Design of Secure Computer Systems

Lab 01

Network Basics
&
Routing Basics

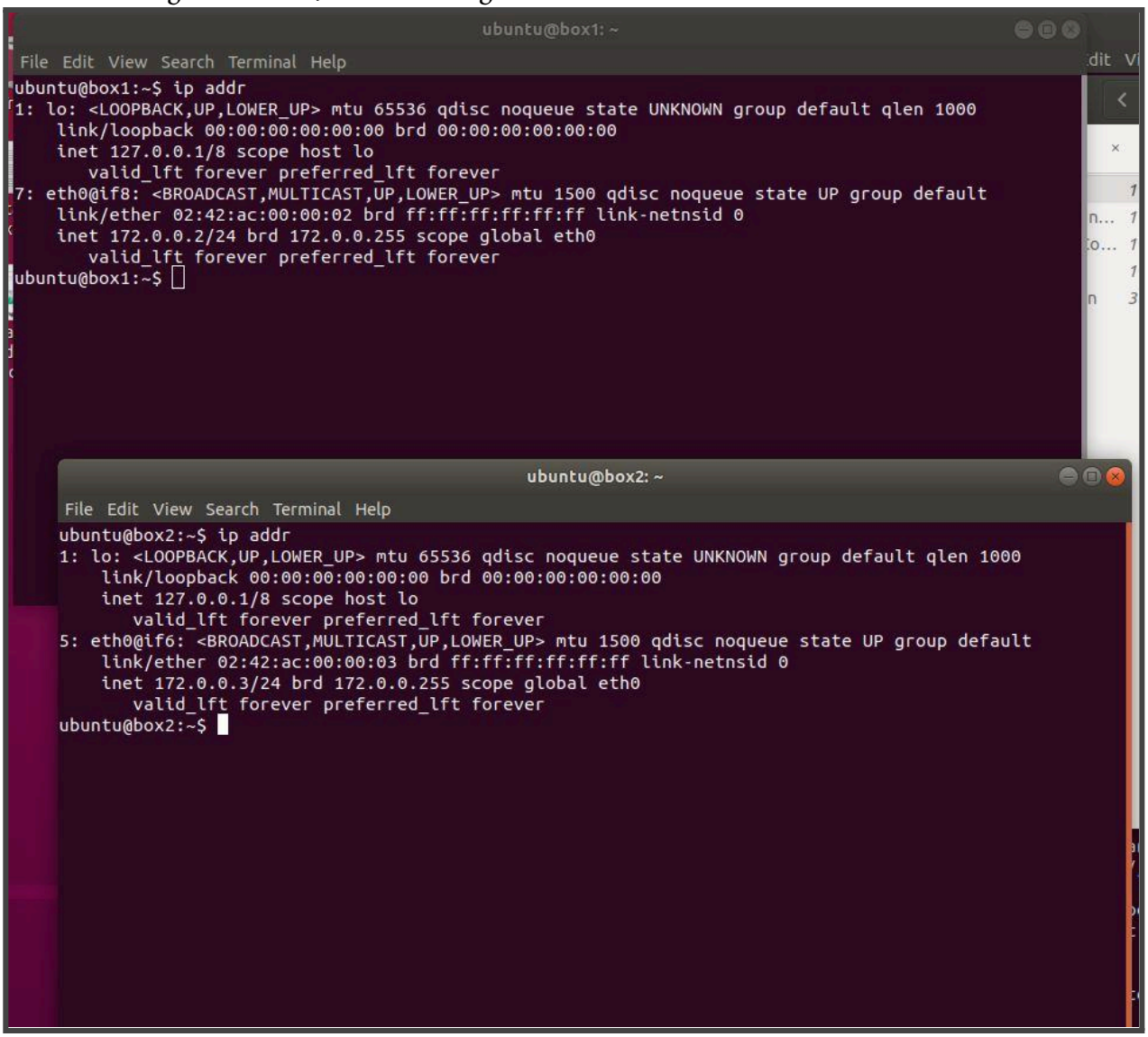
The goal of this lab is to introduce Network & Routing basics like TCP, ARP, TCP Dump, NAT, Routing Table etc.

Name: Rakshita Mathur

Part 1- Network Basics

1. Explore

Used command: **ip addr**
In the following screenshots, we are looking into the machine IP and MAC address.



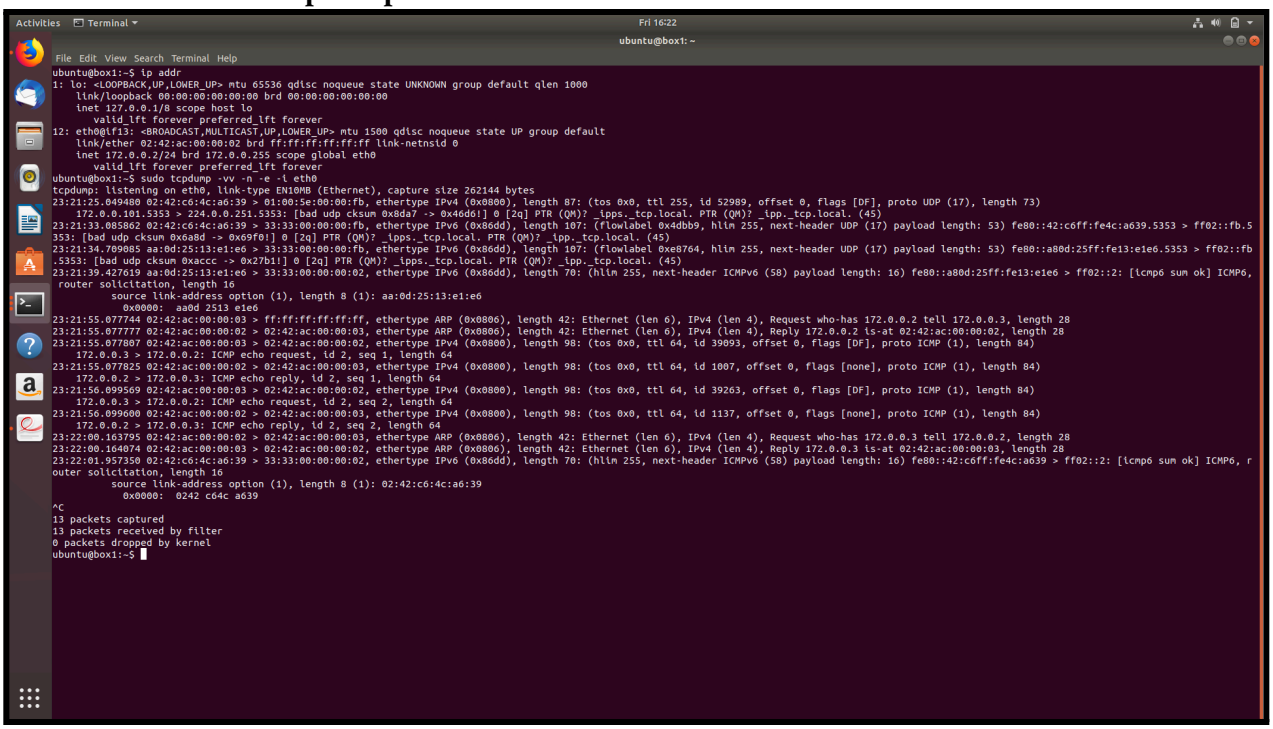
2. ARP

Used command: **arp -a**
The Address Resolution Protocol (ARP) is used to map IP addresses to MAC addresses.

Nothing showed in box2.

So we ran tcpdump on box1 to see the network traffic.

Used command: **sudo tcpdump -vv -n -e -i eth0**

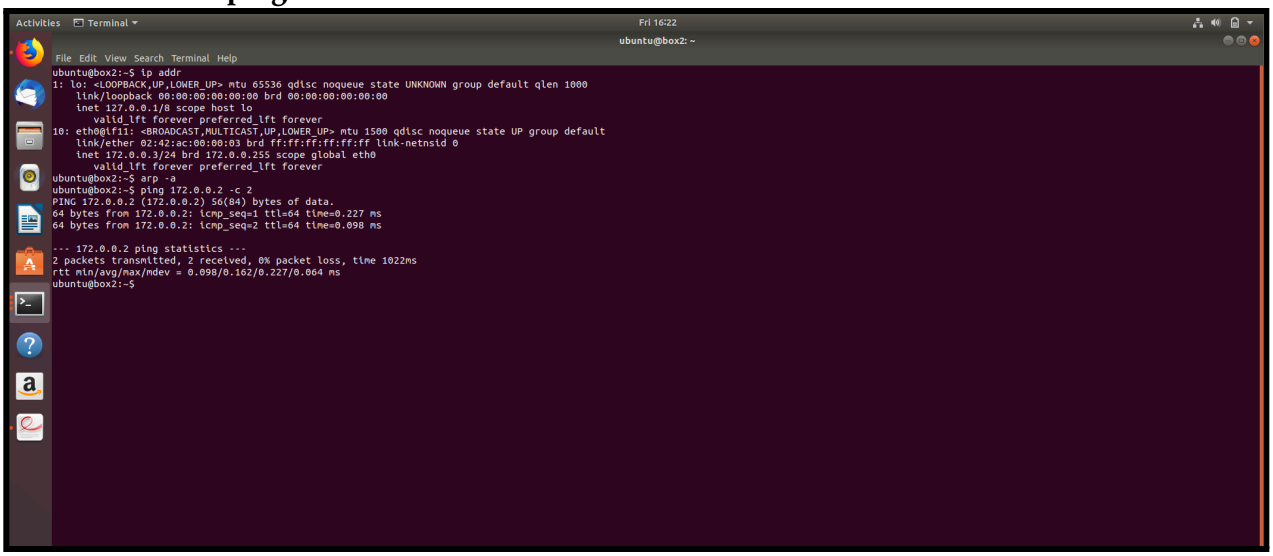


These options to tcpdump are:

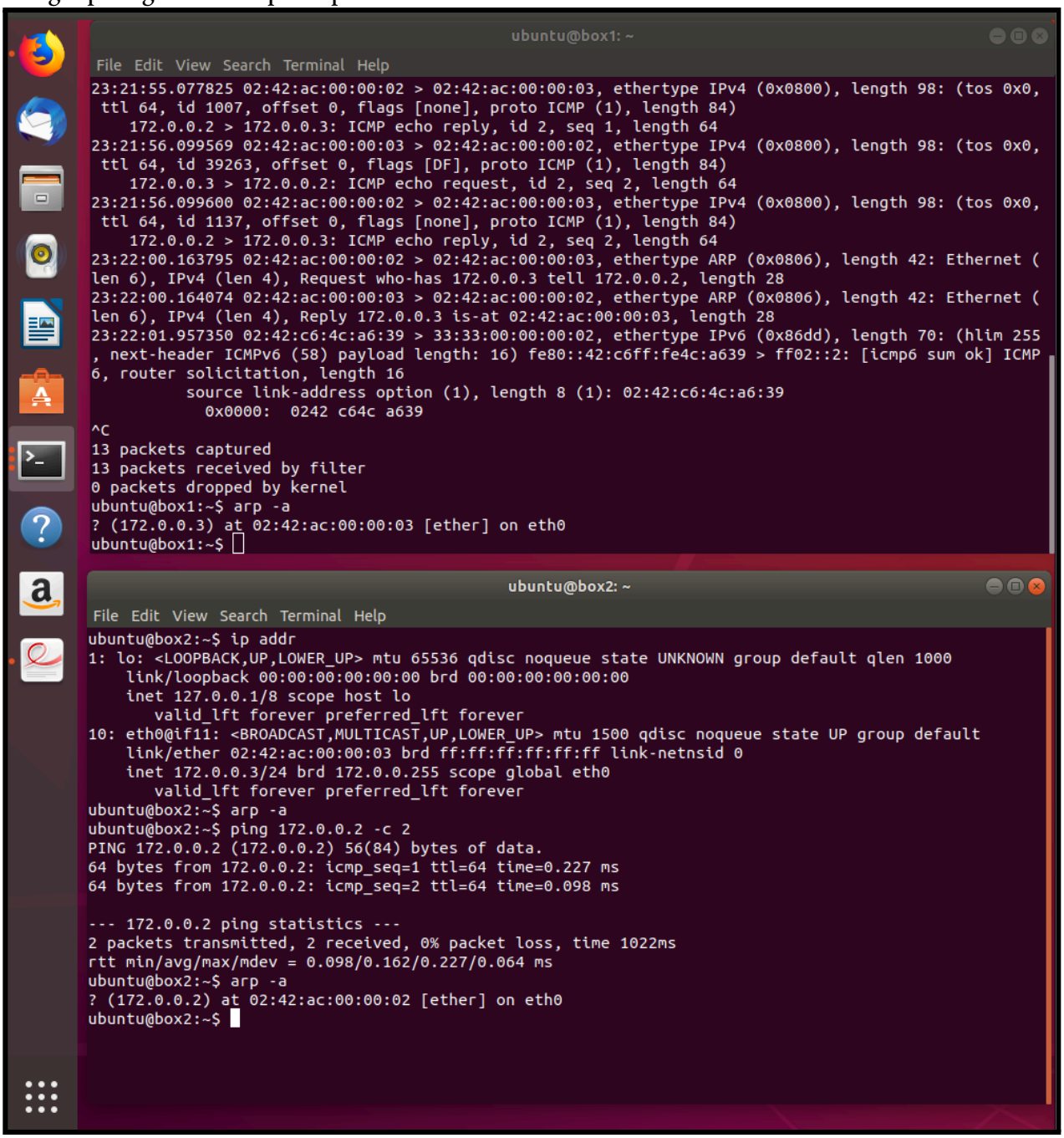
- -vv – Provide verbose output
- -n – Do not perform the reverse DNS lookup, just show the IP addresses.
- -e Show Ethernet MAC addresses.
- -i eth0 Show traffic on interface eth0.

On box2, using the ping command to ping box1:

Used Command: **ping 172.0.0.2 -c 2**



Using arp -a again after tcpdump to show the communication between the two boxes.

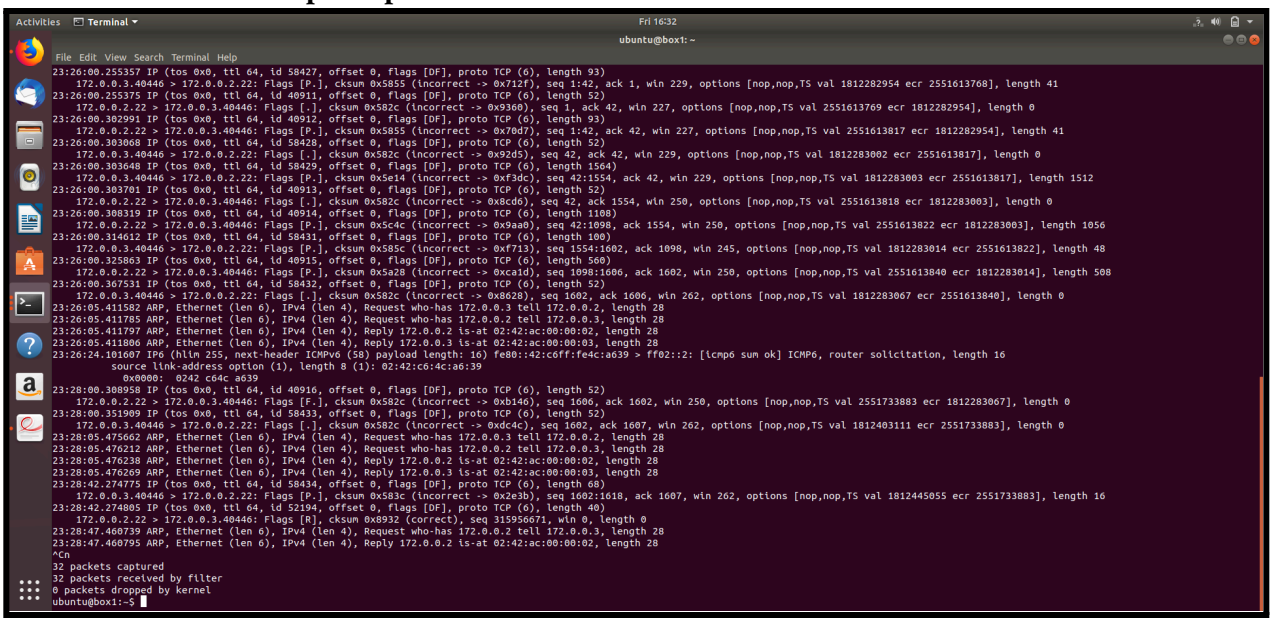


3. TCP

Here we briefly look at some IP packets within a TCP session, specifically the “three-way handshake”.

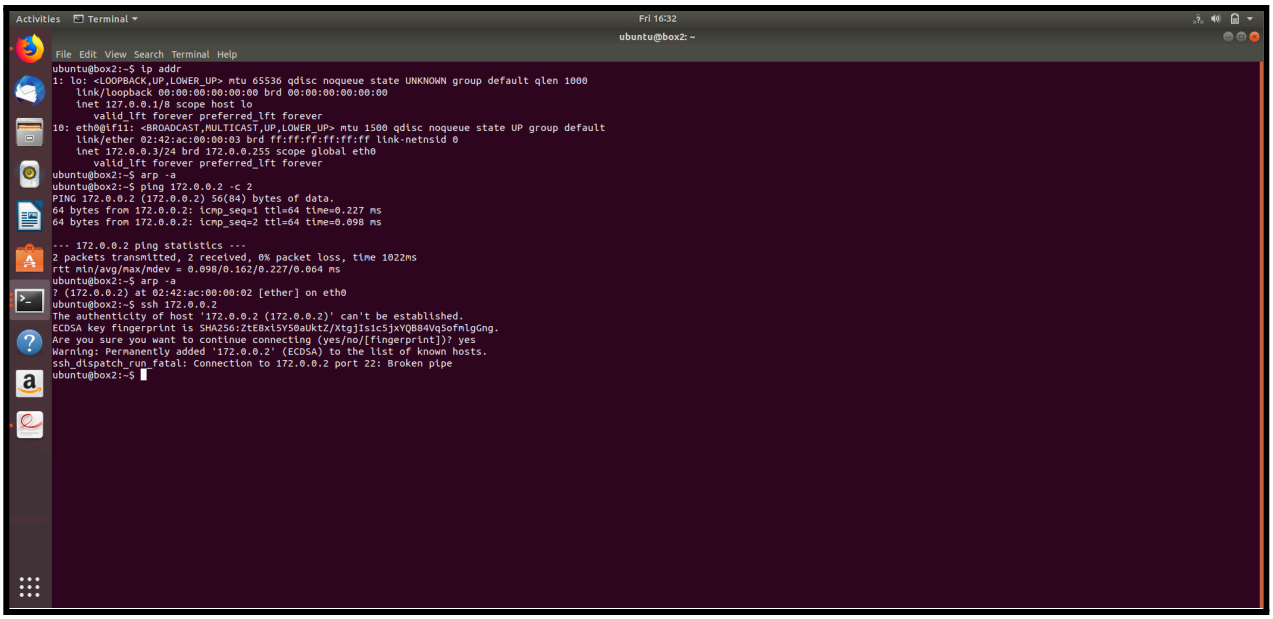
Restart the tcpdump on box1, this time without the -e switch:

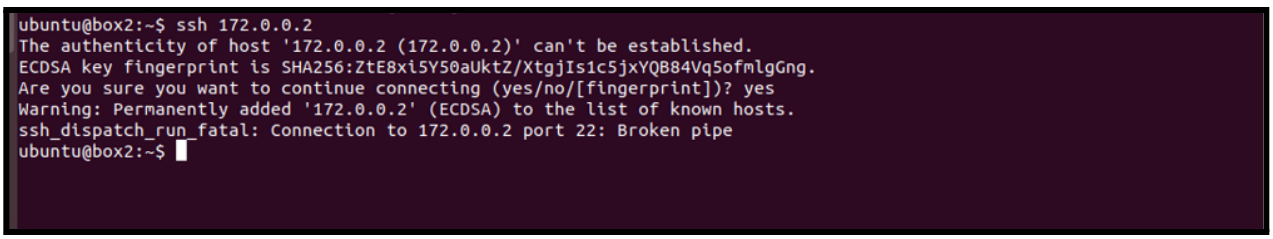
Used command: **sudo tcpdump -vv -n -i eth0**



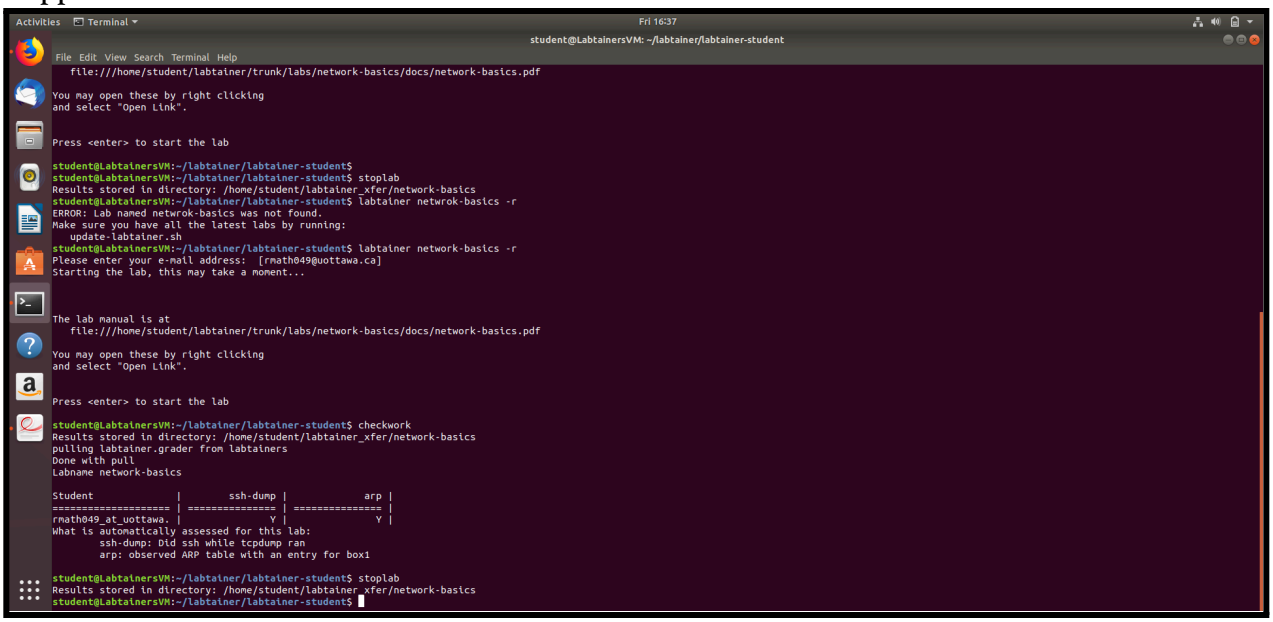
Then, on box2, initiate an ssh session to box1. As we wish to look at the start of the session:

Used Command: **ssh 172.0.0.2**





Stopped the Lab and checked the work at the end.

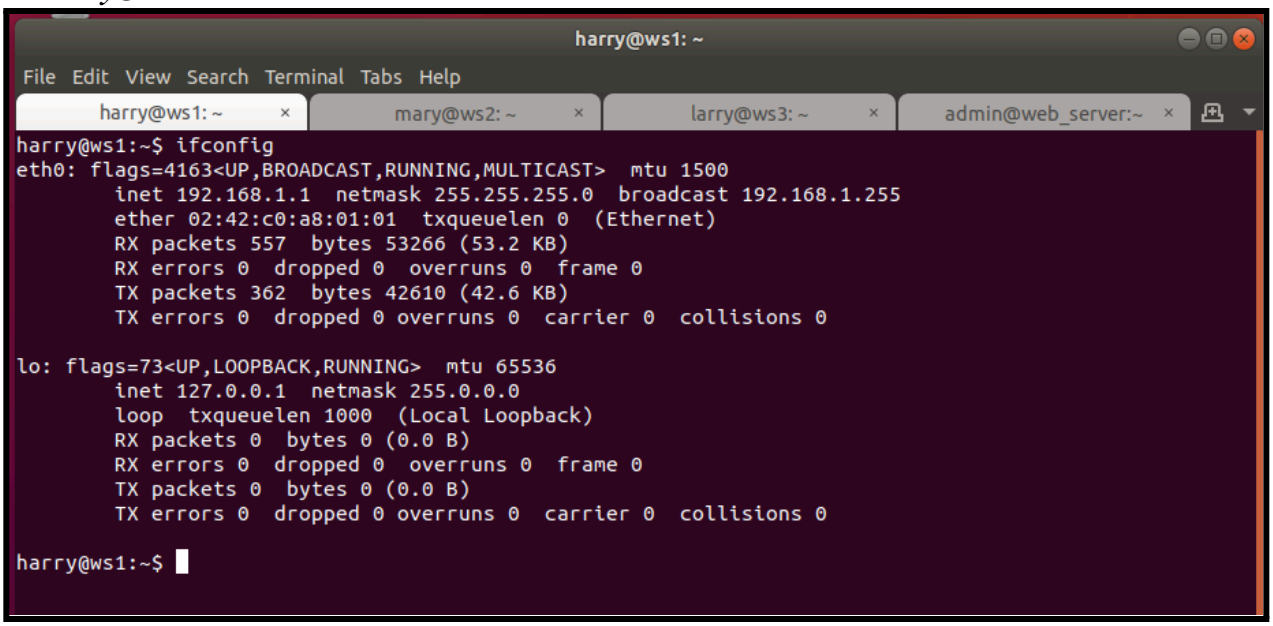


Part 2- Routing Basics

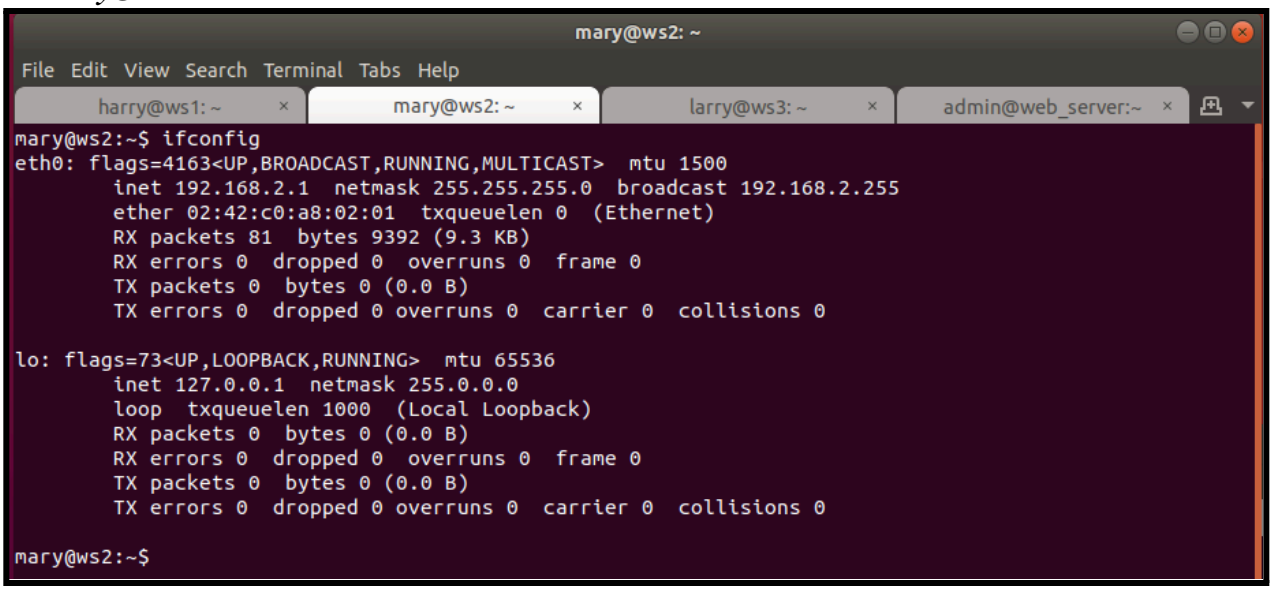
1. Explore

Used command: **ifconfig**
In the following screenshots, we are using ifconfig on the different computers to familiarize ourselves with the subnets associated with each of the computer's network interfaces

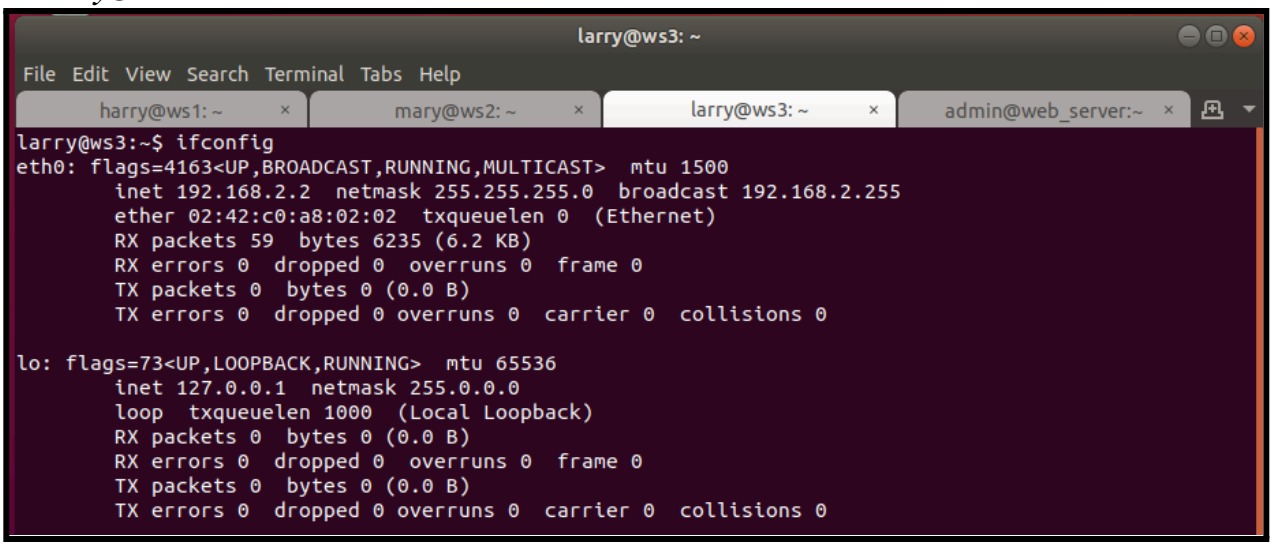
On harry@ws1



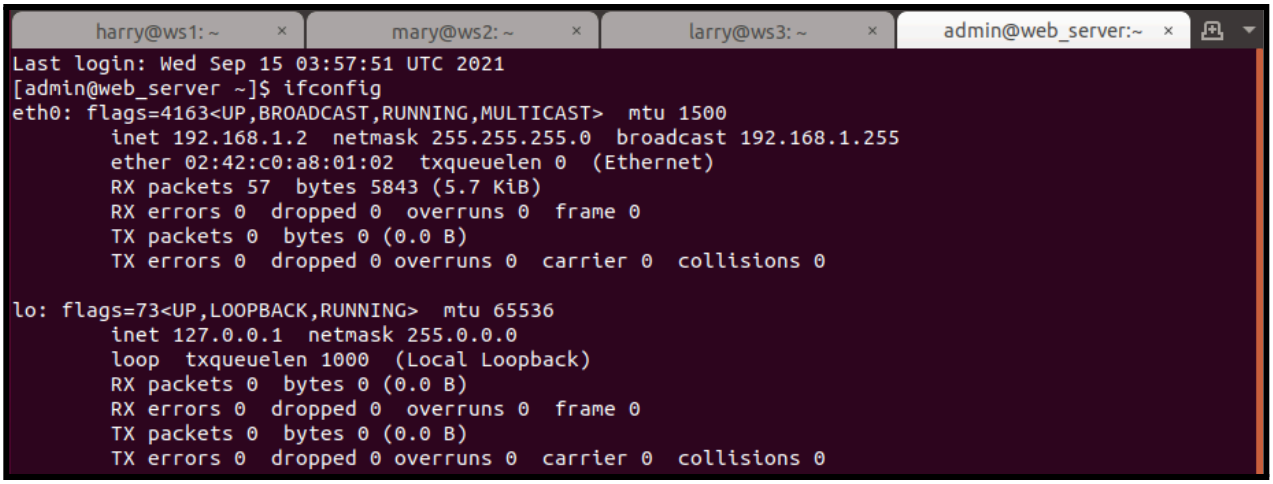
On mary@ws2



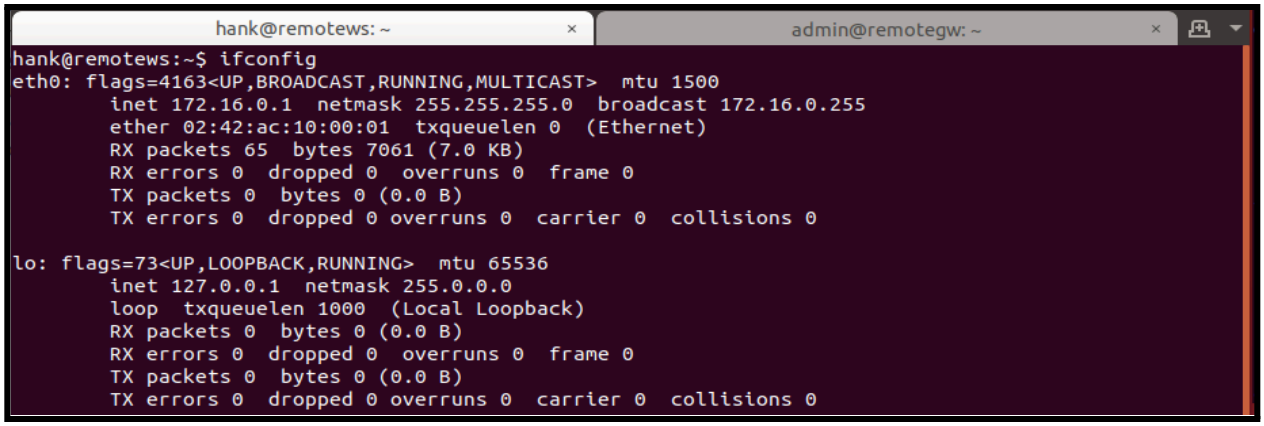
On larry@ws3



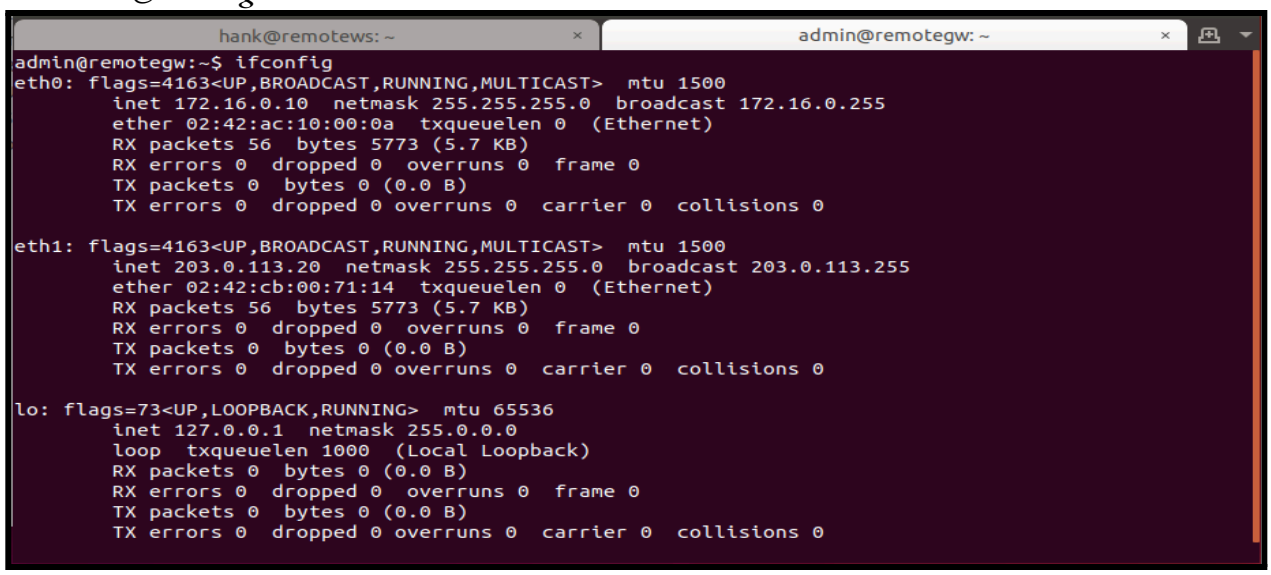
On admin@web_server



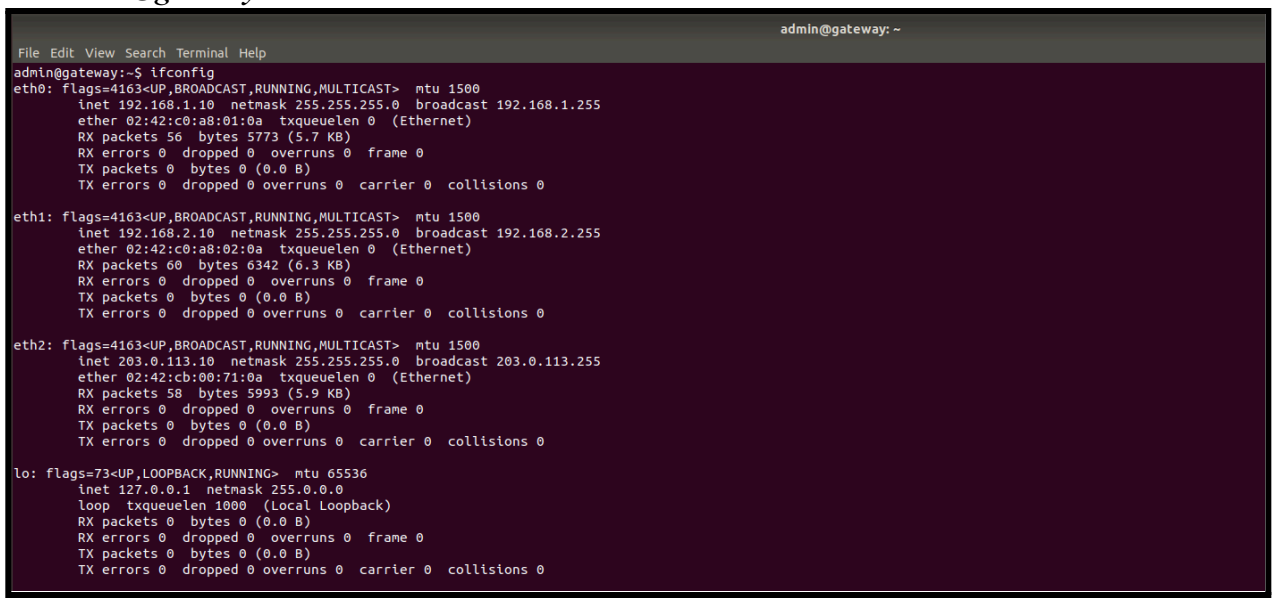
On hank@remotews



On admin@remotegw



On admin@gateway

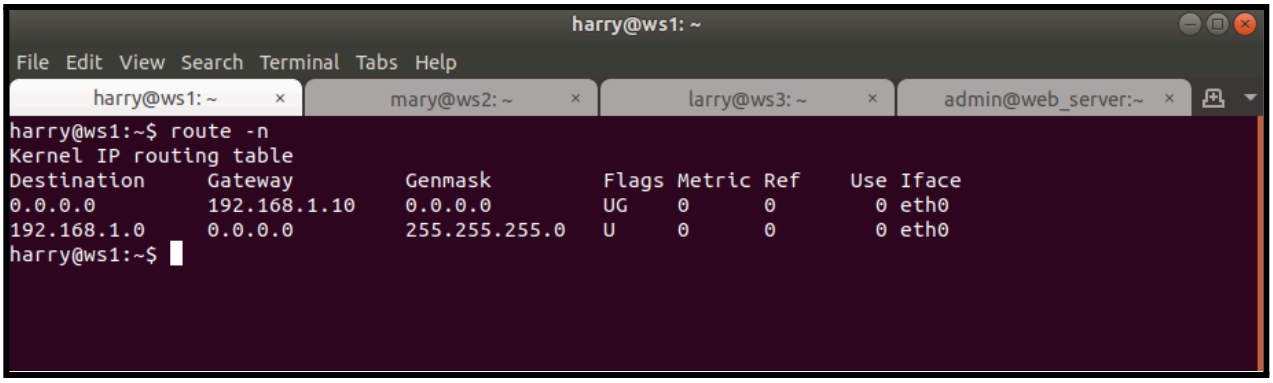


2. Internal Packet Forwarding

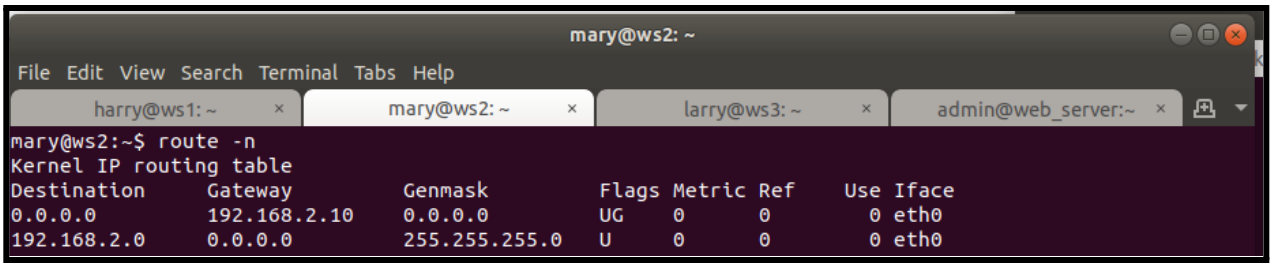
Used command: **route -n**

This shows the routing table for all three web servers.

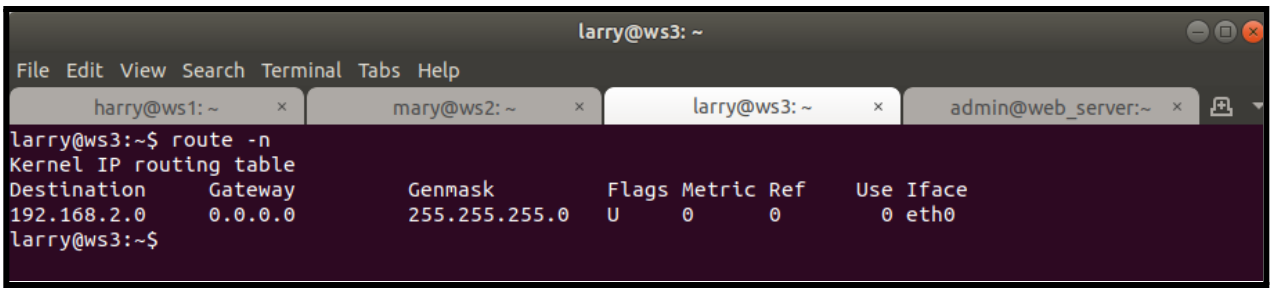
ws1 has a default gateway.



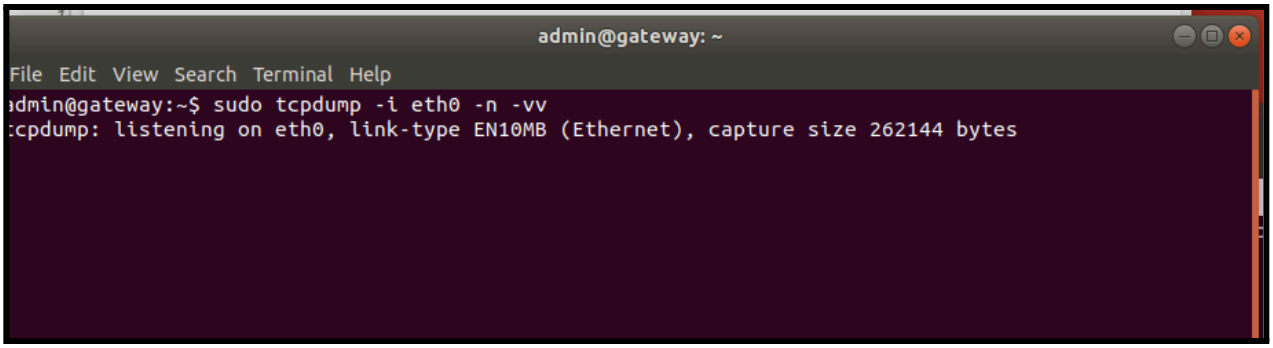
ws2 has a default gateway as well.



ws3 has no default gateway.



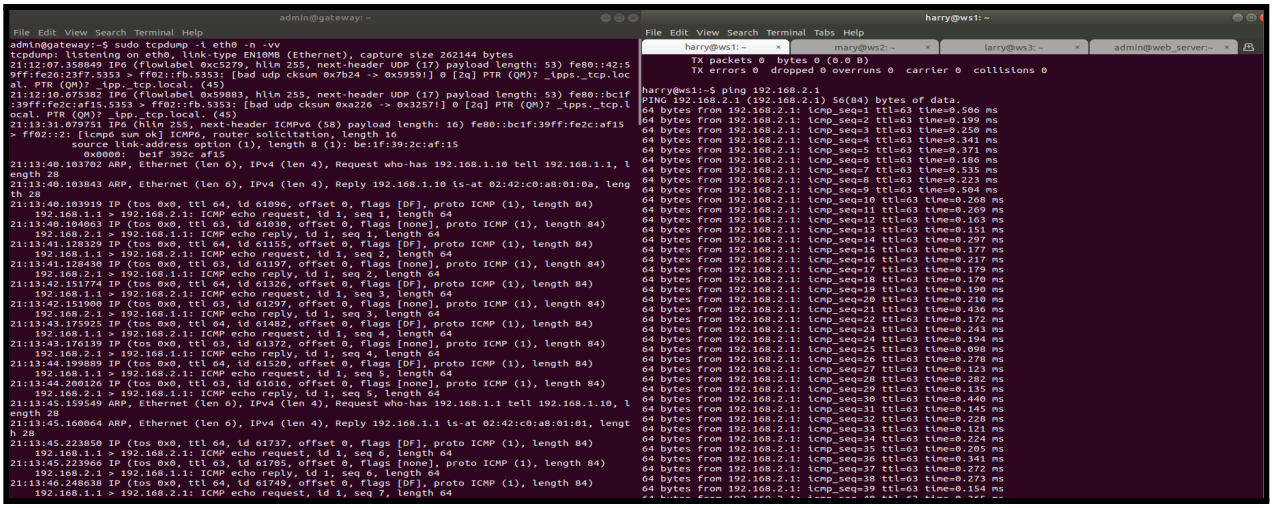
Used command: **sudo tcpdump -i eth0 -n -vv**



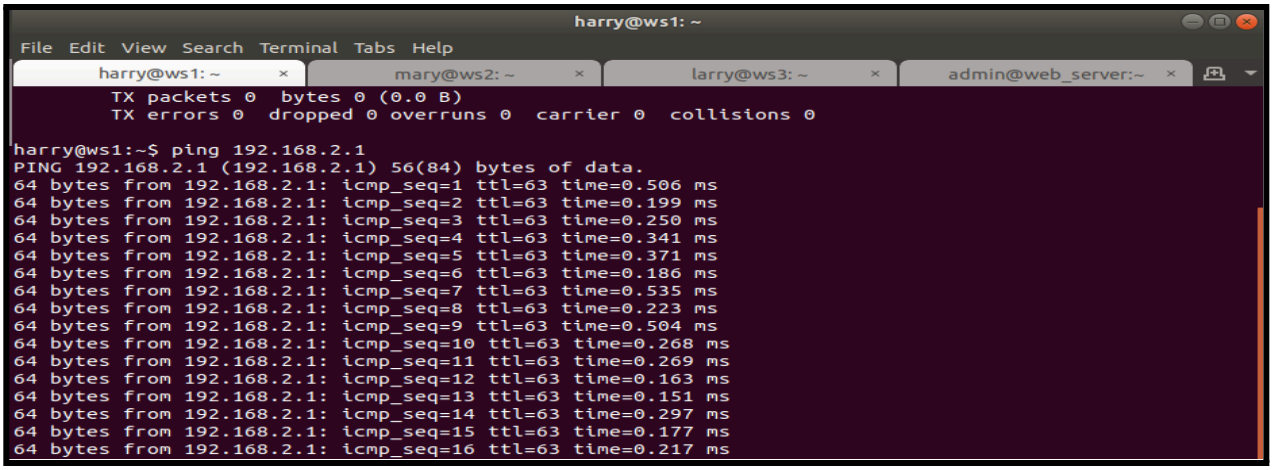
This shows nothing until we ping the ws1 with ws2's IP address.

Used command: **ping [ws2 IP]**

The communication between ws1 and ws2 is established visa the gateways and can also be seen in the tcpdump of the admin.



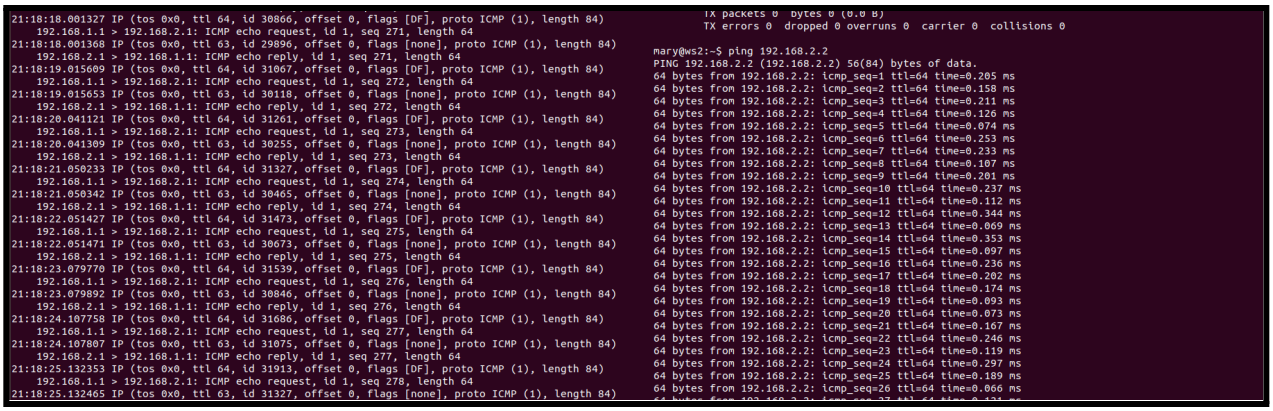
***Zoomed**- the ping command from ws1 to ws2*



***Zoomed**- tcpdump of admin after the ping command*

```
21:13:40.103702 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.1.10 tell 192.168.1.1, l
ength 28
21:13:40.103843 ARP, Ethernet (len 6), IPv4 (len 4), Reply 192.168.1.10 is-at 02:42:c0:a8:01:0a, leng
th 28
21:13:40.103919 IP (tos 0x0, ttl 64, id 61096, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.1 > 192.168.2.1: ICMP echo request, id 1, seq 1, length 64
21:13:40.104063 IP (tos 0x0, ttl 63, id 61030, offset 0, flags [none], proto ICMP (1), length 84)
    192.168.2.1 > 192.168.1.1: ICMP echo reply, id 1, seq 1, length 64
21:13:41.128329 IP (tos 0x0, ttl 64, id 61155, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.1 > 192.168.2.1: ICMP echo request, id 1, seq 2, length 64
21:13:41.128430 IP (tos 0x0, ttl 63, id 61197, offset 0, flags [none], proto ICMP (1), length 84)
    192.168.2.1 > 192.168.1.1: ICMP echo reply, id 1, seq 2, length 64
21:13:42.151774 IP (tos 0x0, ttl 64, id 61326, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.1 > 192.168.2.1: ICMP echo request, id 1, seq 3, length 64
21:13:42.151900 IP (tos 0x0, ttl 63, id 61297, offset 0, flags [none], proto ICMP (1), length 84)
    192.168.2.1 > 192.168.1.1: ICMP echo reply, id 1, seq 3, length 64
21:13:43.175925 IP (tos 0x0, ttl 64, id 61482, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.1 > 192.168.2.1: ICMP echo request, id 1, seq 4, length 64
21:13:43.176139 IP (tos 0x0, ttl 63, id 61372, offset 0, flags [none], proto ICMP (1), length 84)
    192.168.2.1 > 192.168.1.1: ICMP echo reply, id 1, seq 4, length 64
21:13:44.199889 IP (tos 0x0, ttl 64, id 61520, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.1 > 192.168.2.1: ICMP echo request, id 1, seq 5, length 64
21:13:44.200126 IP (tos 0x0, ttl 63, id 61616, offset 0, flags [none], proto ICMP (1), length 84)
    192.168.2.1 > 192.168.1.1: ICMP echo reply, id 1, seq 5, length 64
21:13:45.159549 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.1.1 tell 192.168.1.10, l
ength 28
21:13:45.160064 ARP, Ethernet (len 6), IPv4 (len 4), Reply 192.168.1.1 is-at 02:42:c0:a8:01:01, lengt
h 28
21:13:45.223850 IP (tos 0x0, ttl 64, id 61737, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.1 > 192.168.2.1: ICMP echo request, id 1, seq 6, length 64
21:13:45.223966 IP (tos 0x0, ttl 63, id 61705, offset 0, flags [none], proto ICMP (1), length 84)
    192.168.2.1 > 192.168.1.1: ICMP echo reply, id 1, seq 6, length 64
21:13:46.248638 IP (tos 0x0, ttl 64, id 61749, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.1 > 192.168.2.1: ICMP echo request, id 1, seq 7, length 64
```

Similarly, communicating between ws2 to ws3 using the ws2's default gateway



***Zoomed**- the ping command from ws1 to ws2*

```
mary@ws2:~$ ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
64 bytes from 192.168.2.2: icmp_seq=1 ttl=64 time=0.205 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=64 time=0.158 ms
64 bytes from 192.168.2.2: icmp_seq=3 ttl=64 time=0.211 ms
64 bytes from 192.168.2.2: icmp_seq=4 ttl=64 time=0.126 ms
64 bytes from 192.168.2.2: icmp_seq=5 ttl=64 time=0.074 ms
64 bytes from 192.168.2.2: icmp_seq=6 ttl=64 time=0.253 ms
64 bytes from 192.168.2.2: icmp_seq=7 ttl=64 time=0.233 ms
64 bytes from 192.168.2.2: icmp_seq=8 ttl=64 time=0.107 ms
64 bytes from 192.168.2.2: icmp_seq=9 ttl=64 time=0.201 ms
64 bytes from 192.168.2.2: icmp_seq=10 ttl=64 time=0.237 ms
64 bytes from 192.168.2.2: icmp_seq=11 ttl=64 time=0.112 ms
64 bytes from 192.168.2.2: icmp_seq=12 ttl=64 time=0.344 ms
64 bytes from 192.168.2.2: icmp_seq=13 ttl=64 time=0.069 ms
64 bytes from 192.168.2.2: icmp_seq=14 ttl=64 time=0.353 ms
64 bytes from 192.168.2.2: icmp_seq=15 ttl=64 time=0.097 ms
64 bytes from 192.168.2.2: icmp_seq=16 ttl=64 time=0.236 ms
64 bytes from 192.168.2.2: icmp_seq=17 ttl=64 time=0.202 ms
```

***Zoomed**- tcpdump of admin after the ping command*

```
21:18:46.599735 IP (tos 0x0, ttl 63, id 34420, offset 0, flags [none], proto ICMP (1), length 84)
    192.168.2.1 > 192.168.1.1: ICMP echo reply, id 1, seq 299, length 64
21:18:47.623674 IP (tos 0x0, ttl 64, id 34215, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.1 > 192.168.2.1: ICMP echo request, id 1, seq 300, length 64
21:18:47.623786 IP (tos 0x0, ttl 63, id 34585, offset 0, flags [none], proto ICMP (1), length 84)
    192.168.2.1 > 192.168.1.1: ICMP echo reply, id 1, seq 300, length 64
21:18:48.648538 IP (tos 0x0, ttl 64, id 34330, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.1 > 192.168.2.1: ICMP echo request, id 1, seq 301, length 64
21:18:48.648637 IP (tos 0x0, ttl 63, id 34738, offset 0, flags [none], proto ICMP (1), length 84)
    192.168.2.1 > 192.168.1.1: ICMP echo reply, id 1, seq 301, length 64
21:18:49.672050 IP (tos 0x0, ttl 64, id 34363, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.1 > 192.168.2.1: ICMP echo request, id 1, seq 302, length 64
21:18:49.672110 IP (tos 0x0, ttl 63, id 34927, offset 0, flags [none], proto ICMP (1), length 84)
    192.168.2.1 > 192.168.1.1: ICMP echo reply, id 1, seq 302, length 64
21:18:50.696328 IP (tos 0x0, ttl 64, id 34482, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.1 > 192.168.2.1: ICMP echo request, id 1, seq 303, length 64
21:18:50.696437 IP (tos 0x0, ttl 63, id 34958, offset 0, flags [none], proto ICMP (1), length 84)
    192.168.2.1 > 192.168.1.1: ICMP echo reply, id 1, seq 303, length 64
21:18:51.719995 IP (tos 0x0, ttl 64, id 34532, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.1 > 192.168.2.1: ICMP echo request, id 1, seq 304, length 64
21:18:51.720111 IP (tos 0x0, ttl 63, id 35133, offset 0, flags [none], proto ICMP (1), length 84)
    192.168.2.1 > 192.168.1.1: ICMP echo reply, id 1, seq 304, length 64
21:18:52.744012 IP (tos 0x0, ttl 64, id 34549, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.1.1 > 192.168.2.1: ICMP echo request, id 1, seq 305, length 64
21:18:52.744145 IP (tos 0x0, ttl 63, id 35308, offset 0, flags [none], proto ICMP (1), length 84)
```

When we try to ping ws1 from ws3, the communication is unable to establish as there is no default gateway in ws3

```
larry@ws3:~$ ping 192.168.1.1
ping: connect: Network is unreachable
```

To add a gateway in ws3 we used the following command and then was able to able to ping ws1.
Used command: **sudo route add default gw 193.168.2.10**

```
larry@ws3:~$ sudo route add default gw 192.168.2.10
larry@ws3:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63 time=0.148 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=63 time=0.145 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=63 time=0.136 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=63 time=0.228 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=63 time=0.083 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=63 time=0.125 ms
64 bytes from 192.168.1.1: icmp_seq=7 ttl=63 time=0.127 ms
64 bytes from 192.168.1.1: icmp_seq=8 ttl=63 time=0.088 ms
```

Used command: **route -n**
Now we can see a gateway on ws3 as well.

```
larry@ws3:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.2.10    0.0.0.0         UG    0      0        0 eth0
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

Used command: **wget [ip/website]**
This will get the website page from web server 3 now as there is a gateway.

```
larry@ws3:~$ wget 192.168.1.2/
--2021-09-16 21:25:43--  http://192.168.1.2/
Connecting to 192.168.1.2:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 122 [text/html]
Saving to: 'index.html'

index.html          100%[===================>]     122  --.-KB/s    in 0s

2021-09-16 21:25:43 (11.6 MB/s) - 'index.html' saved [122/122]
```

3. Routing to the Internet

Used command: **wget www.google.com**

ws2 can access the webpage as it has the DNS configuration- nameserver in it.

```
mary@ws2:~$  wget www.google.com
--2021-09-16 21:27:01--  http://www.google.com/
Resolving www.google.com (www.google.com)... 142.250.182.196, 2404:6800:4009:804::2004
Connecting to www.google.com (www.google.com)|142.250.182.196|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'

index.html              [ <=>                ]  16.92K  --.-KB/s    in 0.02s

2021-09-16 21:27:06 (994 KB/s) - 'index.html' saved [17321]
```

ws3 has no DNS config. Hence we can not access the google webpage.

```
larry@ws3:~$ wget www.google.com
--2021-09-16 21:27:46--  http://www.google.com/
Resolving www.google.com (www.google.com)... failed: Temporary failure in name resolution.
wget: unable to resolve host address 'www.google.com'
larry@ws3:~$
```

Copied name server from ws2 and now ws3. Now it is working.

```
larry@ws3:~$ sudo nano /etc/resolv.conf
larry@ws3:~$ wget www.google.com
--2021-09-16 21:32:13--  http://www.google.com/
Resolving www.google.com (www.google.com)... 142.250.182.196, 2404:6800:4009:81a::2004
Connecting to www.google.com (www.google.com)|142.250.182.196|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html.1'

index.html.1            [ <=>                ]  16.95K  --.-KB/s    in 0.01s

2021-09-16 21:32:17 (1.24 MB/s) - 'index.html.1' saved [17352]
```

4. Use of network address translation (NAT)

```
admin@gateway:~$ sudo iptables -L -v -t nat
Chain PREROUTING (policy ACCEPT 22 packets, 1563 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DNAT       tcp  --  eth2   any     anywhere             anywhere             tcp dpt:
http to:192.168.1.2

Chain INPUT (policy ACCEPT 2 packets, 120 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 4 packets, 240 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 2 packets, 168 bytes)
 pkts bytes target     prot opt in     out     source               destination
    6   360 MASQUERADE  all  --  any    eth2    anywhere             anywhere
    1    60 SNAT       tcp  --  any    eth0    anywhere             192.168.1.2          tcp dpt:
http to:192.168.1.10
admin@gateway:~$
```

admin@gateway: ~

File Edit View Search Terminal Help

GNU nano 4.8 /etc/rc.local

```
#!/bin/bash
route delete default
route add default gw 203.0.113.1
#
# get ethernet device names for the three interfaces
# Note this allows us to not know the mapping of addresses to interfaces and can be skipped if the
# interfaces are known and constant.
#
lan1=$(ifconfig | grep -B1 "inet.*192.168.1.10" | awk '$1!="inet" && $1!="--" {print substr($1,1,length($1)-1)}')
lan2=$(ifconfig | grep -B1 "inet.*192.168.2.10" | awk '$1!="inet" && $1!="--" {print substr($1,1,length($1)-1)}')
wan=$(ifconfig | grep -B1 "inet.*203.0.113.10" | awk '$1!="inet" && $1!="--" {print substr($1,1,length($1)-1)}')
#
# Delete all IPTABLE chains
iptables --flush
iptables -t nat --flush
iptables --delete-chain
iptables -t nat --delete-chain
#
# Define NAT for the traffic exiting to the Internet
#
iptables --table nat -I POSTROUTING 1 --out-interface $wan -j MASQUERADE
#
# Set the destination address of web traffic (port 80) to the web server address
#
sudo iptables -t nat -A PREROUTING -i $wan -p tcp --dport 80 -j DNAT --to-destination 192.168.1.2
#
# Set the source address of web traffic (port 80) to the gateway
#
sudo iptables -t nat -A POSTROUTING -o $lan1 -p tcp --dport 80 -d 192.168.1.2 -j SNAT --to-source 192.168.1.10

#
# restart the DNS forwarder (rely on DNS provided by ISP)
#

echo "nameserver 203.0.113.1" > /etc/resolv.conf
route del -host 172.17.0.1
systemctl restart dnsmasq
```

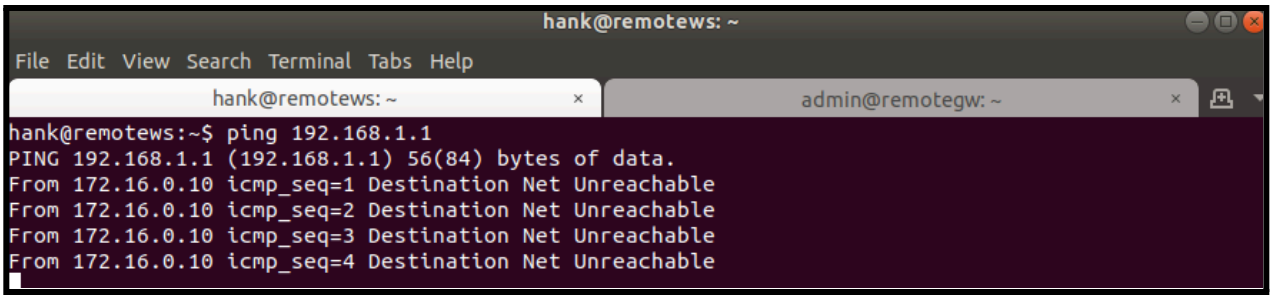
ws1 accessing google.

```
harry@ws1:~$ wget www.google.com
--2021-09-16 21:42:14--  http://www.google.com/
Resolving www.google.com (www.google.com)... 142.250.67.228, 2404:6800:4009:80f::2004
Connecting to www.google.com (www.google.com)|142.250.67.228|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'

index.html              [ <=>                ]  16.93K  --.-KB/s    in 0.02s

2021-09-16 21:42:19 (1.01 MB/s) - 'index.html' saved [17337]
```

Connection is active- shown in tcpdump of the admin.

```
    192.168.1.1.48598 > 192.168.1.10.53: [bad udp cksum 0x8395 -> 0x7344!] 48202+ A? www.google.c
om. (32)
21:42:14.820230 IP (tos 0x0, ttl 64, id 14240, offset 0, flags [DF], proto UDP (17), length 60)
    192.168.1.1.48598 > 192.168.1.10.53: [bad udp cksum 0x8395 -> 0x6ffc!] 49015+ AAAA? www.googl
e.com. (32)
21:42:18.856720 IP (tos 0x0, ttl 64, id 31311, offset 0, flags [DF], proto UDP (17), length 76)
    192.168.1.10.53 > 192.168.1.1.48598: [bad udp cksum 0x83a5 -> 0x5f63!] 48202 q: A? www.google
.com. 1/0/0 www.google.com. A 142.250.67.228 (48)
21:42:18.856941 IP (tos 0x0, ttl 64, id 31312, offset 0, flags [DF], proto UDP (17), length 88)
    192.168.1.10.53 > 192.168.1.1.48598: [bad udp cksum 0x83b1 -> 0x3a37!] 49015 q: AAAA? www.goo
gle.com. 1/0/0 www.google.com. AAAA 2404:6800:4009:80f::2004 (60)
21:42:18.860517 IP (tos 0x0, ttl 64, id 23657, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.1.1.49876 > 142.250.67.228.80: Flags [S], cksum 0x94b6 (incorrect -> 0x556b), seq 355
4761504, win 29200, options [mss 1460,sackOK,TS val 3216849432 ecr 0,nop,wscale 7], length 0
21:42:18.880500 IP (tos 0x0, ttl 61, id 1311, offset 0, flags [none], proto TCP (6), length 44)
    142.250.67.228.80 > 192.168.1.1.49876: Flags [S.], cksum 0x9e7e (correct), seq 15168001, ack
3554761505, win 65535, options [mss 1460], length 0
21:42:18.880639 IP (tos 0x0, ttl 64, id 23658, offset 0, flags [DF], proto TCP (6), length 40)
    192.168.1.1.49876 > 142.250.67.228.80: Flags [.], cksum 0x94a2 (incorrect -> 0x442b), seq 1,
ack 1, win 29200, length 0
21:42:18.880880 IP (tos 0x0, ttl 64, id 23659, offset 0, flags [DF], proto TCP (6), length 181)
    192.168.1.1.49876 > 142.250.67.228.80: Flags [P.], cksum 0x952f (incorrect -> 0xc7cb), seq 1:
142, ack 1, win 29200, length 141: HTTP, length: 141
        GET / HTTP/1.1
        User-Agent: Wget/1.20.3 (linux-gnu)
        Accept: */*
        Accept-Encoding: identity
        Host: www.google.com
        Connection: Keep-Alive
```

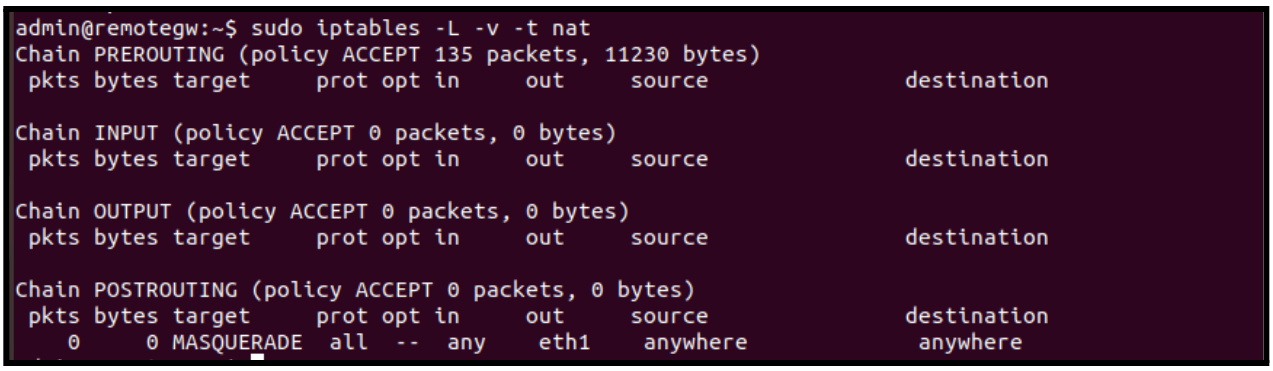
pinging Remote can not access the device.



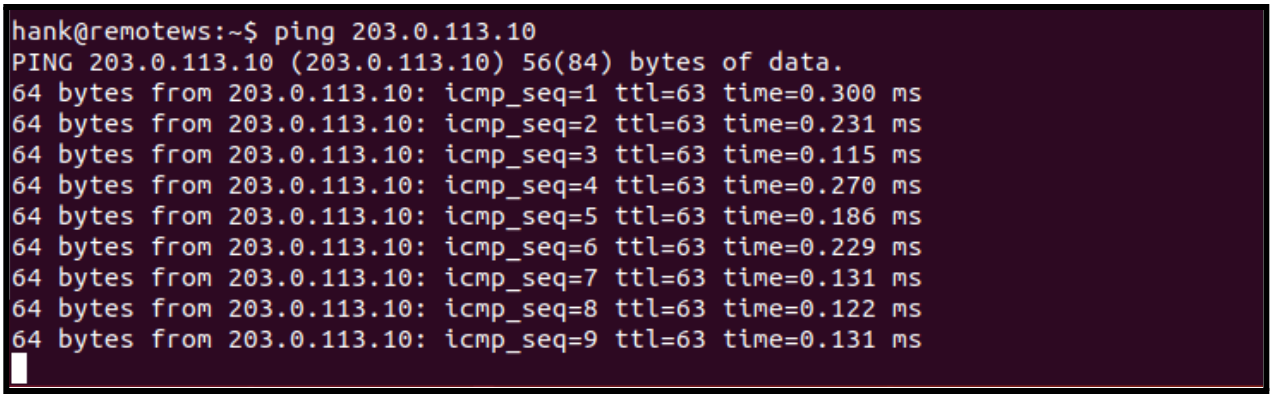
5. Service behind NAT

Used command: **sude iptable -L -v -t nat**

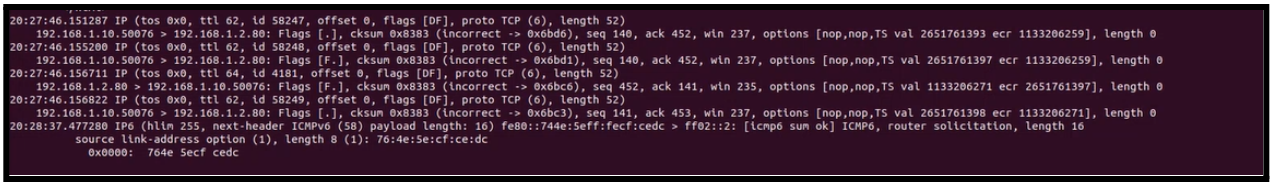
iptable of remote admin



Connecting the remote server to 203.0.113.10

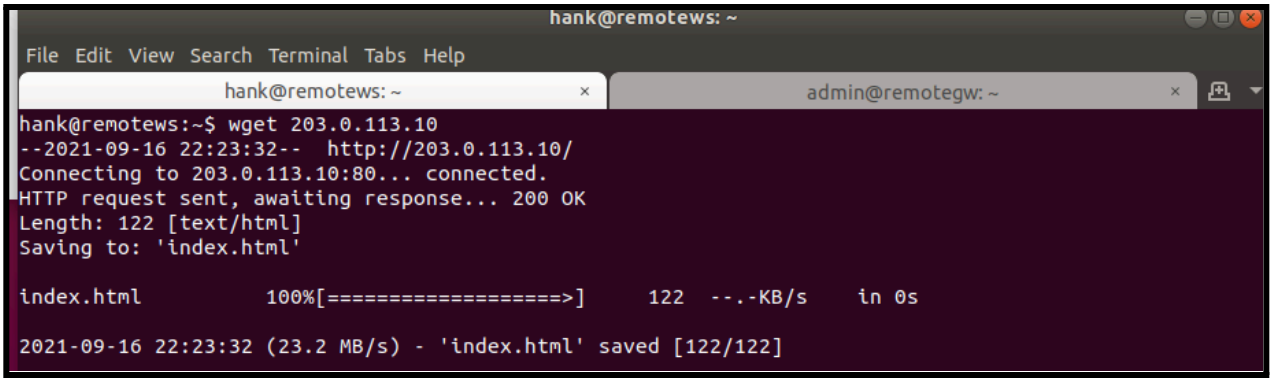


Using tcpdump showing the connection.



So we can not see ws1 from the remote survey. Thus protecting the ws1 server.

Used Command: **wget 203.0.113.10**
To get the webpage using a remote server.



Using the check lab and stop lab command.