

## UCS1511- NETWORKS LAB

Name : Prasanna Kumaran D

RegNo : 185001110

### Exercise 1: Network Commands

#### 1) tcpdump

**Syntax:** tcpdump [-options ] [ -B buffer\_size ]

**Description:** Tcpdump is a command line utility that allows the user to capture and analyze network traffic going through the system. It is often used to help troubleshoot network issues, as well as a security tool.

**Output:**

**tcpdump -d**

```
legion@Legion: ~
File Edit View Search Terminal Help
legion@Legion:~$ tcpdump -D
1.wlo1 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.eno1 [Up]
5.bluetooth0 (Bluetooth adapter number 0)
6.nflog (Linux netfilter log (NFLOG) interface)
7.nfqueue (Linux netfilter queue (NFQUEUE) interface)
8.usbmon1 (USB bus number 1)
9.usbmon2 (USB bus number 2)
legion@Legion:~$
```

**sudo tcpdump -i[interface]**

```
legion@Legion:~$ sudo tcpdump -i wlo1 -c 10
[sudo] password for legion:
Sorry, try again.
[sudo] password for legion:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
22:59:11.296928 IP ec2-3-6-207-117.ap-south-1.compute.amazonaws.com.https > Legion.56540: Flags [P.], seq 1310897265:1310898360, ack 1521682396, win 16, options [nop,nop,TS val 1222547860 ecr 3602585875], length 1095
22:59:11.296874 IP Legion.56540 > ec2-3-6-207-117.ap-south-1.compute.amazonaws.com.https: Flags [.], ack 1095, win 493, options [nop,nop,TS val 3602586212 ecr 1222547860], length 0
22:59:12.059823 IP Legion.36156 > naao5s05-ln-f3.1e100.net.https: Flags [.], ack 2760349968, win 501, options [nop,nop,TS val 3578008966 ecr 2384807126], length 0
22:59:12.059857 IP Legion.46274 > naao5s05-ln-f2.1e100.net.https: Flags [.], ack 549552476, win 501, options [nop,nop,TS val 8901257 ecr 1145358727], length 0
22:59:12.059881 IP Legion.34794 > del03s10-ln-f2.1e100.net.https: Flags [.], ack 859285486, win 875, options [nop,nop,TS val 2073535517 ecr 176633246], length 0
22:59:12.059900 IP Legion.54618 > 161.117.111.214.https: Flags [.], ack 3659155903, win 501, length 0
22:59:12.059911 IP Legion.55422 > del03s16-ln-f2.1e100.net.https: Flags [.], ack 3937637902, win 501, options [nop,nop,TS val 2001643452 ecr 858179855], length 0
22:59:12.209501 IP Legion.32959 > _gateway.domain: 48374+ [1au] PTR: 163.163.217.172.ln-addr.arpa. (57)
22:59:12.228595 IP _gateway.domain > Legion.32959: 48374 1/0/1 PTR naao5s05-ln-f3.1e100.net. (95)
22:59:12.229803 IP Legion.53294 > _gateway.domain: 39526+ [1au] PTR: 162.163.217.172.ln-addr.arpa. (57)
10 packets captured
50 packets received by filter
42 packets dropped by kernel
legion@Legion:~$ ^C
legion@Legion:~$
```

#### 2) netstat:

**Syntax:** netsat [-option]

**Description:** netstat is one of a number of command- line tools available to check the functioning of a network. It provides a way to check if various aspects of TCP/IP are working and what connections are present.

**Output:**

netstat -a

```
legion@Legion:~$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 Legion:55696            del03s17-in-f14.1:https ESTABLISHED
tcp        0      0 Legion:39060            104.19.155.83:https    ESTABLISHED
tcp        0      0 Legion:53896            e2a.google.com:https   ESTABLISHED
tcp        0      0 Legion:50954            maa03s22-in-f161.:https ESTABLISHED
tcp        0      0 Legion:33082            del11s05-in-f2.1e:https ESTABLISHED
tcp        0      0 Legion:37984            whatsapp-cdn-shv-:https ESTABLISHED
tcp        0      0 Legion:53894            e2a.google.com:https   ESTABLISHED
tcp        0      0 Legion:49132            ec2-52-212-195-14:https ESTABLISHED
tcp        0      0 Legion:36038            del03s17-in-f3.1e:https ESTABLISHED
tcp        0      0 Legion:33112            del03s17-in-f10.1:https ESTABLISHED
tcp        0      0 Legion:43952            del03s15-in-f3.1e:https ESTABLISHED
tcp        0      0 Legion:36476            maa05s05-in-f3.1e:https ESTABLISHED
tcp        0      0 Legion:41678            server-54-230-90-:https ESTABLISHED
tcp        0      0 Legion:49446            sa-in-f189.1e100.:https ESTABLISHED
tcp        0      0 Legion:56012            del03s16-in-f2.1e:https ESTABLISHED
tcp        0      0 Legion:42426            maa05s03-in-f4.1e:https ESTABLISHED
tcp        0      0 Legion:35590            del03s18-in-f2.1e:https ESTABLISHED
tcp        0      0 Legion:37450            maa05s01-in-f3.1e:https ESTABLISHED
tcp        0      0 Legion:42630            maa05s06-in-f3.1e:https ESTABLISHED
tcp        0      0 Legion:48124            del03s13-in-f2.1e:https ESTABLISHED
tcp        0      0 Legion:37430            maa03s29-in-f2.1e:https ESTABLISHED
tcp        0      0 Legion:42642            maa05s06-in-f3.1e:https ESTABLISHED
tcp        0      0 Legion:35746            nrt12s12-in-f202.:https ESTABLISHED
tcp        0      0 Legion:35764            nrt12s12-in-f202.:https ESTABLISHED
tcp        0      0 Legion:32956            maa05s06-in-f6.1e:https ESTABLISHED
^C
```

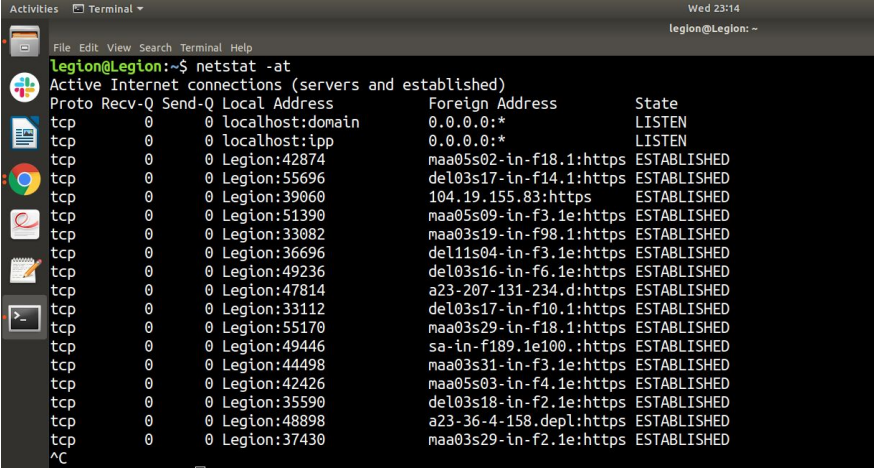
netstat -s

```

legion@Legion:~$ netstat -s
Ip:
  Forwarding: 2
  81592 total packets received
  2 with invalid addresses
  0 forwarded
  0 incoming packets discarded
  81359 incoming packets delivered
  70334 requests sent out
Icmp:
  1 ICMP messages received
  0 input ICMP message failed
  ICMP input histogram:
    destination unreachable: 1
  1 ICMP messages sent
  0 ICMP messages failed
  ICMP output histogram:
    destination unreachable: 1
IcmpMsg:
  InType3: 1
  OutType3: 1
Tcp:
  1090 active connection openings
  0 passive connection openings
  12 failed connection attempts
  277 connection resets received
  43 connections established
  78582 segments received
  75754 segments sent out
  85 segments retransmitted
  3 bad segments received
  732 resets sent
Udp:
  2829 packets received
  1 packets to unknown port received
  0 packet receive errors
  2841 packets sent

```

netstat -at



```

legion@Legion:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:42874           maa05s02-in-f18.1:https ESTABLISHED
tcp        0      0 0.0.0.0:55696           del03s17-in-f14.1:https ESTABLISHED
tcp        0      0 0.0.0.0:39060           104.19.155.83:https     ESTABLISHED
tcp        0      0 0.0.0.0:51390           maa05s09-in-f3.1e:https ESTABLISHED
tcp        0      0 0.0.0.0:33082           maa03s19-in-f98.1:https ESTABLISHED
tcp        0      0 0.0.0.0:36696           del11s04-in-f3.1e:https ESTABLISHED
tcp        0      0 0.0.0.0:49236           del03s16-in-f6.1e:https ESTABLISHED
tcp        0      0 0.0.0.0:47814           a23-207-131-234.d:https ESTABLISHED
tcp        0      0 0.0.0.0:33112           del03s17-in-f10.1:https ESTABLISHED
tcp        0      0 0.0.0.0:55170           maa03s29-in-f18.1:https ESTABLISHED
tcp        0      0 0.0.0.0:49446           sa-in-f189.1e100:https  ESTABLISHED
tcp        0      0 0.0.0.0:44498           maa03s31-in-f3.1e:https ESTABLISHED
tcp        0      0 0.0.0.0:42426           maa05s03-in-f4.1e:https ESTABLISHED
tcp        0      0 0.0.0.0:35590           del03s18-in-f2.1e:https ESTABLISHED
tcp        0      0 0.0.0.0:48898           a23-36-4-158.depl:https ESTABLISHED
tcp        0      0 0.0.0.0:37430           maa03s29-in-f2.1e:https ESTABLISHED
^C

```

netstat -au

```

legion@Legion:~$ netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 0.0.0.0:bootpc         0.0.0.0:*
udp        0      0 0.0.0.0:ipp             0.0.0.0:*
udp        0      0 0.0.0.0:49894          0.0.0.0:*
udp        0      0 224.0.0.251:mdns       0.0.0.0:*
udp        0      0 224.0.0.251:mdns       0.0.0.0:*
udp        0      0 0.0.0.0:mdns           0.0.0.0:*
udp6       0      0 [::]:56144             [::]:*
udp6       0      0 [::]:mdns              [::]:*
legion@Legion:~$

```

netstat -l

```

legion@Legion:~$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*              LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*              LISTEN
tcp6       0      0 ip6-localhost:ipp      [::]:*                 LISTEN
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 0.0.0.0:bootpc         0.0.0.0:*
udp        0      0 0.0.0.0:ipp            0.0.0.0:*
udp        0      0 0.0.0.0:49894          0.0.0.0:*
udp        0      0 224.0.0.251:mdns       0.0.0.0:*
udp        0      0 224.0.0.251:mdns       0.0.0.0:*
udp        0      0 0.0.0.0:mdns           0.0.0.0:*
udp6       0      0 [::]:56144             [::]:*
udp6       0      0 [::]:mdns              [::]:*
raw6       0      0 [::]:ipv6-icmp         [::]:*                  7

Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State       I-Node      Path
unix  2      [ ACC ]     STREAM    LISTENING   39945       /tmp/.ICE-unix/1215
unix  2      [ ACC ]     STREAM    LISTENING   34655       /tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM    LISTENING   39944       @/tmp/.ICE-unix/1215
unix  2      [ ACC ]     STREAM    LISTENING   40189       @/tmp/.ICE-unix/2277
unix  2      [ ACC ]     SEQPACKET LISTENING   16703       /run/udev/control
unix  2      [ ACC ]     STREAM    LISTENING   40122       /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM    LISTENING   32163       /run/user/121/systemd/private
unix  2      [ ACC ]     STREAM    LISTENING   40126       /run/user/1000/bus
unix  2      [ ACC ]     STREAM    LISTENING   26541       /run/user/121/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM    LISTENING   40127       /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM    LISTENING   26542       /run/user/121/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM    LISTENING   40128       /run/user/1000/gnupg/S.dirmgr
unix  2      [ ACC ]     STREAM    LISTENING   40129       /run/user/1000/snapd-session-agent.socket
unix  2      [ ACC ]     STREAM    LISTENING   26543       /run/user/121/pulse/native
unix  2      [ ACC ]     STREAM    LISTENING   40130       /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM    LISTENING   26544       /run/user/121/bus
unix  2      [ ACC ]     STREAM    LISTENING   40131       /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM    LISTENING   26545       /run/user/121/gnupg/S.dirmgr
unix  2      [ ACC ]     STREAM    LISTENING   40132       /run/user/1000/gnupg/S.gpg-agent.extra

```

netstat -lt

```

legion@Legion:~$ netstat -lt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*              LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*              LISTEN
tcp6       0      0 ip6-localhost:ipp      [::]:*                 LISTEN
legion@Legion:~$

```



netstat -lu

```

File Edit View Search Terminal Help
legion@Legion:~$ netstat -lu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp      0      0 localhost:domain        0.0.0.0:*
udp      0      0 0.0.0.0:bootpc         0.0.0.0:*
udp      0      0 0.0.0.0:ipp            0.0.0.0:*
udp      0      0 0.0.0.0:49894          0.0.0.0:*
udp      0      0 224.0.0.251:mdns       0.0.0.0:*
udp      0      0 224.0.0.251:mdns       0.0.0.0:*
udp      0      0 0.0.0.0:mdns           0.0.0.0:*
udp6     0      0 [::]:56144             [::]:*
udp6     0      0 [::]:mdns              [::]:*
legion@Legion:~$

```

### 3) ifconfig

**Syntax :** ifconfi [...OPTIONS][INTERFACE]

**Description:** ifconfig stand for “interface configuration”. It is used to view and change the configurations of the network interfaces on your system.

**Output:**

ifconfig

```

legion@Legion:~$ ifconfig
eno1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether e4:e7:49:52:11:ca txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    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 2173 bytes 228987 (228.9 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2173 bytes 228987 (228.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.4 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::9aea:997b:d5fe:7db prefixlen 64 scopeid 0x20<link>
    ether fc:77:74:b8:49:e9 txqueuelen 1000 (Ethernet)
    RX packets 205487 bytes 222946937 (222.9 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 77522 bytes 31472869 (31.4 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

legion@Legion:~$

```

## ifconfig -a

```

legion@Legion:~$ ifconfig -a
eno1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether e4:e7:49:52:11:ca txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    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 2199 bytes 231986 (231.9 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2199 bytes 231986 (231.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.4 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::9aea:997b:d5fe:7db prefixlen 64 scopeid 0x20<link>
    ether fc:77:74:b8:49:e9 txqueuelen 1000 (Ethernet)
    RX packets 206718 bytes 223444151 (223.4 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 78416 bytes 32194934 (32.1 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

legion@Legion:~$

```

## ifconfig -s

```

legion@Legion:~$ ifconfig -s

```

Iface	MTU	RX-OK	RX-ERR	RX-DRP	RX-OVR	TX-OK	TX-ERR	TX-DRP	TX-OVR	Flg
eno1	1500	0	0	0	0	0	0	0	0	BMU
lo	65536	2227	0	0	0	2227	0	0	0	LRU
wlo1	1500	208349	0	0	0	79572	0	0	0	BMRU

```

legion@Legion:~$

```

## 4) nslookup

**Syntax:** nslookup (Name server Lookup) is a useful command for getting information from DNS server. It is a network administration tool for querying the DOmain Name Sysyem (DNS) to obtain domain name or IP address mapping or any other specific DNS record.

### Output:

nslookup[domain\_name]

```

legion@Legion:~$ nslookup www.google.com
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 172.217.31.4
Name:   www.google.com
Address: 2404:6800:4002:802::2004

```

## 5) traceroute

**Syntax:** traceroute [options] host\_Address [pathlength]

**Description :** traceroute command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all the hops that a packet takes.

**Output:**

traceroute [domain\_name\_or\_ip\_addr]

```
File Edit View Search Terminal Help
legion@Legion:~$ nslookup www.google.com
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 172.217.31.4
Name:   www.google.com
Address: 2404:6800:4002:802::2004
```

## 6) ping

**Syntax:** ping [options] [ domain\_name or ip\_addr]

**Description:** PING (Packet Internet Groper) command is used to check the network connectivity between host and server/host. This command takes as input the IP address or the URL and send a data packet to the specified address with the message "PING" and get a response form the server/host.

**Output:**

ping [ip\_addr]

```
File Edit View Search Terminal Help
legion@Legion:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=3.37 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=3.02 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=2.89 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=2.85 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=2.98 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 2.851/3.024/3.373/0.187 ms
legion@Legion:~$
```

ping [domain\_name]

```

legion@legion:~$ ping www.youtube.com
PING youtube-ui.l.google.com (216.58.196.174) 56(84) bytes of data.
64 bytes from maa03s31-in-f14.1e100.net (216.58.196.174): icmp_seq=1 ttl=117 time=5.02 ms
64 bytes from maa03s31-in-f14.1e100.net (216.58.196.174): icmp_seq=2 ttl=117 time=5.37 ms
64 bytes from maa03s31-in-f14.1e100.net (216.58.196.174): icmp_seq=3 ttl=117 time=5.14 ms
64 bytes from maa03s31-in-f14.1e100.net (216.58.196.174): icmp_seq=4 ttl=117 time=5.14 ms
64 bytes from maa03s31-in-f14.1e100.net (216.58.196.174): icmp_seq=5 ttl=117 time=5.20 ms
64 bytes from maa03s31-in-f14.1e100.net (216.58.196.174): icmp_seq=6 ttl=117 time=6.53 ms
64 bytes from maa03s31-in-f14.1e100.net (216.58.196.174): icmp_seq=7 ttl=117 time=5.44 ms
64 bytes from maa03s31-in-f14.1e100.net (216.58.196.174): icmp_seq=8 ttl=117 time=5.03 ms
^C
--- youtube-ui.l.google.com ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7012ms
rtt min/avg/max/mdev = 5.021/5.362/6.534/0.471 ms
legion@legion:~$

```

## 7) iwconfig

**Syntax:** iwconfig [INTERFACE] [OPTIONS]

**Description:** iwconfig command in Linux is like ifconfig command, in the sense it works with kernel- resident network interface but it is dedicated to wireless networking interfaces only. It is used to set the parameters of the network interface that are particular to the wireless operation like SSID, frequency etc.

**Output:**

iwconfig

```

legion@legion:~$ iwconfig
wlo1 IEEE 802.11 ESSID:"Airtel_9884641153"
Mode:Managed Frequency:5.745 GHz Access Point: A8:49:4D:56:4B:0C
Bit Rate=650 Mb/s Tx-Power=19 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Power Management:on
Link Quality=70/70 Signal level=-39 dBm
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:30 Missed beacon:0

eno1 no wireless extensions.

lo no wireless extensions.

```