

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.

```
ubuntu@box1:~$ ip addr
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
7: eth0@if8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:00:00:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.0.0.2/24 brd 172.0.0.255 scope global eth0
        valid_lft forever preferred_lft forever
ubuntu@box1:~$ 

ubuntu@box2:~$ ip addr
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
5: eth0@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:00:00:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.0.0.3/24 brd 172.0.0.255 scope global eth0
        valid_lft forever preferred_lft forever
ubuntu@box2:~$ 
```

2. ARP

Used command: **arp -a**

The Address Resolution Protocol (ARP) is used to map IP addresses to MAC addresses.

```
ubuntu@box2:~$ ip addr  
ubuntu@box2:~$ ip link  
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 brd 127.0.0.1 scope host lo  
        valid_lif forever preferred_lif forever  
10: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state UP group default  
    link/ether 02:42:ac:08:00:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0  
    inet 172.0.0.3/24 brd 172.0.0.255 scope global eth0  
        valid_lif forever preferred_lif forever  
ubuntu@box2:~$ arp -a
```

Nothing showed in box2.

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

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

```
Activities Terminal Fri 16:22
ubuntu@box1:~
```

File Edit View Search Terminal Help

```
ubuntu@box1:~$ ping -c 1 www.google.com
PING www.google.com (172.217.16.21) 56(84) bytes of data.
64 bytes from 172.217.16.21: icmp_seq=1 ttl=56 time=1.00 ms

--- www.google.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss
round-trip min/avg/max/stddev = 1.00/1.00/1.00/0.00 ms
```

```
ubuntu@box1:~$ sudo tcqdump -n -e -l eth0
tcqdmp: listening on eth0, link-type EN10MB (Ethernet), capture size 202144 bytes
23:21:52.084000 02:42:ac:00:00:03 > ffff:ffff:ffff:ff, ethertype ARP (0x0806), length 42: Ethernet (len 6), IPv4 (len 4), Request who-has 172.0.0.3 tell 172.0.0.3, length 28
23:21:52.084000 02:42:ac:00:00:03 > 02:42:ac:00:00:03, ethertype ARP (0x0806), length 42: Ethernet (len 6), IPv4 (len 4), Reply 172.0.0.2 is-at 02:42:ac:00:00:02, length 28
23:21:55.077777 02:42:ac:00:00:02 > 02:42:ac:00:00:03, ethertype ARP (0x0806), length 42: Ethernet (len 6), IPv4 (len 4), Reply 172.0.0.2 is-at 02:42:ac:00:00:02, length 28
23:21:55.077777 02:42:ac:00:00:03 > 02:42:ac:00:00:02, ethertype ARP (0x0806), length 42: Ethernet (len 6), IPv4 (len 4), Request who-has 172.0.0.3 tell 172.0.0.3, length 28
23:21:55.077777 02:42:ac:00:00:03 > 02:42:ac:00:00:02, ethertype ARP (0x0806), length 42: Ethernet (len 6), IPv4 (len 4), Reply 172.0.0.3 is-at 02:42:ac:00:00:02, length 28
23:21:56.099569 02:42:ac:00:00:03 > 02:42:ac:00:00:02, ethertype ARP (0x0806), length 42: Ethernet (len 6), IPv4 (len 4), Request who-has 172.0.0.3 tell 172.0.0.3, length 28
23:21:56.099569 02:42:ac:00:00:03 > 02:42:ac:00:00:02, ethertype ARP (0x0806), length 42: Ethernet (len 6), IPv4 (len 4), Reply 172.0.0.3 is-at 02:42:ac:00:00:02, length 28
23:22:00.163799 02:42:ac:00:00:02 > 02:42:ac:00:00:03, ethertype ARP (0x0806), length 42: Ethernet (len 6), IPv4 (len 4), Request who-has 172.0.0.3 tell 172.0.0.2, length 28
23:22:00.163799 02:42:ac:00:00:03 > 02:42:ac:00:00:02, ethertype ARP (0x0806), length 42: Ethernet (len 6), IPv4 (len 4), Reply 172.0.0.2 is-at 02:42:ac:00:00:03, length 28
23:22:00.163799 02:42:ac:00:00:03 > 02:42:ac:00:00:02, ethertype ARP (0x0806), length 42: Ethernet (len 6), IPv4 (len 4), Request who-has 172.0.0.3 tell 172.0.0.2, length 28
23:22:00.163799 02:42:ac:00:00:03 > 02:42:ac:00:00:02, ethertype ARP (0x0806), length 42: Ethernet (len 6), IPv4 (len 4), Reply 172.0.0.2 is-at 02:42:ac:00:00:03, length 28
outer solicitation, length 16
source link-address option (1), length 8 (1): 02:42:c6:4c:a639
02:42:c6:4c:a639
```

```
^C
13 packets captured
0 packets received by filter
0 packets dropped by kernel
ubuntu@box1:~$
```

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:

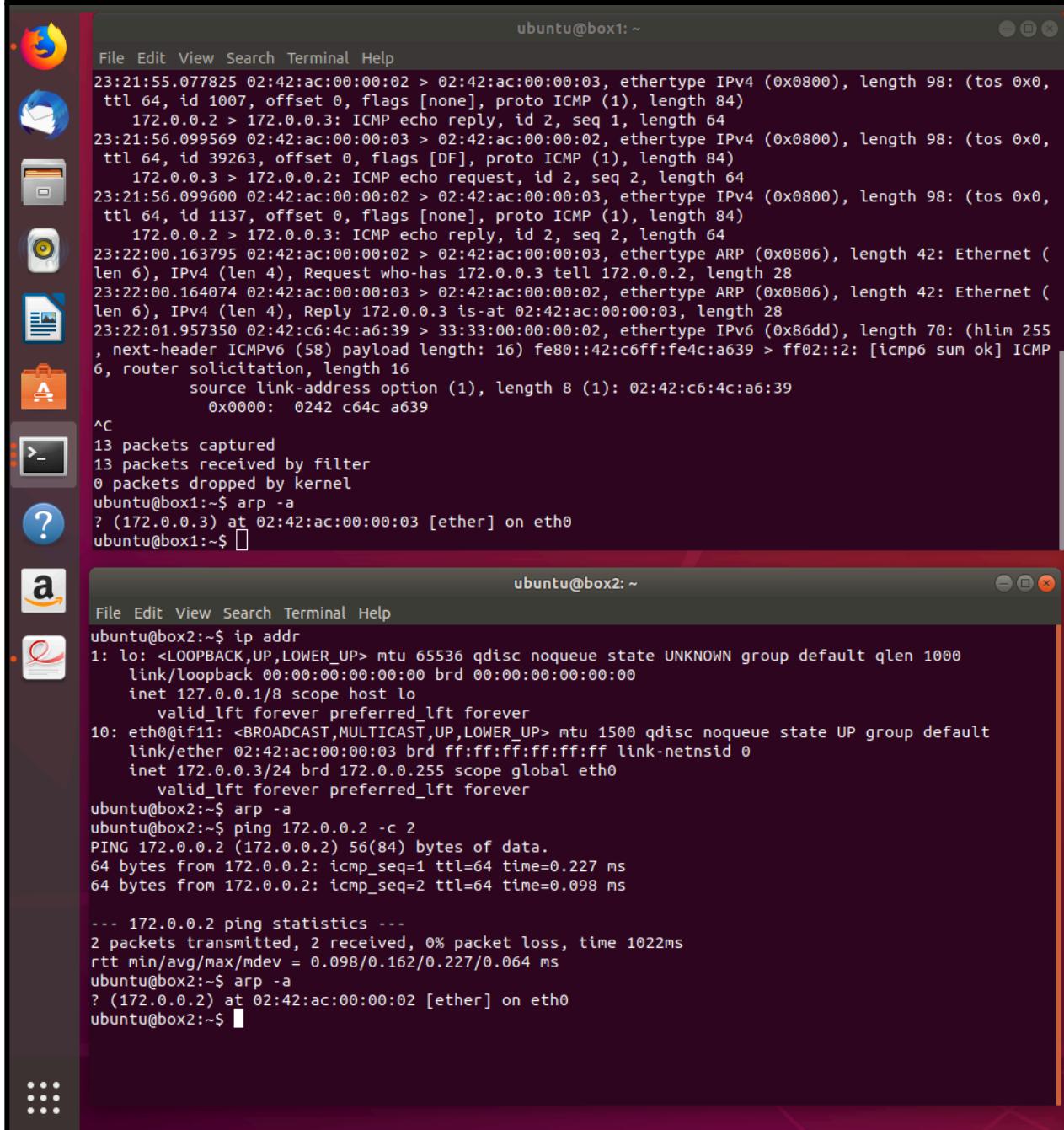
Used Command: **ping 172.0.0.2 -c 2**

```
Activities Terminal Fri 16:22
ubuntu@box2:~
```

File Edit View Search Terminal Help

```
ubuntu@box2:~$ ip addr
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 brd 127.0.0.1 scope host lo
        valid_lft forever preferred_lft forever
10: eth0@if11: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:00:00:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.0.0.3/24 brd 172.0.0.255 scope global eth0
        valid_lft forever preferred_lft forever
ubuntu@box2:~$ ping -c 2 172.0.0.2
PING 172.0.0.2 (172.0.0.2) 56(64) bytes of data.
64 bytes from 172.0.0.2: icmp_seq=1 ttl=64 time=0.227 ms
64 bytes from 172.0.0.2: icmp_seq=2 ttl=64 time=0.098 ms
--- 172.0.0.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1022ms
rtt min/avg/max/mdev = 0.098/0.162/0.227/0.064 ms
ubuntu@box2:~$
```

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



The image shows two terminal windows side-by-side. The left terminal window is titled "ubuntu@box1: ~" and displays the output of a packet capture. It shows several ICMP echo requests and replies between two hosts, followed by an ARP request from host 172.0.0.3 to find its own MAC address. The right terminal window is titled "ubuntu@box2: ~" and shows the results of an "arp -a" command, listing the MAC addresses of the interfaces on host 172.0.0.2. Below the terminals, the desktop environment's taskbar is visible with icons for various applications like a browser, file manager, and system monitor.

```
ubuntu@box1: ~
File Edit View Search Terminal Help
23:21:55.077825 02:42:ac:00:00:02 > 02:42:ac:00:00:03, ethertype IPv4 (0x0800), length 98: (tos 0x0,
ttl 64, id 1007, offset 0, flags [none], proto ICMP (1), length 84)
    172.0.0.2 > 172.0.0.3: ICMP echo reply, id 2, seq 1, length 64
23:21:56.099569 02:42:ac:00:00:03 > 02:42:ac:00:00:02, ethertype IPv4 (0x0800), length 98: (tos 0x0,
ttl 64, id 39263, offset 0, flags [DF], proto ICMP (1), length 84)
    172.0.0.3 > 172.0.0.2: ICMP echo request, id 2, seq 2, length 64
23:21:56.099600 02:42:ac:00:00:02 > 02:42:ac:00:00:03, ethertype IPv4 (0x0800), length 98: (tos 0x0,
ttl 64, id 1137, offset 0, flags [none], proto ICMP (1), length 84)
    172.0.0.2 > 172.0.0.3: ICMP echo reply, id 2, seq 2, length 64
23:22:00.163795 02:42:ac:00:00:02 > 02:42:ac:00:00:03, ethertype ARP (0x0806), length 42: Ethernet (len 6), IPv4 (len 4), Request who-has 172.0.0.3 tell 172.0.0.2, length 28
23:22:00.164074 02:42:ac:00:00:03 > 02:42:ac:00:00:02, ethertype ARP (0x0806), length 42: Ethernet (len 6), IPv4 (len 4), Reply 172.0.0.3 is-at 02:42:ac:00:00:03, length 28
23:22:01.957350 02:42:c6:4c:a6:39 > 33:33:00:00:00:02, ethertype IPv6 (0x86dd), length 70: (hlim 255
, next-header ICMPv6 (58) payload length: 16) fe80::42:c6ff:fe4c:a639 > ff02::2: [icmp6 sum ok] ICMP
6, router solicitation, length 16
    source link-address option (1), length 8 (1): 02:42:c6:4c:a6:39
    0x0000: 0242 c64c a639
^C
13 packets captured
13 packets received by filter
0 packets dropped by kernel
ubuntu@box1:~$ arp -a
? (172.0.0.3) at 02:42:ac:00:00:03 [ether] on eth0
ubuntu@box1:~$ 
```



```
ubuntu@box2: ~
File Edit View Search Terminal Help
ubuntu@box2:~$ ip addr
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
10: eth0@if11: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:00:00:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
        inet 172.0.0.3/24 brd 172.0.0.255 scope global eth0
            valid_lft forever preferred_lft forever
ubuntu@box2:~$ arp -a
ubuntu@box2:~$ ping 172.0.0.2 -c 2
PING 172.0.0.2 (172.0.0.2) 56(84) bytes of data.
64 bytes from 172.0.0.2: icmp_seq=1 ttl=64 time=0.227 ms
64 bytes from 172.0.0.2: icmp_seq=2 ttl=64 time=0.098 ms

--- 172.0.0.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1022ms
rtt min/avg/max/mdev = 0.098/0.162/0.227/0.064 ms
ubuntu@box2:~$ arp -a
? (172.0.0.2) at 02:42:ac:00:00:02 [ether] on eth0
ubuntu@box2:~$ 
```

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`

```
Fri 16:32
ubuntu@box1:~$ sudo tcpdump -vv -n -i eth0
23:26:00.255357 IP (tos 0x0, ttl 64, id 58427, offset 0, flags [DF], proto TCP (6), length 93)
    172.0.0.3.40446 > 172.0.0.2.55357: Flags [.], cksum 0x585b (incorrect -> 0xb12d), seq 1:42, ack 1, win 229, options [nop,nop,T5 val 1812282954 ecr 2551613768], length 41
23:26:00.255371 IP (tos 0x0, ttl 64, id 58428, offset 0, flags [DF], proto TCP (6), length 93)
    172.0.0.2.23 > 172.0.0.3.40446: Flags [.], cksum 0x585b (incorrect -> 0xb12d), seq 1:42, ack 2, win 227, options [nop,nop,T5 val 2551613769 ecr 1812282954], length 0
23:26:00.302991 IP (tos 0x0, ttl 64, id 40912, offset 0, flags [DF], proto TCP (6), length 93)
    172.0.0.2.23 > 172.0.0.3.40446: Flags [.], cksum 0x585b (incorrect -> 0xb12d), seq 1:42, ack 2, win 227, options [nop,nop,T5 val 2551613817 ecr 1812282954], length 41
23:26:00.303068 IP (tos 0x0, ttl 64, id 58428, offset 0, flags [DF], proto TCP (6), length 52)
    172.0.0.3.40446 > 172.0.0.2.22: Flags [.], cksum 0x585c (incorrect -> 0x92d5), seq 42:44, ack 42, win 229, options [nop,nop,T5 val 1812283002 ecr 2551613817], length 0
23:26:00.303071 IP (tos 0x0, ttl 64, id 40913, offset 0, flags [DF], proto TCP (6), length 1512)
    172.0.0.3.40446 > 172.0.0.2.22: Flags [.], cksum 0x585c (incorrect -> 0x92d5), seq 42:1554, ack 42, win 229, options [nop,nop,T5 val 1812283003 ecr 2551613817], length 1512
    172.0.0.3.40446 > 172.0.0.2.22: Flags [.], cksum 0x585c (incorrect -> 0x92d5), seq 42:1554, ack 42, win 1554, options [nop,nop,T5 val 2551613818 ecr 1812283003], length 0
23:26:00.308319 IP (tos 0x0, ttl 64, id 40914, offset 0, flags [DF], proto TCP (6), length 108)
23:26:00.308321 IP (tos 0x0, ttl 64, id 40914, offset 0, flags [DF], proto TCP (6), length 108)
    172.0.0.3.40446 > 172.0.0.2.22: Flags [.], cksum 0x585c (incorrect -> 0x92d5), seq 42:1098, ack 1554, win 250, options [nop,nop,T5 val 2551613822 ecr 1812283003], length 1056
23:26:00.308321 IP (tos 0x0, ttl 64, id 40914, offset 0, flags [DF], proto TCP (6), length 108)
    172.0.0.3.40446 > 172.0.0.2.22: Flags [.], cksum 0x585c (incorrect -> 0x92d5), seq 42:1098, ack 1554, win 250, options [nop,nop,T5 val 2551613822 ecr 1812283003], length 1056
23:26:00.325863 IP (tos 0x0, ttl 64, id 40915, offset 0, flags [DF], proto TCP (6), length 560)
    172.0.0.3.40446 > 172.0.0.2.22: Flags [.], cksum 0x585c (incorrect -> 0x92d5), seq 42:1098, ack 1602, win 250, options [nop,nop,T5 val 2551613822 ecr 1812283014], length 48
23:26:00.367516 IP (tos 0x0, ttl 64, id 58432, offset 0, flags [DF], proto TCP (6), length 52)
    172.0.0.3.40446 > 172.0.0.2.22: Flags [.], cksum 0x585c (incorrect -> 0x92d5), seq 42:1098, ack 1602, win 262, options [nop,nop,T5 val 1812283007 ecr 2551613840], length 0
    172.0.0.3.40446 > 172.0.0.2.22: Flags [.], cksum 0x585c (incorrect -> 0x92d5), seq 42:1098, ack 1602, win 262, options [nop,nop,T5 val 1812283007 ecr 2551613840], length 0
23:26:05.411785 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 172.0.0.2 tell 172.0.0.3, length 28
23:26:05.411797 ARP, Ethernet (len 6), IPv4 (len 4), Reply 172.0.0.2 is-at 02:42:ac:00:00:02, length 28
23:26:05.411806 ARP, Ethernet (len 6), IPv4 (len 4), Reply 172.0.0.3 is-at 02:42:ac:00:00:03, length 28
23:26:24.101607 IP6 (hlim 255, next-header ICMPv6 (58) payload length: 16) fe80::42:6ff:fe4:a639 > fe80::42:6ff:fe4:a639 [icmp6 sum ok] ICMP6, router solicitation, length 16
    source address option (1), length 8 (1): 02:42:6c:04:4c:a639
^C
32 packets captured
32 packets received by filter
0 packets dropped by kernel
ubuntu@box1:~$
```

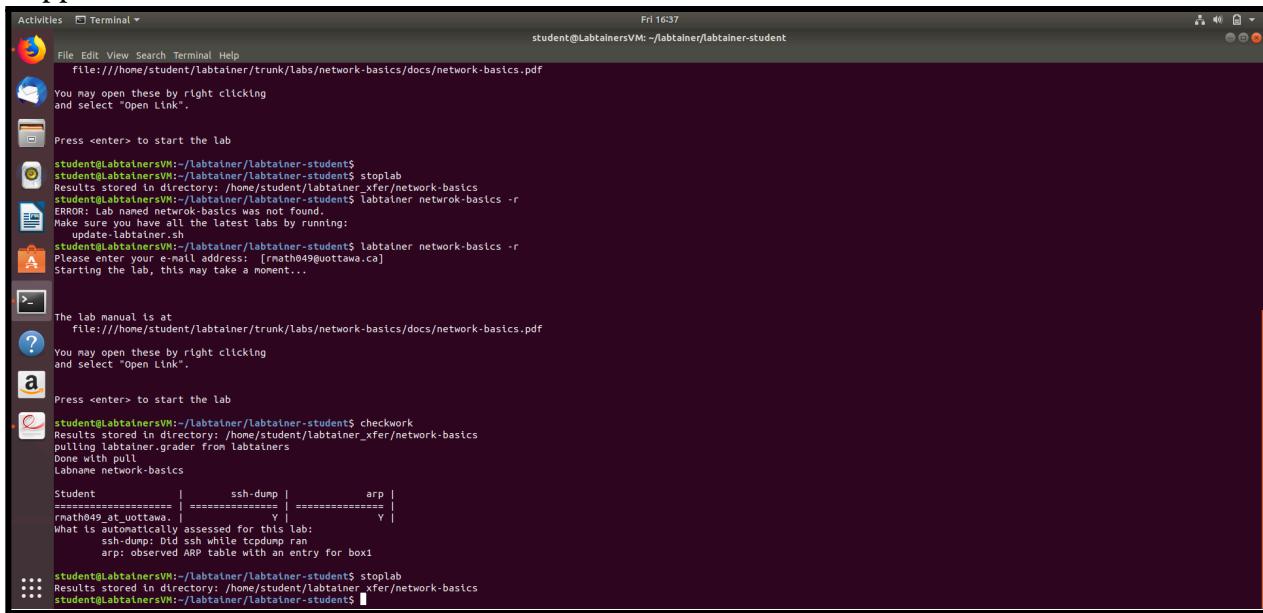
Then, on box2, initiate an ssh session to box1. As we wish to look at the start of the session:

Used Command: `ssh 172.0.0.2`

```
Fri 16:32
ubuntu@box2:~$ ssh 172.0.0.2
File Edit View Search Terminal Help
ubuntu@box2:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 5356 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 brd 127.0.0.1 scope host lo
        valid_lft forever preferred_lft forever
10: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 56:84:7a brd ff:ff:ff:ff:ff:ff brd ff:ff:ff:ff:ff:ff
    inet 172.0.0.2/24 brd 172.0.0.255 scope global eth0
        valid_lft forever preferred_lft forever
ubuntu@box2:~$ arp -a
ubuntu@box2:~$ ping 172.0.0.2 -c 2
PING 172.0.0.2 (172.0.0.2) 56(84) bytes of data.
64 bytes from 172.0.0.2: icmp_seq=1 ttl=4 time=0.227 ms
64 bytes from 172.0.0.2: icmp_seq=2 ttl=4 time=0.098 ms
...
172.0.0.2 ping statistics ...
2 packets transmitted, 2 received, 0% packet loss, time 1022ms
rtt min/avg/max/mdev = 0.098/0.162/0.227/0.064 ms
? (172.0.0.2) at 02:42:ac:00:00:02 [ether] on eth0
ubuntu@box2:~$ ssh 172.0.0.2
The authenticity of host '172.0.0.2 (172.0.0.2)' can't be established.
ECDSA key fingerprint is SHA256:ZtE8xi5Y50aUktZ/XtgjIs1c5jxYQB84Vq5ofmlgGng.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.0.0.2' (ECDSA) to the list of known hosts.
ssh_dispatch_run_fatal: Connection to 172.0.0.2 port 22: Broken pipe
ubuntu@box2:~$
```

```
ubuntu@box2:~$ ssh 172.0.0.2
The authenticity of host '172.0.0.2 (172.0.0.2)' can't be established.
ECDSA key fingerprint is SHA256:ZtE8xi5Y50aUktZ/XtgjIs1c5jxYQB84Vq5ofmlgGng.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.0.0.2' (ECDSA) to the list of known hosts.
ssh_dispatch_run_fatal: Connection to 172.0.0.2 port 22: Broken pipe
ubuntu@box2:~$
```

Stopped the Lab and checked the work at the end.



The screenshot shows a terminal window titled "Terminal" with the command "student@LabtainerVM: ~/labtainer/labtainer-student\$". The window displays the following output:

```
File Edit View Search Terminal Help
Fri 16:37
student@LabtainerVM: ~/labtainer/labtainer-student$ file:///home/student/labtainer/trunk/labs/network-basics/docs/network-basics.pdf
You may open these by right clicking and select "Open Link".
Press <enter> to start the lab
student@LabtainerVM:~/labtainer/labtainer-student$ stoplab
Results stored in directory: /home/student/labtainer_xfer/network-basics
student@LabtainerVM:~/labtainer/labtainer-student$ labtainer network-basics -r
ERROR: Lab named network-basics was not found.
Make sure you have all the latest tabs by running:
    updated_labtainer.sh
student@LabtainerVM:~/labtainer/labtainer-student$ labtainer network-basics -r
Please enter your e-mail address: [rnath049@ottawa.ca]
Starting the lab, this may take a moment...
The lab manual ls at
file:///home/student/labtainer/trunk/labs/network-basics/docs/network-basics.pdf
You may open these by right clicking and select "Open Link".
a
Press <enter> to start the lab
student@LabtainerVM:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/network-basics
pulling labtainer.grader from labtainers
Done with pull
Labname network-basics
Student | ssh-dump | arp |
===== | ===== | ===== |
rnath049_at_ottawa | | Y |
What is automatically assessed for this lab:
ssh-dump: Did ssh while tcpreplay ran
arp: observed ARP table with an entry for box1
student@LabtainerVM:~/labtainer/labtainer-student$ stoplab
Results stored in directory: /home/student/labtainer_xfer/network-basics
student@LabtainerVM:~/labtainer/labtainer-student$
```

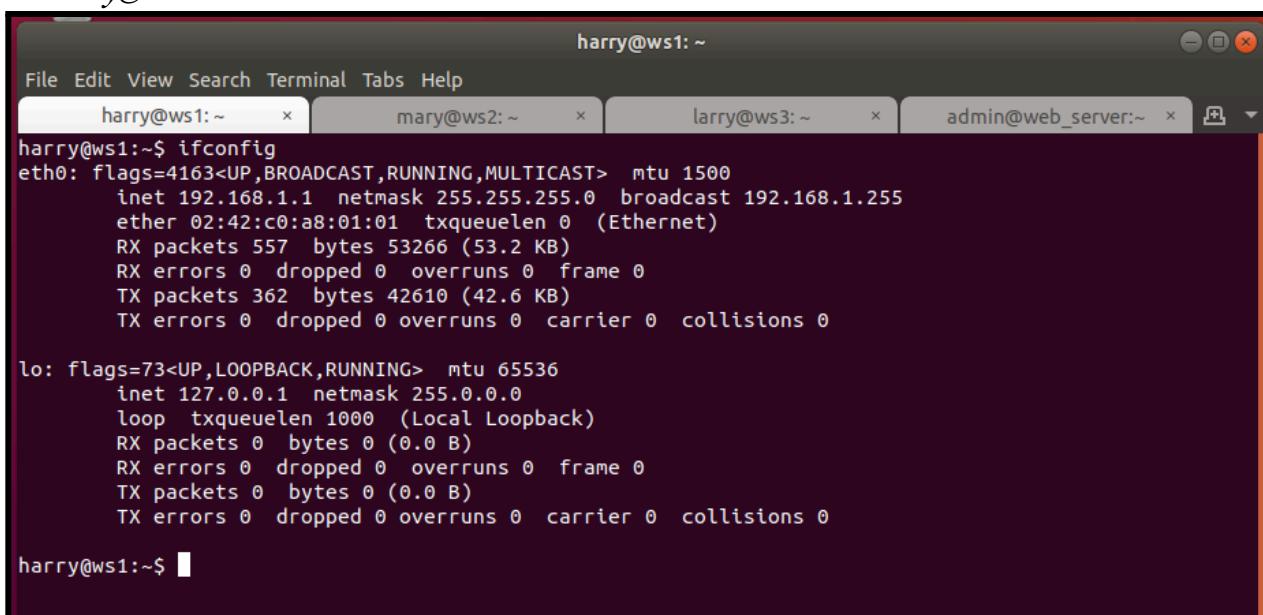
Part 2- Routing Basics

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



The screenshot shows a desktop environment with four terminal tabs open:

- harry@ws1: ~
- mary@ws2: ~
- larry@ws3: ~
- admin@web_server: ~

The "harry@ws1: ~" tab is active and displays the output of the "ifconfig" command:

```
harry@ws1:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.1.1 netmask 255.255.255.0 broadcast 192.168.1.255
                ether 02:42:c0:a8:01:01 txqueuelen 0 (Ethernet)
                RX packets 557 bytes 53266 (53.2 KB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 362 bytes 42610 (42.6 KB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                loop txqueuelen 1000 (Local Loopback)
                RX packets 0 bytes 0 (0.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 0 bytes 0 (0.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

harry@ws1:~$
```

On mary@ws2

```
mary@ws2:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.2.1 netmask 255.255.255.0 broadcast 192.168.2.255
                ether 02:42:c0:a8:02:01 txqueuelen 0 (Ethernet)
                RX packets 81 bytes 9392 (9.3 KB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 0 bytes 0 (0.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                loop txqueuelen 1000 (Local Loopback)
                RX packets 0 bytes 0 (0.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 0 bytes 0 (0.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

mary@ws2:~$
```

On larry@ws3

```
larry@ws3:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.2.2 netmask 255.255.255.0 broadcast 192.168.2.255
                ether 02:42:c0:a8:02:02 txqueuelen 0 (Ethernet)
                RX packets 59 bytes 6235 (6.2 KB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 0 bytes 0 (0.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                loop txqueuelen 1000 (Local Loopback)
                RX packets 0 bytes 0 (0.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 0 bytes 0 (0.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

On admin@web_server

```
Last login: Wed Sep 15 03:57:51 UTC 2021
[admin@web_server ~]$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.1.2 netmask 255.255.255.0 broadcast 192.168.1.255
                ether 02:42:c0:a8:01:02 txqueuelen 0 (Ethernet)
                RX packets 57 bytes 5843 (5.7 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 0 bytes 0 (0.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                loop txqueuelen 1000 (Local Loopback)
                RX packets 0 bytes 0 (0.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 0 bytes 0 (0.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

On hank@remotews

```

hank@remotews:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.0.1 netmask 255.255.255.0 broadcast 172.16.0.255
        ether 02:42:ac:10:00:01 txqueuelen 0 (Ethernet)
        RX packets 65 bytes 7061 (7.0 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        loop txqueuelen 1000 (Local Loopback)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

On admin@remotegw

```

admin@remotegw:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.0.10 netmask 255.255.255.0 broadcast 172.16.0.255
        ether 02:42:ac:10:00:0a txqueuelen 0 (Ethernet)
        RX packets 56 bytes 5773 (5.7 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 203.0.113.20 netmask 255.255.255.0 broadcast 203.0.113.255
        ether 02:42:c8:00:71:14 txqueuelen 0 (Ethernet)
        RX packets 56 bytes 5773 (5.7 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        loop txqueuelen 1000 (Local Loopback)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

On admin@gateway

```

File Edit View Search Terminal Help
admin@gateway:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.10 netmask 255.255.255.0 broadcast 192.168.1.255
        ether 02:42:c8:a8:01:0a txqueuelen 0 (Ethernet)
        RX packets 56 bytes 5773 (5.7 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.2.10 netmask 255.255.255.0 broadcast 192.168.2.255
        ether 02:42:c8:a8:02:0a txqueuelen 0 (Ethernet)
        RX packets 60 bytes 6342 (6.3 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 203.0.113.10 netmask 255.255.255.0 broadcast 203.0.113.255
        ether 02:42:c8:00:71:0a txqueuelen 0 (Ethernet)
        RX packets 58 bytes 5993 (5.9 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        loop txqueuelen 1000 (Local Loopback)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

2. Internal Packet Forwarding

Used command: **route -n**

This shows the routing table for all three web servers.

ws1 has a default gateway.

```
harry@ws1:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.10   0.0.0.0        UG    0      0        0 eth0
192.168.1.0    0.0.0.0        255.255.255.0  U     0      0        0 eth0
harry@ws1:~$
```

ws2 has a default gateway as well.

```
mary@ws2:~$ 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
mary@ws2:~$
```

ws3 has no default gateway.

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

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

```
admin@gateway:~$ sudo tcpdump -i eth0 -n -vv
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
admin@gateway:~$
```

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 via the gateways and can also be seen in the tcpdump of the admin.

```

admin@gateway:~$ sudo tcpdump -i eth0 -n -vv
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 202144 bytes
21:12:10.075382 IP (tos 0x0, ttl 255, next-header UDP (17) payload length: 53) fe80::42:15
    .fe26:23ff:ff! > fe80::fe2c:fb.5e8b [bad udp cksum 0xaxb4 -> 0x5959] 0 [24] PTR (QH?) _lpp$._tcp.loc
al PTR (QH?) _lpp$._tcp.local. (45)
21:12:10.075382 IPP (tos 0x0, ttl 255, next-header UDP (17) payload length: 53) fe80::42:15
    .fe26:23ff:ff! > fe80::fe2c:fb.5e8b [bad udp cksum 0xaxb4 -> 0x5959] 0 [24] PTR (QH?) _lpp$._tcp.loc
al PTR (QH?) _lpp$._tcp.local. (45)
21:13:31.079751 IP6 (hlim 255, next-header ICMPV6 (58) payload length: 16) fe80::bcf:39ff:fe2c:a1f5
> ff02::1:21.1.1.1 ICMPv6 Router solicitation, length 16
    source link-layer option (1), length 8 (1): be:39:2c:af:15
        ox0000: be:39:2c:af:15
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 ls-at 02:42:c0:a8:01:0a, leng
th 28
21:13:40.103919 IP (tos 0x0, ttl 64, id 51096, 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
21:13:40.104063 IP (tos 0x0, ttl 63, id 61030, 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
21:13:41.128438 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
21:13:41.151774 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
21:13:42.020126 IP (tos 0x0, ttl 63, id 61020, offset 0, flags [DF], 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
21:13:43.175925 IP (tos 0x0, ttl 64, id 61482, 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)
    192.168.2.1 > 192.168.1.1: 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)
    192.168.1.1 > 192.168.2.1: 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
21:13:45.159549 ARP, Ethernet (len 6), IPv4 (len 4), Reply 192.168.1.1 ls-at 02:42:c0:a8:01:01, leng
th 28
21:13:45.223058 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
21:13:45.223058 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
21:13:45.223058 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 7, length 64

```

Zoomed- the ping command from ws1 to ws2

```

harry@ws1:~$ ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=63 time=0.506 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=63 time=0.199 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=63 time=0.250 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=63 time=0.341 ms
64 bytes from 192.168.2.1: icmp_seq=5 ttl=63 time=0.371 ms
64 bytes from 192.168.2.1: icmp_seq=6 ttl=63 time=0.186 ms
64 bytes from 192.168.2.1: icmp_seq=7 ttl=63 time=0.535 ms
64 bytes from 192.168.2.1: icmp_seq=8 ttl=63 time=0.223 ms
64 bytes from 192.168.2.1: icmp_seq=9 ttl=63 time=0.504 ms
64 bytes from 192.168.2.1: icmp_seq=10 ttl=63 time=0.268 ms
64 bytes from 192.168.2.1: icmp_seq=11 ttl=63 time=0.269 ms
64 bytes from 192.168.2.1: icmp_seq=12 ttl=63 time=0.163 ms
64 bytes from 192.168.2.1: icmp_seq=13 ttl=63 time=0.151 ms
64 bytes from 192.168.2.1: icmp_seq=14 ttl=63 time=0.297 ms
64 bytes from 192.168.2.1: icmp_seq=15 ttl=63 time=0.177 ms
64 bytes from 192.168.2.1: icmp_seq=16 ttl=63 time=0.210 ms
64 bytes from 192.168.2.1: icmp_seq=17 ttl=63 time=0.210 ms
64 bytes from 192.168.2.1: icmp_seq=18 ttl=63 time=0.170 ms
64 bytes from 192.168.2.1: icmp_seq=19 ttl=63 time=0.170 ms
64 bytes from 192.168.2.1: icmp_seq=20 ttl=63 time=0.170 ms
64 bytes from 192.168.2.1: icmp_seq=21 ttl=63 time=0.436 ms
64 bytes from 192.168.2.1: icmp_seq=22 ttl=63 time=0.172 ms
64 bytes from 192.168.2.1: icmp_seq=23 ttl=63 time=0.172 ms
64 bytes from 192.168.2.1: icmp_seq=24 ttl=63 time=0.194 ms
64 bytes from 192.168.2.1: icmp_seq=25 ttl=63 time=0.098 ms
64 bytes from 192.168.2.1: icmp_seq=26 ttl=63 time=0.123 ms
64 bytes from 192.168.2.1: icmp_seq=27 ttl=63 time=0.123 ms
64 bytes from 192.168.2.1: icmp_seq=28 ttl=63 time=0.282 ms
64 bytes from 192.168.2.1: icmp_seq=29 ttl=63 time=0.135 ms
64 bytes from 192.168.2.1: icmp_seq=30 ttl=63 time=0.111 ms
64 bytes from 192.168.2.1: icmp_seq=31 ttl=63 time=0.145 ms
64 bytes from 192.168.2.1: icmp_seq=32 ttl=63 time=0.228 ms
64 bytes from 192.168.2.1: icmp_seq=33 ttl=63 time=0.228 ms
64 bytes from 192.168.2.1: icmp_seq=34 ttl=63 time=0.224 ms
64 bytes from 192.168.2.1: icmp_seq=35 ttl=63 time=0.205 ms
64 bytes from 192.168.2.1: icmp_seq=36 ttl=63 time=0.307 ms
64 bytes from 192.168.2.1: icmp_seq=37 ttl=63 time=0.172 ms
64 bytes from 192.168.2.1: icmp_seq=38 ttl=63 time=0.273 ms
64 bytes from 192.168.2.1: icmp_seq=39 ttl=63 time=0.154 ms

```

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 ls-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
21:13:41.128239 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
21:13:42.020126 IP (tos 0x0, ttl 64, id 61616, offset 0, flags [none], proto ICMP (1), length 84)
    192.168.1.1 > 192.168.2.1: ICMP echo request, id 1, seq 3, length 64
21:13:42.020126 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
21:13:43.175925 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

```

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

	tx packets 0 bytes 0 (0.0 B)	rx packets 0 bytes 0 (0.0 B)
21:18:18.001327 IP (tos 0x0, ttl 64, id 30866, offset 0, flags [DF], proto ICMP (1), length 84)		
192.168.1.1 -> 192.168.2.1: ICMP echo request, id 1, seq 271, length 64		
21:18:18.001368 IP (tos 0x0, ttl 63, id 29896, offset 0, flags [none], proto ICMP (1), length 84)		
192.168.2.1 -> 192.168.1.1: ICMP echo reply, id 1, seq 271, length 64		
21:18:19.015699 IP (tos 0x0, ttl 64, id 31062, offset 0, flags [DF], proto ICMP (1), length 84)		
192.168.1.1 -> 192.168.2.1: ICMP echo request, id 1, seq 272, length 64		
21:18:19.015653 IP (tos 0x0, ttl 63, id 30118, offset 0, flags [none], proto ICMP (1), length 84)		
192.168.2.1 -> 192.168.1.1: ICMP echo reply, id 1, seq 272, length 64		
21:18:20.041121 IP (tos 0x0, ttl 64, id 31261, offset 0, flags [DF], proto ICMP (1), length 84)		
192.168.1.1 -> 192.168.2.1: ICMP echo request, id 1, seq 273, length 64		
21:18:20.041309 IP (tos 0x0, ttl 63, id 30255, offset 0, flags [none], proto ICMP (1), length 84)		
192.168.2.1 -> 192.168.1.1: ICMP echo reply, id 1, seq 273, length 64		
21:18:21.050233 IP (tos 0x0, ttl 64, id 31327, offset 0, flags [DF], proto ICMP (1), length 84)		
192.168.1.1 -> 192.168.2.1: ICMP echo request, id 1, seq 274, length 64		
21:18:21.050260 IP (tos 0x0, ttl 63, id 30246, offset 0, flags [DF], proto ICMP (1), length 84)		
192.168.2.1 -> 192.168.1.1: ICMP echo reply, id 1, seq 274, length 64		
21:18:22.051427 IP (tos 0x0, ttl 64, id 31473, offset 0, flags [DF], proto ICMP (1), length 84)		
192.168.1.1 -> 192.168.2.1: ICMP echo request, id 1, seq 275, length 64		
21:18:22.051471 IP (tos 0x0, ttl 63, id 30673, offset 0, flags [none], proto ICMP (1), length 84)		
192.168.2.1 -> 192.168.1.1: ICMP echo reply, id 1, seq 275, length 64		
21:18:23.079770 IP (tos 0x0, ttl 64, id 31539, offset 0, flags [DF], proto ICMP (1), length 84)		
192.168.1.1 -> 192.168.2.1: ICMP echo request, id 1, seq 276, length 64		
21:18:23.079794 IP (tos 0x0, ttl 63, id 30846, offset 0, flags [DF], proto ICMP (1), length 84)		
192.168.2.1 -> 192.168.1.1: ICMP echo reply, id 1, seq 276, length 64		
21:18:24.107750 IP (tos 0x0, ttl 64, id 31686, offset 0, flags [DF], proto ICMP (1), length 84)		
192.168.1.1 -> 192.168.2.1: ICMP echo request, id 1, seq 277, length 64		
21:18:24.107807 IP (tos 0x0, ttl 63, id 31075, offset 0, flags [none], proto ICMP (1), length 84)		
192.168.2.1 -> 192.168.1.1: ICMP echo reply, id 1, seq 277, length 64		
21:18:25.132353 IP (tos 0x0, ttl 64, id 31913, offset 0, flags [DF], proto ICMP (1), length 84)		
192.168.1.1 -> 192.168.2.1: ICMP echo request, id 1, seq 278, length 64		
21:18:25.132465 IP (tos 0x0, ttl 63, id 31327, offset 0, flags [none], proto ICMP (1), length 84)		

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:~$
```

Lab Report-1 Network And Routing Basics

```
File Edit View Search Terminal Help
GNU nano 4.8
admin@gateway: ~
#!/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($1)-1)}')
wan2=$(ifconfig | grep -B1 "inet.*192.168.2.10" | awk '$1!="inet" && $1!="-" {print substr($1,1,length($1)-1)}')
wan=5$(ifconfig | grep -B1 "inet.*203.0.113.10" | awk '$1!="inet" && $1!="-" {print substr($1,1,length($1)-1)})'
#
# Delete all IPTABLES 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.

```
11:42:17.017707 IP (tos 0x0, ttl 64, id 14229, offset 0, flags [DF], proto UDP (17), length 60)
    192.168.1.1.48598 > 192.168.1.10.53: [bad udp csum 0x8395 -> 0x7344!] 48202+ A? www.google.com. (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 csum 0x8395 -> 0x6ffc!] 49015+ AAAA? www.google.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 csum 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 csum 0x83b1 -> 0x3a37!] 49015 q: AAAA? www.google.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 [.], 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, 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.

```
hank@remotews:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
From 172.16.0.10 icmp_seq=1 Destination Net Unreachable
From 172.16.0.10 icmp_seq=2 Destination Net Unreachable
From 172.16.0.10 icmp_seq=3 Destination Net Unreachable
From 172.16.0.10 icmp_seq=4 Destination Net Unreachable
```

5. Service behind NAT

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

iptable of remote admin

```
admin@remotegw:~$ sudo iptables -L -v -t nat
Chain PREROUTING (policy ACCEPT 135 packets, 11230 bytes)
  pkts bytes target     prot opt in     out     source          destination
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source          destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source          destination
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source          destination
    0     0 MASQUERADE  all  --  any    eth1    anywhere      anywhere
```

Connecting the remote server to 203.0.113.10

```
hank@remotews:~$ ping 203.0.113.10
PING 203.0.113.10 (203.0.113.10) 56(84) bytes of data.
64 bytes from 203.0.113.10: icmp_seq=1 ttl=63 time=0.300 ms
64 bytes from 203.0.113.10: icmp_seq=2 ttl=63 time=0.231 ms
64 bytes from 203.0.113.10: icmp_seq=3 ttl=63 time=0.115 ms
64 bytes from 203.0.113.10: icmp_seq=4 ttl=63 time=0.270 ms
64 bytes from 203.0.113.10: icmp_seq=5 ttl=63 time=0.186 ms
64 bytes from 203.0.113.10: icmp_seq=6 ttl=63 time=0.229 ms
64 bytes from 203.0.113.10: icmp_seq=7 ttl=63 time=0.131 ms
64 bytes from 203.0.113.10: icmp_seq=8 ttl=63 time=0.122 ms
64 bytes from 203.0.113.10: icmp_seq=9 ttl=63 time=0.131 ms
```

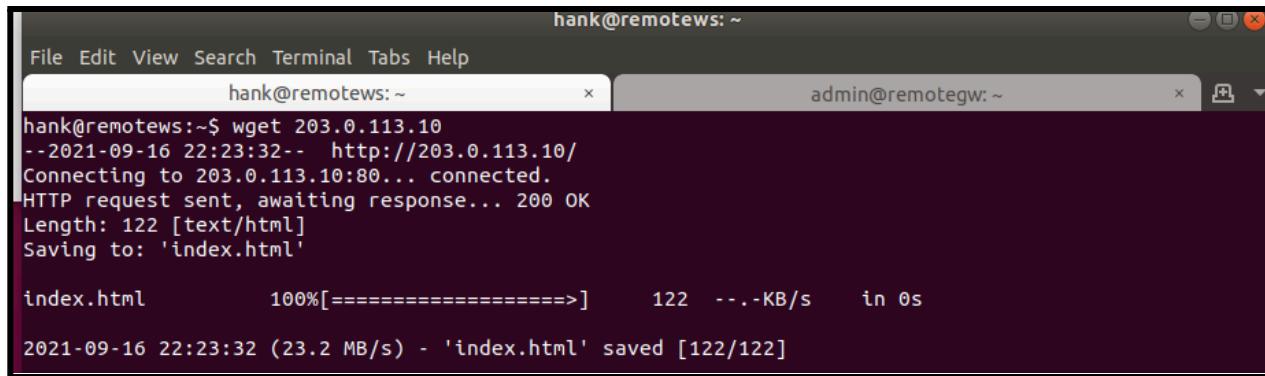
Using tcpdump showing the connection.

```
20:27:46.151287 IP (tos 0x0, ttl 62, id 58247, offset 0, flags [DF], proto TCP (6), length 52)
  192.168.1.10.50076 > 192.168.1.2.80: Flags [.], cksum 0x8383 (incorrect -> 0xb6d6), seq 140, ack 452, win 237, options [nop,nop,TS val 2651761393 ecr 1133206259], length 0
20:27:46.155208 IP (tos 0x0, ttl 62, id 58248, offset 0, flags [DF], proto TCP (6), length 52)
  192.168.1.10.50076 > 192.168.1.2.80: Flags [F.], cksum 0x8383 (incorrect -> 0xb6d1), seq 140, ack 452, win 237, options [nop,nop,TS val 2651761397 ecr 1133206259], length 0
20:27:46.156711 IP (tos 0x0, ttl 64, id 4181, offset 0, flags [DF], proto TCP (6), length 52)
  192.168.1.2.80 > 192.168.1.10.50076: Flags [.], cksum 0x8383 (incorrect -> 0xbc6), seq 452, ack 141, win 235, options [nop,nop,TS val 1133206271 ecr 2651761397], length 0
20:27:46.156822 IP (tos 0x0, ttl 62, id 58249, offset 0, flags [DF], proto TCP (6), length 52)
  192.168.1.10.50076 > 192.168.1.2.80: Flags [.], cksum 0x8383 (incorrect -> 0xb6c3), seq 141, ack 453, win 237, options [nop,nop,TS val 2651761398 ecr 1133206271], length 0
20:28:37.477280 IP6 (hlim 255, next_header ICMPv6 (58) payload length: 16) fe80::744e:5eff:fedc>ff02::2: [icmp6 sum ok] ICMP6, router solicitation, length 16
  source link-layer option (1), length 8 (i): 76:4e:5e:cfc:edc
  source link-layer option (1), length 8 (i): 0x0000: 764 Secf cedc
```

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.

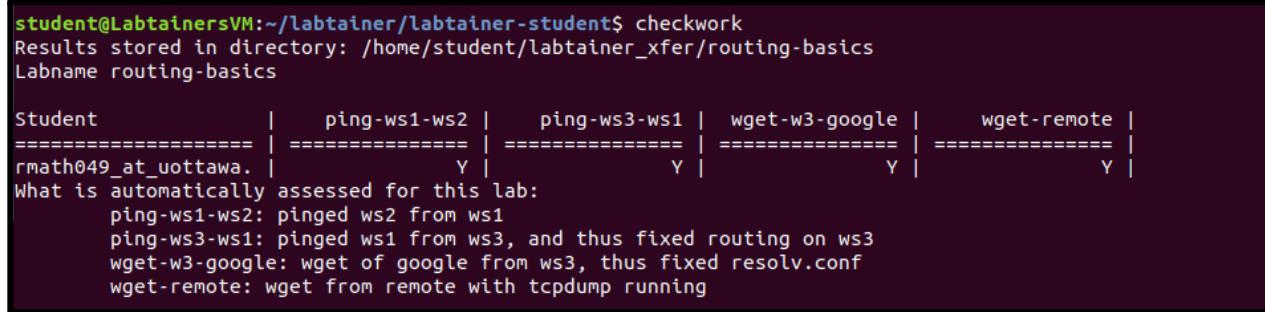


```
hank@remotews: ~
File Edit View Search Terminal Tabs Help
hank@remotews: ~ x admin@remotegw: ~ x
hank@remotews:~$ wget 203.0.113.10
--2021-09-16 22:23:32-- http://203.0.113.10/
Connecting to 203.0.113.10:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 122 [text/html]
Saving to: 'index.html'

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

2021-09-16 22:23:32 (23.2 MB/s) - 'index.html' saved [122/122]
```

Using the check lab and stop lab command.



```
student@LabtainerVM:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/routing-basics
Labname routing-basics

Student          | ping-ws1-ws2 | ping-ws3-ws1 | wget-w3-google | wget-remote |
===== | ===== | ===== | ===== | ===== |
rmath049_at_uottawa. | Y | Y | Y | Y |
What is automatically assessed for this lab:
    ping-ws1-ws2: pinged ws2 from ws1
    ping-ws3-ws1: pinged ws1 from ws3, and thus fixed routing on ws3
    wget-w3-google: wget of google from ws3, thus fixed resolv.conf
    wget-remote: wget from remote with tcpdump running
```