Name : Shriram Karpoora Sundara Pandian

Course : CSEC 600 Introduction to Cyber Security

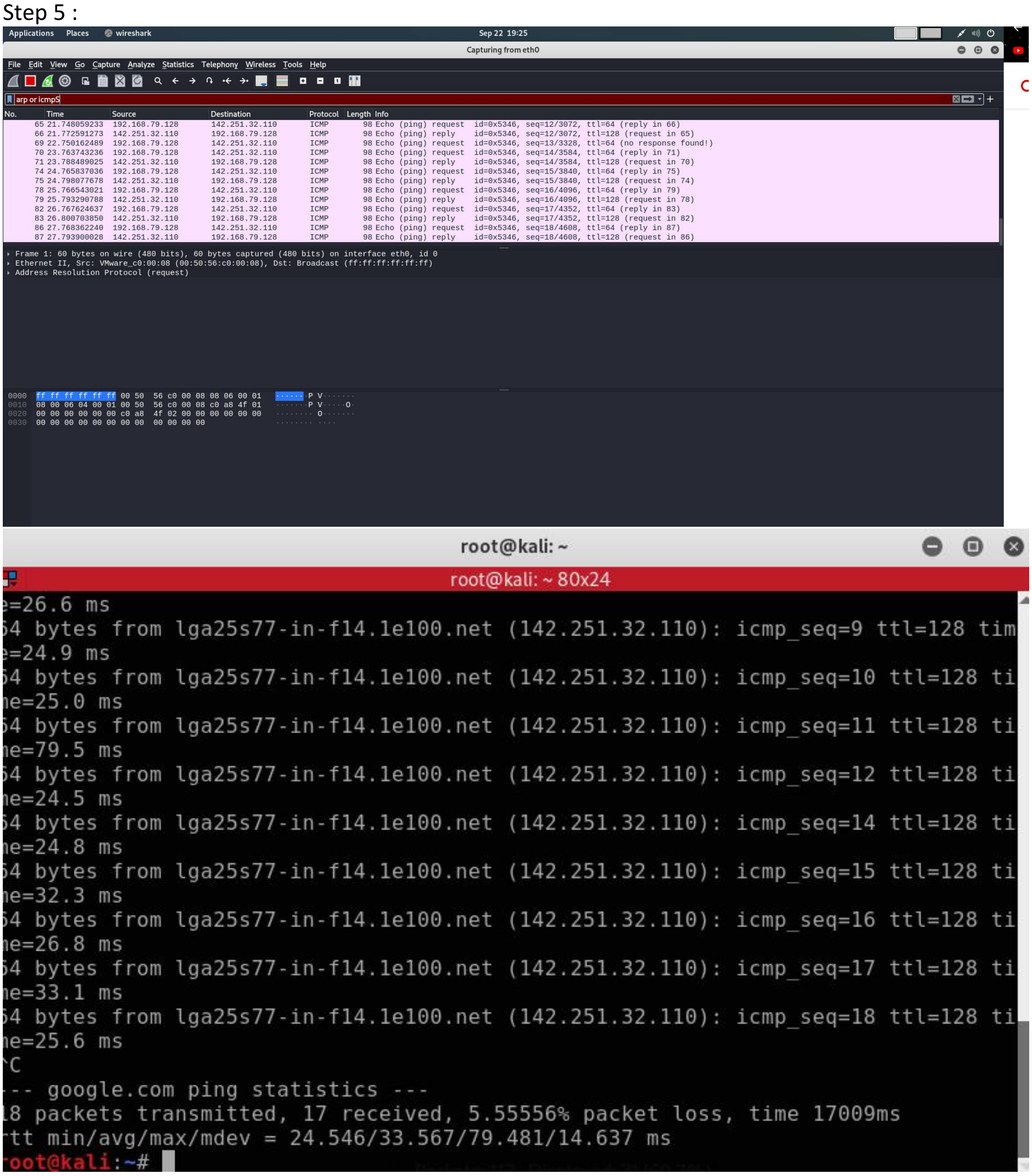
Title : Packet Sniffing

Lab : 4

Chapter : 6 (TCP/IP Basics)

Exercise 6. 04 :

Packet Sniffing
Step 5 :



Step 8 :

```
root@kali:~# arp -a
_gateway (192.168.79.2) at 00:50:56:e1:d0:25 [ether] on eth0
? (192.168.79.254) at 00:50:56:ee:17:c9 [ether] on eth0
root@kali:~# arp -d
arp: need host name
root@kali:~# arp -a
_gateway (192.168.79.2) at 00:50:56:e1:d0:25 [ether] on eth0
? (192.168.79.254) at 00:50:56:ee:17:c9 [ether] on eth0
root@kali:~# ping www.flcc.edu
PING www.flcc.edu (192.156.234.2) 56(84) bytes of data.
^C
--- www.flcc.edu ping statistics ---
67 packets transmitted, 0 received, 100% packet loss, time 67576ms

root@kali:~# ping google.com
PING google.com (142.250.80.14) 56(84) bytes of data.
64 bytes from lga34s33-in-f14.1e100.net (142.250.80.14): icmp_seq=1 ttl=128 time=27.0 ms
64 bytes from lga34s33-in-f14.1e100.net (142.250.80.14): icmp_seq=2 ttl=128 time=33.5 ms
64 bytes from lga34s33-in-f14.1e100.net (142.250.80.14): icmp_seq=3 ttl=128 time=26.0 ms
64 bytes from lga34s33-in-f14.1e100.net (142.250.80.14): icmp_seq=4 ttl=128 time=59.2 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 25.968/36.405/59.173/13.460 ms
root@kali:~# ping -4 www.google.com
PING www.google.com (142.250.64.68) 56(84) bytes of data.
64 bytes from lga34s30-in-f4.1e100.net (142.250.64.68): icmp_seq=1 ttl=128 time=28.9 ms
64 bytes from lga34s30-in-f4.1e100.net (142.250.64.68): icmp_seq=2 ttl=128 time=26.1 ms
64 bytes from lga34s30-in-f4.1e100.net (142.250.64.68): icmp_seq=3 ttl=128 time=26.8 ms
64 bytes from lga34s30-in-f4.1e100.net (142.250.64.68): icmp_seq=4 ttl=128 time=26.8 ms
^C
--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 26.055/27.122/28.874/1.053 ms
```

Packet List Column	Local Communication	Remote Communication
No.	2	504
Time	0.366942243	340.508348263
Source	VMware_c0:00:08	VMware_ee:17:c9
Destination	Broadcast	VMware_5c:fb:2c
Protocol	ARP	ARP
Length	60	60
Info	Who has 192.168.79.2? Tell 192.168.79.1	192.168.79.254 is at 00:50:56:ee:17:c9

Step 9 :

ARP Row Field	Local Communication	Remote communication
Sender MAC address	VMware_c0:00:08 (00:50:56:c0:00:08)	VMware_ee:17:c9 (00:50:56:ee:17:c9)
Sender IP address	192.168.79.1	192.168.79.254
Target MAC address	00:00:00:00:00:00 (00:00:00:00:00:00)	VMware_5c:fb:2c (00:0c:29:5c:fb:2c)
Target IP address	192.168.79.2	192.168.79.128

Ethernet II Row Field	Local Communication	Remote Communication
Destination	Broadcast(ff:ff:ff:ff:ff:ff)	VMware_5c:fb:2c (00:0c:29:5c:fb:2c)
Source	Vmware_c0:00:08 (00:50:56:c0:00:08)	VMware_e1:d0:25 (00:50:56:e1:d0:25)
Type	Arp(0x0806)	Arp(0x0806)

Step 10 :

Packet List Column	Local Communication	Remote Communication
No.	42	79
Time	52.19542322	198.033778833
Source	VMware_5c:fb:2c	VMware_e1:d0:25
Destination	VMware_e1:d0:25	VMware_5c:fb:2c
Protocol	ARP	ARP
Length	42	60
Info	192.168.79.128 is at 00:0c:29:5c:fb:2c	192.168.79.2 is at 00:50:56:e1:d0:25

Step 11 :

ARP Row Field	Local Communication	Remote communication
Sender MAC address	VMware_:5c:fb:2c (00:0c:29:5c:fb:2c)	VMware_e1:d0:25 (00:50:56:ee:d0:25)
Sender IP address	192.168.79.128	192.168.79.2
Target MAC address	VMware_:e1:d0:25 (00:50:56:e1:d0:25)	VMware_5c:fb:2c (00:0c:29:5c:fb:2c)
Target IP address	192.168.79.2	192.168.79.128

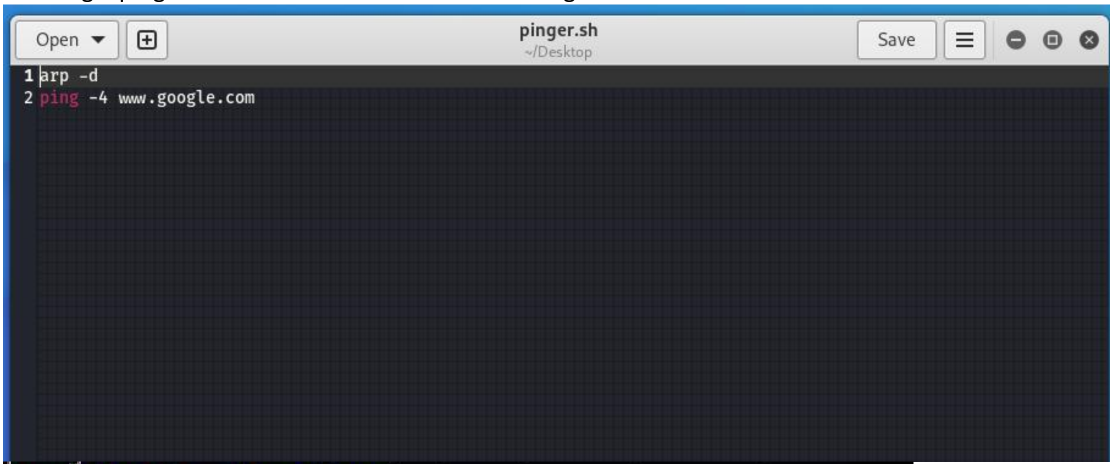
Ethernet II Row Field	Local Communication	Remote Communication
Destination	Broadcast(ff:ff:ff:ff:ff:ff)	VMware_5c:fb:2c (00:0c:29:5c:fb:2c)
Source	Vmware_c0:00:08 (00:50:56:c0:00:08)	VMware_e1:d0:25 (00:50:56:e1:d0:25)
Type	Arp(0x0806)	Arp(0x0806)

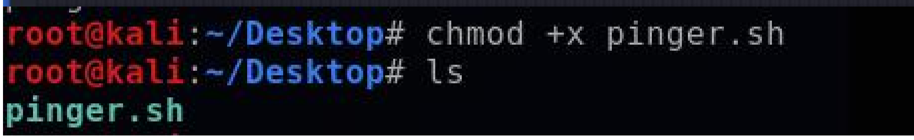
Step 12 :

Ethernet II Row Field	Local Communication	Remote Communication
Destination	VMware_e1:d0:25 (00:50:56:e1:d0:25)	VMware_e1:d0:25 (00:50:56:e1:d0:25)
Source	VMware_5c:fb:2c (00:0c:29:5c:fb:2c)	VMware_5c:fb:2c (00:0c:29:5c:fb:2c)
Type	IPv4 (0x0800)	IPv4 (0x0800)

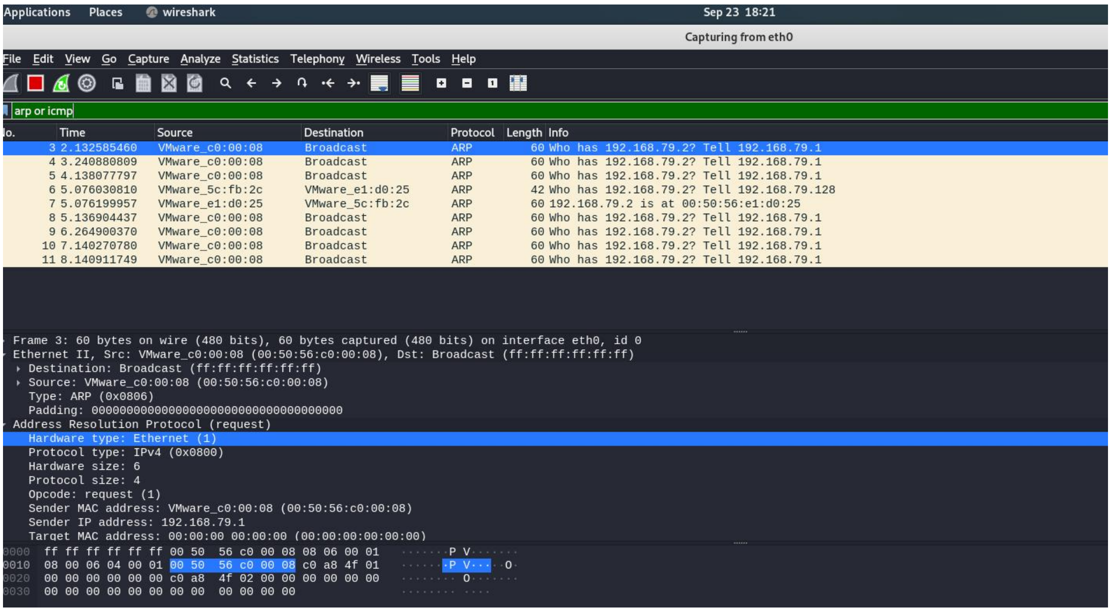
Internet Protocol Version 4	Local Communication	Remote Communication
Source	192.168.79.128	192.168.79.128
Destination	192.168.1.34	142.251.32.110

Step 13
Creating a pinger file with .sh extension as I am using Kali linux.





I am doing “chmod +x pinger.sh” so that I can give permission to this file for activation.



I started the wireshark before starting the file.

```
root@kali:~/Desktop# ls
pinger.sh
root@kali:~/Desktop# ./pinger.sh
arp: need host name
PING www.google.com (142.250.81.228) 56(84) bytes of data.
64 bytes from lga25s74-in-f4.1e100.net (142.250.81.228): icmp_seq=1 ttl=128 time=27.2 ms
64 bytes from lga25s74-in-f4.1e100.net (142.250.81.228): icmp_seq=2 ttl=128 time=26.5 ms
64 bytes from lga25s74-in-f4.1e100.net (142.250.81.228): icmp_seq=3 ttl=128 time=26.8 ms
64 bytes from lga25s74-in-f4.1e100.net (142.250.81.228): icmp_seq=4 ttl=128 time=27.5 ms
64 bytes from lga25s74-in-f4.1e100.net (142.250.81.228): icmp_seq=5 ttl=128 time=33.1 ms
64 bytes from lga25s74-in-f4.1e100.net (142.250.81.228): icmp_seq=6 ttl=128 time=31.9 ms
64 bytes from lga25s74-in-f4.1e100.net (142.250.81.228): icmp_seq=7 ttl=128 time=29.5 ms
64 bytes from lga25s74-in-f4.1e100.net (142.250.81.228): icmp_seq=8 ttl=128 time=27.9 ms
64 bytes from lga25s74-in-f4.1e100.net (142.250.81.228): icmp_seq=9 ttl=128 time=30.6 ms
64 bytes from lga25s74-in-f4.1e100.net (142.250.81.228): icmp_seq=10 ttl=128 time=27.3 ms
64 bytes from lga25s74-in-f4.1e100.net (142.250.81.228): icmp_seq=11 ttl=128 time=26.6 ms
64 bytes from lga25s74-in-f4.1e100.net (142.250.81.228): icmp_seq=12 ttl=128 time=31.9 ms
64 bytes from lga25s74-in-f4.1e100.net (142.250.81.228): icmp_seq=13 ttl=128 time=28.1 ms
64 bytes from lga25s74-in-f4.1e100.net (142.250.81.228): icmp_seq=14 ttl=128 time=29.2 ms
64 bytes from lga25s74-in-f4.1e100.net (142.250.81.228): icmp_seq=15 ttl=128 time=32.2 ms
64 bytes from lga25s74-in-f4.1e100.net (142.250.81.228): icmp_seq=16 ttl=128 time=31.8 ms
^C
--- www.google.com ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15109ms
rtt min/avg/max/mdev = 26.461/29.258/33.131/2.254 ms
```

I ran the file and it send packets successfully

```
50 60.612065185  VMware_5c:fb:2c   VMware_e1:d0:25   ARP   42 Who has 192.168.79.2? Tell 192.168.79.128
51 60.612226237  VMware_e1:d0:25   VMware_5c:fb:2c   ARP   60 192.168.79.2 is at 00:50:56:e1:d0:25
```

The ARP packet replied successfully.

Step 14

	Local Communication	Remote Communication
a	Destination of the ping	Default Gateway
b	Destination of the MAC	Default Gateway
c	Source of the ping	Source of the ping
d	Source of the ping	Default gateway
e	Source of the ping	Default gateway
f	Source of the ping	Destination of the ping
g	Destination of the ping	Default gateway
h	Destination of the ping	Destination of the ping
i	Destination of the ping	Default gateway
j	Destination of the ping	Destination of the ping
k	Source of the ping	Default gateway
l	Source of the ping	Source of the ping
m	Default gateway	Destination of the ping

Step 15 :

The network design is similar to UPS delivering the package on the same street or in a different state. Both use the same technologies, like ARP, ICMP, and IP, but work differently and forward messages differently. The beauty of networking is how it is interconnected with the devices. For local communication, sending an ARP request will be broadcast, and the ARP reply will be unicast. If I shout at the street, everyone will get the notice, and target Smith's will understand the call and come to meet me about why I shouted, which is funny by the way. But for a remote connection, it is different. ARP requests the router or default gateway, and it handles the connection from there to other routers and follows on. As we deliver the package to a local UPS store, they will send it to other UPS stores near the destination.

The local network is bound within the network of devices, which only interacts with local devices, and the destination would be the devices, not the router. As if we want to find the address within the street, we never go to UPS! ICMP echo and replies will happen with the devices in the network for local connections, whereas they happen between the router and the destination server in remote connections. Echoes and replies act as mediators to collect the information by passing the request, which is cool and gets the information back to the router, and the router passes back to the device that initiated the request.

The IP and MAC addresses are useful for identifying the devices on the network. I think the MAC address is crucial on a remote network. For finding the device that is using the particular IP, we need the MAC address to identify it, and the ICMP reply will carry the MAC address of the device to showcase the device at the IP address. Also, the IP address determines whether the connection is a local or remote connection, and IP helps the router send the packet to the destination accordingly, so IP plays a vital role in handling multiple networks.

Overall, IP and MAC addresses are very important for the packets to reach and return properly. Also, ARP and ICMP protocols play a vital role in carrying out the information and helping to form the proper network.

Exercise 6. 05 :

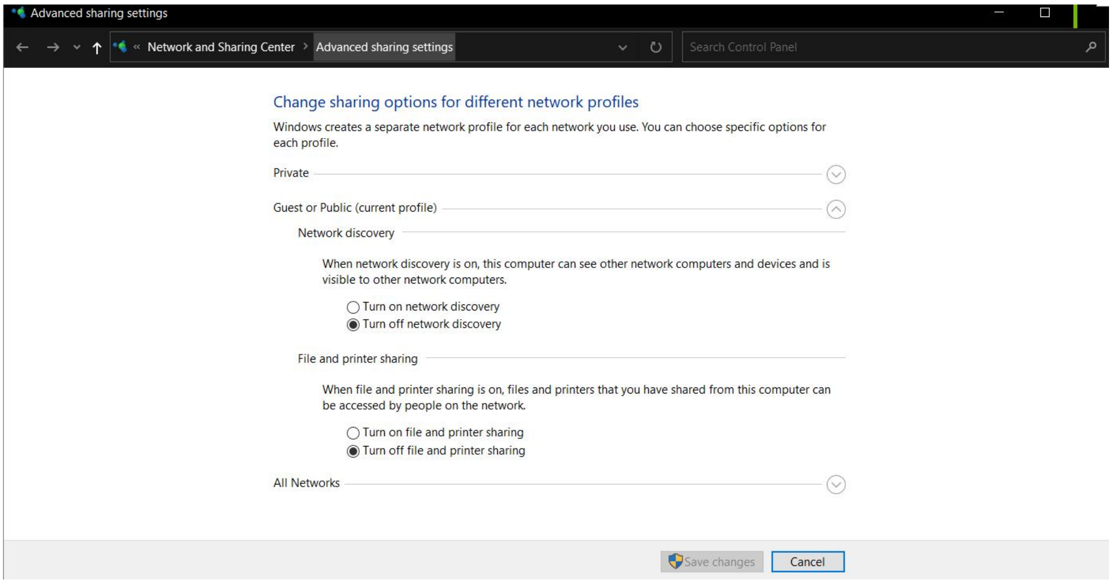
Step 2 :

We assign static IP and subnet mask for both the system :

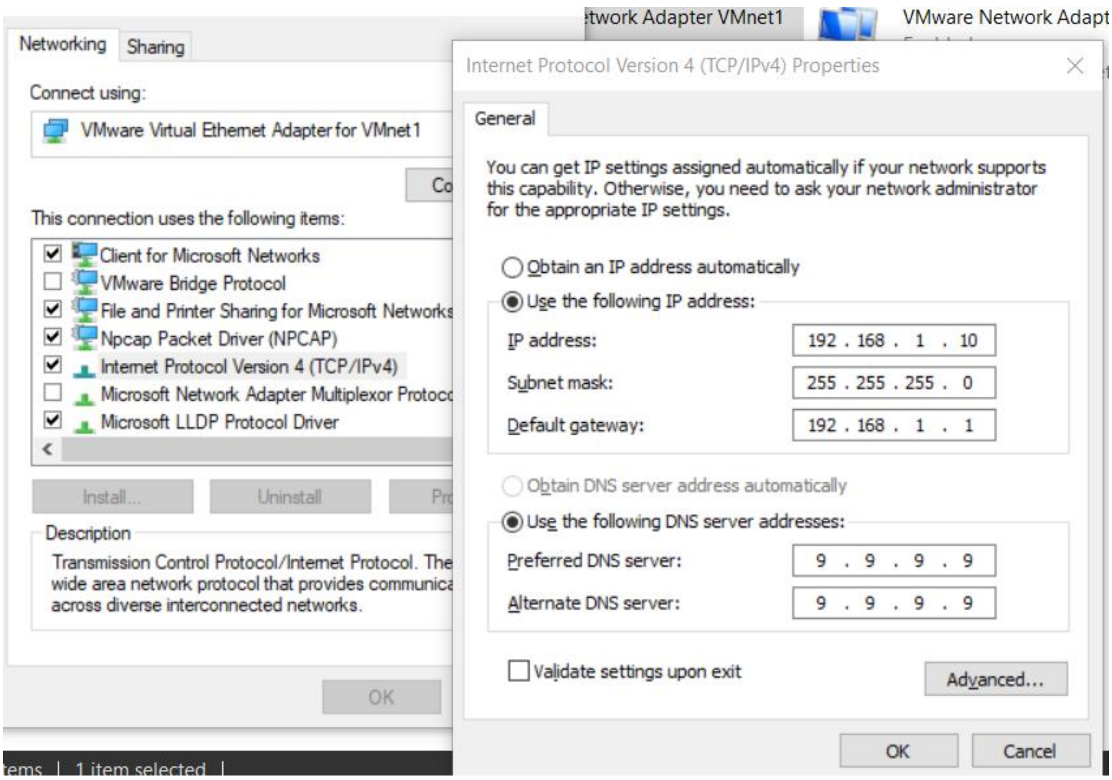
Computer	IP address	Subnet Mask
Computer A	192.168.1.10	255.255.255.0
Computer B	192.168.1.50	255.255.255.0

Step 3 :

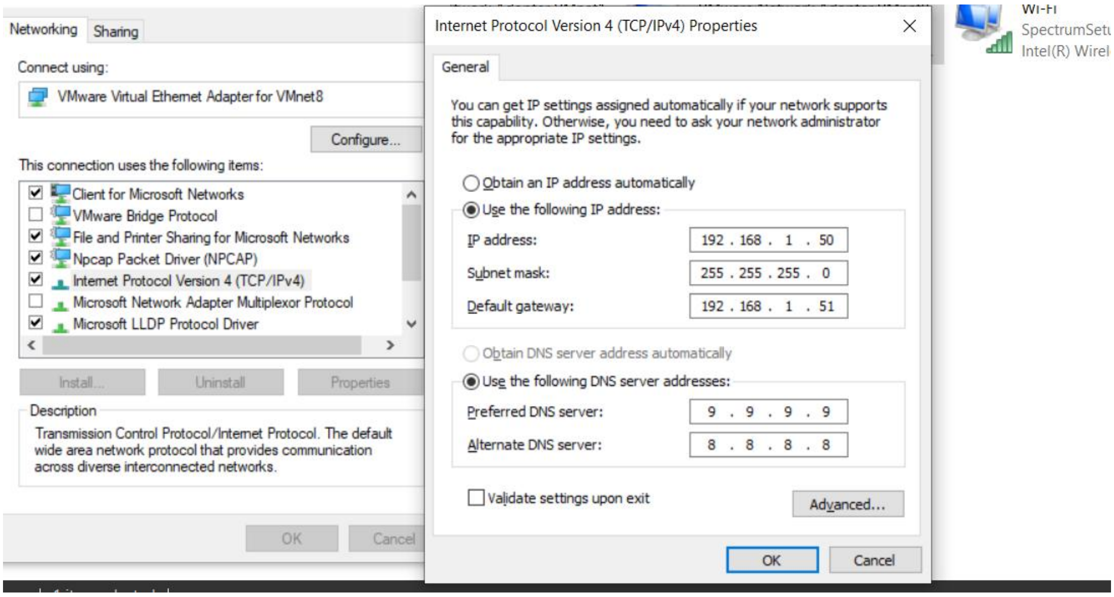
C.


Advanced sharing settings
Network and Sharing Center
Advanced sharing settings
Search Control Panel
Change sharing options for different network profiles
Windows creates a separate network profile for each network you use. You can choose specific options for each profile.
Private
Guest or Public (current profile)
Network discovery
When network discovery is on, this computer can see other network computers and devices and is visible to other network computers.
Turn on network discovery
Turn off network discovery
File and printer sharing
When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.
Turn on file and printer sharing
Turn off file and printer sharing
All Networks
Save changes
Cancel

H & I :


Networking
Sharing
Connect using:
VMware Virtual Ethernet Adapter for VMnet1
This connection uses the following items:
Client for Microsoft Networks
VMware Bridge Protocol
File and Printer Sharing for Microsoft Networks
Npcap Packet Driver (NPCAP)
Internet Protocol Version 4 (TCP/IPv4)
Microsoft LLDP Protocol Driver
Install...
Uninstall
Description
OK
1 item selected
VMware Network Adapt
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 10
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 9 . 9 . 9 . 9
Alternate DNS server: 9 . 9 . 9 . 9
Validate settings upon exit
Advanced...
OK
Cancel

Step 4 :



Step 5 :

```
C:\Users\dinot>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms
```