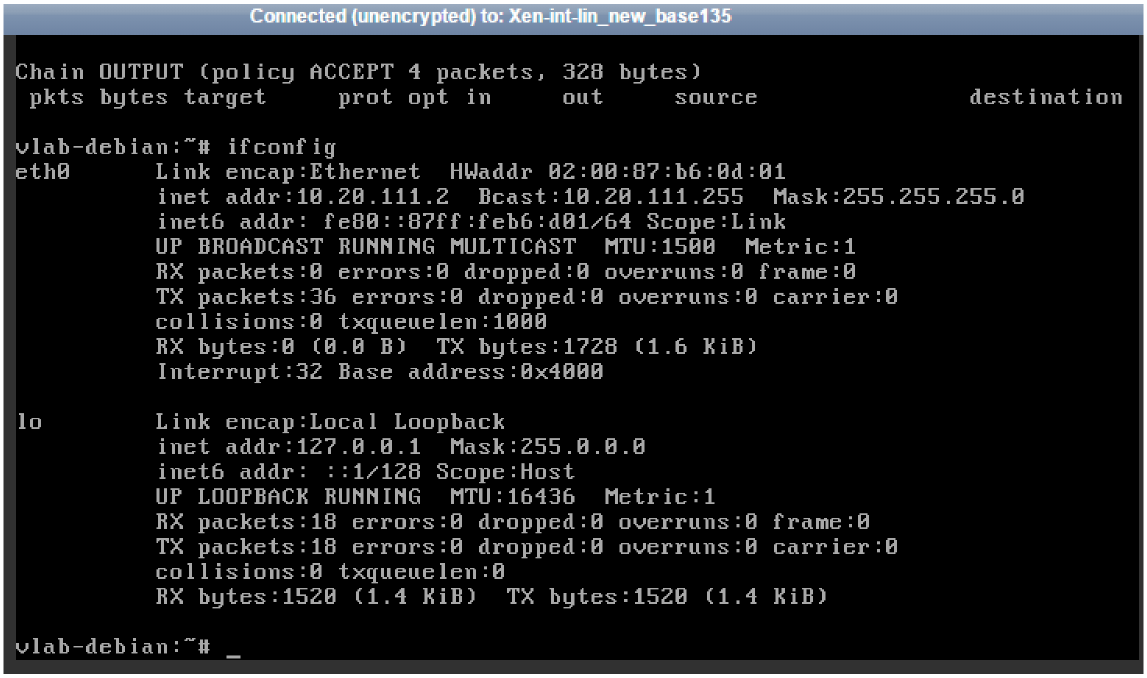
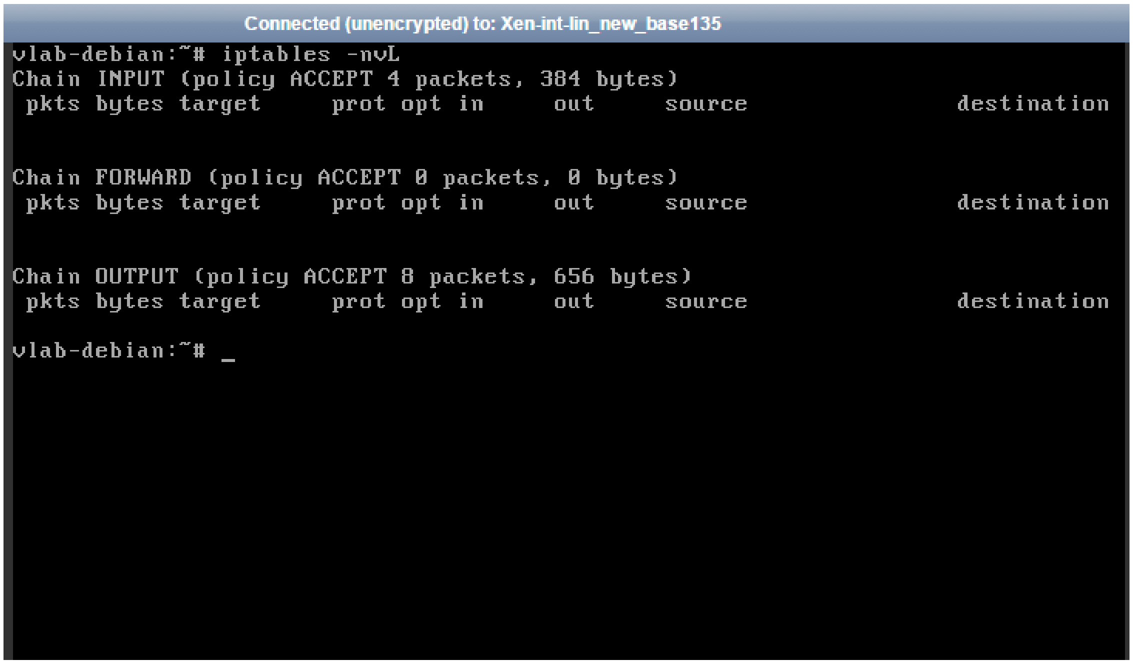
Internal Linux: IP configuration



```
Chain OUTPUT (policy ACCEPT 4 packets, 328 bytes)
 pkts bytes target     prot opt in     out     source               destination

vlab-debian:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 02:00:87:b6:0d:01
          inet addr:10.20.111.2  Bcast:10.20.111.255  Mask:255.255.255.0
          inet6 addr: fe80::87ff:feb6:d01/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:1728 (1.6 KiB)
          Interrupt:32 Base address:0x4000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1520 (1.4 KiB)  TX bytes:1520 (1.4 KiB)

vlab-debian:~# _
```

Initial IP Table:

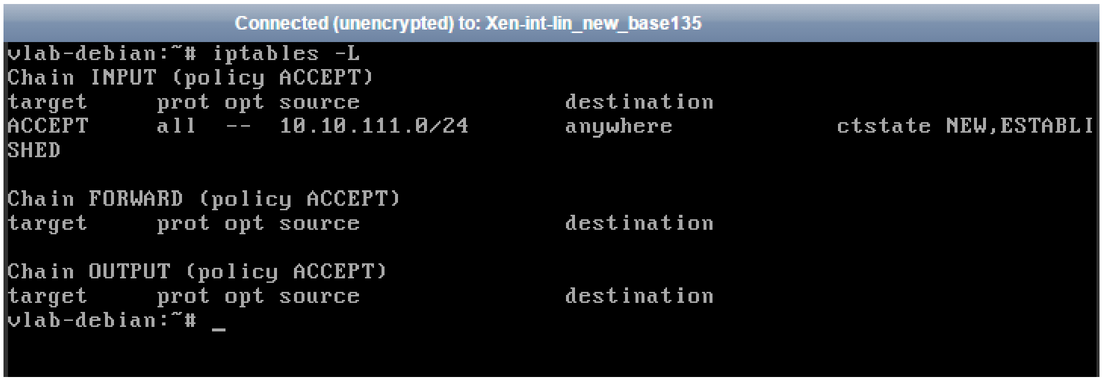


```
vlab-debian:~# iptables -nvL
Chain INPUT (policy ACCEPT 4 packets, 384 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy ACCEPT 8 packets, 656 bytes)
 pkts bytes target     prot opt in     out     source               destination

vlab-debian:~# _
```

PART A

1) [15 pts] The internal machine should respond to a ping from 10.10.111.0/24:

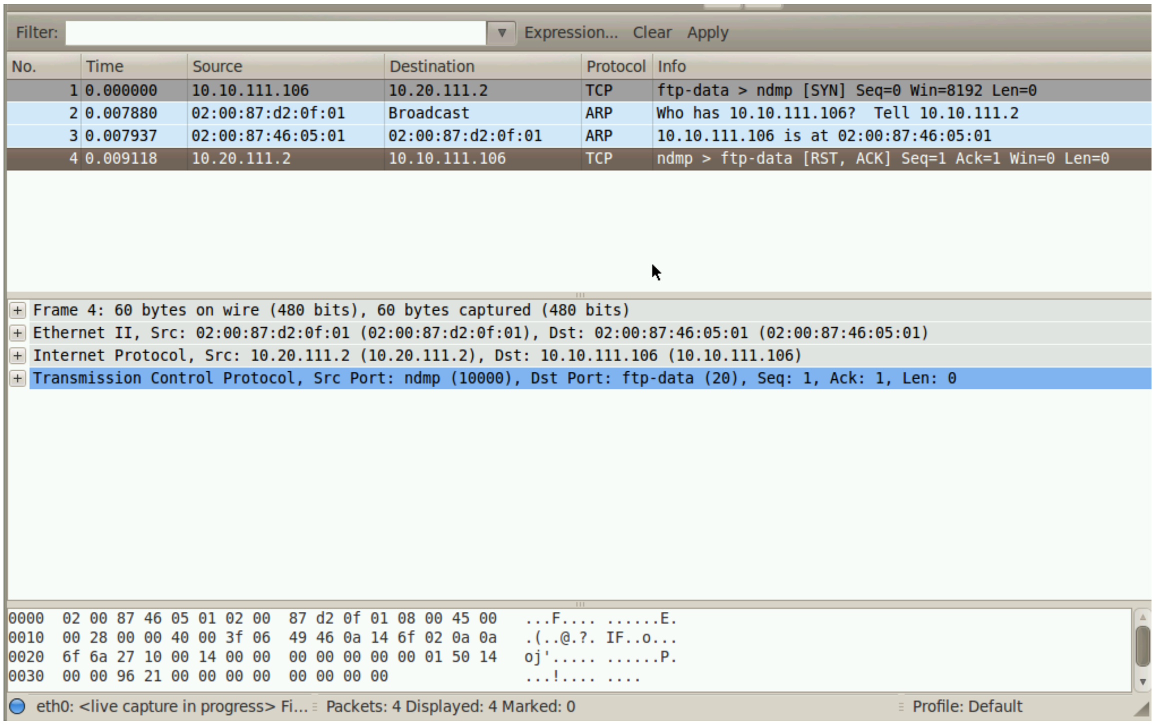
-> iptables -A INPUT -s 10.10.111.0/24 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT



Connected (unencrypted) to: Xen-int-lin_new_base135

```
vlab-debian:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  10.10.111.0/24       anywhere             ctstate NEW,ESTABLI
SHED

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
vlab-debian:~# _
```

TCP Packet sent from BT5 and monitored using WIRESHARK



No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.10.111.106	10.20.111.2	TCP	ftp-data > ndmp [SYN] Seq=0 Win=8192 Len=0
2	0.007880	02:00:87:d2:0f:01	Broadcast	ARP	Who has 10.10.111.106? Tell 10.10.111.2
3	0.007937	02:00:87:46:05:01	02:00:87:d2:0f:01	ARP	10.10.111.106 is at 02:00:87:46:05:01
4	0.009118	10.20.111.2	10.10.111.106	TCP	ndmp > ftp-data [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

```
+ Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
+ Ethernet II, Src: 02:00:87:d2:0f:01 (02:00:87:d2:0f:01), Dst: 02:00:87:46:05:01 (02:00:87:46:05:01)
+ Internet Protocol, Src: 10.20.111.2 (10.20.111.2), Dst: 10.10.111.106 (10.10.111.106)
+ Transmission Control Protocol, Src Port: ndmp (10000), Dst Port: ftp-data (20), Seq: 1, Ack: 1, Len: 0
```

```
0000  02 00 87 46 05 01 02 00  87 d2 0f 01 08 00 45 00   ...F.... ......E.
0010  00 28 00 00 40 00 3f 06  49 46 0a 14 6f 02 0a 0a   .(..@.?. IF..o...
0020  6f 6a 27 10 00 14 00 00  00 00 00 00 00 01 50 14   oj'..... ......P.
0030  00 00 96 21 00 00 00 00  00 00 00 00              ...!.... ....
```

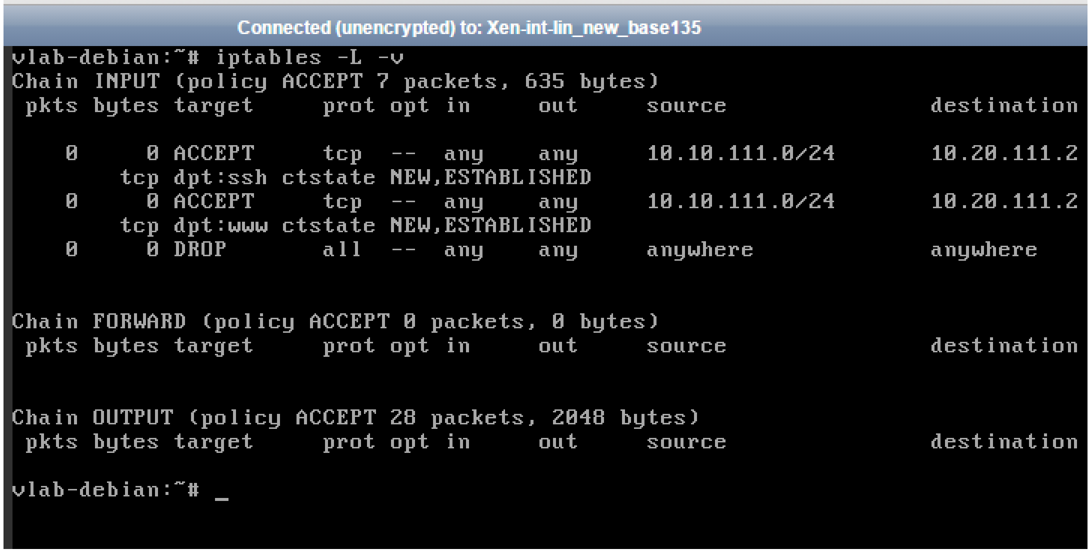
eth0: <live capture in progress> Fi... Packets: 4 Displayed: 4 Marked: 0 Profile: Default

2) [15 pts] The internal machine (10.20.111.2) should accept all incoming SSH and http requests from 10.10.111.0/24.

-> iptables -A INPUT -p tcp –dport ssh -d 10.20.111.2 -s 10.10.111.0/24 -m conntrack –ctstate NEW,EXTABLISHED -j ACCEPT

-> iptables -A INPUT -p tcp --dport 80 -d 10.20.111.2 -s 10.10.111.0/24 -m conntrack –ctstate NEW,EXTABLISHED -j ACCEPT

-> iptables -A INPUT -j DROP {to drop any other request other than SSH and WWW}

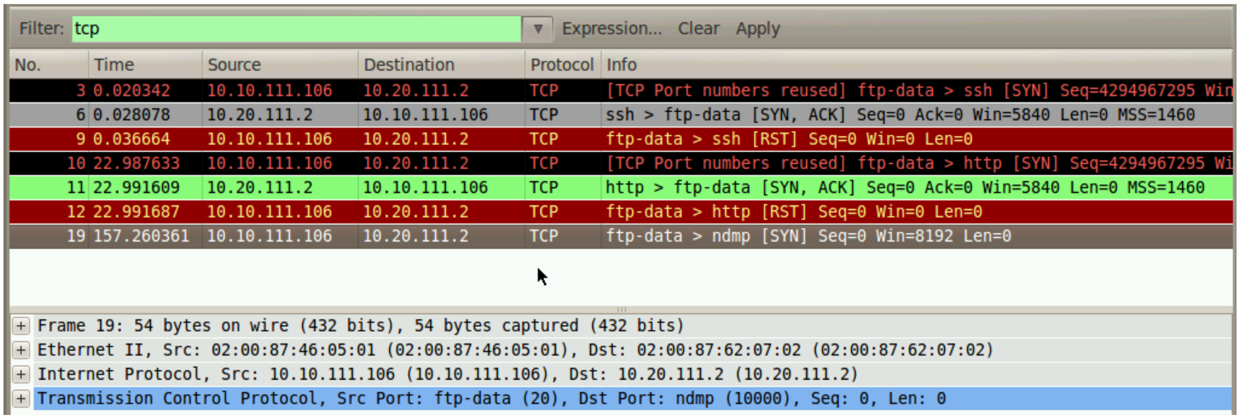


Connected (unencrypted) to: Xen-int-lin_new_base135

```
vlab-debian:~# iptables -L -v
Chain INPUT (policy ACCEPT 7 packets, 635 bytes)
 pkts bytes target     prot opt in     out     source               destination

    0     0 ACCEPT     tcp  --  any    any     10.10.111.0/24       10.20.111.2
        tcp dpt:ssh ctstate NEW,ESTABLISHED
    0     0 ACCEPT     tcp  --  any    any     10.10.111.0/24       10.20.111.2
        tcp dpt:www ctstate NEW,ESTABLISHED
    0     0 DROP       all  --  any    any     anywhere             anywhere


Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy ACCEPT 28 packets, 2048 bytes)
 pkts bytes target     prot opt in     out     source               destination

vlab-debian:~# _
```

After sending 3 packets to the internal linux router i.e., at port 22(SSH), port 80(WWW) and port 10000, we received response for the first 2 packets but no response for the last one as the iptable has DROP entry for anything other than port 22 and port 80.

Wireshark shows the same in below screenshot

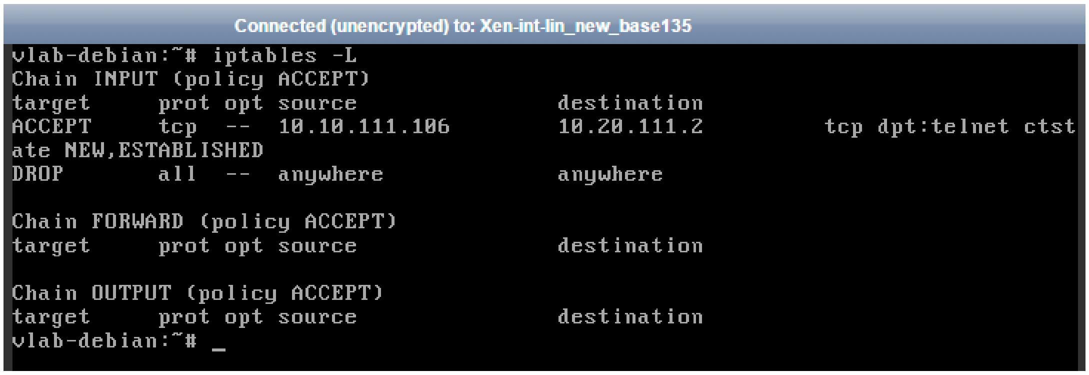


```
No.   Time        Source          Destination     Protocol  Info
    3 0.020342    10.10.111.106   10.20.111.2     TCP       [TCP Port numbers reused] ftp-data > ssh [SYN] Seq=4294967295 Win
    6 0.028078    10.20.111.2     10.10.111.106   TCP       ssh > ftp-data [SYN, ACK] Seq=0 Ack=0 Win=5840 Len=0 MSS=1460
    9 0.036664    10.10.111.106   10.20.111.2     TCP       ftp-data > ssh [RST] Seq=0 Win=0 Len=0
   10 22.987633   10.10.111.106   10.20.111.2     TCP       [TCP Port numbers reused] ftp-data > http [SYN] Seq=4294967295 Wi
   11 22.991609   10.20.111.2     10.10.111.106   TCP       http > ftp-data [SYN, ACK] Seq=0 Ack=0 Win=5840 Len=0 MSS=1460
   12 22.991687   10.10.111.106   10.20.111.2     TCP       ftp-data > http [RST] Seq=0 Win=0 Len=0
   19 157.260361  10.10.111.106   10.20.111.2     TCP       ftp-data > ndmp [SYN] Seq=0 Win=8192 Len=0

+ Frame 19: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
+ Ethernet II, Src: 02:00:87:46:05:01 (02:00:87:46:05:01), Dst: 02:00:87:62:07:02 (02:00:87:62:07:02)
+ Internet Protocol, Src: 10.10.111.106 (10.10.111.106), Dst: 10.20.111.2 (10.20.111.2)
+ Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: ndmp (10000), Seq: 0, Len: 0
```

3) [20 pts] The internal machine should accept telnet connections from the BT Machine only.

-> iptables -A INPUT -p tcp –dport telnet -d 10.20.111.2 -s 10.10.111.106 -m conntrack –ctstate NEW,EXTABLISHED -j ACCEPT

-> iptables -A INPUT -j DROP {to drop any other request other than TELNET}

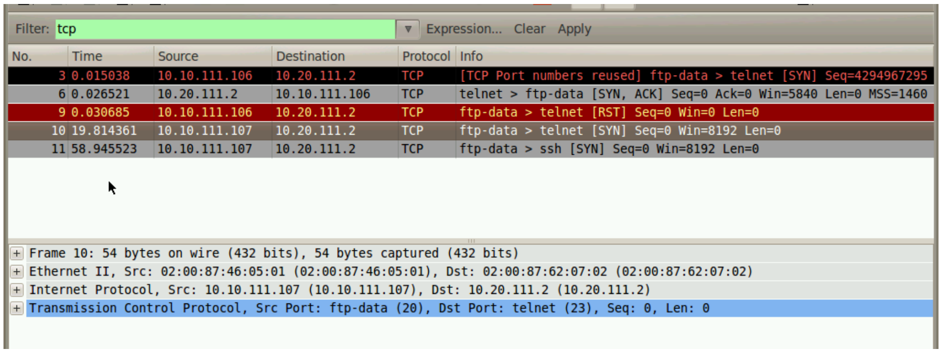


```
vlab-debian:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  10.10.111.106        10.20.111.2          tcp dpt:telnet ctst
ate NEW,ESTABLISHED
DROP       all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
vlab-debian:~# _
```

First packet sent with BT5 IP address i.e., 10.10.111.106 to port 23 and in Wireshark it is observed that a response is obtained from Internal Linux machine.

Other than this 2 more packets were sent one with IP address 10.10.111.107 and one with IP address as 10.10.111.107, port=22, for both of the packet no response obtained from the Linux machine as we have used Drop which drops all the packets that are not from BT5 and to port 23.

Wireshark shows the same in the below screenshot.

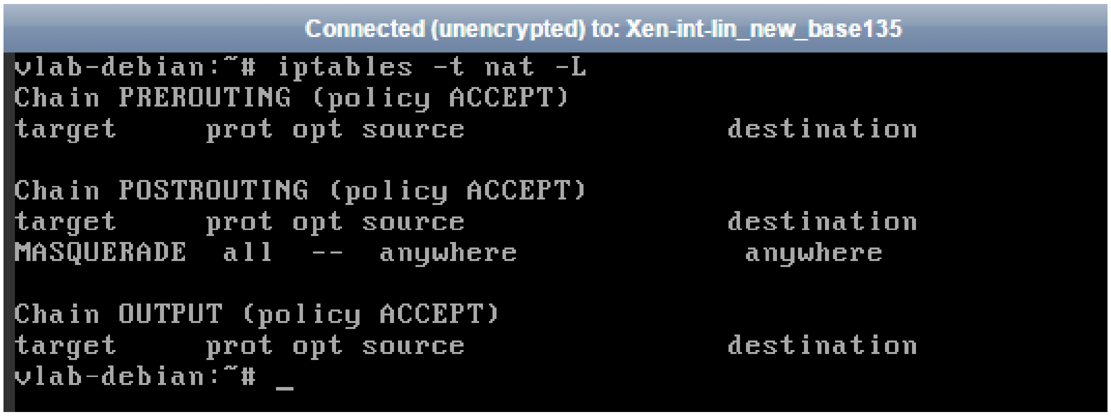


No.	Time	Source	Destination	Protocol	Info
3	0.015038	10.10.111.106	10.20.111.2	TCP	[TCP Port numbers reused] ftp-data > telnet [SYN] Seq=4294967295
6	0.026521	10.20.111.2	10.10.111.106	TCP	telnet > ftp-data [SYN, ACK] Seq=0 Ack=0 Win=5840 Len=0 MSS=1460
9	0.030685	10.10.111.106	10.20.111.2	TCP	ftp-data > telnet [RST] Seq=0 Win=0 Len=0
10	19.814361	10.10.111.107	10.20.111.2	TCP	ftp-data > telnet [SYN] Seq=0 Win=8192 Len=0
11	58.945523	10.10.111.107	10.20.111.2	TCP	ftp-data > ssh [SYN] Seq=0 Win=8192 Len=0

```
+ Frame 10: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
+ Ethernet II, Src: 02:00:87:46:05:01 (02:00:87:46:05:01), Dst: 02:00:87:62:07:02 (02:00:87:62:07:02)
+ Internet Protocol, Src: 10.10.111.107 (10.10.111.107), Dst: 10.20.111.2 (10.20.111.2)
+ Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: telnet (23), Seq: 0, Len: 0
```

PART B

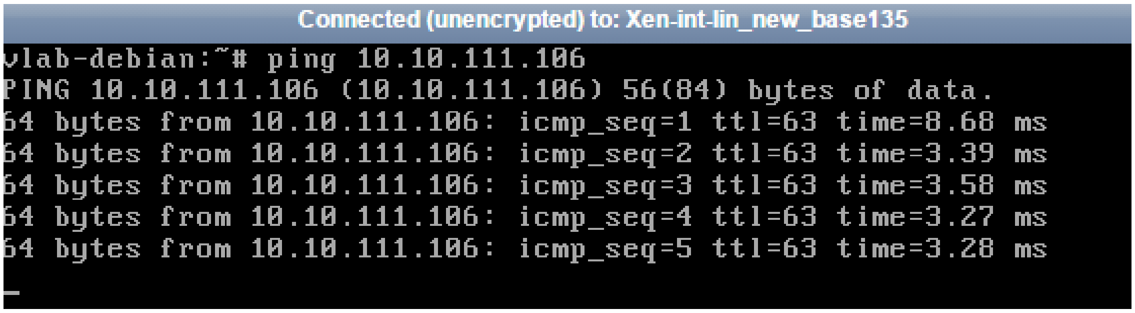
-> iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE



Connected (unencrypted) to: Xen-int-lin_new_base135

```
vlab-debian:~# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
vlab-debian:~# _
```

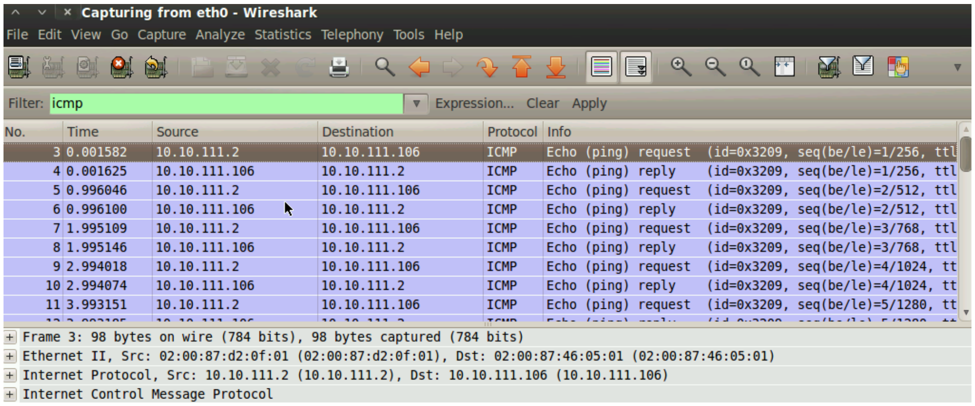
ICMP packets were sent using PING from Linux machine (10.20.111.2) to my BT5 machine (10.10.111.106) using command ‘ping 10.10.111.106’.



Connected (unencrypted) to: Xen-int-lin_new_base135

```
vlab-debian:~# ping 10.10.111.106
PING 10.10.111.106 (10.10.111.106) 56(84) bytes of data.
64 bytes from 10.10.111.106: icmp_seq=1 ttl=63 time=8.68 ms
64 bytes from 10.10.111.106: icmp_seq=2 ttl=63 time=3.39 ms
64 bytes from 10.10.111.106: icmp_seq=3 ttl=63 time=3.58 ms
64 bytes from 10.10.111.106: icmp_seq=4 ttl=63 time=3.27 ms
64 bytes from 10.10.111.106: icmp_seq=5 ttl=63 time=3.28 ms
_
```

For the internal router interface eth0 has IP (10.10.111.2)



Capturing from eth0 - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: icmp
Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
3	0.001582	10.10.111.2	10.10.111.106	ICMP	Echo (ping) request (id=0x3209, seq(be/le)=1/256, ttl
4	0.001625	10.10.111.106	10.10.111.2	ICMP	Echo (ping) reply (id=0x3209, seq(be/le)=1/256, ttl
5	0.996046	10.10.111.2	10.10.111.106	ICMP	Echo (ping) request (id=0x3209, seq(be/le)=2/512, ttl
6	0.996100	10.10.111.106	10.10.111.2	ICMP	Echo (ping) reply (id=0x3209, seq(be/le)=2/512, ttl
7	1.995109	10.10.111.2	10.10.111.106	ICMP	Echo (ping) request (id=0x3209, seq(be/le)=3/768, ttl
8	1.995146	10.10.111.106	10.10.111.2	ICMP	Echo (ping) reply (id=0x3209, seq(be/le)=3/768, ttl
9	2.994018	10.10.111.2	10.10.111.106	ICMP	Echo (ping) request (id=0x3209, seq(be/le)=4/1024, tt
10	2.994074	10.10.111.106	10.10.111.2	ICMP	Echo (ping) reply (id=0x3209, seq(be/le)=4/1024, tt
11	3.993151	10.10.111.2	10.10.111.106	ICMP	Echo (ping) request (id=0x3209, seq(be/le)=5/1280, tt

```
+ Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
+ Ethernet II, Src: 02:00:87:d2:0f:01 (02:00:87:d2:0f:01), Dst: 02:00:87:46:05:01 (02:00:87:46:05:01)
+ Internet Protocol, Src: 10.10.111.2 (10.10.111.2), Dst: 10.10.111.106 (10.10.111.106)
+ Internet Control Message Protocol
```

The packets reached at BT5 seen using Wireshark shows the source IP for ICMP as 10.10.111.2 which is the IP of the eth0 interface of the internal router.

PART C

1) [5 pts] In your own words describe how iptables works?

Ans: IPTables consists of set of rules which governs the network traffic at the firewall. Every packet that reaches the firewall must match the rules mentioned in the iptables to pass through. If the packet does not match any rule, the packet is rejected or dropped based on the iptables settings.

When the packet matches any rule, the action takes place that is mentioned in the rule as target.

2) [5 pts] What is the difference between input, output and forward chains?

Ans: INPUT: This chain handles all the packets that are addressed to your server.

OUTPUT: This chain handles the response/traffic generated by your server

FORWARD: This chain is used to deal with traffic destined for other servers that are not created on your server.

3) [5 pts] What is the difference between deny, reject and accept?

Ans: DENY(DROP): This is the target mentioned in the IPTables, the packet matching the rules containing this as target will drop the packet without any reply to the sender.

REJECT: This is the target mentioned in the IPTables, the packet matching the rules containing this as target will drop the packet but will also send a reply to the sender mentioning the packet is rejected.

ACCEPT: This the target mentioned in the IPTables, the packet matching the rule containing this as target will accept the packet and will perform the action based on the type of chain.