn assn/assn2$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
172.24.144.1             ether   00:15:5d:da:90:48   C                     eth0
sharma406@LAPTOP-N4BIN1J0:/mnt/d/coding assn sem6/cn assn/assn2$ arp -v
Address                  HWtype  HWaddress           Flags Mask            Iface
LAPTOP-N4BIN1J0.mshome.  ether   00:15:5d:da:90:48   C                     eth0
Entries: 1      Skipped: 0      Found: 1
sharma406@LAPTOP-N4BIN1J0:/mnt/d/coding assn sem6/cn assn/assn2$ arp -e
Address                  HWtype  HWaddress           Flags Mask            Iface
LAPTOP-N4BIN1J0.mshome.  ether   00:15:5d:da:90:48   C                     eth0
sharma406@LAPTOP-N4BIN1J0:/mnt/d/coding assn sem6/cn assn/assn2$ arp -a
LAPTOP-N4BIN1J0.mshome.net (172.24.144.1) at 00:15:5d:da:90:48 [ether] on eth0
sharma406@LAPTOP-N4BIN1J0:/mnt/d/coding assn sem6/cn assn/assn2$
```

1. No, we cannot use arp to find MAC address of google.com as arp can run only on local networks

4. **arping**

1. it can be used to find hosts on a particular network
2. we can see the ip using arp list by doing

    ```
    arp -n
    ```

3.
    ```
    sudo apring 172.24.144.1
    ```

```
sharma406@LAPTOP-N4BIN1J0:/mnt/d/coding assn sem6/cn assn/assn2$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
172.24.144.1             ether   00:15:5d:da:90:48   C                     eth0
sharma406@LAPTOP-N4BIN1J0:/mnt/d/coding assn sem6/cn assn/assn2$ sudo arping 172.24.144.1
[sudo] password for sharma406:
ARPING 172.24.144.1
42 bytes from 00:15:5d:da:90:48 (172.24.144.1): index=0 time=319.000 usec
42 bytes from 00:15:5d:da:90:48 (172.24.144.1): index=1 time=449.700 usec
42 bytes from 00:15:5d:da:90:48 (172.24.144.1): index=2 time=582.700 usec
42 bytes from 00:15:5d:da:90:48 (172.24.144.1): index=3 time=543.000 usec
42 bytes from 00:15:5d:da:90:48 (172.24.144.1): index=4 time=484.900 usec
42 bytes from 00:15:5d:da:90:48 (172.24.144.1): index=5 time=569.400 usec
42 bytes from 00:15:5d:da:90:48 (172.24.144.1): index=6 time=505.700 usec
42 bytes from 00:15:5d:da:90:48 (172.24.144.1): index=7 time=729.500 usec
42 bytes from 00:15:5d:da:90:48 (172.24.144.1): index=8 time=645.800 usec
^C
--- 172.24.144.1 statistics ---
9 packets transmitted, 9 packets received,   0% unanswered (0 extra)
rtt min/avg/max/std-dev = 0.319/0.537/0.730/0.111 ms
```

1. arping is different from ping because ping works at network layer and arping works at link layer
2. another point is arping can be run only on local system but ping can also run on remote host

5. **netstat**

   - netstat is used to see the status of an ip such as what ports are listening or are already connected or which ports are using tcp / udp etc. it is also used to see routing tables, interface statistics etc.

   - we can fire various commands to in netstat such as

```
$ netstat -a  (give all the ports)
$ netstat -at (give all tcp ports)
$ netstat -au (gives all udp ports)
$ netstat -l (gives all listening ports)
$ netstat -lt (gives all listening tcp ports)
$ netstat -lu (gives all listening udp ports)
```

   - some commands are shown below:

```
┌─[eu-academy-1]─[10.10.14.197]─[htb-ac261257@pwnbox-base]─[~]
└──╼ [★]$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:5901          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:http            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN
tcp        0      0 htb-ow3epv6cgp.htb:http proxy-uk.htb-clou:39508 ESTABLISHED
tcp        0      0 localhost:39198         localhost:5901          ESTABLISHED
tcp        0      0 localhost:39196         localhost:5901          ESTABLISHED
tcp        0      0 localhost:5901          localhost:39198         ESTABLISHED
tcp        0      0 htb-ow3epv6cgp.htb:http proxy-uk.htb-clou:39504 ESTABLISHED
tcp        0      0 localhost:5901          localhost:39196         ESTABLISHED
tcp6       0      0 localhost:5901          [::]:*                  LISTEN
```

```
┌─[eu-academy-1]─[10.10.14.197]─[htb-ac261257@pwnbox-base]─[~]
└──╼ [★]$ netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 0.0.0.0:36079           0.0.0.0:*
udp        0      0 10.106.0.137:bootpc     169.254.169.253:bootps  ESTABLISHED
udp        0      0 htb-ow3epv6cgp.h:bootpc 169.254.169.253:bootps  ESTABLISHED
udp        0      0 0.0.0.0:ipsec-nat-t     0.0.0.0:*
udp        0      0 0.0.0.0:isakmp          0.0.0.0:*
udp6       0      0 [::]:ipsec-nat-t        [::]:*
udp6       0      0 [::]:isakmp             [::]:*
```

6. **nslookup** (used to query internet name servers)
    - nslookup iitj.ac.in

```
sharma406@LAPTOP-N4BIN1J0:/mnt/d/coding assn sem6/cn assn/assn2$ nslookup iitj.ac.in
Server:         172.24.144.1
Address:        172.24.144.1#53

Non-authoritative answer:
Name:   iitj.ac.in
Address: 14.139.37.5
Name:   ns.iitj.ac.in
Address: 14.139.37.4
```

    - nslookup google.com

```
sharma406@LAPTOP-N4BIN1J0:/mnt/d/coding assn sem6/cn assn/assn2$ nslookup google.com
Server:         172.24.144.1
Address:        172.24.144.1#53

Non-authoritative answer:
Name:   google.com
Address: 216.58.196.206
Name:   google.com
Address: 2404:6800:4002:805::200e
```

    - nslookup yahoo.com

```
sharma406@LAPTOP-N4BIN1J0:/mnt/d/coding assn sem6/cn assn/assn2$ nslookup yahoo.com
Server:         172.24.144.1
Address:        172.24.144.1#53

Non-authoritative answer:
Name:   yahoo.com
Address: 74.6.143.26
Name:   yahoo.com
Address: 74.6.231.21
Name:   yahoo.com
Address: 74.6.231.20
Name:   yahoo.com
Address: 74.6.143.25
Name:   yahoo.com
Address: 98.137.11.163
Name:   yahoo.com
Address: 98.137.11.164
Name:   yahoo.com
Address: 2001:4998:124:1507::f001
Name:   yahoo.com
Address: 2001:4998:24:120d::1:0
Name:   yahoo.com
Address: 2001:4998:24:120d::1:1
Name:   yahoo.com
Address: 2001:4998:124:1507::f000
Name:   yahoo.com
Address: 2001:4998:44:3507::8001
Name:   yahoo.com
Address: 2001:4998:44:3507::8000
```

- the output can be explained in this way like it is showing us the DNS name and address for a paricular ip which are present in our DNS cache

7. **ssh**

- connecting to iitj remote server

> ssh u108@172.25.0.42

```
┌──[zsh@LINUX]-[~]
└─── ❯❯❯ ssh u108@172.25.0.42
u108@172.25.0.42's password:
Activate the web console with: systemctl enable --now cockpit.socket

Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Fri Jan 28 14:04:24 2022 from 192.168.80.9
[u108@gpu2 ~]$ ls
Pytorch_CV_Lab  Untitled.ipynb  file1.txt  testfiel.ipynb
[u108@gpu2 ~]$
```

- keygen

```
sharma406@LAPTOP-N4BIN1J0:/mnt/d/coding assn sem6/cn assn/assn2$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/sharma406/.ssh/id_rsa): key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in key
Your public key has been saved in key.pub
The key fingerprint is:
SHA256:QQtdJ7BugcjcDm45S7A9ZeIxU9Y0mX99GnITRQ8/hRs sharma406@LAPTOP-N4BIN1J0
The key's randomart image is:
+---[RSA 3072]----+
|      ++==o . .++|
|   o = +=+ o  Eoo|
|  . X = =.    . =o|
|   * @ . o. o * o|
|  . X . S  . o = |
|   o + .      .  |
|    .            |
|                 |
|                 |
+----[SHA256]-----+
```

- scp nirbhay.txt u108@172.25.0.42:

```
┌──[zsh@LINUX]-[/mnt/…/cyber-assn/assn2]
└─── ❯❯❯ ls
Capture1.PNG  Capture2.PNG  Report.md  nirbhay.txt

┌──[zsh@LINUX]-[/mnt/…/cyber-assn/assn2]
└─── ❯❯❯ scp nirbhay.txt u108@172.25.0.42:
u108@172.25.0.42's password:
nirbhay.txt                                   100%   22     0.4KB/s   00:00

┌──[zsh@LINUX]-[/mnt/…/cyber-assn/assn2]
└─── ❯❯❯
```

- scp u108@172.25.0.42:file1.txt file1.txt

```
┌──[/mnt/…/cyber-assn/assn2]
└─── ❯❯❯ scp u108@172.25.0.42:file1.txt file1.txt
u108@172.25.0.42's password:
file1.txt                                     100%   88     1.4KB/s   00:00

┌──[zsh@LINUX]-[/mnt/…/cyber-assn/assn2]
└─── ❯❯❯
```

8. **traceroute**
   - It is used to determine the path between two connections, it returns the name and ip of all the routers that occur between two devices
   - examples

```
sharma406@LAPTOP-N4BIN1J0:/mnt/d/coding assn sem6/cn assn/assn2$ traceroute www.google.com
traceroute to www.google.com (142.250.193.196), 30 hops max, 60 byte packets
 1  LAPTOP-N4BIN1J0.mshome.net (172.24.144.1)  1.143 ms  1.086 ms  0.953 ms
 2  EARTH-1010.bbrouter (192.168.1.1)  6.865 ms  6.669 ms  6.780 ms
 3  100.80.0.1 (100.80.0.1)  30.947 ms  30.916 ms  30.862 ms
 4  172.31.200.137 (172.31.200.137)  30.756 ms  30.690 ms  30.674 ms
 5  72.14.195.18 (72.14.195.18)  30.621 ms  30.612 ms  30.569 ms
 6  74.125.244.193 (74.125.244.193)  16.183 ms 74.125.243.97 (74.125.243.97)  27.512 ms 74.125.244.193 (7
4.125.244.193)  17.373 ms
 7  142.251.54.95 (142.251.54.95)  17.346 ms 142.251.54.97 (142.251.54.97)  14.728 ms  14.033 ms
 8  del11s17-in-f4.1e100.net (142.250.193.196)  14.276 ms  14.242 ms  14.235 ms
```

- we can trace packet to iitj.ac.in as follows

```
sharma406@LAPTOP-N4BIN1J0:/mnt/d/coding assn sem6/cn assn/assn2$ sudo traceroute -T iitj.ac.in
[sudo] password for sharma406:
traceroute to iitj.ac.in (14.139.37.5), 30 hops max, 60 byte packets
 1  LAPTOP-N4BIN1J0.mshome.net (172.24.144.1)  0.250 ms  0.207 ms  0.143 ms
 2  EARTH-1010.bbrouter (192.168.1.1)  3.511 ms  3.447 ms  3.419 ms
 3  * * *
 4  172.31.200.137 (172.31.200.137)  17.518 ms  17.439 ms  17.403 ms
 5  172.31.200.49 (172.31.200.49)  14.167 ms  14.148 ms  14.125 ms
 6  172.31.200.168 (172.31.200.168)  14.060 ms  12.993 ms  12.967 ms
 7  136.232.149.125.static.jio.com (136.232.149.125)  16.016 ms  15.196 ms  15.101 ms
 8  172.25.115.26 (172.25.115.26)  17.332 ms  19.137 ms 172.25.115.24 (172.25.115.24)  19.026 ms
 9  172.25.115.26 (172.25.115.26)  18.964 ms 172.25.115.24 (172.25.115.24)  18.856 ms 136.232.148.178.static.jio.com (13
6.232.148.178)  19.001 ms
10  10.119.234.161 (10.119.234.161)  19.046 ms 136.232.148.178.static.jio.com (136.232.148.178)  16.245 ms  16.229 ms
11  * * *
12  * * *
13  * * *
14  14.139.37.109 (14.139.37.109)  51.610 ms *  51.594 ms
15  14.139.37.109 (14.139.37.109)  51.563 ms 14.139.37.5 (14.139.37.5)  49.608 ms 14.139.37.109 (14.139.37.109)  50.603
ms
```

- yes, we can find RTT to using traceroute command, so basically traceroute by default send three packets in one hop and hence it gives three RTT time in ms for each hop
- Traceroute most commonly uses ICMP echo packets for windows
- and for linux / mac it uses UDP packets as default