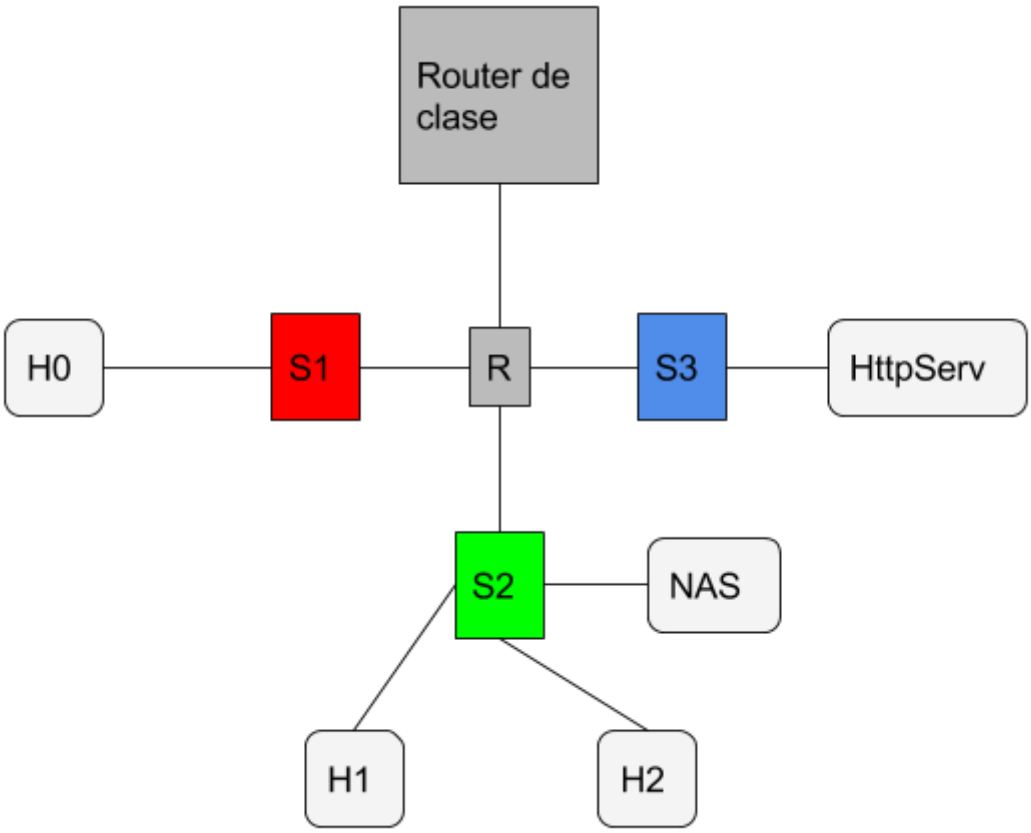
La estructura elegida para mi empresa seria así:



Mi red roja seria la enp0s9, la red verde seria la enp0s3 y la red azul seria la enp0s8.
El router tendría esta configuración de red:

Red Verde

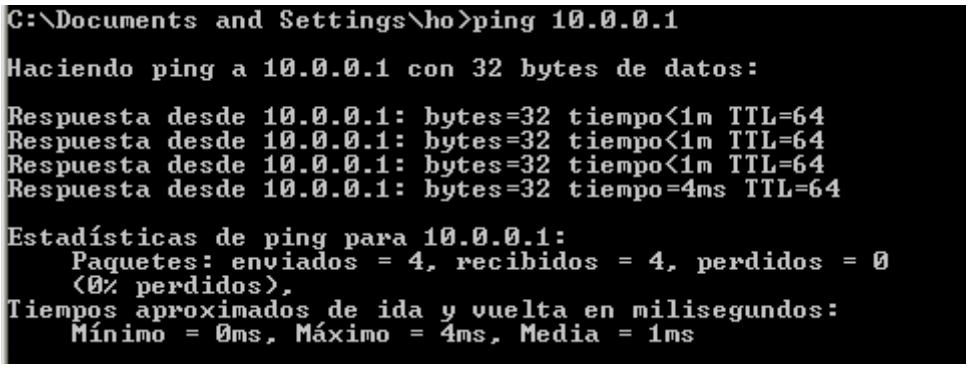
Red azul

Red roja

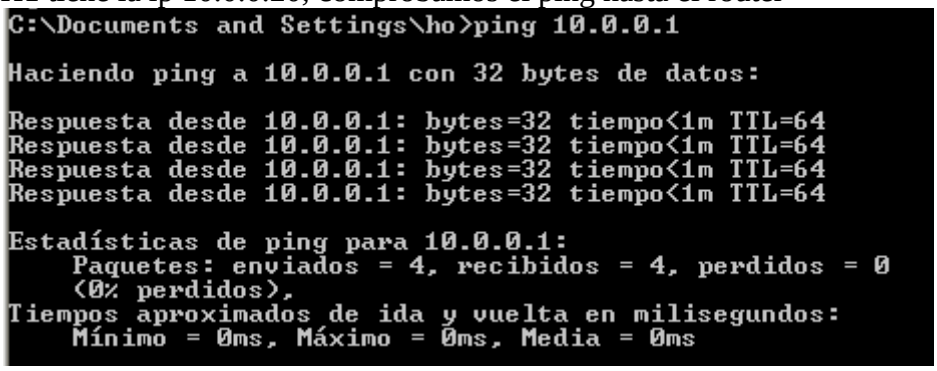
Salida a internet

```
enp0s3    Link encap:Ethernet  direcciónHW 08:00:27:b2:f2:8f
          Direc. inet:10.0.0.1  Difus.:10.0.0.255  Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:feb2:f28f/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1
          Paquetes RX:524 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:36 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:51811 (51.8 KB)  TX bytes:2800 (2.8 KB)

enp0s8    Link encap:Ethernet  direcciónHW 08:00:27:28:63:26
          Direc. inet:10.0.1.1  Difus.:10.0.1.255  Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:fe28:6326/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1
          Paquetes RX:447 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:29 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:44028 (44.0 KB)  TX bytes:2228 (2.2 KB)

enp0s9    Link encap:Ethernet  direcciónHW 08:00:27:f3:56:cc
          Direc. inet:10.0.2.1  Difus.:10.0.2.255  Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:fef3:56cc/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1
          Paquetes RX:315 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:34 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:29190 (29.1 KB)  TX bytes:2642 (2.6 KB)

enp0s10   Link encap:Ethernet  direcciónHW 08:00:27:2b:6b:62
          Direc. inet:192.168.3.224  Difus.:192.168.3.255  Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:fe2b:6b62/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1
          Paquetes RX:5988 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:988 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:3197893 (3.1 MB)  TX bytes:70339 (70.3 KB)
```

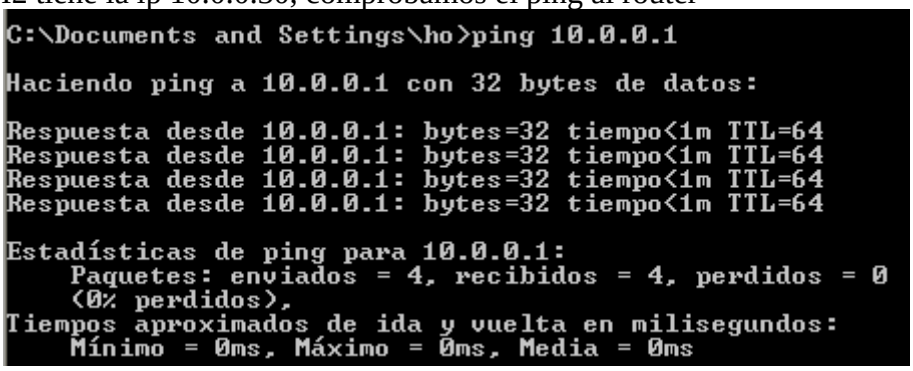
El ordenador H0 de la red roja tiene la ip 10.0.2.5, comprobamos que hace ping al router



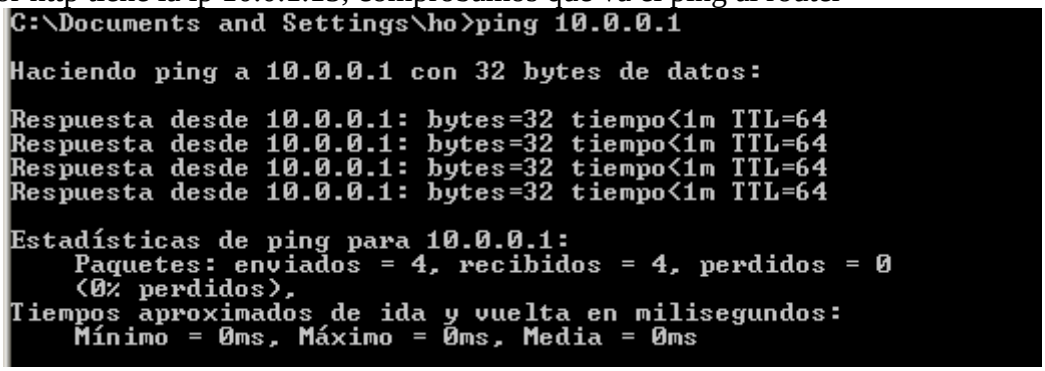
El ordenador H1 tiene la ip 10.0.0.20, comprobamos el ping hasta el router



El ordenador H2 tiene la ip 10.0.0.30, comprobamos el ping al router



El servidor http tiene la ip 10.0.1.15, comprobamos que va el ping al router



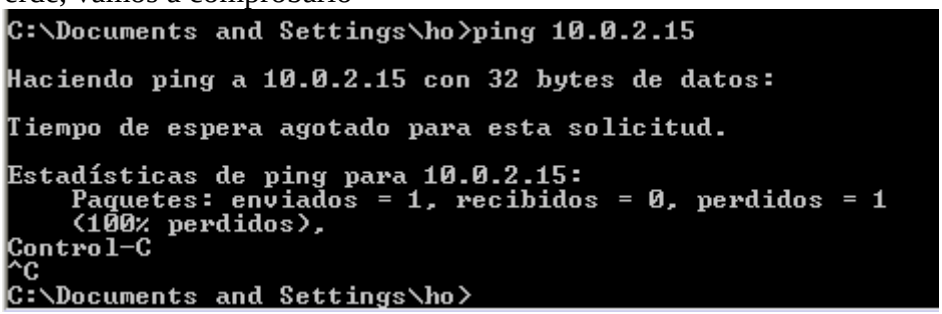
El script que he hecho para poder tener seguridad en la red es el siguiente:

```
#!/bin/bash

echo 1 > /proc/sys/net/ipv4/ip_forward

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

#por defecto
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

echo 1

#router
iptables -t nat -A POSTROUTING -o enp0s10 -j MASQUERADE

echo 1

#wifi (rojo)
iptables -A FORWARD -i enp0s9 -o enp0s10 -p tcp -m multiport --dport 80,443,53 -j ACCEPT
iptables -A FORWARD -o enp0s9 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s8 -p tcp -m multiport --dport 80,443 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s10 -p udp -m multiport --dport 80,443,53 -j ACCEPT
echo 3

#Verde
iptables -A FORWARD -i enp0s3 -s 10.0.0.20 -o enp0s8 -p tcp -m multiport --dport 22,80,443 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s8 -p tcp -m multiport --dport 80,443,53 -j ACCEPT
iptables -A FORWARD -i enp0s3 -s 10.0.0.20 -o enp0s10 -p tcp -m multiport --dport 22,80,443 -j ACCE$
                                [ 49 líneas leídas ]
^G Ver ayuda  ^O Guardar    ^W Buscar      ^K Cortar Text^J Justificar ^C Posición   ^Y Pág. ant.
^X Salir      ^R Leer fich. ^\ Reemplazar  ^U Pegar txt  ^T Corrector  ^_ Ir a línea ^V Pág. sig.
```

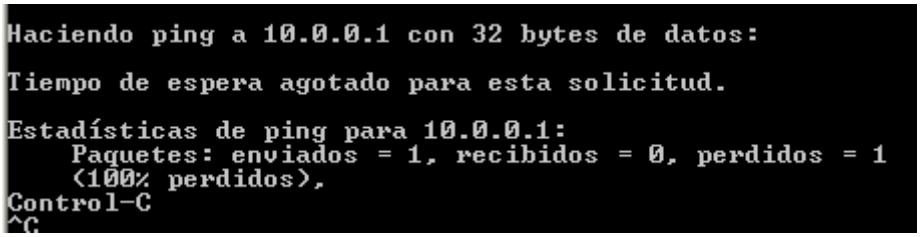
```
iptables -t nat -A POSTROUTING -o enp0s10 -j MASQUERADE

echo 1

#wifi (rojo)
iptables -A FORWARD -i enp0s9 -o enp0s10 -p tcp -m multiport --dport 80,443,53 -j ACCEPT
iptables -A FORWARD -o enp0s9 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s8 -p tcp -m multiport --dport 80,443 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s10 -p udp -m multiport --dport 80,443,53 -j ACCEPT
echo 3

#Verde
iptables -A FORWARD -i enp0s3 -s 10.0.0.20 -o enp0s8 -p tcp -m multiport --dport 22,80,443 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s8 -p tcp -m multiport --dport 80,443,53 -j ACCEPT
iptables -A FORWARD -i enp0s3 -s 10.0.0.20 -o enp0s10 -p tcp -m multiport --dport 22,80,443 -j ACCE$
iptables -A FORWARD -i enp0s3 -o enp0s10 -p tcp -m multiport --dport 80,443,53 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s10 -p udp -m multiport --dport 80,443,53 -j ACCEPT
echo 4
#http
iptables -A FORWARD -i enp0s8 -o enp0s10 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s9 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s3 -m state --state ESTABLISHED,RELATED -j ACCEPT
echo 5
#internet
iptables -A FORWARD -i enp0s10 -o enp0s9 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i enp0s10 -o enp0s3 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i enp0s10 -o enp0s8 -m state --state ESTABLISHED,RELATED -j ACCEPT
echo 6
#router
iptables -A INPUT -i enp0s3 -s 10.0.0.20
echo 7


^G Ver ayuda  ^O Guardar    ^W Buscar      ^K Cortar Text^J Justificar ^C Posición   ^Y Pág. ant.
^X Salir      ^R Leer fich. ^\ Reemplazar  ^U Pegar txt  ^T Corrector  ^_ Ir a línea ^V Pág. sig.
```

cuando ejecutamos nuestro script no nos tendría que dar ningún error, en mi script para ver que todo funciona bien e puesto un “echo” y el numero de la red para que si todo funciona bien salga echo y todos los números

Una vez ejecutado tenemos que comprobar que funciona, no tendria que poder hacer ping la red roja a la red verde, vamos a comprobarlo



Vemos que no podemos hacer ping de una red a otra, porque es una red segura.
Al router tampoco puede hacer porque solo un ordenador puede acceder al router



Desde la red rojo vemos que tampoco puede hacer ping al router