Lab-1

111801015 - Harsh Parihar

Q1.

1. Arp: It is used to find MAC address from IP address. MAC address is physical address on the board.
   OPTIONS:
   a. Arp -a [hostname] : Used to show the entries of the specified host. If nothing is passed, all entries will be displayed.
   b. Arp -v: To show the verbose information. Verbose mode provides additional information.
   c. -d [hostname]: Removes any entry for the specified host.

2. Ifconfig: It stands for “Interface Configuration”. It displays all the information about the interfaces.
   a. Ifconfig -a : Displays all the available interfaces.
   b. Ifconfig -s : Displays the short list.

3. Route: This command displays the routing table. Routing table contains the path information of each interface, like destination, gateway, genmask etc.
   a. Route -n : To display routing table in full numeric form.
   b. `sudo route add default gw ……` : This assigns a gateway address on which all the packets that do not belong to the network are forwarded.

4. Host: It is used to find IP address of specified hostname and also hostname can be found by specifying the IP address.
   a. Host [hostname]: gives IP address of the hostname.
   b. Host [IP_address]: gives hostname of the specified IP_address.

5. Ping: It is used to add an IP address to the network. This command takes as input the IP address or the URL and sends data packet to the specified address with the message “PING” and get a response from the server. This way the connection is established.
   a. Ping -c [int] [hostname] : sends [int] packets across the connection.

b. Ping -c [int] -q [hostname] : shows only the summary about network use.

6. Tcpdump: It is used to capture, filter, and analyze network traffic such as TCP/IP packets going through your system. It saves the captured information in a pcap file.

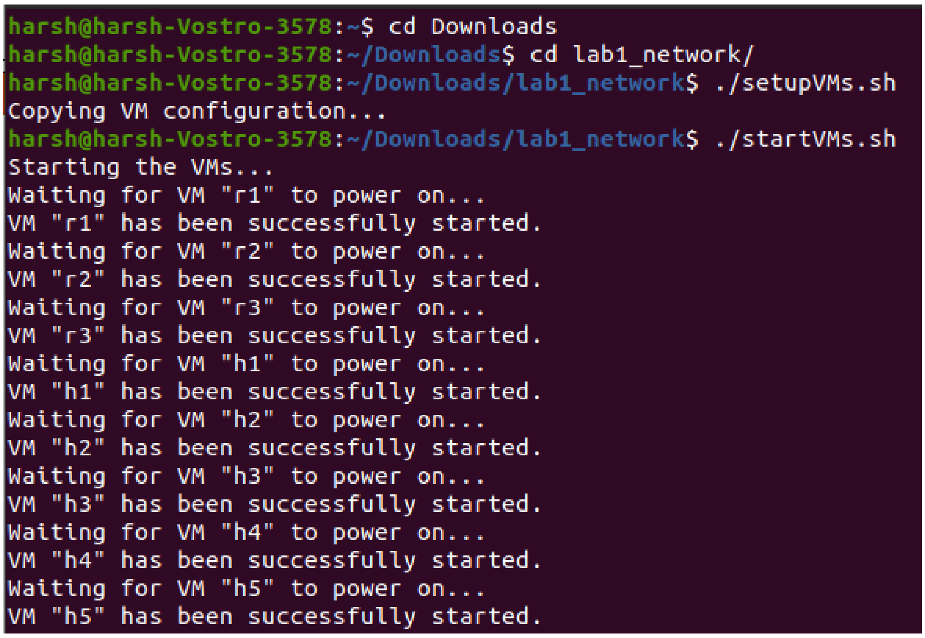
a. Sudo tcpdump: This will capture the packets from the current interface of the network through which the system is connected to the internet.
b. sudo tcpdump -i wlo1: To capture packets from a specific network interface.
c. sudo tcpdump -w file_name.pcap -i wlo1: To store captured packets into a file.

7. Netstat: Netstat command displays various network related information such as network connections, routing tables, interface statistics etc.

a. Netstat -a: To show both listening and non-listening sockets.
b. Netstat -at: to list all tcp ports.
c. Netstat -au: to list all udp ports.

Q2.

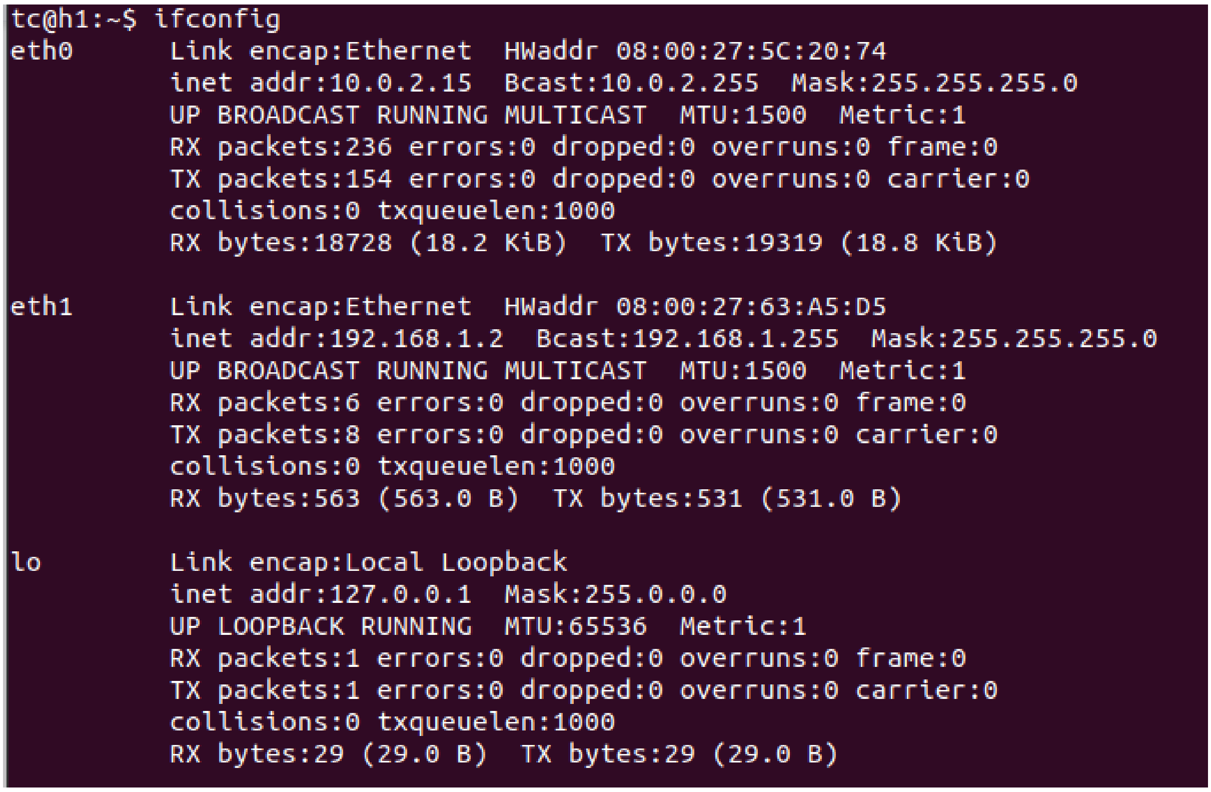
1. Setup and start the VM.



```
harsh@harsh-Vostro-3578:~$ cd Downloads
harsh@harsh-Vostro-3578:~/Downloads$ cd lab1_network/
harsh@harsh-Vostro-3578:~/Downloads/lab1_network$ ./setupVMs.sh
Copying VM configuration...
harsh@harsh-Vostro-3578:~/Downloads/lab1_network$ ./startVMs.sh
Starting the VMs...
Waiting for VM "r1" to power on...
VM "r1" has been successfully started.
Waiting for VM "r2" to power on...
VM "r2" has been successfully started.
Waiting for VM "r3" to power on...
VM "r3" has been successfully started.
Waiting for VM "h1" to power on...
VM "h1" has been successfully started.
Waiting for VM "h2" to power on...
VM "h2" has been successfully started.
Waiting for VM "h3" to power on...
VM "h3" has been successfully started.
Waiting for VM "h4" to power on...
VM "h4" has been successfully started.
Waiting for VM "h5" to power on...
VM "h5" has been successfully started.
```

2. For h1:

Interface	IP address
eth0	10.0.2.15
eth1	192.168.1.2
lo	127.0.0.1



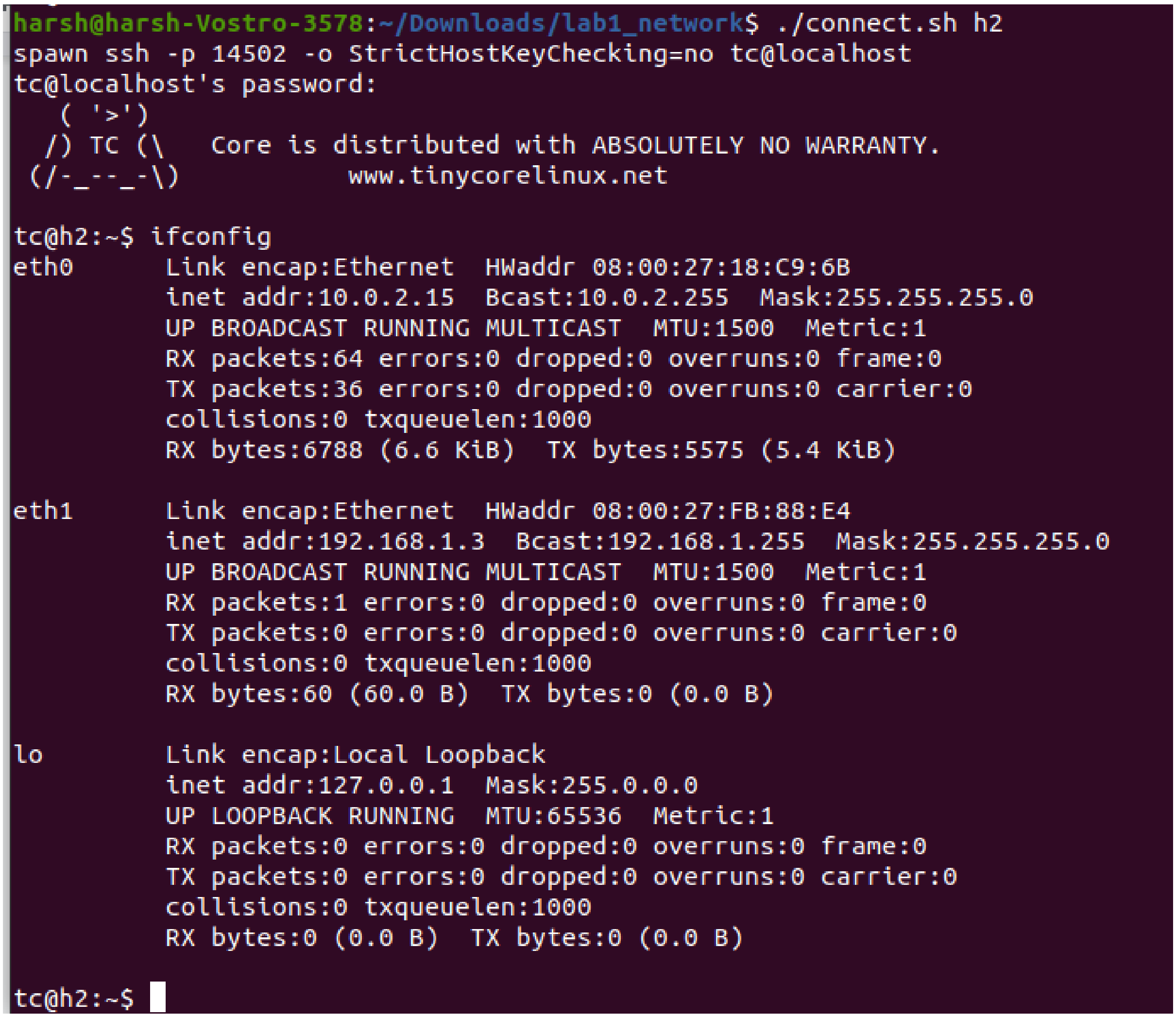
```
tc@h1:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:5C:20:74
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:236 errors:0 dropped:0 overruns:0 frame:0
          TX packets:154 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:18728 (18.2 KiB)  TX bytes:19319 (18.8 KiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:63:A5:D5
          inet addr:192.168.1.2  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:563 (563.0 B)  TX bytes:531 (531.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:29 (29.0 B)  TX bytes:29 (29.0 B)
```

For h2:

Interface	IP address
eth0	10.0.2.15
eth1	192.168.1.3
lo	127.0.0.1



```
harsh@harsh-Vostro-3578:~/Downloads/lab1_network$ ./connect.sh h2
spawn ssh -p 14502 -o StrictHostKeyChecking=no tc@localhost
tc@localhost's password:
   ( '>')
  /) TC (\   Core is distributed with ABSOLUTELY NO WARRANTY.
 (/-_--_-\)           www.tinycorelinux.net

tc@h2:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:18:C9:6B
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:64 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6788 (6.6 KiB)  TX bytes:5575 (5.4 KiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:FB:88:E4
          inet addr:192.168.1.3  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:60 (60.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tc@h2:~$ 
```

	Interface	IP address

h3	eth0	10.0.2.15
	eth1	192.168.2.2
	lo	127.0.0.1

h4	eth0	10.0.2.15
	eth1	192.168.2.3
	lo	127.0.0.1
h5	eth0	10.0.2.15
	eth1	192.168.3.2
	lo	127.0.0.1
r1	eth0	10.0.2.15
	eth1	192.168.1.1
	eth2	192.168.101.1
	eth3	192.168.102.1
	lo	127.0.0.1
r2	eth0	10.0.2.15
	eth1	192.168.2.1
	eth2	192.168.101.2
	eth3	192.168.103.1
	lo	127.0.0.1

r3	eth0	10.0.2.15

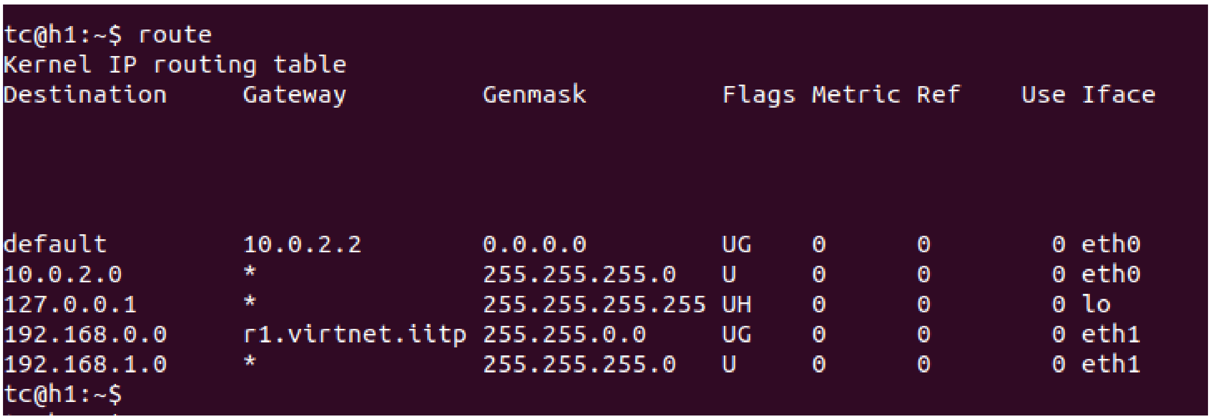
	eth1	192.168.3.1
	eth2	192.168.102.2
	eth3	192.168.103.2
	lo	127.0.0.1

3. Deduce and write down the complete network topology, including details about interfaces, IP address, subnet, and MAC address.

IP address and Interface name were found earlier in the 2nd ques.

The lo interface is not associated with a hardware network interface (it's a virtual loopback interface), it does not have a MAC address.

Running the command “route” gives the default gateway, and ifconfig gave the other information.



```
tc@h1:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface



default         10.0.2.2        0.0.0.0         UG    0      0        0 eth0
10.0.2.0        *               255.255.255.0   U     0      0        0 eth0
127.0.0.1       *               255.255.255.255 UH    0      0        0 lo
192.168.0.0     r1.virtnet.iitp 255.255.0.0     UG    0      0        0 eth1
192.168.1.0     *               255.255.255.0   U     0      0        0 eth1
tc@h1:~$
```

Virtual Machine	Default Gateway	Interface	MAC addr	Netmask
h1	10.0.2.2	eth0	08:00:27:5C:20:74	255.255.255.0
		eth1	08:00:27:63:A5:D5	255.255.255.0
		lo		255.0.0.0
h2	10.0.2.2	eth0	08:00:27:18:C9:6B	255.255.255.0

		eth1	08:00:27:FB:88:E4	255.255.255.0
		lo		255.0.0.0
h3	10.0.2.2	eth0	08:00:27:86:F0:A4	255.255.255.0
		eth1	08:00:27:47:0D:B8	255.255.255.0
		lo		255.0.0.0
h4	10.0.2.2	eth0	08:00:27:0C:62:2B	255.255.255.0
		eth1	08:00:27:7F:48:C9	255.255.255.0
		lo		255.0.0.0
h5	10.0.2.2	eth0	08:00:27:C1:98:3F	255.255.255.0
		eth1	08:00:27:5D:FB:8B	255.255.255.0
		lo		255.0.0.0

r1	10.0.2.2	eth0	08:00:27:C9:61:5A	255.255.255.0
		eth1	08:00:27:E5:D8:04	255.255.255.0
		eth2	08:00:27:D0:7C:CD	255.255.255.0
		eth3	08:00:27:DB:3F:85	255.255.255.0
		lo		255.0.0.0
r2	10.0.2.2	eth0	08:00:27:24:97:41	255.255.255.0
		eth1	08:00:27:03:03:21	255.255.255.0
		eth2	08:00:27:A6:EF:5D	255.255.255.0
		eth3	08:00:27:C4:F2:BE	255.255.255.0
		lo		255.0.0.0

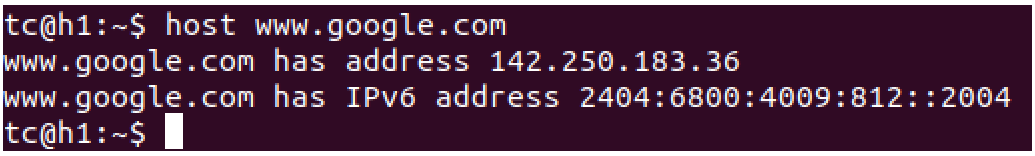
r3	10.0.2.2	eth0	08:00:27:8D:EA:6D	255.255.255.0
		eth1	08:00:27:45:1B:1C	255.255.255.0
		eth2	08:00:27:44:EE:79	255.255.255.0
		eth3	08:00:27:C5:42:09	255.255.255.0
		lo		255.0.0.0

Q4 Does this network have an authoritative DNS server? If yes, give its IP and the port it is listening on.

Ans.

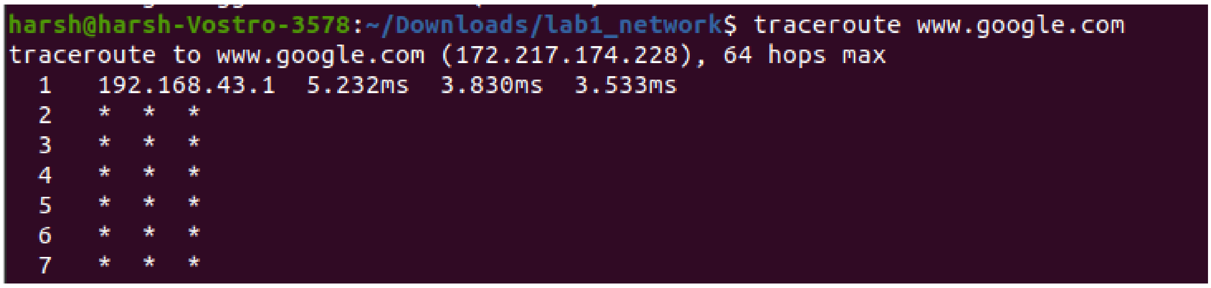
Q5 Find out the IP address for domain “www.google.com”. What is the IP address of the first hop node on the path to “www.google.com”?

Ans.



```
tc@h1:~$ host www.google.com
www.google.com has address 142.250.183.36
www.google.com has IPv6 address 2404:6800:4009:812::2004
tc@h1:~$ 
```

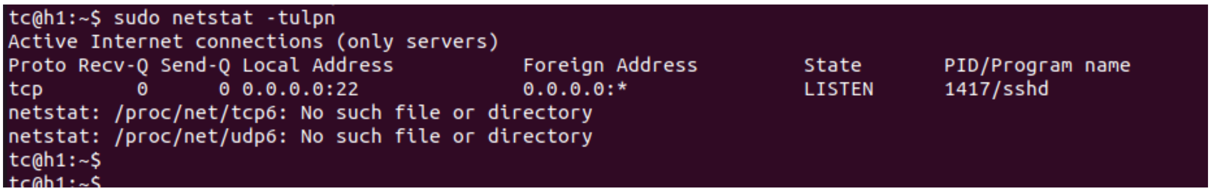
Hence IP address of www.google.com is 142.250.183.36. And the first hop between the route of www.google.com is 192.168.43.1.



```
harsh@harsh-Vostro-3578:~/Downloads/lab1_network$ traceroute www.google.com
traceroute to www.google.com (172.217.174.228), 64 hops max
  1   192.168.43.1  5.232ms  3.830ms  3.533ms
  2   *  *  *
  3   *  *  *
  4   *  *  *
  5   *  *  *
  6   *  *  *
  7   *  *  *
```

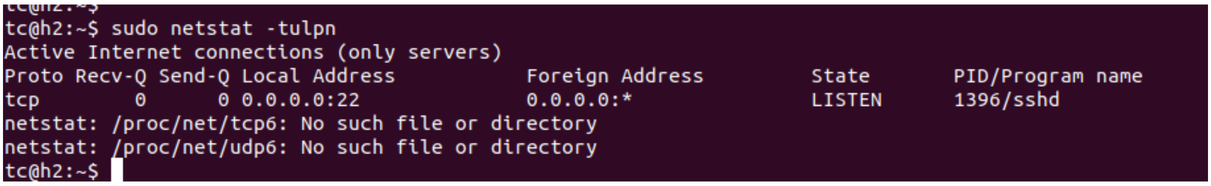
Q6 List the ports on which services are listening on each VMs, and also identify these services.

Ans. For h1: Ssh service having PID 1417 is listening on port 22.



```
tc@h1:~$ sudo netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1417/sshd
netstat: /proc/net/tcp6: No such file or directory
netstat: /proc/net/udp6: No such file or directory
tc@h1:~$
tc@h1:~$
```

For h2: ssh service having PID 1396 listening on port 22.



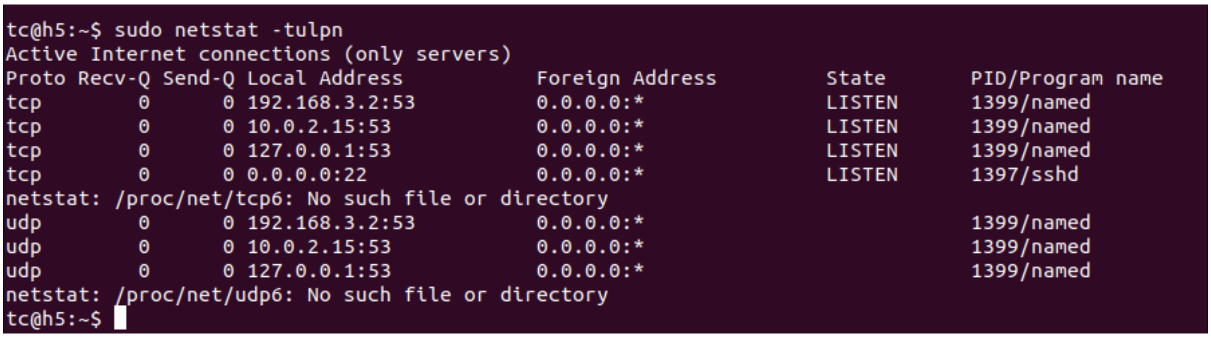
```
tc@h2:~$
tc@h2:~$ sudo netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1396/sshd
netstat: /proc/net/tcp6: No such file or directory
netstat: /proc/net/udp6: No such file or directory
tc@h2:~$ 
```

For h3: ssh service having PID 1396 listening on port 22.

For h4: ssh service having PID 1397 listening on port 22.

For h5:

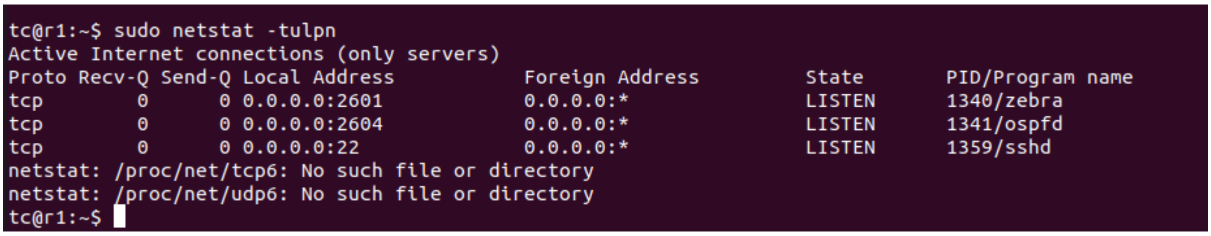
1. Named service having PID 1399 listening on port 53.
2. Ssh service having PID 1397 listening on port 22.



```
tc@h5:~$ sudo netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 192.168.3.2:53          0.0.0.0:*               LISTEN      1399/named
tcp        0      0 10.0.2.15:53            0.0.0.0:*               LISTEN      1399/named
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      1399/named
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1397/sshd
netstat: /proc/net/tcp6: No such file or directory
udp        0      0 192.168.3.2:53          0.0.0.0:*                           1399/named
udp        0      0 10.0.2.15:53            0.0.0.0:*                           1399/named
udp        0      0 127.0.0.1:53            0.0.0.0:*                           1399/named
netstat: /proc/net/udp6: No such file or directory
tc@h5:~$ 
```

For r1:

1. Zebra service with PID 1340 listening on 2601 port no.
2. Ospfd service with PID 1341 listening on 2604.
3. Ssh with PID 1359 listening on 22.



```
tc@r1:~$ sudo netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:2601            0.0.0.0:*               LISTEN      1340/zebra
tcp        0      0 0.0.0.0:2604            0.0.0.0:*               LISTEN      1341/ospfd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1359/sshd
netstat: /proc/net/tcp6: No such file or directory
netstat: /proc/net/udp6: No such file or directory
tc@r1:~$ 
```

For r2:

1. Zebra with PID 1347 listening on port no. 2601.
2. Ospfd with PID 1348 listening on port no. 2604.
3. Ssh with PID 1355 listening on port no. 22.

For r3:

1. Zebra with PID 1356 listening on port no. 2601.
2. Ospfd with PID 1357 listening on port no. 2604.
3. Ssh with PID 1366 listening on port no. 22.

Q7 Do a reverse DNS lookup on all the IPs in the virtual network and note them down.

Ans. lo and eth0 don’t have their domain name.

Using host [IP_addr] the domain name can be found. Alternatively, nslookup command can also be used.

h1	192.168.1.2	h1.virtnet.iitpkd0
h2	192.168.1.3	h2.virtnet.iitpkd
h3	192.168.2.2	h3.virtnet.iitpkd
h4	192.168.2.3	h4.virtnet.iitpkd
h5	192.168.3.2	h5.virtnet.iitpkd
r1		
eth1	192.168.1.1	r1.virtnet.iitpkd
eth2	192.168.101.1	r1.virtnet.iitpkd
eth3	192.168.102.1	r1.virtnet.iitpkd
r2		
eth1	192.168.2.1	r2.virtnet.iitpkd
eth2	192.168.101.2	r2.virtnet.iitpkd
eth3	192.168.103.1	r2.virtnet.iitpkd

r3		
eth1	192.168.3.1	r3.virtnet.iitpkd
eth2	192.168.102.2	r3.virtnet.iitpkd
eth3	192.168.103.2	r3.virtnet.iitpkd