

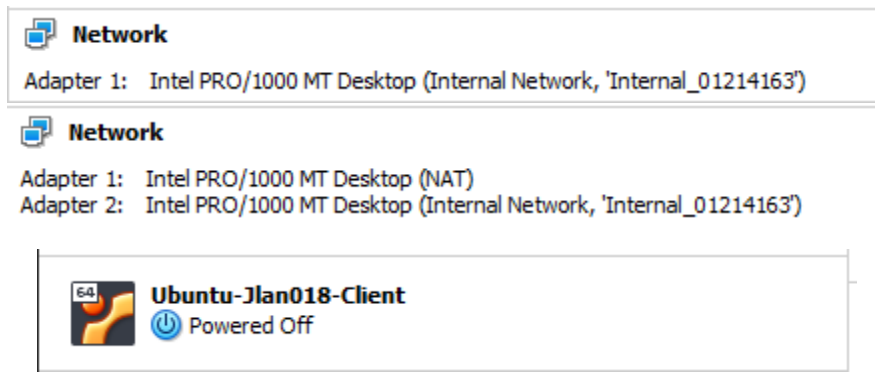
Justin Landolina

UID: 01214163

Assignment 13 – Advanced Network Configurations

CYSE270_33410 LINUX SYSTEM FOR CYBERSECURITY

TASK A:



In these screenshots I connected two VMs to the same internal network and named it “Internal 01214163 (my UIN)”. I also changed the client host name to include my MIDAS.

```
justin@justin-VirtualBox:~$ sudo ifconfig enp0s8 192.168.11.100
justin@justin-VirtualBox:~$ 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::6187:7b8d:ad10:5018 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:60:be:29 txqueuelen 1000 (Ethernet)
    RX packets 386 bytes 247159 (247.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 407 bytes 40435 (40.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.11.100 netmask 255.255.255.0 broadcast 192.168.11.255
    ether 08:00:27:95:09:22 txqueuelen 1000 (Ethernet)
    RX packets 81 bytes 21394 (21.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 205 bytes 32544 (32.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
justin@justin-VirtualBox:~$ sudo ifconfig enp0s3 192.168.11.101
[sudo] password for justin:
justin@justin-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.11.101 netmask 255.255.255.0 broadcast 192.168.11.255
    ether 08:00:27:da:b4:b2 txqueuelen 1000 (Ethernet)
    RX packets 48 bytes 11116 (11.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 109 bytes 17598 (17.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

In these two screenshots I set the temporary IP address on Gateway and Client.

```
justin@justin-VirtualBox:~$ sudo ip route add default via 192.168.11.100
justin@justin-VirtualBox:~$ route -n
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0        192.168.11.100 0.0.0.0         UG    0      0        0 enp0s3
169.254.0.0    0.0.0.0        255.255.0.0     U     1000    0        0 enp0s3
192.168.11.0   0.0.0.0        255.255.255.0   U      0      0        0 enp0s3
```

Configured the routing table above on Client

```
justin@justin-VirtualBox: ~  
justin@justin-VirtualBox:~$ cat /etc/resolv.conf  
# This file is managed by man:systemd-resolved(8). Do not edit.  
#  
# This is a dynamic resolv.conf file for connecting local clients to the  
# internal DNS stub resolver of systemd-resolved. This file lists all  
# configured search domains.  
#  
# Run "resolvectl status" to see details about the uplink DNS servers  
# currently in use.  
#  
# Third party programs must not access this file directly, but only through the  
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,  
# replace this symlink by a static file or a different symlink.  
#  
# See man:systemd-resolved.service(8) for details about the supported modes of  
# operation for /etc/resolv.conf.  
  
nameserver 192.168.1.109  
options edns0 trust-ad  
justin@justin-VirtualBox:~$
```

This screenshot shows me configure the DNS. I use 192.168.1.109 as my DNS because that is my raspberry pi DNS server

```
justin@justin-VirtualBox:~$ sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE  
justin@justin-VirtualBox:~$ sudo iptables -A FORWARD -i enp0s3 -o enp0s8 -m state --sta  
te RELATED,ESTABLISHED -j ACCEPT  
justin@justin-VirtualBox:~$ sudo iptables -A FORWARD -i enp0s8 -o enp0s3 -j ACCEPT  
justin@justin-VirtualBox:~$ 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  
justin@justin-VirtualBox:~$
```

This screenshot shows me configuring NAT on the Gateway

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

This screenshot shows me switching to root user to change the ip_forward value to 1.

```
root@justin-VirtualBox: /home/justin
justin@justin-VirtualBox:~$ sudo iptables -A FORWARD -i enp0s3 -o enp0s8 -m state --state
ELATED,ESTABLISHED -j ACCEPT
justin@justin-VirtualBox:~$ sudo iptables -A FORWARD -i enp0s8 -o enp0s3 -j ACCEPT
justin@justin-VirtualBox:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target    prot opt source      destination
Chain FORWARD (policy ACCEPT)
target    prot opt source      destination
Chain OUTPUT (policy ACCEPT)
target    prot opt source      destination
justin@justin-VirtualBox:~$ su root
Password:
su: Authentication failure
justin@justin-VirtualBox:~$ sudo passwd
New password:
Retype new password:
passwd: password updated successfully
justin@justin-VirtualBox:~$ su root
root@justin-VirtualBox: /home/justin# echo 1 > /proc/sys/net/ipv4/ip_forward
root@justin-VirtualBox: /home/justin# cat /proc/sys/net/ipv4/ip_forward
1
root@justin-VirtualBox: /home/justin#
```

```
Justin@Justin-VirtualBox: ~
nameserver 192.168.1.109
options edns0 trust-ad
Justin@Justin-VirtualBox:~$ 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=57 time=14.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=57 time=13.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=57 time=14.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=57 time=14.7 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=57 time=13.2 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 5374ms
rtt min/avg/max/mdev = 13.228/13.905/14.680/0.538 ms
Justin@Justin-VirtualBox:~$ ping www.google.com
PING www.google.com (172.253.63.103) 56(84) bytes of data:
64 bytes from bl-in-f103.1e100.net (172.253.63.103): icmp_seq=1 ttl=103 time=15.1 ms
64 bytes from bl-in-f103.1e100.net (172.253.63.103): icmp_seq=2 ttl=103 time=26.7 ms
64 bytes from bl-in-f103.1e100.net (172.253.63.103): icmp_seq=3 ttl=103 time=14.6 ms
64 bytes from bl-in-f103.1e100.net (172.253.63.103): icmp_seq=4 ttl=103 time=14.0 ms
64 bytes from bl-in-f103.1e100.net (172.253.63.103): icmp_seq=5 ttl=103 time=15.1 ms
64 bytes from bl-in-f103.1e100.net (172.253.63.103): icmp_seq=6 ttl=103 time=23.1 ms
64 bytes from bl-in-f103.1e100.net (172.253.63.103): icmp_seq=7 ttl=103 time=15.2 ms
^C
--- www.google.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 8125ms
rtt min/avg/max/mdev = 14.001/17.681/26.674/4.672 ms
Justin@Justin-VirtualBox:~$
```

In this screenshot I show the two VMs side by side and demonstrate that the client has connection to the internet and has name resolution capabilities.

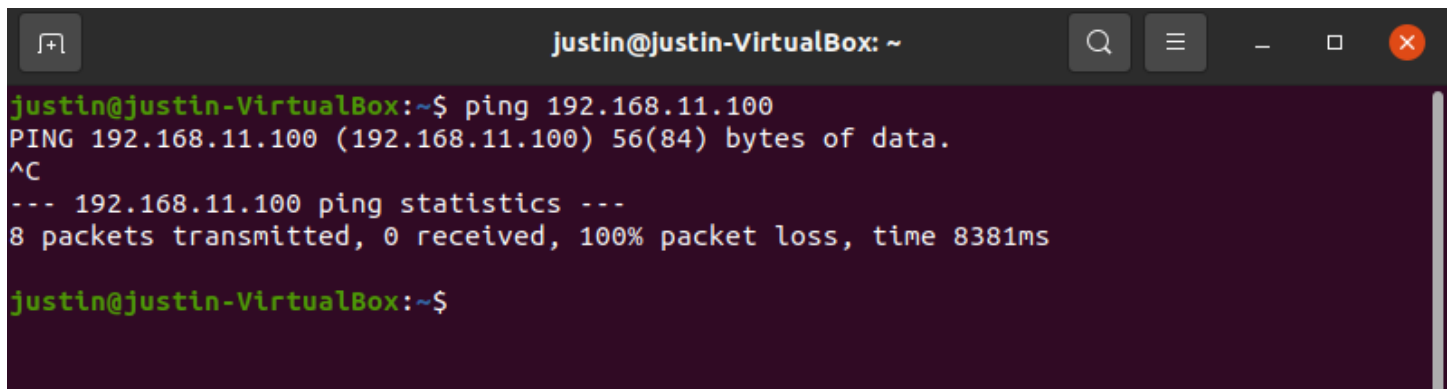
TASK B:

```
root@justin-VirtualBox: /home/justin# iptables -L
Chain INPUT (policy ACCEPT)
target    prot opt source      destination
DROP      icmp -- anywhere anywhere

Chain FORWARD (policy ACCEPT)
target    prot opt source      destination
ACCEPT    all  -- anywhere anywhere
ACCEPT    all  -- anywhere anywhere

Chain OUTPUT (policy ACCEPT)
target    prot opt source      destination
DROP      icmp -- anywhere anywhere
root@justin-VirtualBox: /home/justin#
```

Iptables showing that ICMP requests as both input and output will be dropped.

A terminal window titled 'justin@justin-VirtualBox: ~' with standard window controls. The terminal shows a user running a ping command to 192.168.11.100. The output indicates that 8 packets were transmitted but none were received, resulting in a 100% packet loss. The user then presses Ctrl-C to stop the command.

```
justin@justin-VirtualBox:~$ ping 192.168.11.100
PING 192.168.11.100 (192.168.11.100) 56(84) bytes of data.
^C
--- 192.168.11.100 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 8381ms

justin@justin-VirtualBox:~$
```

This screenshot shows me unable to ping 192.168.11.100 (Ubuntu Gateway) after blocking ICMP.