Myrna E Santiago

12/4/2023

CYSE 270: Linux System for Cybersecurity

Lab 12 – Advanced Network configurations

Scenario: You, as a network admin, are going to set up your Ubuntu VM as a gateway to provide Internet access to another client Ubuntu VM. The client VM needs to be in the same internal network as the gateway (**as shown in Figure 1**). Once the connection is ready, you need to configure the firewall to secure the network properly. The following requirements need to be satisfied to receive full credits.

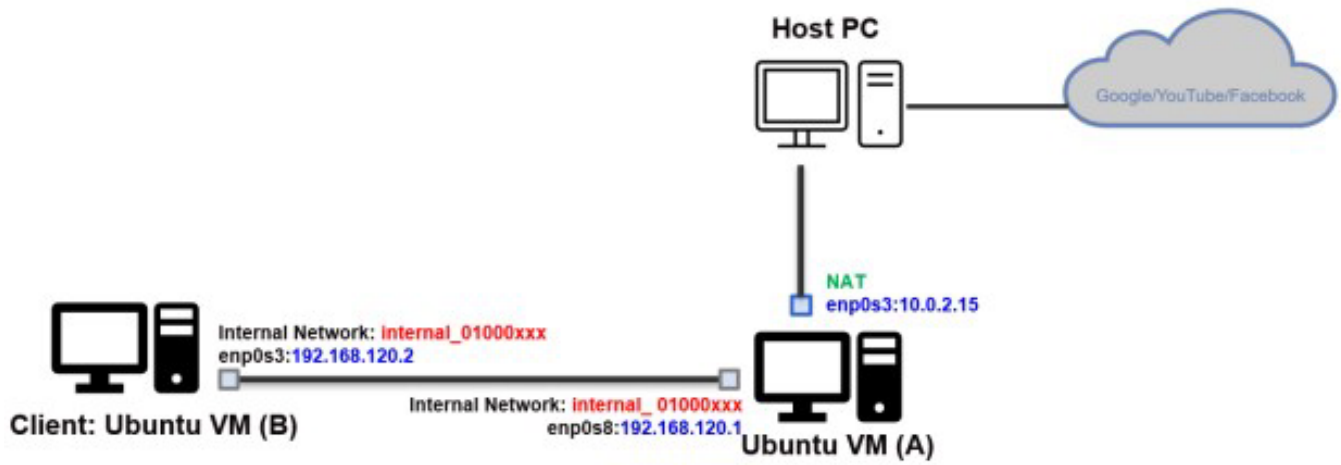


Figure 1 Desired Network Topology

Please note that you need to customize the value in the fields marked in RED above.

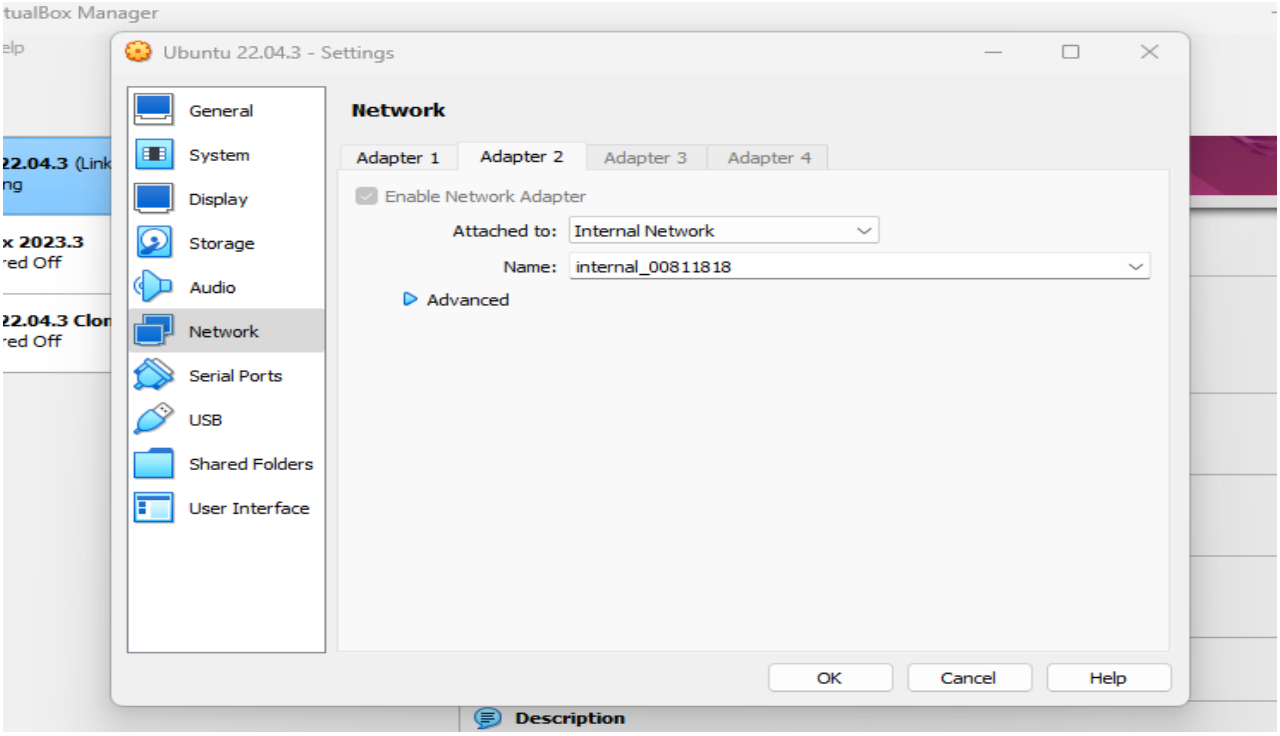
Please configure the network with the following requirement: (You need to clone the existing VM)

Task A –Network Configuration (**60 points**)

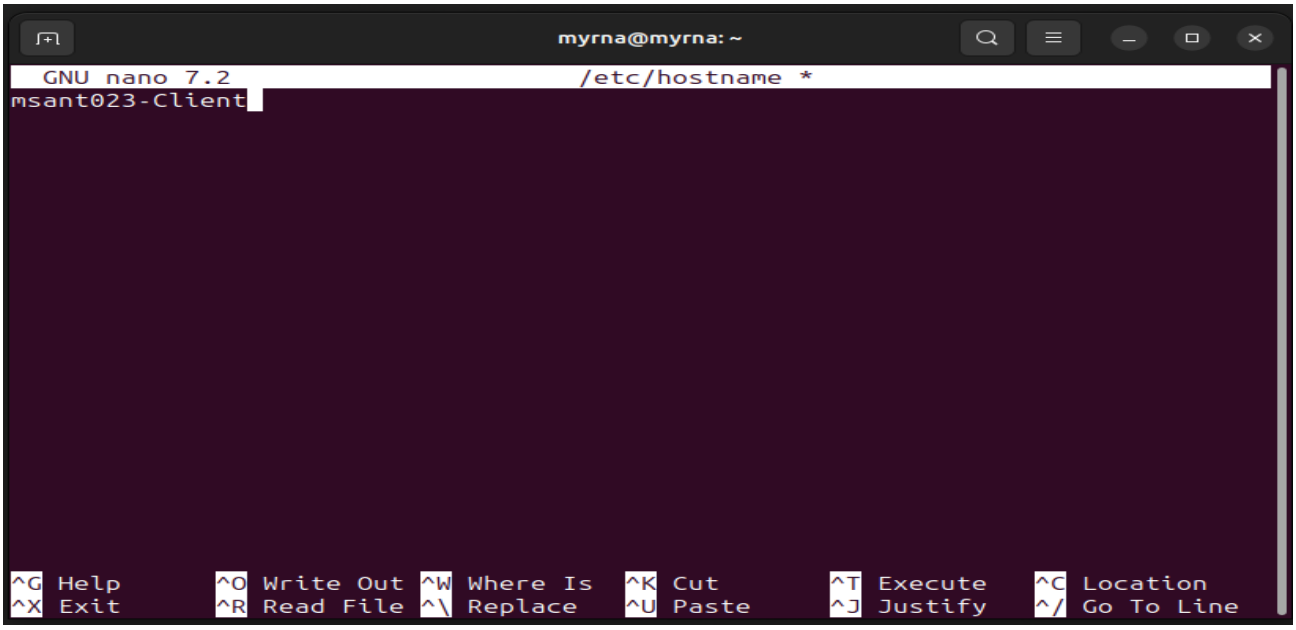
Please submit the screenshot for all the steps.

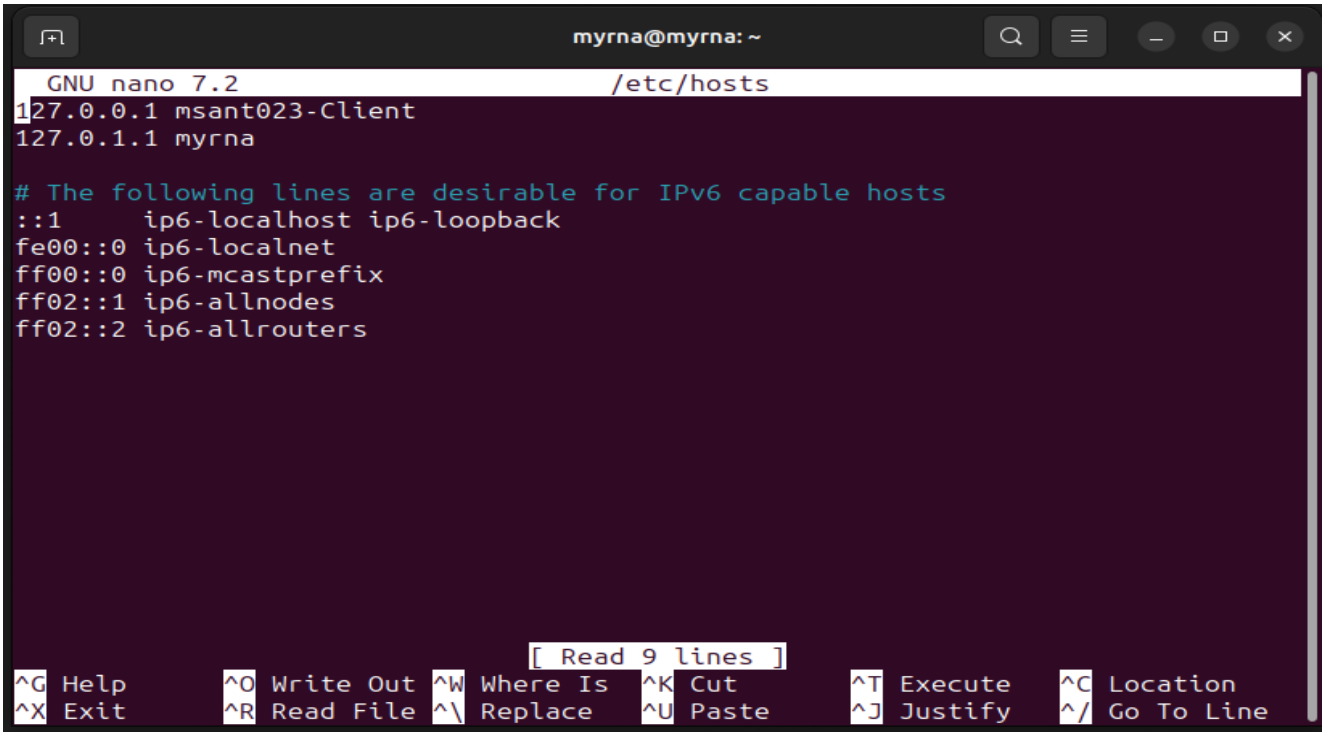
1. In the virtual box setting, connect two VMs in the same internal network, "internal_{UIN}".

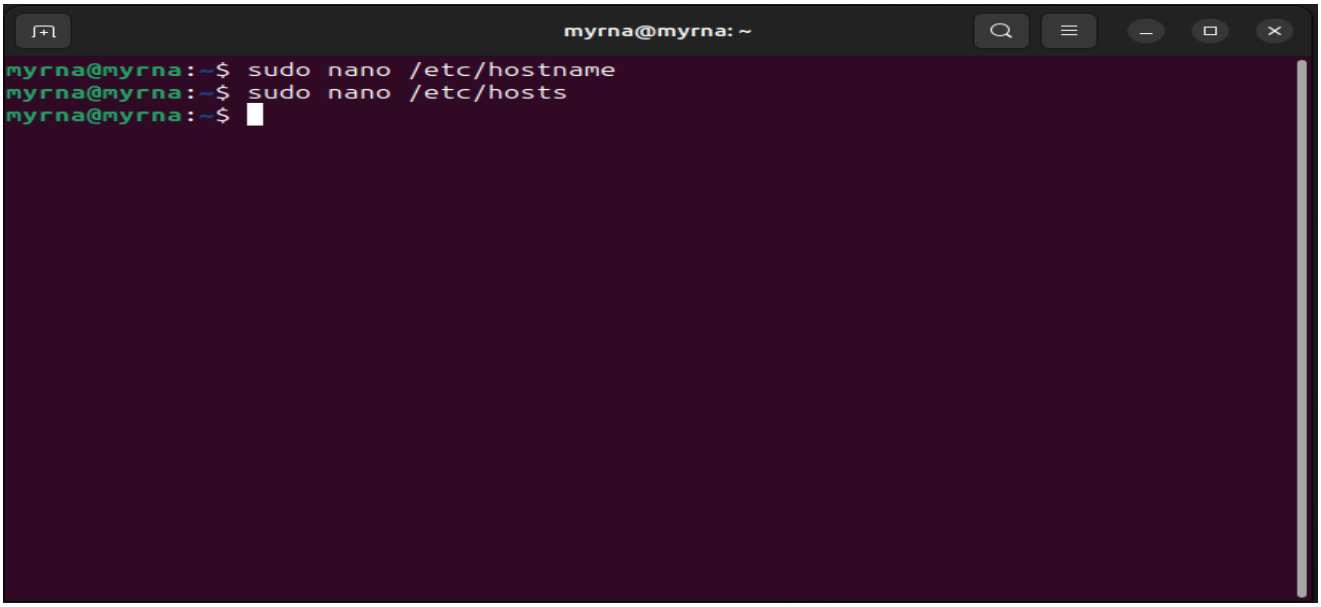
Replace {UIN} with your real UIN.



2. <u>Change the hostname</u> of the Client VM to "{MIDASname}-Client." **Replace {MIDAS name} with your real MIDAS name.** **Don't forget to reboot your client VM to reflect the change in hostname.**







3. Configure the temporary IP address on the Gateway Ubuntu, as shown in Figure 1.

```
myrna@myrna: ~
myrna@myrna:~$ sudo ip address add 192.168.120.1/24 dev enp0s8
myrna@myrna:~$
```

```
myrna@myrna: ~
myrna@myrna:~$ sudo ip address add 192.168.120.1/24 dev enp0s8
RTNETLINK answers: File exists
myrna@myrna:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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 pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:89:9c:53 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 86144sec preferred_lft 86144sec
    inet6 fe80::a00:27ff:fe89:9c53/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:38:41:3c brd ff:ff:ff:ff:ff:ff
    inet 192.168.120.1/24 scope global enp0s8
       valid_lft forever preferred_lft forever
myrna@myrna:~$
```

4. Configure the temporary IP address, routing table, and DNS server on Client VM as shown in Figure 1.

```
myrna@msant023-Client: ~
myrna@msant023-Client:~$ sudo ip address add 192.168.120.2/24 dev enp0s3
[sudo] password for myrna:
myrna@msant023-Client:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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 pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:47:4d:e2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.120.2/24 scope global enp0s3
       valid_lft forever preferred_lft forever
myrna@msant023-Client:~$
```

```
myrna@msant023-Client: ~
myrna@msant023-Client:~$ sudo ip route add default via 192.168.120.1
RTNETLINK answers: File exists
myrna@msant023-Client:~$ sudo ip route add 192.168.120.0/24 dev enp0s3
RTNETLINK answers: File exists
myrna@msant023-Client:~$
```

```
myrna@myrna: ~
myrna@myrna:~$ sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
myrna@myrna:~$ sudo iptables -A FORWARD -i enp0s3 -o enp0s8 -m state --state RELATED,ESTABLISHED -j ACCEPT
myrna@myrna:~$ sudo iptables -A FORWARD -i enp0s8 -o enp0s3 -j ACCEPT
myrna@myrna:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
ACCEPT     all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
myrna@myrna:~$
```

5. Configure gateway Ubuntu to enable IP forwarding (to forward the traffic) (also NAT configuration)

```
root@myrna: /home/myrna
myrna@myrna:~$ sudo echo 1 > /proc/sys/net/ipv4/ip_forward
bash: /proc/sys/net/ipv4/ip_forward: Permission denied
myrna@myrna:~$ su root
Password:
su: Authentication failure
myrna@myrna:~$ sudo passwd
New password:
Retype new password:
passwd: password updated successfully
myrna@myrna:~$ sudo echo 1 > /proc/sys/net/ipv4/ip_forward
bash: /proc/sys/net/ipv4/ip_forward: Permission denied
myrna@myrna:~$ su root
Password:
root@myrna:/home/myrna# echo 1 > /proc/sys/net/ipv4/ip_forward
root@myrna:/home/myrna# cat /proc/sys/net/ipv4/ip_forward
1
root@myrna:/home/myrna#
```

6. Test your ping connection to 8.8.8.8 and www.google.com in the client VM, respectively.

```
myrna@msant023-Client: ~
myrna@msant023-Client:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=58 time=15.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=58 time=16.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=58 time=19.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=58 time=18.2 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=58 time=19.1 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 15.204/17.637/19.103/1.498 ms
myrna@msant023-Client:~$ ping www.google.com
ping: www.google.com: Temporary failure in name resolution
myrna@msant023-Client:~$
```

```
myrna@msant023-Client: ~
myrna@msant023-Client:~$ sudo nano /etc/resolv.conf
[sudo] password for myrna:
myrna@msant023-Client:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=58 time=14.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=58 time=16.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=58 time=14.6 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 14.638/15.299/16.485/0.840 ms
myrna@msant023-Client:~$ ping www.google.com
PING www.google.com (172.253.62.147) 56(84) bytes of data.
64 bytes from bc-in-f147.1e100.net (172.253.62.147): icmp_seq=1 ttl=58 time=15.5
 ms
64 bytes from bc-in-f147.1e100.net (172.253.62.147): icmp_seq=2 ttl=58 time=17.9
 ms
64 bytes from bc-in-f147.1e100.net (172.253.62.147): icmp_seq=3 ttl=58 time=15.4
 ms
64 bytes from bc-in-f147.1e100.net (172.253.62.147): icmp_seq=4 ttl=58 time=14.5
 ms
^C
--- www.google.com ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4009ms
```

```
myrna@msant023-Client: ~
myrna@msant023-Client:~$ ping www.google.com
PING www.google.com (172.253.63.104) 56(84) bytes of data.
64 bytes from bi-in-f104.1e100.net (172.253.63.104): icmp_seq=1 ttl=58 time=15.8 ms
64 bytes from bi-in-f104.1e100.net (172.253.63.104): icmp_seq=2 ttl=58 time=17.6 ms
64 bytes from bi-in-f104.1e100.net (172.253.63.104): icmp_seq=3 ttl=58 time=16.7 ms
^C
--- www.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 15.778/16.696/17.563/0.729 ms
myrna@msant023-Client:~$ ping www.odu.edu
PING www.odu.edu (35.170.140.174) 56(84) bytes of data.
64 bytes from ec2-35-170-140-174.compute-1.amazonaws.com (35.170.140.174): icmp_seq=1 ttl=55 time=17.0 ms
64 bytes from ec2-35-170-140-174.compute-1.amazonaws.com (35.170.140.174): icmp_seq=2 ttl=55 time=28.2 ms
64 bytes from ec2-35-170-140-174.compute-1.amazonaws.com (35.170.140.174): icmp_seq=3 ttl=55 time=22.7 ms
64 bytes from ec2-35-170-140-174.compute-1.amazonaws.com (35.170.140.174): icmp_seq=4 ttl=55 time=19.6 ms
^C
--- www.odu.edu ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 17.020/21.866/28.169/4.156 ms
myrna@msant023-Client:~$
```

Task B –Firewall Configuration (**40 points**)

1. Configure the iptables on the gateway Ubuntu to block all the inbound ICMP packets from the Client VM.

2. Configure the iptables on the gateway Ubuntu to block all the outbound ICMP packets that originated from the gateway Ubuntu itself.

Image shows both steps.

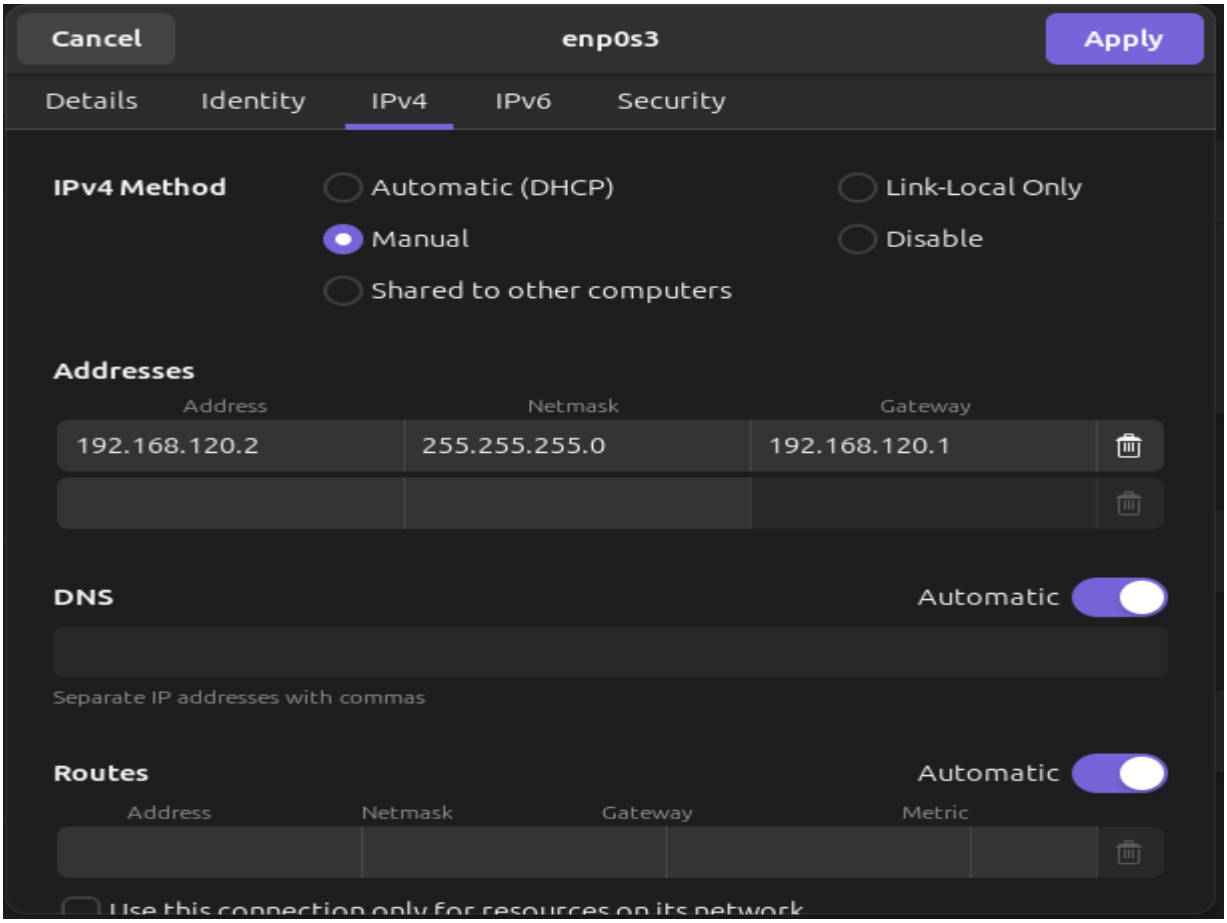
```
myrna@msant023-Client: ~
myrna@msant023-Client:~$ sudo iptables -A INPUT -p icmp --icmp-type 8 -s 192.168.120.2 -j DROP
myrna@msant023-Client:~$ sudo iptables -A OUTPUT -p icmp --icmp-type 8 -s 192.168.120.2 -j DROP
myrna@msant023-Client:~$ iptables -L
iptables v1.8.9 (nf_tables): Could not fetch rule set generation id: Permission denied (you must be root)
myrna@msant023-Client:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  192.168.120.2        anywhere             icmp echo-request
DROP       icmp --  192.168.120.2        anywhere             icmp echo-request
DROP       icmp --  192.168.120.2        anywhere             icmp echo-request
DROP       icmp --  192.168.120.2        anywhere             icmp echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  192.168.120.2        anywhere             icmp echo-request
DROP       icmp --  192.168.120.2        anywhere             icmp echo-request
myrna@msant023-Client:~$
```

Extra credit:

Set the permanent IP address on the Client Ubuntu based on the above network topology.


Cancel
enp0s3
Apply
Details
Identity
IPv4
IPv6
Security
IPv4 Method
Automatic (DHCP)
Link-Local Only
Manual
Disable
Shared to other computers
Addresses
Address
Netmask
Gateway
192.168.120.2
255.255.255.0
192.168.120.1
DNS
Automatic
Separate IP addresses with commas
Routes
Automatic
Address
Netmask
Gateway
Metric