VPN Task 1 and Task 2

10.0.2.22: VPN Server

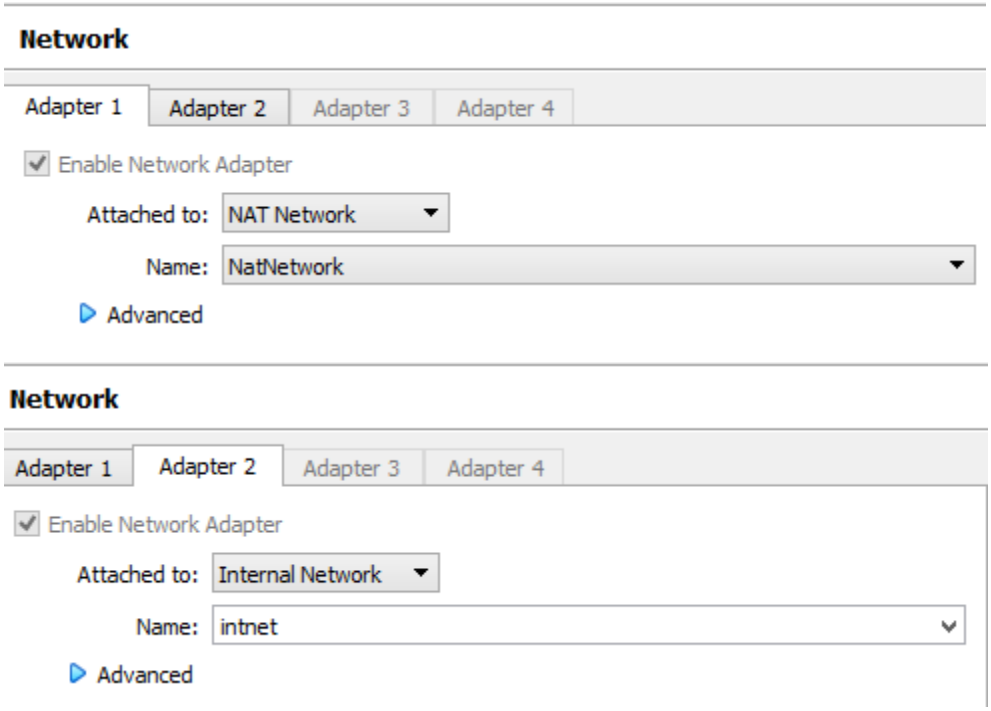
10.0.2.15: VPN Client (Host U)

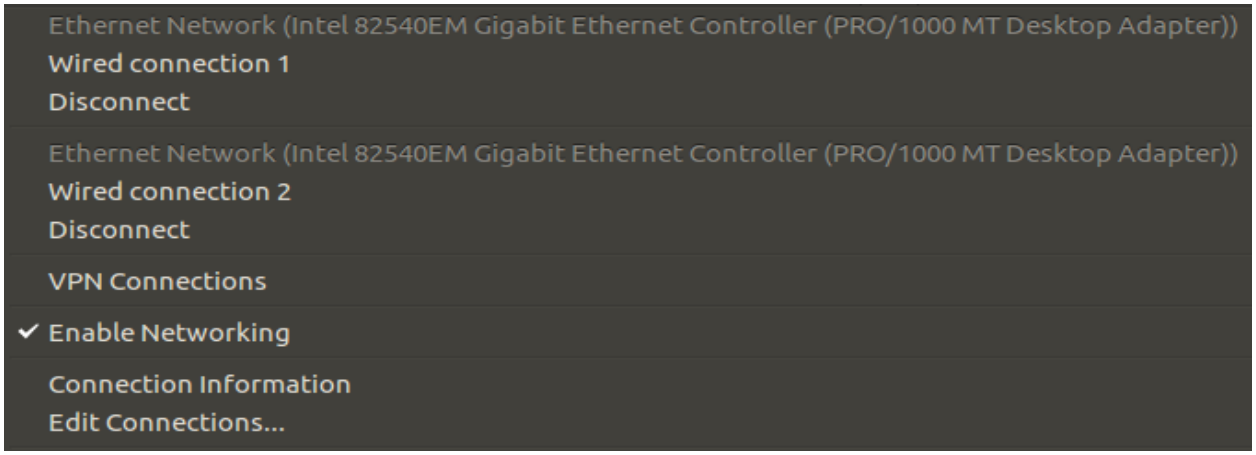
10.0.2.10: Host V

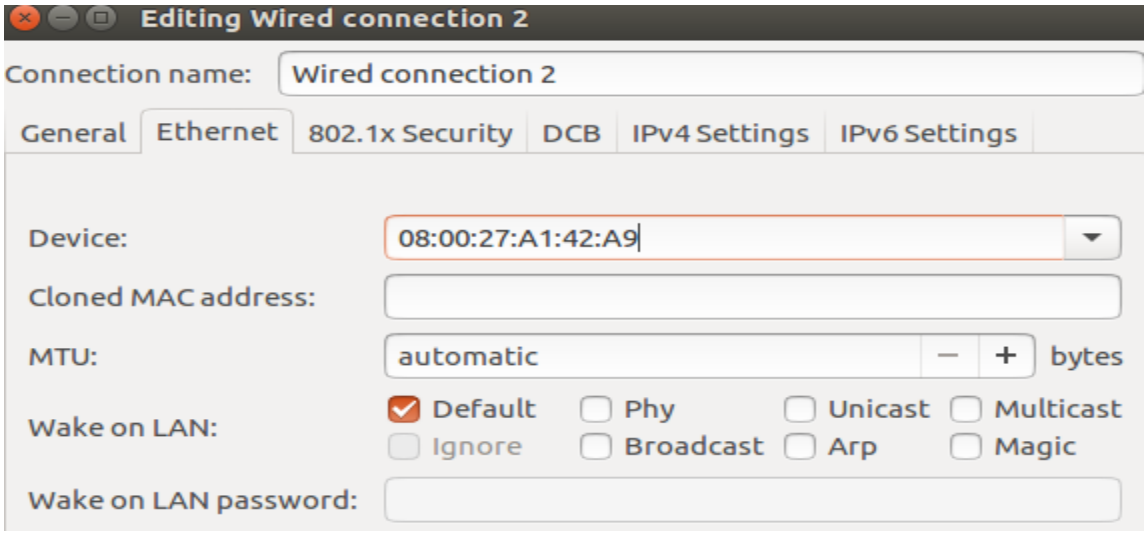
Task 1: VM Setup:

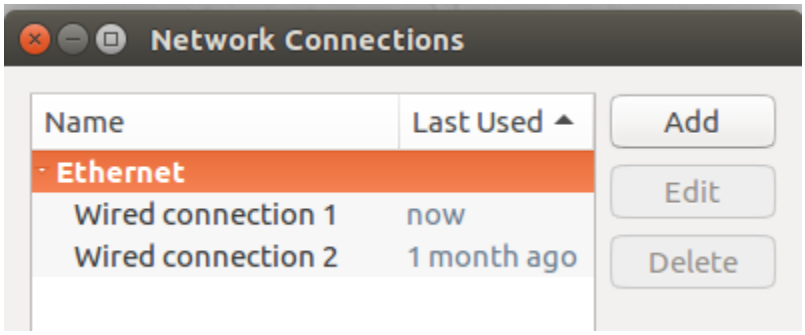
VPN Server:

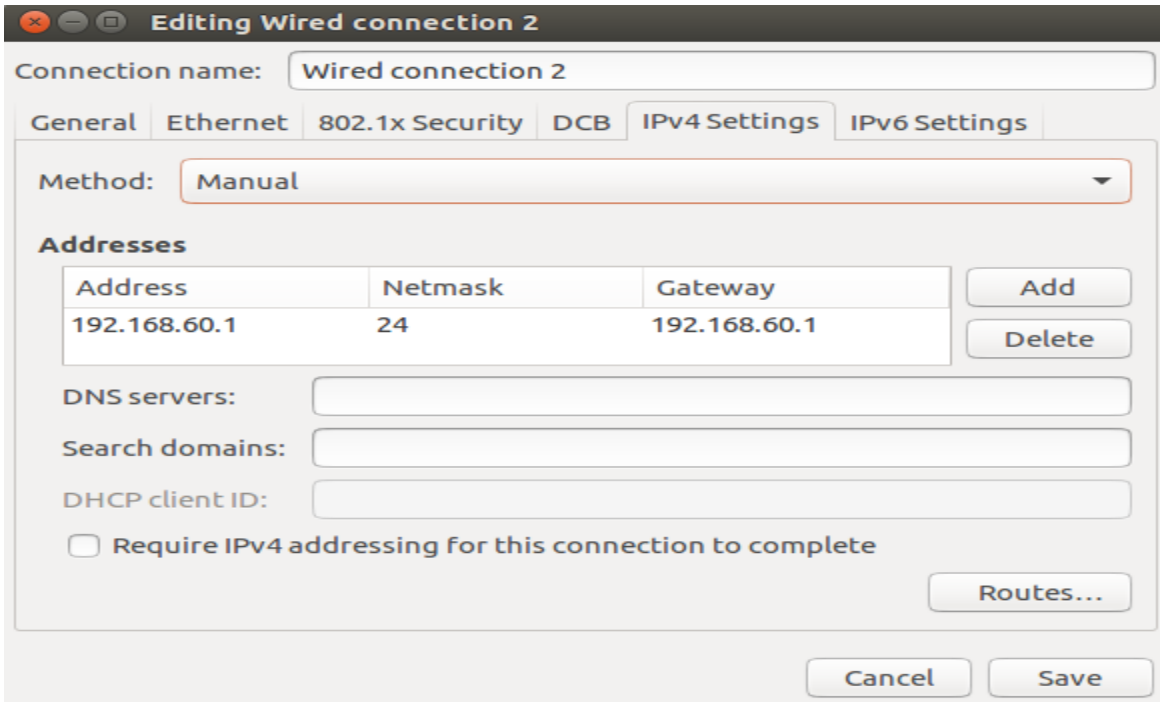
In the VPN server we enable two Network adapters (interfaces), one adapter contains the original mac address of the server. We manually configure the other network adapter to be the gateway to the internal network.





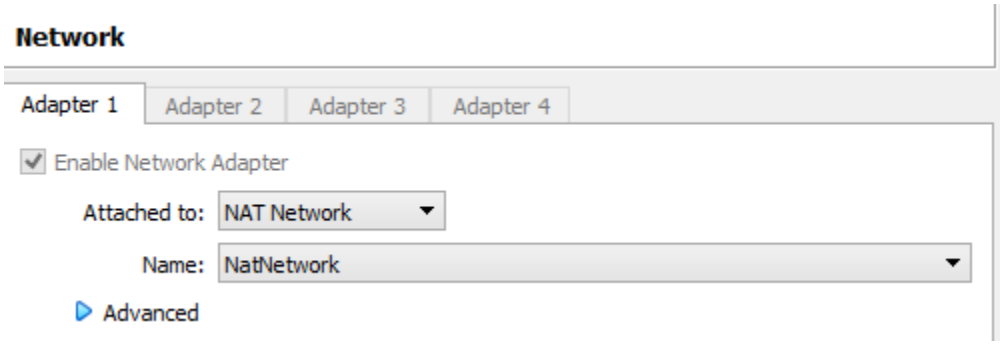

Editing Wired connection 2
Connection name:
Wired connection 2
General
Ethernet
802.1x Security
DCB
IPv4 Settings
IPv6 Settings
Device:
08:00:27:A1:42:A9
Cloned MAC address:
MTU:
automatic
bytes
Wake on LAN:
Default
Phy
Unicast
Multicast
Ignore
Broadcast
Arp
Magic
Wake on LAN password:


Network Connections
Name
Last Used
Add
Ethernet
Edit
Wired connection 1
now
Wired connection 2
1 month ago
Delete


Editing Wired connection 2
Connection name:
Wired connection 2
General
Ethernet
802.1x Security
DCB
IPv4 Settings
IPv6 Settings
Method:
Manual
Addresses
Address
Netmask
Gateway
Add
192.168.60.1
24
192.168.60.1
Delete
DNS servers:
Search domains:
DHCP client ID:
Require IPv4 addressing for this connection to complete
Routes...
Cancel
Save

```
[03/26/2020 19:51] Rakshith-10.0.2.22@VM:~/.../vpn$ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:fa:24:f5 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.22/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 1124sec preferred_lft 1124sec
    inet6 fe80::e146:4544:9715:1084/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:a1:42:a9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.60.1/24 brd 192.168.60.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::215f:64c8:419f:5aa6/64 scope link
       valid_lft forever preferred_lft forever
```

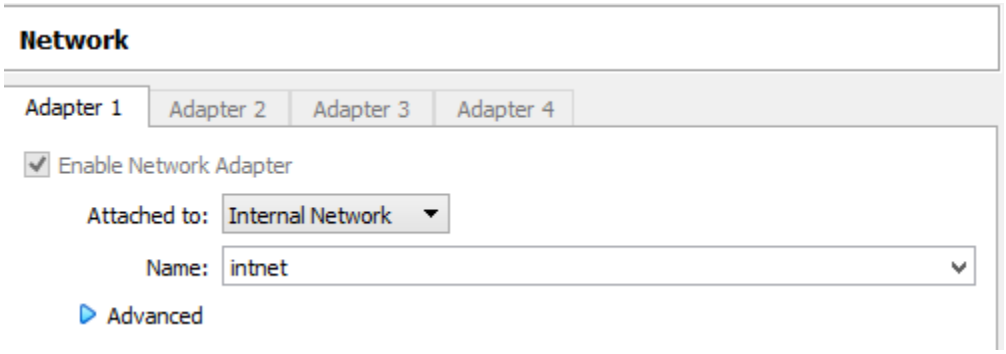
Host U or Client:



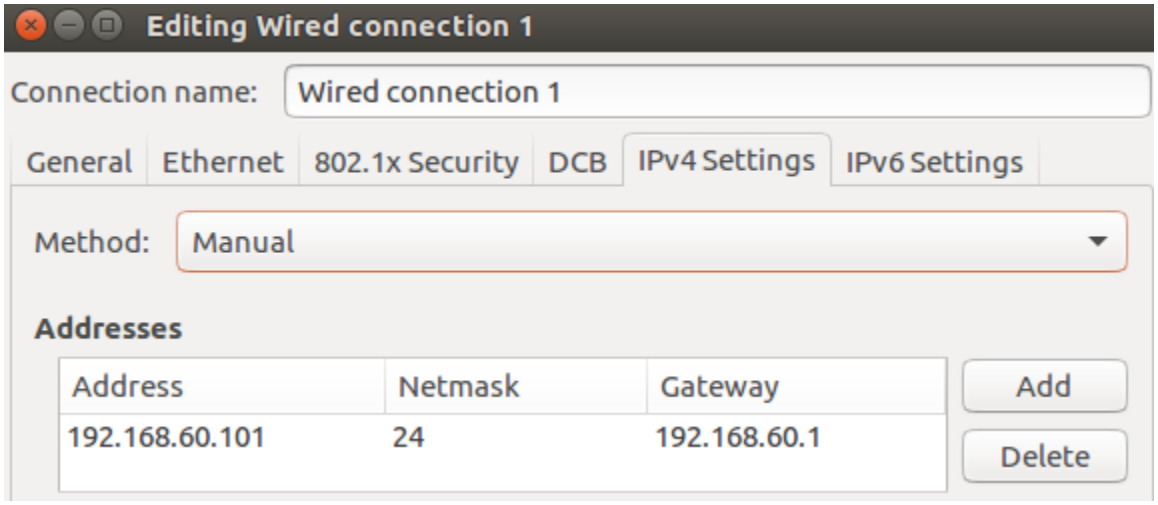
There are no additional configurations required for the client network / host U yet.

```
[03/25/2020 23:05] Rakshith-10.0.2.15@VM:~/vpn$ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:cb:0d:d0 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 1111sec preferred_lft 1111sec
    inet6 fe80::df3f:2f1a:dc4a:2401/64 scope link
       valid_lft forever preferred_lft forever
```

Host V or Internal Network:



Host V or Internal Network is part of VPN server's network where clients would like to connect. To simulate this we disconnect a VM from the original NAT network, we manually configure an IP address to this host and configure the gateway which matches the VPN Server's gateway that we configured.




```
[03/26/2020 20:00] Rakshith-10.0.2.10@VM:~$ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:3b:2b:b3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.60.101/24 brd 192.168.60.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::f90c:59a8:65c4:6084/64 scope link
       valid_lft forever preferred_lft forever
[03/26/2020 20:00] Rakshith-10.0.2.10@VM:~$
```

Step 1: Run VPN Server:

In this step we are creating a tunnel interface, and we are enabling the routing capabilities to our server.

```
[03/25/2020 17:21] Rakshith-10.0.2.22@VM:~/VPN-lab$unzip vpn.zip
Archive:  vpn.zip
   creating: vpn/
  inflating: vpn/README
  inflating: vpn/vpnclient.c
  inflating: vpn/Makefile
  inflating: vpn/vpnserver.c
[03/25/2020 17:21] Rakshith-10.0.2.22@VM:~/VPN-lab$ls
vpn  vpn.zip
[03/25/2020 17:21] Rakshith-10.0.2.22@VM:~/VPN-lab$cd vpn/
[03/25/2020 17:21] Rakshith-10.0.2.22@VM:~/.../vpn$ls
Makefile  README  vpnclient.c  vpnserver.c
[03/25/2020 17:21] Rakshith-10.0.2.22@VM:~/.../vpn$vi vpnserver.c
[03/25/2020 17:27] Rakshith-10.0.2.22@VM:~/.../vpn$gcc -o vpnserver vpnserver.c
[03/25/2020 17:27] Rakshith-10.0.2.22@VM:~/.../vpn$ls
Makefile  README  vpnclient.c  vpnserver  vpnserver.c
[03/25/2020 17:27] Rakshith-10.0.2.22@VM:~/.../vpn$sudo ./vpnserver
[sudo] password for seed:
```

```
/bin/bash 161x3
[03/25/2020 17:28] Rakshith-10.0.2.22@VM:~/.../vpn$sudo ifconfig tun0 192.168.53.1/24 up
[sudo] password for seed:
[03/25/2020 17:28] Rakshith-10.0.2.22@VM:~/.../vpn$sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
[03/25/2020 17:29] Rakshith-10.0.2.22@VM:~/.../vpn$
```

```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:192.168.53.1  P-t-P:192.168.53.1  Mask:255.255.255.0
          inet6 addr: fe80::2590:5c86:65c3:f12b/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:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

[03/25/2020 17:30] Rakshith-10.0.2.22@VM:~/.../vpn$
```

Step 2: Run VPN Client

In this step we are creating a tunnel interface in the client and enabling it.

```
[03/25/2020 17:36] Rakshith-10.0.2.15@VM:~$scp 10.0.2.22:/home/seed/Downloads/vpn.zip .
The authenticity of host '10.0.2.22 (10.0.2.22)' can't be established.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp5xa+eKRi561aFDaPE1/xq1eYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.22' (ECDSA) to the list of known hosts.
seed@10.0.2.22's password:
vpn.zip                                       100% 2728     2.7KB/s   00:00
```

```
[03/25/2020 17:37] Rakshith-10.0.2.15@VM:~$unzip vpn.zip
Archive:  vpn.zip
   creating: vpn/
  inflating: vpn/README
  inflating: vpn/vpnclient.c
  inflating: vpn/Makefile
  inflating: vpn/vpnserver.c
[03/25/2020 17:37] Rakshith-10.0.2.15@VM:~$cd vpn
[03/25/2020 17:37] Rakshith-10.0.2.15@VM:~/vpn$ls
Makefile  README  vpnclient.c  vpnserver.c
[03/25/2020 17:37] Rakshith-10.0.2.15@VM:~/vpn$
```

```
[03/25/2020 17:58] Rakshith-10.0.2.15@VM:~/vpn$gcc -o vpnclient vpnclient.c
[03/25/2020 17:59] Rakshith-10.0.2.15@VM:~/vpn$sudo ./vpnclient
[sudo] password for seed:
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
```

```
[03/25/2020 17:42] Rakshith-10.0.2.15@VM:~/vpn$sudo ifconfig tun0 192.168.53.5/24 up
[sudo] password for seed:
```

```
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::53b2:d69d:d1bf:9860/64 Scope:Link
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:48 (48.0 B)

[03/25/2020 17:59] Rakshith-10.0.2.15@VM:~/vpn$
```

Step 3: Set Up Routing on Client and Server VMs:

On Client VM:

We manually add two routes to our client VM one if the prefix of our tunnel interface and other is the prefix of internal network of VPN server and we route them via our tunnel interface.

```
[03/25/2020 17:59] Rakshith-10.0.2.15@VM:~/vpn$sudo route add -net 192.168.60.0/24 tun0
[03/25/2020 18:08] Rakshith-10.0.2.15@VM:~/vpn$sudo route add -net 192.168.53.0/24 tun0
[03/25/2020 18:11] Rakshith-10.0.2.15@VM:~/vpn$
```

On Server VM:

We manually add routes of our tunnel interface and route it via tun0.

```
[03/25/2020 17:31] Rakshith-10.0.2.22@VM:~/.../vpn$sudo route add -net 192.168.53.0/24 tun0
[sudo] password for seed:
[03/25/2020 18:11] Rakshith-10.0.2.22@VM:~/.../vpn$
```

Step 4: Set Up Routing on Host V:

All traffic in Host V must pass through VPN server, so we add the VPN server's route to it and route it via the sole interface.

```
[03/26/2020 20:00] Rakshith-10.0.2.10@VM:~$sudo route add -net 10.0.2.0/24 enp0s3
[sudo] password for seed:
[03/26/2020 20:14] Rakshith-10.0.2.10@VM:~$
```

Step 5: Test the VPN Tunnel:

Ping Host V from Host U

We are trying to ping Host V by Host U (client network), and we are successfully able to connect to it, as we can see in the wireshark we get the desired results our packets are encapsulated inside original client's software, then reach VPN server and then get routed to the host V.

```
[03/26/2020 22:46] Rakshith-10.0.2.15@VM:~/vpn$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
```

```
[03/26/2020 22:21] Rakshith-10.0.2.22@VM:~/.../vpn$route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.2.1        0.0.0.0         UG    100    0        0 enp0s3
0.0.0.0         192.168.60.1    0.0.0.0         UG    101    0        0 enp0s8
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
192.168.53.0    0.0.0.0         255.255.255.0   U     0      0        0 tun0
192.168.53.0    0.0.0.0         255.255.255.0   U     0      0        0 tun0
192.168.60.0    0.0.0.0         255.255.255.0   U     100    0        0 enp0s8
[03/26/2020 22:37] Rakshith-10.0.2.22@VM:~/.../vpn$
```

```
[03/26/2020 22:21] Rakshith-10.0.2.22@VM:~/.../vpn$sudo ./vpnserver
[sudo] password for seed:
Connected with the client: `
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
Got a packet from TUN
```

```
[03/26/2020 21:14] Rakshith-10.0.2.15@VM:~/vpn$ping 192.168.60.101
PING 192.168.60.101 (192.168.60.101) 56(84) bytes of data.
64 bytes from 192.168.60.101: icmp_seq=1 ttl=63 time=2.76 ms
64 bytes from 192.168.60.101: icmp_seq=2 ttl=63 time=4.23 ms
64 bytes from 192.168.60.101: icmp_seq=3 ttl=63 time=2.23 ms
64 bytes from 192.168.60.101: icmp_seq=4 ttl=63 time=2.43 ms
64 bytes from 192.168.60.101: icmp_seq=5 ttl=63 time=2.71 ms
^C
--- 192.168.60.101 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 2.232/2.875/4.230/0.707 ms
[03/26/2020 21:14] Rakshith-10.0.2.15@VM:~/vpn$
```

2	2020-03-26 21…	192.168.53.5	192.168.60.101	ICMP	100	Echo (ping) request id=0x1d9f, seq=1/256, ttl=64 (reply i…
3	2020-03-26 21…	10.0.2.15	10.0.2.22	UDP	128	53113 → 55555 Len=84
4	2020-03-26 21…	10.0.2.22	10.0.2.15	UDP	128	55555 → 53113 Len=84
5	2020-03-26 21…	192.168.60.101	192.168.53.5	ICMP	100	Echo (ping) reply id=0x1d9f, seq=1/256, ttl=63 (request…
6	2020-03-26 21…	192.168.53.5	192.168.60.101	ICMP	100	Echo (ping) request id=0x1d9f, seq=2/512, ttl=64 (reply i…
7	2020-03-26 21…	10.0.2.15	10.0.2.22	UDP	128	53113 → 55555 Len=84
8	2020-03-26 21…	10.0.2.22	10.0.2.15	UDP	128	55555 → 53113 Len=84
9	2020-03-26 21…	192.168.60.101	192.168.53.5	ICMP	100	Echo (ping) reply id=0x1d9f, seq=2/512, ttl=63 (request…
10	2020-03-26 21…	192.168.53.5	192.168.60.101	ICMP	100	Echo (ping) request id=0x1d9f, seq=3/768, ttl=64 (reply i…
11	2020-03-26 21…	10.0.2.15	10.0.2.22	UDP	128	53113 → 55555 Len=84
12	2020-03-26 21…	10.0.2.22	10.0.2.15	UDP	128	55555 → 53113 Len=84
13	2020-03-26 21…	192.168.60.101	192.168.53.5	ICMP	100	Echo (ping) reply id=0x1d9f, seq=3/768, ttl=63 (request…
14	2020-03-26 21…	192.168.53.5	192.168.60.101	ICMP	100	Echo (ping) request id=0x1d9f, seq=4/1024, ttl=64 (reply …
15	2020-03-26 21…	10.0.2.15	10.0.2.22	UDP	128	53113 → 55555 Len=84
16	2020-03-26 21…	10.0.2.22	10.0.2.15	UDP	128	55555 → 53113 Len=84
17	2020-03-26 21…	192.168.60.101	192.168.53.5	ICMP	100	Echo (ping) reply id=0x1d9f, seq=4/1024, ttl=63 (reques…
18	2020-03-26 21…	192.168.53.5	192.168.60.101	ICMP	100	Echo (ping) request id=0x1d9f, seq=5/1280, ttl=64 (reply …
19	2020-03-26 21…	10.0.2.15	10.0.2.22	UDP	128	53113 → 55555 Len=84
20	2020-03-26 21…	10.0.2.22	10.0.2.15	UDP	128	55555 → 53113 Len=84

Telnet Host V from Host U

```
[03/26/2020 21:17] Rakshith-10.0.2.15@VM:~/vpn$telnet 192.168.60.101
Trying 192.168.60.101...
Connected to 192.168.60.101.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Thu Mar 26 20:58:01 EDT 2020 from 192.168.53.5 on pts/18
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.

[03/26/2020 21:17] Rakshith-10.0.2.10@VM:~$
```

2	2020-03-26 21…	192.168.53.5	192.168.60.101	TCP	76	38096 → 23 [SYN] Seq=1083998816 Win=29200 Len=0 MSS=1460 S…
3	2020-03-26 21…	10.0.2.15	10.0.2.22	UDP	104	53113 → 55555 Len=60
4	2020-03-26 21…	10.0.2.22	10.0.2.15	UDP	104	55555 → 53113 Len=60
5	2020-03-26 21…	192.168.60.101	192.168.53.5	TCP	76	23 → 38096 [SYN, ACK] Seq=537445016 Ack=1083998817 Win=289…
6	2020-03-26 21…	192.168.53.5	192.168.60.101	TCP	68	38096 → 23 [ACK] Seq=1083998817 Ack=537445017 Win=29312 Le…
7	2020-03-26 21…	10.0.2.15	10.0.2.22	UDP	96	53113 → 55555 Len=52
8	2020-03-26 21…	192.168.53.5	192.168.60.101	TELNET	95	Telnet Data ...
9	2020-03-26 21…	10.0.2.15	10.0.2.22	UDP	123	53113 → 55555 Len=79
10	2020-03-26 21…	10.0.2.22	10.0.2.15	UDP	96	55555 → 53113 Len=52
11	2020-03-26 21…	192.168.60.101	192.168.53.5	TCP	68	23 → 38096 [ACK] Seq=537445017 Ack=1083998844 Win=29056 Le…
12	2020-03-26 21…	10.0.2.22	10.0.2.15	UDP	108	55555 → 53113 Len=64
13	2020-03-26 21…	192.168.60.101	192.168.53.5	TELNET	80	Telnet Data ...
14	2020-03-26 21…	192.168.53.5	192.168.60.101	TCP	68	38096 → 23 [ACK] Seq=1083998844 Ack=537445029 Win=29312 Le…
15	2020-03-26 21…	10.0.2.15	10.0.2.22	UDP	96	53113 → 55555 Len=52
16	2020-03-26 21…	10.0.2.22	10.0.2.15	UDP	135	55555 → 53113 Len=91
17	2020-03-26 21…	192.168.60.101	192.168.53.5	TELNET	107	Telnet Data ...
18	2020-03-26 21…	192.168.53.5	192.168.60.101	TCP	68	38096 → 23 [ACK] Seq=1083998844 Ack=537445068 Win=29312 Le…
19	2020-03-26 21…	10.0.2.15	10.0.2.22	UDP	96	53113 → 55555 Len=52
20	2020-03-26 21…	192.168.53.5	192.168.60.101	TELNET	134	Telnet Data ...
21	2020-03-26 21…	10.0.2.15	10.0.2.22	UDP	162	53113 → 55555 Len=118

Decode as IPv4 in Wireshark to see packet encapsulation

```
▸ Frame 3: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.22
▸ User Datagram Protocol, Src Port: 53113, Dst Port: 55555
▸ Internet Protocol Version 4, Src: 192.168.53.5, Dst: 192.168.60.101
▸ Transmission Control Protocol, Src Port: 38096, Dst Port: 23, Seq: 1083998816, Len: 0
```

Step 6: Tunnel-Breaking Test:

We can break the tunnel by bringing down the tunnel interface or by setting the tunnel link down. Once we do this our telnet connection will freeze. Once we bring the tunnel interface back up, the telnet connection will resume.

Initial configuration:

```
[03/26/2020 23:06] Rakshith-10.0.2.15@VM:~/vpn$telnet 192.168.60.101
Trying 192.168.60.101...
Connected to 192.168.60.101.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Thu Mar 26 22:31:19 EDT 2020 from 192.168.53.5 on pts/20
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.

[03/26/2020 22:48] Rakshith-10.0.2.10@VM:~$
```

```
[03/26/2020 22:53] Rakshith-10.0.2.15@VM:~/vpn$sudo ip link set tun0 down
[sudo] password for seed:
[03/26/2020 23:08] Rakshith-10.0.2.15@VM:~/vpn$sudo ifconfig tun0 192.168.53.5/24 up
```

After session resumes

```
[03/26/2020 22:48] Rakshith-10.0.2.10@VM:~$asddfhjsadhsjgfjgfjg
asddfhjsadhsjgfjgfjg: command not found
[03/26/2020 22:51] Rakshith-10.0.2.10@VM:~$
[03/26/2020 22:51] Rakshith-10.0.2.10@VM:~$
[03/26/2020 22:51] Rakshith-10.0.2.10@VM:~$
[03/26/2020 22:51] Rakshith-10.0.2.10@VM:~$asdfjsdfh
asdfjsdfh: command not found
[03/26/2020 22:51] Rakshith-10.0.2.10@VM:~$
```

When the session froze:

32	2020-03-26 23…	127.0.0.1	127.0.0.1	TCP	76	52896 → 5037 [SYN] Seq=893043086 Win=43690 Len=0 MSS=65495…
33	2020-03-26 23…	127.0.0.1	127.0.0.1	TCP	56	5037 → 52896 [RST, ACK] Seq=0 Ack=893043087 Win=0 Len=0
34	2020-03-26 23…	127.0.0.1	127.0.0.1	TCP	76	52898 → 5037 [SYN] Seq=893043089 Win=43690 Len=0 MSS=65495…
35	2020-03-26 23…	127.0.0.1	127.0.0.1	TCP	56	5037 → 52898 [RST, ACK] Seq=0 Ack=893043090 Win=0 Len=0
36	2020-03-26 23…	127.0.0.1	127.0.0.1	TCP	76	52900 → 5037 [SYN] Seq=893043092 Win=43690 Len=0 MSS=65495…
37	2020-03-26 23…	127.0.0.1	127.0.0.1	TCP	56	5037 → 52900 [RST, ACK] Seq=0 Ack=893043093 Win=0 Len=0
38	2020-03-26 23…	127.0.0.1	127.0.0.1	TCP	76	52902 → 5037 [SYN] Seq=893043095 Win=43690 Len=0 MSS=65495…
39	2020-03-26 23…	127.0.0.1	127.0.0.1	TCP	56	5037 → 52902 [RST, ACK] Seq=0 Ack=893043096 Win=0 Len=0
40	2020-03-26 23…	127.0.0.1	127.0.0.1	TCP	76	52904 → 5037 [SYN] Seq=893043098 Win=43690 Len=0 MSS=65495…
41	2020-03-26 23…	127.0.0.1	127.0.0.1	TCP	56	5037 → 52904 [RST, ACK] Seq=0 Ack=893043099 Win=0 Len=0
42	2020-03-26 23…	127.0.0.1	127.0.0.1	TCP	76	52906 → 5037 [SYN] Seq=893043101 Win=43690 Len=0 MSS=65495…
43	2020-03-26 23…	127.0.0.1	127.0.0.1	TCP	56	5037 → 52906 [RST, ACK] Seq=0 Ack=893043102 Win=0 Len=0
44	2020-03-26 23…	127.0.0.1	127.0.0.1	TCP	76	52908 → 5037 [SYN] Seq=893043104 Win=43690 Len=0 MSS=65495…
45	2020-03-26 23…	127.0.0.1	127.0.0.1	TCP	56	5037 → 52908 [RST, ACK] Seq=0 Ack=893043105 Win=0 Len=0
46	2020-03-26 23…	127.0.0.1	127.0.0.1	TCP	76	52910 → 5037 [SYN] Seq=893043107 Win=43690 Len=0 MSS=65495…
47	2020-03-26 23…	127.0.0.1	127.0.0.1	TCP	56	5037 → 52910 [RST, ACK] Seq=0 Ack=893043108 Win=0 Len=0
48	2020-03-26 23…	127.0.0.1	127.0.0.1	TCP	76	52912 → 5037 [SYN] Seq=893043110 Win=43690 Len=0 MSS=65495…
49	2020-03-26 23…	127.0.0.1	127.0.0.1	TCP	56	5037 → 52912 [RST, ACK] Seq=0 Ack=893043111 Win=0 Len=0
50	2020-03-26 23…	127.0.0.1	127.0.0.1	TCP	76	52914 → 5037 [SYN] Seq=893043113 Win=43690 Len=0 MSS=65495…
51	2020-03-26 23…	127.0.0.1	127.0.0.1	TCP	56	5037 → 52914 [RST, ACK] Seq=0 Ack=893043114 Win=0 Len=0

When the session resumes:

179	2020-03-26 23…	192.168.60.101	192.168.53.5	TELNET	113	Telnet Data ...
180	2020-03-26 23…	192.168.53.5	192.168.60.101	TCP	68	45390 → 23 [ACK] Seq=3024523107 Ack=497385893 Win=237 Len=…
181	2020-03-26 23…	10.0.2.15	10.0.2.22	UDP	96	38545 → 55555 Len=52
182	2020-03-26 23…	10.0.2.22	10.0.2.15	UDP	139	55555 → 38545 Len=95
183	2020-03-26 23…	192.168.60.101	192.168.53.5	TELNET	111	Telnet Data ...
184	2020-03-26 23…	192.168.53.5	192.168.60.101	TCP	68	45390 → 23 [ACK] Seq=3024523107 Ack=497385936 Win=237 Len=…
185	2020-03-26 23…	10.0.2.15	10.0.2.22	UDP	96	38545 → 55555 Len=52
186	2020-03-26 23…	10.0.2.22	10.0.2.15	UDP	98	55555 → 38545 Len=54
187	2020-03-26 23…	192.168.60.101	192.168.53.5	TELNET	70	Telnet Data ...
188	2020-03-26 23…	192.168.53.5	192.168.60.101	TCP	68	45390 → 23 [ACK] Seq=3024523107 Ack=497385938 Win=237 Len=…
189	2020-03-26 23…	10.0.2.15	10.0.2.22	UDP	96	38545 → 55555 Len=52
190	2020-03-26 23…	10.0.2.22	10.0.2.15	UDP	139	55555 → 38545 Len=95
191	2020-03-26 23…	192.168.60.101	192.168.53.5	TELNET	111	Telnet Data ...
192	2020-03-26 23…	192.168.53.5	192.168.60.101	TCP	68	45390 → 23 [ACK] Seq=3024523107 Ack=497385981 Win=237 Len=…
193	2020-03-26 23…	10.0.2.15	10.0.2.22	UDP	96	38545 → 55555 Len=52
194	2020-03-26 23…	10.0.2.22	10.0.2.15	UDP	98	55555 → 38545 Len=54
195	2020-03-26 23…	192.168.60.101	192.168.53.5	TELNET	70	Telnet Data ...
196	2020-03-26 23…	192.168.53.5	192.168.60.101	TCP	68	45390 → 23 [ACK] Seq=3024523107 Ack=497385983 Win=237 Len=…
197	2020-03-26 23…	10.0.2.15	10.0.2.22	UDP	96	38545 → 55555 Len=52
198	2020-03-26 23…	10.0.2.22	10.0.2.15	UDP	139	55555 → 38545 Len=95
199	2020-03-26 23…	192.168.60.101	192.168.53.5	TELNET	111	Telnet Data ...
200	2020-03-26 23…	192.168.53.5	192.168.60.101	TCP	68	45390 → 23 [ACK] Seq=3024523107 Ack=497386026 Win=237 Len=…
201	2020-03-26 23…	10.0.2.15	10.0.2.22	UDP	96	38545 → 55555 Len=52
202	2020-03-26 23…	10.0.2.22	10.0.2.15	UDP	98	55555 → 38545 Len=54
203	2020-03-26 23…	192.168.60.101	192.168.53.5	TELNET	70	Telnet Data ...
204	2020-03-26 23…	192.168.53.5	192.168.60.101	TCP	68	45390 → 23 [ACK] Seq=3024523107 Ack=497386028 Win=237 Len=…
205	2020-03-26 23…	10.0.2.15	10.0.2.22	UDP	96	38545 → 55555 Len=52
206	2020-03-26 23…	10.0.2.22	10.0.2.15	UDP	186	55555 → 38545 Len=142