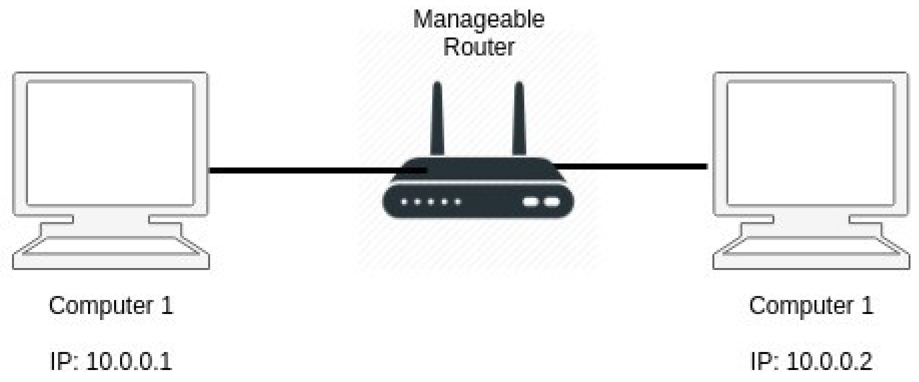
Program – 7

Build a Firewall using iptables

Required Components

- Computers or Laptops - 02
- Manageable Router / Switch - 01
- LAN Cables – 02

Network Diagram



Note:

The following screenshots infer

Computer 1 - Raspberry Pi with the IP – 10.0.0.1
Computer 2 – Laptop with the IP – 10.0.0.2

Installation of nmap and iptables using Internet (College Network)

Install nmap

```
sudo apt-get install nmap
```

Install nmap

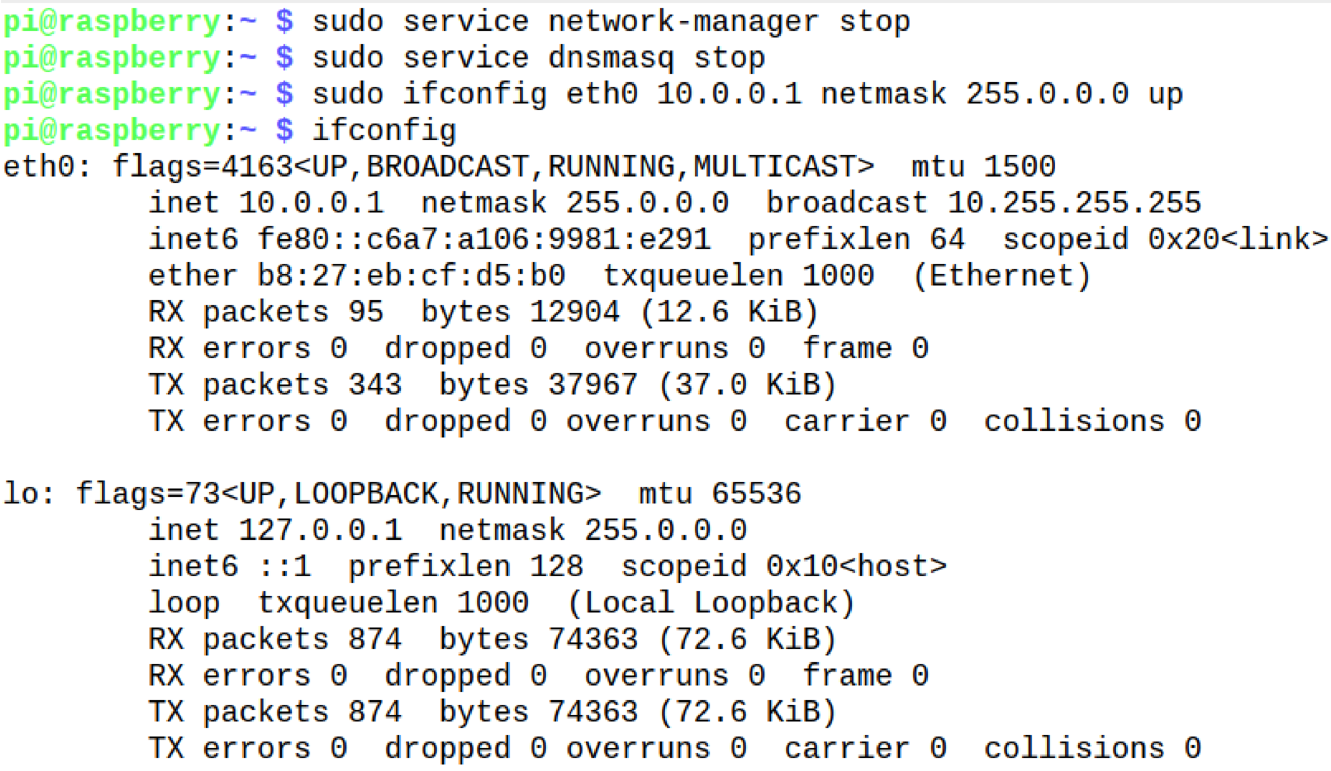
```
sudo apt-get install iptables
```

Update the system

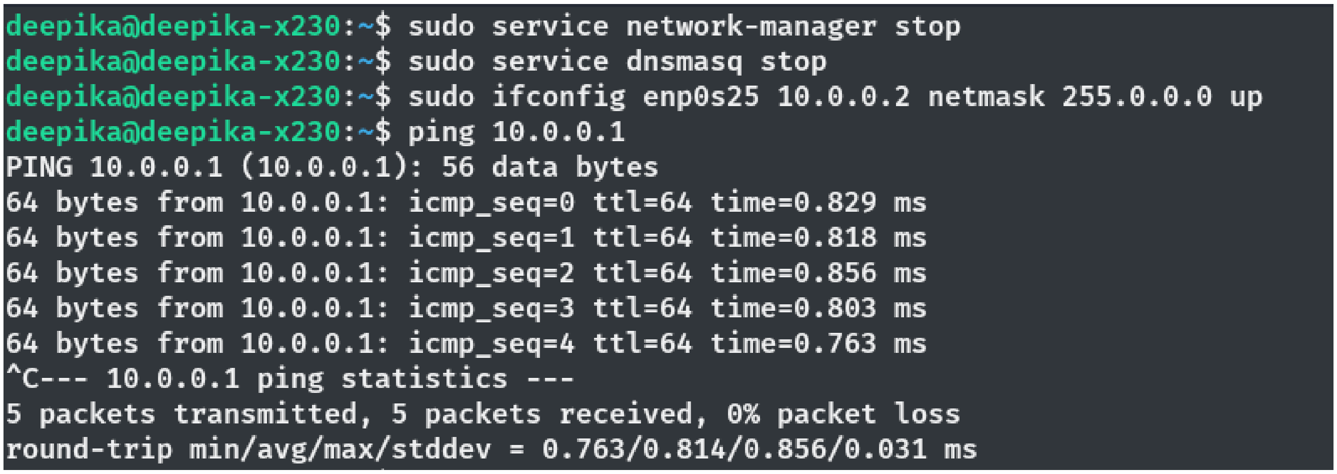
```
sudo apt-get update
```

Terminate the system from the College Network and Create a Private LAN as shown in the network diagram

Step 1: Stop the network manager, dnsmasq and set the IP for both the Computers



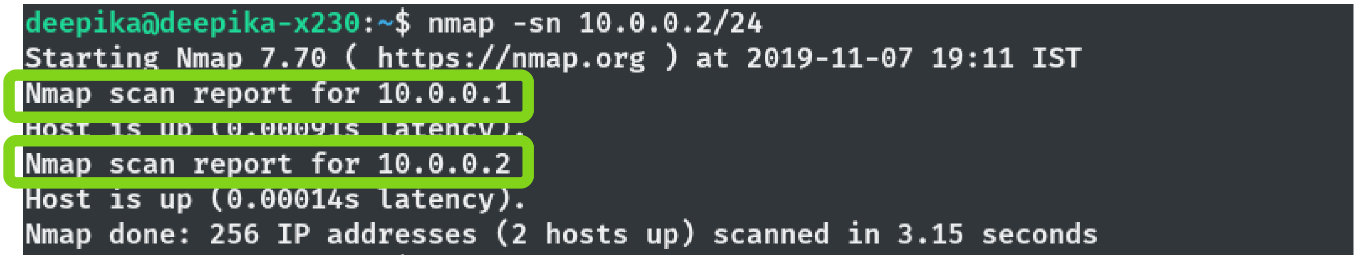
```
pi@raspberry:~ $ sudo service network-manager stop
pi@raspberry:~ $ sudo service dnsmasq stop
pi@raspberry:~ $ sudo ifconfig eth0 10.0.0.1 netmask 255.0.0.0 up
pi@raspberry:~ $ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.1  netmask 255.0.0.0  broadcast 10.255.255.255
        inet6 fe80::c6a7:a106:9981:e291  prefixlen 64  scopeid 0x20<link>
        ether b8:27:eb:cf:d5:b0  txqueuelen 1000  (Ethernet)
        RX packets 95  bytes 12904 (12.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 343  bytes 37967 (37.0 KiB)
        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
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 874  bytes 74363 (72.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 874  bytes 74363 (72.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



```
deepika@deepika-x230:~$ sudo service network-manager stop
deepika@deepika-x230:~$ sudo service dnsmasq stop
deepika@deepika-x230:~$ sudo ifconfig enp0s25 10.0.0.2 netmask 255.0.0.0 up
deepika@deepika-x230:~$ ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1): 56 data bytes
64 bytes from 10.0.0.1: icmp_seq=0 ttl=64 time=0.829 ms
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=0.818 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=0.856 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=0.803 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=0.763 ms
^C--- 10.0.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.763/0.814/0.856/0.031 ms
```

Step 2: Check all the machines connected in the network on Computer 2

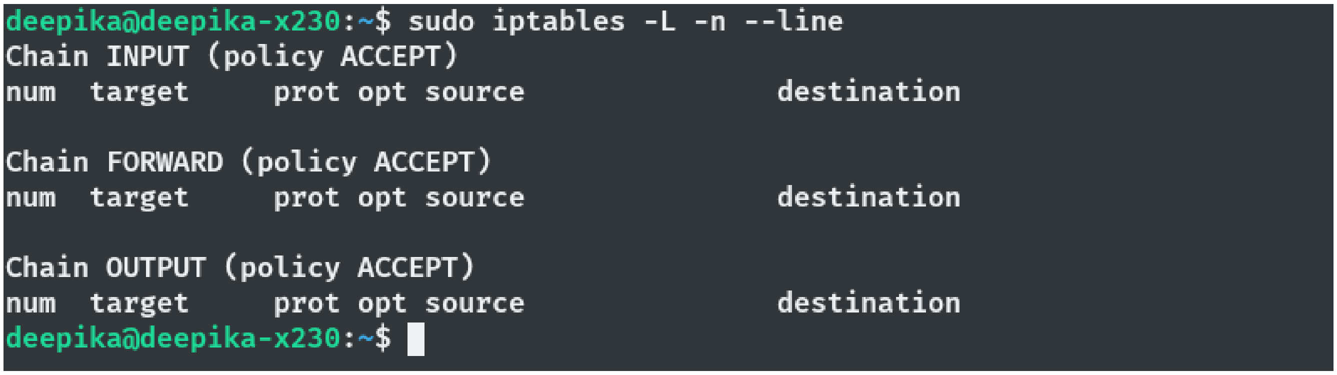
```
nmap -sn 10.0.0.2/24
```



```
deepika@deepika-x230:~$ nmap -sn 10.0.0.2/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-07 19:11 IST
Nmap scan report for 10.0.0.1
Host is up (0.00091s latency).
Nmap scan report for 10.0.0.2
Host is up (0.00014s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.15 seconds
```

Step 3: Check the current status of iptables on Computer 2

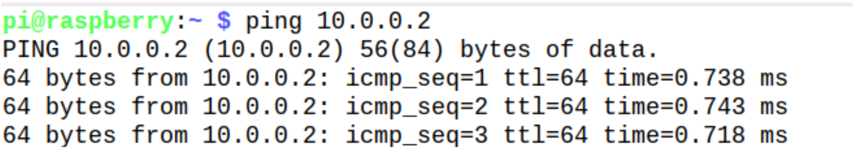
```
sudo iptables -L -n --line
```



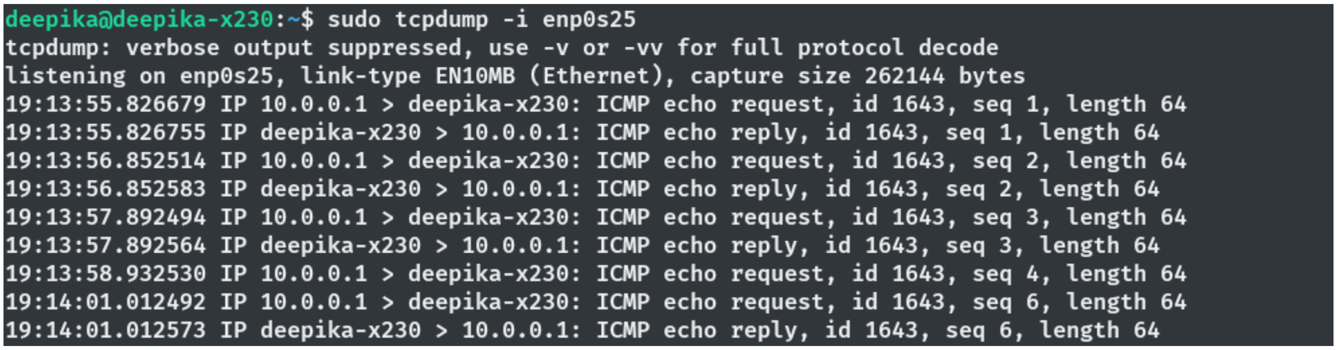
```
deepika@deepika-x230:~$ sudo iptables -L -n --line
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
deepika@deepika-x230:~$ 
```

Step 4: Ping Computer 2 from Computer 1 and run the following command on Computer 2

```
sudo tcpdump -i <ethernet-interface-name-Computer2>
```



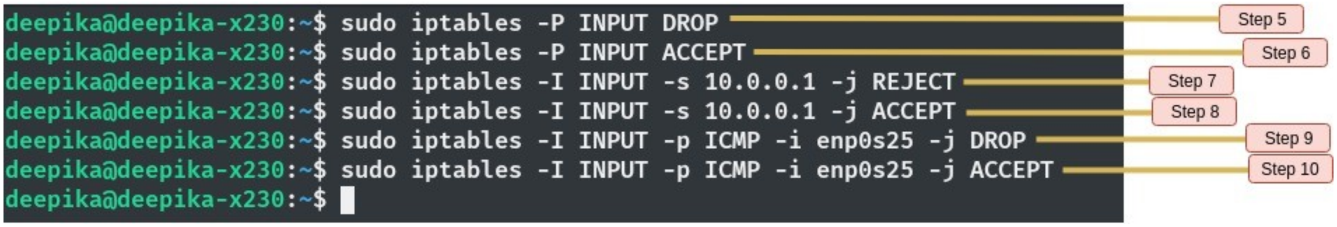
```
pi@raspberry:~ $ ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=0.738 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.743 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.718 ms
```



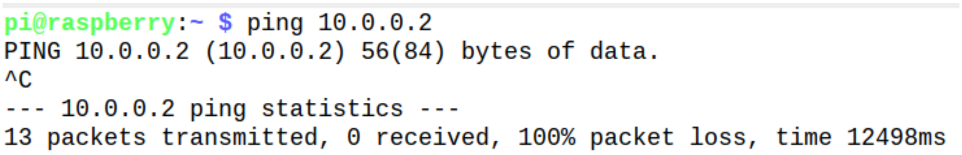
```
deepika@deepika-x230:~$ sudo tcpdump -i enp0s25
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s25, link-type EN10MB (Ethernet), capture size 262144 bytes
19:13:55.826679 IP 10.0.0.1 > deepika-x230: ICMP echo request, id 1643, seq 1, length 64
19:13:55.826755 IP deepika-x230 > 10.0.0.1: ICMP echo reply, id 1643, seq 1, length 64
19:13:56.852514 IP 10.0.0.1 > deepika-x230: ICMP echo request, id 1643, seq 2, length 64
19:13:56.852583 IP deepika-x230 > 10.0.0.1: ICMP echo reply, id 1643, seq 2, length 64
19:13:57.892494 IP 10.0.0.1 > deepika-x230: ICMP echo request, id 1643, seq 3, length 64
19:13:57.892564 IP deepika-x230 > 10.0.0.1: ICMP echo reply, id 1643, seq 3, length 64
19:13:58.932530 IP 10.0.0.1 > deepika-x230: ICMP echo request, id 1643, seq 4, length 64
19:14:01.012492 IP 10.0.0.1 > deepika-x230: ICMP echo request, id 1643, seq 6, length 64
19:14:01.012573 IP deepika-x230 > 10.0.0.1: ICMP echo reply, id 1643, seq 6, length 64
```

Step 5: Drop all the traffic on Computer 2

```
sudo iptables -P INPUT DROP
```



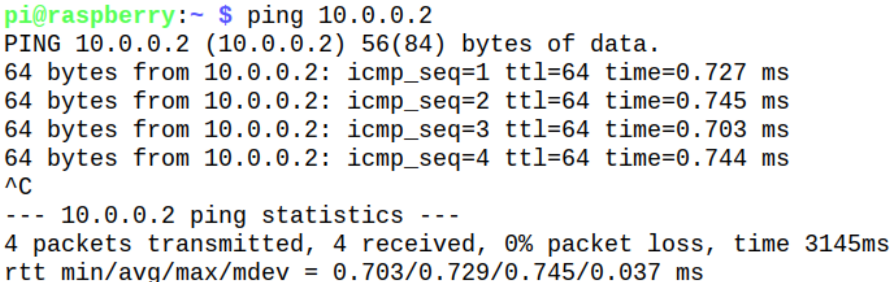
```
deepika@deepika-x230:~$ sudo iptables -P INPUT DROP
deepika@deepika-x230:~$ sudo iptables -P INPUT ACCEPT
deepika@deepika-x230:~$ sudo iptables -I INPUT -s 10.0.0.1 -j REJECT
deepika@deepika-x230:~$ sudo iptables -I INPUT -s 10.0.0.1 -j ACCEPT
deepika@deepika-x230:~$ sudo iptables -I INPUT -p ICMP -i enp0s25 -j DROP
deepika@deepika-x230:~$ sudo iptables -I INPUT -p ICMP -i enp0s25 -j ACCEPT
deepika@deepika-x230:~$
```



```
pi@raspberry:~ $ ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
^C
--- 10.0.0.2 ping statistics ---
13 packets transmitted, 0 received, 100% packet loss, time 12498ms
```

Step 6: Accept all the traffic on Computer 2

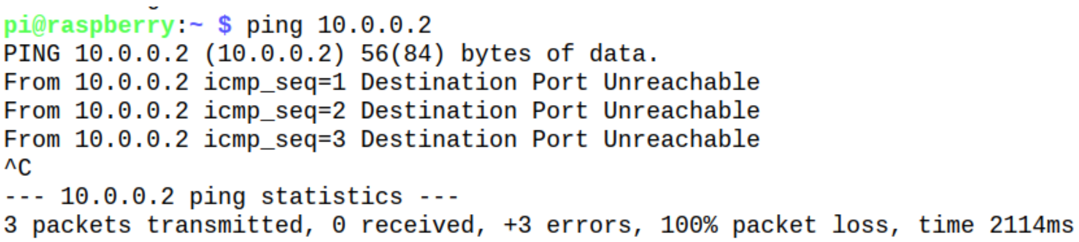
```
sudo iptables -P INPUT ACCEPT
```



```
pi@raspberry:~ $ ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=0.727 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.745 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.703 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=0.744 ms
^C
--- 10.0.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3145ms
rtt min/avg/max/mdev = 0.703/0.729/0.745/0.037 ms
```

Step 7: Reject all the traffic on Computer 2

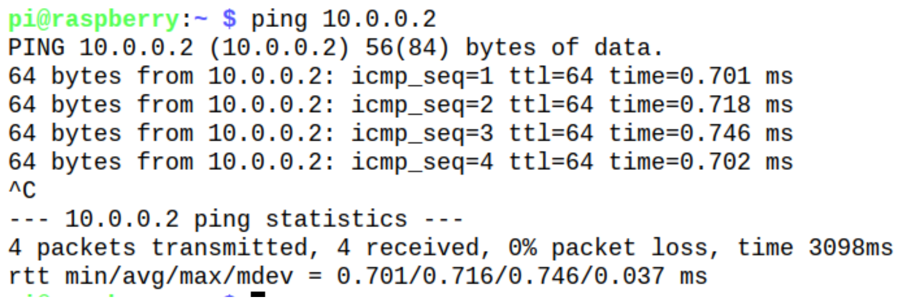
```
sudo iptables -P INPUT -s 10.0.0.1 -j REJECT
```



```
pi@raspberry:~ $ ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
From 10.0.0.2 icmp_seq=1 Destination Port Unreachable
From 10.0.0.2 icmp_seq=2 Destination Port Unreachable
From 10.0.0.2 icmp_seq=3 Destination Port Unreachable
^C
--- 10.0.0.2 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2114ms
```

Step 8: Accept all the traffic on Computer 2

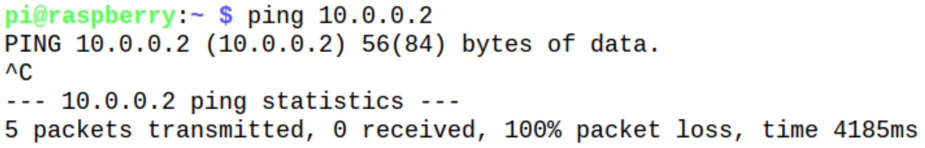
```
sudo iptables -P INPUT -s 10.0.0.1 -j ACCEPT
```



```
pi@raspberry:~ $ ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=0.701 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.718 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.746 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=0.702 ms
^C
--- 10.0.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3098ms
rtt min/avg/max/mdev = 0.701/0.716/0.746/0.037 ms
```

Step 9: Block incoming ping request with iptables

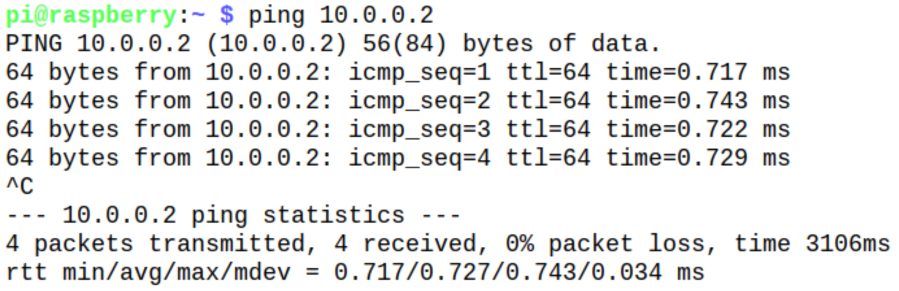
```
sudo iptables -P INPUT -p ICMP -i <ethernet-interface-name-Computer2> -j DROP
```



```
pi@raspberry:~ $ ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
^C
--- 10.0.0.2 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4185ms
```

Step 10: Accept incoming ping request with iptables

```
sudo iptables -P INPUT -p ICMP -i <ethernet-interface-name-Computer2> -j
ACCEPT
```



```
pi@raspberry:~ $ ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=0.717 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.743 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.722 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=0.729 ms
^C
--- 10.0.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3106ms
rtt min/avg/max/mdev = 0.717/0.727/0.743/0.034 ms
```

Additional

Try to drop and accept packets from particular MAC address