Experiment 13 **Date:** 13/06/2023

Aim:

Course Outcome(CO2):

Perform system administration tasks.

Procedure:

$ sudo apt update

```
mca@u31:~$ sudo apt update
[sudo] password for mca:
Hit:1 http://in.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:4 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [2,23
2 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu focal-updates/main i386 Packages [838
kB]
```

$ sudo apt install net-tools

```
mca@u31:~$ sudo apt install net-tools
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 696 not upgraded.
Need to get 196 kB of archives.
After this operation, 864 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu focal/main amd64 net-tools amd64 1.60+
git20180626.aebd88e-1ubuntu1 [196 kB]
Fetched 196 kB in 2s (124 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 153306 files and directories currently installed.)
Preparing to unpack .../net-tools_1.60+git20180626.aebd88e-1ubuntu1_amd64.deb ..
.
Unpacking net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Setting up net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Processing triggers for man-db (2.9.1-1) ...
```

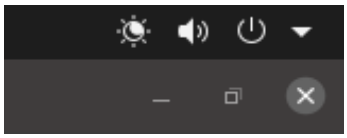
$ ifconfig-used to find out network interface,ip address and mac address

```
mca@u32:~$ ifconfig
enp5s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.6.202  netmask 255.255.255.0  broadcast 192.168.6.255
        inet6 fe80::7561:22e8:9e2b:3433  prefixlen 64  scopeid 0x20<link>
        ether 0c:9d:92:0e:91:2c  txqueuelen 1000  (Ethernet)
        RX packets 108978  bytes 111382007 (111.3 MB)
        RX errors 0  dropped 39  overruns 0  frame 0
        TX packets 51388  bytes 15278403 (15.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

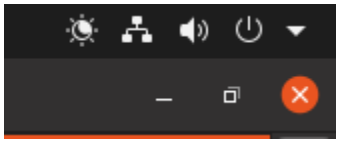
$ sudo apt install ifupdown

```
mca@u31:~$ sudo apt update
[sudo] password for mca:
Hit:1 http://in.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:4 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [2,23
2 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu focal-updates/main i386 Packages [838
kB]
```

$ sudo ifconfig enp5s0 down -used to tear down the network interface



$ sudo ifconfig enp5s0 up - activate nw interface



$ ping google .com

```
mca@u31:~$ ping google.com
PING google.com (142.250.182.78) 56(84) bytes of data.
64 bytes from maa05s20-in-f14.1e100.net (142.250.182.78): icmp_seq=1 ttl=248 tim
e=15.9 ms
64 bytes from maa05s20-in-f14.1e100.net (142.250.182.78): icmp_seq=2 ttl=248 tim
e=15.9 ms
64 bytes from maa05s20-in-f14.1e100.net (142.250.182.78): icmp_seq=3 ttl=248 tim
e=15.9 ms
64 bytes from maa05s20-in-f14.1e100.net (142.250.182.78): icmp_seq=4 ttl=248 tim
e=15.9 ms
```

$ Ping - Used to detect the connectivity between the host and the server
Used for detecting devices on a network and for troubleshooting problems
Eg: **ping google.com** OR **$ ping 192.168.6.201**(ipaddress)

Ping -c 5 google.com -only send 5 packets and stop.

```
mca@u31:~$ ping -c 2 google.com
PING google.com (142.250.193.110) 56(84) bytes of data.
64 bytes from maa05s24-in-f14.1e100.net (142.250.193.110): icmp_seq=1 ttl=248 t
ime=15.1 ms
64 bytes from maa05s24-in-f14.1e100.net (142.250.193.110): icmp_seq=2 ttl=248 t
ime=15.1 ms

--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 15.069/15.085/15.102/0.016 ms
```

If you want to check the connectivity of another server running on the same
Network we can use the **$ ping ip_address**

$ traceroute google.com
$ sudo apt install traceroute

Used to identify the route taken by the packet to reach the destination.

```
mca@u31:~$ traceroute google.com
traceroute to google.com (142.250.182.78), 30 hops max, 60 byte packets
 1  _gateway (192.168.6.100)  0.145 ms  0.121 ms  0.198 ms
 2  136.232.57.109 (136.232.57.109)  1.538 ms  1.517 ms  1.678 ms
 3  172.20.97.57 (172.20.97.57)  14.736 ms  14.718 ms  14.750 ms
 4  172.27.9.126 (172.27.9.126)  16.774 ms  16.739 ms  16.713 ms
 5  172.27.9.125 (172.27.9.125)  16.801 ms  16.367 ms  17.649 ms
 6  172.27.109.51 (172.27.109.51)  16.563 ms  16.414 ms  16.382 ms
 7  172.16.5.90 (172.16.5.90)  16.577 ms  16.773 ms  16.738 ms
 8  108.170.253.106 (108.170.253.106)  16.181 ms 108.170.253.97 (108.170.253.97
)  17.135 ms 142.250.228.80 (142.250.228.80)  17.352 ms
 9  maa05s20-in-f14.1e100.net (142.250.182.78)  16.082 ms 108.170.253.121 (108.
170.253.121)  16.579 ms maa05s20-in-f14.1e100.net (142.250.182.78)  16.004 ms
```

$ sudo apt install whois
$ whois google.com

Used to find all information about a particular domain.

```
mca@u31:~$ whois google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProh
ibited
```

$ nslookup www.ajce.in

```
mca@u31:~$ nslookup www.ajce.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.ajce.in     canonical name = ajce.in.
Name:   ajce.in
Address: 103.148.156.198
```

$ wget “download link”

```
mca@u31:~$ wget https://ia801006.us.archive.org/13/items/OceanofPDF.comTheAlche
mist/_OceanofPDF.com_The_Alchemist.pdf
--2023-06-13 15:05:57--  https://ia801006.us.archive.org/13/items/OceanofPDF.co
mTheAlchemist/_OceanofPDF.com_The_Alchemist.pdf
Resolving ia801006.us.archive.org (ia801006.us.archive.org)... 207.241.228.86
Connecting to ia801006.us.archive.org (ia801006.us.archive.org)|207.241.228.86|
:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1102910 (1.1M) [application/pdf]
Saving to: '_OceanofPDF.com_The_Alchemist.pdf'

_OceanofPDF.com_The 100%[==================>]   1.05M   344KB/s    in 3.1s

2023-06-13 15:06:01 (344 KB/s) - '_OceanofPDF.com_The_Alchemist.pdf' saved [110
2910/1102910]
```

$ sudo tcpdump

To capture the packets of current network interface along with time

```
mca@u31:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:13:44.507461 ARP, Request who-has 192.168.6.144 tell 192.168.6.126, length 4
6
15:13:44.509051 IP u31.35952 > dns.google.domain: 51872+ [1au] PTR? 144.6.168.1
92.in-addr.arpa. (55)
15:13:44.526580 IP dns.google.domain > u31.35952: 51872 NXDomain 0/0/1 (55)
15:13:44.526804 IP u31.35952 > dns.google.domain: 51872+ PTR? 144.6.168.192.in-
addr.arpa. (44)
```

$ sudo tcpdump -D

Available network insterface

```
mca@u31:~$ sudo tcpdump -D
1.enp5s0 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
```

$ sudo tcpdump -i enp5s0

To capture packets from one interface,

```
mca@u31:~$ sudo tcpdump -i enp5s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:25:07.988232 IP maa03s46-in-f10.1e100.net.https > u31.57370: Flags [P.], seq
 4031706644:4031706729, ack 4149293171, win 1050, options [nop,nop,TS val 28428
92389 ecr 2231929350], length 85
15:25:07.988277 IP u31.57370 > maa03s46-in-f10.1e100.net.https: Flags [.], ack
85, win 1461, options [nop,nop,TS val 2231937412 ecr 2842892389], length 0
15:25:07.988292 IP maa03s46-in-f10.1e100.net.https > u31.57370: Flags [P.], seq
```

$ sudo tcpdump -c 5 -i enp5s0

Capture particular number (5) of packets from a particular interface

```
mca@u31:~$ sudo tcpdump -c 5 -i enp5s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:29:41.077405 IP 192.168.6.93.6771 > 239.192.152.143.6771: UDP, length 137
15:29:41.078974 IP u31.60095 > dns.google.domain: 28844+ [1au] PTR? 143.152.192
.239.in-addr.arpa. (57)
15:29:41.122244 IP dns.google.domain > u31.60095: 28844 NXDomain 0/1/1 (114)
15:29:41.122510 IP u31.60095 > dns.google.domain: 28844+ PTR? 143.152.192.239.i
n-addr.arpa. (46)
15:29:41.130385 ARP, Request who-has 192.168.6.142 tell _gateway, length 46
5 packets captured
25 packets received by filter
0 packets dropped by kernel
```

$ sudo tcpdump -A -i enp5s0

Askey formatted display of details’

```
mca@u31:~$ sudo tcpdump -A -i enp5s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:28:31.032829 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request
 from 04:09:73:fd:e4:7c (oui Unknown), length 261
E..!....@.y.........D.C..7L....u}.....................       s..|..........
..............................................................................
..............................................................................
.............................c.Sc5..9..@7.}.B.*....C..
15:28:31.231771 ARP, Request who-has 192.168.90.1 tell 192.168.90.60, length 46
........D1...U..Z<........Z...................
15:28:31.232493 IP u31.37711 > dns.google.domain: 49463+ [1au] PTR? 1.90.168.19
2.in-addr.arpa. (54)
E..R..@.@.............O.5.>...7...........1.90.168.192.in-addr.arpa.......).....
```

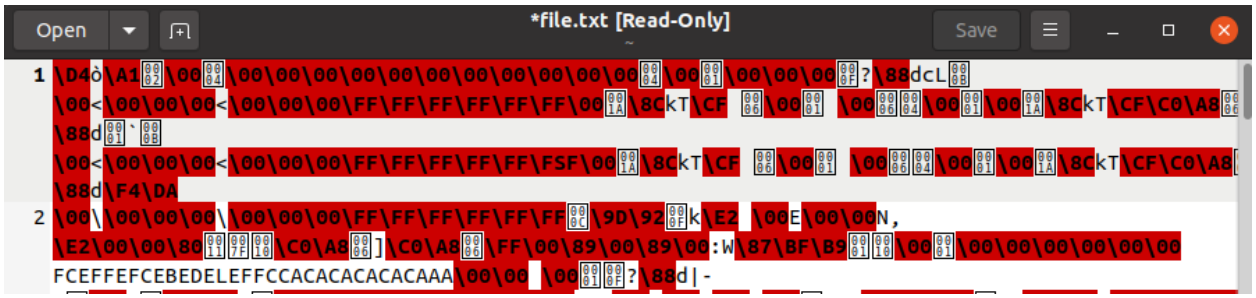
$ sudo tcpdump -XX -i enp5s0

Display the captured packets in hexadecimal format.

```
mca@u31:~$ sudo tcpdump -XX -i enp5s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp5s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:31:29.771321 ARP, Request who-has 192.168.6.144 tell _gateway, length 46
        0x0000:  ffff ffff ffff 001a 8c6b 54cf 0806 0001  .........kT.....
        0x0010:  0800 0604 0001 001a 8c6b 54cf c0a8 0664  .........kT....d
        0x0020:  0000 0000 0000 c0a8 0690 0000 0000 0000  ................
        0x0030:  0000 0000 0000 0000 0000 0000            ............
15:31:29.772925 IP u31.59126 > dns.google.domain: 20671+ [1au] PTR? 144.6.168.1
92.in-addr.arpa. (55)
```

$ sudo tcpdump -w file.txt -i enp5s0

To save the packet info into a file.



$ sudo tcpdump -r file.txt

To read the packet details saved in the file

$ sudo apt install wireshark

```
mca@u31:~$ sudo apt update
[sudo] password for mca:
Get:1 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Hit:2 http://in.archive.ubuntu.com/ubuntu focal InRelease
Get:3 http://in.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:4 http://security.ubuntu.com/ubuntu focal-security/main amd64 DEP-11 Metada
ta [60.0 kB]
```

$ sudo wireshark