CS4150: Computer Networks Lab

Lab1

111901030
Mayank Singla

Q1. Read the man pages for the following commands: arp ifconfig route host ping tcpdump and netstat. Study the different options associated with each command. Explain each of the above commands in 2-3 sentences.

arp:

It represents the ARP (Address Resolution Protocol) table in the memory which is created by Kernel. It's primary use is to convert an interface's IPv4 address to the device's MAC (Media Access Control) address.

```
arp                          # Print current contents of the table
arp -d <address>             # Deletes an entry from the table with
                               IP address corresponding to the address
arp -s <ip-addr> <hw-addr>   # Insert a new table entry
                               with MAC address as hw_addr.
```

ifconfig: (interface configuration)

It is used to display the running/active interfaces. It is additionally used during the system boot up to initialize all interfaces.

```
ifconfig -a                  # Displays all available interfaces even if down
ifconfig <interface> <up/down>   # Activate/Deactivate the drives
                                   for the given interface
ifconfig <interface> <add/del> <addr>
        # Add/remove an IPv6 address to an interface
```

route :

Kernel creates an IP routing table to map the topology of the network it is in. The main usage of the route command is to add static routes info into the IP routing table and also to display the IP routing table.

```
route                    # Display the routing table entries
sudo route add <name> <gateway> <address>
                         # Add a static route to the IP routing table
sudo route del <name>
                         # Deleting the static route from the IP routing table
```

host :

Used for performing DNS lookups. DNS converts a domain name into the IP address of the corresponding interface. It is also used for performing reverse DNS lookups.

```
host <name>              # DNS lookup
host <ip_addr>           # Reverse DNS lookup
```

ping :

Used to test if a device in the network is reachable or not. The ping command sends a request over the network to corresponding device and upon successful ping, device sends back a response indicating device is reachable in the network.

```
ping google.com
ping -c 5 -q google.com  # Controlling numbers of pings and
                           getting summary only
ping -w 3 google.com     # Timeout ping after sometime
```

tcpdump:

It prints out the details about the live packets that are passing through the network interface. It filters the packets and prints out only a few which satisfy a specific boolean condition

```
sudo tcpdump # Capture packets of current network interface
sudo tcpdump -i <interface> # Prints out the packets received by the interface
sudo tcpdump -n -i wlo1 # Capture the packets with IP addresses
sudo tcpdump -D # Checks all the available interfaces for tcpdump
```

netstat: (network statistics)

It is used to display the network connections, routing tables, and other network statistics. It is mainly used to find the amount of traffic on the network for performance measures.

```
netstat -a # Show both listening and non-listening ports
netstat -l # List all listening ports
netstat -s # Display summary statistics for each protocol
netstat -plut # Display the ports on which services are running
```

Q2. Follow the below instructions to set up a virtual network and write down the interfaces (along with IP address) of each of the VMs in this network:

- **Download the file "lab1 network.tar.xz" from the folder lab1.**
- **Extract this file and step into the extracted directory.**
- **Setup the virtual machines by issuing the command "./setupVMs.sh"**
- **Start the virtual machines by issuing the command "./startVMs.sh"**
- **There are 8 VMs in this network namely h1, h2, h3, h4, h5, r1, r2, r3. The first 5 VMs are hosts and the rest are routers. You can connect to VM x by issuing the command "./connect.sh x".**

```
111901030@aha-acdgf-004l:~/CN_Lab/Lab1/lab1_network$ ./setupVMs.sh
Copying VM configuration...
111901030@aha-acdgf-004l:~/CN_Lab/Lab1/lab1_network$
```

```
111901030@aha-acdgf-004l:~/CN_Lab/Lab1/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.
111901030@aha-acdgf-004l:~/CN_Lab/Lab1/lab1_network$
```

```
111901030@aha-acdgf-004l:~/CN_Lab/Lab1/lab1_network$ ./connect.sh h1
spawn ssh -p 14501 -o StrictHostKeyChecking=no tc@localhost
tc@localhost's password:
   ( '>')
  /) TC (\   Core is distributed with ABSOLUTELY NO WARRANTY.
 (/-_--_-\)           www.tinycorelinux.net

tc@h1:~$
```

Hence, we are successfully able to connect to the VMs in this network.

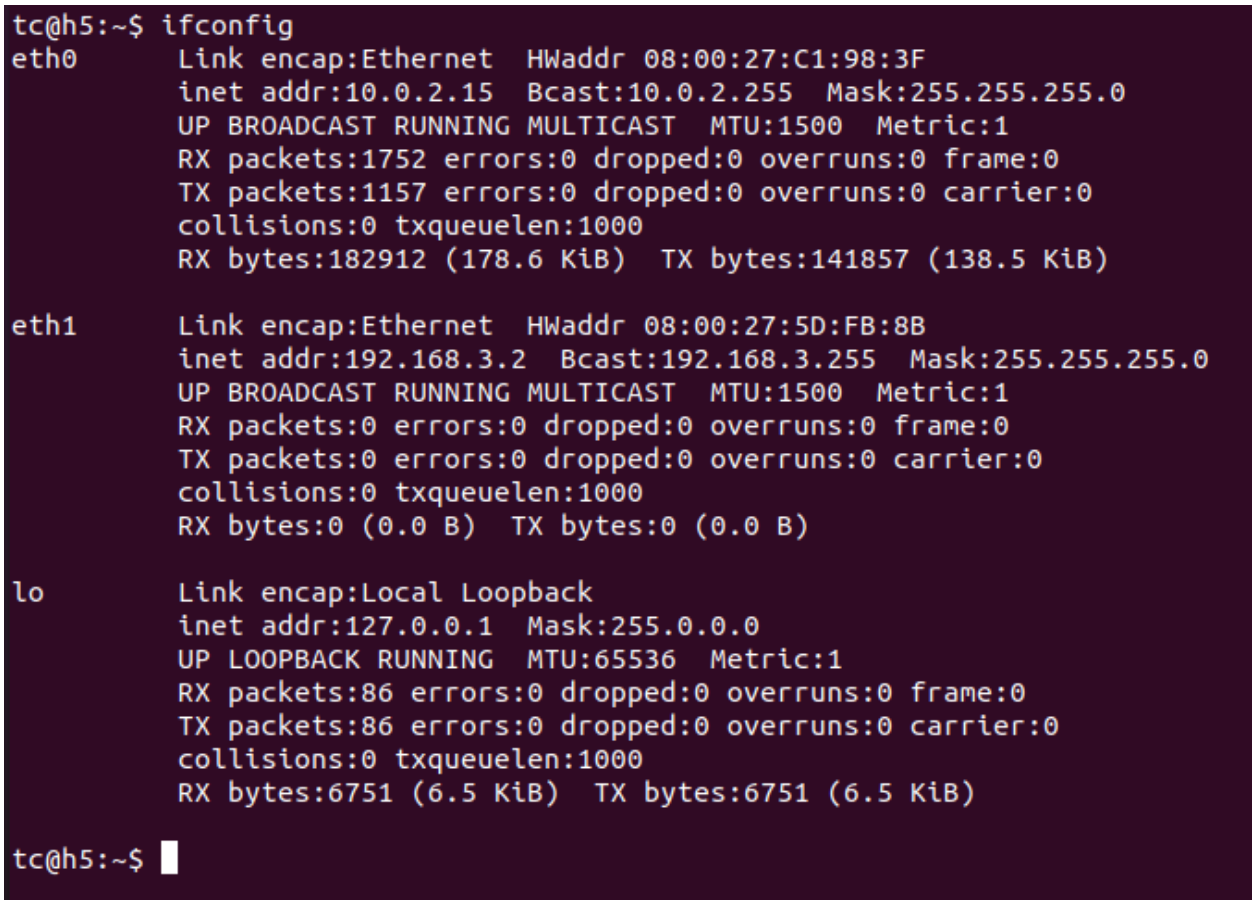
To get the interfaces along with their IP addresses, we will execute the **ifconfig** command on each of the VMs. The IP address is the inet addr and MAC address is the HWaddr.

```
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:915 errors:0 dropped:0 overruns:0 frame:0
          TX packets:578 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:92855 (90.6 KiB)  TX bytes:89173 (87.0 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:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:720 (720.0 B)  TX bytes:1048 (1.0 KiB)

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)

tc@h1:~$
```

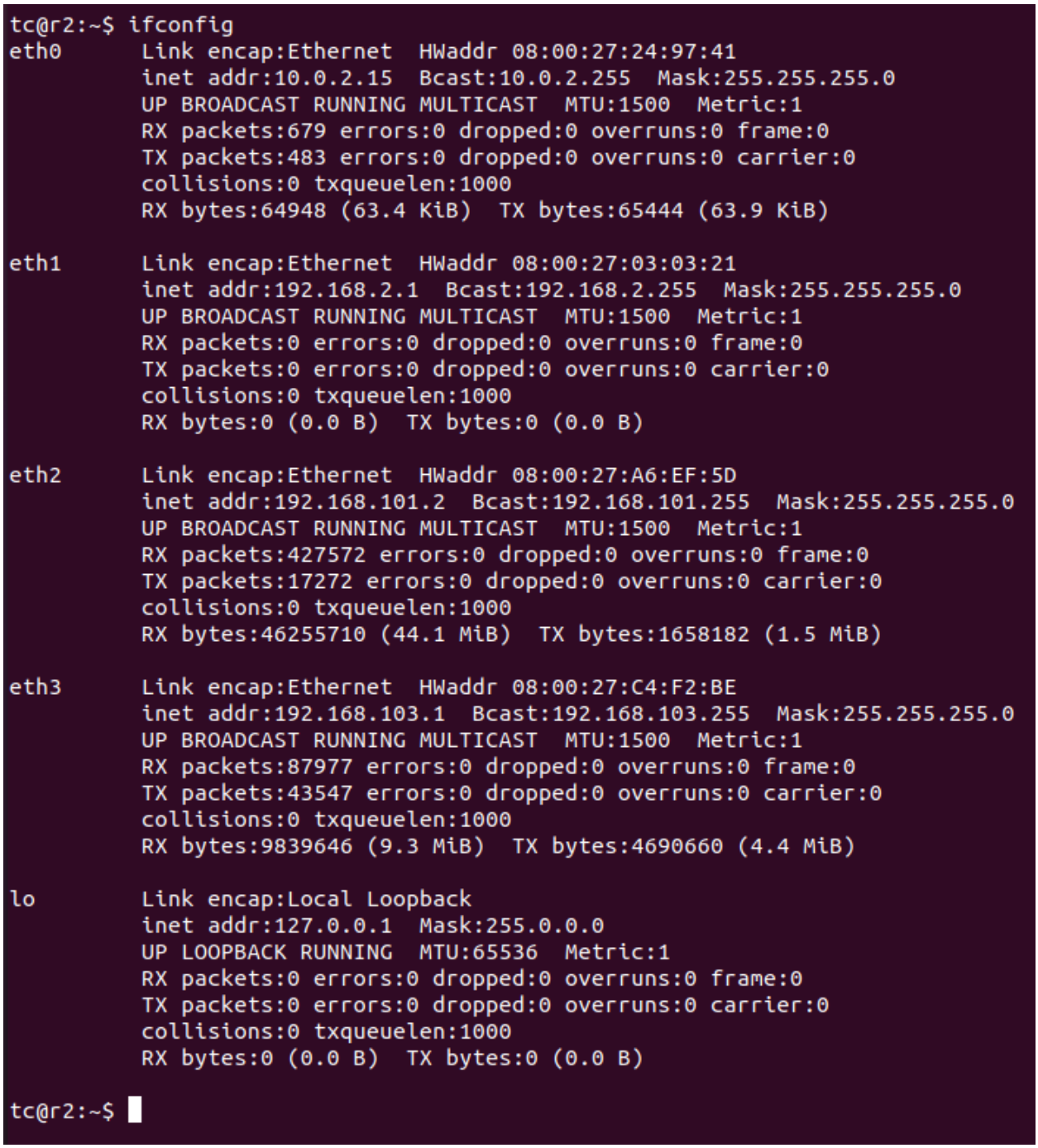
```
tc@h2:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:18:C9:6B
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:391 errors:0 dropped:0 overruns:0 frame:0
          TX packets:251 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:40516 (39.5 KiB)  TX bytes:40140 (39.1 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:~$
```

```
tc@h3:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:86:F0:A4
          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:528 errors:0 dropped:0 overruns:0 frame:0
          TX packets:350 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:52107 (50.8 KiB)  TX bytes:52601 (51.3 KiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:47:0D:B8
          inet addr:192.168.2.2  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  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)

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@h3:~$
```

```
tc@h4:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0C:62:2B
          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:305 errors:0 dropped:0 overruns:0 frame:0
          TX packets:195 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:30218 (29.5 KiB)  TX bytes:30314 (29.6 KiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:7F:48:C9
          inet addr:192.168.2.3  Bcast:192.168.2.255  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:5 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:60 (60.0 B)  TX bytes:390 (390.0 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@h5:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:C1:98:3F
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:1752 errors:0 dropped:0 overruns:0 frame:0
TX packets:1157 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:182912 (178.6 KiB) TX bytes:141857 (138.5 KiB)
eth1 Link encap:Ethernet HWaddr 08:00:27:5D:FB:8B
inet addr:192.168.3.2 Bcast:192.168.3.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 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)
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:86 errors:0 dropped:0 overruns:0 frame:0
TX packets:86 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:6751 (6.5 KiB) TX bytes:6751 (6.5 KiB)
tc@h5:~$

```
tc@r1:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:C9:61:5A
          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:563 errors:0 dropped:0 overruns:0 frame:0
          TX packets:370 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:58345 (56.9 KiB)  TX bytes:62231 (60.7 KiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:E5:D8:04
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1048 (1.0 KiB)  TX bytes:120 (120.0 B)

eth2      Link encap:Ethernet  HWaddr 08:00:27:D0:7C:CD
          inet addr:192.168.101.1  Bcast:192.168.101.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:162253 errors:0 dropped:0 overruns:0 frame:0
          TX packets:77836 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17237748 (16.4 MiB)  TX bytes:8375242 (7.9 MiB)

eth3      Link encap:Ethernet  HWaddr 08:00:27:DB:3F:85
          inet addr:192.168.102.1  Bcast:192.168.102.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:132003 errors:0 dropped:0 overruns:0 frame:0
          TX packets:62324 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14364112 (13.6 MiB)  TX bytes:6555724 (6.2 MiB)

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@r1:~$
```


tc@r2:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:24:97:41
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:679 errors:0 dropped:0 overruns:0 frame:0
TX packets:483 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:64948 (63.4 KiB) TX bytes:65444 (63.9 KiB)
eth1 Link encap:Ethernet HWaddr 08:00:27:03:03:21
inet addr:192.168.2.1 Bcast:192.168.2.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 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)
eth2 Link encap:Ethernet HWaddr 08:00:27:A6:EF:5D
inet addr:192.168.101.2 Bcast:192.168.101.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:427572 errors:0 dropped:0 overruns:0 frame:0
TX packets:17272 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:46255710 (44.1 MiB) TX bytes:1658182 (1.5 MiB)
eth3 Link encap:Ethernet HWaddr 08:00:27:C4:F2:BE
inet addr:192.168.103.1 Bcast:192.168.103.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:87977 errors:0 dropped:0 overruns:0 frame:0
TX packets:43547 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:9839646 (9.3 MiB) TX bytes:4690660 (4.4 MiB)
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@r2:~$

```
tc@r3:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:8D:EA:6D
          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:492 errors:0 dropped:0 overruns:0 frame:0
          TX packets:314 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:51025 (49.8 KiB)  TX bytes:51167 (49.9 KiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:45:1B:1C
          inet addr:192.168.3.1  Bcast:192.168.3.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  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)

eth2      Link encap:Ethernet  HWaddr 08:00:27:44:EE:79
          inet addr:192.168.102.2  Bcast:192.168.102.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:330457 errors:0 dropped:0 overruns:0 frame:0
          TX packets:26939 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:34987914 (33.3 MiB)  TX bytes:2552952 (2.4 MiB)

eth3      Link encap:Ethernet  HWaddr 08:00:27:C5:42:09
          inet addr:192.168.103.2  Bcast:192.168.103.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:207704 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27216 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:22759760 (21.7 MiB)  TX bytes:2731924 (2.6 MiB)

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@r3:~$
```

From the **ifconfig** command, we can infer a lot of information. Interface **eth0** is used for setting up the virtual network, interface **eth1** is used by the hosts to connect to the routers. Routers can have more than one interface. Here, interface **eth2** and **eth3** are used by the routers to connect to each other. Every interface has a network address (IP address) and a link layer address (MAC address). Every ethernet card has a unique MAC address each of which creates an interface. Hence, every router here has 3 different MAC addresses corresponding to each interface.

IP Address Table:

VMs	Interface: eth0	Interface: eth1	Interface: eth2	Interface: eth3	Interface: lo
r1	10.0.2.15	192.168.1.1	192.168.101.1	192.168.102.1	127.0.0.1
r2	10.0.2.15	192.168.2.1	192.168.101.2	192.168.103.1	127.0.0.1
r3	10.0.2.15	192.168.3.1	192.168.102.2	192.168.103.2	127.0.0.1
h1	10.0.2.15	192.168.1.2			127.0.0.1
h2	10.0.2.15	192.168.1.3			127.0.0.1
h3	10.0.2.15	192.168.2.2			127.0.0.1
h4	10.0.2.15	192.168.2.3			127.0.0.1
h5	10.0.2.15	192.168.3.2			127.0.0.1

Q3. Deduce and write down the complete network topology, including details about interfaces, IP address, subnet, and MAC address.

The details of interfaces and IP addresses were already computed in the previous question.

MAC address Table: (Using the **ifconfig** command from previous question)

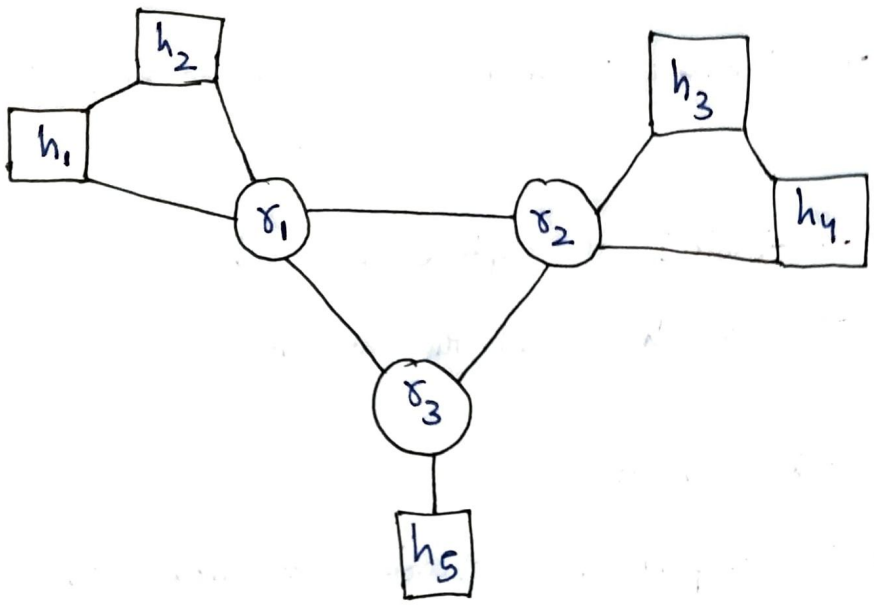
VMs	Interface: eth0	Interface: eth1	Interface: eth2	Interface: eth3
r1	08:00:27:C9:61:5A	08:00:27:E5:D8:04	08:00:27:D0:7C:CD	08:00:27:DB:3F:85
r2	08:00:27:24:97:41	08:00:27:03:03:21	08:00:27:A6:EF:5D	08:00:27:C4:F2:BE
r3	08:00:27:8D:EA:6D	08:00:27:45:1B:1C	08:00:27:44:EE:79	08:00:27:C5:42:09
h1	08:00:27:5C:20:74	08:00:27:63:A5:D5		
h2	08:00:27:18:C9:6B	08:00:27:FB:88:E4		

h3	08:00:27:86:F0:A4	08:00:27:47:0D:B8		
h4	08:00:27:0C:62:2B	08:00:27:7F:48:C9		
h5	08:00:27:C1:98:3F	08:00:27:5D:FB:8B		

Subnets:
Since, the subnet mask for all the interfaces is **255.255.255.0**, we need to compare the first 24 (from the binary representation) bits from the IP address to compute which all virtual machines will be in the same subnet and are connected together. Hence, we get the following subnets in the virtual network:

Subnet IP	VMs
192.168.1.0/24	r1, h1, h2
192.168.2.0/24	r2, h3, h4
192.168.3.0/24	r3, h5
192.168.101.0/24	r1, r2
192.168.102.0/24	r3, r1
192.168.103.0/24	r2, r3

Network Topology:
From the above found subnets, we can construct the following network topology:



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

```
tc@h5:~$ sudo netstat -plnt
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      1382/named
tcp        0      0 10.0.2.15:53            0.0.0.0:*               LISTEN      1382/named
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      1382/named
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1386/sshd
netstat: /proc/net/tcp6: No such file or directory
tc@h5:~$
```

Yes, the VM **h5** provides the DNS utility to the whole network as it has the DNS program called **named**. So, it is acting as a DNS server. We can see from the above command (**sudo netstat -plnt**) that it is listening on the **port 53** and has the **IP address** as **192.168.3.2**
The **named** program is responsible for converting the DNS and reverse DNS lookup in the virtual network from any other machine.

```
111901030@aha-acdgf-004l:~/CN_Lab/Lab1/lab1_network$ ./connect.sh h3
spawn ssh -p 14503 -o StrictHostKeyChecking=no tc@localhost
tc@localhost's password:
   ( '>')
  /) TC (\   Core is distributed with ABSOLUTELY NO WARRANTY.
 (/-_--_-\)           www.tinycorelinux.net

tc@h3:~$ cat /etc/resolv.conf
nameserver 192.168.3.2
tc@h3:~$
```

We can also see that all the other machines have the **nameserver** with the same IP address as that of the machine **h5** in their **/etc/resolv.conf** file.

```
tc@h5:~$ dig -t ns h1.virtnet.iitpkd

; <<>> DiG 9.14.3 <<>> -t ns h1.virtnet.iitpkd
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 34108
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: bd844f3bf4c08ea8fb2464a8630f69cdf614842aa3a12670 (good)
;; QUESTION SECTION:
;h1.virtnet.iitpkd.             IN      NS

;; AUTHORITY SECTION:
.                       84465   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2022083100 1800 900 604800 86400

;; Query time: 0 msec
;; SERVER: 192.168.3.2#53(192.168.3.2)
;; WHEN: Wed Aug 31 14:01:49 UTC 2022
;; MSG SIZE  rcvd: 149
```

```
tc@h5:~$ dig -t ns r1.virtnet.iitpkd

; <<>> DiG 9.14.3 <<>> -t ns r1.virtnet.iitpkd
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 38251
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 370a8c9817ce0aff40d640b2630f69db54d70c48ee0570a3 (good)
;; QUESTION SECTION:
;r1.virtnet.iitpkd.             IN      NS

;; AUTHORITY SECTION:
.                       84451   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2022083100 1800 900 604800 86400

;; Query time: 0 msec
;; SERVER: 192.168.3.2#53(192.168.3.2)
;; WHEN: Wed Aug 31 14:02:03 UTC 2022
;; MSG SIZE  rcvd: 149
```

We can also see that executing the command **dig -t ns <ip_address>** will give the IP address along with the port of the authoritative DNS server in the **AUTHORITY SECTION**, which also confirms that the VM **h5** is the authoritative DNS server in this virtual network.

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”?

```
111901030@aha-acdgf-004l:~/CN_Lab/Lab1/lab1_network$ host www.google.com
www.google.com has address 142.251.42.36
www.google.com has IPv6 address 2404:6800:4007:81a::2004
111901030@aha-acdgf-004l:~/CN_Lab/Lab1/lab1_network$
```

The IP address for the domain “www.google.com” is **142.251.42.36** as found from the above command.

```
111901030@aha-acdgf-004l:~/CN_Lab/Lab1/lab1_network$ ./connect.sh r2
spawn ssh -p 14602 -o StrictHostKeyChecking=no tc@localhost
tc@localhost's password:
   ( '>')
  /) TC (\   Core is distributed with ABSOLUTELY NO WARRANTY.
 (/-_--_-\)           www.tinycorelinux.net

tc@r2:~$ traceroute www.google.com
traceroute to www.google.com (142.251.42.36), 30 hops max, 38 byte packets
 1  10.0.2.2 (10.0.2.2)  0.017 ms  0.349 ms  0.519 ms
 2  _gateway (10.64.1.1)  2.853 ms  0.902 ms  1.032 ms
 3  14.139.174.49 (14.139.174.49)  6.338 ms  2.985 ms  1.402 ms
 4  *  *  *
 5  *  *  *
 6  *  *  *
 7  10.119.73.122 (10.119.73.122)  27.635 ms  27.094 ms  25.269 ms
 8  72.14.195.128 (72.14.195.128)  28.562 ms  26.139 ms  26.774 ms
 9  *  *  *
10  142.251.55.40 (142.251.55.40)  26.046 ms  216.239.59.170 (216.239.59.170)  25.712 ms  142.251.49.216 (142.251.49.216)  25.865 ms
11  108.170.253.119 (108.170.253.119)  26.310 ms  74.125.242.130 (74.125.242.130)  27.070 ms  74.125.242.147 (74.125.242.147)  29.518 ms
12  209.85.251.14 (209.85.251.14)  69.039 ms  142.251.49.232 (142.251.49.232)  47.980 ms  142.250.212.0 (142.250.212.0)  54.417 ms
13  108.170.248.177 (108.170.248.177)  66.553 ms  142.250.238.206 (142.250.238.206)  58.691 ms  108.170.248.161 (108.170.248.161)  44.439 ms
14  142.251.69.45 (142.251.69.45)  45.008 ms  142.251.69.43 (142.251.69.43)  68.701 ms  108.170.248.177 (108.170.248.177)  66.875 ms
15  142.251.69.45 (142.251.69.45)  44.495 ms  bom12s20-in-f4.1e100.net (142.251.42.36)  52.038 ms  142.251.69.45 (142.251.69.45)  43.907 ms
```

```
111901030@aha-acdgf-004l:~/CN_Lab/Lab1/lab1_network$ ./connect.sh h5
spawn ssh -p 14505 -o StrictHostKeyChecking=no tc@localhost
tc@localhost's password:
   ( '>')
  /) TC (\   Core is distributed with ABSOLUTELY NO WARRANTY.
 (/-_--_-\)           www.tinycorelinux.net

tc@h5:~$ traceroute www.google.com
traceroute to www.google.com (142.250.71.4), 30 hops max, 38 byte packets
 1  10.0.2.2 (10.0.2.2)  0.407 ms  0.284 ms  0.253 ms
 2  10.64.1.1 (10.64.1.1)  1.359 ms  1.031 ms  0.663 ms
 3  14.139.174.49 (14.139.174.49)  0.919 ms  1.198 ms  1.248 ms
 4  * * *
 5  * * *
 6  * * *
 7  10.119.73.122 (10.119.73.122)  26.155 ms  25.203 ms  27.732 ms
 8  72.14.213.20 (72.14.213.20)  27.484 ms  27.725 ms  27.191 ms
 9  * * *
10  74.125.242.129 (74.125.242.129)  27.091 ms  142.251.55.236 (142.251.55.236)  25.358 ms  142.250.228.220 (142.250.228.220)  26.179 ms
11  74.125.242.130 (74.125.242.130)  26.253 ms  172.253.73.29 (172.253.73.29)  25.906 ms  26.048 ms
12  maa03s34-in-f4.1e100.net (142.250.71.4)  26.025 ms  25.902 ms  108.170.253.97 (108.170.253.97)  27.472 ms
```

Executing the **traceroute** command from the routers and hosts in the virtual network, the IP address of the first hop node on the path to **"www.google.com"** is **10.0.2.2**

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

Executing the command **sudo netstat -plnt** on each VM to list the services and the ports on which these services are listening.

```
tc@h1:~$ sudo netstat -plnt
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      1406/sshd
netstat: /proc/net/tcp6: No such file or directory
tc@h1:~$
```

```
tc@h2:~$ sudo netstat -plnt
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      1388/sshd
netstat: /proc/net/tcp6: No such file or directory
tc@h2:~$
```

```
tc@h3:~$ sudo netstat -plnt
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      1388/sshd
netstat: /proc/net/tcp6: No such file or directory
tc@h3:~$
```

```
tc@h4:~$ sudo netstat -plnt
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      1390/sshd
netstat: /proc/net/tcp6: No such file or directory
```

```
tc@h5:~$ sudo netstat -plnt
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      1382/named
tcp        0      0 10.0.2.15:53            0.0.0.0:*               LISTEN      1382/named
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      1382/named
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1386/sshd
netstat: /proc/net/tcp6: No such file or directory
tc@h5:~$
```

```
tc@r1:~$ sudo netstat -plnt
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      1346/zebra
tcp        0      0 0.0.0.0:2604            0.0.0.0:*               LISTEN      1347/ospfd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1356/sshd
netstat: /proc/net/tcp6: No such file or directory
tc@r1:~$
```

```
tc@r2:~$ sudo netstat -plnt
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      1336/zebra
tcp        0      0 0.0.0.0:2604            0.0.0.0:*               LISTEN      1337/ospfd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1346/sshd
netstat: /proc/net/tcp6: No such file or directory
tc@r2:~$
```

```
tc@r3:~$ sudo netstat -plnt
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      1344/zebra
tcp        0      0 0.0.0.0:2604            0.0.0.0:*               LISTEN      1345/ospfd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1354/sshd
netstat: /proc/net/tcp6: No such file or directory
tc@r3:~$
```

VM	Service Name	Port Number
h1	sshd	22
h2	sshd	22
h3	sshd	22
h4	sshd	22

h5	named	53
h5	sshd	22
r1	zebra	2601
r1	ospfd	2604
r1	sshd	22
r2	zebra	2601
r2	ospfd	2604
r2	sshd	22
r3	zebra	2601
r3	ospfd	2604
r3	sshd	22

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

```
tc@h5:~$ host 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer r1.virtnet.iitpkd.
tc@h5:~$ host 192.168.101.1
1.101.168.192.in-addr.arpa domain name pointer r1.virtnet.iitpkd.
tc@h5:~$ host 192.168.102.1
1.102.168.192.in-addr.arpa domain name pointer r1.virtnet.iitpkd.
tc@h5:~$ host 192.168.2.1
1.2.168.192.in-addr.arpa domain name pointer r2.virtnet.iitpkd.
tc@h5:~$ host 192.168.101.2
2.101.168.192.in-addr.arpa domain name pointer r2.virtnet.iitpkd.
tc@h5:~$ host 192.168.103.1
1.103.168.192.in-addr.arpa domain name pointer r2.virtnet.iitpkd.
tc@h5:~$ host 192.168.3.1
1.3.168.192.in-addr.arpa domain name pointer r3.virtnet.iitpkd.
tc@h5:~$ host 192.168.102.2
2.102.168.192.in-addr.arpa domain name pointer r3.virtnet.iitpkd.
tc@h5:~$ host 192.168.103.2
2.103.168.192.in-addr.arpa domain name pointer r3.virtnet.iitpkd.
tc@h5:~$ host 192.168.1.2
2.1.168.192.in-addr.arpa domain name pointer h1.virtnet.iitpkd.
tc@h5:~$ host 192.168.1.3
3.1.168.192.in-addr.arpa domain name pointer h2.virtnet.iitpkd.
tc@h5:~$ host 192.168.2.2
2.2.168.192.in-addr.arpa domain name pointer h3.virtnet.iitpkd.
tc@h5:~$ host 192.168.2.3
3.2.168.192.in-addr.arpa domain name pointer h4.virtnet.iitpkd.
tc@h5:~$ host 192.168.3.2
2.3.168.192.in-addr.arpa domain name pointer h5.virtnet.iitpkd.
tc@h5:~$
```

Using the **host <ip_address>** command to do a reverse DNS lookup.

IP Address(s)	Domain Name
192.168.1.2	h1.virtnet.iitpkd
192.168.1.3	h2.virtnet.iitpkd
192.168.2.2	h3.virtnet.iitpkd
192.168.2.3	h4.virtnet.iitpkd
192.168.3.2	h5.virtnet.iitpkd
192.168.1.1 / 192.168.101.1 / 192.168.102.1	r1.virtnet.iitpkd

192.168.2.1 / 192.168.101.2 / 192.168.103.1	r2.virtnet.iitpkd
192.168.3.1 / 192.168.102.2 / 192.168.103.2	r3.virtnet.iitpkd