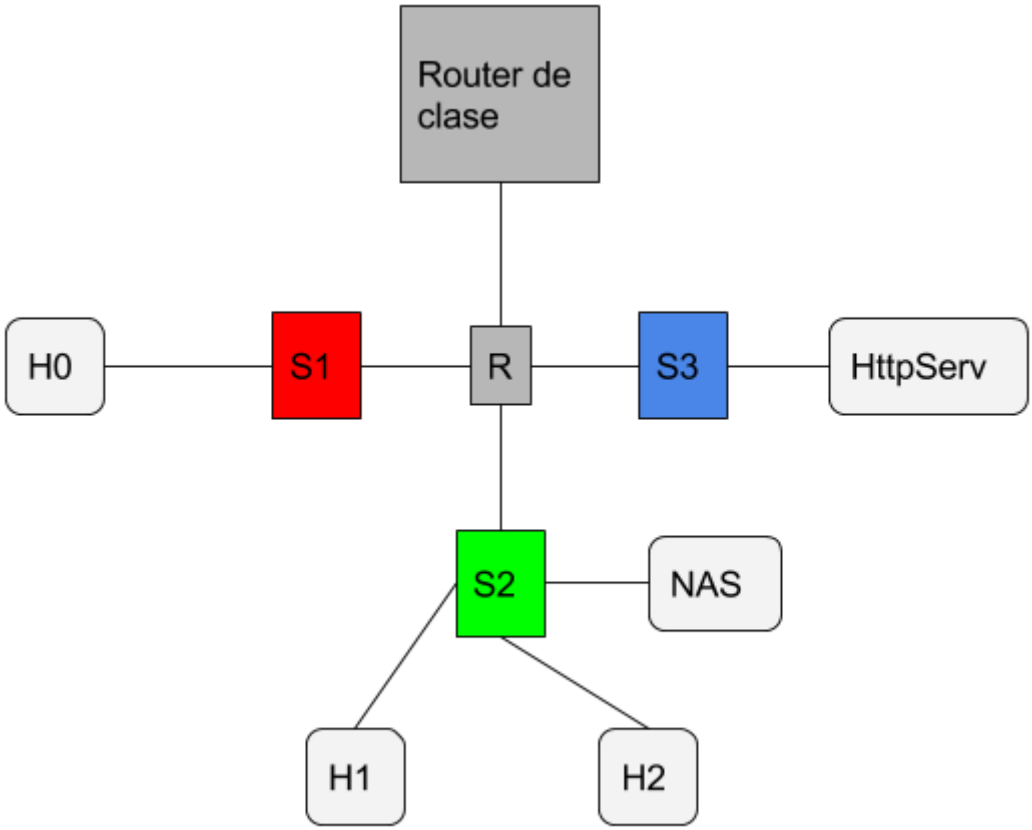
PRACTICA IPTABLES

Vamos a crear una red donde hay
Red Roja: Es una red wifi y por lo tanto no segura.
Red verde: Es la red interna de la empresa, es una red fiable. Aquí se encuentran los trabajadores y un NAS.
Red azul: Es una red donde hay servidores http públicos.

Me he guiado del siguiente esquema para esta práctica.



He creado las maquinas H0 → en mi caso lo he llamado wifi,H1,H2, Servidor http y el Ruter.
Con las siguientes IPs:

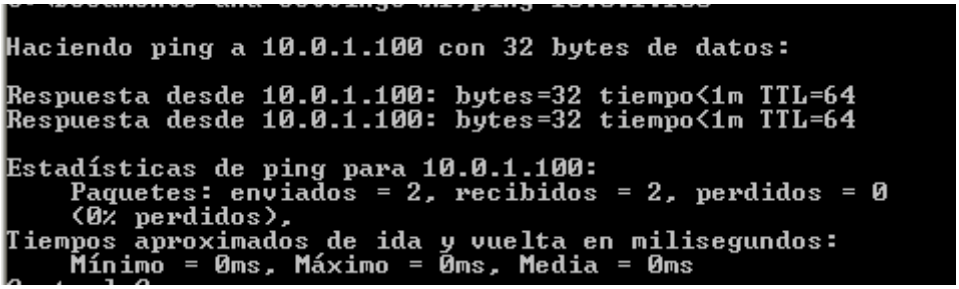
H0→ 10.0.1.1
H1 → 10.0.2.1
H2 → 10.0.2.2
Servidor http → 10.0.3.1

Y el ruter →
enp0s3 → Bridge
enp0s8 → 10.0.1.100
enp0s9 → 10.0.2.100
enp0s10 → 10.0.3.100

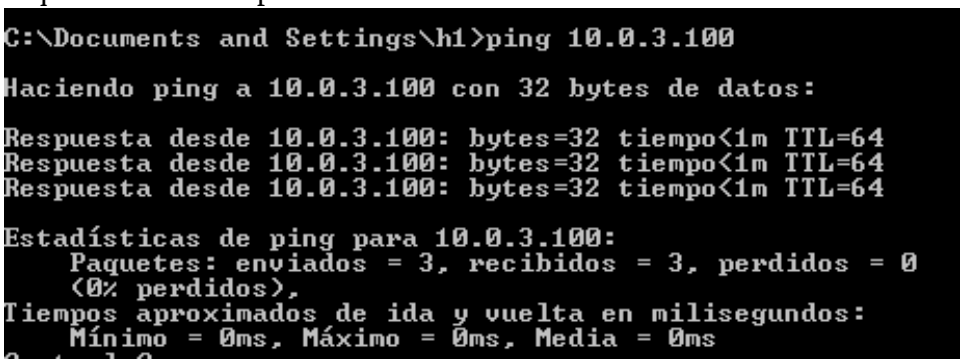
Maquinas instaladas

Lo primero que voy a hacer, ya he puesto a todos en la red que les corresponde y voy a ver si se conectan correctamente.

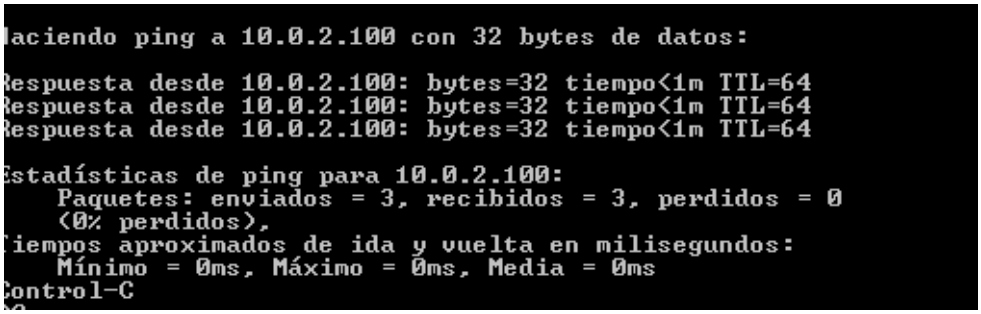
Ping de la maquina wifi al ruter



Ping de la maquina servidor http al ruter



Ping de h2 a ruter

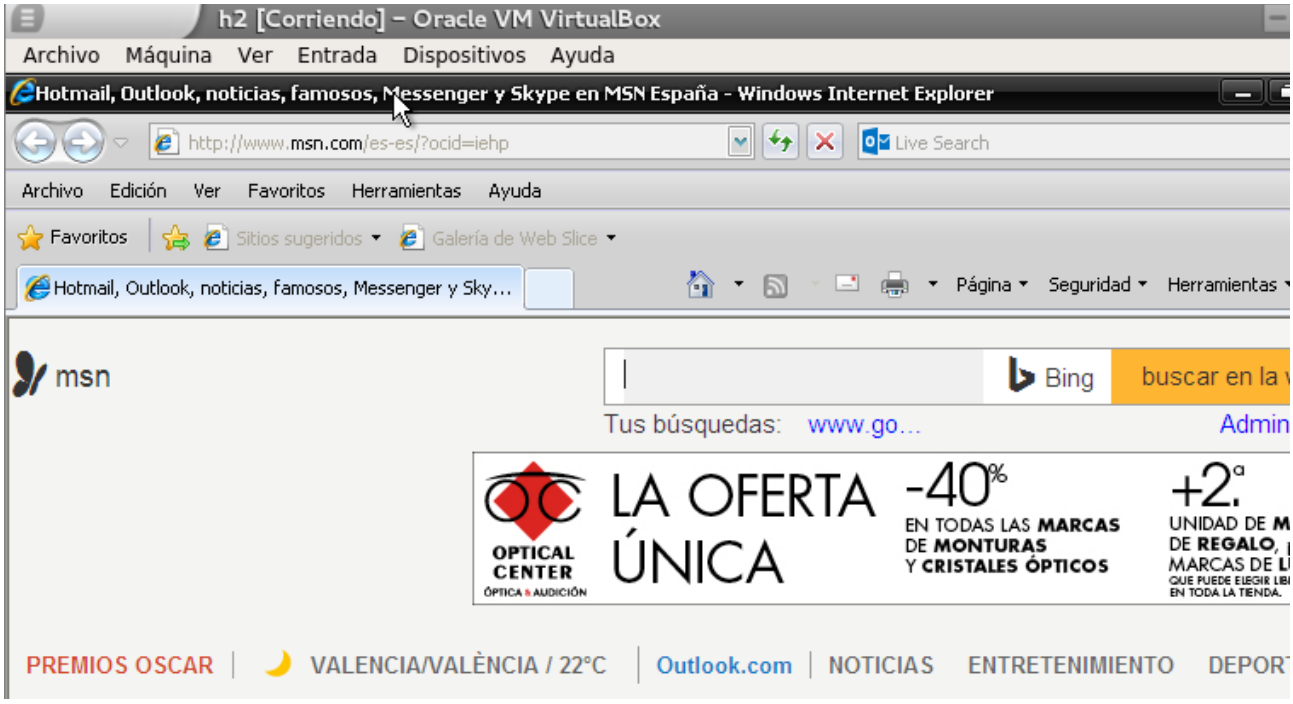


Una vez que todo conecta correctamente ahora tenemos que ver como conseguir acceso a internet

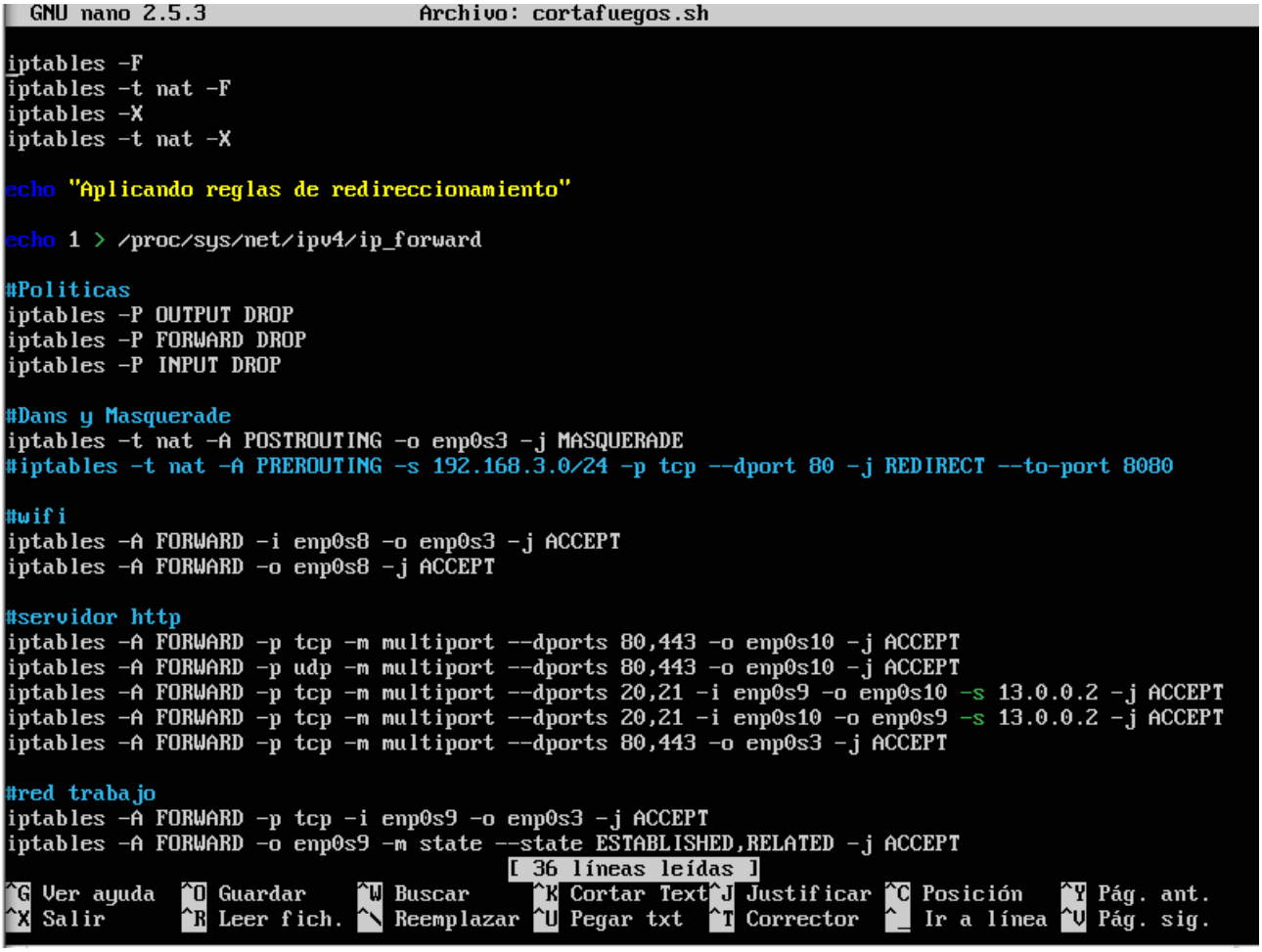
Crearemos un fichero para configurar las iptables de golpe así nos va a ser mucho mas comodo. Y lo ejecutamos con: **bash nuestro_script**

```
iptables -F
iptables -t nat -F
iptables -X
iptables -t nat -X

echo "Aplicando reglas de redireccionamiento"

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

#Politicas
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P INPUT ACCEPT

#Dans y Masquerade
iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
```

Prueba de que va:

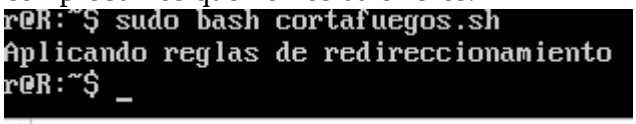


Ahora que hemos comprobado que funciona internet lo que vamos a hacer es proteger nuestras red privada y nuestro servidor http. He creado las siguientes reglas:



Su continuación:

Lo ejecutamos con bash y comprobamos que no nos da errores.



Aqui instalando apache en la maquina del servidor nos hemos dado cuenta de que no se puede instalar porque es una maquina xp, he creado un linux con la misma configuración.

Y aquí la comprobacion desde la maquina del ADM que va apache2.