

Virtual Private Network Lab

Name : Ankith J Rai

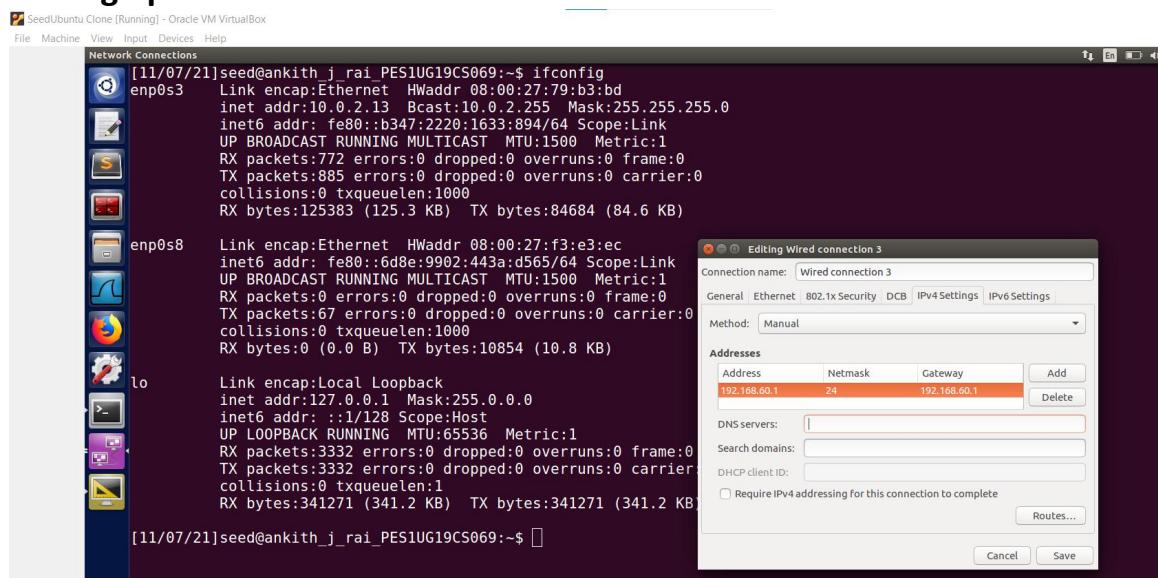
SRN : PES1UG19CS069

SEC : B

<u>Machine</u>	<u>IP address</u>
VPN Client	10.0.2.12
VPN Server	10.0.2.13(NAT network) 192.168.60.1(Internal network)
Host V	192.168.60.101(Internal network)

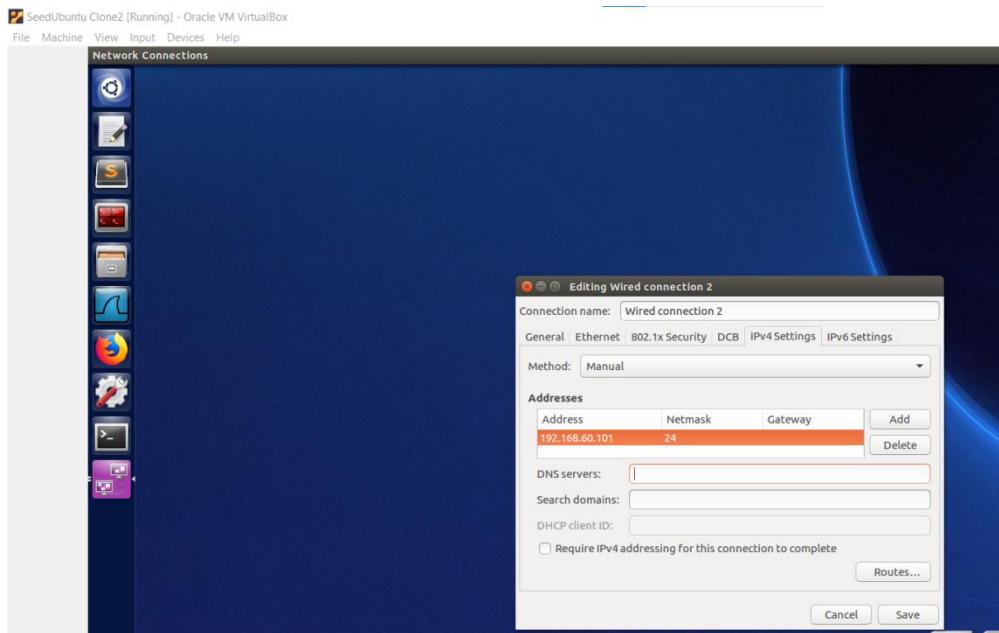
Task 1: VM Setup

Setting up for VM server:



We can see that we have VM Server has been configured.

Setting up for Host V:



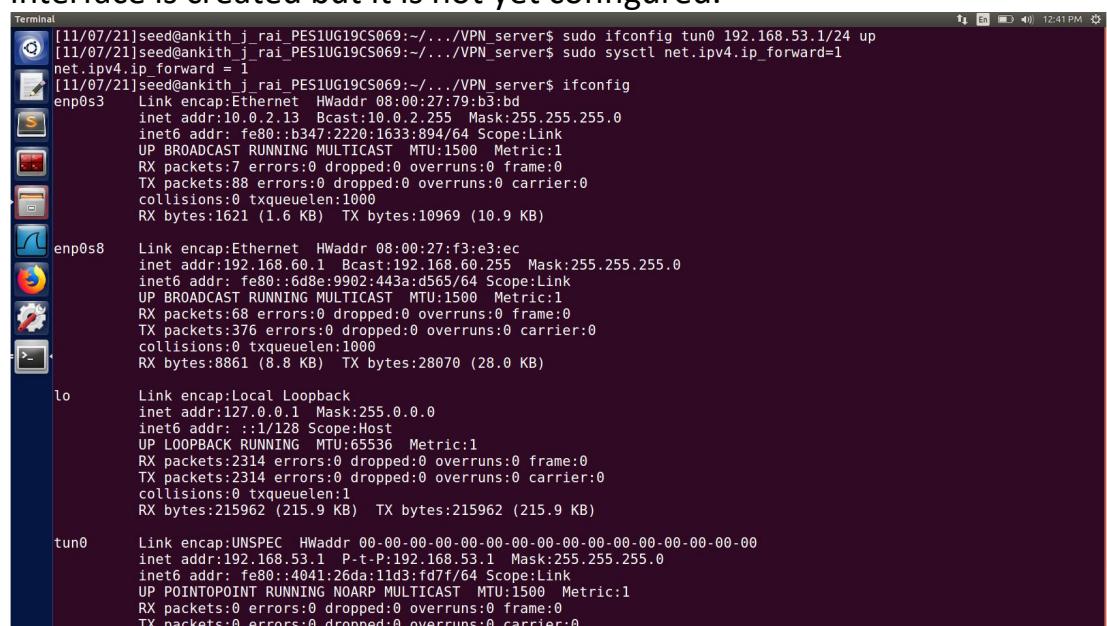
We can see that we have Host V has been configured.

Task 2: Creating a VPN Tunnel using TUN/TA:

Step 1: Run VPN server and set it's IP address of the interface – (Run on VPNServer VM)



We can see that the `vpnserver` program is running. By running this `tun0` interface is created but it is not yet configured.

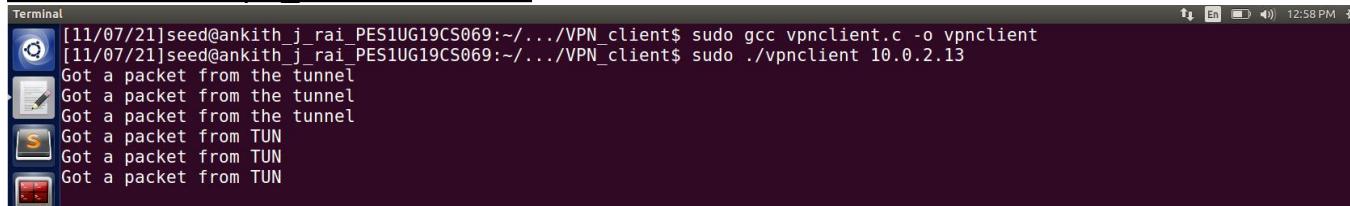


From the above screenshot we can see that a new interface tun0 has been configured and it's ip address is 192.168.53.1 .

From the above screenshot we can also conclude that enp0s3 is the NAT network interface and enp0s8 is the internal network interface.

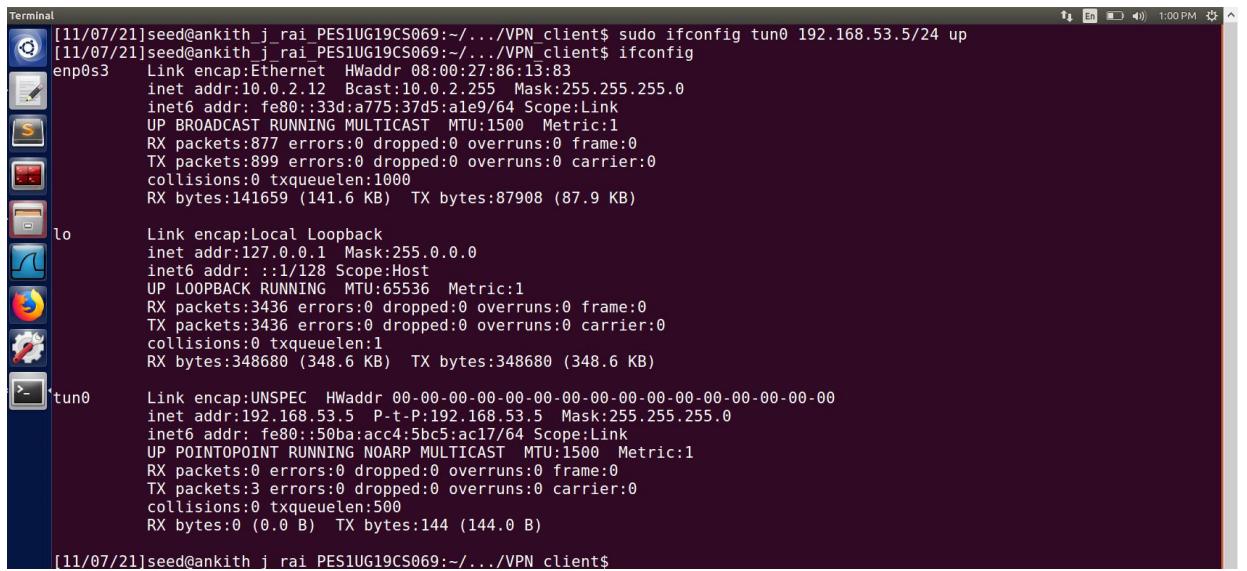
Step 2: Run VPN Client and set IP address of the interface - (Run on VPNClient VM)

Scrennshot of vpn_client machine:



```
[11/07/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$ sudo gcc vpnclient.c -o vpnclient
[11/07/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$ sudo ./vpnclient 10.0.2.13
Got a packet from the tunnel
Got a packet from the tunnel
Got a packet from the tunnel
Got a packet from TUN
Got a packet from TUN
Got a packet from TUN
```

We can see from above screenshot that vpnclient.c program is running and we can see that the tunnel is created between the VPN client and VPN server. Due to the running of vpcclient.c program a new interface called tun0 has been created but it is not yet configured.



```
[11/07/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$ sudo ifconfig tun0 192.168.53.5/24 up
[11/07/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:86:13:83
            inet addr:10.0.2.12 Bcast:10.0.2.255 Mask:255.255.255.0
            inet6 addr: fe80::33d:a775:37d5:ale9/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:877 errors:0 dropped:0 overruns:0 frame:0
            TX packets:899 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:141659 (141.6 KB) TX bytes:87908 (87.9 KB)

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:65536 Metric:1
            RX packets:3436 errors:0 dropped:0 overruns:0 frame:0
            TX packets:3436 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1
            RX bytes:348680 (348.6 KB) TX bytes:348680 (348.6 KB)

tun0        Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
            inet addr:192.168.53.5 P-t-P:192.168.53.5 Mask:255.255.255.0
            inet6 addr: fe80::50ba:acc4:5bc5:ac17/64 Scope:Link
              UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0
            TX packets:3 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:500
            RX bytes:0 (0.0 B) TX bytes:144 (144.0 B)

[11/07/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$
```

We can see that the new interface tun0 which got created when the vpnclient.c was run has been configured and it's ip address is 192.168.53.5 .

Scrennshot of vpn_server machine:

```
[11/07/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_server$ sudo gcc vpnserver.c -o vpnserver
[11/07/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_server$ sudo ./vpnserver
Connected with the client: Hello
Got a packet from TUN
Got a packet from TUN
Got a packet from TUN
Got a packet from the tunnel
Got a packet from the tunnel
Got a packet from the tunnel
```

Step 3: Set up routing on Client and Server VMs

Scrennshot of VPN_client

```
[11/07/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$ sudo route add -net 192.168.53.0/24 tun0
[11/07/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$ route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
0.0.0.0         10.0.2.1       0.0.0.0        UG    100   0    0 enp0s3
10.0.2.0        0.0.0.0        255.255.255.0  U      100   0    0 enp0s3
169.254.0.0     0.0.0.0        255.255.0.0   U      1000  0    0 enp0s3
192.168.53.0    0.0.0.0        255.255.255.0  U      0     0    0 tun0
192.168.53.0    0.0.0.0        255.255.255.0  U      0     0    0 tun0
[11/07/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$ sudo route add -net 192.168.60.0/24 tun0
[11/07/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$ route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
0.0.0.0         10.0.2.1       0.0.0.0        UG    100   0    0 enp0s3
10.0.2.0        0.0.0.0        255.255.255.0  U      100   0    0 enp0s3
169.254.0.0     0.0.0.0        255.255.0.0   U      1000  0    0 enp0s3
192.168.53.0    0.0.0.0        255.255.255.0  U      0     0    0 tun0
192.168.53.0    0.0.0.0        255.255.255.0  U      0     0    0 tun0
192.168.60.0    0.0.0.0        255.255.255.0  U      0     0    0 tun0
[11/07/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$
```

The routes have been successfully added and the now we can route the packets from local tunnel to internal network.

Scrennshot of VPN_server:

```
[11/07/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_server$ sudo route add -net 192.168.53.0/24 tun0
[11/07/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_server$ route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
0.0.0.0         192.168.60.1   0.0.0.0        UG    100   0    0 enp0s8
0.0.0.0         10.0.2.1       0.0.0.0        UG    101   0    0 enp0s3
10.0.2.0        0.0.0.0        255.255.255.0  U      100   0    0 enp0s3
169.254.0.0     0.0.0.0        255.255.0.0   U      1000  0    0 enp0s8
192.168.53.0    0.0.0.0        255.255.255.0  U      0     0    0 tun0
192.168.53.0    0.0.0.0        255.255.255.0  U      0     0    0 tun0
192.168.60.0    0.0.0.0        255.255.255.0  U      0     0    0 tun0
[11/07/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_server$
```

The routes have been successfully added on the VPN server and the now we can route the packets from local tunnel to internal network.

Step 4: Set up routing on HOST V

Scrennshot of Host_V:

The image shows two terminal windows side-by-side. Both windows have a dark purple header bar with icons for battery, signal, and time (11:21 PM). The first window's title is 'Terminal' and it shows the command 'sudo route add -net 10.0.2.0/24 enp0s3' being run, followed by the output of the 'route -n' command which lists three routes to 10.0.2.0 via enp0s3. The second window has a similar title and shows the command 'sudo route add -net 192.168.53.0/24 gw 192.168.60.1 enp0s3' being run, followed by the output of 'route -n' which lists four routes to 192.168.53.0 via enp0s3.

The routes have been successfully added to the routing tables of Host V.

Step 5: Test the VPN tunnel (ping and telnet)

Screenshot of pinging 192.168.60.101 from VPN client:

This terminal window shows a ping session from a VPN client to the IP address 192.168.60.101. The output includes 10 successful packets transmitted, 10 received, and no packet loss. The round-trip time (rtt) statistics show a minimum of 1.233 ms, an average of 2.372 ms, a maximum of 2.872 ms, and a median of 0.494 ms.

Screenshot of terminal of VPN Server:

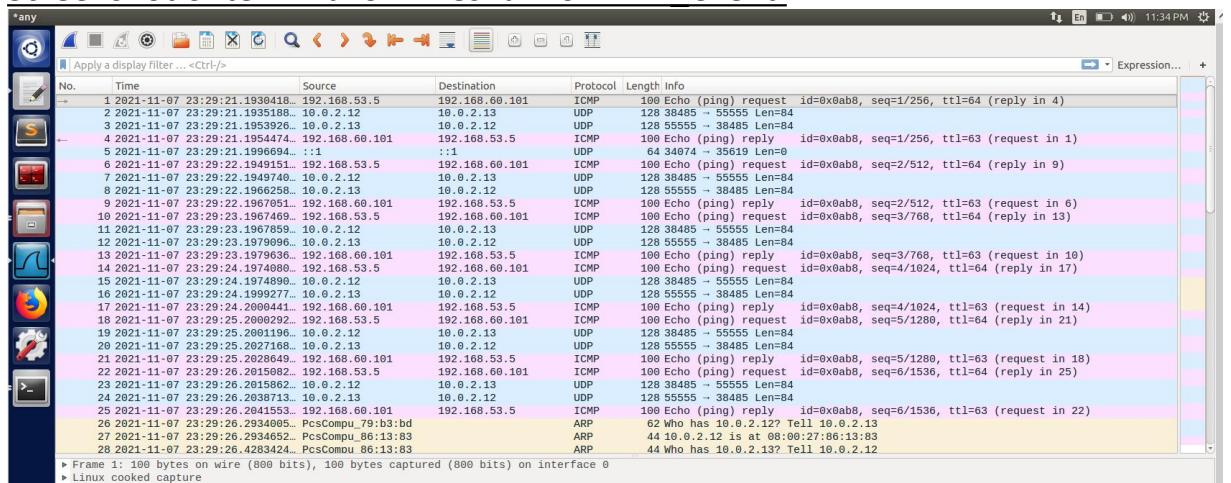
This terminal window displays a log of packet receptions from a VPN server using a TUN interface. The log shows numerous entries where the server is receiving packets from the TUN interface, indicating an active VPN connection.

Screenshot of terminal of VPN Client:

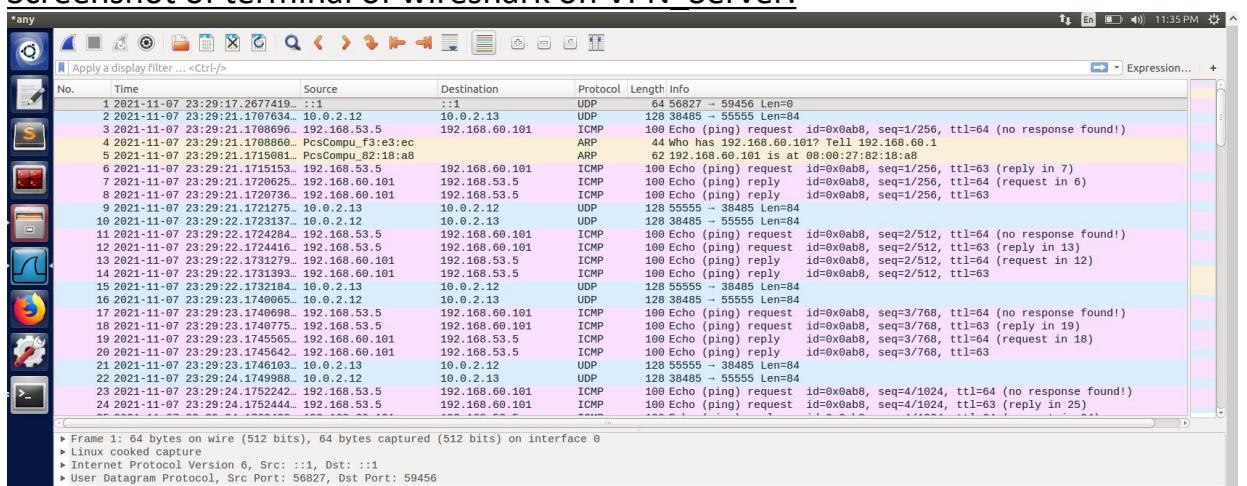
```
[11/07/21]seed@ankith_j_rai_PESIUG19CS069:~/.VPN_client$ sudo gcc vpnclient.c -o vpnclient
[11/07/21]seed@ankith_j_rai_PESIUG19CS069:~/.VPN_client$ sudo ./vpnclient 10.0.2.1
Got a packet from the tunnel
Got a packet from the tunnel
Got a packet from TUN
```

From the above screenshot's we can see that the tunnel has been established successfully and the packets are sent through the tunnel.

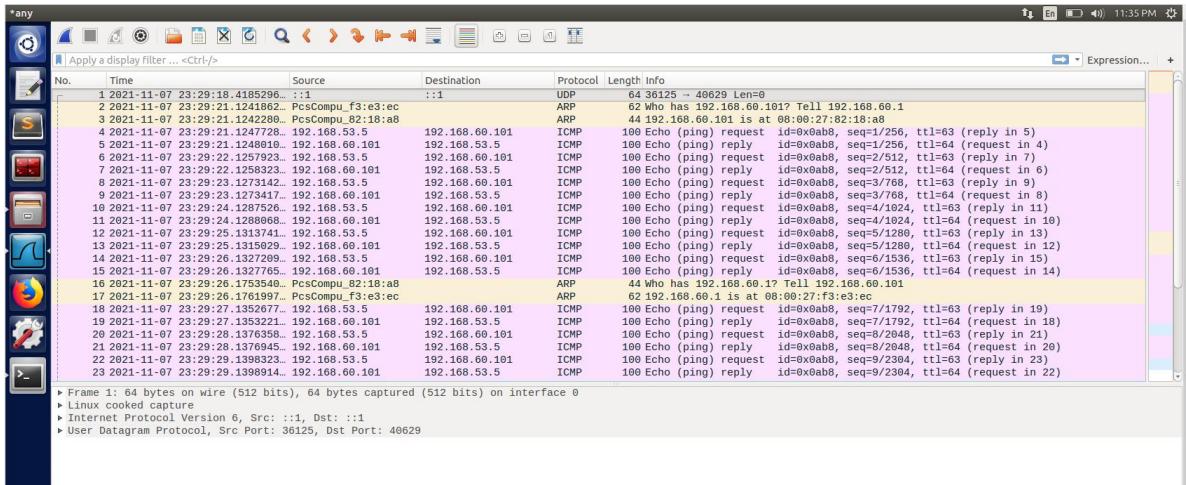
Screenshot of terminal of wireshark on VPN Client:



Screenshot of terminal of wireshark on VPN Server:



Screenshot of terminal of wireshark on Host V:



From the above screenshots we can tell that VPN client's ping request goes to VPN server and VPN server it is redirected to internal network and from there it is sent to Host V. Host V receives the packet and send back the reply to VPN server and the VPN server machine sends back the packet to VPN Client through the tunnel.

Telnet connection:

Screenshots of terminals of VPN Client:

```
[11/07/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$ telnet 192.168.60.101
Trying 192.168.60.101...
Connected to 192.168.60.101.
Escape character is '^>'.
Ubuntu 16.04.2 LTS
ankith_j_rai PES1UG19CS069 login: seed
Password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

1 package can be updated.
0 updates are security updates.

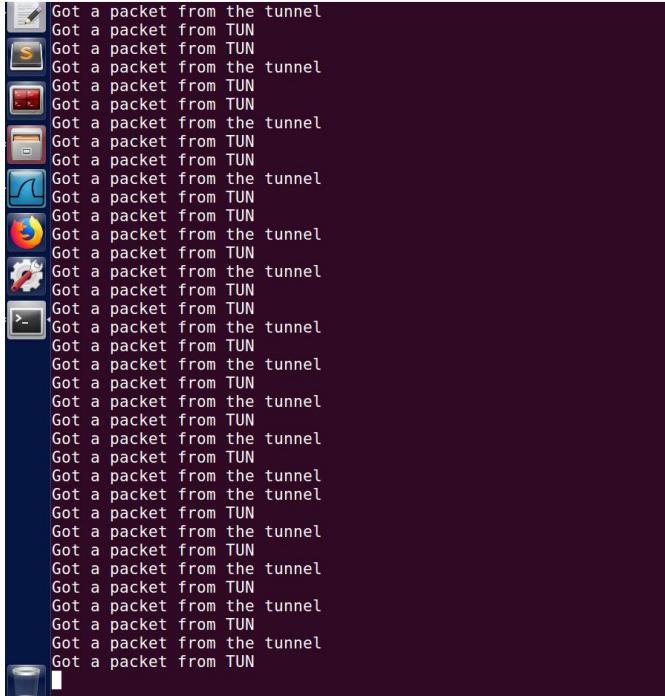
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

[11/07/21]seed@ankith_j_rai_PES1UG19CS069:~$ ]
```

The telnet connection has been successfully established.

Screenshot of VPN client:



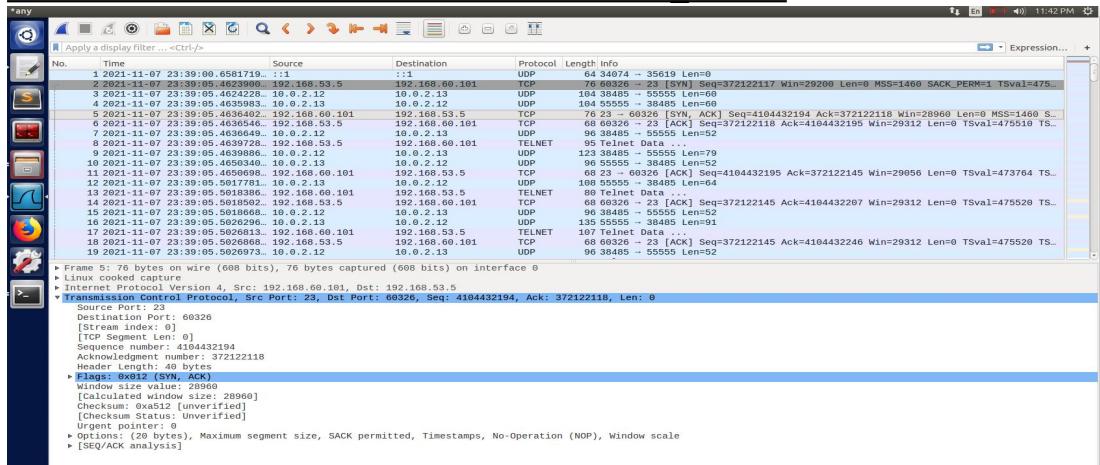
```

Got a packet from the tunnel
Got a packet from TUN
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from TUN

```

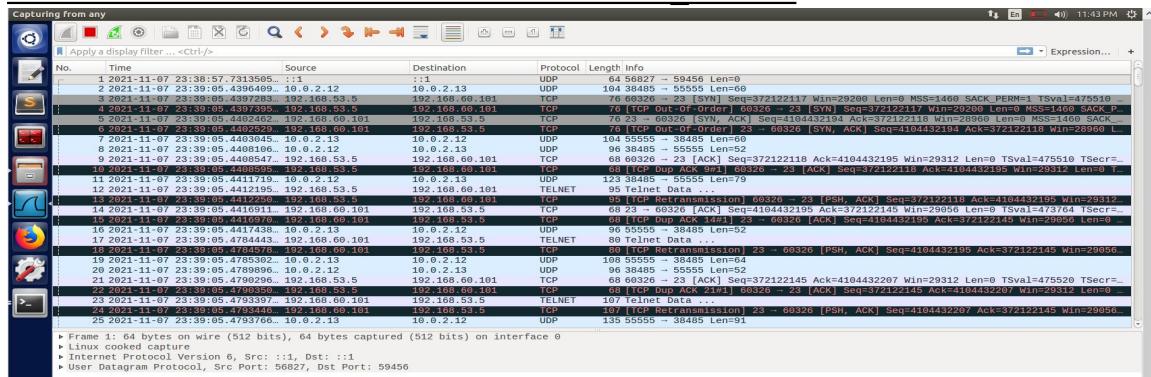
We can see that the packets have been successfully sent through the VPN tunnel.

Screenshot of terminal of wireshark on VPN Client:

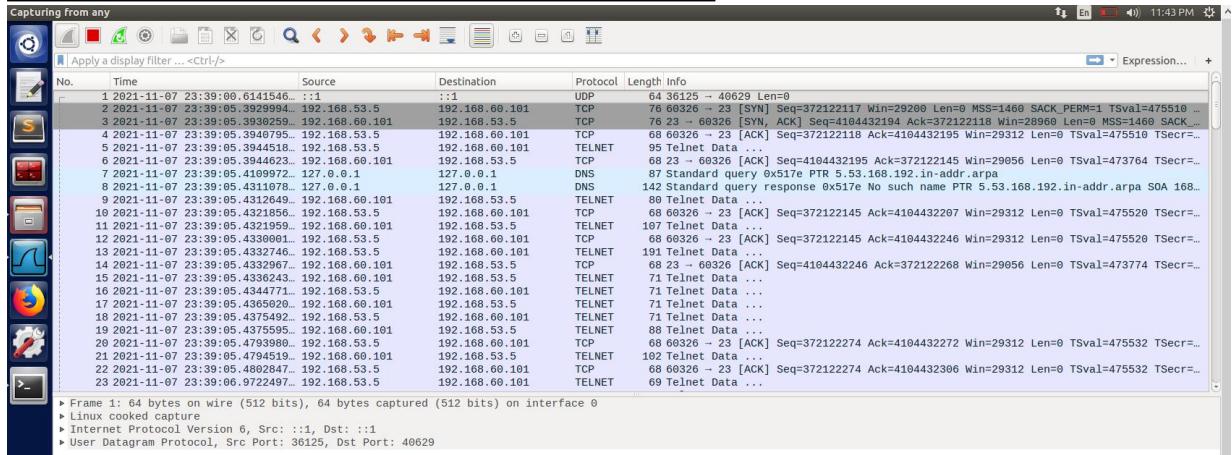


Here we observe that it is TCP instead of ICMP this is because telnet uses TCP.

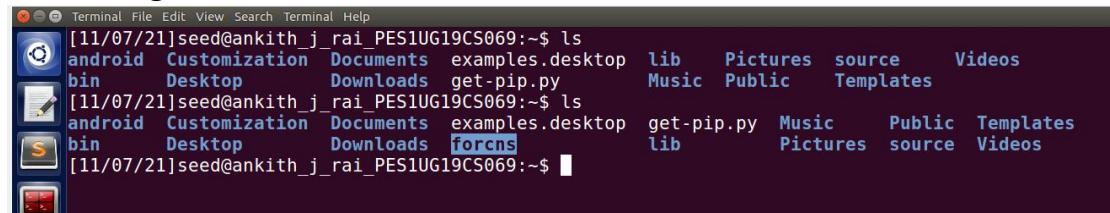
Screenshot of terminal of wireshark on VPN Server:



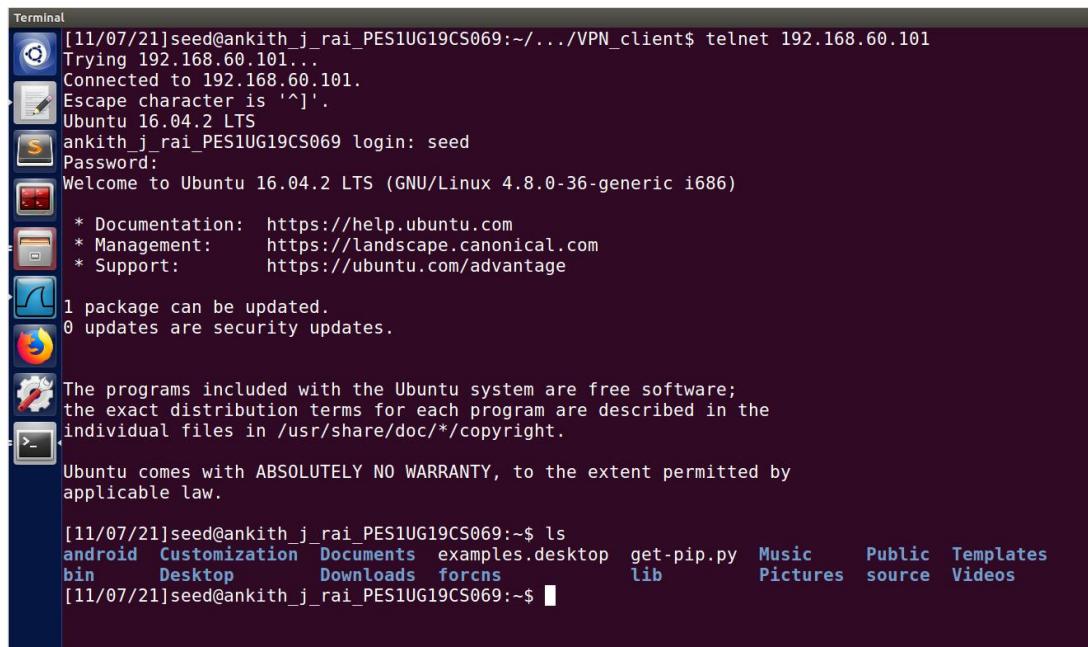
Screenshot of terminal of wireshark on Host V:



Now using ls command



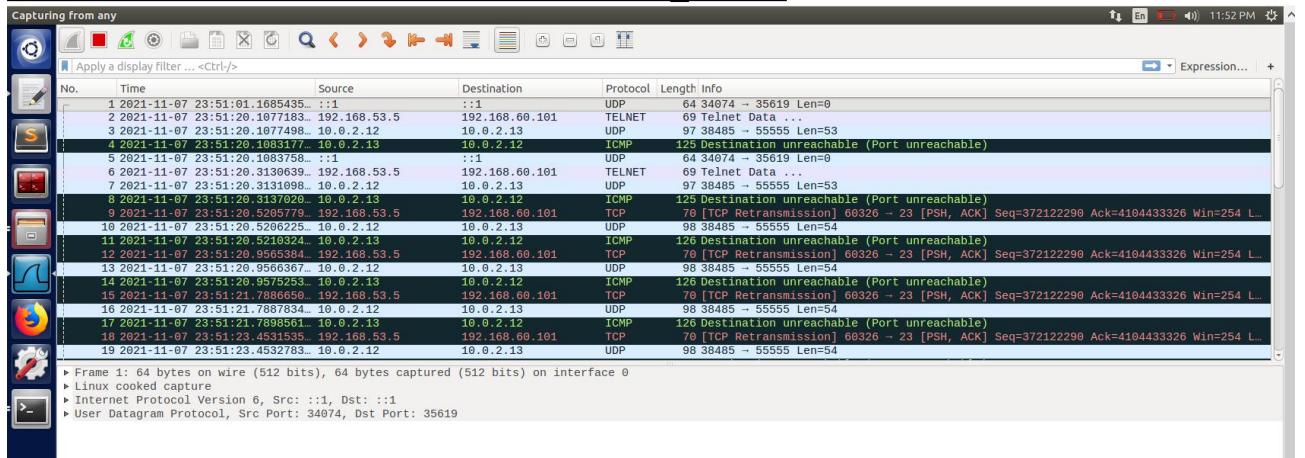
We can see that **forcns** has been created on Host V.



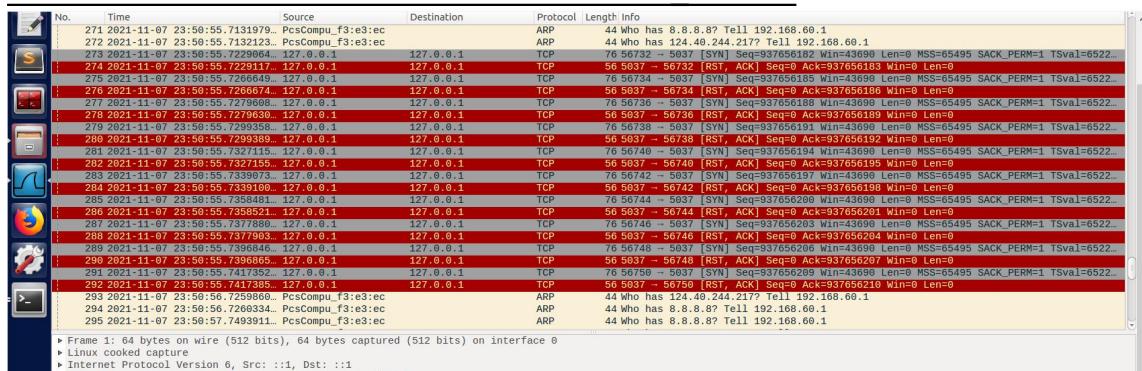
From above screenshot we can see that **forcns** is also visible on the telnet connection.

Step 6: Tunnel-Breaking Test:

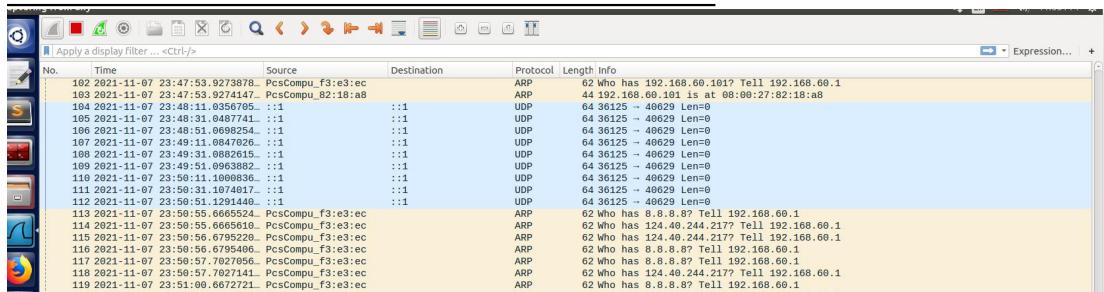
Screenshot of terminal of wireshark on VPN Client:



Screenshot of terminal of wireshark on VPN Server:



Screenshot of terminal of wireshark on Host V:



Screenshot of terminal of VPN client

```
[11/07/21]seed@ankith_j_rai_PES1UG19CS069:~$
```

We can see that we are not able to type anything on vpn client machine after breaking the tunnel.But from wireshark screenshot's we can see that the tcp connection's are still there, hence everything we type are stored in the buffer.

On restarting the vpnserver.c program we can see that the connection has been already lost.

Screenshot of terminal of wireshark on VPN Server:

Time	Source	Destination	Protocol	Details
440 2021-11-07 23:56:11.326242424	192.168.60.1	192.168.60.1	ICMP	93 Destination unreachable (Host unreachable)
441 2021-11-07 23:56:14.3263443	::1	::1	UDP	64 56827 ~ 59456 Len=0
442 2021-11-07 23:56:16.2783496	127.0.0.1	127.0.0.1	TCP	76 33321 ~ 953 [SYN] Seq=4292862132 Win=43698 Len=0 MSS=65495 SACK_PERM=1 TStamp=732424 TSval=732424 TSec=0
443 2021-11-07 23:56:16.2783562	127.0.0.1	127.0.0.1	TCP	76 953 ~ 33321 [SYN, ACK] Seq=2465138669 Ack=4202862133 Win=43698 Len=0 MSS=65495 SA_Offset=130667
444 2021-11-07 23:56:16.2783617	127.0.0.1	127.0.0.1	TCP	68 33321 ~ 953 [ACK] Seq=4292862133 Ack=2465138667 Win=43776 Len=0 TStamp=732424 TSval=732424 TSec=0
445 2021-11-07 23:56:16.2783651	127.0.0.1	127.0.0.1	SMP	218 SMP Bind_receiver
446 2021-11-07 23:56:16.2783660	127.0.0.1	127.0.0.1	TCP	68 953 ~ 33321 [ACK] Seq=2465138667 Ack=4202862288 Win=44800 Len=0 TStamp=732424 TSval=732424 TSec=0
447 2021-11-07 23:56:16.2788838	127.0.0.1	127.0.0.1	SMP	248 SMP Bind_receiver
448 2021-11-07 23:56:16.2788987	127.0.0.1	127.0.0.1	TCP	68 33321 ~ 953 [ACK] Seq=4292862280 Ack=2465138787 Win=44800 Len=0 TStamp=732424 TSval=732424 TSec=0
449 2021-11-07 23:56:16.2789276	127.0.0.1	127.0.0.1	TCP	241 33321 ~ 953 [PSH, ACK] Seq=4202862280 Ack=2465138787 Win=44800 Len=173 TStamp=732424 TSval=732424 TSec=0
450 2021-11-07 23:56:16.3041354	127.0.0.1	127.0.0.1	TCP	252 953 ~ 33321 [PSH, ACK] Seq=2465138787 Ack=4202862453 Win=45952 Len=184 TStamp=732431 TSval=732431 TSec=0
451 2021-11-07 23:56:16.3058350	127.0.0.1	127.0.0.1	TCP	68 33321 ~ 953 [FIN, ACK] Seq=4202862453 Ack=2465138971 Win=45952 Len=0 TStamp=732431 TSval=732431 TSec=0
452 2021-11-07 23:56:16.3108551	127.0.0.1	127.0.0.1	TCP	68 33321 ~ 953 [FIN, ACK] Seq=2465138971 Ack=4202862454 Win=45952 Len=0 TStamp=732432 TSval=732432 TSec=0
453 2021-11-07 23:56:16.3089797	127.0.0.1	127.0.0.1	TCP	68 33321 ~ 953 [ACK] Seq=4292862454 Ack=2465138972 Win=45952 Len=0 TStamp=732432 TSval=732432 TSec=0
454 2021-11-07 23:56:34.3377786	::1	::1	UDP	64 56827 ~ 59456 Len=0