Lab 1 – Introduction to Networking Concepts

Shrutika Joshi

University of Maryland Baltimore County

Presented To – Ian Coston

Date – 14th SEP 2023

Introduction

In this lab, you will be running different commands to check network configuration and to become familiar with the commands built-in and networking concepts such as routing and ports.

Pre-Lab

For this lab, you will require kali Linux and windows

Practical

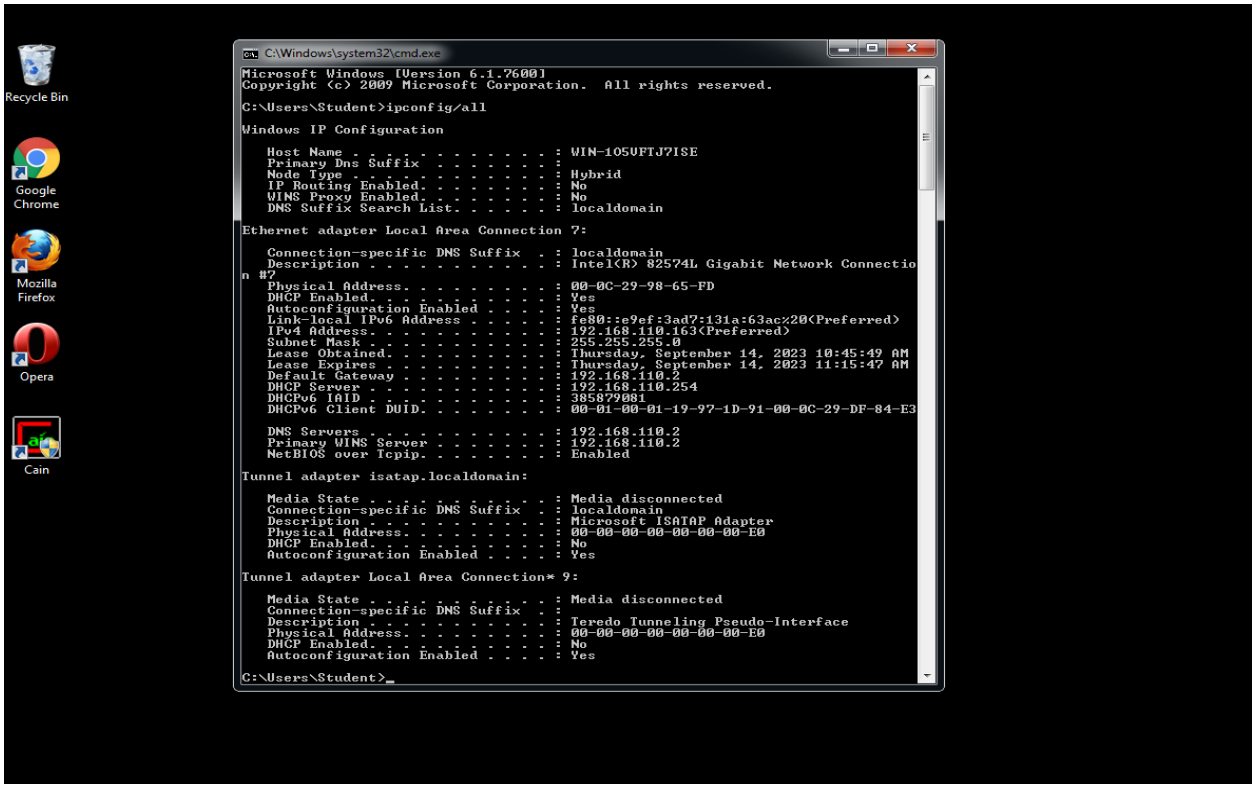
1. Network Connectivity

Network configuration for all VMs is set to NAT.

1. Document the IP address, subnet, and gateway of system. Write the command to perform the operation.
   Windows 7

- Open the command prompt from start menu and use command ‘ipconfig/all’ to check IP address, default gateway, and subnet details of Windows machine
  Command use – ipconfig/all

IP Address – 192.168.110.163
Default Gateway – 192.168.110.1
Subnet – 255.255.255.0



Kali Linux

- Open the command prompt and use below commands to check IP address, default gateway, and subnet details of Kali Linux machine

Command use – ip addr show eth0 to check IP address details
IP Address – 192.168.110.164
Subnet mask – 255.255.255.0

```
┌──(kali㉿kali)-[~]
└─$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:3d:01:37 brd ff:ff:ff:ff:ff:ff
    inet 192.168.110.164/24 brd 192.168.110.255 scope global dynamic noprefixroute eth0
       valid_lft 1661sec preferred_lft 1661sec
    inet6 fe80::eca:82b0:33d7:4d9f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Command use – ip route| grep default
Default gateway – 192.168.110.2

```
┌──(kali㉿kali)-[~]
└─$ ip route | grep default
default via 192.168.110.2 dev eth0 proto dhcp src 192.168.110.164 metric 100
```

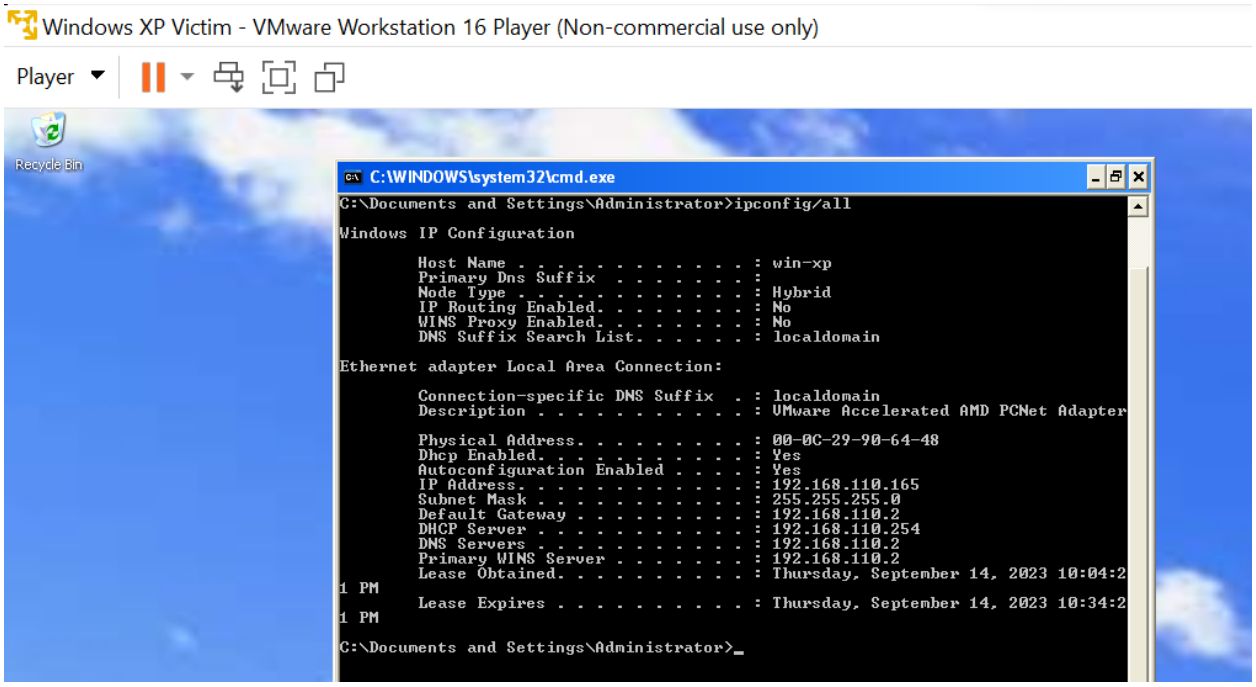
Alternatively, you can use ifconfig to view ip address and default gateway and subnet mask details

```
┌──(kali㉿kali)-[~]
└─$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.110.164  netmask 255.255.255.0  broadcast 192.168.110.255
        inet6 fe80::eca:82b0:33d7:4d9f  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:3d:01:37  txqueuelen 1000  (Ethernet)
        RX packets 252  bytes 39172 (38.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 80  bytes 10322 (10.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Windows XP

- Open the command prompt and use below commands to check IP address, default gateway, and subnet details of Windows XP machine

Command use – ipconfig/all
IP Address – 192.168.110.165
Default Gateway – 192.168.110.2
Subnet – 255.255.255.0



2. How many potential hosts could be available on that same network?
   The number of potential hosts available on the network depends on the subnet mask. It can be calculated using formula 2^x-2 where x is a number of host ID bits in the IP and 2 bits are used for host ID and Broadcast address

   IPV4 address includes total 32 bits.
   For example, consider 192.168.110.164/24 then 24 bits are used for the subnet mask
   So (32-24) = 8
   If you put 8 into the formula, it is (2^8) – 2. 2^8 is 256 and 256 – 2 is 254 total hosts can be allowed.

3. Find other hosts. Write the tool to find the other hosts.

- I am using Kali Linux to check available hosts on the same network and using nmap tool to check available hosts on the network.
  In the below snapshot we can see three hosts are available on the network including kali linux and one is the default gateway
  Command – nmap -sn 192.168.110.164/24
  Hosts available on the network –
  192.168.110.2 – subnet mask
  192.168.110.163
  192.168.110.164
  192.168.110.165

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.110.164/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-14 12:40 EDT
Nmap scan report for 192.168.110.2
Host is up (0.0033s latency).
Nmap scan report for 192.168.110.163
Host is up (0.0038s latency).
Nmap scan report for 192.168.110.164
Host is up (0.0022s latency).
Nmap scan report for 192.168.110.165
Host is up (0.0034s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.70 seconds
```

4. Using the OS ping utility, try pinging random addresses to see if you can find another host online.
   - Below hosts are online as I am able to ping to this addresses. We can also see packets transmitted and received count is same.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.110.163
PING 192.168.110.163 (192.168.110.163) 56(84) bytes of data.
64 bytes from 192.168.110.163: icmp_seq=1 ttl=128 time=0.948 ms
64 bytes from 192.168.110.163: icmp_seq=2 ttl=128 time=0.642 ms
64 bytes from 192.168.110.163: icmp_seq=3 ttl=128 time=0.794 ms
64 bytes from 192.168.110.163: icmp_seq=4 ttl=128 time=0.663 ms
64 bytes from 192.168.110.163: icmp_seq=5 ttl=128 time=0.621 ms
64 bytes from 192.168.110.163: icmp_seq=6 ttl=128 time=0.484 ms
64 bytes from 192.168.110.163: icmp_seq=7 ttl=128 time=0.639 ms
^C
── 192.168.110.163 ping statistics ──
7 packets transmitted, 7 received, 0% packet loss, time 6070ms
rtt min/avg/max/mdev = 0.484/0.684/0.948/0.136 ms

┌──(kali㉿kali)-[~]
└─$ ping 192.168.110.165
PING 192.168.110.165 (192.168.110.165) 56(84) bytes of data.
64 bytes from 192.168.110.165: icmp_seq=1 ttl=128 time=0.421 ms
64 bytes from 192.168.110.165: icmp_seq=2 ttl=128 time=0.475 ms
64 bytes from 192.168.110.165: icmp_seq=3 ttl=128 time=0.839 ms
64 bytes from 192.168.110.165: icmp_seq=4 ttl=128 time=0.538 ms
64 bytes from 192.168.110.165: icmp_seq=5 ttl=128 time=1.60 ms
64 bytes from 192.168.110.165: icmp_seq=6 ttl=128 time=0.613 ms
64 bytes from 192.168.110.165: icmp_seq=7 ttl=128 time=0.301 ms
64 bytes from 192.168.110.165: icmp_seq=8 ttl=128 time=0.538 ms
^C
── 192.168.110.165 ping statistics ──
8 packets transmitted, 8 received, 0% packet loss, time 7123ms
rtt min/avg/max/mdev = 0.301/0.665/1.598/0.381 ms
```

-

5. Using the OS ping utility, ping google.com and umbc.edu.

```
┌──(kali㉿kali)-[~]
└─$ ping google.com
PING google.com (172.253.62.102) 56(84) bytes of data.
64 bytes from bc-in-f102.1e100.net (172.253.62.102): icmp_seq=1 ttl=128 time=25.3 ms
64 bytes from bc-in-f102.1e100.net (172.253.62.102): icmp_seq=2 ttl=128 time=21.3 ms
64 bytes from bc-in-f102.1e100.net (172.253.62.102): icmp_seq=3 ttl=128 time=22.1 ms
64 bytes from bc-in-f102.1e100.net (172.253.62.102): icmp_seq=4 ttl=128 time=20.7 ms
64 bytes from bc-in-f102.1e100.net (172.253.62.102): icmp_seq=5 ttl=128 time=19.0 ms
64 bytes from bc-in-f102.1e100.net (172.253.62.102): icmp_seq=6 ttl=128 time=19.9 ms
64 bytes from bc-in-f102.1e100.net (172.253.62.102): icmp_seq=7 ttl=128 time=18.1 ms
64 bytes from bc-in-f102.1e100.net (172.253.62.102): icmp_seq=8 ttl=128 time=15.4 ms
64 bytes from bc-in-f102.1e100.net (172.253.62.102): icmp_seq=9 ttl=128 time=16.1 ms
64 bytes from bc-in-f102.1e100.net (172.253.62.102): icmp_seq=10 ttl=128 time=16.6 ms
64 bytes from bc-in-f102.1e100.net (172.253.62.102): icmp_seq=11 ttl=128 time=15.3 ms
64 bytes from bc-in-f102.1e100.net (172.253.62.102): icmp_seq=12 ttl=128 time=17.4 ms
64 bytes from bc-in-f102.1e100.net (172.253.62.102): icmp_seq=13 ttl=128 time=41.0 ms
^C
── google.com ping statistics ──
13 packets transmitted, 13 received, 0% packet loss, time 12028ms
rtt min/avg/max/mdev = 15.336/20.645/41.049/6.518 ms

┌──(kali㉿kali)-[~]
└─$ ping umbc.edu
PING umbc.edu (23.185.0.4) 56(84) bytes of data.
64 bytes from 23.185.0.4 (23.185.0.4): icmp_seq=1 ttl=128 time=20.7 ms
64 bytes from 23.185.0.4 (23.185.0.4): icmp_seq=2 ttl=128 time=17.3 ms
64 bytes from 23.185.0.4 (23.185.0.4): icmp_seq=3 ttl=128 time=20.2 ms
64 bytes from 23.185.0.4 (23.185.0.4): icmp_seq=4 ttl=128 time=17.7 ms
64 bytes from 23.185.0.4 (23.185.0.4): icmp_seq=5 ttl=128 time=20.8 ms
64 bytes from 23.185.0.4 (23.185.0.4): icmp_seq=6 ttl=128 time=18.4 ms
64 bytes from 23.185.0.4 (23.185.0.4): icmp_seq=7 ttl=128 time=18.3 ms
64 bytes from 23.185.0.4 (23.185.0.4): icmp_seq=8 ttl=128 time=17.4 ms
64 bytes from 23.185.0.4 (23.185.0.4): icmp_seq=9 ttl=128 time=15.7 ms
64 bytes from 23.185.0.4 (23.185.0.4): icmp_seq=10 ttl=128 time=16.2 ms
^C
── umbc.edu ping statistics ──
10 packets transmitted, 10 received, 0% packet loss, time 9020ms
rtt min/avg/max/mdev = 15.737/18.281/20.817/1.702 ms
```

6. What services are in use on your local system?

Kali Linux –

Nessus Scanner and Docker container is running on the local system

To check which services are running on local system ‘netstat’ or ‘ss’ command can be used to check port numbers listening on local system.

0.0.0.0:8834 – This means it can accept connections from any IP address
127.0.0.01:32777 – It will only accept connections from local machine
[::]: 8834 – It can only accept connections from all IPV6 addressess

```
┌──(kali㉿kali)-[~]
└─$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:8834            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:32775         0.0.0.0:*               LISTEN
tcp6       0      0 :::8834                 :::*                    LISTEN

┌──(kali㉿kali)-[~]
└─$ ss -tuln
Netid               State                Recv-Q               Send-Q                             Local Address:Port                 Peer Address:Port              Process
tcp                 LISTEN               0                    1024                                  0.0.0.0:8834                      0.0.0.0:*
tcp                 LISTEN               0                    4096                              127.0.0.1:32775                       0.0.0.0:*
tcp                 LISTEN               0                    1024                                  [::]:8834                         [::]:*
```

Alternatively, Command – ‘sudo lsof –I’ can be used to check for open ports and services running

```
┌──(kali㉿kali)-[~]
└─$ sudo lsof -i
COMMAND   PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
NetworkMa 471 root   25u  IPv4 113405      0t0  UDP 192.168.110.164:bootpc→192.168.110.254:bootps
nessusd   545 root   16u  IPv4  17383      0t0  TCP *:8834 (LISTEN)
nessusd   545 root   19u  IPv6  17384      0t0  TCP *:8834 (LISTEN)
container 563 root   13u  IPv4  15233      0t0  TCP localhost:32775 (LISTEN)
```

Alternatively, nmap can be used to check which ports are open and which services are running on the local system.
Command – nmap –p- 1270.0.0.1

```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-14 15:49 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00035s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE
8834/tcp  open  nessus-xmlrpc
32775/tcp open  sometimes-rpc13

Nmap done: 1 IP address (1 host up) scanned in 5.11 seconds
```

Windows 7 –

After scanning the Windows machine using Kali Linux, I have seen many ports are open as shown in the snapshot such as netbios-ssn, RDP port 3389 which are security concerns here.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 192.168.110.163
Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-14 18:26 EDT
Nmap scan report for 192.168.110.163
Host is up (0.00093s latency).
Not shown: 65522 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 60.02 seconds
```

Windows XP –

In windows xp, netbios-ssn, ftp ports are open which should be open for specific services or application only.

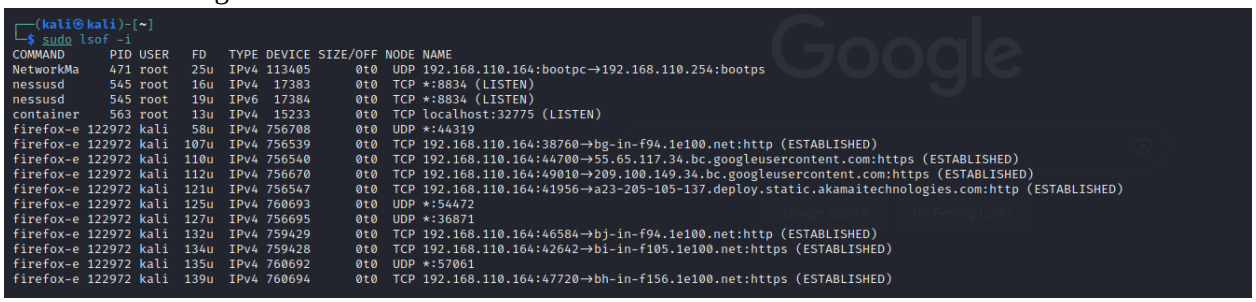
```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 192.168.110.165
Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-14 20:02 EDT
Nmap scan report for 192.168.110.165
Host is up (0.0017s latency).
Not shown: 65527 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS

Nmap done: 1 IP address (1 host up) scanned in 19.54 seconds
```

7. What ports are listed and what is connected to the system? List the ports

Kali Linux-
8834 – nessus scanner
32777 – docker container
Windows 7 –
135 – msrpc
139 – netbios –ssn
445 – Microsoft-ds
554 – rtsp
2869 – icslap
3389 – ms-wbt-server

Windows XP-
21 - ftp
25 - smtp
80 – http
135 – msrpc
139 – netbios -ssn
443 – https
445 – Microsoft-ds
1025 – NFS-or-IISx`

8. Launch a browser and go to google.com and repeat #7?
   I launched Firefox and entered the google.com site and after that checked services which are running on the local system. Since I have used Firefox to launch google.com all remaining Firefox services have been showing



2. Routing

1. What route/ARP information does your system have?
   Linux:
   I am using the command **'route –n'** to check the routing table details
   In the below snapshot, the default gateway is being used 192.168.110.2 and packets are being sent to IP address 172.17.0.0 and 192.168.110.0

```
┌──(kali㉿kali)-[~]
└─$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.110.2   0.0.0.0         UG    100    0        0 eth0
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
192.168.110.0   0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

I am using **'arp –a'** to check IP address and Mac address mapping.
ARP is a protocol used to map IP address to a physical address (Mac Address)

```
┌──(kali㉿kali)-[~]
└─$ arp -a
? (192.168.110.254) at 00:50:56:ee:be:24 [ether] on eth0
? (192.168.110.1) at 00:50:56:c0:00:08 [ether] on eth0
? (192.168.110.2) at 00:50:56:ff:5b:4a [ether] on eth0
? (192.168.110.163) at 00:0c:29:98:65:fd [ether] on eth0
? (192.168.110.165) at 00:0c:29:90:64:48 [ether] on eth0
```

Windows:

I am using **'route print'** command **'arp –a'** to check routing details and IP address to Mac address mapping.

```
C:\Users\Student>route print
===========================================================================
Interface List
 20...00 0c 29 98 65 fd ......Intel(R) 82574L Gigabit Network Connection #7
  1...........................Software Loopback Interface 1
 12...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 13...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.110.2  192.168.110.163     10
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
    192.168.110.0    255.255.255.0         On-link    192.168.110.163    266
  192.168.110.163  255.255.255.255         On-link    192.168.110.163    266
  192.168.110.255  255.255.255.255         On-link    192.168.110.163    266
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link    192.168.110.163    266
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link    192.168.110.163    266
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    306 ::1/128                  On-link
 20    266 fe80::/64                On-link
 20    266 fe80::e9ef:3ad7:131a:63ac/128
                                    On-link
  1    306 ff00::/8                 On-link
 20    266 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

```
C:\Users\Student>arp -a

Interface: 192.168.110.163 --- 0x14
  Internet Address      Physical Address      Type
  192.168.110.1         00-50-56-c0-00-08     dynamic
  192.168.110.2         00-50-56-ff-5b-4a     dynamic
  192.168.110.164       00-0c-29-3d-01-37     dynamic
  192.168.110.254       00-50-56-ee-be-24     dynamic
  192.168.110.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Windows XP:

```
C:\Documents and Settings\Student>route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 0c 29 90 64 48 ...... AMD PCNET Family PCI Ethernet Adapter - Packet S
cheduler Miniport
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.110.2  192.168.110.165       10
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1        1
    192.168.110.0    255.255.255.0  192.168.110.165  192.168.110.165       10
  192.168.110.165  255.255.255.255        127.0.0.1        127.0.0.1       10
  192.168.110.255  255.255.255.255  192.168.110.165  192.168.110.165       10
      224.0.0.0        240.0.0.0  192.168.110.165  192.168.110.165       10
  255.255.255.255  255.255.255.255  192.168.110.165  192.168.110.165       1
Default Gateway:     192.168.110.2
===========================================================================
Persistent Routes:
  None
```

```
C:\Documents and Settings\Student>arp -a

Interface: 192.168.110.165 --- 0x2
  Internet Address      Physical Address      Type
  192.168.110.1         00-50-56-c0-00-08     dynamic
  192.168.110.2         00-50-56-ff-5b-4a     dynamic

C:\Documents and Settings\Student>
```

2. What “extra” information do you know about the system in #3?

- From the previous question 3, there are total 4 host online out of which one is default gateway. Nmap have scan total 256 IP addresses and 4 hosts are up out of that.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.110.164/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-14 12:40 EDT
Nmap scan report for 192.168.110.2
Host is up (0.0033s latency).
Nmap scan report for 192.168.110.163
Host is up (0.0038s latency).
Nmap scan report for 192.168.110.164
Host is up (0.0022s latency).
Nmap scan report for 192.168.110.165
Host is up (0.0034s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.70 seconds
```

3. Trace a route to an internal IP that responded in the previous section.

```
┌──(kali㉿kali)-[~]
└─$ traceroute 192.168.110.0
traceroute to 192.168.110.0 (192.168.110.0), 30 hops max, 60 byte packets
 1  192.168.110.164 (192.168.110.164)  3059.394 ms !H  3059.165 ms !H  3059.124 ms !H
```

4. Trace a route to an external IP that responded in the previous section, such as umbc.edu's IP?

```
┌──(kali㉿kali)-[~]
└─$ traceroute 23.185.0.4
traceroute to 23.185.0.4 (23.185.0.4), 30 hops max, 60 byte packets
 1  192.168.110.2 (192.168.110.2)  0.403 ms  0.253 ms  0.148 ms
 2  * * *
 3  * * *
```