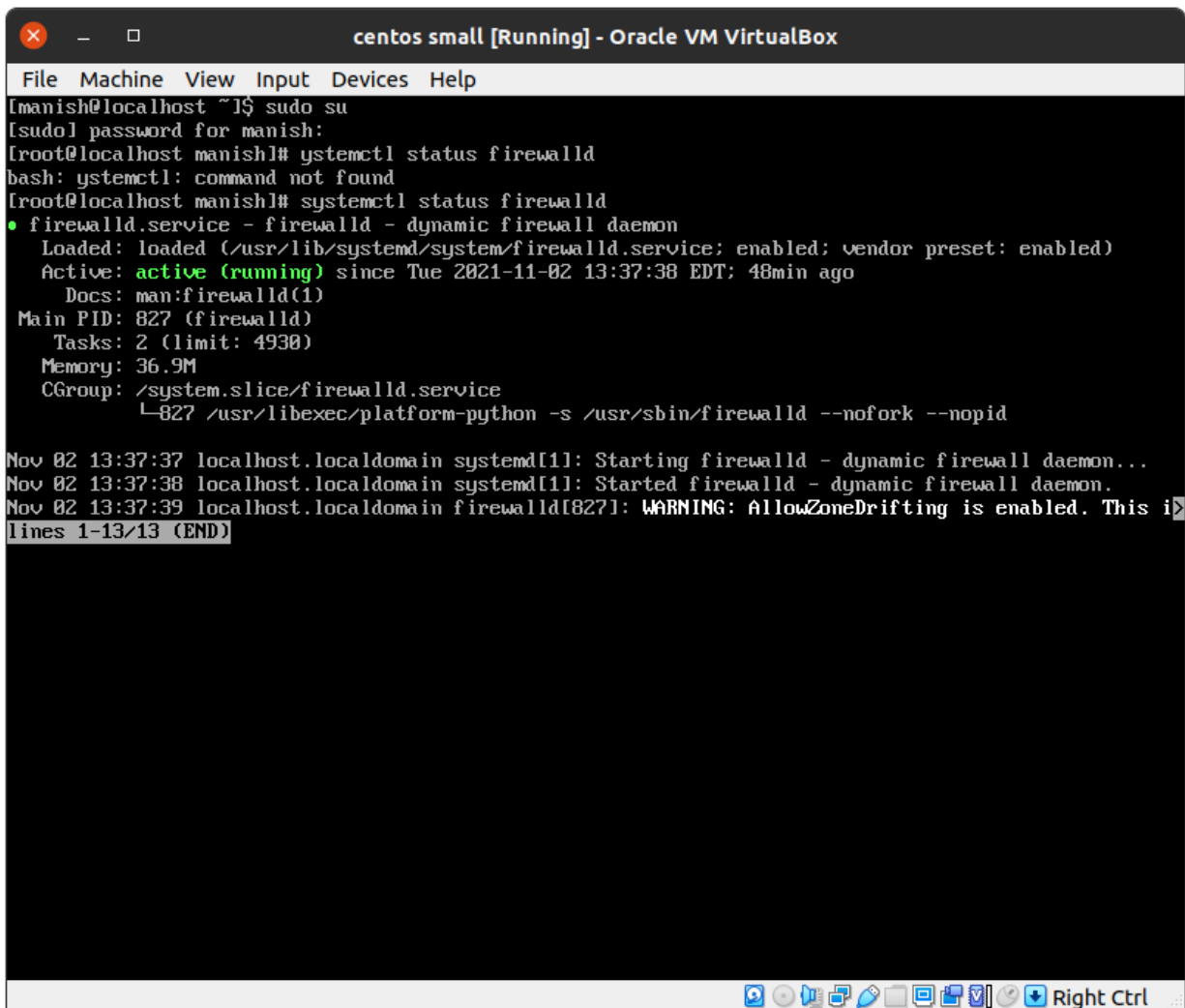


Firewall in CentOS

Firewalld is already installed by default and active in cent os so it is not required to install again.

I. The status of the firewall is checked with the command:

sudo systemctl status firewalld



```
centos small [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[manish@localhost ~]$ sudo su
[sudo] password for manish:
[root@localhost manish]# ystemctl status firewalld
bash: ystemctl: command not found
[root@localhost manish]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2021-11-02 13:37:38 EDT; 48min ago
     Docs: man:firewalld(1)
  Main PID: 827 (firewalld)
    Tasks: 2 (limit: 4930)
   Memory: 36.9M
   CGroup: /system.slice/firewalld.service
           └─827 /usr/libexec/platform-python -s /usr/sbin/firewalld --nofork --nopid

Nov 02 13:37:37 localhost.localdomain systemd[1]: Starting firewalld - dynamic firewall daemon...
Nov 02 13:37:38 localhost.localdomain systemd[1]: Started firewalld - dynamic firewall daemon.
Nov 02 13:37:39 localhost.localdomain firewalld[827]: WARNING: AllowZoneDrifting is enabled. This i
lines 1-13/13 (END)
```

li. Blocking an ip permanently in centos:

Example : ip address of reddit.com is **192.232.45.148**

The complete command to block the above ip address is:

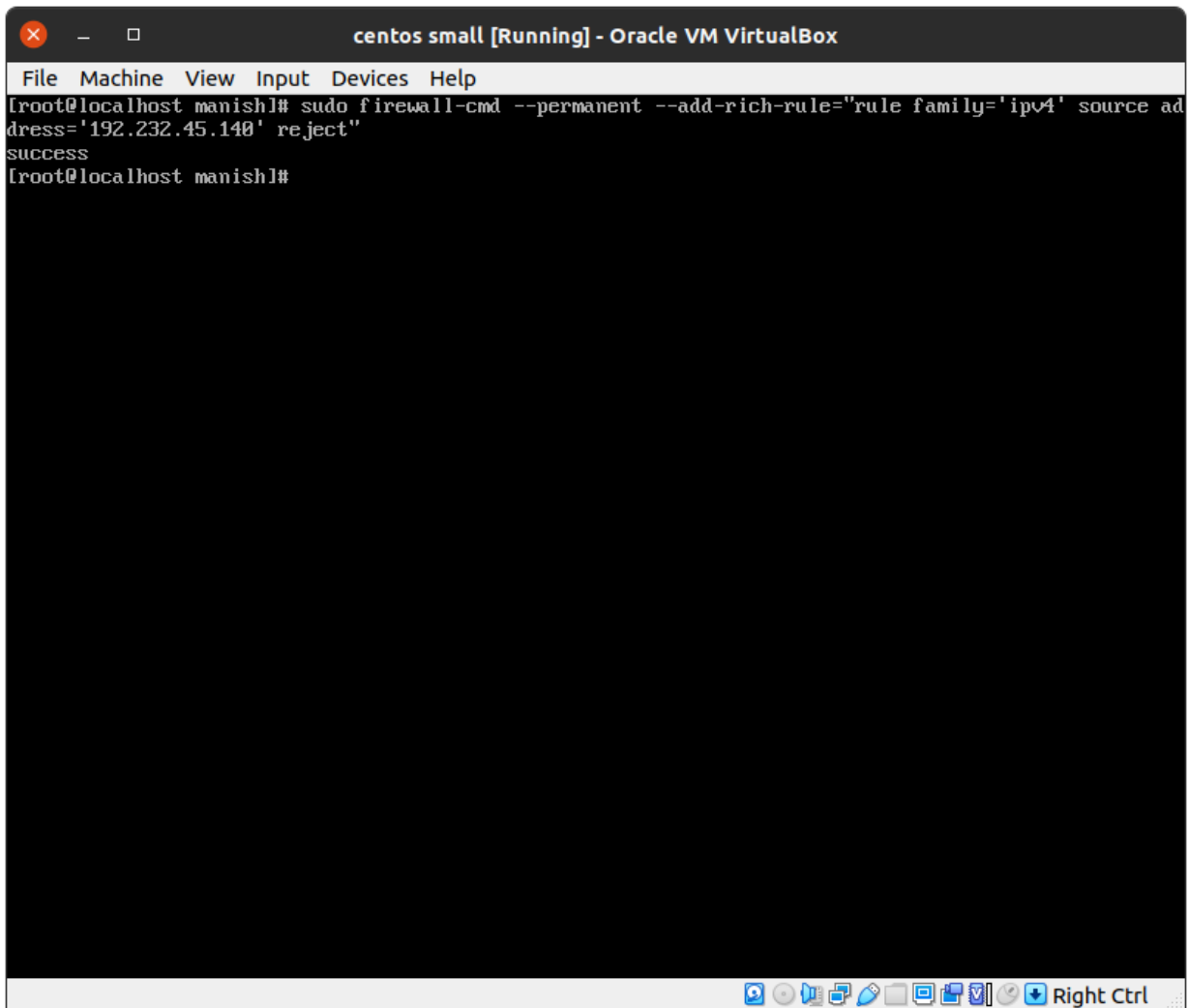
```
sudo firewall-cmd \  
--permanent \  
--add-rich="rule family='ipv4' \  
-- source address='192.232.45.148' \  
reject "
```

Then the firewall is reloaded with the command:

```
sudo firewall-cmd --reload
```

The firewall rules can be listed as:

```
sudo firewall-cmd --list-all
```



lii. Allow ssh, http and https connections in the firewall:

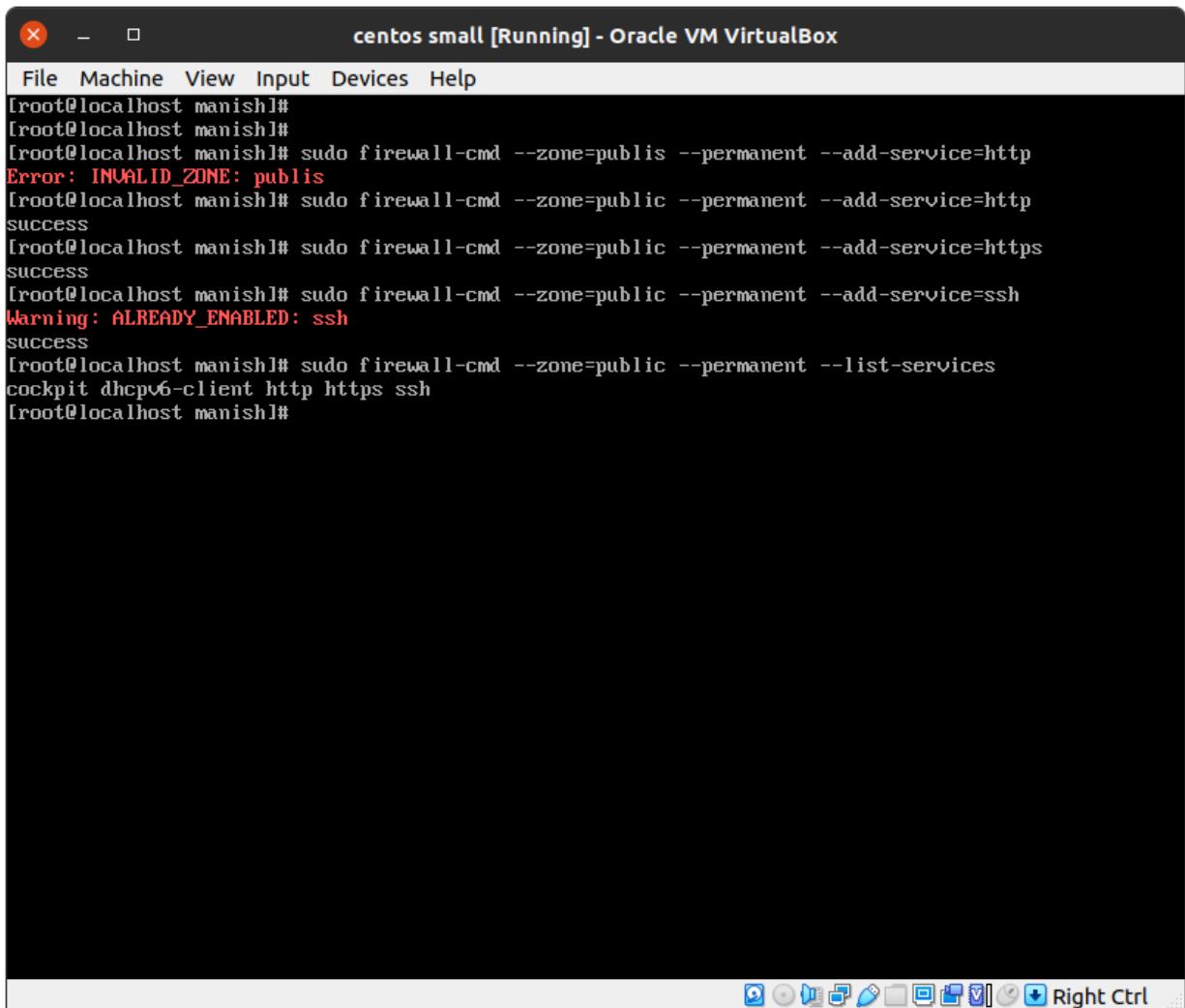
In cent os/rhel a service can be allowed using the command:

```
sudo firewall-cmd --zone=public --permanent -add-service=  
service_name
```

Therefore http, https and ssh were allowed using the commands as below:

```
sudo firewall-cmd --zone=public --permanent -add-service =ssh  
sudo firewall-cmd --zone=public --permanent -add-service =https
```

sudo firewall-cmd --zone=public --permanent --add-service=http



```
[root@localhost manish]#  
[root@localhost manish]#  
[root@localhost manish]# sudo firewall-cmd --zone=publis --permanent --add-service=http  
Error: INVALID_ZONE: publis  
[root@localhost manish]# sudo firewall-cmd --zone=public --permanent --add-service=http  
success  
[root@localhost manish]# sudo firewall-cmd --zone=public --permanent --add-service=https  
success  
[root@localhost manish]# sudo firewall-cmd --zone=public --permanent --add-service=ssh  
Warning: ALREADY_ENABLED: ssh  
success  
[root@localhost manish]# sudo firewall-cmd --zone=public --permanent --list-services  
cockpit dhcpv6-client http https ssh  
[root@localhost manish]#
```

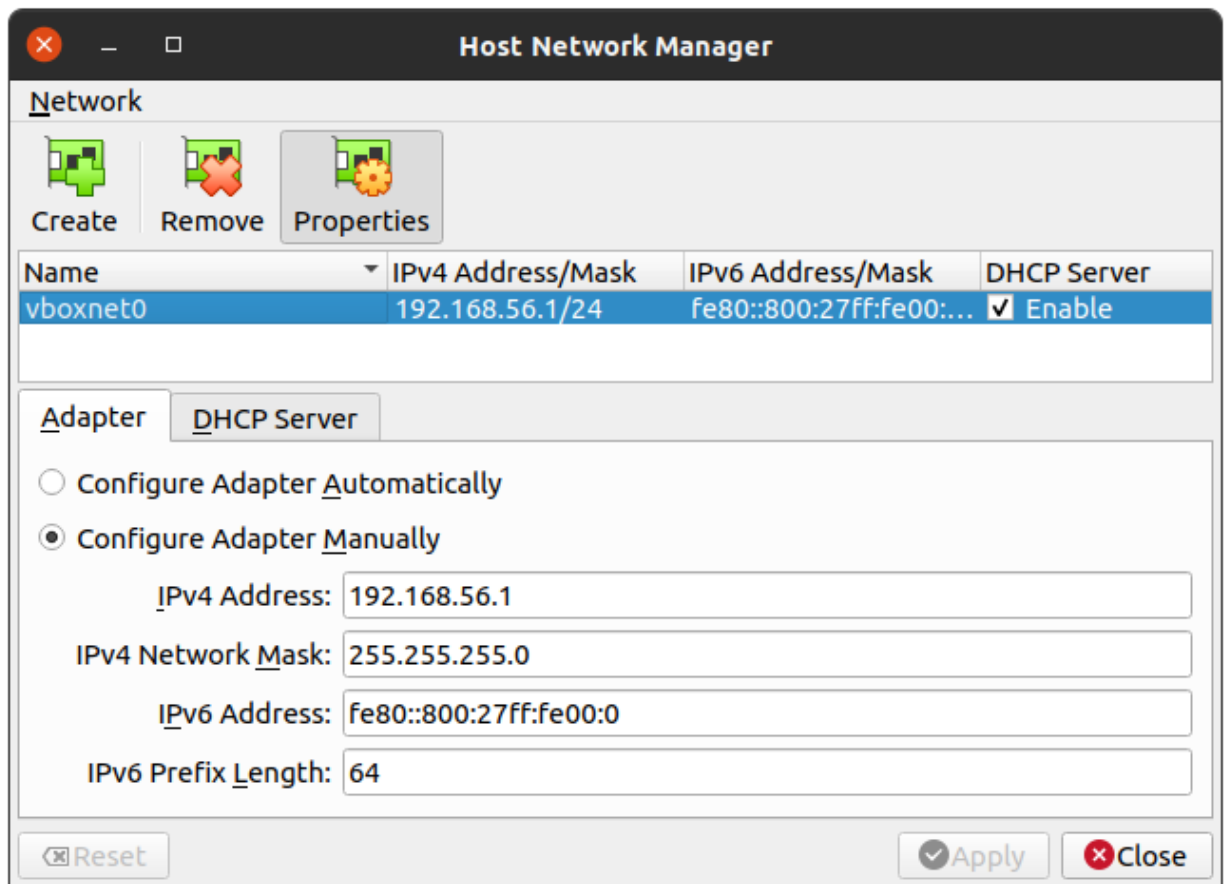
2. Configuring a VM as a router and a second VM as a node/client and NATing from a VM

VM1= Vm which is configured as router

VM2= Vm which acts as client/node

Steps:

I. In the virtual box's host network manager, a network(**vboxnet0**) was created.

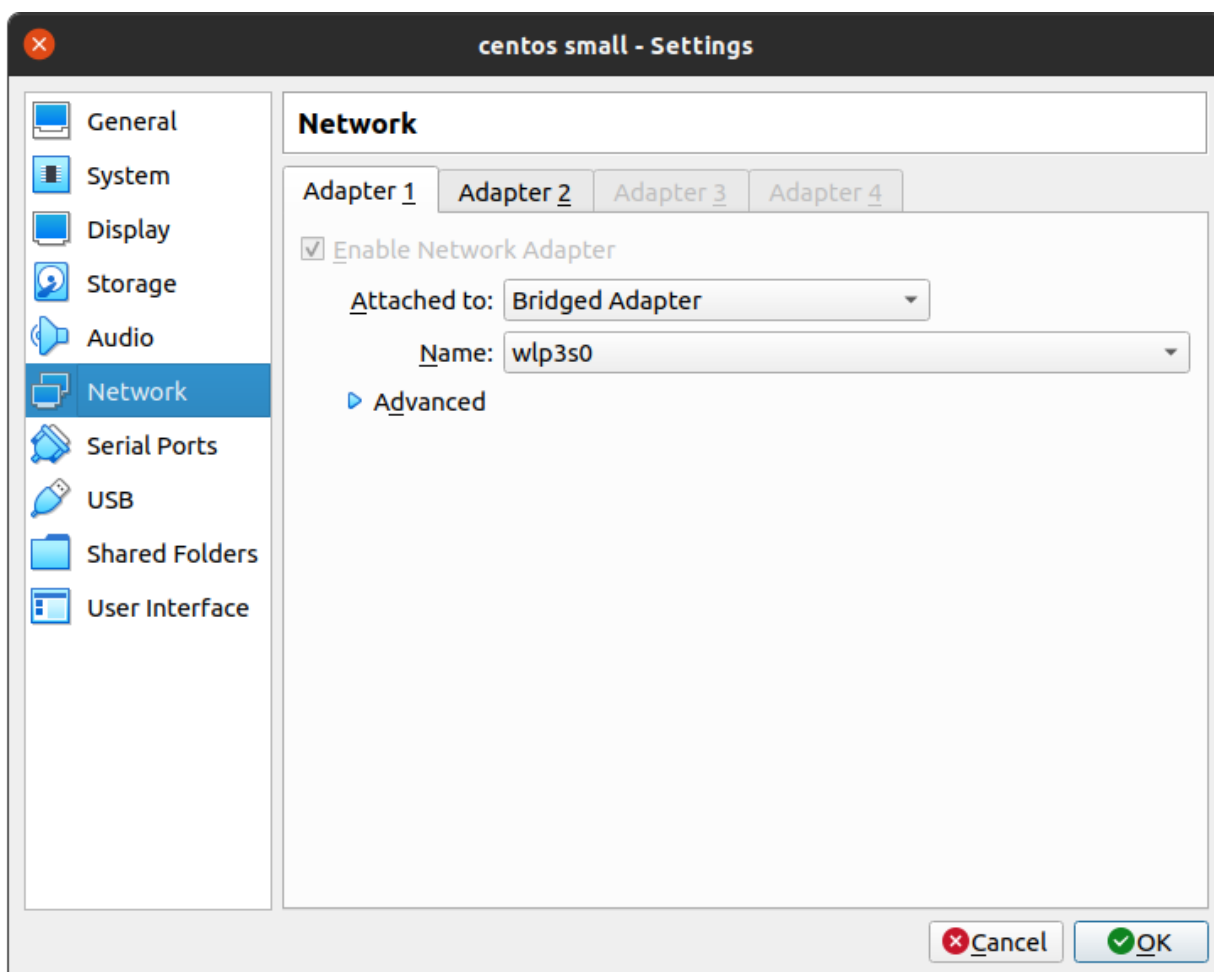


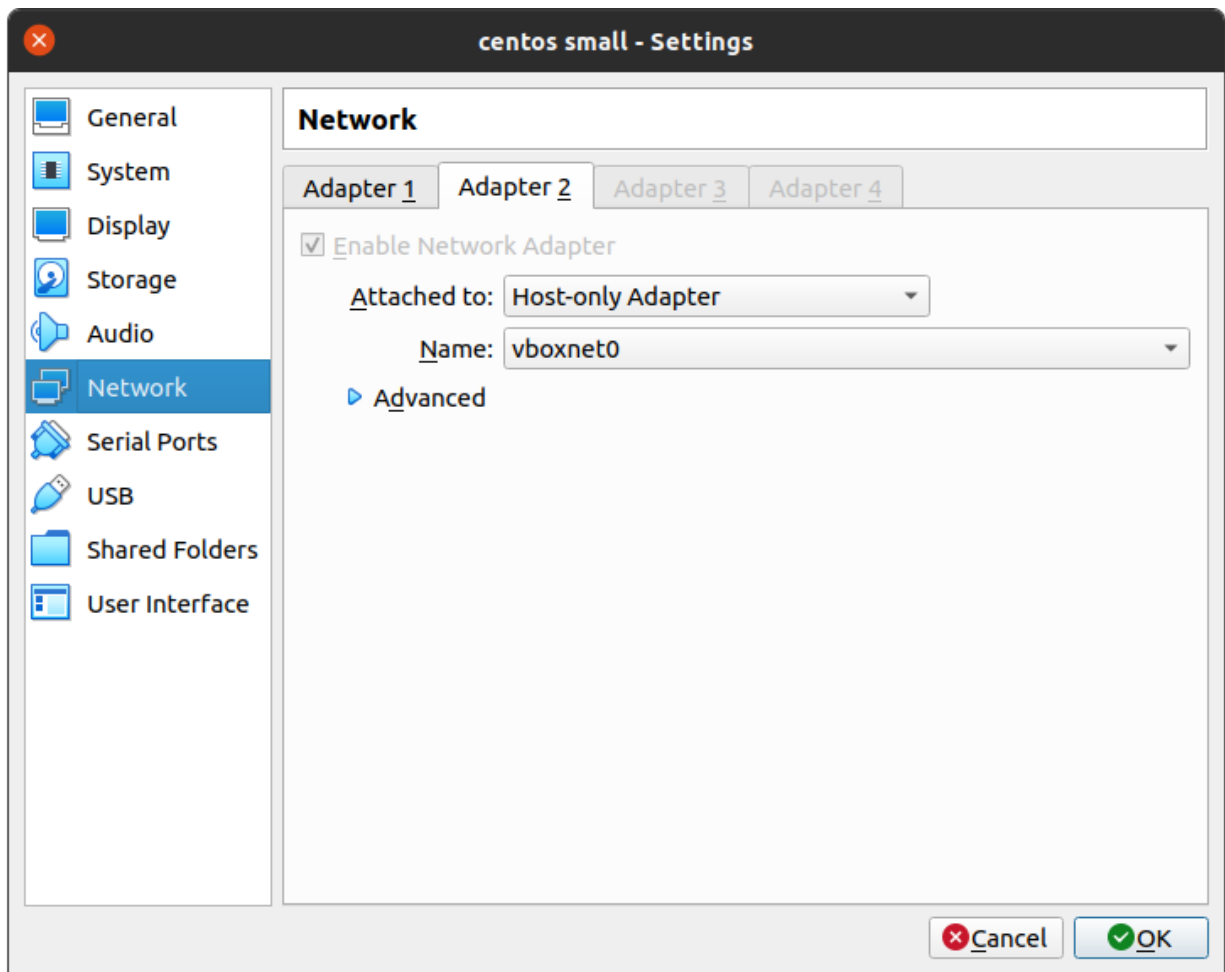
li. We created 2 cent os VMs, the first one with two network adapters, **bridged and host-only** network adapters. The second VM only had **a host-only** network adapter.

In VM 1 :

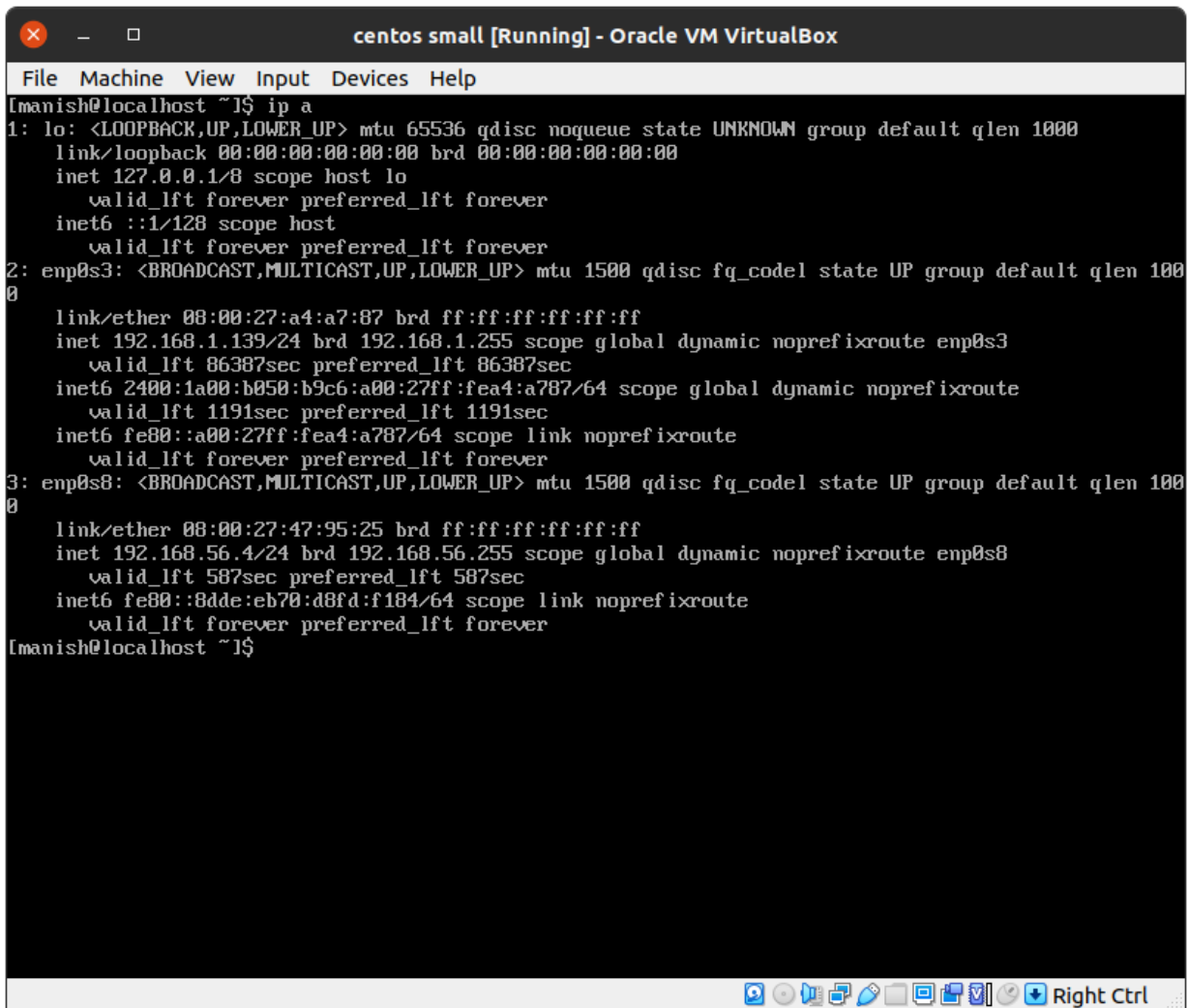
Bridged Adapter= **enp0s3**

Host only adapter= **enp0s8**





- The bridged adapter(**enp0s3**) acts as a WAN as it shares the network with the host machine.
- The host-only adapter(**enp0s8**) acts as a LAN. It is given a static IP address. Through this adapter, VM 2 can access the other network interface in VM 1.



```
centos small [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
lmanish@localhost ~1$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:a4:a7:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.129/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
        valid_lft 86387sec preferred_lft 86387sec
    inet6 2400:1a00:b050:b9c6:a00:27ff:fea4:a787/64 scope global dynamic noprefixroute
        valid_lft 1191sec preferred_lft 1191sec
    inet6 fe80::a00:27ff:fea4:a787/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:47:95:25 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.4/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s8
        valid_lft 587sec preferred_lft 587sec
    inet6 fe80::8dde:eb70:d8fd:f184/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
lmanish@localhost ~1$
```

The enp0s8

The enp0s8 interface was brought up with :

ifup enp0s8

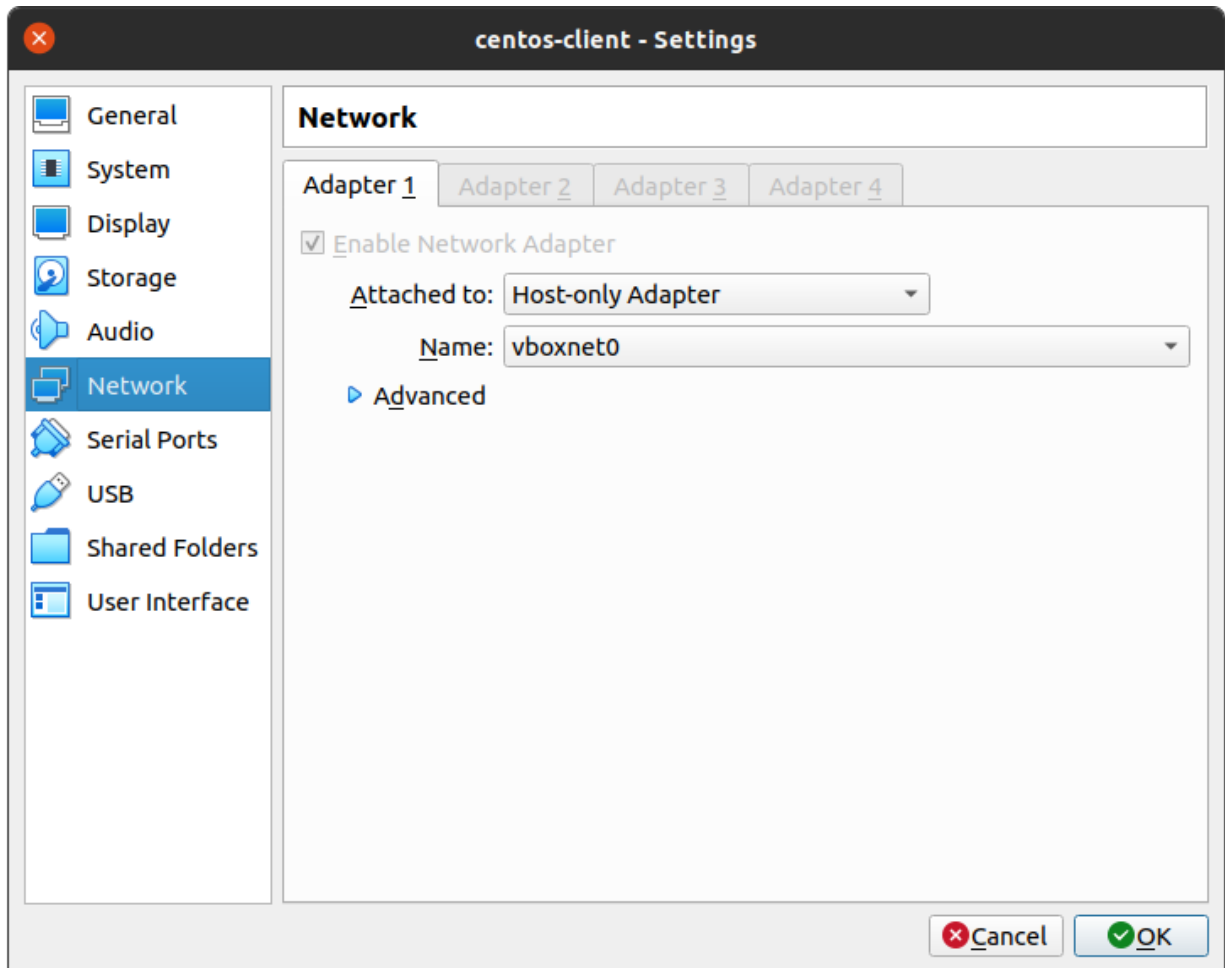
Ip addresses of the interfaces in VM 1 are :

Enp0s3: **192.168.1.129**

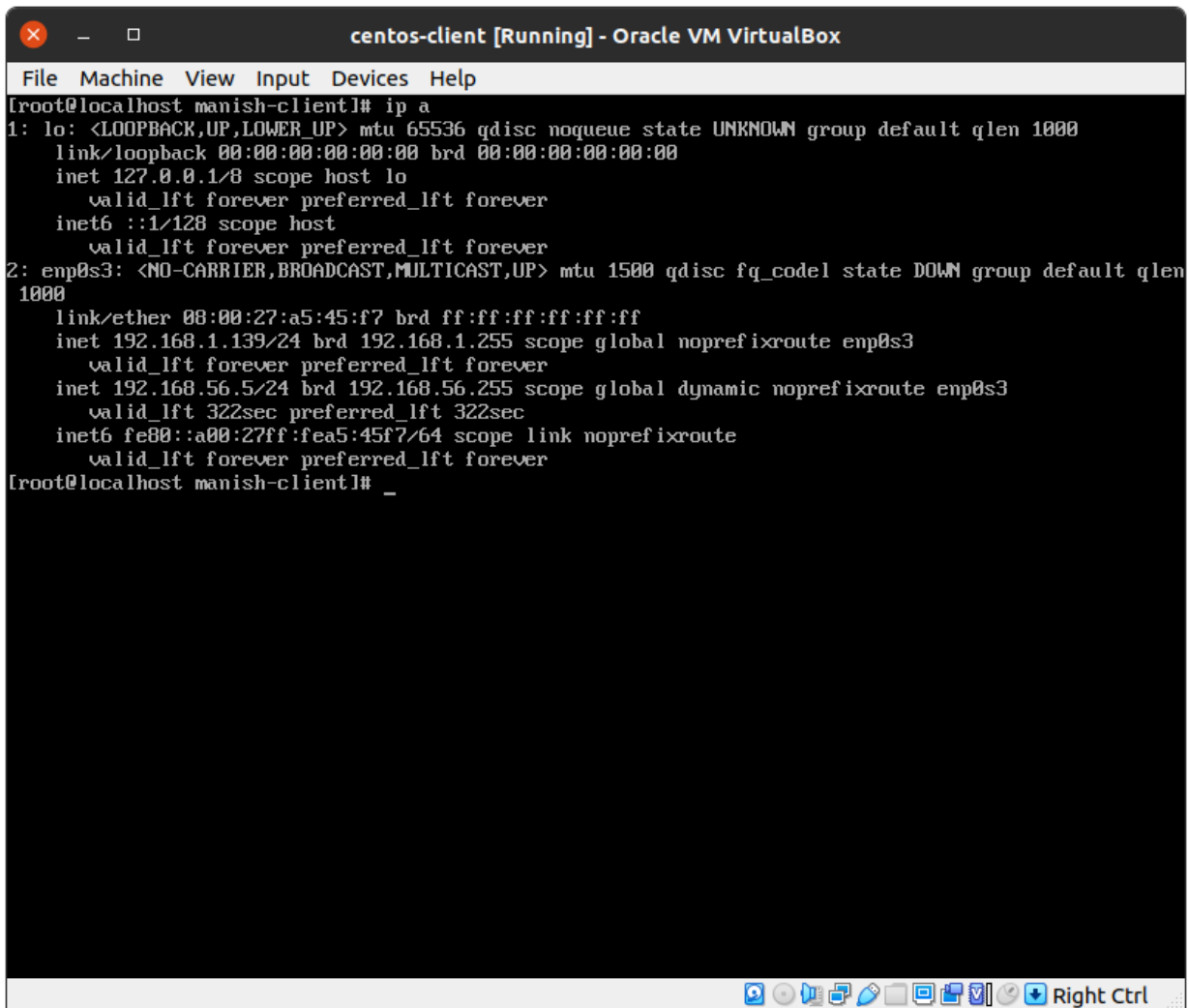
Enp0s8: **192.168.56.4**

In VM 2:

There is only one host only network adapter.



Host only adapter= **enp0s3**

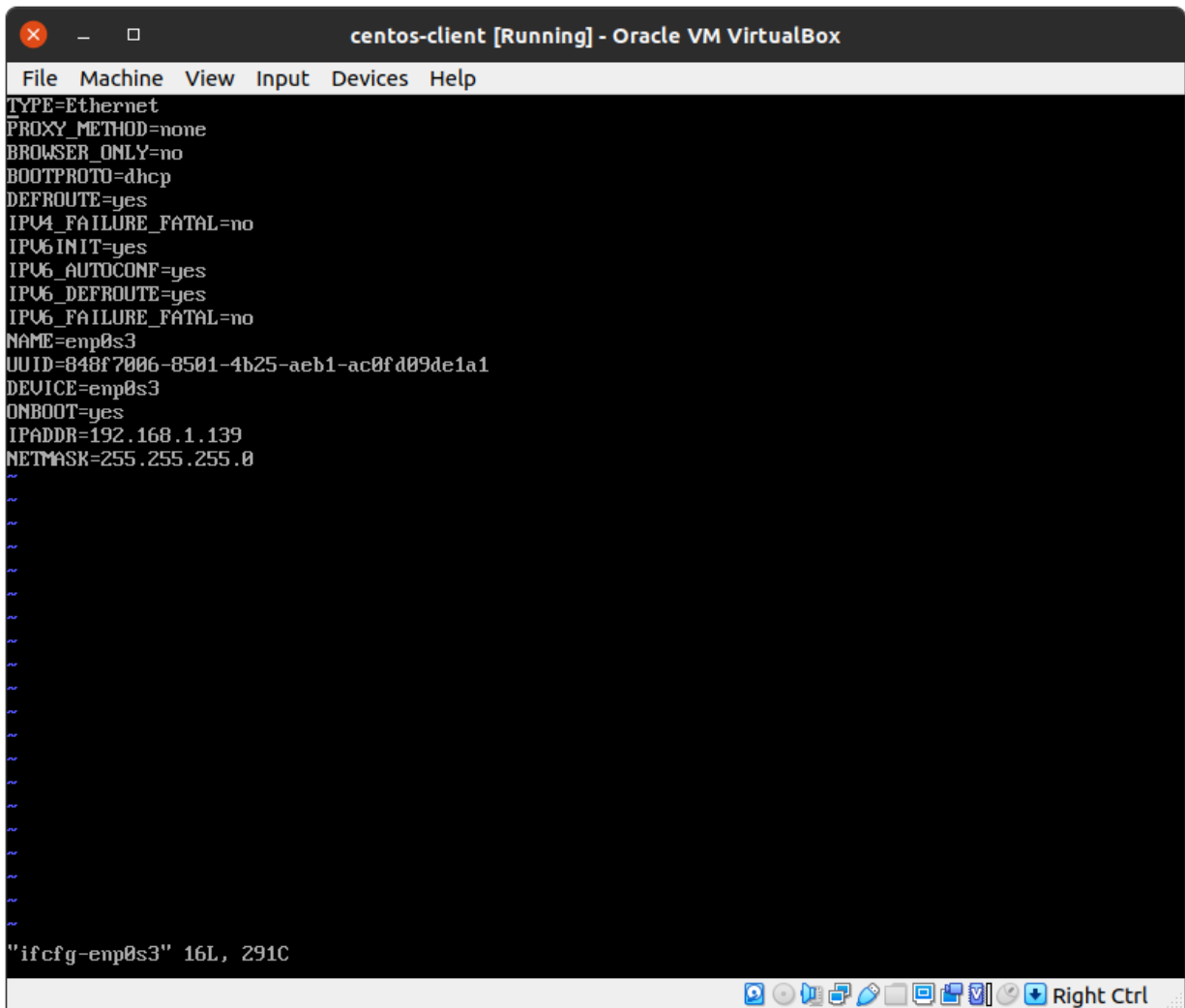


```
centos-client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[root@localhost manish-client1]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen
1000
    link/ether 08:00:27:a5:45:f7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.139/24 brd 192.168.1.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet 192.168.56.5/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s3
        valid_lft 322sec preferred_lft 322sec
    inet6 fe80::a00:27ff:fea5:45f7/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@localhost manish-client1]# _
```

- VM1;s bridged adapter's (**enp0s3**) IP address is added in the routing table with ifconfig.

ifconfig enp0s3 192.168.1.139 netmaask 255.255.255.0

I had an errorwhile adding with ifconfig so , I added static IP address by editing the **/etc/sysconfig/network-scripts/ifcfg-enp0s3** file.

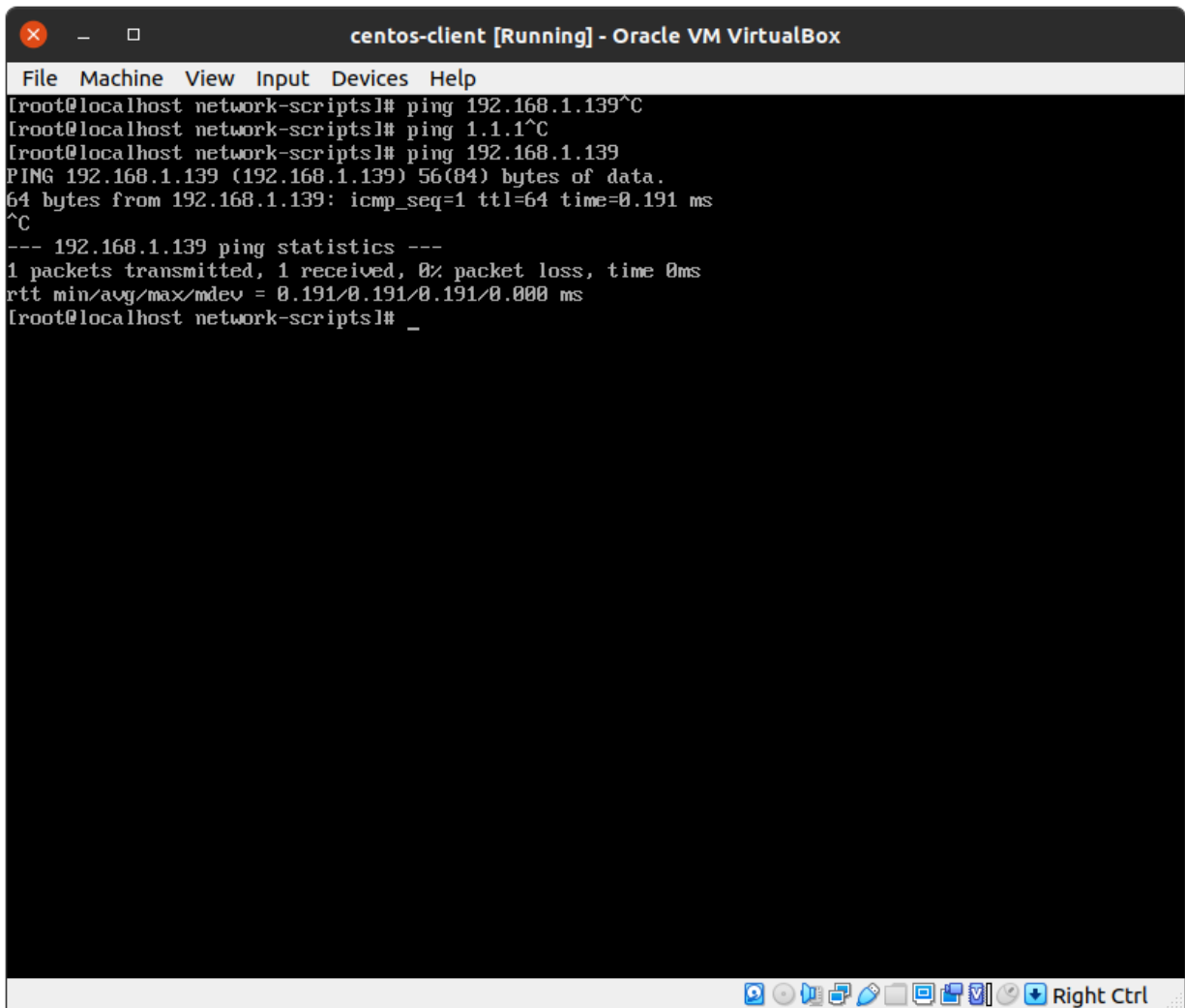


net-tools package was installed in the both VM before starting these processes.

iii. Now we can ping the second VM from the first and vice versa using their ip addresses.

Pinging the VM1 from VM2 with
ping 192.168.1.139

192.168.1.129 is the ip address of bridged network adapter of VM1



```
centos-client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[root@localhost network-scripts]# ping 192.168.1.139^C
[root@localhost network-scripts]# ping 1.1.1.1^C
[root@localhost network-scripts]# ping 192.168.1.139
PING 192.168.1.139 (192.168.1.139) 56(84) bytes of data.
64 bytes from 192.168.1.139: icmp_seq=1 ttl=64 time=0.191 ms
^C
--- 192.168.1.139 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.191/0.191/0.191/0.000 ms
[root@localhost network-scripts]# _
```

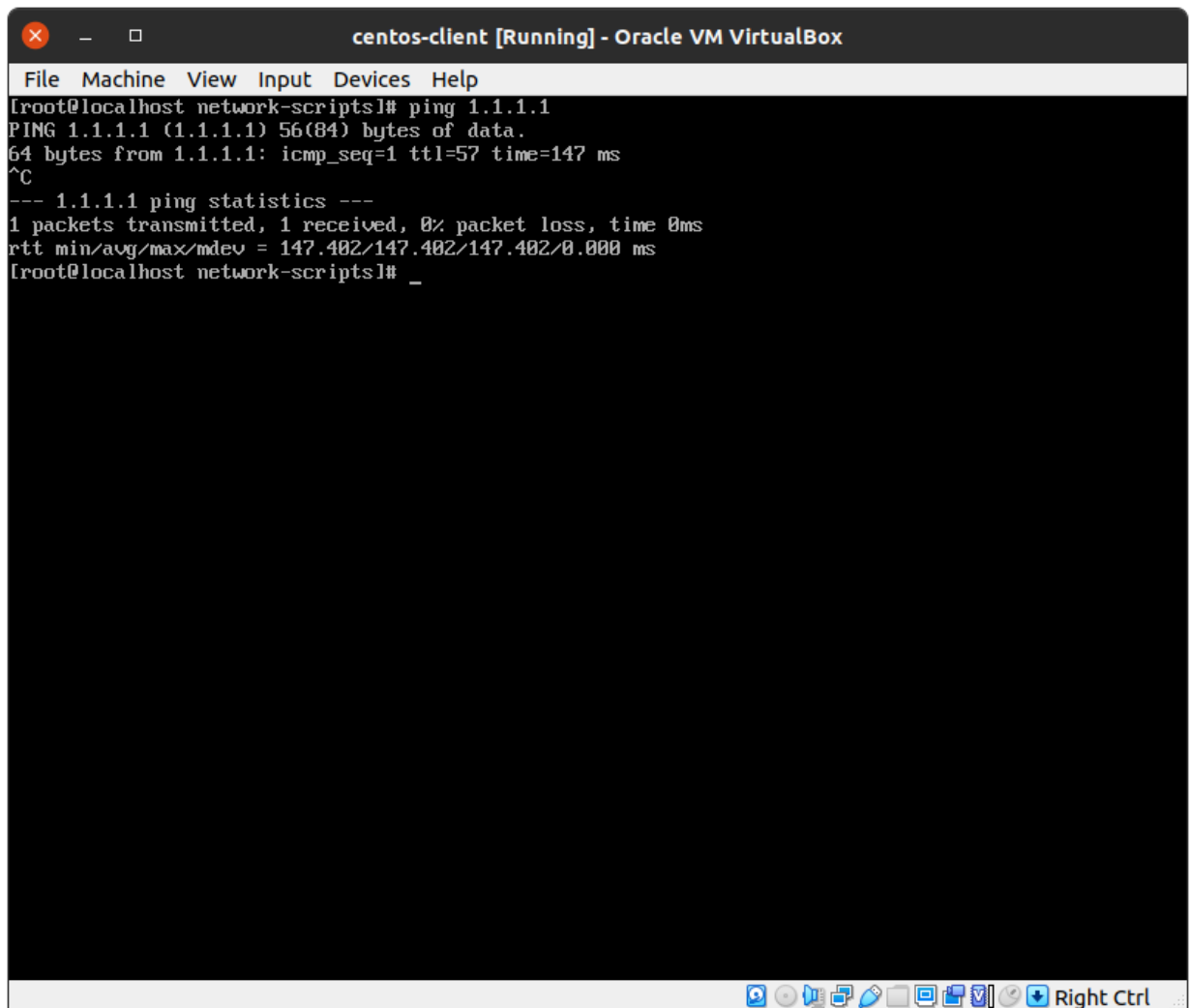
VM1 was successfully pinged from VM2 and vice versa.

iv. Finally, tables rules are added for forwarding and masquerading the requests from VM2 to the internet.

```
# modprobe iptable_nat
# echo 1 > /proc/sys/net/ipv4/ip_forward
# iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
# iptables -A FORWARD -i enp0s8 -j ACCEPT
```

v. Testing ping on IP address of Cloudflare (1.1.1.1) from VM2

ping 1.1.1.1



The screenshot shows a terminal window titled "centos-client [Running] - Oracle VM VirtualBox". The terminal output displays the results of a ping command to 1.1.1.1. The output includes the command executed, the data received, and the statistics for the ping test.

```
File Machine View Input Devices Help
[root@localhost network-scripts]# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data:
64 bytes from 1.1.1.1: icmp_seq=1 ttl=57 time=147 ms
^C
--- 1.1.1.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 147.402/147.402/147.402/0.000 ms
[root@localhost network-scripts]# _
```