Computer Networks Lab 1 : Overview

1. **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.**

a) **arp :**

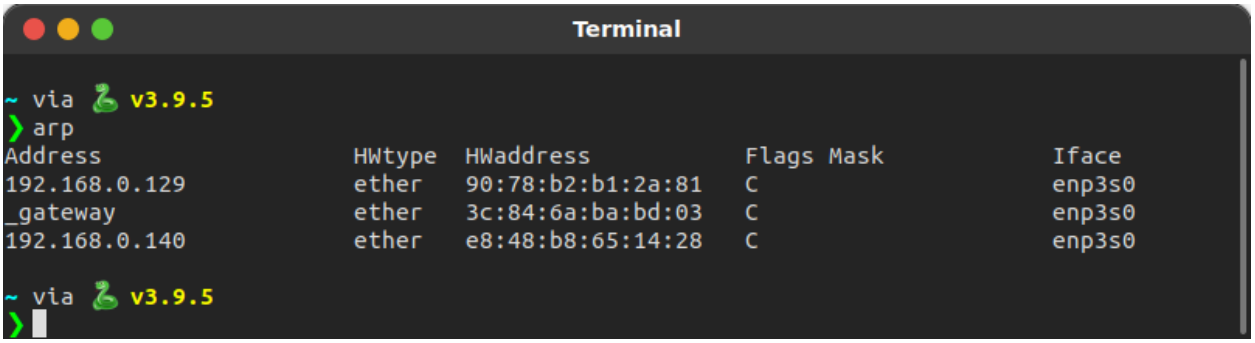
The ***arp*** command displays the ARP (Address Resolution Protocol) table in the memory which is created by the kernel. The primary use of ARP is to convert an interface's IPv4 address to the device's MAC (Media Access Control) address. For this purpose the kernel maintains an ARP table with the map between several IPv4 addresses and the corresponding MAC addresses of the devices in the same subnet.

Important Usage:

i) arp -d <address> :
Deletes an entry from the ARP table with the corresponding IP address matching the address in the command.

ii) arp -s <address> <hw_addr>:
Inserting a new table entry with IP address corresponding to address and the MAC address corresponding to hw_addr.

The ARP table can be found at **/proc/net/arp.**



In the following ARP table, the Address Column corresponds to the IPv4 address of an interface in the subnet, HWtype refers to the interface type, HWaddress refers to the MAC address and Iface refers to the name of the interface.

b) Ifconfig :

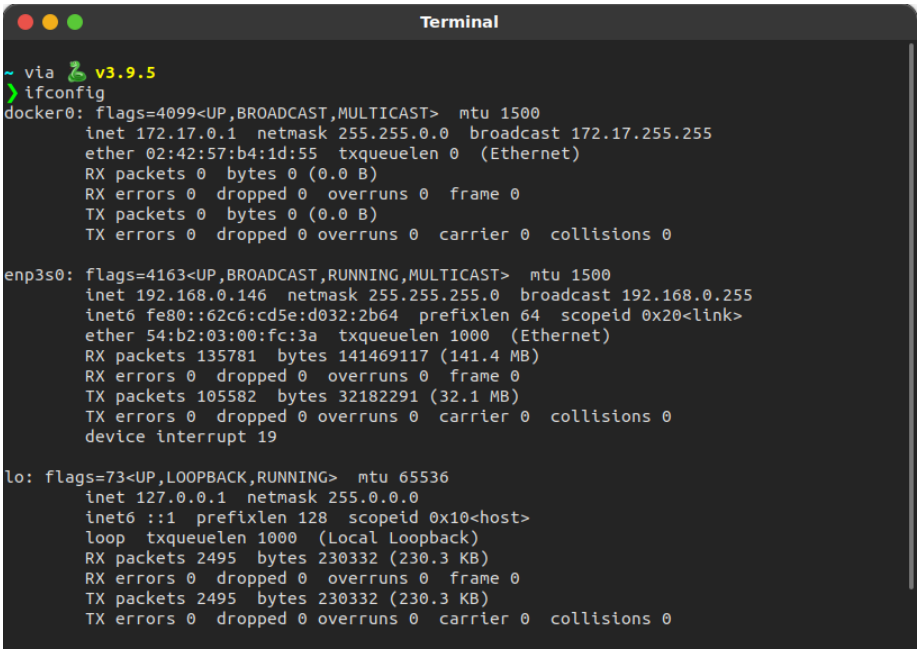
(*short for interface configuration*) This command is used to display the status of the running/active interfaces. This command is additionally used during the system boot up to initialize interfaces.

Important Usage:

i) ifconfig -a : Displays all the available interfaces i.e all the interfaces active/inactive.

ii) ifconfig <interface> :
Displays the status of the interface whose name matches with the interface name given in the command.

iii) ifconfig <up/down> :
The up flag causes interfaces to be activated and the down flag shuts down the interface.



Here we can see one of the interfaces “enp3s0” and its details. The IP address of this interface is described by the **inet** field.

c) route :

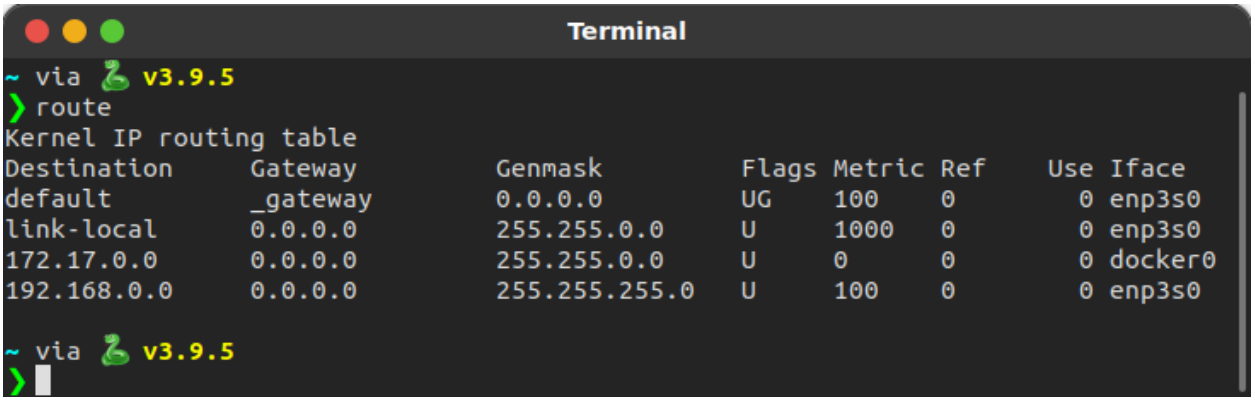
IP routing table is created by the kernel to map the topology of the network it is in. Some automated procedures in the kernel help building the IP routing table. The main use of the **route** command is to add static routes into the IP routing table and also to display the IP routing table. Static routes are the routes that are not discovered by the kernel because they are not part of the network.

Important Usage:

i) route add <name> <gateway> <address>:
For adding a static route to the IP routing table.

ii) route del <name>:
Deleting the static route from the IP routing table.

As we can see the routing table consists of the destination address for each of the interfaces it is connected to hence getting the overall network topology.



d) host :

The host command is used for performing Domain Name System (DNS) lookups. DNS converts a domain name into the IP address of the corresponding interface. But host is also used for performing reverse DNS lookups i.e converting the IP address of the interface into the domain name of the host it is connected to.

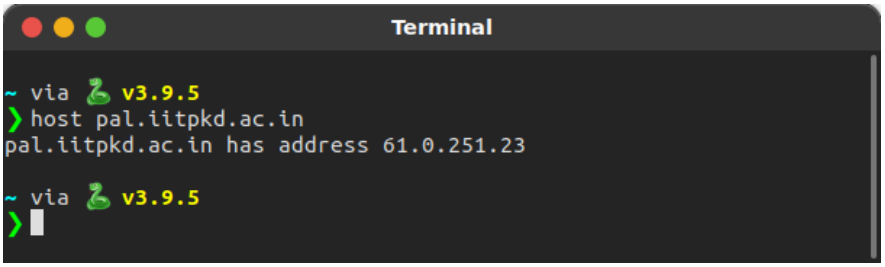
Important Usage:

i) host <name> :

Displays the IP address associated with the corresponding domain name.

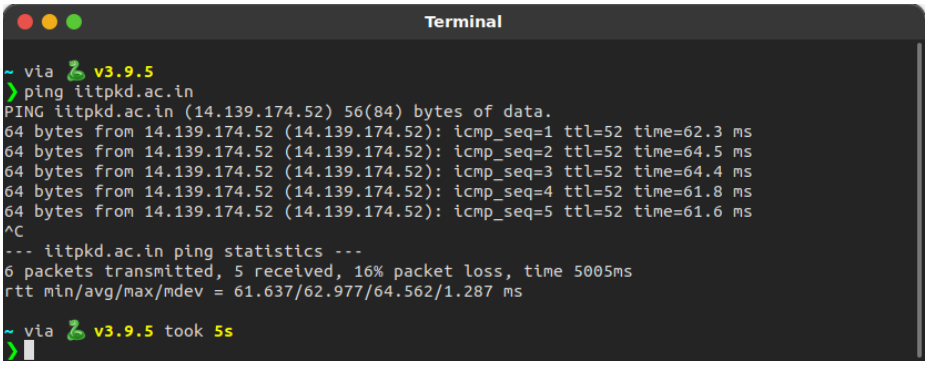
ii) host <address>: (Reverse DNS lookup)

Displays the name of the host corresponding to the ip address.



e) ping :

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



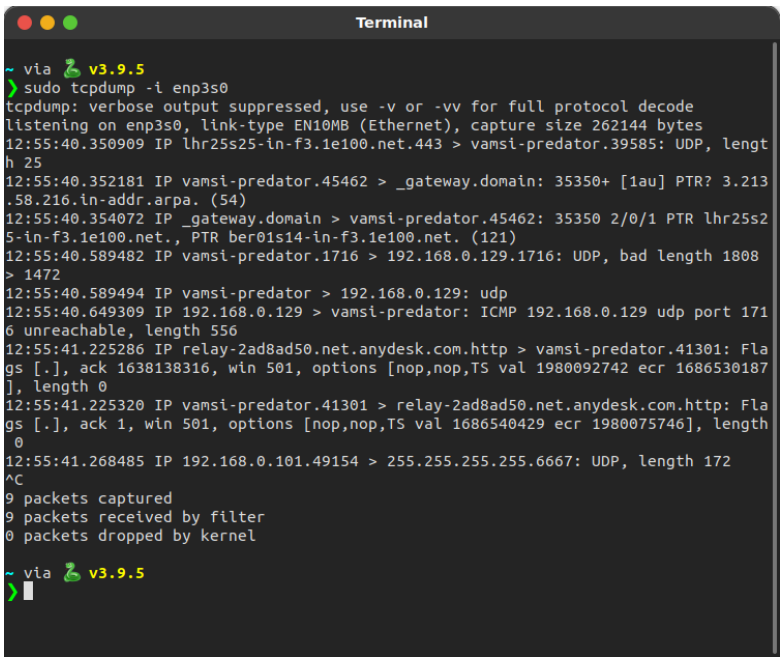
f) tcpdump :

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

Important Usage:

i) sudo tcdump -i <interface name> :
Prints out packets received by the particular interface.

ii) sudo tcpdump -D : Checks all the available interfaces for tcpdump.

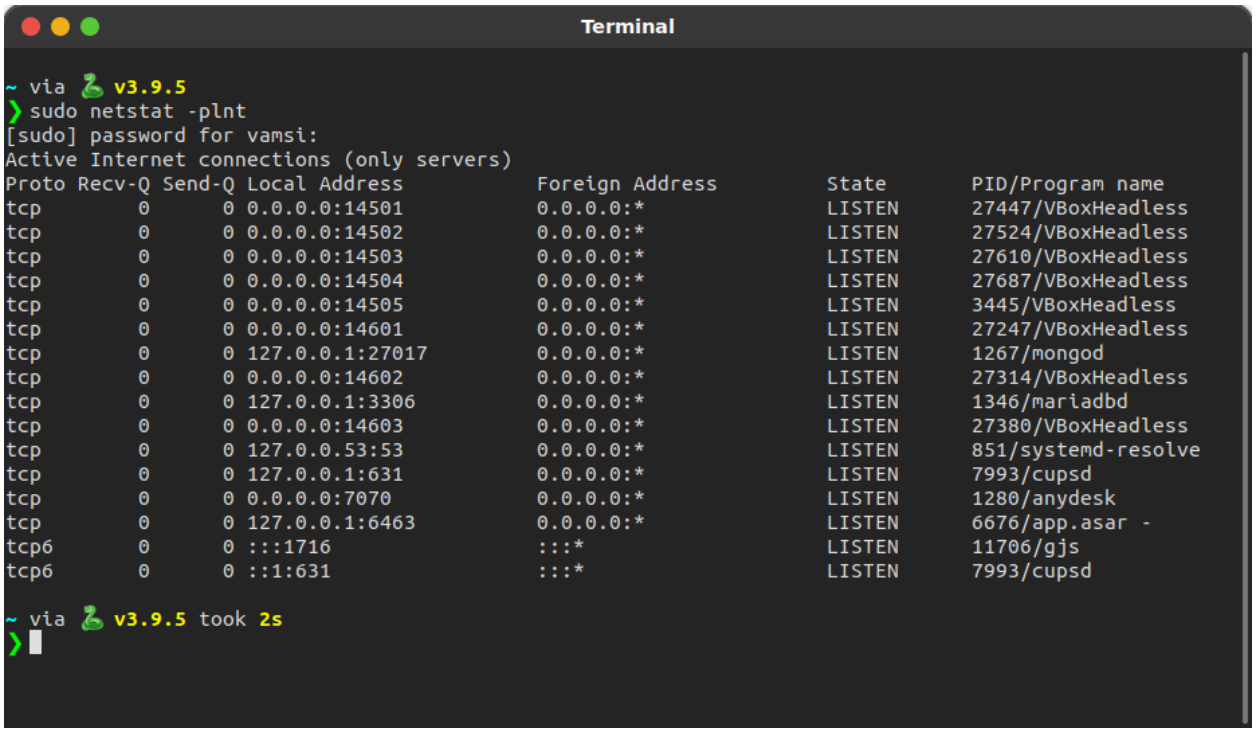


e) netstat :

(*network statistics*) netstat is a command that is used to display the network connections, routing tables, and other network statistics. This is mainly used for finding the amount of traffic on the network for performance measurements.

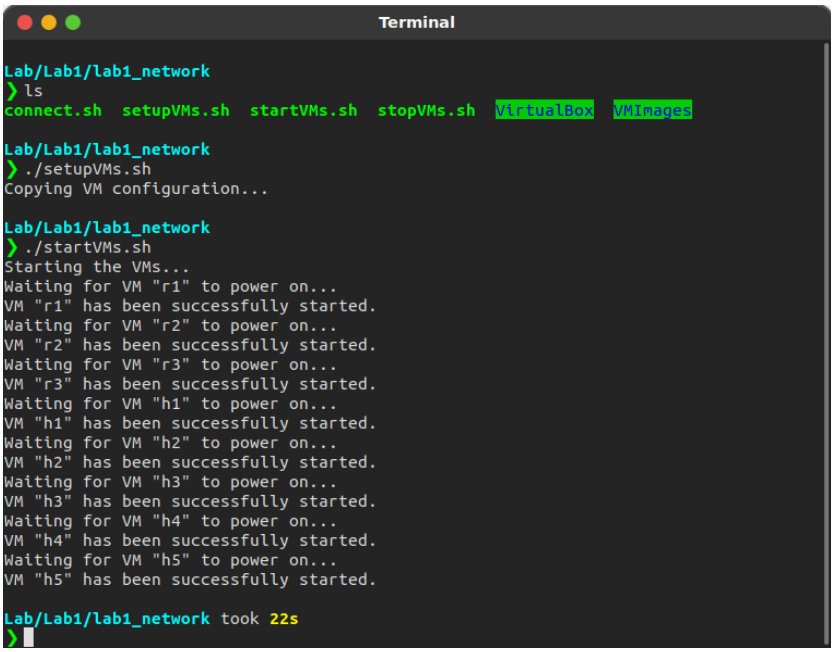
Important Usage:

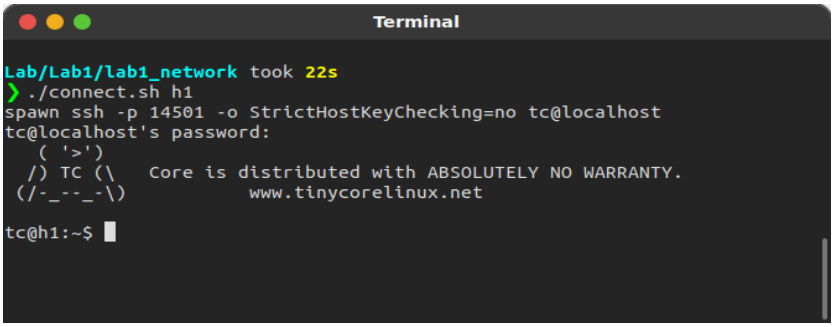
i) netstat -l : Lists all the listening ports
ii) netstat -s: Displays statistics by protocol
iii) netstat -plnt: Displays the ports on which services are running



2. 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 6 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”.**





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

```
Lab/Lab1/lab1_network
$ ./connect.sh r1
spawn ssh -p 14601 -o StrictHostKeyChecking=no tc@localhost
tc@localhost's password:
   ( '>')
  /) TC (\   Core is distributed with ABSOLUTELY NO WARRANTY.
 (/-_--_-\)           www.tinycorelinux.net

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:89 errors:0 dropped:0 overruns:0 frame:0
          TX packets:54 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12612 (12.3 KiB)  TX bytes:10108 (9.8 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.
5.0
          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:D0:7C:CD
          inet addr:192.168.101.1  Bcast:192.168.101.255  Mask:255.255.
5.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:159 errors:0 dropped:0 overruns:0 frame:0
          TX packets:173 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13566 (13.2 KiB)  TX bytes:14842 (14.4 KiB)

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.
5.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:149 errors:0 dropped:0 overruns:0 frame:0
          TX packets:161 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12810 (12.5 KiB)  TX bytes:13538 (13.2 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: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:~$
```

```
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:~$ 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:90 errors:0 dropped:0 overruns:0 frame:0
          TX packets:55 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12666 (12.3 KiB)  TX bytes:10168 (9.9 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:163 errors:0 dropped:0 overruns:0 frame:0
          TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14206 (13.8 KiB)  TX bytes:14046 (13.7 KiB)

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:148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:159 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12460 (12.1 KiB)  TX bytes:13418 (13.1 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: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:~$
```

```
Lab/Lab1/lab1_network
$ ./connect.sh r3
spawn ssh -p 14603 -o StrictHostKeyChecking=no tc@localhost
tc@localhost's password:
   ( '>')
  /) TC (\   Core is distributed with ABSOLUTELY NO WARRANTY.
 (/-_--_-\)           www.tinycorelinux.net

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:255.255.25
5.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:105 errors:0 dropped:0 overruns:0 frame:0
          TX packets:64 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13746 (13.4 KiB)  TX bytes:11048 (10.7 KiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:45:1B:1C
          inet addr:192.168.3.1  Bcast:192.168.3.255  Mask:255.2
55.255.0
          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:2
55.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:150 errors:0 dropped:0 overruns:0 frame:0
          TX packets:156 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12820 (12.5 KiB)  TX bytes:13208 (12.8 KiB)

eth3      Link encap:Ethernet  HWaddr 08:00:27:C5:42:09
          inet addr:192.168.103.2  Bcast:192.168.103.255  Mask:2
55.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:156 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12700 (12.4 KiB)  TX bytes:12940 (12.6 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: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:~$
[2] 0:bash*                                                    "vamsi-predator" 08:51 27-Aug-21
```

```
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:255.255.25
5.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:186 errors:0 dropped:0 overruns:0 frame:0
          TX packets:116 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:23790 (23.2 KiB)  TX bytes:19844 (19.3 KiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:63:A5:D5
          inet addr:192.168.1.2  Bcast:192.168.1.255  Mask:255.2
55.255.0
          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@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:148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:88 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:18503 (18.0 KiB)  TX bytes:15133 (14.7 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: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@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:144 errors:0 dropped:0 overruns:0 frame:0
          TX packets:88 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:18257 (17.8 KiB)  TX bytes:14981 (14.6 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:126 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14328 (13.9 KiB)  TX bytes:11280 (11.0 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: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@h4:~$
```

```
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:125 errors:0 dropped:0 overruns:0 frame:0
          TX packets:87 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:18065 (17.6 KiB)  TX bytes:12154 (11.8 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: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@h5:~$
[1] 0:bash*                                                    "vamsi-predator" 08:51 27-Aug-21
```

IP Address Table:

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

MAC Address Tables:

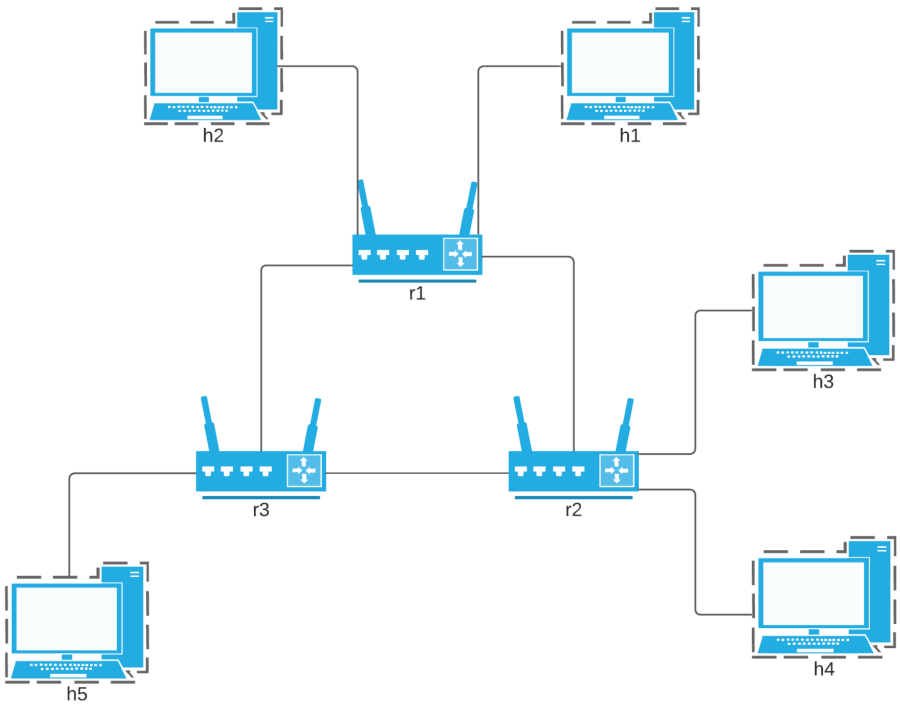
Machine	MAC Address
h1	08:00:27:63:A5:D5
h2	08:00:27:FB:88:E4
h3	08:00:27:47:0D:B8
h4	08:00:27:7F:48:C9
h5	08:00:27:5D:FB:8B

Machine	Interface: eth1	Interface: eth2	Interface: eth3
r1	08:00:27:E5:D8:04	08:00:27:D0:7C:CD	08:00:27:DB:3F:85
r2	08:00:27:03:03:21	08:00:27:A6:EF:5D	08:00:27:C4:F2:BE
r3	08:00:27:45:1B:1C	08:00:27:44:EE:79	08:00:27:C5:42:09

Subnets:

Subnets	Machines
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:



About the network topology:

From the **ifconfig** command we can extract a lot of information, like interface details, IP addresses, Subnet Mask, MAC addresses etc,...,. Interface **eth0** is used for setting up the virtual network, interface **eth1** is used by the hosts to connect to the routers. Routers have more than one interface, and hence the interfaces **eth2, eth3** are used by the routers to connect with each other. Every interface has a link layer address (MAC Address) and a network address (IP address) and hence we can see that a single router will be having 3 different MAC addresses the router has three interfaces. To be more specific an ethernet card has a unique MAC address, and with this we can say that the router has 3 cards each of which creates an interface.

From the IP addresses we can infer that the VMs h1, h2, r1 are under a single subnet with the IP **192.168.1.0/24** since the first 24 bits of the IP addresses of h1,h2,r1 are equal which indicates that they are connected together and form a subnet**.** And in a similar manner h3, h4, r2 are connected with the subnet IP **192.168.2.0/24** and h5, r2 are connected together with the subnet IP **192.168.3.0/24.** The routers are connected to each other in a cyclic manner which forms 3 different subnets with **192.168.101.0/24 (r1, r2), 192.168.102.0/24 (r3, r1), 192.168.103.0/24 (r2, r3).**

4. 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      1397/named
tcp        0      0 10.0.2.15:53            0.0.0.0:*               LISTEN      1397/named
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      1397/named
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1401/sshd
netstat: /proc/net/tcp6: No such file or directory
tc@h5:~$
```

The machine h5 has the DNS program called named which provides the DNS utility to the entire network and hence making it the DNS server. This program is listening on port 53, and the IP address of the server is 192.168.3.2.

```
tc@h5:/etc$ ls
fstab          inittab        mtab           protocols      skel/
group          issue          nsswitch.conf  resolv.conf    sudoers
gshadow        ld.so.cache    os-release     rpc            sysconfig/
host.conf      ld.so.conf     passwd         securetty      udev/
hostname       mke2fs.conf    pcmcia/        services
hosts          modprobe.conf  profile        shadow
init.d/        motd           profile.d/     shells
tc@h5:/etc$ cat resolv.conf
nameserver 192.168.3.2
nameserver 10.0.2.3
tc@h5:/etc$
```

The named program is responsible for converting the DNS into IP address anywhere in the network i.e if we call a dns lookup in any other machine in the network the query is broadcasted to the DNS server, VM h5 in this case, and the domain name is converted into its corresponding IP address and is sent as a response.

5. 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"?

```
tc@r2:~$ traceroute www.google.com
traceroute to www.google.com (142.250.195.228), 30 hops max, 38 byte packets
 1  10.0.2.2 (10.0.2.2)  0.285 ms  1.707 ms  0.162 ms
 2  _gateway (192.168.0.1)  2.707 ms  1.451 ms  1.920 ms
 3  10.141.0.1 (10.141.0.1)  8.550 ms  3.350 ms  3.065 ms
 4  *  broadband.actcorp.in (183.83.249.10)  58.416 ms  23.102 ms
 5  *  *  *
 6  broadband.actcorp.in (183.82.14.34)  17.838 ms  15.880 ms  16.680 ms
 7  108.170.253.97 (108.170.253.97)  17.515 ms  108.170.253.113 (108.170.253.113)  16.172 ms  108.170.253.
97 (108.170.253.97)  17.355 ms
 8  142.250.224.7 (142.250.224.7)  16.150 ms  15.499 ms  216.239.56.71 (216.239.56.71)  16.097 ms
 9  maa03s43-in-f4.1e100.net (142.250.195.228)  17.188 ms  16.853 ms  16.551 ms
tc@r2:~$
```

```
Terminal

~ via 🐍 v3.9.5
❯ traceroute www.google.com
traceroute to www.google.com (142.250.195.196), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  3.441 ms  3.405 ms  3.387 ms
 2  10.141.0.1 (10.141.0.1)  10.395 ms  11.555 ms  11.537 ms
 3  broadband.actcorp.in (183.83.249.10)  11.520 ms  11.504 ms  12.743 ms
 4  * * *
 5  broadband.actcorp.in (183.82.14.34)  16.915 ms  18.227 ms  18.212 ms
 6  108.170.253.97 (108.170.253.97)  19.442 ms 108.170.253.113 (108.170.253.113)
 15.812 ms  15.776 ms
 7  142.251.49.219 (142.251.49.219)  16.847 ms  16.960 ms 142.251.49.217 (142.251
.49.217)  15.986 ms
 8  maa03s42-in-f4.1e100.net (142.250.195.196)  16.578 ms  16.797 ms  17.452 ms

~ via 🐍 v3.9.5
❯
```

Running the command on VM:

First Hop Node IP Address - 10.0.2.2

Running the command on machine:

Fist Hop Node IP Address - 192.168.0.1

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

```
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      1404/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      1376/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      1379/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      1396/sshd
netstat: /proc/net/tcp6: No such file or directory
tc@h4:~$
```

```
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      1397/named
tcp        0      0 10.0.2.15:53            0.0.0.0:*               LISTEN      1397/named
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      1397/named
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1401/sshd
netstat: /proc/net/tcp6: No such file or directory
tc@h5:~$
```

```
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      1352/zebra
tcp        0      0 0.0.0.0:2604            0.0.0.0:*               LISTEN      1353/ospfd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1362/sshd
netstat: /proc/net/tcp6: No such file or directory
tc@r2:~$
```

Machine	Port Number	Service
h1	22	sshd
h2	22	sshd
h3	22	sshd
h4	22	sshd
h5	53	named
h5	22	sshd
r1	22	sshd
r1	2601	zebra
r1	2604	ospfd
r2	22	sshd
r2	2601	zebra
r2	2604	ospfd
r3	22	sshd
r3	2601	zebra
r3	2604	ospfd

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

Command used: host <address>

IP Address	Domain Name
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
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