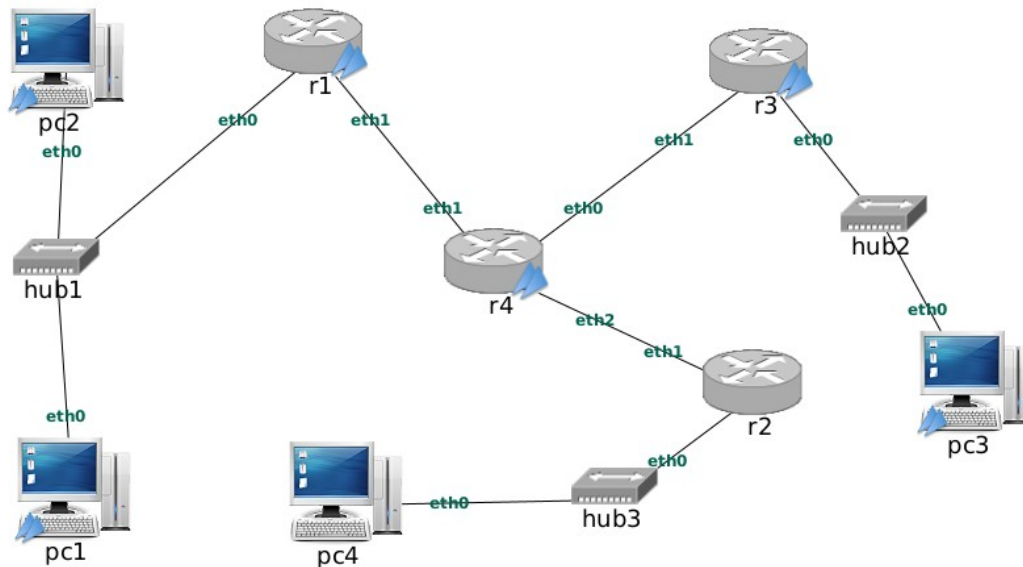




LABORATORIO VPN 1

Redes II, Tecnicatura en Administración de Sistemas y Software Libre

1.



2.

```
pc1:~# ping -c 3 pc2
PING pc2 (10.0.20.21) 56(84) bytes of data.
64 bytes from pc2 (10.0.20.21): icmp_seq=1 ttl=64 time=0.128 ms
64 bytes from pc2 (10.0.20.21): icmp_seq=2 ttl=64 time=0.445 ms
64 bytes from pc2 (10.0.20.21): icmp_seq=3 ttl=64 time=0.740 ms
```

```
--- pc2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2009ms
rtt min/avg/max/mdev = 0.128/0.437/0.740/0.251 ms
pc1:~#
```

```
pc1:~# ping -c 3 pc3
PING pc3 (10.0.30.20) 56(84) bytes of data.

--- pc3 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2010ms
```

```
pc1:~#
```

podemos hacer un tracepat

```
pc1:~# tracepath pc3
```



```
1: pc1 (10.0.20.20)          0.093ms pmtu 1500
1: 10.0.20.1 (10.0.20.1)     9.307ms
1: 10.0.20.1 (10.0.20.1)     0.099ms
2: no reply
3: no reply

pc1:~#
```

podemos ver que no está saliendo desde r4, por lo que es posible que a ese router le falte un gateway por defecto.

3.

Configuraciones de las pcs (.startup)

```
#pc1
ifconfig eth0 10.0.20.20/24 hw ether AA:BB:CC:00:01:01 up
route add default gw 10.0.20.1

#pc2
ifconfig eth0 10.0.20.21/24 hw ether AA:BB:CC:00:01:02 up
route add default gw 10.0.20.1

#pc3
ifconfig eth0 10.0.30.20/24 hw ether AA:BB:CC:00:01:03 up
route add default gw 10.0.30.1

#pc4
ifconfig eth0 10.0.40.21/24 hw ether AA:BB:CC:00:01:04 up
route add default gw 10.0.40.2
```

Podemos ver que es la configuracion habitual de host – router.

Configuraciones de los routers

```
#r1
ifconfig eth0 10.0.20.1/24 hw ether AA:BB:CC:00:01:05 up
ifconfig eth1 100.60.60.1/24 hw ether AA:BB:CC:00:01:06 up
route add default gw 100.60.60.2

#r2
ifconfig eth1 100.80.80.1/24 hw ether AA:BB:CC:00:01:10 up
ifconfig eth0 10.0.40.2/24 hw ether AA:BB:CC:00:01:09 up
route add default gw 100.80.80.2

#r3
ifconfig eth1 100.50.50.1/24 hw ether AA:BB:CC:00:01:11 up
ifconfig eth0 10.0.30.1/24 hw ether AA:BB:CC:00:01:12 up
route add default gw 100.50.50.2

#r4
ifconfig eth0 100.50.50.2/24 hw ether AA:BB:CC:00:01:08 up
ifconfig eth1 100.60.60.2/24 hw ether AA:BB:CC:00:01:07 up
ifconfig eth2 100.80.80.2/24 hw ether AA:BB:CC:00:01:07 up
```

En este caso el unico router que no tiene un gw por defecto es r4, lo que hace que un ping que trate de ir de pc1 a pc4 no llegaria, o a pc3.

4.



```
r1:~# ifconfig
eth0  Link encap:Ethernet HWaddr aa:bb:cc:00:01:05
      inet addr:10.0.20.1 Bcast:10.0.20.255 Mask:255.255.255.0
      inet6 addr: fe80::fc46:c8ff:fe27:2cd5/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:35 errors:0 dropped:0 overruns:0 frame:0
      TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:18012 (17.5 KiB) TX bytes:1774 (1.7 KiB)
      Interrupt:5

eth1  Link encap:Ethernet HWaddr aa:bb:cc:00:01:06
      inet addr:100.60.60.1 Bcast:100.60.60.255 Mask:255.255.255.0
      inet6 addr: fe80::6853:15ff:fe46:255/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:8 errors:0 dropped:0 overruns:0 frame:0
      TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:440 (440.0 B) TX bytes:14472 (14.1 KiB)
      Interrupt:5

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:2 errors:0 dropped:0 overruns:0 frame:0
      TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:100 (100.0 B) TX bytes:100 (100.0 B)

r1:~#
```

```
r3:~# ifconfig
eth0  Link encap:Ethernet HWaddr aa:bb:cc:00:01:12
      inet addr:10.0.30.1 Bcast:10.0.30.255 Mask:255.255.255.0
      inet6 addr: fe80::e4b1:84ff:fec3:6102/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:6 errors:0 dropped:0 overruns:0 frame:0
      TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:384 (384.0 B) TX bytes:468 (468.0 B)
      Interrupt:5

eth1  Link encap:Ethernet HWaddr aa:bb:cc:00:01:11
      inet addr:100.50.50.1 Bcast:100.50.50.255 Mask:255.255.255.0
      inet6 addr: fe80::90b8:a4ff:fed9:e7bd/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:6 errors:0 dropped:0 overruns:0 frame:0
      TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
```



```
collisions:0 txqueuelen:1000
RX bytes:384 (384.0 B) TX bytes:468 (468.0 B)
Interrupt:5

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:2 errors:0 dropped:0 overruns:0 frame:0
      TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:100 (100.0 B) TX bytes:100 (100.0 B)

r3:~#
```

En el caso de r1, tiene activas las dos interfaces

5.

```
r3:~# /etc/init.d/openvpn start
Starting virtual private network daemon: serverOut of memory: kill process 325 (portmap)
score 439 or a child
Killed process 325 (portmap)
Out of memory: kill process 1074 (openssl-vulnkey) score 326 or a child
Killed process 1074 (openssl-vulnkey)
.
r3:~#
```

```
r1:~# /etc/init.d/openvpn start
Starting virtual private network daemon: clientOut of memory: kill process 325 (portmap)
score 439 or a child
Killed process 325 (portmap)
Out of memory: kill process 1098 (openssl-vulnkey) score 326 or a child
Killed process 1098 (openssl-vulnkey)
.
r1:~#
```

Luego verificamos las interfaces

```
r3:~# ifconfig
eth0  Link encap:Ethernet HWaddr aa:bb:cc:00:01:12
      inet addr:10.0.30.1 Bcast:10.0.30.255 Mask:255.255.255.0
      inet6 addr: fe80::e4b1:84ff:fec3:6102/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:6 errors:0 dropped:0 overruns:0 frame:0
      TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:384 (384.0 B) TX bytes:468 (468.0 B)
      Interrupt:5

eth1  Link encap:Ethernet HWaddr aa:bb:cc:00:01:11
```



```
inet addr:100.50.50.1 Bcast:100.50.50.255 Mask:255.255.255.0
inet6 addr: fe80::90b8:a4ff:fed9:e7bd/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:96 errors:0 dropped:0 overruns:0 frame:0
TX packets:95 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:10397 (10.1 KiB) TX bytes:13507 (13.1 KiB)
Interrupt:5

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:2 errors:0 dropped:0 overruns:0 frame:0
TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:100 (100.0 B) TX bytes:100 (100.0 B)

tun0  Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
00
inet addr:10.8.0.1 P-t-P:10.8.0.2 Mask:255.255.255.255
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:100
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

r3::~#

r1::~# ifconfig
eth0  Link encap:Ethernet HWaddr aa:bb:cc:00:01:05
inet addr:10.0.20.1 Bcast:10.0.20.255 Mask:255.255.255.0
inet6 addr: fe80::fc46:c8ff:fe27:2cd5/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:35 errors:0 dropped:0 overruns:0 frame:0
TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:18012 (17.5 KiB) TX bytes:1774 (1.7 KiB)
Interrupt:5

eth1  Link encap:Ethernet HWaddr aa:bb:cc:00:01:06
inet addr:100.60.60.1 Bcast:100.60.60.255 Mask:255.255.255.0
inet6 addr: fe80::6853:15ff:fe46:255/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:108 errors:0 dropped:0 overruns:0 frame:0
TX packets:121 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:13032 (12.7 KiB) TX bytes:26698 (26.0 KiB)
Interrupt:5

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:2 errors:0 dropped:0 overruns:0 frame:0
TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:100 (100.0 B) TX bytes:100 (100.0 B)

tun0    Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
00
inet addr:10.8.0.6 P-t-P:10.8.0.5 Mask:255.255.255.255
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:100
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

r1:~#
```

Ahora tenemos una nueva interfaz llamada tun0.

6.

```
pc1:~# ping -c 3 pc2
PING pc2 (10.0.20.21) 56(84) bytes of data.
64 bytes from pc2 (10.0.20.21): icmp_seq=1 ttl=64 time=10.2 ms
64 bytes from pc2 (10.0.20.21): icmp_seq=2 ttl=64 time=0.361 ms
64 bytes from pc2 (10.0.20.21): icmp_seq=3 ttl=64 time=0.306 ms

--- pc2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.306/3.642/10.260/4.679 ms
pc1:~# ping -c 3 pc3
PING pc3 (10.0.30.20) 56(84) bytes of data.
64 bytes from pc3 (10.0.30.20): icmp_seq=1 ttl=62 time=0.773 ms
64 bytes from pc3 (10.0.30.20): icmp_seq=2 ttl=62 time=2.94 ms
64 bytes from pc3 (10.0.30.20): icmp_seq=3 ttl=62 time=2.22 ms

--- pc3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2006ms
rtt min/avg/max/mdev = 0.773/1.980/2.949/0.905 ms
pc1:~#

pc2:~# ping -c 3 pc1
PING pc1 (10.0.20.20) 56(84) bytes of data.
64 bytes from pc1 (10.0.20.20): icmp_seq=1 ttl=64 time=0.112 ms
64 bytes from pc1 (10.0.20.20): icmp_seq=2 ttl=64 time=0.501 ms
64 bytes from pc1 (10.0.20.20): icmp_seq=3 ttl=64 time=0.311 ms

--- pc1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 0.112/0.308/0.501/0.158 ms
```



```
pc2:~# ping -c 3 pc3
PING pc3 (10.0.30.20) 56(84) bytes of data.
64 bytes from pc3 (10.0.30.20): icmp_seq=1 ttl=62 time=10.9 ms
64 bytes from pc3 (10.0.30.20): icmp_seq=2 ttl=62 time=2.16 ms
64 bytes from pc3 (10.0.30.20): icmp_seq=3 ttl=62 time=1.05 ms

--- pc3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 1.054/4.715/10.924/4.414 ms
pc2:~#
```

```
pc3:~# ping -c 3 pc1
PING pc1 (10.0.20.20) 56(84) bytes of data.
64 bytes from pc1 (10.0.20.20): icmp_seq=1 ttl=62 time=1.96 ms
64 bytes from pc1 (10.0.20.20): icmp_seq=2 ttl=62 time=0.637 ms
64 bytes from pc1 (10.0.20.20): icmp_seq=3 ttl=62 time=0.724 ms

--- pc1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 0.637/1.109/1.966/0.607 ms
pc3:~# ping -c 3 pc2
PING pc2 (10.0.20.21) 56(84) bytes of data.
64 bytes from pc2 (10.0.20.21): icmp_seq=1 ttl=62 time=0.780 ms
64 bytes from pc2 (10.0.20.21): icmp_seq=2 ttl=62 time=0.623 ms
64 bytes from pc2 (10.0.20.21): icmp_seq=3 ttl=62 time=1.97 ms

--- pc2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2017ms
rtt min/avg/max/mdev = 0.623/1.125/1.972/0.602 ms
pc3:~#
```

como no podíamos llegar de pc1 a pc3 hacemos un tracepath

```
pc1:~# tracepath pc3
  1: pc1 (10.0.20.20) 0.085ms pmtu 1500
    1: 10.0.20.1 (10.0.20.1) 10.288ms
      1: 10.0.20.1 (10.0.20.1) 0.128ms
        2: 10.8.0.1 (10.8.0.1) 0.877ms
          3: pc3 (10.0.30.20) 10.952ms reached
      Resume: pmtu 1500 hops 3 back 62
pc1:~#
```

vemos que en un punto pasa por la ip de la interfaz de la vpn.

7.

```
pc4:~# ping -c 3 pc1
PING pc1 (10.0.20.20) 56(84) bytes of data.

--- pc1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2008ms

pc4:~# ping -c 3 pc2
```



```
PING pc2 (10.0.20.21) 56(84) bytes of data.

--- pc2 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2012ms

pc4:~# ping -c 3 pc3
PING pc3 (10.0.30.20) 56(84) bytes of data.

--- pc3 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2004ms

pc4:~#
```

para poder conectar la red 10.0.40.0/24 tendremos que conectar r2 a la vpn, como ya tenemos generadas las claves de r2 (r2.crt y r2.key) podemos llevarnoslo a la carpeta de /r2/etc/openvpn.

tendremos que crear el client.conf con lo siguiente

```
client
port 1194
proto tcp
dev tun
remote 100.50.50.1 1194
ca ca.crt
cert r2.crt
key r2.key
keepalive 10 120
comp-lzo
persist-key
persist-tun
status openvpn-status.log
log openvpn.log
verb 3

# linea necesaria para que el trafico que va por la vpn
route 10.0.20.0 255.255.255.0
```

Adicionalmente en r3 tendremos que agregar el archivo r2 (sin extensión) en la carpeta /etc/openvpn/clients. Sirve para que el servidor vpn pueda enrutar el trafico de dicha red.

```
iroute 10.0.40.0 255.255.255.0
```

Ademas en el archivo /etc/openvpn/server.conf agregar la linea *route* .

```
route 10.0.40.0 255.255.255.0
```

Adicionalmente tambien tiene que ir al final del archivo client.conf en r1.

```
r1:~# nano /etc/openvpn/client.conf
...
# linea necesaria para que el trafico que va por la vpn
route 10.0.40.0 255.255.255.0
...
```




La línea *route* le indicara a el servidor openvpn que esa red se alcanza mediante un tunel vpn. Y el archivo *r2* en *client* indica que el cliente *r2* es quien se encarga de encaminar el trafico de la red indiada por *iroute*.

Los routers tienen que saber que esas redes se alcanzan por medio de la vpn, si agregamos la línea push “*route ...* “ pero los router *r1* entenderian que el trafico que va a hacia su red tiene que ir por la vpn y nunca pasa a los host detras de el.

8. Una vpn sirve para poder usar servicios de una red privada como si estuviéramos en la misma red, sin la necesidad de que esos servicios estén abiertos públicamente (lo que puede ser peligroso). Es sumamente útil para lugares con oficinas separadas y necesitan actuar como si estuvieran en el mismo red física (organismos estatales, policiales, sucursales empresariales, etc). En el caso del laboratorio también nos muestran que podemos conectar mediante vpn, redes que están separadas entre sí (en este caso *r4* no tiene gateway y no podemos llegar de una red a la otra) y de esta manera comunicarse entre sí.

Además algo que yo no sabía es que se pueden conectar redes, yo pensaba que solo se podían conectar host como si fueran parte de esa red privada, pero con el *iroute* se pueden decir que host (router) encamina el tráfico de una red en particular. Esto me parece bueno por que podemos tener una vpn en un router que este haciendo PAT y NAT (hacia internet), pudiendo conectarme desde cualquier red pública, y poder acceder a resto de redes privadas del otro lado de la vpn.