NETWORKING & SYSTEM ADMINISTRATION LAB

Name: Swetha Prakash

Roll No: 46

Batch: MCA B

Date: 02-06-2022

Experiment No.: 20

Aim

Familiarization of basic network commands in linux

Procedure

1. sudo apt update && sudo install tcpdump

This commands in Linux allows you to install the tcpdump packet analyzer on your system

Syntax:- $ sudo apt update && sudo install tcpdump

Output:-

```
mca@S46:~$ sudo apt update && sudo apt install tcpdump
Hit:1 http://in.archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 https://dl.google.com/linux/chrome/deb stable InRelease
Err:3 http://ppa.launchpad.net/jonathonf/python-3.6/ubuntu bionic InRelease
  403  Forbidden [IP: 185.125.190.52 80]
Ign:4 https://repo.mongodb.org/apt/ubuntu trusty/mongodb-org/3.6 InRelease
Get:5 https://repo.mongodb.org/apt/ubuntu trusty/mongodb-org/3.6 Release [2,495 B]
Hit:6 http://ppa.launchpad.net/ubuntu-mozilla-security/ppa/ubuntu bionic InRelease
Hit:7 http://ppa.launchpad.net/webupd8team/java/ubuntu bionic InRelease
Get:8 https://repo.mongodb.org/apt/ubuntu trusty/mongodb-org/3.6 Release.gpg [801 B]
Err:8 https://repo.mongodb.org/apt/ubuntu trusty/mongodb-org/3.6 Release.gpg
  The following signatures were invalid: EXPKEYSIG 58712A2291FA4AD5 MongoDB 3.6 Release Signing Key <packaging@mongodb.com>
Reading package lists... Done
E: Failed to fetch http://ppa.launchpad.net/jonathonf/python-3.6/ubuntu/dists/bionic/InRelease  403  Forbidden [IP: 185.125.190.52 80]
E: The repository 'http://ppa.launchpad.net/jonathonf/python-3.6/ubuntu bionic InRelease' is no longer signed.
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
W: An error occurred during the signature verification. The repository is not updated and the previous index files will be used. GPG error: ht
tps://repo.mongodb.org/apt/ubuntu trusty/mongodb-org/3.6 Release: The following signatures were invalid: EXPKEYSIG 58712A2291FA4AD5 MongoDB 3.
6 Release Signing Key <packaging@mongodb.com>
```

2. sudo tcpdump -D

To see the ist of network interfaces vailable on the system on which tcpdump can capture packets

Syntax:- $ sudo tcpdump -D

Output:-

```
mca@S46:~$ sudo tcpdump -D
1.enp3s0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.docker0 [Up]
5.nflog (Linux netfilter log (NFLOG) interface)
6.nfqueue (Linux netfilter queue (NFQUEUE) interface)
7.usbmon1 (USB bus number 1)
8.usbmon2 (USB bus number 2)
9.usbmon3 (USB bus number 3)
10.usbmon4 (USB bus number 4)
```

3. sudo tcpdump -i enp3s0

To capture the packets following through a specific interface, we can use the -i flag with the interface name. Without the -i interface , tcpdump will pick up the first network interface it comes across.

Syntax:- $ sudo tcpdump -i enp3s0

Output:-

```
mca@S46:~$ sudo tcpdump -i enp3s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:03:56.222780 ARP, Request who-has 192.168.6.135 tell 0.0.0.0, length 46
15:03:56.222798 IP6 fe80::dce6:e9a6:5b6:2af3 > ip6-allnodes: ICMP6, neighbor advertisement, tgt is fe80::dce6:e9a6:5b6:2af3, length 32
15:03:56.223420 IP S46.47507 > dns.google.domain: 27170+ [1au] PTR? 135.6.168.192.in-addr.arpa. (55)
15:03:56.237774 IP dns.google.domain > S46.47507: 27170 NXDomain 0/0/1 (55)
15:03:56.241271 IP S46.33444 > dns.google.domain: 21124+ [1au] PTR? 46.6.168.192.in-addr.arpa. (54)
15:03:56.248263 IP 192.168.6.135.netbios-ns > 192.168.6.255.netbios-ns: NBT UDP PACKET(137): REGISTRATION; REQUEST; BROADCAST
15:03:56.248304 IP 192.168.6.135.netbios-ns > 192.168.6.255.netbios-ns: NBT UDP PACKET(137): REGISTRATION; REQUEST; BROADCAST
15:03:56.255479 ARP, Request who-has 192.168.6.227 tell _gateway, length 46
15:03:56.255490 ARP, Request who-has 192.168.6.228 tell _gateway, length 46
15:03:56.256727 IP S46.50405 > dns.google.domain: 55077+ [1au] PTR? 255.6.168.192.in-addr.arpa. (55)
15:03:56.263658 ARP, Request who-has 192.168.6.254 tell 192.168.6.135, length 46
15:03:56.273724 IP dns.google.domain > S46.50405: 55077 NXDomain 0/0/1 (55)
15:03:56.275068 IP S46.60641 > dns.google.domain: 57373+ [1au] PTR? 227.6.168.192.in-addr.arpa. (55)
15:03:56.289227 IP dns.google.domain > S46.60641: 57373 NXDomain 0/0/1 (55)
15:03:56.308929 IP S46.37917 > dns.google.domain: 36766+ [1au] PTR? 228.6.168.192.in-addr.arpa. (55)
15:03:56.326678 IP S46.54361 > dns.google.domain: 12745+ [1au] PTR? 254.6.168.192.in-addr.arpa. (55)
15:03:56.341118 IP dns.google.domain > S46.54361: 12745 NXDomain 0/0/1 (55)
15:03:56.767195 IP 192.168.6.43.51445 > 239.255.255.250.1900: UDP, length 175
15:03:56.768726 IP 192.168.6.200.58449 > 239.255.255.250.1900: UDP, length 174
15:03:56.768959 IP S46.40964 > dns.google.domain: 25901+ [1au] PTR? 43.6.168.192.in-addr.arpa. (54)
15:03:56.785018 IP dns.google.domain > S46.40964: 25901 NXDomain 0/0/1 (54)
15:03:56.786592 IP S46.42110 > dns.google.domain: 61764+ [1au] PTR? 200.6.168.192.in-addr.arpa. (55)
15:03:56.801789 IP dns.google.domain > S46.42110: 61764 NXDomain 0/0/1 (55)
15:03:56.882797 ARP, Request who-has 10.104.42.7 tell 192.168.6.191, length 46
15:03:56.883527 IP S46.39581 > dns.google.domain: 4315+ [1au] PTR? 7.42.104.10.in-addr.arpa. (53)
15:03:56.899340 IP dns.google.domain > S46.39581: 4315 NXDomain 0/0/1 (53)
15:03:56.900824 IP S46.37326 > dns.google.domain: 25028+ [1au] PTR? 191.6.168.192.in-addr.arpa. (55)
```

4. sudo tcpdump -c 5 –i enp3s0

This command is used to show the details of last 4 packets only

Syntax:- $ sudo tcpdump -c 5 -i enp3s0

Output:-

```
mca@S46:~$ sudo tcpdump -c 5 -i enp3s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:04:10.665489 IP 192.168.6.212.50031 > 224.0.0.253.3544: UDP, length 40
15:04:10.667403 IP S46.34487 > dns.google.domain: 1491+ [1au] PTR? 212.6.168.192.in-addr.arpa. (55)
15:04:10.679795 IP 192.168.6.69.51963 > 239.255.255.250.1900: UDP, length 175
15:04:10.683669 IP dns.google.domain > S46.34487: 1491 NXDomain 0/0/1 (55)
15:04:10.685177 IP S46.49832 > dns.google.domain: 54526+ [1au] PTR? 46.6.168.192.in-addr.arpa. (54)
5 packets captured
12 packets received by filter
3 packets dropped by kernel
```

5. sudo tcpdump -XX -i enp3s0

This command helps to see the information of the ip address in terms of ipv6 addressing (in hexadecimal format)

Syntax:- $ sudo tcpdump -XX -i enp3s0

Output:-

```
mca@S46:~$ sudo tcpdump -XX -i enp3s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:04:32.636133 IP 192.168.6.53.mdns > 224.0.0.251.mdns: 0 PTR (QM)? _googlecast._tcp.local. (40)
        0x0000:  0100 5e00 00fb 2c56 dc9b c19f 0800 4500  ..^...,V......E.
        0x0010:  0044 63c1 4000 0111 6e0f c0a8 0635 e000  .Dc.@...n....5..
        0x0020:  00fb 14e9 14e9 0030 e3ca 0000 0000 0001  .......0........
        0x0030:  0000 0000 0000 0b5f 676f 6f67 6c65 6361  ......._googleca
        0x0040:  7374 045f 7463 7005 6c6f 6361 6c00 000c  st._tcp.local...
        0x0050:  0001                                     ..
15:04:32.638498 IP S46.55391 > dns.google.domain: 28575+ [1au] PTR? 53.6.168.192.in-addr.arpa. (54)
        0x0000:  001a 8c6b 54cf 7824 afba c213 0800 4500  ...kT.x$......E.
        0x0010:  0052 5f2f 4000 4011 0486 c0a8 062e 0808  .R_/@.@.........
        0x0020:  0808 d85f 0035 003e 596d 6f9f 0100 0001  ..._.5.>Ymo.....
        0x0030:  0000 0000 0001 0235 3301 3603 3136 3803  .......53.6.168.
        0x0040:  3139 3207 696e 2d61 6464 7204 6172 7061  192.in-addr.arpa
        0x0050:  0000 0c00 0100 0029 0200 0000 0000 0000  .......).........
15:04:32.642598 IP 192.168.6.28.mdns > 224.0.0.251.mdns: 0 PTR (QM)? _googlecast._tcp.local. (40)
        0x0000:  0100 5e00 00fb 4016 7eae 103b 0800 4500  ..^...@.~..;..E.
        0x0010:  0044 8617 4000 0111 4bd2 c0a8 061c e000  .D..@...K.......
        0x0020:  00fb 14e9 14e9 0030 e3e3 0000 0000 0001  .......0........
        0x0030:  0000 0000 0000 0b5f 676f 6f67 6c65 6361  .......googleca
        0x0040:  7374 045f 7463 7005 6c6f 6361 6c00 000c  st._tcp.local...
        0x0050:  0001                                     ..
15:04:32.655276 IP dns.google.domain > S46.55391: 28575 NXDomain 0/0/1 (54)
        0x0000:  7824 afba c213 001a 8c6b 54cf 0800 4500  x$.......kT...E.
        0x0010:  0052 3b37 0000 3c11 6c7e 0808 0808 c0a8  .R;7..<.l~......
        0x0020:  062e 0035 d85f 003e d8e9 6f9f 8183 0001  ...5._.>..o.....
        0x0030:  0000 0000 0001 0235 3301 3603 3136 3803  .......53.6.168.
        0x0040:  3139 3207 696e 2d61 6464 7204 6172 7061  192.in-addr.arpa
        0x0050:  0000 0c00 0100 0029 0200 0000 0000 0000  .......).........
15:04:32.657136 IP S46.48618 > dns.google.domain: 22002+ [1au] PTR? 46.6.168.192.in-addr.arpa. (54)
        0x0000:  001a 8c6b 54cf 7824 afba c213 0800 4500  ...kT.x$......E.
        0x0010:  0052 5f30 4000 4011 0485 c0a8 062e 0808  .R_0@.@.........
        0x0020:  0808 bdea 0035 003e 8a90 55f2 0100 0001  .....5.>..U.....
        0x0030:  0000 0000 0001 0234 3601 3603 3136 3803  .......46.6.168.
```

6. sudo tcpdump -i enp3s0 –c 5 port 80

To access information of packet from a specific port number

Syntax: $ sudo tcpdump -i <your_ethernet_interface> -c5 port <port_number>

Output:-

```
mca@S46:~$ sudo tcpdump -i enp3s0 -c 5 port 80
\[sudo] password for mca:
Sorry, try again.
[sudo] password for mca:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:17:28.192283 IP S46.36030 > 123.35.104.34.bc.googleusercontent.com.http: Flags [.], ack 1683466236, win 24576, options [nop,nop,TS val 1431
967724 ecr 1271307211], length 0
14:17:28.791616 IP S46.48944 > 84.170.224.35.bc.googleusercontent.com.http: Flags [S], seq 2706376065, win 29200, options [mss 1460,sackOK,TS
val 2208167591 ecr 0,nop,wscale 7], length 0
14:17:29.033444 IP 84.170.224.35.bc.googleusercontent.com.http > S46.48944: Flags [S.], seq 2312560620, ack 2706376066, win 64768, options [ms
s 1420,sackOK,TS val 3355191856 ecr 2208167591,nop,wscale 7], length 0
14:17:29.033533 IP S46.48944 > 84.170.224.35.bc.googleusercontent.com.http: Flags [.], ack 1, win 229, options [nop,nop,TS val 2208167833 ecr
3355191856], length 0
14:17:29.033714 IP S46.48944 > 84.170.224.35.bc.googleusercontent.com.http: Flags [P.], seq 1:88, ack 1, win 229, options [nop,nop,TS val 2208
167834 ecr 3355191856], length 87: HTTP: GET / HTTP/1.1
5 packets captured
5 packets received by filter
0 packets dropped by kernel
```

7. sudo tcpdump –i enp3s0 icmp

To filter packets based on ICMP protocol.

Syntax : $ sudo tcpdump –i enp3s0 icmp

Output:-

```
mca@S46:~$ sudo tcpdump -i enp3s0 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:20:33.516886 IP 192.168.6.41 > S46: ICMP 192.168.6.41 udp port 56061 unreachable, length 98
14:20:33.518703 IP 192.168.6.41 > S46: ICMP 192.168.6.41 udp port 58155 unreachable, length 98
14:20:33.573973 IP 192.168.6.41 > S46: ICMP 192.168.6.41 udp port 52680 unreachable, length 98
14:20:33.575323 IP 192.168.6.41 > S46: ICMP 192.168.6.41 udp port 48289 unreachable, length 98
14:20:33.587330 IP 192.168.6.41 > S46: ICMP 192.168.6.41 udp port 59502 unreachable, length 98
14:20:33.588733 IP 192.168.6.41 > S46: ICMP 192.168.6.41 udp port 59111 unreachable, length 98
14:21:02.296065 IP 192.168.6.42 > S46: ICMP 192.168.6.42 udp port 56032 unreachable, length 98
14:21:02.372292 IP 192.168.6.42 > S46: ICMP 192.168.6.42 udp port 50518 unreachable, length 98
14:21:02.385999 IP 192.168.6.42 > S46: ICMP 192.168.6.42 udp port 35869 unreachable, length 98
14:21:02.386974 IP 192.168.6.42 > S46: ICMP 192.168.6.42 udp port 46359 unreachable, length 98
^C
10 packets captured
10 packets received by filter
0 packets dropped by kernel
```

7. sudo tcpdump -i enp3s0 -c 10 -w icmp.pcap

To store packet information limited by lines,words

Syntax:- $ sudo tcpdump -i <your_ethernet_interface> -c <lines> -w <filename>

Output:-

```
mca@S46:~$ sudo tcpdump -i enp3s0 -c 10 -w icmp.pcap
tcpdump: listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
10 packets captured
27 packets received by filter
0 packets dropped by kernel
```

8. sudo tcpdump -r icmp.pcap

To read the content of a packet capture by using tcpdump

Syntax: $ sudo tcpdump -r <filename>

Output:-

```
mca@S46:~$ sudo tcpdump -r icmp.pcap
reading from file icmp.pcap, link-type EN10MB (Ethernet)
14:22:06.197171 IP6 fe80::6bb5:9d6e:bb7:fbf.mdns > ff02::fb.mdns: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
14:22:06.595582 IP 192.168.6.93.52680 > 239.255.255.250.1900: UDP, length 175
14:22:06.724620 IP 192.168.6.178.49640 > 239.255.255.250.1900: UDP, length 172
14:22:06.814672 IP S46.53008 > maa05s20-in-f5.1e100.net.https: Flags [.], seq 882305532:882306992, ack 3816759450, win 65535, length 1460
14:22:06.814678 IP S46.53008 > maa05s20-in-f5.1e100.net.https: Flags [P.], seq 1460:1482, ack 1, win 65535, length 22
14:22:06.814785 IP maa05s20-in-f5.1e100.net.https > S46.53008: Flags [.], ack 1460, win 65535, length 0
14:22:06.814795 IP maa05s20-in-f5.1e100.net.https > S46.53008: Flags [.], ack 1482, win 65535, length 0
14:22:06.814801 IP S46.53008 > maa05s20-in-f5.1e100.net.https: Flags [P.], seq 1482:1658, ack 1, win 65535, length 176
14:22:06.814858 IP maa05s20-in-f5.1e100.net.https > S46.53008: Flags [.], ack 1658, win 65535, length 0
14:22:06.830269 IP maa05s20-in-f5.1e100.net.https > S46.53008: Flags [P.], seq 1:40, ack 1658, win 65535, length 39
```

9. sudo apt-get install netcat

To install netcat on Ubuntu.

Syntax: $ sudo apt-get install netcat

```
mca@S46:~$ sudo apt-get install netcat
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libpcre16-3 libpcre3-dev libpcre32-3 libpcrecpp0v5 libssl-dev libssl-doc php-common php-pear php-xml php7.2-cli php7.2-common php7.2-json
  php7.2-opcache php7.2-readline php7.2-xml pkg-php-tools shtool
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  netcat-traditional
The following NEW packages will be installed:
  netcat netcat-traditional
0 upgraded, 2 newly installed, 0 to remove and 13 not upgraded.
Need to get 65.1 kB of archives.
After this operation, 157 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 netcat-traditional amd64 1.10-41.1 [61.7 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 netcat all 1.10-41.1 [3,436 B]
Fetched 65.1 kB in 1s (119 kB/s)
Selecting previously unselected package netcat-traditional.
(Reading database ... 226211 files and directories currently installed.)
Preparing to unpack .../netcat-traditional_1.10-41.1_amd64.deb ...
Unpacking netcat-traditional (1.10-41.1) ...
Selecting previously unselected package netcat.
Preparing to unpack .../netcat_1.10-41.1_all.deb ...
Unpacking netcat (1.10-41.1) ...
Setting up netcat-traditional (1.10-41.1) ...
Setting up netcat (1.10-41.1) ...
Processing triggers for man-db (2.8.3-2) ...
```

10. sudo nc -l -p 1234

To send message from one console and receive from another console by an advanced packet analyser.

Syntax: $ nc -l -p 1234

$ nc <ip address>

Output:-

```
mca@S46:~$ sudo nc -l -p 1234
[sudo] password for mca:
dfdsf
tytyy
kjjfg
jgkjtgkjg
MCA Department
```

```
mca@S46:~$ sudo nc 192.168.6.46 1234
dfdsf
tytyy
kjjfg
jgkjtgkjg
MCA Department
```