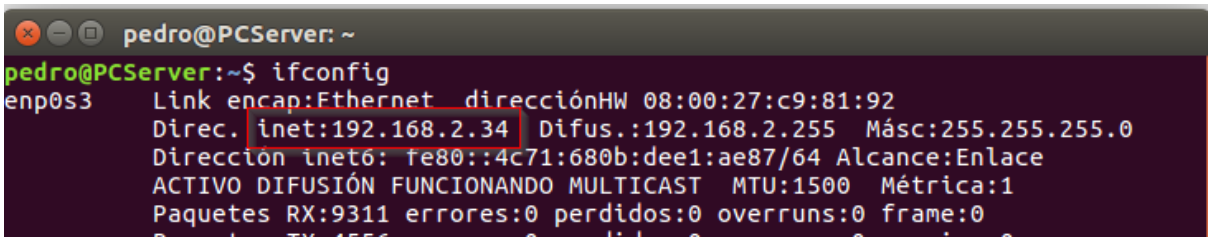
1. Descriu cóm utilitzar hping per verificar si el servei FTP està activat i si es troba redireccionat en un host interno.

Comprobar que el servicio FTP está activado:

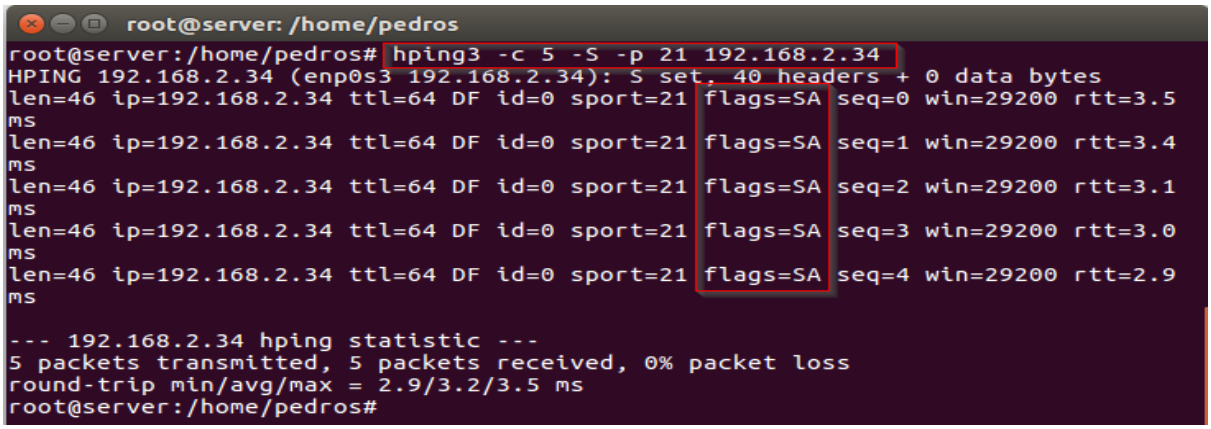
Con la herramienta hping se envían **5** paquetes solicitando la conexión al servicio ftp por el puerto **21**.

Vamos a probarlo con un par de máquinas virtuales. Una de ellas tiene el puerto 21 abierto. Realizamos un ifconfig en la máquina a la que vamos hacer el ping para saber que IP tiene:

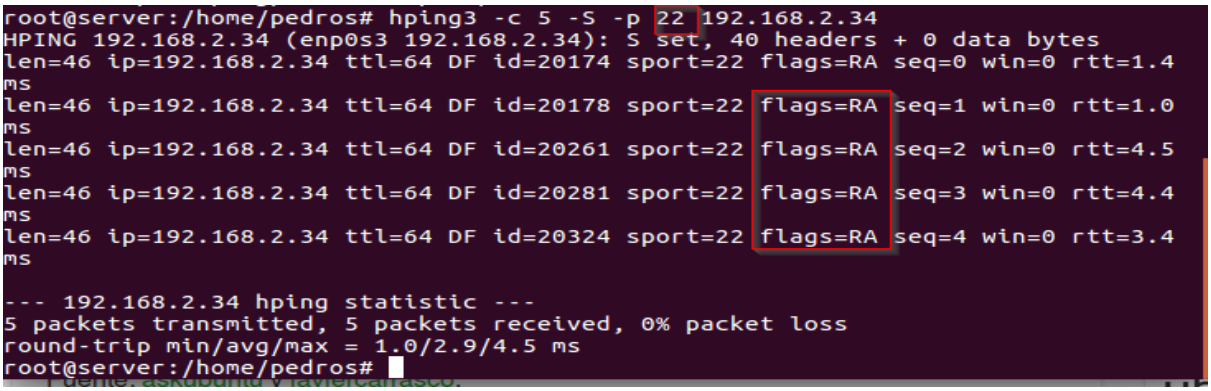


Ahora procedemos a realizar el ping sobre el puerto 21 sobre la máquina con IP **192.168.2.34**:

hping3 -c 5 -S -p 21 192.168.2.34



Si ahora cambiamos el puerto (**22**) y hacemos el ping sobre la misma máquina obtenemos el siguiente resultado:



Ahora realizaremos el ping sobre otra máquina al puerto **21** que sabemos que está cerrado:

```
root@server:/home/pedros# hping3 -c 5 -S -p 21 192.168.2.50
HPING 192.168.2.50 (enp0s3 192.168.2.50): S set, 40 headers + 0 data bytes

--- 192.168.2.50 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@server:/home/pedros#
```

De las pruebas anteriores podemos sacar las siguientes conclusiones:

- Si en la respuesta aparece **SA** el puerto está activo

- Si en la respuesta aparece **RA** el puerto está cerrado

- Si no hay respuesta es que el puerto está **filtrado por un firewall.**

- **c 5** → Esto quiere decir que se van a enviar 5 paquetes a ese destino.

- **S** → Indica el tipo de señal que activará. En este caso SYN indica la intención de iniciar una nueva conexión.

- **p** → Especifica el número de puerto destino.

Comprobar si el servicio FTP está redireccionado:

Para descubrir si el puerto se encuentra redireccionado, debemos enviar la misma petición a diferentes números de puerto y fijarnos en los valores de las variables **len** o **TTL**. Si estas difieren según el puerto, y en algunas de ellas recibimos la respuesta más tarde, podemos sacar la conclusión de que ese puerto está redireccionado en un host interno.

2. Construeix una ordre de iptables que accepti el tràfic TCP amb el port de destí sigui el 80 en la interfície eth1 amb IP origen 10.10.10.10.

iptables -A INPUT -i eth1 -s 10.10.10.10/8 -p TCP --dport 80 -j ACCEPT

Se acepta el tráfico **TCP** con destino el Puerto **80** por la interface **eth1** a la ip **10.10.10.10/8**

3. Construir una regla amb iptables que tanqui tots els ports des de el 1 al 1024.

iptables -A INPUT -p tcp --dport 1:1024 -j DROP

Con esta regla se deniega la entrada tcp a los paquetes con destino el rango de puertos del 1 a 1024.

iptables -A OUTPUT -p tcp --dport 1:1024 -j DROP

Con esta regla se deniega la salida tcp a los paquetes con destino el rango de puertos del 1 a 1024.

```
root@server:/home/pedros# iptables -A INPUT -p tcp --dport 1:1024 -j DROP
root@server:/home/pedros#
root@server:/home/pedros# iptables -A OUTPUT -p tcp --dport 1:1024 -j DROP
root@server:/home/pedros#
root@server:/home/pedros# iptables -L -n -v
Chain INPUT (policy ACCEPT 4 packets, 620 bytes)
 pkts bytes target     prot opt in     out     source               destination

    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
          tcp dpts:1:1024

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


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

    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
          tcp dpts:1:1024
root@server:/home/pedros#
```

4. Descriu quins paràmetres s'han de modificar per que un equip no respongui a un ping extern.

iptables -t filter -A INPUT -p icmp --icmp-type echo-request -j REJECT

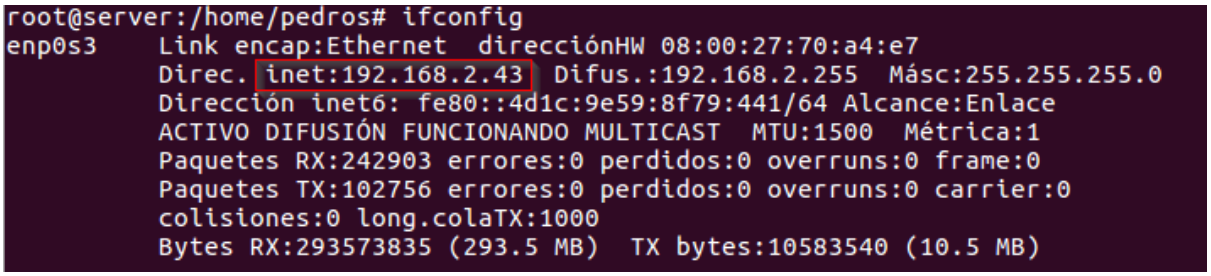
Con estas directivas se rechazan los mensajes icmp de **tipoecho- request** que entren por el Puerto icmp.

Para ver la configuración de Iptables introducimos el siguiente comando:

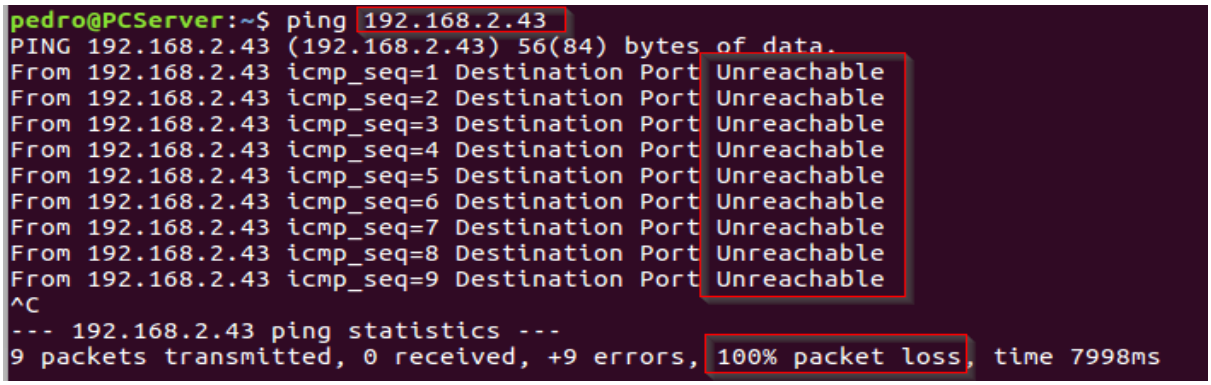
Iptables -L

```
root@server:/home/pedros# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     icmp --  anywhere             anywhere             icmp echo-request
reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@server:/home/pedros#
```

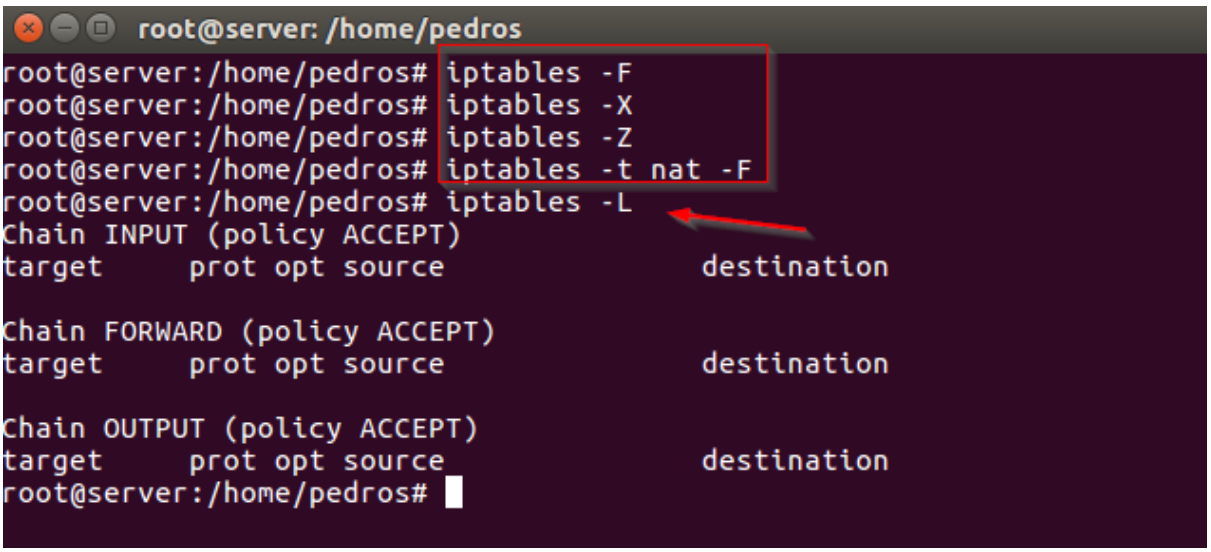
Ahora vamos a cualquier host dentro de la red y ejecutamos un ping a ver si responde. Antes hacemos un ifconfig para saber la IP del host:

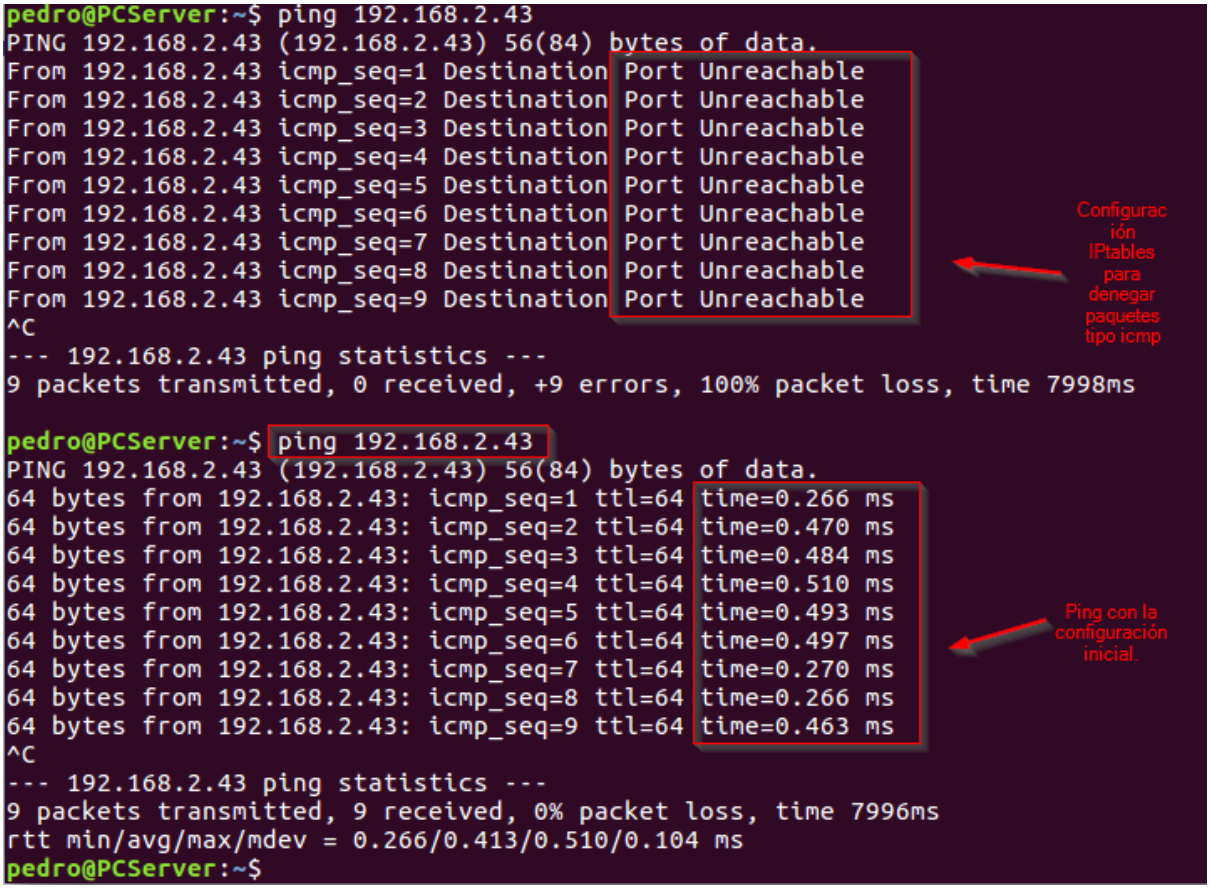


Realizamos el ping:



Ahora borraremos la configuración de Iptables y volveremos a realizar el ping a ver si hay respuesta del host:




pedro@PCServer:~$ ping 192.168.2.43
PING 192.168.2.43 (192.168.2.43) 56(84) bytes of data.
From 192.168.2.43 icmp_seq=1 Destination Port Unreachable
From 192.168.2.43 icmp_seq=2 Destination Port Unreachable
From 192.168.2.43 icmp_seq=3 Destination Port Unreachable
From 192.168.2.43 icmp_seq=4 Destination Port Unreachable
From 192.168.2.43 icmp_seq=5 Destination Port Unreachable
From 192.168.2.43 icmp_seq=6 Destination Port Unreachable
From 192.168.2.43 icmp_seq=7 Destination Port Unreachable
From 192.168.2.43 icmp_seq=8 Destination Port Unreachable
From 192.168.2.43 icmp_seq=9 Destination Port Unreachable
^C
--- 192.168.2.43 ping statistics ---
9 packets transmitted, 0 received, +9 errors, 100% packet loss, time 7998ms
Configuración IPtables para denegar paquetes tipo icmp
pedro@PCServer:~$ ping 192.168.2.43
PING 192.168.2.43 (192.168.2.43) 56(84) bytes of data.
64 bytes from 192.168.2.43: icmp_seq=1 ttl=64 time=0.266 ms
64 bytes from 192.168.2.43: icmp_seq=2 ttl=64 time=0.470 ms
64 bytes from 192.168.2.43: icmp_seq=3 ttl=64 time=0.484 ms
64 bytes from 192.168.2.43: icmp_seq=4 ttl=64 time=0.510 ms
64 bytes from 192.168.2.43: icmp_seq=5 ttl=64 time=0.493 ms
64 bytes from 192.168.2.43: icmp_seq=6 ttl=64 time=0.497 ms
64 bytes from 192.168.2.43: icmp_seq=7 ttl=64 time=0.270 ms
64 bytes from 192.168.2.43: icmp_seq=8 ttl=64 time=0.266 ms
64 bytes from 192.168.2.43: icmp_seq=9 ttl=64 time=0.463 ms
^C
--- 192.168.2.43 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 7996ms
rtt min/avg/max/mdev = 0.266/0.413/0.510/0.104 ms
pedro@PCServer:~$
Ping con la configuración inicial.