Computer Networks Lab 1

CS F303

Susmit Wani 2018A7PS0116G

Lab 1 Network Commands

Vinayak Naik • Jan 23

Labs • 24 points **Due 7:00 PM**

Following is a list of commands, which you will execute. For each command, have screenshot and write an explanation about the output seen. For help, you can refer Linux manual.

1. tcpdump
2. ifconfig
3. dig
4. arp
5. netstat
6. telnet
7. traceroute
8. ping
9. top
10. wall
11. uptime
12. nslookup

Put all the screenshots and the explanations in a PDF and submit it.

1. tcpdump

```
lenovo@susmits-lenovo:~$ sudo tcpdump -c 10
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:50:20.622405 IP sb-in-f188.1e100.net.5228 > susmits-lenovo.33166: Flags [P.], seq 1822351911:1822351937, ack 3626456906, win 284, options [nop,nop,TS
val 3224077131 ecr 977948564], length 26
13:50:20.622474 IP susmits-lenovo.33166 > sb-in-f188.1e100.net.5228: Flags [.], ack 26, win 501, options [nop,nop,TS val 977948643 ecr 3224077131], lengt
h 0
13:50:20.624178 IP susmits-lenovo.37705 > 125.99.61.254.domain: 35401+ [1au] PTR? 6.0.168.192.in-addr.arpa. (53)
13:50:20.639361 IP 125.99.61.254.domain > susmits-lenovo.37705: 35401 NXDomain* 0/1/1 (108)
13:50:20.639660 IP susmits-lenovo.37705 > 125.99.61.254.domain: 35401+ PTR? 6.0.168.192.in-addr.arpa. (42)
13:50:20.653596 IP 125.99.61.254.domain > susmits-lenovo.37705: 35401 NXDomain* 0/1/0 (97)
13:50:20.655304 IP susmits-lenovo.59312 > 125.99.61.254.domain: 6510+ [1au] PTR? 188.130.125.74.in-addr.arpa. (56)
13:50:20.668581 IP susmits-lenovo.58428 > 125.99.61.254.domain: 51792+ [1au] PTR? 254.61.99.125.in-addr.arpa. (55)
13:50:20.680757 IP 125.99.61.254.domain > susmits-lenovo.58428: 51792 NXDomain 0/1/1 (129)
13:50:21.814402 IP susmits-lenovo.48756 > ec2-3-91-65-45.compute-1.amazonaws.com.https: Flags [.], ack 4058305825, win 501, options [nop,nop,TS val 41959
8226 ecr 304559200], length 0
10 packets captured
16 packets received by filter
3 packets dropped by kernel
lenovo@susmits-lenovo:~$
```

- The tcpdump command is used to check the packets being sent over a network. Command needs to be used with the keyword sudo.
- Keeps checking for packets until interrupt is given.
- Records the time at which packet was sent/received
- Also keeps track of IPs from which the request was sent and the IP to which it was sent.

2. ifconfig

- The ifconfig allows us to configure the network interfaces.
- It gives you the IPv4, IPv6 and mac addresses and also the amount of data shared over the network(packets/size).
- It also tells you the amount of networks you are on.

```
lenovo@susmits-lenovo:~$ ifconfig
enp2s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 8c:16:45:32:5b:bc  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 3449  bytes 356723 (356.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3449  bytes 356723 (356.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.6  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::d911:c386:bbac:a085  prefixlen 64  scopeid 0x20<link>
        ether 70:c9:4e:d2:91:d7  txqueuelen 1000  (Ethernet)
        RX packets 411205  bytes 370467526 (370.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 154314  bytes 36232096 (36.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lenovo@susmits-lenovo:~$
```

3. dig

- DIG stands for Domain Information Groper
- It shows DNS data in the terminal.
- It collects data about DNS and is useful in tackling DNS problems.

```
lenovo@susmits-lenovo:~$ dig

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22247
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       263105  IN      NS      g.root-servers.net.
.                       263105  IN      NS      f.root-servers.net.
.                       263105  IN      NS      m.root-servers.net.
.                       263105  IN      NS      b.root-servers.net.
.                       263105  IN      NS      c.root-servers.net.
.                       263105  IN      NS      j.root-servers.net.
.                       263105  IN      NS      h.root-servers.net.
.                       263105  IN      NS      e.root-servers.net.
.                       263105  IN      NS      k.root-servers.net.
.                       263105  IN      NS      l.root-servers.net.
.                       263105  IN      NS      d.root-servers.net.
.                       263105  IN      NS      i.root-servers.net.
.                       263105  IN      NS      a.root-servers.net.

;; Query time: 37 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Jan 25 14:41:59 IST 2021
;; MSG SIZE  rcvd: 239
```

4. arp

```
lenovo@susmits-lenovo:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   e4:6f:13:b6:ed:d9   C                     wlp3s0
192.168.0.5              ether   f6:0f:cc:7f:20:bd   C                     wlp3s0
```

- ARP stands for Address Resolution Protocol
- The arp command manipulates or displays the kernel's IPv4 network neighbour cache.
- Can use this to add/remove/view entries in the network neighbor table.

5. netstat

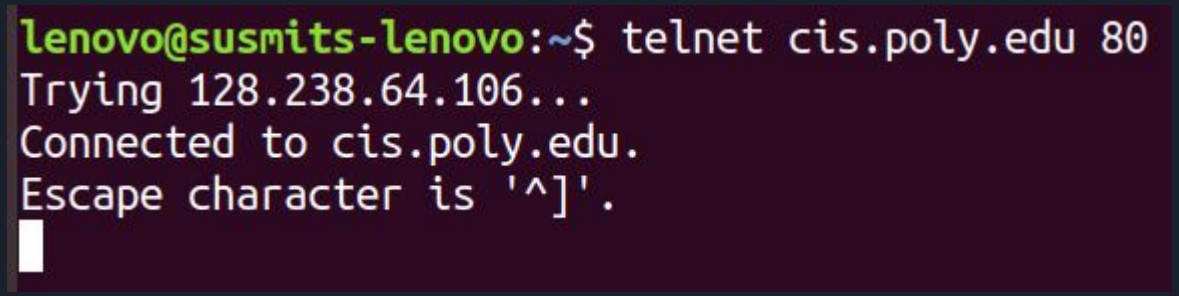
- The command shows all the network related info like the connections, protocols, local and foreign addresses and the state of the connection.
- It shows Internet connections as well as UNIX sockets.
- The use of this command is mostly to check the status of network and protocols.

```
lenovo@susmits-lenovo:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 susmits-lenovo:32988    a104-71-100-96.de:https ESTABLISHED
tcp        0      0 susmits-lenovo:44796    159.127.41.114:https    TIME_WAIT
tcp        0      0 susmits-lenovo:47550    202.88.134.167:https    ESTABLISHED
tcp        0      0 susmits-lenovo:42290    ads.us.e-planning:https ESTABLISHED
tcp        0      0 susmits-lenovo:40416    whatsapp-cdn-shv-:https ESTABLISHED
tcp        0      0 susmits-lenovo:53406    202.88.132.10:https     TIME_WAIT
tcp        0      0 susmits-lenovo:50406    103.231.98.193:https    ESTABLISHED
tcp        0      0 susmits-lenovo:41584    74.118.186.210:https    ESTABLISHED
tcp        0      0 susmits-lenovo:40006    49.44.205.56:https      ESTABLISHED
tcp        0      0 susmits-lenovo:55932    server-13-35-217-:https ESTABLISHED
tcp        0      0 susmits-lenovo:59100    aeab55d76dd13c9bb:https ESTABLISHED
tcp        0      0 susmits-lenovo:40004    49.44.205.56:https      ESTABLISHED
tcp        0      0 susmits-lenovo:39234    202.88.132.39:https     ESTABLISHED
tcp        0      0 susmits-lenovo:40812    8.159.244.35.bc.g:https ESTABLISHED
tcp        0      0 susmits-lenovo:33166    sb-in-f188.1e100.n:5228 ESTABLISHED
tcp        0      0 susmits-lenovo:48300    104.26.1.240:https      ESTABLISHED
tcp        0      0 susmits-lenovo:46904    server-13-35-221-:https ESTABLISHED
tcp        0      0 susmits-lenovo:44788    159.127.41.114:https    ESTABLISHED
tcp        0      0 susmits-lenovo:42618    69.173.159.50:https     TIME_WAIT
udp        0      0 susmits-lenovo:53402    del03s18-in-f2.1e10:443 ESTABLISHED
udp        0      0 susmits-lenovo:41200    del11s04-in-f14.1e1:443 ESTABLISHED
udp        0      0 susmits-lenovo:37143    del03s18-in-f2.1e10:443 ESTABLISHED
udp        0      0 susmits-lenovo:49562    bom07s31-in-f14.1e1:443 ESTABLISHED
udp        0      0 susmits-lenovo:41599    del03s06-in-f10.1e1:443 ESTABLISHED
```

```
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    33391    /run/user/1000/systemd/notify
unix  2      [ ]         DGRAM                    28071    /run/user/120/systemd/notify
unix  3      [ ]         DGRAM                    13807    /run/systemd/notify
unix  26     [ ]         DGRAM                    13822    /run/systemd/journal/dev-log
unix  2      [ ]         DGRAM                    13832    /run/systemd/journal/syslog
unix  9      [ ]         DGRAM                    13836    /run/systemd/journal/socket
unix  2      [ ]         DGRAM                    28036    /run/wpa_supplicant/wlp3s0
unix  2      [ ]         DGRAM                    25396    /run/wpa_supplicant/p2p-dev-wlp3
unix  3      [ ]         SEQPACKET  CONNECTED     45107    @00000f
unix  3      [ ]         SEQPACKET  CONNECTED     45124    @00010
unix  3      [ ]         STREAM     CONNECTED     125317
unix  3      [ ]         STREAM     CONNECTED     37764    /run/systemd/journal/stdout
unix  2      [ ]         DGRAM                    33384
```

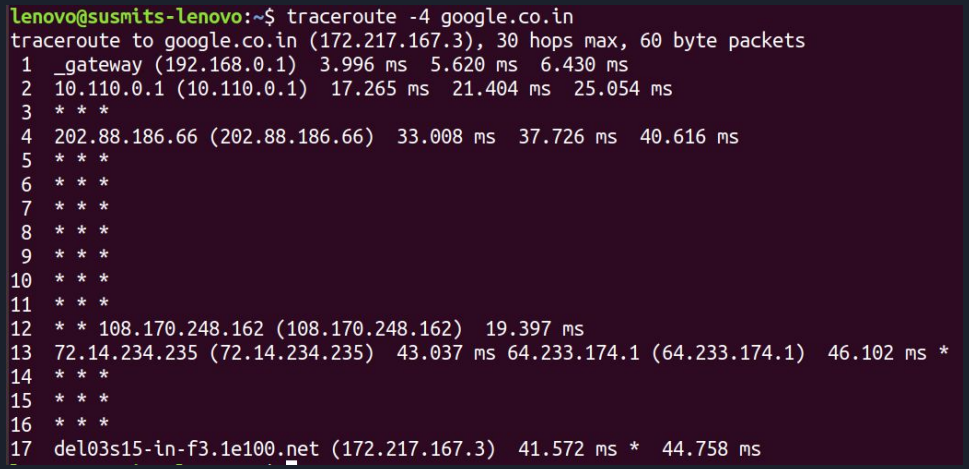
6. telnet

- The telnet command makes a connection with a system over a TCP/IP network.
- It can be used to create remote sessions and type commands in the terminal of the other user.



7. traceroute

- Traceroute is used to trace the path a packet takes to reach the destination.
- It also shows the details of time taken to reach the IPs
- It sends three packets to the Ip typed and we get the result back.



8. ping

- The ping command returns the time delay in sending and receiving the packet to the specified IP.
- We can specify the packet size in the command. The command also tells us the cumulative time, packet loss and other details used to transmit data.

```
lenovo@susmits-lenovo:~$ ping -c 10 google.co.in
PING google.co.in (172.217.167.3) 56(84) bytes of data.
64 bytes from del03s15-in-f3.1e100.net (172.217.167.3): icmp_seq=1 ttl=114 time=68.1 ms
64 bytes from del03s15-in-f3.1e100.net (172.217.167.3): icmp_seq=2 ttl=114 time=39.6 ms
64 bytes from del03s15-in-f3.1e100.net (172.217.167.3): icmp_seq=3 ttl=114 time=43.8 ms
64 bytes from del03s15-in-f3.1e100.net (172.217.167.3): icmp_seq=4 ttl=114 time=40.1 ms
64 bytes from del03s15-in-f3.1e100.net (172.217.167.3): icmp_seq=5 ttl=114 time=40.7 ms
64 bytes from del03s15-in-f3.1e100.net (172.217.167.3): icmp_seq=6 ttl=114 time=39.0 ms
64 bytes from del03s15-in-f3.1e100.net (172.217.167.3): icmp_seq=7 ttl=114 time=71.8 ms
64 bytes from del03s15-in-f3.1e100.net (172.217.167.3): icmp_seq=8 ttl=114 time=37.8 ms
64 bytes from del03s15-in-f3.1e100.net (172.217.167.3): icmp_seq=9 ttl=114 time=48.1 ms
64 bytes from del03s15-in-f3.1e100.net (172.217.167.3): icmp_seq=10 ttl=114 time=39.5 ms

--- google.co.in ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9012ms
rtt min/avg/max/mdev = 37.810/46.898/71.850/11.906 ms
```

9. top

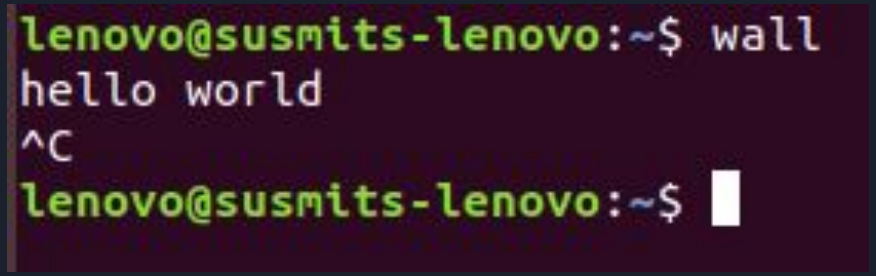
```
top - 17:14:50 up  3:58,  1 user,  load average: 4.36, 3.50, 2.78
Tasks: 373 total,   1 running, 293 sleeping,   5 stopped,   0 zombie
%Cpu(s): 15.9 us,  5.0 sy,  0.0 ni, 78.3 id,  0.0 wa,  0.0 hi,  0.8 si,  0.0 st
KiB Mem :  7945904 total,   241868 free,  4178032 used,  3526004 buff/cache
KiB Swap:  2097148 total,  2096368 free,      780 used.  2328364 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
 3914 lenovo    20   0 22.944g 355468 117144 S  63.7  4.5  12:20.60 chrome
 2827 lenovo    20   0  766932 168936  77432 S  22.1  2.1  34:37.35 chrome
 2105 lenovo    20   0 4532676 279388 134432 S  21.5  3.5  15:19.22 gnome-shell
 2625 lenovo    20   0 1775448 483068 150316 S  17.8  6.1  26:31.30 chrome
 2131 lenovo     9 -11 2645740  18156  13632 S  14.5  0.2  23:56.63 pulseaudio
 1918 lenovo    20   0 2259388  83372  48812 S  11.2  1.0  12:19.65 Xorg
 3592 lenovo    20   0 1315380  62364  49064 S   7.3  0.8  11:25.30 chrome
```

- It gave the processes and threads running in the background.
- It also shows memory utilisation, CPu utilisation and which appliction is using it.
- It shows real time processes.

10. wall

- Wall stands for write all
- Wall displays a message on terminals of all logged in users
- Not connected to a network so can’t show the output of the line.



11. uptime

```
lenovo@susmits-lenovo:~$ uptime
 17:24:15 up  4:07,  1 user,  load average: 1.81, 2.54, 2.64
```

- The command simple tells us the time, the uptime of the PC, the number of users using the system and the load for past 1, 5, 15 minutes.

12. nslookup

- Stands for Name Server Lookup
- It is used to get the domain name, the server IP and the address.