Computer Networks

==========

Name: Jitendra Kumar Patel **Roll Number:** MT2014044

Ankit Mishra MT2014009

Ankit Ratnawat MT2014010

==========

Question 1 : Perform NAT and ip filtering using 'iptables' . Access internet from your wired client using the router system.

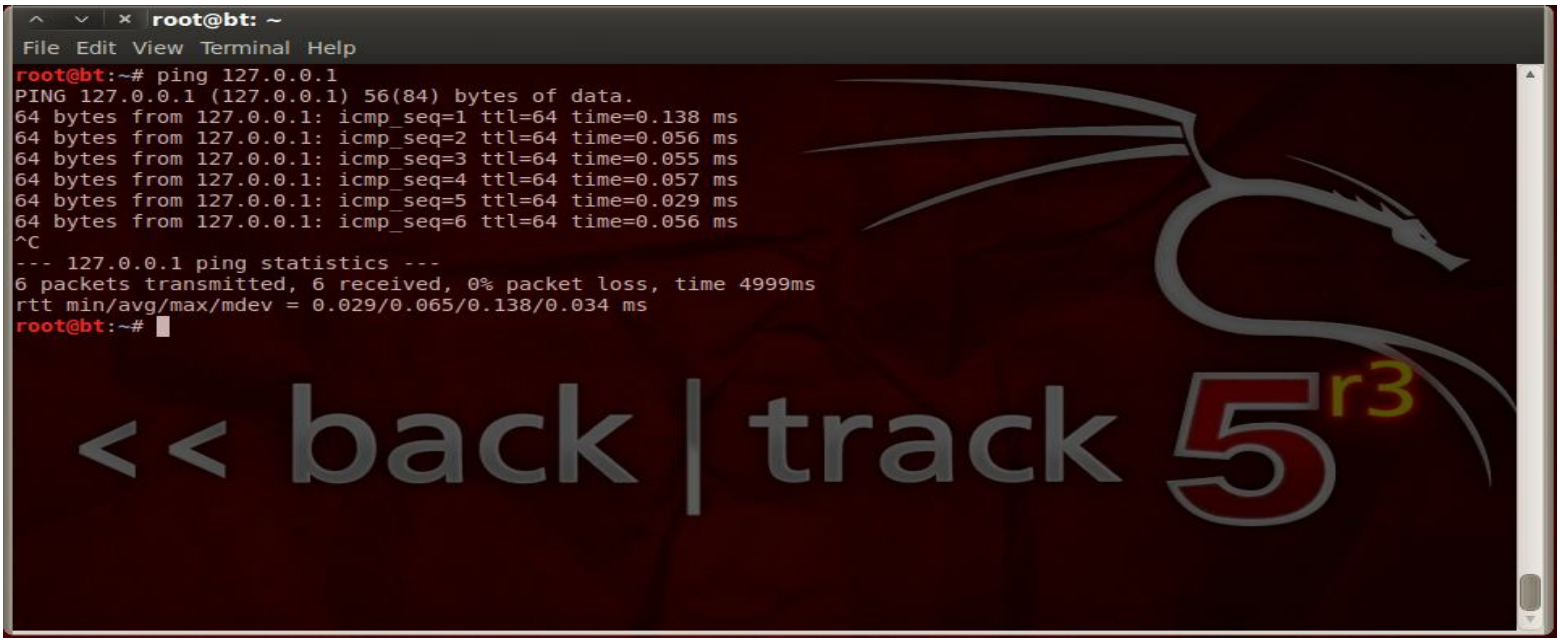
(I). Learn & perform how to accept or reject packets using 'iptables'. Take for example Ping Packets :

Sol. **To Accept :** iptables -A INPUT -s 0/0 -p icmp -j Accept

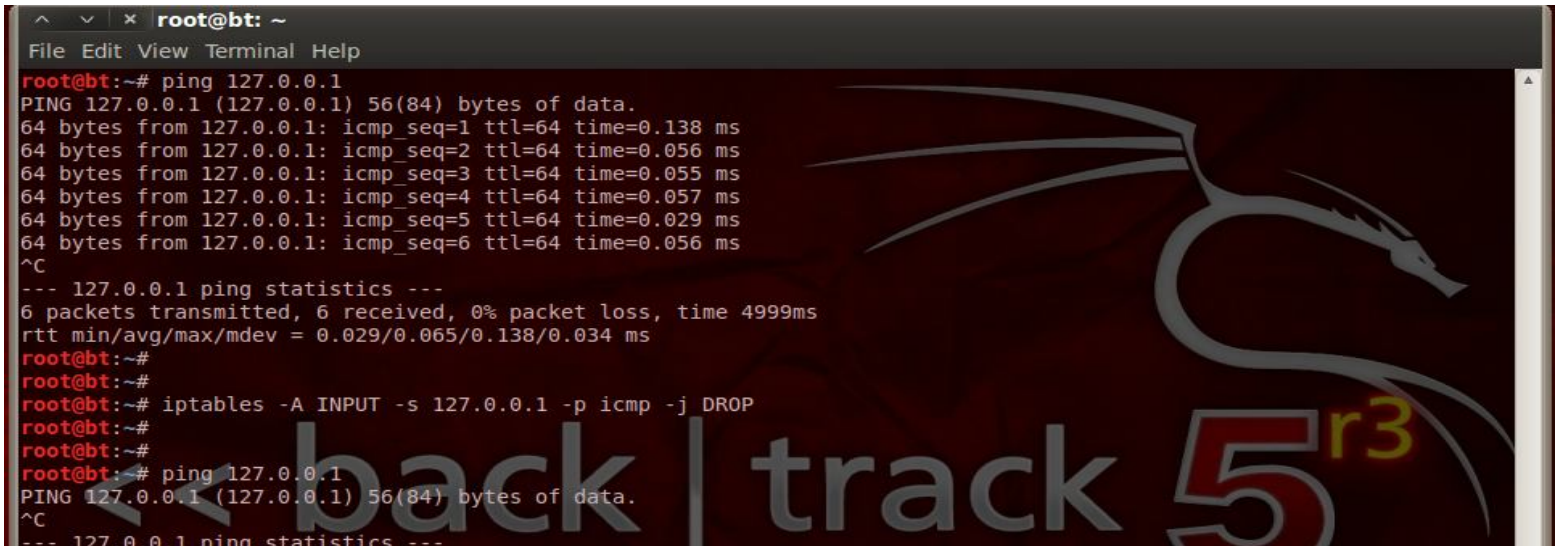
To Reject : iptables -A INPUT -s 0/0 -p icmp -j DROP

Screenshot :

Ping Reply Before configuring iptables to block ICMP packets.



Ping Blocked After configuring iptables to block ICMP packets.



(II). Learn & perform NATting on a particular interface using 'iptables'

Sol.

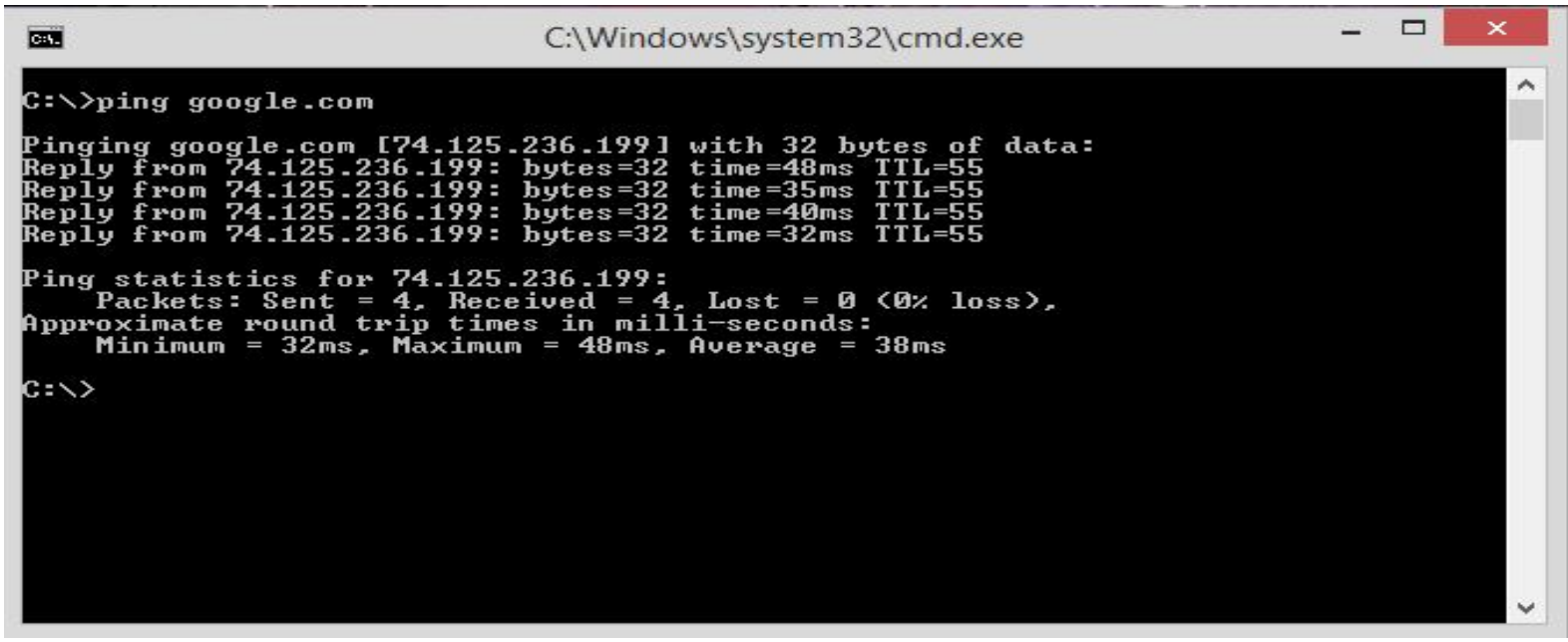
At Router:

iptables -t nat -A POSTROUTING -o wlan0 -j MASQUERADE

iptables -A FORWARD -i eth0 -j ACCEPT

At Wired Client :

ping google.com



Question 2 : ARP(Address Resolution Protocols)

IP Address ------ARP TABLE-------> MAC address

(I). Where is the ARP table stored in my machine?

Sol. ARP table is/can be stored in any of the networking device like Router,Switches,Network Printers,Personal Computers etc.

For Windows : Cache (arp -a >> arp.txt)

For Linux : Cache (/proc/net/arp)

(II). How can I use 'ip' command to flush all the entries of ARP Table?(Is there any such option available with 'arp' command)

Sol. 'ip' command is only available for linux which can be used to flush all the entries of ARP Table.

The command is "ip n flush all" without quotes.

'arp' command is not able to clear all the entries in arp table but can remove individual entries.

However to flush all the entries of ARP Table in Windows we can use the command

"netsh interface ip delete arpcache" without quotes.

Screenshot :

ARP Entries Before Flush Linux

```
root@bt: ~/Desktop/untitled folder
File  Edit  View  Terminal  Help
root@bt:~/Desktop/untitled folder# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.71.2             ether   00:50:56:f4:ea:a9   C                     eth1
192.168.71.254           ether   00:50:56:f3:c8:ad   C                     eth1
192.168.71.130           ether   00:0c:29:44:71:7c   C                     eth1
root@bt:~/Desktop/untitled folder#
```

ARP Entries After Flush Linux

```
root@bt: ~/Desktop/untitled folder
File  Edit  View  Terminal  Help
root@bt:~/Desktop/untitled folder# ip n flush all
root@bt:~/Desktop/untitled folder# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.71.2                     (incomplete)                              eth1
192.168.71.254                   (incomplete)                              eth1
192.168.71.130                   (incomplete)                              eth1
root@bt:~/Desktop/untitled folder#
```

ARP Entries Before Flush windows

```
Administrator: Command Prompt

C:\>arp -a

Interface: 10.5.49.35 --- 0x4
  Internet Address      Physical Address      Type
  10.5.48.1             40-f2-e9-39-90-eb     dynamic
  10.5.49.30            e0-06-e6-8d-ba-ab     dynamic
  10.5.49.108           44-6d-57-9e-35-e9     dynamic
  10.5.49.135           40-f2-e9-39-90-eb     dynamic
  10.5.49.220           40-f2-e9-39-90-eb     dynamic
  10.5.51.90            00-24-2c-a1-05-21     dynamic
  10.5.55.255           ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 172.19.0.1 --- 0x1a
  Internet Address      Physical Address      Type
  172.19.0.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.16.1 --- 0x1d
  Internet Address      Physical Address      Type
  192.168.16.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.71.1 --- 0x1e
  Internet Address      Physical Address      Type
  192.168.71.130        00-0c-29-44-71-7c     dynamic
  192.168.71.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\>_
```

ARP Entries After Flush Windows

```
Administrator: Command Prompt
C:\>netsh interface ip delete arpcache
Ok.

C:\>arp -a

Interface: 10.5.49.35 --- 0x4
  Internet Address      Physical Address      Type
  10.5.48.1             40-f2-e9-39-90-eb     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 172.19.0.1 --- 0x1a
  Internet Address      Physical Address      Type
  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

Interface: 192.168.16.1 --- 0x1d
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.71.1 --- 0x1e
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\>
```

(III). How can I create manual entry in ARP Table for a host using 'arp' command?

Sol. Manual entry can be created using the arp utility and different availabel swtiches in different Operating System .

For Windows : arp -s 192.168.1.10 aa:bb:cc:dd:ee:ff

For Linux : arp -i eth1 192.168.1.55 aa:bb:cc:dd:ee:ff

<u>Screenshot :</u>

ARP entries before adding static entry in Windows

```
Administrator: Command Prompt
C:\Windows\system32>arp -a

Interface: 10.5.49.35 --- 0x4
  Internet Address      Physical Address      Type
  10.5.48.1             40-f2-e9-39-90-eb     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.56.1 --- 0x16
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 172.19.0.1 --- 0x1a
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.16.1 --- 0x1d
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.71.1 --- 0x1e
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\Windows\system32>
```

ARP entries after adding static entry in windows

```
Administrator: Command Prompt
C:\Windows\system32>arp -a

Interface: 10.5.49.35 --- 0x4
  Internet Address      Physical Address      Type
  10.5.48.1             40-f2-e9-39-90-eb     dynamic
  10.5.55.255           ff-ff-ff-ff-ff-ff     static
  192.168.1.10          aa-bb-cc-dd-ee-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.56.1 --- 0x16
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 172.19.0.1 --- 0x1a
  Internet Address      Physical Address      Type
  172.19.0.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.16.1 --- 0x1d
  Internet Address      Physical Address      Type
  192.168.16.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.71.1 --- 0x1e
  Internet Address      Physical Address      Type
  192.168.71.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\Windows\system32>
```

ARP entries before adding static entry in Linux

```
root@bt: /
File Edit View Terminal Help
root@bt:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.71.2             ether   00:50:56:f4:ea:a9   C                     eth1
root@bt:/#
```

ARP entries after adding static entry in Linux

```
root@bt: /
File Edit View Terminal Help
root@bt:/# arp -i eth1 -s 192.168.1.10 aa:bb:cc:dd:ee:ff
root@bt:/#
root@bt:/#
root@bt:/#
root@bt:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.71.2             ether   00:50:56:f4:ea:a9   C                     eth1
192.168.1.10             ether   aa:bb:cc:dd:ee:ff   CM                    eth1
root@bt:/#
```

(IV). Is the entry created a static or dynamic? (Hint: ping)

Sol. The entry created after pinging a host is of type "Dynamic".

<u>ScreenShot :</u>

ARP Entry Before Executing Ping Command Linux

```
root@bt: /
File Edit View Terminal Help
root@bt:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.71.2             ether   00:50:56:f4:ea:a9   C                     eth1
root@bt:/#
```

ARP Entry After Executing Ping Command Linux

```
root@bt: /
File  Edit  View  Terminal  Help
root@bt:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.71.2             ether   00:50:56:f4:ea:a9   C                     eth1
root@bt:/# ping 192.168.71.130
PING 192.168.71.130 (192.168.71.130) 56(84) bytes of data.
64 bytes from 192.168.71.130: icmp_seq=1 ttl=64 time=9.39 ms
64 bytes from 192.168.71.130: icmp_seq=2 ttl=64 time=0.280 ms
64 bytes from 192.168.71.130: icmp_seq=3 ttl=64 time=0.478 ms
64 bytes from 192.168.71.130: icmp_seq=4 ttl=64 time=0.355 ms
64 bytes from 192.168.71.130: icmp_seq=5 ttl=64 time=0.242 ms
64 bytes from 192.168.71.130: icmp_seq=6 ttl=64 time=0.459 ms
^C
--- 192.168.71.130 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5002ms
rtt min/avg/max/mdev = 0.242/1.868/9.398/3.368 ms
root@bt:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.71.2             ether   00:50:56:f4:ea:a9   C                     eth1
192.168.71.130           ether   00:0c:29:44:71:7c   C                     eth1
root@bt:/#
```

ARP Entry Before Executing Ping Command Windows

```
Administrator: Command Prompt
C:\>arp -a

Interface: 10.5.49.35 --- 0x4
  Internet Address      Physical Address      Type
  10.5.48.1             40-f2-e9-39-90-eb     dynamic
  10.5.55.255           ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     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

Interface: 172.19.0.1 --- 0x1a
  Internet Address      Physical Address      Type
  172.19.0.255          ff-ff-ff-ff-ff-ff     static
  192.168.173.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     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

Interface: 192.168.16.1 --- 0x1d
  Internet Address      Physical Address      Type
  192.168.16.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     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

Interface: 192.168.71.1 --- 0x1e
  Internet Address      Physical Address      Type
  192.168.71.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\>
```

ARP Entry After Executing Ping Command Windows

```
Administrator: Command Prompt

C:\>ping 192.168.71.130

Pinging 192.168.71.130 with 32 bytes of data:
Reply from 192.168.71.130: bytes=32 time=18ms TTL=64
Reply from 192.168.71.130: bytes=32 time<1ms TTL=64
Reply from 192.168.71.130: bytes=32 time<1ms TTL=64
Reply from 192.168.71.130: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.71.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 18ms, Average = 4ms

C:\>arp -a

Interface: 10.5.49.35 --- 0x4
  Internet Address      Physical Address      Type
  10.5.48.1             40-f2-e9-39-90-eb     dynamic
  10.5.49.220           40-f2-e9-39-90-eb     dynamic
  10.5.55.255           ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     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

Interface: 172.19.0.1 --- 0x1a
  Internet Address      Physical Address      Type
  172.19.0.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     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

Interface: 192.168.16.1 --- 0x1d
  Internet Address      Physical Address      Type
  192.168.16.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     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

Interface: 192.168.71.1 --- 0x1e
  Internet Address      Physical Address      Type
  192.168.71.130        00-0c-29-44-71-7c     dynamic
  192.168.71.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\>
```

(V). How can you set a policy for accepting/rejecting packets from a particular source IP using 'iptables' command ?

Sol. **To Accept :** iptables -A INPUT -s 127.0.0.1 -p icmp -j Accept

To Reject : iptables -A INPUT -s 127.0.0.1 -p icmp -j DROP

<u>Screenshot :</u>

Ping Reply Before configuring iptables to block ICMP packets.

```
root@bt: ~
File  Edit  View  Terminal  Help
root@bt:~# ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.138 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.056 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.055 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.057 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.029 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.056 ms
^C
--- 127.0.0.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
```

Ping Blocked After configuring iptables to block ICMP packets.

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.138 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.056 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.055 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.057 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.029 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.056 ms
^C
--- 127.0.0.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
rtt min/avg/max/mdev = 0.029/0.065/0.138/0.034 ms
root@bt:~#
root@bt:~#
root@bt:~# iptables -A INPUT -s 127.0.0.1 -p icmp -j DROP
root@bt:~#
root@bt:~#
root@bt:~# ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
^C
--- 127.0.0.1 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7002ms

root@bt:~#
```

Question 3 : Make your linux box into a router and create static routes to establish communication to your teammate's machine having ip in different subnet.

(I). Make use of 'route' command to connect to wireless & wired client from the router

Sol.

At Router :

route add -host 192.168.1.44 gw 192.168.1.44 dev eth0

route add -host 10.100.100.9 gw 10.100.100.9 dev wlan0

At Wired Client :

route add -host 10.100.100.9 gw 192.168.1.10 eth0

At Wireless Client :

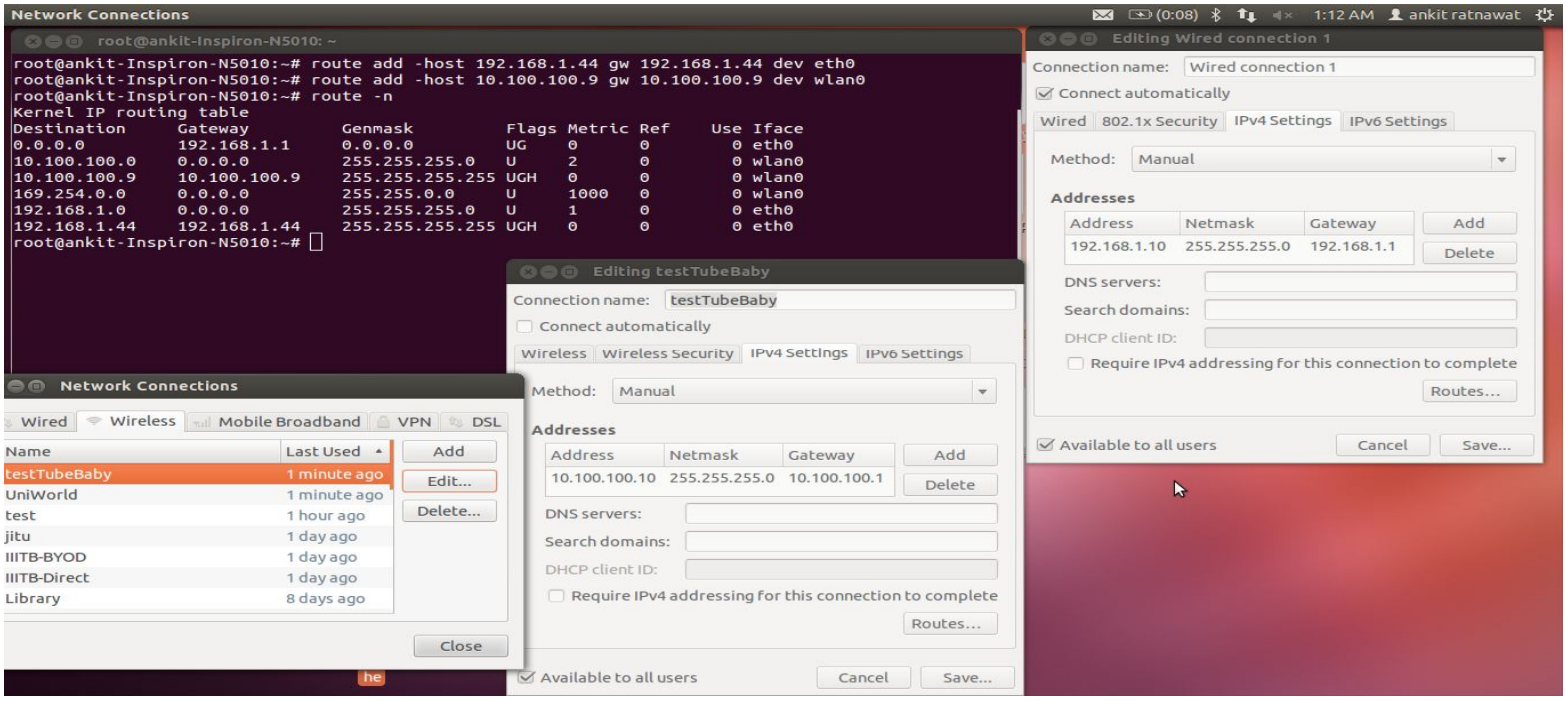
route add -host 192.168.1.44 gw 10.100.100.10 wlan0

<u>Screenshot :</u>

Ip Forwarding is enabled

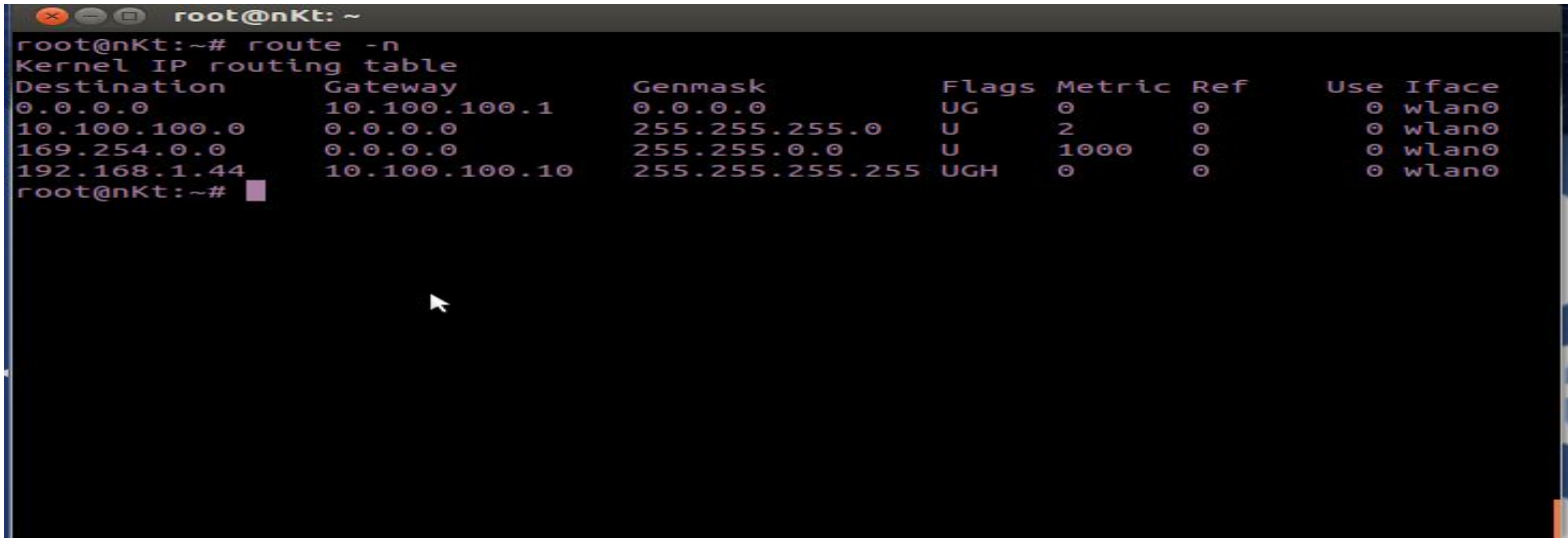
```
root@ankit-Inspiron-N5010: ~
root@ankit-Inspiron-N5010:~# cat /proc/sys/net/ipv4/ip_forward
1
root@ankit-Inspiron-N5010:~#
```

Router Configuration



Wired Client Configuration

Wireless Client Configuration



(II). Use 'iptables' command to forward the packets accordingly.

Sol.

At Router :

iptables -t nat -A POSTROUTING -o wlan0 -j ACCEPT

iptables -A FORWARD -i eth0 -j ACCEPT

(III). Use 'wireshark' to capture the differences.

Sol. Done

Question 4 : Perform NAT and ip filtering using 'iptables' . Access internet from your wired client using the router system.

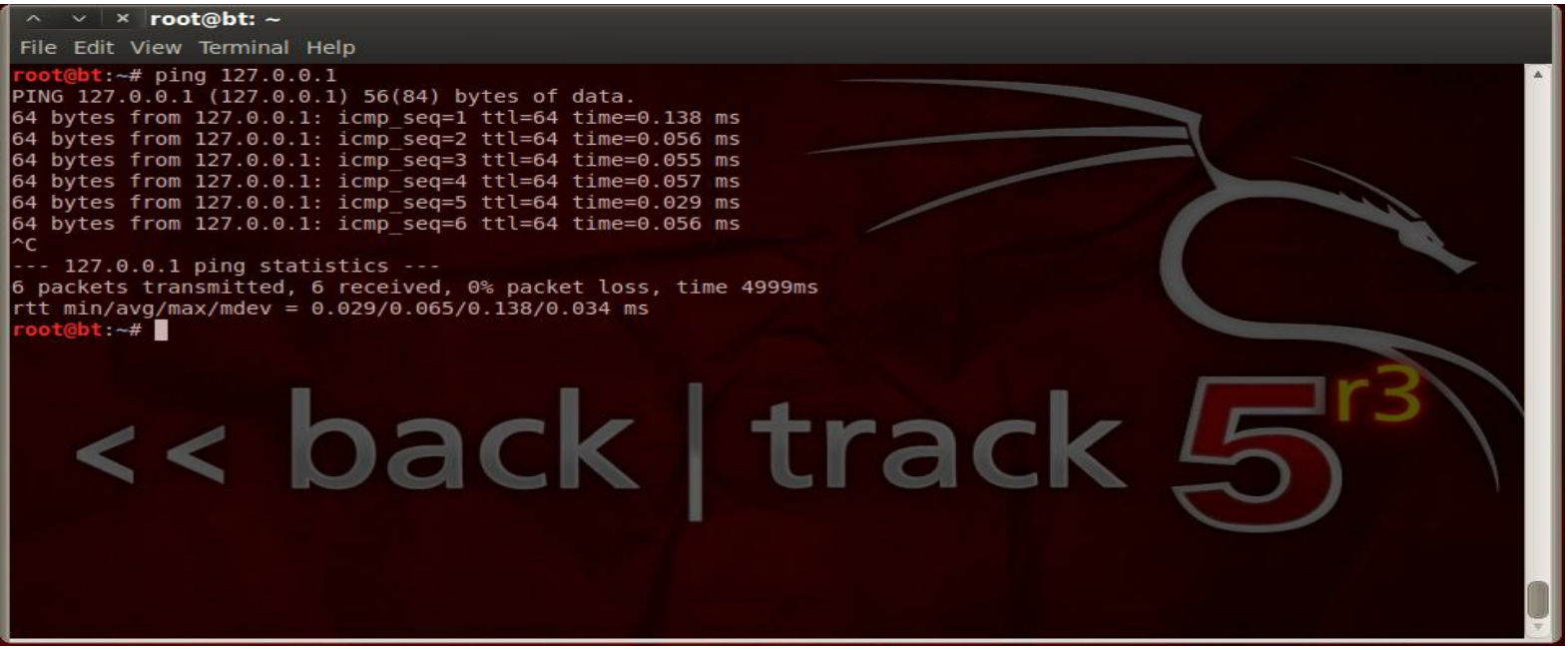
(I). Learn & perform how to accept or reject packets using 'iptables'.

Sol. **To Accept :** iptables -A INPUT -s 0/0 -p icmp -j Accept

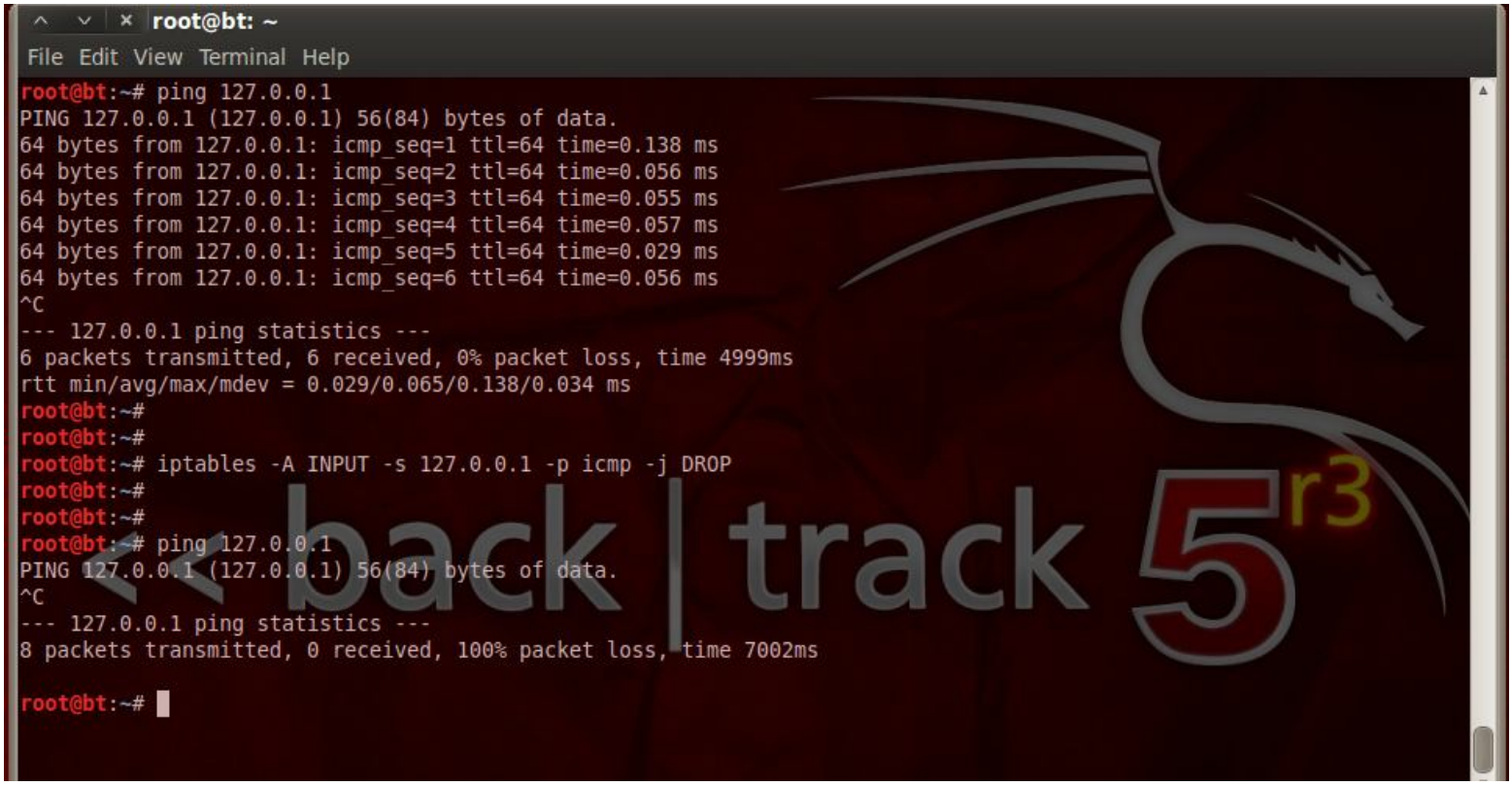
To Reject : iptables -A INPUT -s 0/0 -p icmp -j DROP

<u>Screenshot :</u>

Ping Reply Before configuring iptables to block ICMP packets.



Ping Blocked After configuring iptables to block ICMP packets.



(II). Learn & perform NATting on a particular interface using 'iptables'.

Sol.

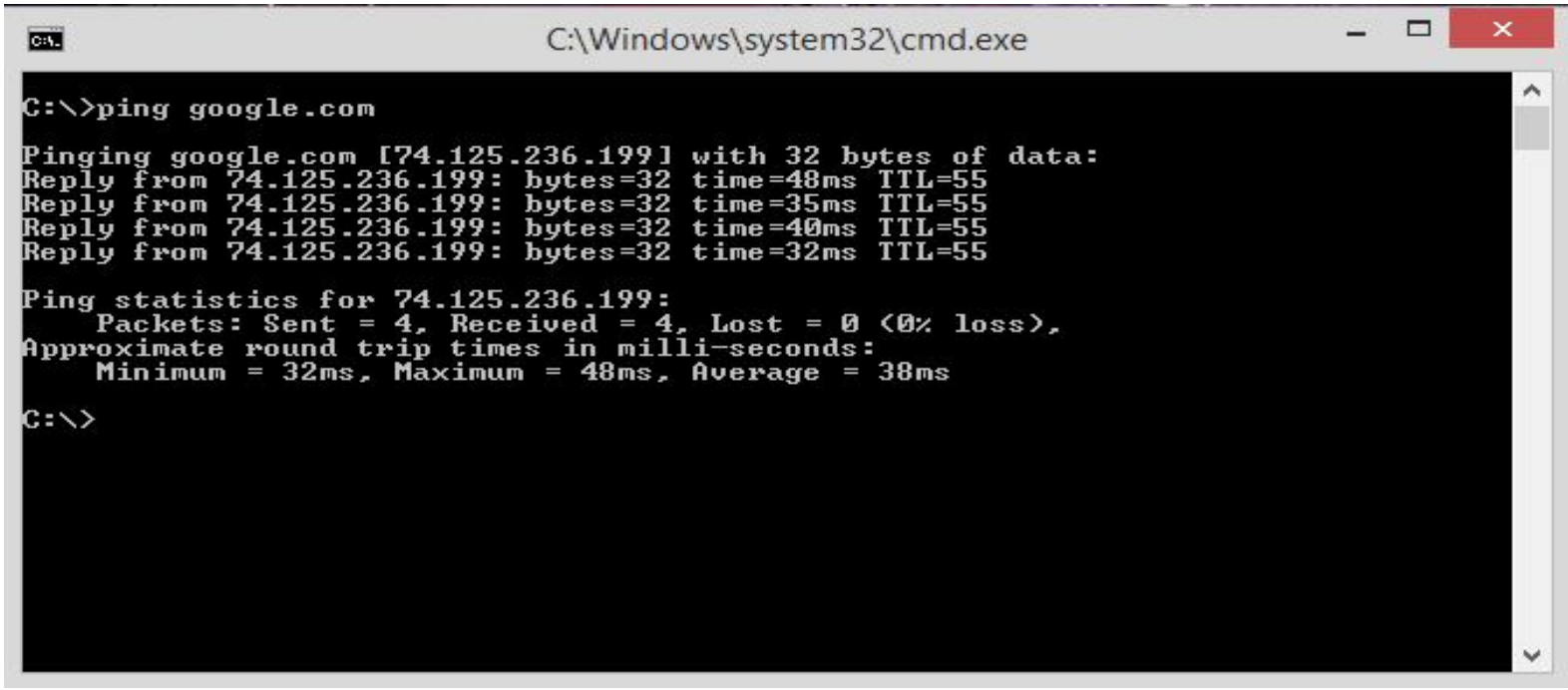
At Router :

iptables -t nat -A POSTROUTING -o wlan0 -j MASQUERADE

iptables -A FORWARD -i eth0 -j ACCEPT

At Wired Client :

ping google.com



==========END==========