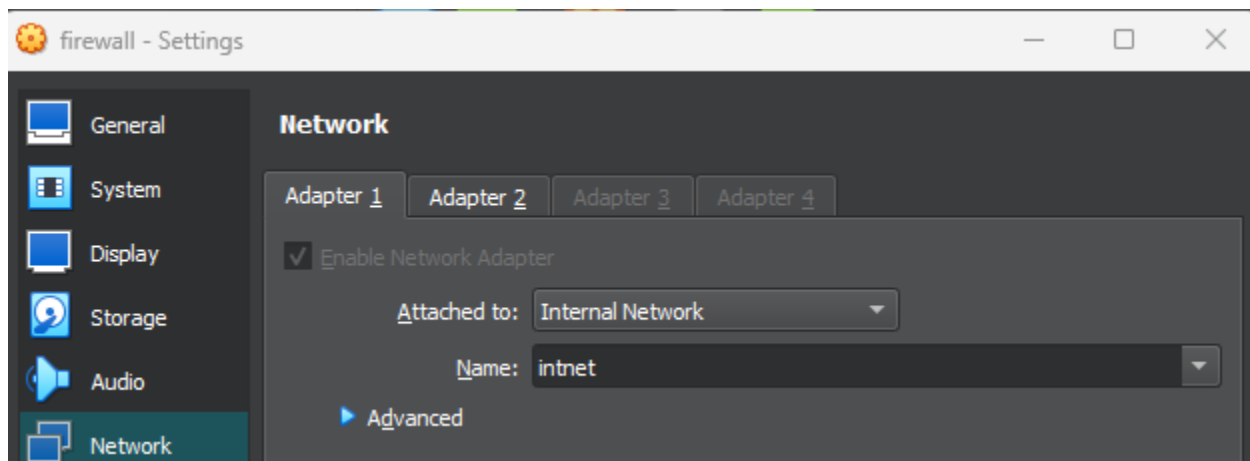


Module:- NDC
(IP_Tables-Masquerade and LoadBalancing)
Name:- Prithviraj Nikam

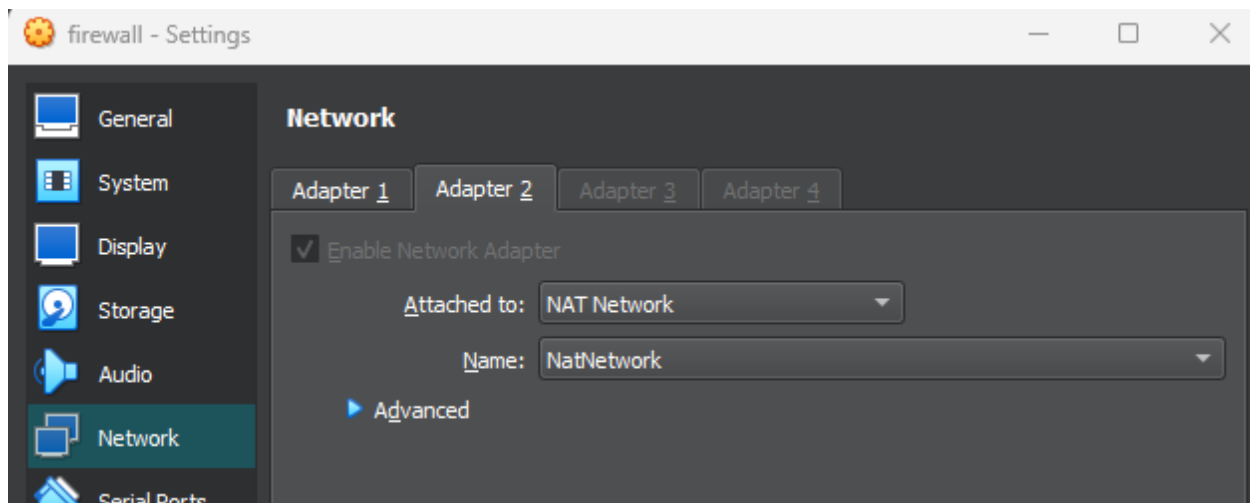
MASQUERADE

FIREWALL Side

Step-1:-Create Firewall Machine and set the Internal Network on Adapter-1



Step-2:-Set the NAT Network on Adapter-2



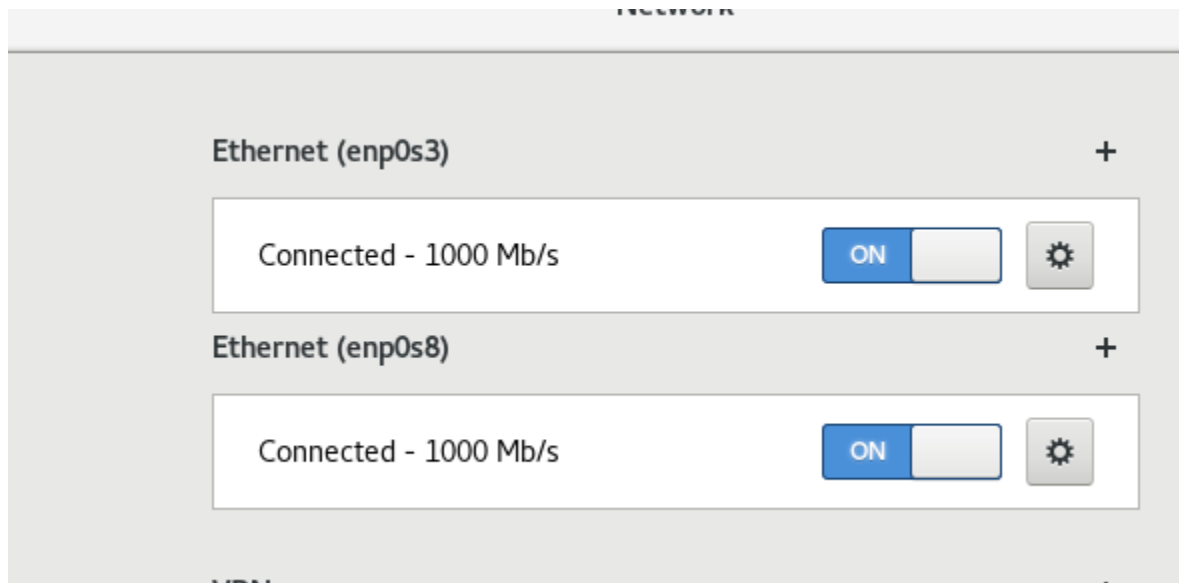
Step- 3:-Open the Firewall machine and Install the net tools
#dnf install net-tools

```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# dnf install net-tools  
Last metadata expiration check: 3:56:27 ago on Friday 23 December 2022 01:15:06 PM IST.  
Package net-tools-2.0-9-53.20160812.el9.x86_64 is already installed
```

Step - 4:-check ip of Firewall machine

```
Activities Terminal Dec 23 16:35  
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# ifconfig  
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255  
    inet6 fe80::a00:27ff:fe7e:39e2 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:7e:39:e2 txqueuelen 1000 (Ethernet)  
    RX packets 56818 bytes 85318313 (81.3 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 20330 bytes 1266717 (1.2 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.0.2.7 netmask 255.255.255.0 broadcast 10.0.2.255  
    inet6 fe80::2a14:d98e:1bf:65d1 prefixlen 64 scopeid 0x20<link>
```

Step-5:- Go to network Setting and set ip



Go to Ethernet (enp0s3) and Set IP Manually Because in my system Ethernet (enp0s3) work as Internal Network

The image shows a 'Wired' network settings window. At the top are 'Cancel' and 'Apply' buttons. Below is a tab bar with 'Details', 'Identity', 'IPv4' (selected), 'IPv6', and 'Security'. Under the 'IPv4' tab, the 'IPv4 Method' section has four radio buttons: 'Automatic (DHCP)', 'Link-Local Only', 'Manual' (which is selected), and 'Disable'. Below this is the 'Addresses' section with a table. The table has three columns: 'Address', 'Netmask', and 'Gateway'. The first row contains the values '192.168.0.2', '255.255.0.0', and an empty field with a close button (X).

Address	Netmask	Gateway
192.168.0.2	255.255.0.0	

Go to Ethernet (enp0s8) and Set IP Automatic(DHCP) Because in my system Ethernet (enp0s3) work as NAT Network

The image shows the same 'Wired' network settings window, but with 'Automatic (DHCP)' selected under 'IPv4 Method'. Below the method selection is the 'DNS' section, which includes a label 'DNS', the text 'Automatic', and a toggle switch currently set to 'ON'. Below the toggle is an empty text input field. At the bottom, there is a small note: 'Separate IP addresses with commas'.

Then go to Terminal check the ip

```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# ifconfig  
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.0.2 netmask 255.255.0.0 broadcast 192.168.255.255  
    inet6 fe80::a00:27ff:fe7e:39e2 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:7e:39:e2 txqueuelen 1000 (Ethernet)  
    RX packets 56939 bytes 85341012 (81.3 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 20823 bytes 1339662 (1.2 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.0.2.7 netmask 255.255.255.0 broadcast 10.0.2.255  
    inet6 fe80::2a14:d98e:1bf:65d1 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:70:67:5c txqueuelen 1000 (Ethernet)
```

[OR]

You Can set IP through Command Line

#ifconfig enp0s3 down

#ifconfig enp0s3 192.168.0.2

#ifconfig enp0s8 down

#ifconfig enp0s8 10.0.2.7

Step -6:- Now Add rule in ip tables

#iptables -S -t nat

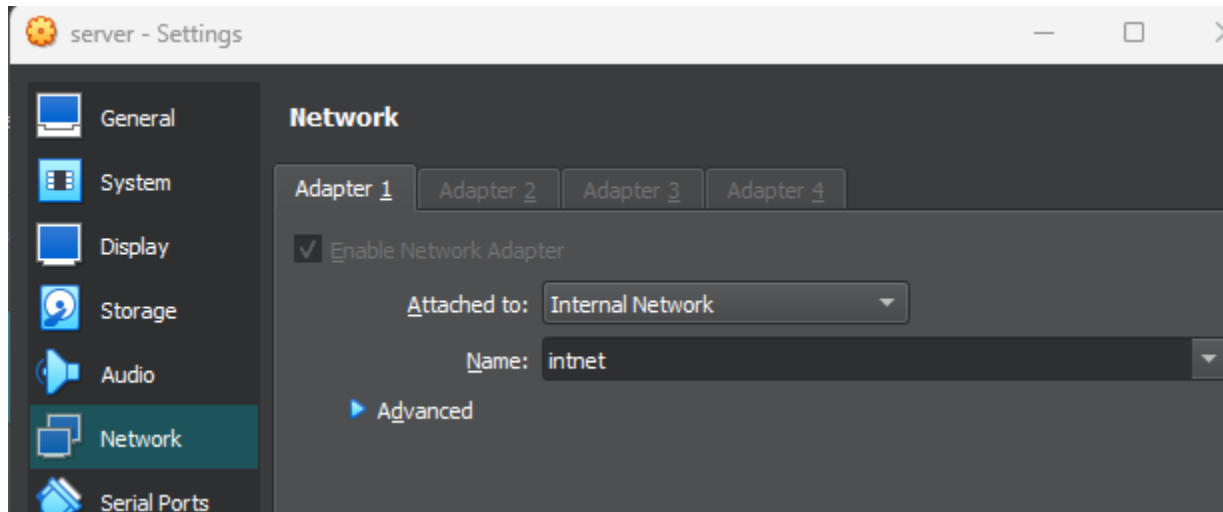
#iptables -A POSTROUTING -t nat -s 10.0.0.0/24 -d 192.168.0.0/24 -j

MASQUERADE

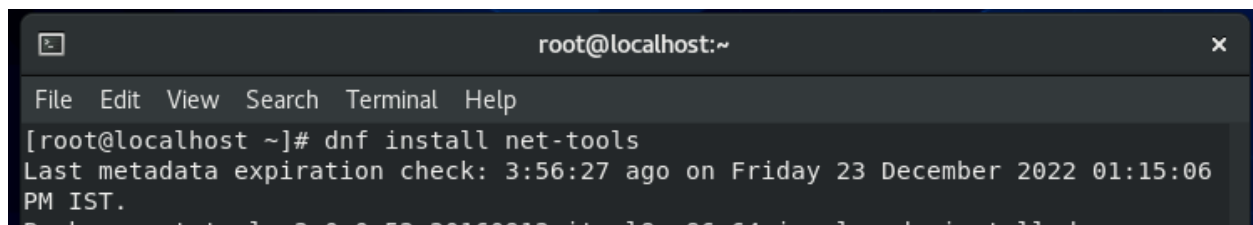
```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# iptables -S -t nat  
-P PREROUTING ACCEPT  
-P INPUT ACCEPT  
-P POSTROUTING ACCEPT  
-P OUTPUT ACCEPT  
-N LIBVIRT_PRT  
[root@localhost ~]# iptables -A POSTROUTING -t nat -s 10.0.0.0/24 -d 192.168.0.0/24 -j  
MASQUERADE  
[root@localhost ~]# iptables -S -t nat  
-P PREROUTING ACCEPT  
-P INPUT ACCEPT  
-P POSTROUTING ACCEPT  
-P OUTPUT ACCEPT  
-N LIBVIRT_PRT  
-A POSTROUTING -s 10.0.0.0/24 -d 192.168.0.0/24 -j MASQUERADE  
[root@localhost ~]#
```

Server Side

Step-1:-Create Server Machine and set the Internal network on Adapter-1



Step-2:- Open the server machine and Install the net tools #dnf install net-tools



Step-3:-Go to Ethernet (enp0s3) and Set IP Manually Because in my system Ethernet (enp0s3) work as Internal Network

Cancel Wired Apply

Details Identity **IPv4** IPv6 Security

IPv4 Method

☐ Automatic (DHCP)
 ☐ Link-Local Only
 ☒ Manual
 ☐ Disable

Addresses

Address	Netmask	Gateway
192.168.0.1	255.255.255.0	

```

[server:running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Dec 23 17:01
root@localhost:~
File Edit View Search Terminal Help
[root@localhost ~]# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.1 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::a00:27ff:fe2b:c0a3 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:2b:c0:a3 txqueuelen 1000 (Ethernet)
    RX packets 61342 bytes 91888568 (87.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24292 bytes 1510295 (1.4 MiB)
  
```

[OR]

You Can set IP through Command Line

#ifconfig enp0s3 down

#ifconfig enp0s3 192.168.0.1

Step-4:- Now add the gateway

#route add -net default gw 10.0.2.7

#netstat -rn

#route del -net default gw 10.0.2.1



root@localhost:~

File Edit View Search Terminal Help

```
[root@localhost ~]# route add -net default gw 192.168.0.2
```

```
[root@localhost ~]# netstat -rn
```

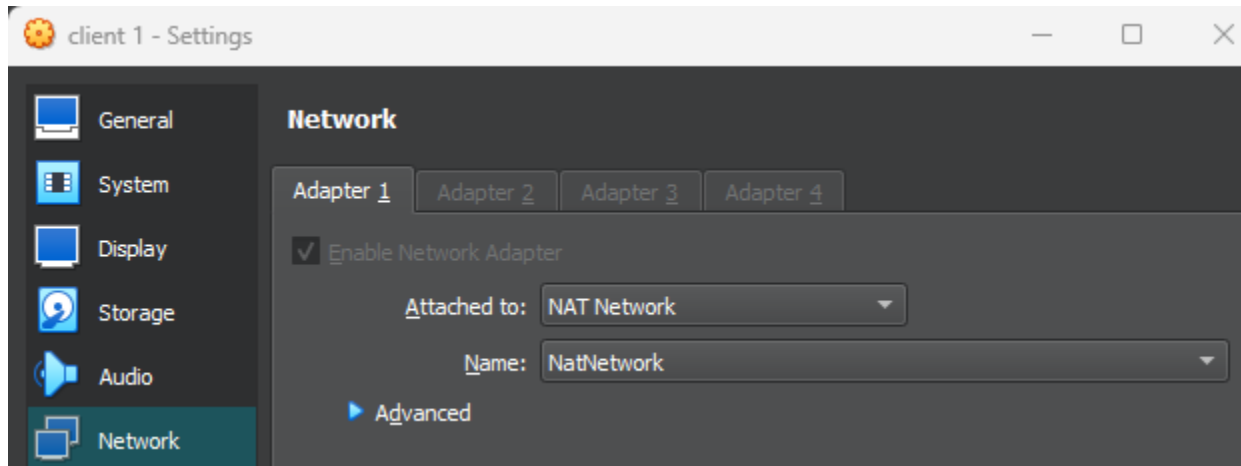
Kernel IP routing table

Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
0.0.0.0	192.168.0.2	0.0.0.0	UG	0	0	0	enp0s3
192.168.0.0	0.0.0.0	255.255.255.0	U	0	0	0	enp0s3
192.168.122.0	0.0.0.0	255.255.255.0	U	0	0	0	virbr0

```
[root@localhost ~]#
```


Client -1 Side

Step-1:- Create Client Machine and set the NAT Network on Adapter-1



Step- 2:- Open the Client-1 machine and Install the net tools

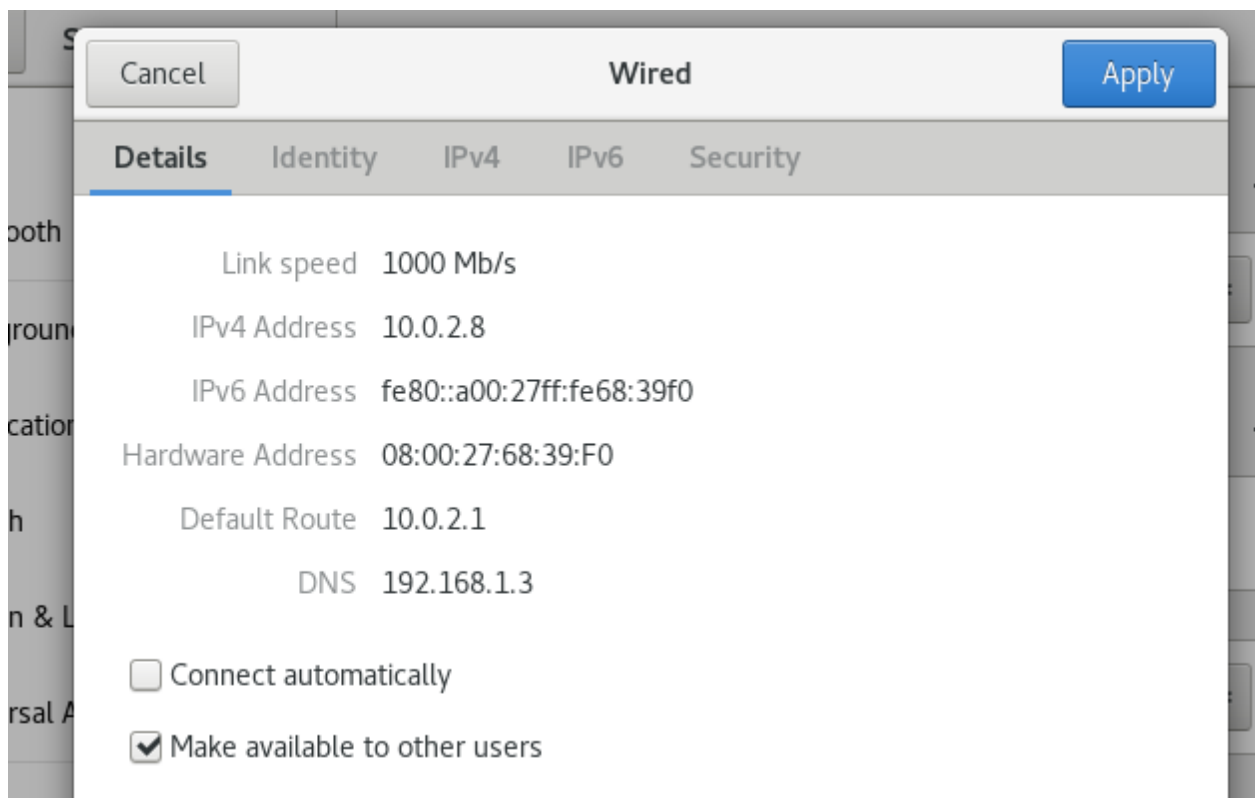
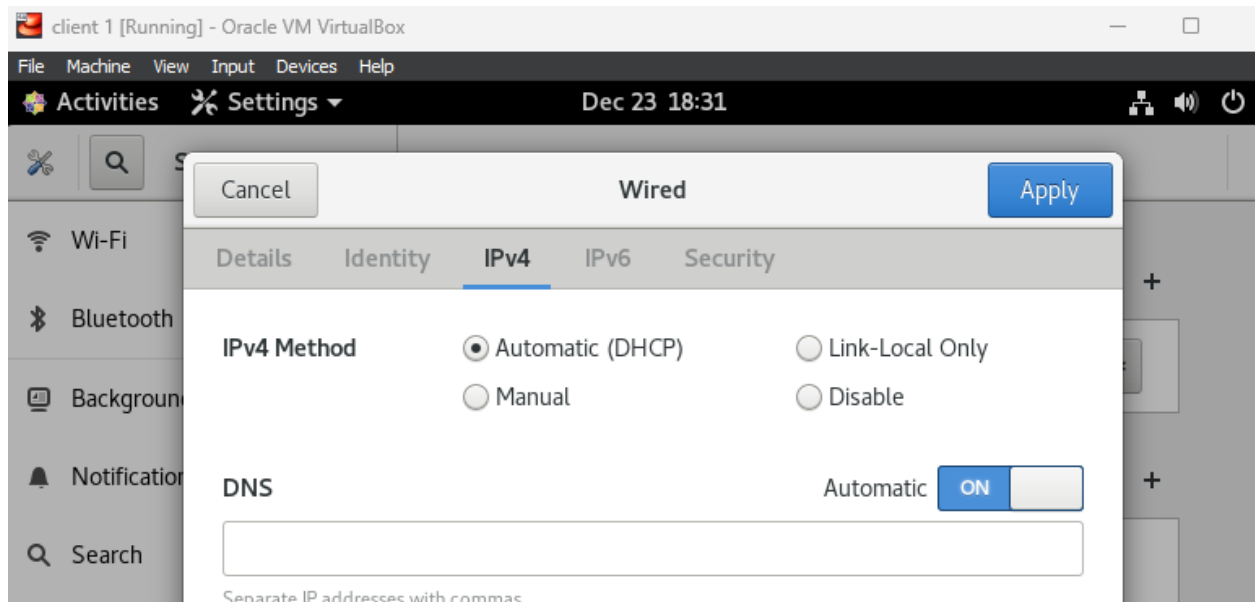
#dnf install net-tools

```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# dnf install net-tools  
Last metadata expiration check: 3:56:27 ago on Friday 23 December 2022 01:15:06 PM IST.  
Package net-tools-2.0-0-53-20160812.el8.x86_64 is already installed
```

Step-3:-check ip of client -1 machine

```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# ifconfig  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 40 bytes 3404 (3.3 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0
```

Step- 4:- Go to network Setting Ethernet (enp0s8) and set ip is Automatic(DHCP)



[OR]

You Can set IP through Command Line

#ifconfig enp0s3 down

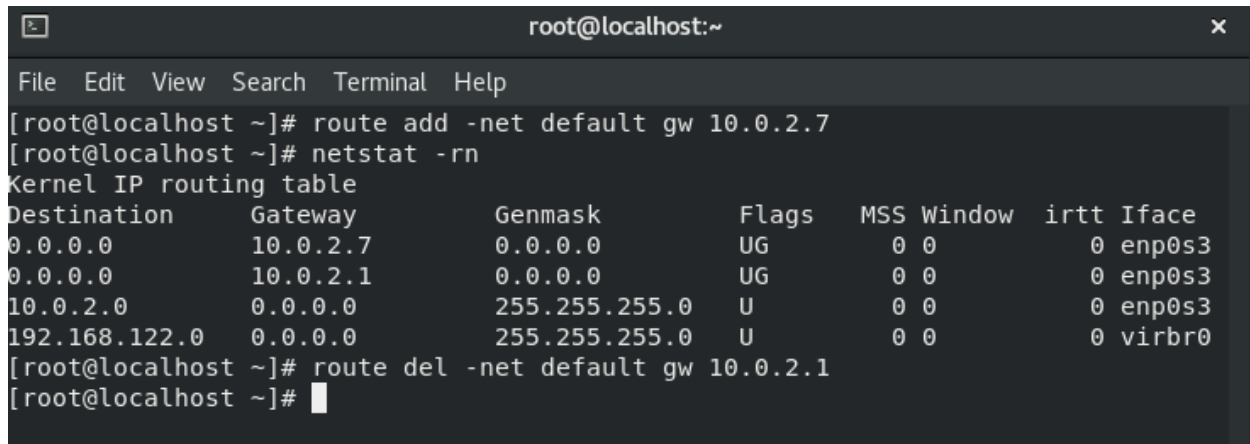
#ifconfig enp0s3 10.0.2.8

Step-5:- Now add the gateway

#route add -net default gw 10.0.2.7

#netstat -rn

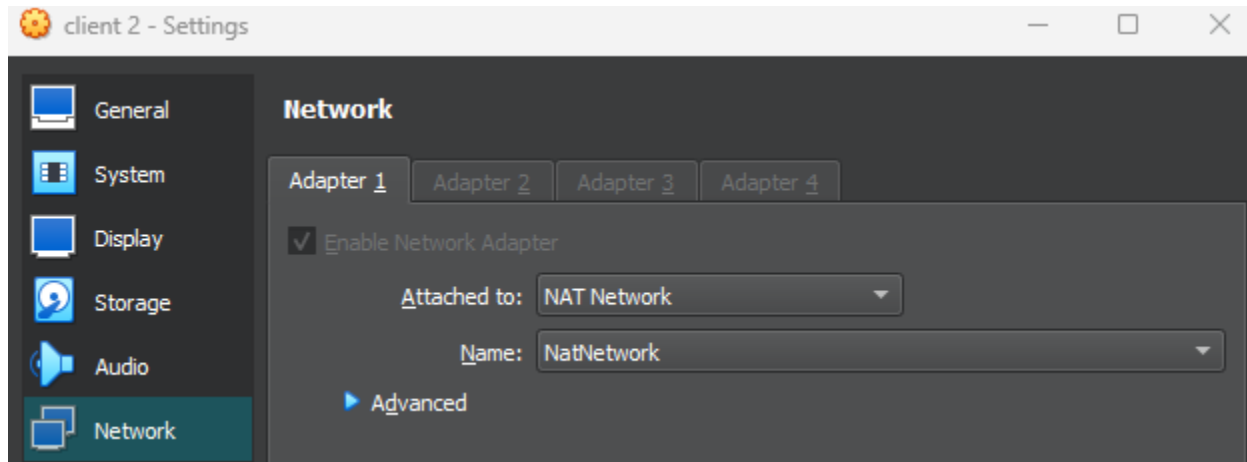
#route del -net default gw 10.0.2.1



```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# route add -net default gw 10.0.2.7  
[root@localhost ~]# netstat -rn  
Kernel IP routing table  
Destination      Gateway          Genmask          Flags      MSS Window  irtt Iface  
0.0.0.0          10.0.2.7         0.0.0.0          UG          0 0        0 enp0s3  
0.0.0.0          10.0.2.1         0.0.0.0          UG          0 0        0 enp0s3  
10.0.2.0         0.0.0.0          255.255.255.0    U           0 0        0 enp0s3  
192.168.122.0    0.0.0.0          255.255.255.0    U           0 0        0 virbr0  
[root@localhost ~]# route del -net default gw 10.0.2.1  
[root@localhost ~]#
```

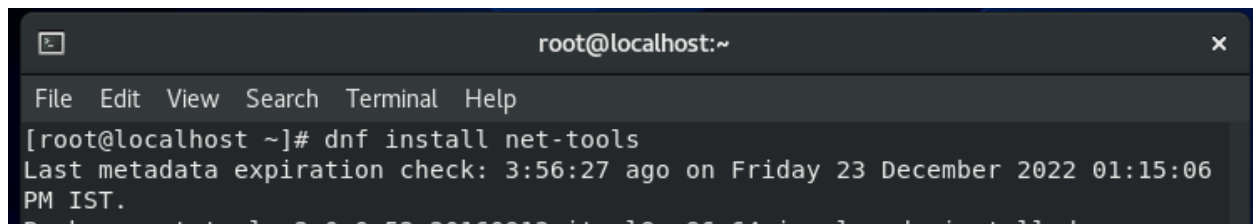
Client -2 Side

Step-1:- Create Client Machine and set the NAT Network on Adapter-1

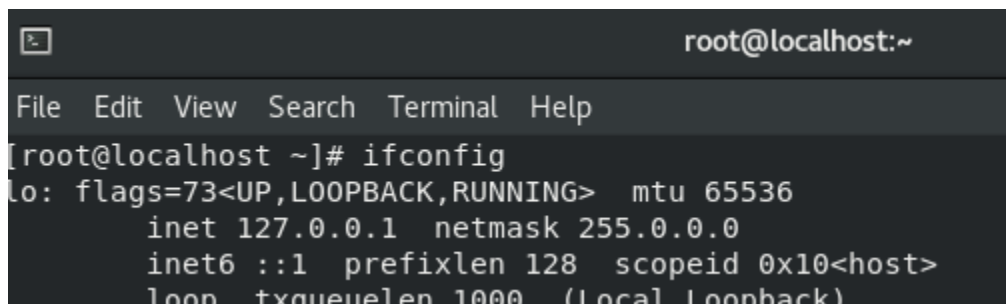


Step- 2:- Open the Client-2 machine and Install the net tools

#dnf install net-tools



Step-3:-check ip of client -2 machine



Step- 4:- Go to network Setting Ethernet (enp0s8) and set ip is Automatic(DHCP)

Cancel **Wired** Apply

Details Identity **IPv4** IPv6 Security

IPv4 Method

☒ Automatic (DHCP) ☐ Link-Local Only

☐ Manual ☐ Disable

DNS Automatic **ON**

Cancel **Wired** Apply

Details Identity IPv4 IPv6 Security

Link speed 1000 Mb/s

IPv4 Address 10.0.2.9

IPv6 Address fe80::a00:27ff:fe7e:26eb

Hardware Address 08:00:27:7E:26:EB

Default Route 10.0.2.1

```
root@localhost:~  
File Edit View Search Terminal Help  
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 10.0.2.9 netmask 255.255.255.0 broadcast 10.0.2.255  
inet6 fe80::a00:27ff:fe7e:26eb prefixlen 64 scopeid 0x20<link>  
ether 08:00:27:7e:26:eb txqueuelen 1000 (Ethernet)  
RX packets 81074 bytes 119930972 (114.3 MiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 33209 bytes 2178009 (2.0 MiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

[OR]

You Can set IP through Command Line

#ifconfig enp0s3 down

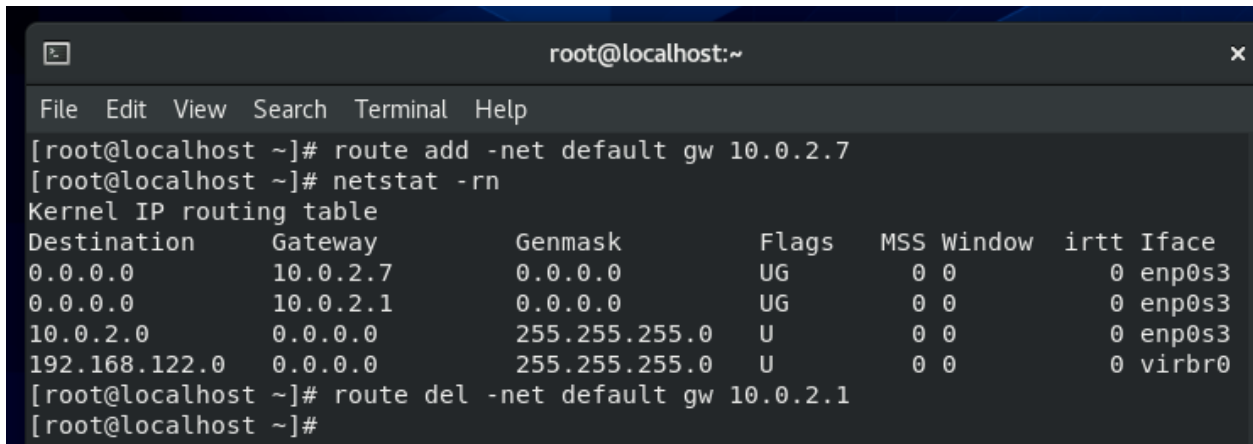
#ifconfig enp0s3 10.0.2.9

Step-5:- Now add the gateway

#route add -net default gw 10.0.2.7

#netstat -rn

#route del -net default gw 10.0.2.1



```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# route add -net default gw 10.0.2.7  
[root@localhost ~]# netstat -rn  
Kernel IP routing table  
Destination      Gateway          Genmask          Flags      MSS Window  irtt Iface  
0.0.0.0          10.0.2.7        0.0.0.0          UG          0 0       0 enp0s3  
0.0.0.0          10.0.2.1        0.0.0.0          UG          0 0       0 enp0s3  
10.0.2.0         0.0.0.0         255.255.255.0    U           0 0       0 enp0s3  
192.168.122.0    0.0.0.0         255.255.255.0    U           0 0       0 virbr0  
[root@localhost ~]# route del -net default gw 10.0.2.1  
[root@localhost ~]#
```

CHECK the Masquerade Client to server

NOW Go to Client-1 and ping the server

```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# ping 192.168.0.1  
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.  
64 bytes from 192.168.0.1: icmp_seq=1 ttl=63 time=2.78 ms  
64 bytes from 192.168.0.1: icmp_seq=2 ttl=63 time=1.45 ms  
64 bytes from 192.168.0.1: icmp_seq=3 ttl=63 time=1.53 ms  
64 bytes from 192.168.0.1: icmp_seq=4 ttl=63 time=1.96 ms  
64 bytes from 192.168.0.1: icmp_seq=5 ttl=63 time=1.41 ms  
64 bytes from 192.168.0.1: icmp_seq=6 ttl=63 time=1.54 ms  
^C  
--- 192.168.0.1 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5020ms  
rtt min/avg/max/mdev = 1.405/1.775/2.775/0.483 ms  
[root@localhost ~]#
```

Go to Client -2 and Ping the server

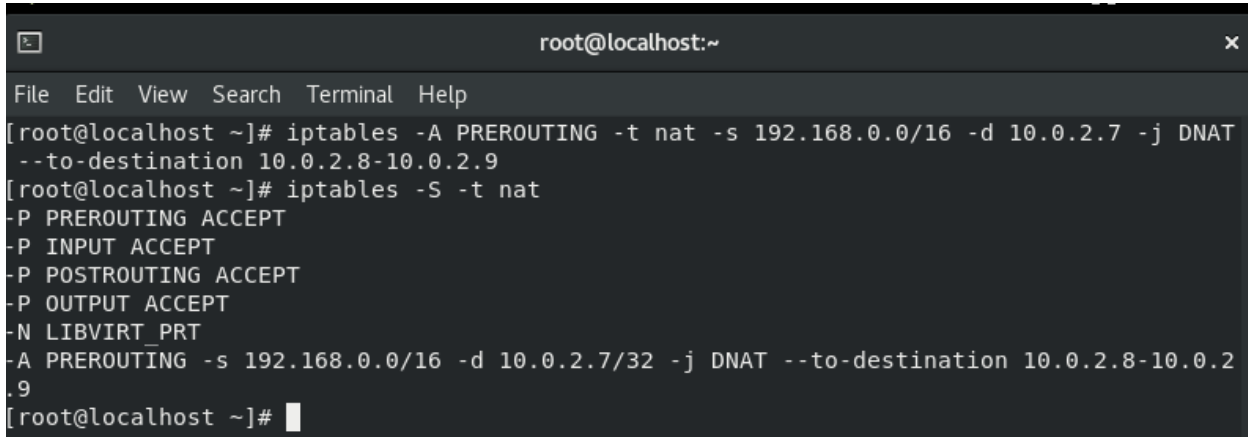
```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# ping 192.168.0.1  
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.  
64 bytes from 192.168.0.1: icmp_seq=1 ttl=63 time=2.44 ms  
64 bytes from 192.168.0.1: icmp_seq=2 ttl=63 time=1.51 ms  
64 bytes from 192.168.0.1: icmp_seq=3 ttl=63 time=1.39 ms  
64 bytes from 192.168.0.1: icmp_seq=4 ttl=63 time=1.47 ms  
64 bytes from 192.168.0.1: icmp_seq=5 ttl=63 time=1.47 ms  
^C  
--- 192.168.0.1 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4043ms  
rtt min/avg/max/mdev = 1.390/1.654/2.435/0.395 ms  
[root@localhost ~]#
```

LOAD BALANCING

FIREWALL Side:-

Step -1:- Open the firewall Machine add the rule in ip tables

```
# iptables -A PREROUTING -t nat -s 192.168.0.0/16 -d 10.0.2.7 -j DNAT  
--to-destination 10.0.2.8-10.0.2.9  
# iptables -S -t nat
```

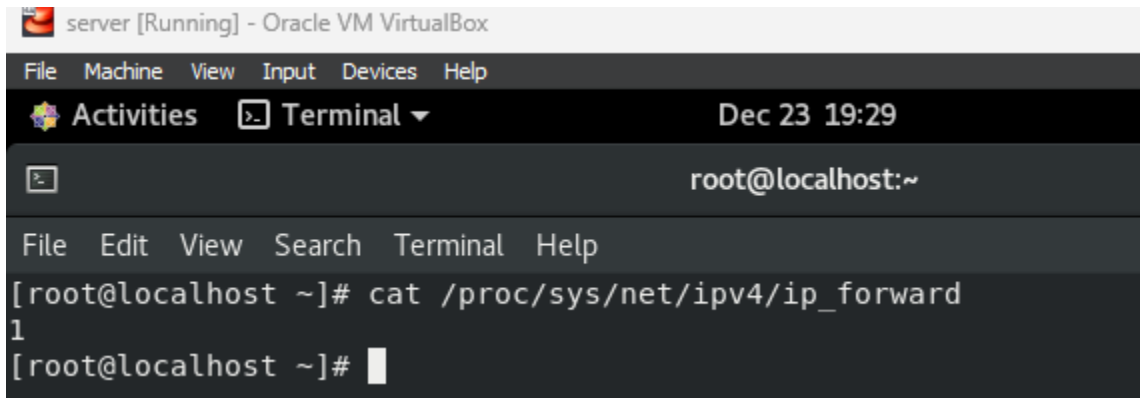
A terminal window titled 'root@localhost:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the execution of two iptables commands. The first command adds a rule to the PREROUTING chain of the nat table, matching source IP 192.168.0.0/16 and destination IP 10.0.2.7, and performing a DNAT to the destination range 10.0.2.8-10.0.2.9. The second command lists the rules for the nat table. The output shows the rule being added and the current state of the table, including the new rule and the existing rule for the same destination range.

```
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# iptables -A PREROUTING -t nat -s 192.168.0.0/16 -d 10.0.2.7 -j DNAT  
--to-destination 10.0.2.8-10.0.2.9  
[root@localhost ~]# iptables -S -t nat  
-P PREROUTING ACCEPT  
-P INPUT ACCEPT  
-P POSTROUTING ACCEPT  
-P OUTPUT ACCEPT  
-N LIBVIRT_PRT  
-A PREROUTING -s 192.168.0.0/16 -d 10.0.2.7/32 -j DNAT --to-destination 10.0.2.8-10.0.2.9  
[root@localhost ~]#
```

Check the ip Forward Status

```
cat /proc/sys/net/ipv4/ip_forward
```

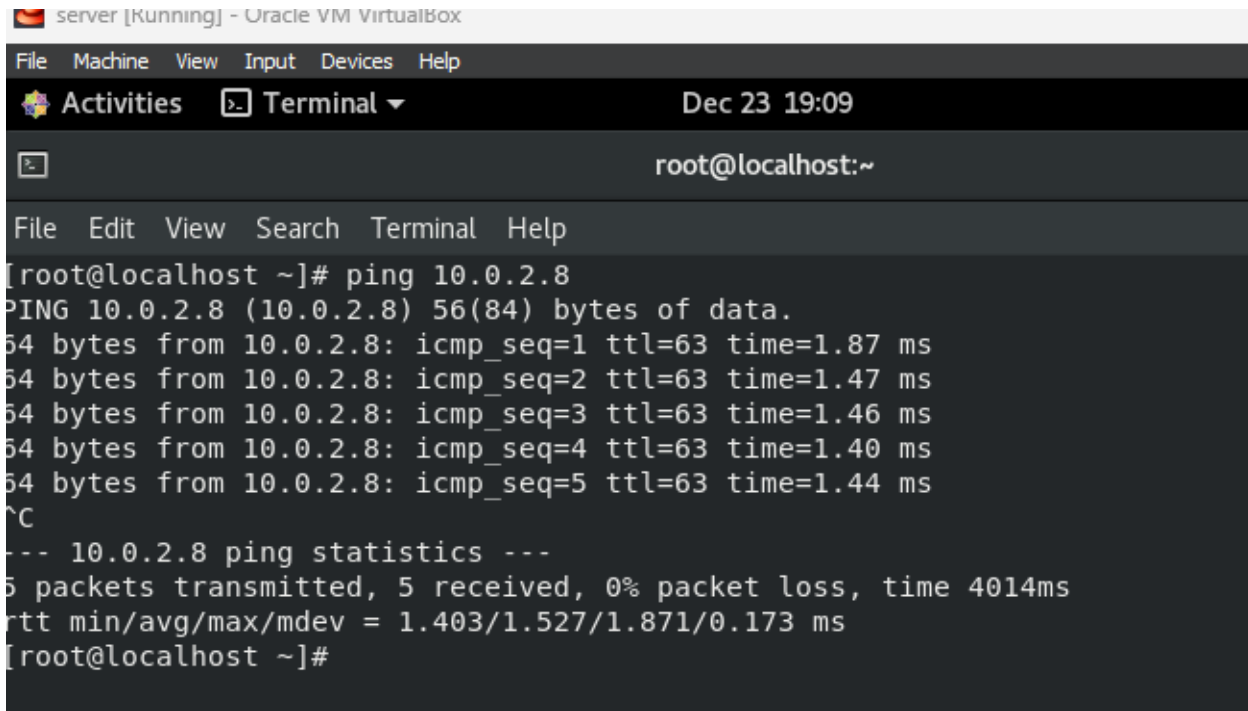
```
echo 1
```

A screenshot of a VirtualBox window titled 'server [Running] - Oracle VM VirtualBox'. It shows a terminal window with a menu bar (File, Machine, View, Input, Devices, Help) and a title bar (Activities, Terminal, Dec 23 19:29). The terminal shows the execution of two commands. The first command cat's the file /proc/sys/net/ipv4/ip_forward, which returns the value 1. The second command echoes 1.

```
server [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
Activities Terminal Dec 23 19:29  
root@localhost:~  
File Edit View Search Terminal Help  
[root@localhost ~]# cat /proc/sys/net/ipv4/ip_forward  
1  
[root@localhost ~]#
```


Server Side

Step-1:- Go to Server and ping the Client-1

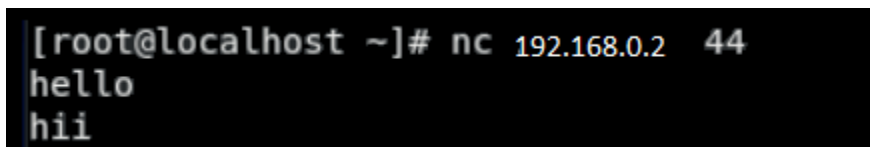


```
server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Dec 23 19:09
root@localhost:~
File Edit View Search Terminal Help
[root@localhost ~]# ping 10.0.2.8
PING 10.0.2.8 (10.0.2.8) 56(84) bytes of data.
64 bytes from 10.0.2.8: icmp_seq=1 ttl=63 time=1.87 ms
64 bytes from 10.0.2.8: icmp_seq=2 ttl=63 time=1.47 ms
64 bytes from 10.0.2.8: icmp_seq=3 ttl=63 time=1.46 ms
64 bytes from 10.0.2.8: icmp_seq=4 ttl=63 time=1.40 ms
64 bytes from 10.0.2.8: icmp_seq=5 ttl=63 time=1.44 ms
^C
--- 10.0.2.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4014ms
rtt min/avg/max/mdev = 1.403/1.527/1.871/0.173 ms
[root@localhost ~]#
```

Step-2:-Type Firewall IP & Port No

nc 192.168.0.2 44

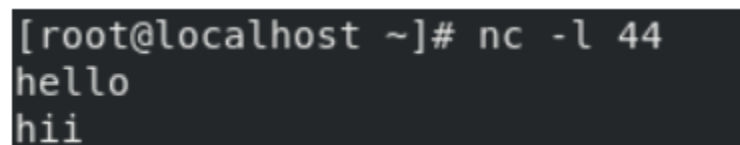
Firewall_ip port



```
[root@localhost ~]# nc 192.168.0.2 44
hello
hii
```

Go to Client Side check incoming Message

#nc -l 44



```
[root@localhost ~]# nc -l 44
hello
hii
```

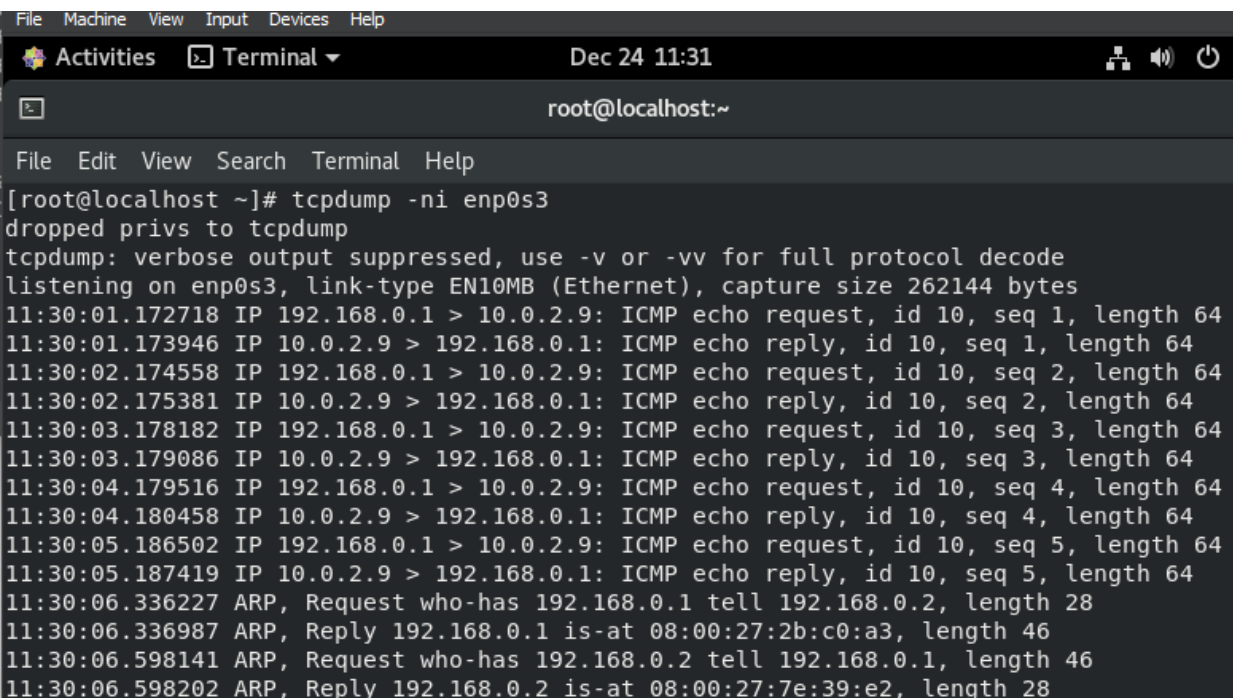
TCPDUMP

Step-1 :-Go to server Ping the Client-1 or client-2

```
[root@localhost ~]# ping 10.0.2.9
PING 10.0.2.9 (10.0.2.9) 56(84) bytes of data.
64 bytes from 10.0.2.9: icmp_seq=1 ttl=63 time=2.04 ms
64 bytes from 10.0.2.9: icmp_seq=2 ttl=63 time=1.59 ms
64 bytes from 10.0.2.9: icmp_seq=3 ttl=63 time=1.70 ms
64 bytes from 10.0.2.9: icmp_seq=4 ttl=63 time=1.72 ms
64 bytes from 10.0.2.9: icmp_seq=5 ttl=63 time=1.66 ms
^C
--- 10.0.2.9 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4014ms
rtt min/avg/max/mdev = 1.586/1.741/2.041/0.160 ms
[root@localhost ~]#
```

Step-2:- Go to Firewall

tcpdump -ni enp0s3

A screenshot of a Linux terminal window. The window title is "Terminal" and it shows the user is logged in as root at localhost. The terminal output shows the command "tcpdump -ni enp0s3" being executed. The output indicates that the capture is listening on the enp0s3 interface. It then shows a series of ICMP echo requests and replies between 192.168.0.1 and 10.0.2.9, as well as ARP requests and replies between 192.168.0.1 and 192.168.0.2.

```
File Machine View Input Devices Help
Activities Terminal Dec 24 11:31
root@localhost:~
File Edit View Search Terminal Help
[root@localhost ~]# tcpdump -ni enp0s3
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
11:30:01.172718 IP 192.168.0.1 > 10.0.2.9: ICMP echo request, id 10, seq 1, length 64
11:30:01.173946 IP 10.0.2.9 > 192.168.0.1: ICMP echo reply, id 10, seq 1, length 64
11:30:02.174558 IP 192.168.0.1 > 10.0.2.9: ICMP echo request, id 10, seq 2, length 64
11:30:02.175381 IP 10.0.2.9 > 192.168.0.1: ICMP echo reply, id 10, seq 2, length 64
11:30:03.178182 IP 192.168.0.1 > 10.0.2.9: ICMP echo request, id 10, seq 3, length 64
11:30:03.179086 IP 10.0.2.9 > 192.168.0.1: ICMP echo reply, id 10, seq 3, length 64
11:30:04.179516 IP 192.168.0.1 > 10.0.2.9: ICMP echo request, id 10, seq 4, length 64
11:30:04.180458 IP 10.0.2.9 > 192.168.0.1: ICMP echo reply, id 10, seq 4, length 64
11:30:05.186502 IP 192.168.0.1 > 10.0.2.9: ICMP echo request, id 10, seq 5, length 64
11:30:05.187419 IP 10.0.2.9 > 192.168.0.1: ICMP echo reply, id 10, seq 5, length 64
11:30:06.336227 ARP, Request who-has 192.168.0.1 tell 192.168.0.2, length 28
11:30:06.336987 ARP, Reply 192.168.0.1 is-at 08:00:27:2b:c0:a3, length 46
11:30:06.598141 ARP, Request who-has 192.168.0.2 tell 192.168.0.1, length 46
11:30:06.598202 ARP, Reply 192.168.0.2 is-at 08:00:27:7e:39:e2, length 28
```