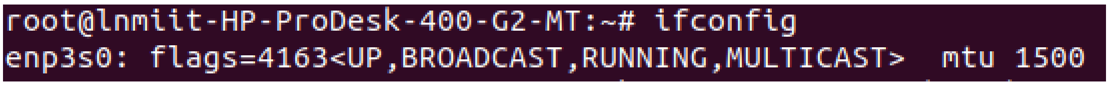
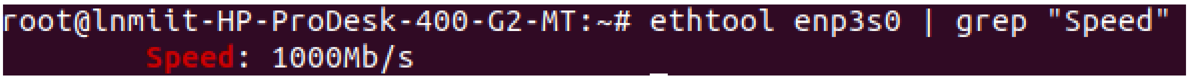
Name - Kartikeya Acharya
Roll no. - 21UEC072
Lab - 2

Task 1: Physical and Data Link Layer

1. Find out the network cards in your machine. What is the speed?

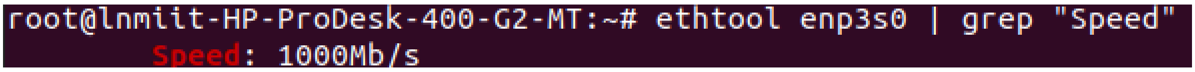


```
root@lnmiit-HP-ProDesk-400-G2-MT:~# ifconfig
enp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
```

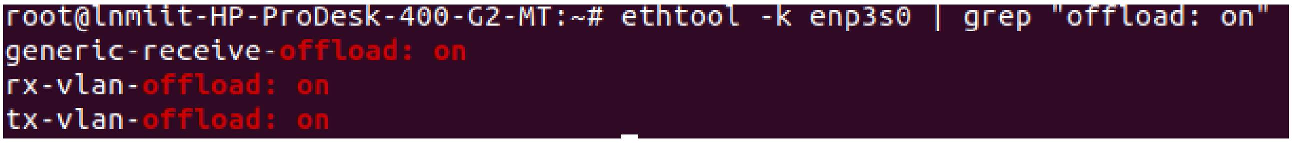


```
root@lnmiit-HP-ProDesk-400-G2-MT:~# ethtool enp3s0 | grep "Speed"
        Speed: 1000Mb/s
```

2. What is the current speed of the network interface? What offload features are enabled?

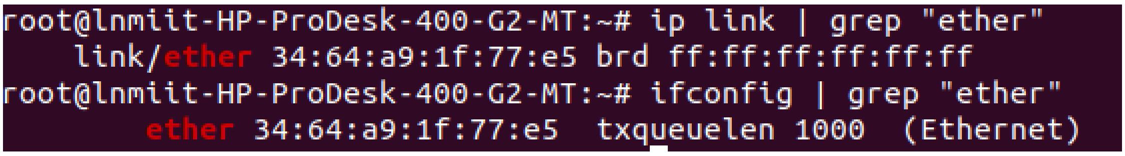


```
root@lnmiit-HP-ProDesk-400-G2-MT:~# ethtool enp3s0 | grep "Speed"
        Speed: 1000Mb/s
```



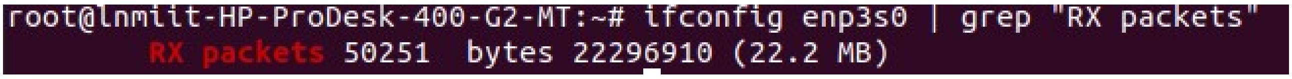
```
root@lnmiit-HP-ProDesk-400-G2-MT:~# ethtool -k enp3s0 | grep "offload: on"
generic-receive-offload: on
rx-vlan-offload: on
tx-vlan-offload: on
```

3. What is the MAC address of your machine?



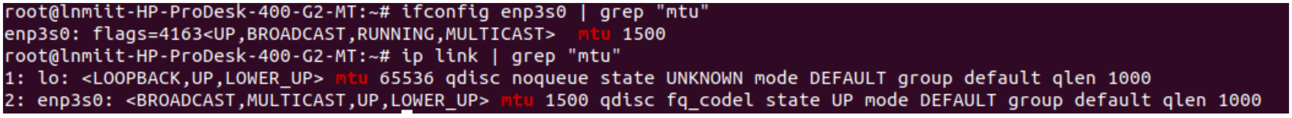
```
root@lnmiit-HP-ProDesk-400-G2-MT:~# ip link | grep "ether"
    link/ether 34:64:a9:1f:77:e5 brd ff:ff:ff:ff:ff:ff
root@lnmiit-HP-ProDesk-400-G2-MT:~# ifconfig | grep "ether"
        ether 34:64:a9:1f:77:e5  txqueuelen 1000  (Ethernet)
```

4. How many bytes did your eth0/eth1 interface receive since booted?



```
root@lnmiit-HP-ProDesk-400-G2-MT:~# ifconfig enp3s0 | grep "RX packets"
        RX packets 50251  bytes 22296910 (22.2 MB)
```

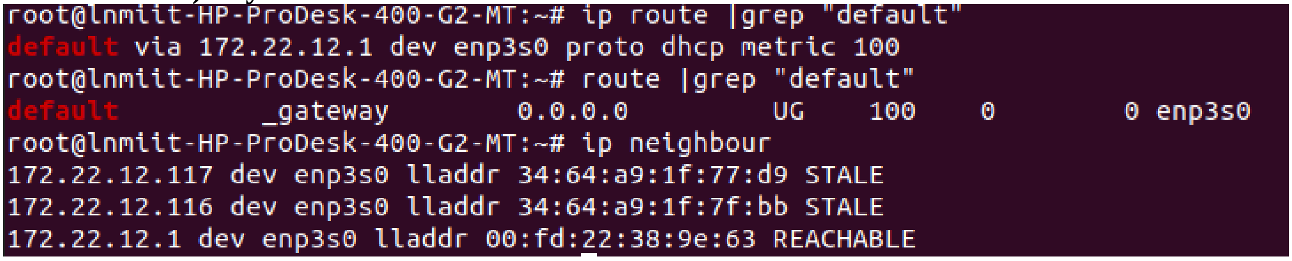
5. What is the MTU setting for eth0/eth1?



```
root@lnmiit-HP-ProDesk-400-G2-MT:~# ifconfig enp3s0 | grep "mtu"
enp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
root@lnmiit-HP-ProDesk-400-G2-MT:~# ip link | grep "mtu"
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
2: enp3s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
```

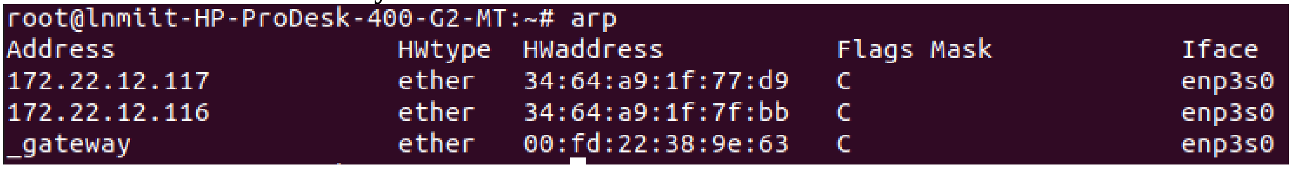
Task 2: Network Layer

1. What is the network address of your machine? What is the default gateway (IP address and MAC address) of your network?



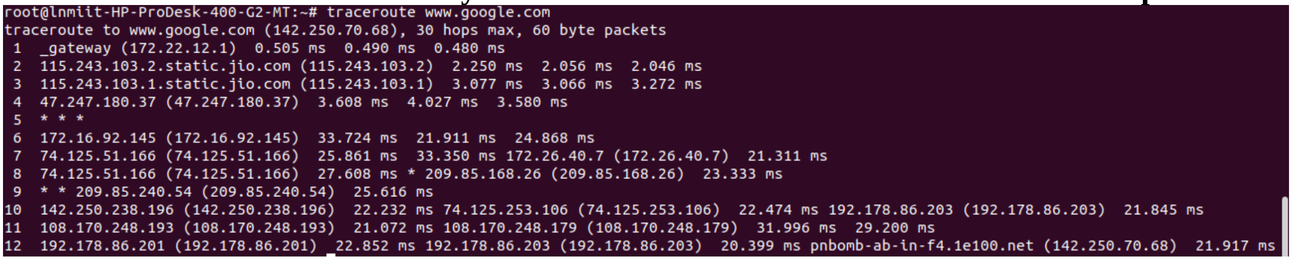
```
root@lnmiit-HP-ProDesk-400-G2-MT:~# ip route |grep "default"
default via 172.22.12.1 dev enp3s0 proto dhcp metric 100
root@lnmiit-HP-ProDesk-400-G2-MT:~# route |grep "default"
default         _gateway        0.0.0.0         UG    100    0        0 enp3s0
root@lnmiit-HP-ProDesk-400-G2-MT:~# ip neighbour
172.22.12.117 dev enp3s0 lladdr 34:64:a9:1f:77:d9 STALE
172.22.12.116 dev enp3s0 lladdr 34:64:a9:1f:7f:bb STALE
172.22.12.1 dev enp3s0 lladdr 00:fd:22:38:9e:63 REACHABLE
```

2. Show the ARP entries in your machine.



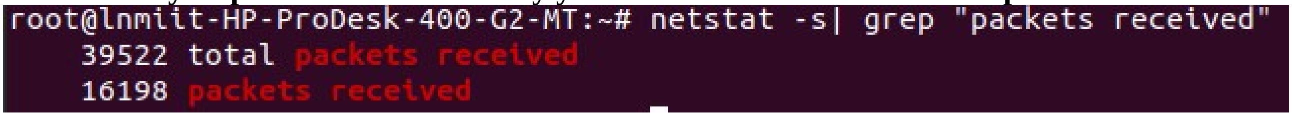
```
root@lnmiit-HP-ProDesk-400-G2-MT:~# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.22.12.117            ether   34:64:a9:1f:77:d9   C                     enp3s0
172.22.12.116            ether   34:64:a9:1f:7f:bb   C                     enp3s0
_gateway                 ether   00:fd:22:38:9e:63   C                     enp3s0
```

3. Perform a traceroute/mtr to any web address. Provide the full traceroute/mtr output.



```
root@lnmiit-HP-ProDesk-400-G2-MT:~# traceroute www.google.com
traceroute to www.google.com (142.250.70.68), 30 hops max, 60 byte packets
 1  _gateway (172.22.12.1)  0.505 ms  0.490 ms  0.480 ms
 2  115.243.103.2.static.jio.com (115.243.103.2)  2.250 ms  2.056 ms  2.046 ms
 3  115.243.103.1.static.jio.com (115.243.103.1)  3.077 ms  3.066 ms  3.272 ms
 4  47.247.180.37 (47.247.180.37)  3.608 ms  4.027 ms  3.580 ms
 5  * * *
 6  172.16.92.145 (172.16.92.145)  33.724 ms  21.911 ms  24.868 ms
 7  74.125.51.166 (74.125.51.166)  25.861 ms  33.350 ms 172.26.40.7 (172.26.40.7)  21.311 ms
 8  74.125.51.166 (74.125.51.166)  27.608 ms * 209.85.168.26 (209.85.168.26)  23.333 ms
 9  * * 209.85.240.54 (209.85.240.54)  25.616 ms
10  142.250.238.196 (142.250.238.196)  22.232 ms 74.125.253.106 (74.125.253.106)  22.474 ms 192.178.86.203 (192.178.86.203)  21.845 ms
11  108.170.248.193 (108.170.248.193)  21.072 ms 108.170.248.179 (108.170.248.179)  31.996 ms  29.200 ms
12  192.178.86.201 (192.178.86.201)  22.852 ms 192.178.86.203 (192.178.86.203)  20.399 ms pnbomb-ab-in-f4.1e100.net (142.250.70.68)  21.917 ms
```

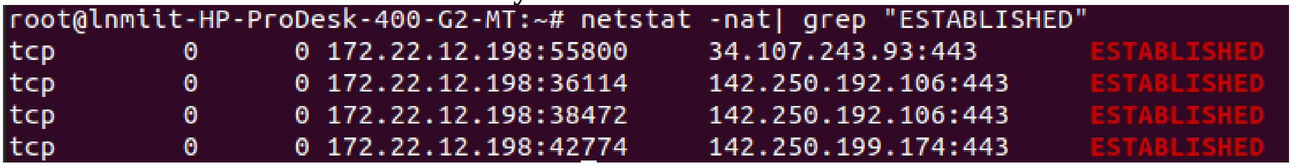
4. How many IP packets are received by your machine after current boot process?



```
root@lnmiit-HP-ProDesk-400-G2-MT:~# netstat -s| grep "packets received"
    39522 total packets received
    16198 packets received
```

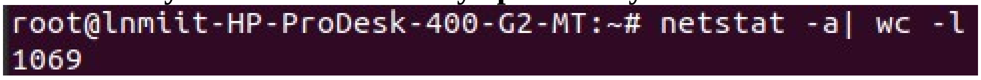
Task 3: Transport Layer

1. Find the active TCP connection on your machine?



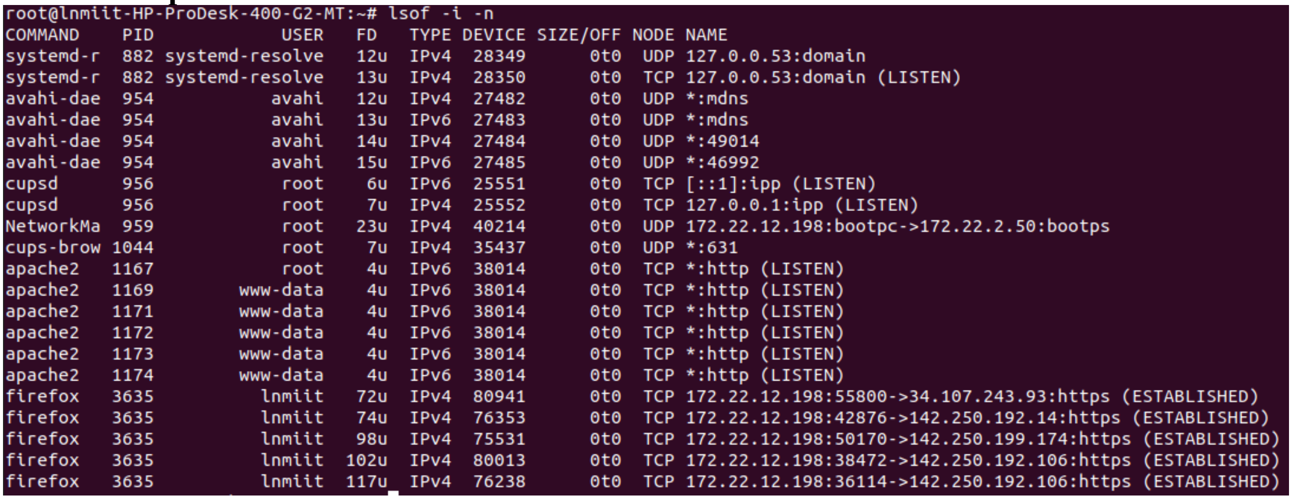
```
root@lnmiit-HP-ProDesk-400-G2-MT:~# netstat -nat| grep "ESTABLISHED"
tcp        0      0 172.22.12.198:55800      34.107.243.93:443       ESTABLISHED
tcp        0      0 172.22.12.198:36114      142.250.192.106:443     ESTABLISHED
tcp        0      0 172.22.12.198:38472      142.250.192.106:443     ESTABLISHED
tcp        0      0 172.22.12.198:42774      142.250.199.174:443     ESTABLISHED
```

2. How many sockets are currently opened on your machine?



```
root@lnmiit-HP-ProDesk-400-G2-MT:~# netstat -a| wc -l
1069
```

3. How many applications are accessing network services on your machine? Also, identify their access protocol.



```
root@lnmiit-HP-ProDesk-400-G2-MT:~# lsof -i -n
COMMAND    PID            USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd-r  882 systemd-resolve   12u  IPv4  28349      0t0  UDP 127.0.0.53:domain
systemd-r  882 systemd-resolve   13u  IPv4  28350      0t0  TCP 127.0.0.53:domain (LISTEN)
avahi-dae  954           avahi   12u  IPv4  27482      0t0  UDP *:mdns
avahi-dae  954           avahi   13u  IPv6  27483      0t0  UDP *:mdns
avahi-dae  954           avahi   14u  IPv4  27484      0t0  UDP *:49014
avahi-dae  954           avahi   15u  IPv6  27485      0t0  UDP *:46992
cupsd      956            root    6u  IPv6  25551      0t0  TCP [::1]:ipp (LISTEN)
cupsd      956            root    7u  IPv4  25552      0t0  TCP 127.0.0.1:ipp (LISTEN)
NetworkMa  959            root   23u  IPv4  40214      0t0  UDP 172.22.12.198:bootpc->172.22.2.50:bootps
cups-brow 1044            root    7u  IPv4  35437      0t0  UDP *:631
apache2   1167            root    4u  IPv6  38014      0t0  TCP *:http (LISTEN)
apache2   1169        www-data    4u  IPv6  38014      0t0  TCP *:http (LISTEN)
apache2   1171        www-data    4u  IPv6  38014      0t0  TCP *:http (LISTEN)
apache2   1172        www-data    4u  IPv6  38014      0t0  TCP *:http (LISTEN)
apache2   1173        www-data    4u  IPv6  38014      0t0  TCP *:http (LISTEN)
apache2   1174        www-data    4u  IPv6  38014      0t0  TCP *:http (LISTEN)
firefox   3635          lnmiit   72u  IPv4  80941      0t0  TCP 172.22.12.198:55800->34.107.243.93:https (ESTABLISHED)
firefox   3635          lnmiit   74u  IPv4  76353      0t0  TCP 172.22.12.198:42876->142.250.192.14:https (ESTABLISHED)
firefox   3635          lnmiit   98u  IPv4  75531      0t0  TCP 172.22.12.198:50170->142.250.199.174:https (ESTABLISHED)
firefox   3635          lnmiit  102u  IPv4  80013      0t0  TCP 172.22.12.198:38472->142.250.192.106:https (ESTABLISHED)
firefox   3635          lnmiit  117u  IPv4  76238      0t0  TCP 172.22.12.198:36114->142.250.192.106:https (ESTABLISHED)
```