

**UNIVERSIDAD LUTERANA SALVADOREÑA
FACULTAD DE CIENCIAS DEL HOMBRE Y LA
NATURALEZA**



**ALUMNA : NORIS MARBELIS GAMEZ
REDES II**

Descripción de proyecto

El proyecto que se implementará consiste configurar un Firewall ó llamado también Cortafuegos con iptables , utilizando dos interfaces de red que serían en este caso dos modem en donde el propósito es que se conecten y compartan internet con el cliente a partir de cualquier interface, utilizando un balance entre las dos interfaces simulando la caída de cualquier de ellas con el propósito de que el cliente no sepa tal hecho además de eso con la red y firewall lo que se busca es que el servidor pueda controlar el flujo de datos en donde aplicara políticas a su conveniencia.

¿Que es un firewall?

Un firewall también es conocido como muro de fuego, este funciona entre las redes conectadas permitiendo o denegando las comunicaciones entre dichas redes. Un firewall también es considerado un filtro que controla el tráfico de varios protocolos como TCP/UDP/ICMP que pasan por el para permitir o denegar algún servicio, el firewall examina la petición y dependiendo de este lo puede bloquear o permitirle el acceso.

Iptables:

Iptables permite al administrador del sistema definir reglas acerca de qué hacer con los paquetes de red. Las reglas se agrupan en cadenas: cada cadena es una lista ordenada de reglas. Las cadenas se agrupan en tablas: cada tabla está asociada con un tipo diferente de procesamiento de paquetes.

- Balanceo de Carga

La Solución de balanceo de carga permite dividir las tareas que tendría que soportar una única máquina, con el fin de maximizar las capacidades de proceso de datos, así como de ejecución de tareas. Esta Solución permite que ningún equipo sea parte vital del servicio que queremos ofrecer. De esta forma evitamos sufrir una parada del servicio debido a una parada de una de las máquinas.

- NAT

Usada cuando se desea hacer los paquetes sean enrutados a una máquina cliente dentro de una red local, pero también podremos enmascarar un red local y tener salida hacia internet.

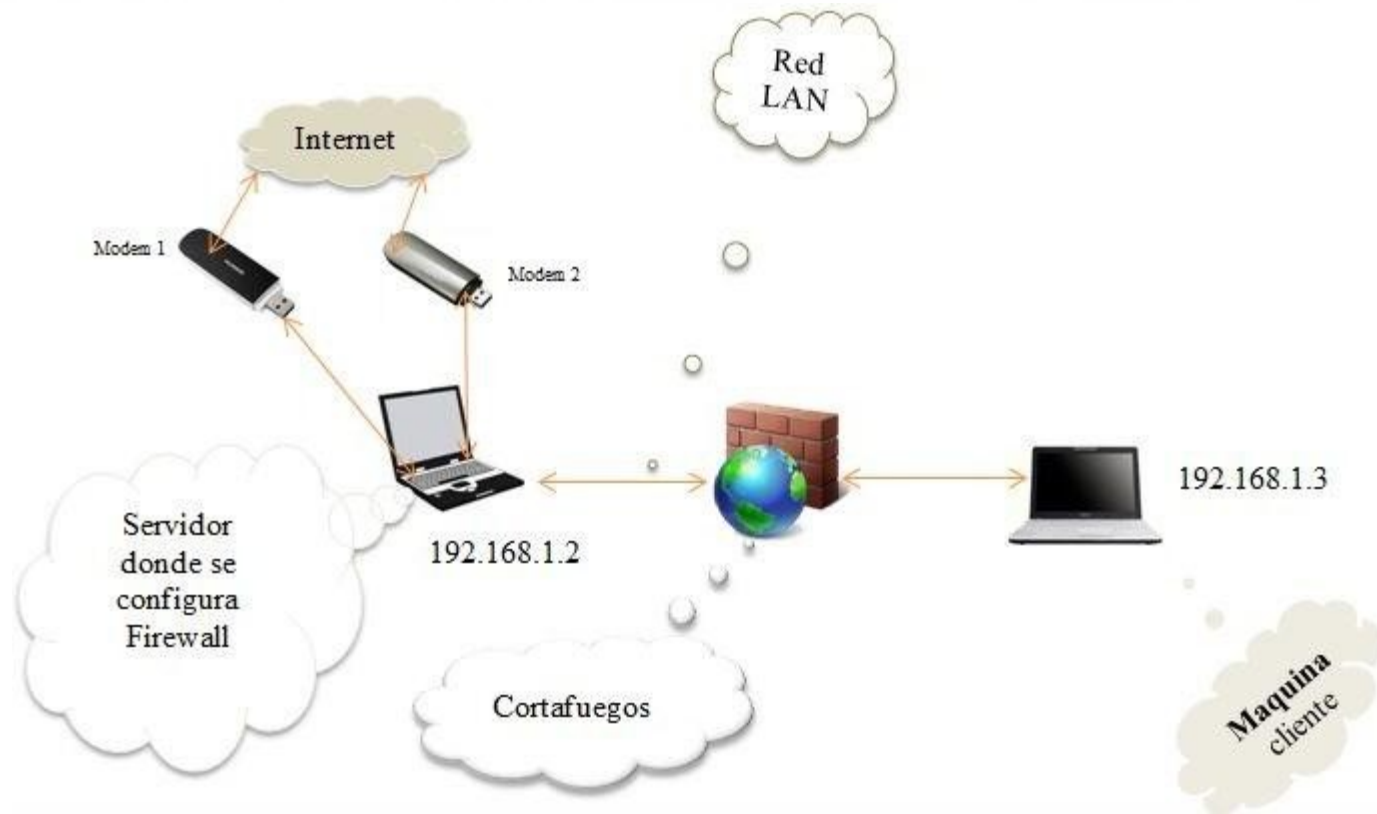
Wireshark

Es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica. Cuenta con todas las características estándar de un analizador de protocolos de forma únicamente hueca.

La funcionalidad que provee es similar a la de tcp ump, pero añade una interfaz gráfica y muchas opciones de organización y filtrado de información. Así, permite ver todo el tráfico que pasa a través de una red (usualmente una red Ethernet, aunque es compatible con algunas otras) estableciendo la configuración en modo promiscuo.

wvdial

Es una utilidad que ayuda a realizar conexiones a Internet basadas en módem y que se incluye en algunas distribuciones de GNU/Linux importantes.



nano /etc/network/interfaces

```
Terminal - usuario@Debian8: ~
Archivo Editar Ver Terminal Pestañas Ayuda
GNU nano 2.2.6 Fichero: /etc/network/interfaces Modificado
# La interfase loopback
#auto lo
#iface lo inet loopback

#auto eth0
#iface eth0 inet dhcp

auto eth0
iface eth0 inet static
address 192.168.1.2
netmask 255.255.255.0

^G Ver ayuda      ^O Guardar      ^R Leer Fich    ^Y Pág Ant      ^K CortarTxt    ^C Pos actual
^X Salir          ^J Justificar   ^W Buscar       ^V Pág Sig      ^U PegarTxt     ^T Ortografía
```

/etc/init.d/networking restart

IFCONFIG

```
Terminal - usuario@Debian8: ~
Archivo Editar Ver Terminal Pestañas Ayuda
3: wlan0: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state DORMANT mode DORMANT group default qlen 1000
  link/ether c4:17:fe:0a:f4:a7 brd ff:ff:ff:ff:ff:ff
root@Debian8:/home/usuario# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:26:b9:a8:92:89
          inet addr:192.168.1.2  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST 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:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

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:45173 errors:0 dropped:0 overruns:0 frame:0
          TX packets:45173 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3961974 (3.7 MiB)  TX bytes:3961974 (3.7 MiB)

wlan0     Link encap:Ethernet  HWaddr c4:17:fe:0a:f4:a7
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:15189 errors:0 dropped:6 overruns:0 frame:130208
```

nano /proc/sys/net/ipv4/conf/all/forwarding

nano /etc/sysctl.conf

```
Terminal - noris@gamez: ~
Archivo Editar Ver Terminal Ir Ayuda
GNU nano 2.2.6 Fichero: /etc/sysctl.conf Modificado

#net.ipv4.tcp_syncookies=1
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip forward=1

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1

#####
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network environments, however, require that these
# settings are disabled so review and enable them as needed.
#
# Do not accept ICMP redirects (prevent MITM attacks)
#net.ipv4.conf.all.accept_redirects = 0
#net.ipv6.conf.all.accept_redirects = 0
# _or_

^G Ver ayuda      ^O Guardar      ^R Leer Fich    ^Y Pág Ant      ^K CortarTxt    ^C Pos actual
^X Salir          ^J Justificar   ^W Buscar       ^V Pág Sig      ^U PegarTxt     ^T Ortografía
```

• Instalación de wvdial nano */etc/wvdial.conf*

```
Terminal - usuario@Debian8: ~
Archivo Editar Ver Terminal Pestañas Ayuda
GNU nano 2.2.6 Fichero: /etc/wvdial.conf

[Dialer claro1]
Init1 = ATV1E0
Init2 = AT+CGMI
Init3 = AT+CGMM
Init4 = ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0
Init5 = AT+CGDCONT=1,"IP","internet.com"
Password = webgprs2002
Phone = *99#
Modem type = Analog Modem
Stupid Mode = 1
Baud = 460800
New PPPD = 1
Dial Command = ATD
Modem = /dev/ttyUSB0
ISDN = 0
Username = webgprs

[Dialer claro2]
Init1 = ATV1E0
Init2 = AT+CGMI
Init3 = AT+CGMM

^G Ver ayuda    ^O Guardar      ^R Leer Fich    ^Y Pág Ant     ^K CortarTxt    ^C Pos actual
^X Salir        ^J Justificar   ^W Buscar       ^V Pág Sig     ^U PegarTxt     ^T Ortografía
```

Comando para compartir internet

```
Terminal
Archivo Editar Ver Terminal Ir Ayuda
GNU nano 2.2.6 Fichero: firewall.sh
#!/bin/bash

# Reenvio de paquetes
echo 1 > /proc/sys/net/ipv4/ip_forward

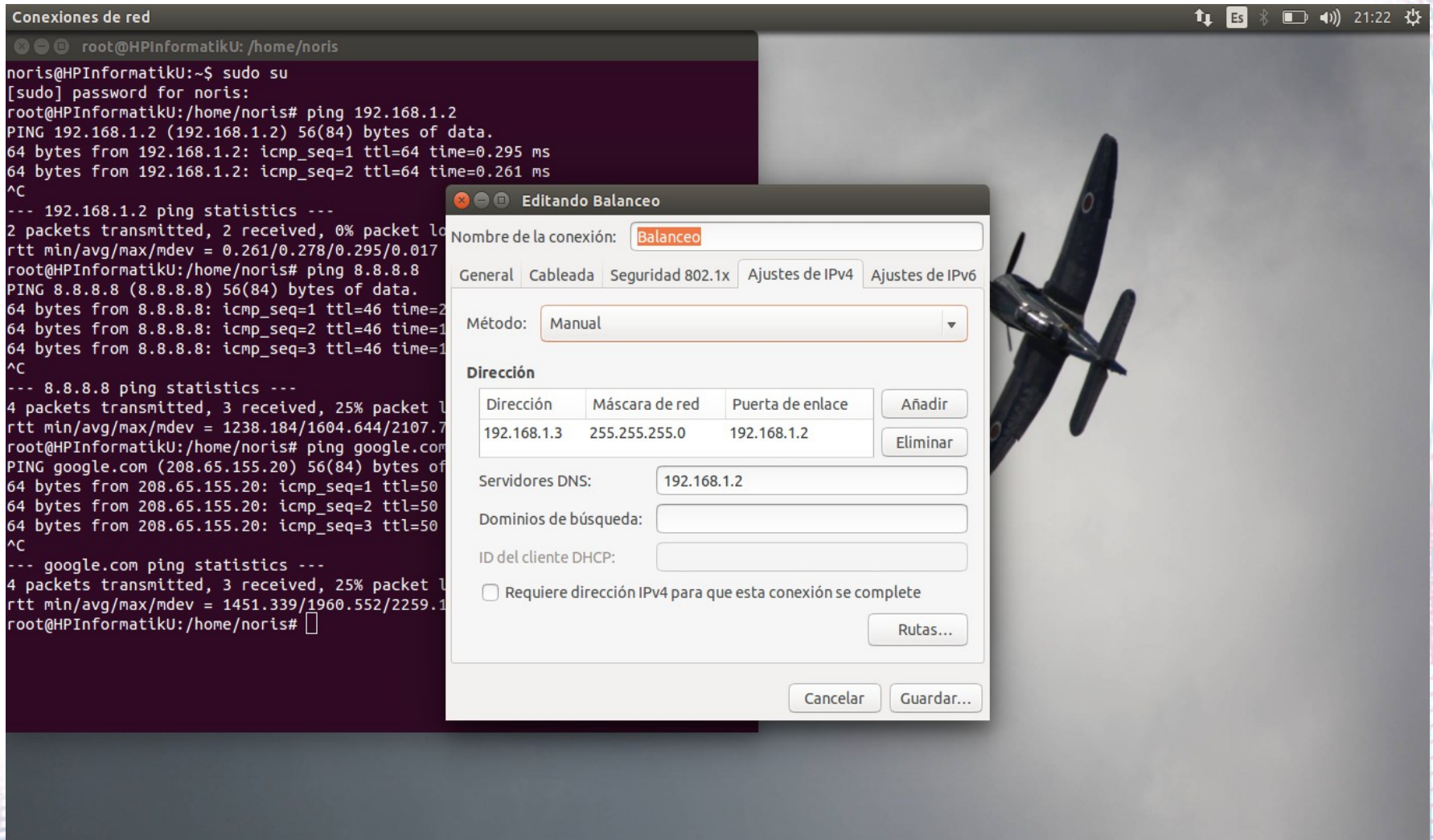
# Borramos reglas anteriores de iptables

iptables -F
iptables -X
iptables -Z
iptables -t nat -F

#Activando NAT en ppp0

iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
iptables -t nat -A POSTROUTING -o ppp1 -j MASQUERADE
iptables --append FORWARD --in-interface eth0 -j ACCEPT
#route add default wt 10.10.10.64 dev ppp0
#Iniciamos DHCP Server en /etc/dnsmasq.conf
```

Configurar al cliente



The image shows a Linux terminal window titled "Conexiones de red" and a network configuration window titled "Editando Balanceo".

Terminal Output:

```
root@HPInformatikU: /home/noris
noris@HPInformatikU:~$ sudo su
[sudo] password for noris:
root@HPInformatikU:/home/noris# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.295 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.261 ms
^C
--- 192.168.1.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time=0.556s
rtt min/avg/max/mdev = 0.261/0.278/0.295/0.017 ms
root@HPInformatikU:/home/noris# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=46 time=1.238 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=46 time=1.184 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=46 time=1.160 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time=4.000s
rtt min/avg/max/mdev = 1238.184/1604.644/2107.711/197.711 ms
root@HPInformatikU:/home/noris# ping google.com
PING google.com (208.65.155.20) 56(84) bytes of data.
64 bytes from 208.65.155.20: icmp_seq=1 ttl=50 time=1451.339 ms
64 bytes from 208.65.155.20: icmp_seq=2 ttl=50 time=1960.552 ms
64 bytes from 208.65.155.20: icmp_seq=3 ttl=50 time=2259.111 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time=4.650s
rtt min/avg/max/mdev = 1451.339/1960.552/2259.111/342.741 ms
root@HPInformatikU:/home/noris#
```

Network Configuration Window (Editando Balanceo):

- Nombre de la conexión: **Balanceo**
- General | Cableada | Seguridad 802.1x | Ajustes de IPv4 | Ajustes de IPv6
- Método: **Manual**
- Dirección:

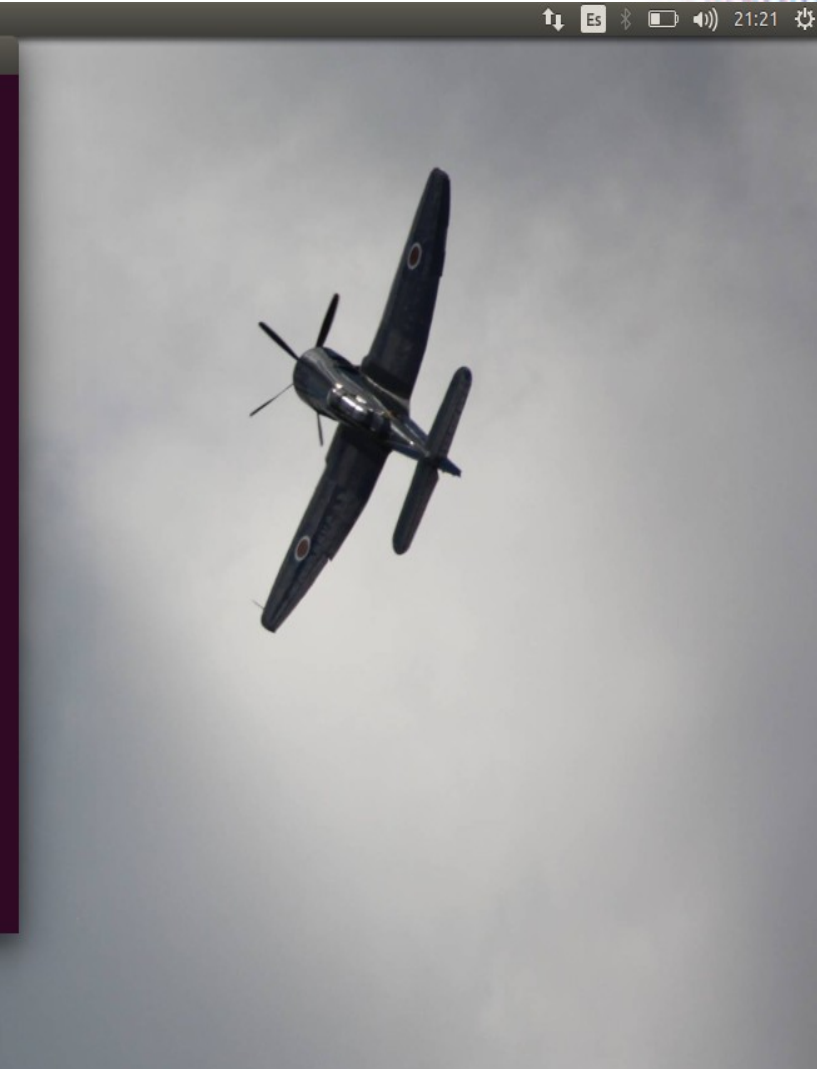
Dirección	Máscara de red	Puerta de enlace	Añadir
192.168.1.3	255.255.255.0	192.168.1.2	Eliminar

- Servidores DNS: **192.168.1.2**
- Dominios de búsqueda:
- ID del cliente DHCP:
- Requiere dirección IPv4 para que esta conexión se complete
- Rutas... (button)
- Cancelar (button) | Guardar... (button)

Haciendo ping

Verificando la conexión

```
Terminal
root@HPInformatikU:~# ping 192.168.1.2
noris@HPInformatikU:~$ sudo su
[sudo] password for noris:
root@HPInformatikU:/home/noris# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.295 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.261 ms
^C
--- 192.168.1.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.261/0.278/0.295/0.017 ms
root@HPInformatikU:/home/noris# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=46 time=2107 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=46 time=1468 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=46 time=1238 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3000ms
rtt min/avg/max/mdev = 1238.184/1604.644/2107.737/367.905 ms, pipe 3
root@HPInformatikU:/home/noris# ping google.com
PING google.com (208.65.155.20) 56(84) bytes of data.
64 bytes from 208.65.155.20: icmp_seq=1 ttl=50 time=2259 ms
64 bytes from 208.65.155.20: icmp_seq=2 ttl=50 time=1451 ms
64 bytes from 208.65.155.20: icmp_seq=3 ttl=50 time=2171 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3879ms
rtt min/avg/max/mdev = 1451.339/1960.552/2259.166/361.858 ms, pipe 3
root@HPInformatikU:/home/noris#
```



Verificar datos de interfaces

```
Terminal - noris@gamez: ~
Archivo Editar Ver Terminal Ir Ayuda
gamez:/home/noris# ip route
default via 10.64.64.64 dev ppp0 proto static
10.64.64.64 dev ppp0 proto kernel scope link src 10.230.5.143
10.64.64.65 dev ppp1 proto kernel scope link src 10.85.2.136
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.2
gamez:/home/noris# █
```

Aplicando los comandos para el balance de interfaces

```
Terminal
Archivo Editar Ver Terminal Ir Ayuda
GNU nano 2.2.6 Fichero: firewall.sh Modificado
IF1=ppp0
IF2=ppp1
IP1=10.230.5.143
IP2=10.85.2.136
P1=10.64.64.64
P2=10.64.64.65
P1_NET=10.230.5.143
P2_NET=10.85.2.136

echo "ip route add $P1_NET dev $IF1 src $IP1 table 1"
ip route add $P1_NET dev $IF1 src $IP1 table 1
echo "ip route add default via $P1 table 1"
ip route add default via $P1 table 1
echo "ip route add $P2_NET dev $IF2 src $IP2 table 2"
ip route add $P2_NET dev $IF2 src $IP2 table 2
echo "ip route add default via $P2 table 2"
ip route add default via $P2 table 2
echo "ip route add $P1_NET dev $IF1 src $IP1"
ip route add $P1_NET dev $IF1 src $IP1
echo "ip route add $P2_NET dev $IF2 src $IP2"
ip route add $P2_NET dev $IF2 src $IP2
echo "ip rule add from $IP1 table T1"

^G Ver ayuda ^O Guardar ^R Leer Fich ^Y Pág Ant ^K CortarTxt ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^V Pág Sig ^U PegarTxt ^T Ortografía
```

Verificamos en que interface esta el trafico

The screenshot shows the Wireshark interface with a list of captured packets. The packets are filtered by the expression 'Expression...'. The list includes ICMP ping requests and replies, and DNS standard queries and responses. The detailed view of the selected packet (No. 62) shows it is a DNS query for 'E.8..@. @....P.. ...Z.i.5 .\${m.... .google. com....'.

No.	Time	Source	Destination	Protocol	Length	Info
50	38.48760100	186.151.236.123	10.80.28.194	ICMP	100	Echo (ping) reply id=0x491e, seq=10/2560, ttl=...
51	38.48795300	10.80.28.194	216.230.147.90	DNS	90	Standard query 0x1639 PTR 123.236.151.186.in-ad...
52	39.08759000	216.230.147.90	10.80.28.194	DNS	142	Standard query response 0x1639 PTR 123.236.151.186.in-ad...
53	39.08793900	10.80.28.194	186.151.236.123	ICMP	100	Echo (ping) request id=0x491e, seq=11/2816, ttl=...
54	39.57731700	186.151.236.123	10.80.28.194	ICMP	100	Echo (ping) reply id=0x491e, seq=11/2816, ttl=...
55	39.57764800	10.80.28.194	216.230.147.90	DNS	90	Standard query 0x02ff PTR 123.236.151.186.in-ad...
56	39.94747800	216.230.147.90	10.80.28.194	DNS	142	Standard query response 0x02ff PTR 123.236.151.186.in-ad...
57	40.08891900	10.80.28.194	186.151.236.123	ICMP	100	Echo (ping) request id=0x491e, seq=12/3072, ttl=...
58	40.34836500	186.151.236.123	10.80.28.194	ICMP	100	Echo (ping) reply id=0x491e, seq=12/3072, ttl=...
59	40.34874300	10.80.28.194	216.230.147.90	DNS	90	Standard query 0x0612 PTR 123.236.151.186.in-ad...
60	45.35271500	10.80.28.194	201.247.155.225	DNS	90	Standard query 0x0612 PTR 123.236.151.186.in-ad...
61	48.35592800	10.80.28.194	200.85.29.129	DNS	90	Standard query 0x0612 PTR 123.236.151.186.in-ad...
62	54.35695000	10.80.28.194	216.230.147.90	DNS	90	Standard query 0x0612 PTR 123.236.151.186.in-ad...

Frame 1: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 1
Linux cooked capture
Internet Protocol Version 4, Src: 10.80.28.194 (10.80.28.194), Dst: 216.230.147.90 (216.230.147.90)
User Datagram Protocol, Src Port: 36201 (36201), Dst Port: domain (53)
Domain Name System (query)

```
000 00 04 02 00 00 00 00 00 00 00 00 00 08 00 .....  
010 45 00 00 38 a7 a7 40 00 40 11 ff ba 0a 50 1c c2 E..8..@. @....P..  
020 d8 e6 93 5a 8d 69 00 35 00 24 3c 6d 8e 8e 01 00 ...Z.i.5 .${m....  
030 00 01 00 00 00 00 00 00 06 67 6f 6f 67 6c 65 03 ..... .google.  
040 63 6f 6d 00 00 01 00 01 com.....
```

The background features a complex, abstract pattern of thin, overlapping lines in red and blue. These lines form a series of interconnected, slightly offset rectangular and polygonal shapes, creating a 3D wireframe effect. The lines are most dense and vibrant in the corners and fade towards the center, which is a plain white space.

Gracias