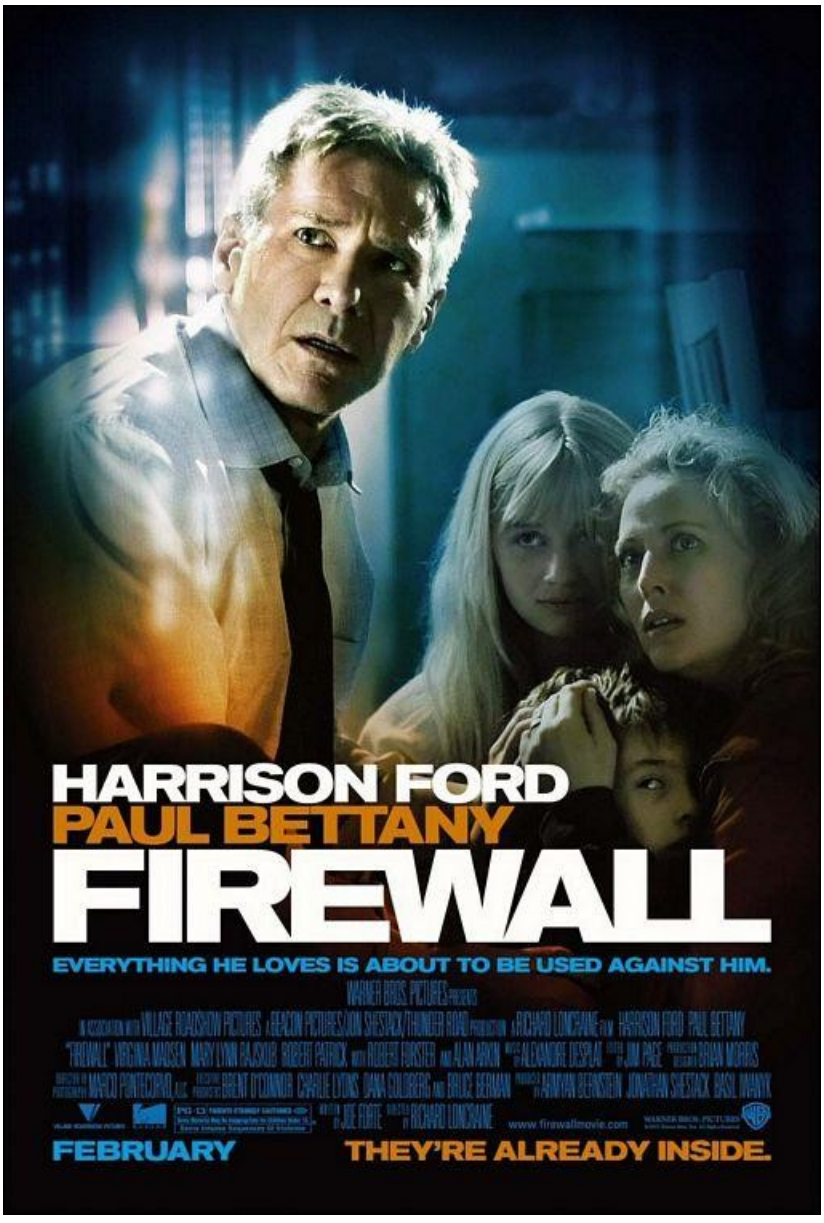
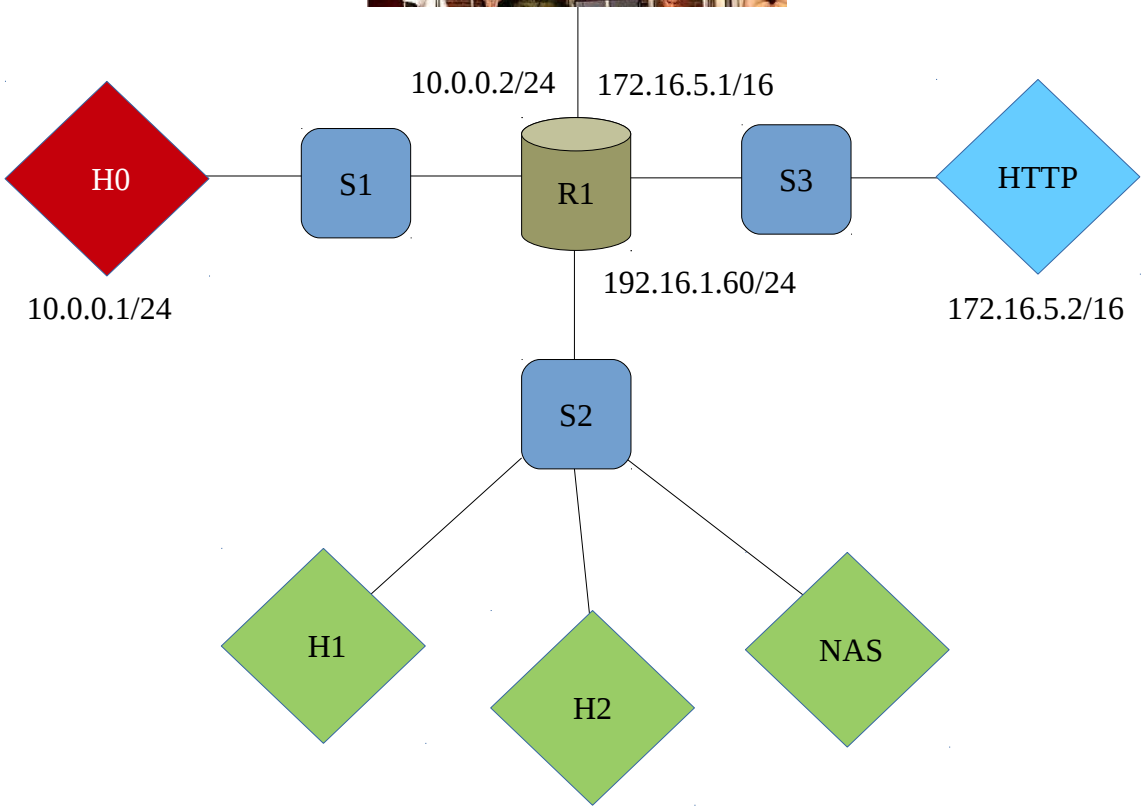
Práctica Firewall

Alejandro Abad



INTERNET

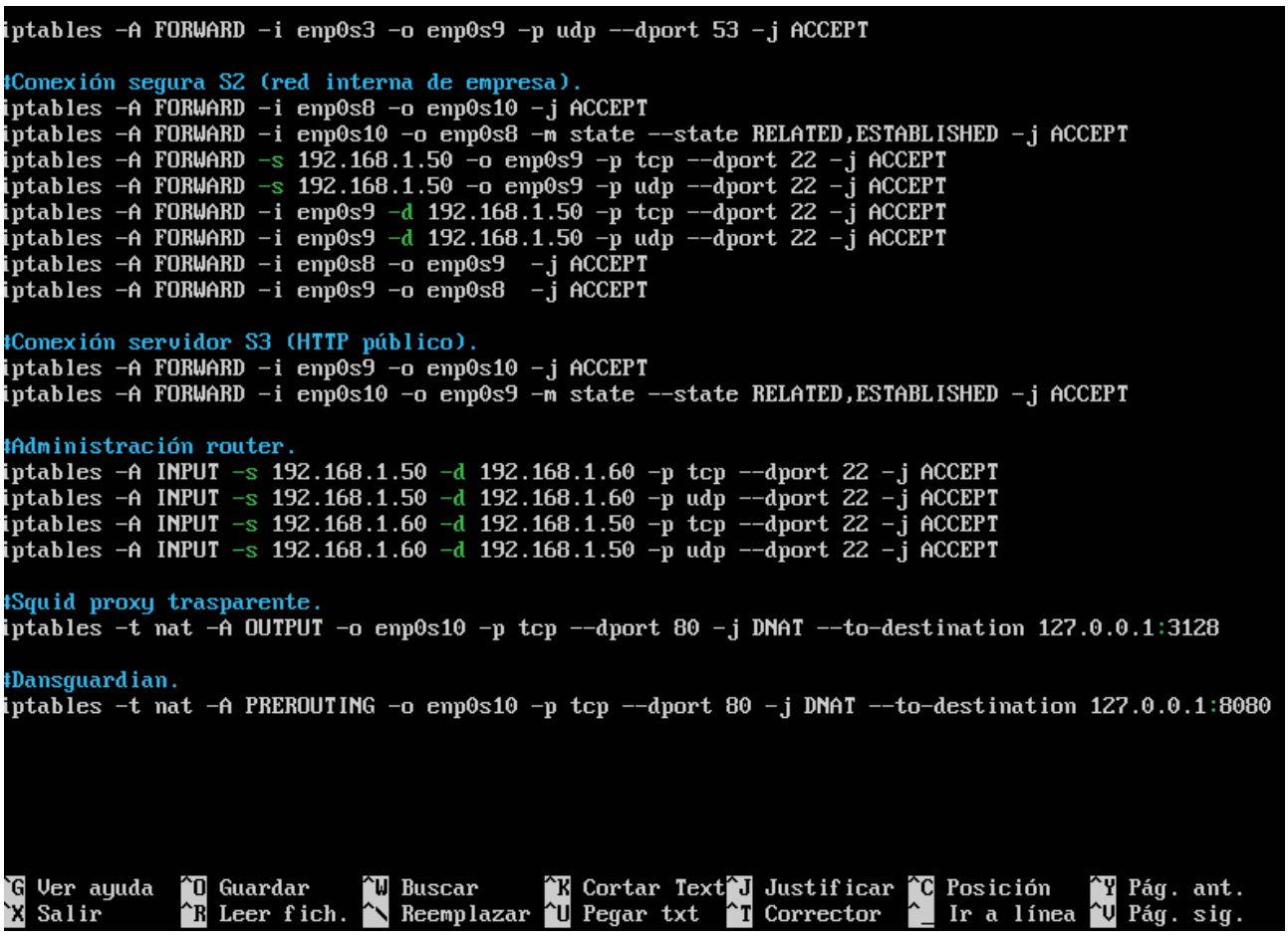


Esquema de las conexiones

En primer lugar he creado los equipos y asignado las ips como indica el gráfico de la página anterior. He comprobado que se hacen ping entre ellos. En H0 bajo el switch S1 tenemos la red roja, una red wi-fi no segura. En H1, H2 y NAS bajo el switch 2 tenemos la red verde, la red interna de la empresa segura. En HTTP bajo el switch 3 tenemos la red azul, una red web pública.

Lo más importante ha sido la correcta configuración de las tablas IP para que los ordenadores puedan navegar por internet con las restricciones necesarias.

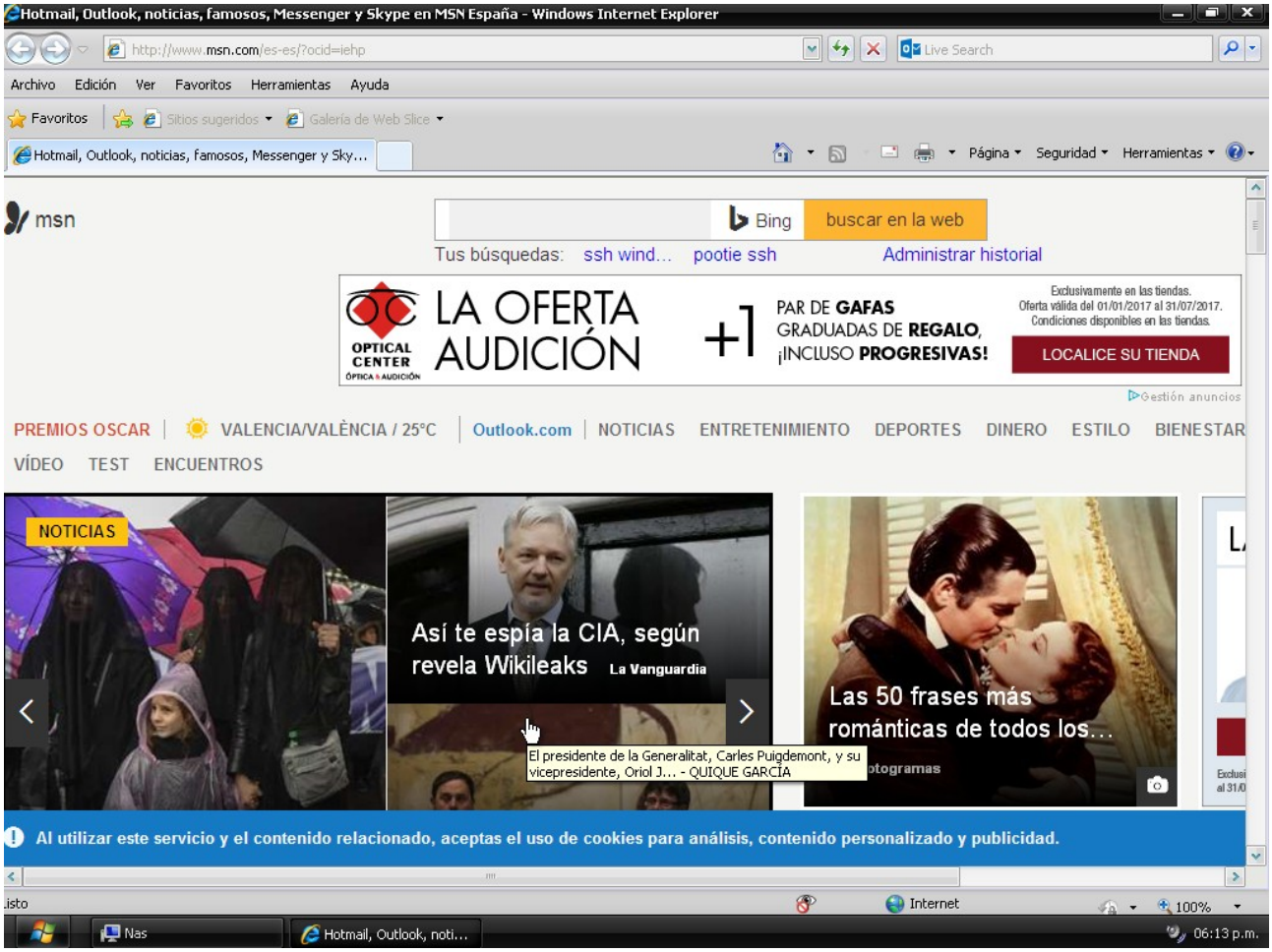
```
  GNU nano 2.5.3                  Archivo: iptables.sh

#!/bin/bash
_

iptables -F
iptables -X
iptables -t nat -F
iptables -P INPUT DROP
iptables -P FORWARD DROP

#Internet a secas.
iptables -t nat -A POSTROUTING -o enp0s10 -j MASQUERADE

#Internet de S1 (red Wi-Fi).
iptables -A FORWARD -i enp0s3 -o enp0s10 -j ACCEPT
iptables -A FORWARD -o enp0s3 -j ACCEPT

#Conexiones públicas de S3 (servidor HTTP).
iptables -A FORWARD -i enp0s9 -o enp0s10 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s10 -p udp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s10 -p tcp --dport 443 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s10 -p udp --dport 443 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s10 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s10 -p udp --dport 53 -j ACCEPT
iptables -A FORWARD -i enp0s10 -o enp0s9 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s10 -o enp0s9 -p udp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s10 -o enp0s9 -p tcp --dport 443 -j ACCEPT
iptables -A FORWARD -i enp0s10 -o enp0s9 -p udp --dport 443 -j ACCEPT
iptables -A FORWARD -i enp0s10 -o enp0s9 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -i enp0s10 -o enp0s9 -p udp --dport 53 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s9 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s9 -p udp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s9 -p tcp --dport 443 -j ACCEPT

^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.
```



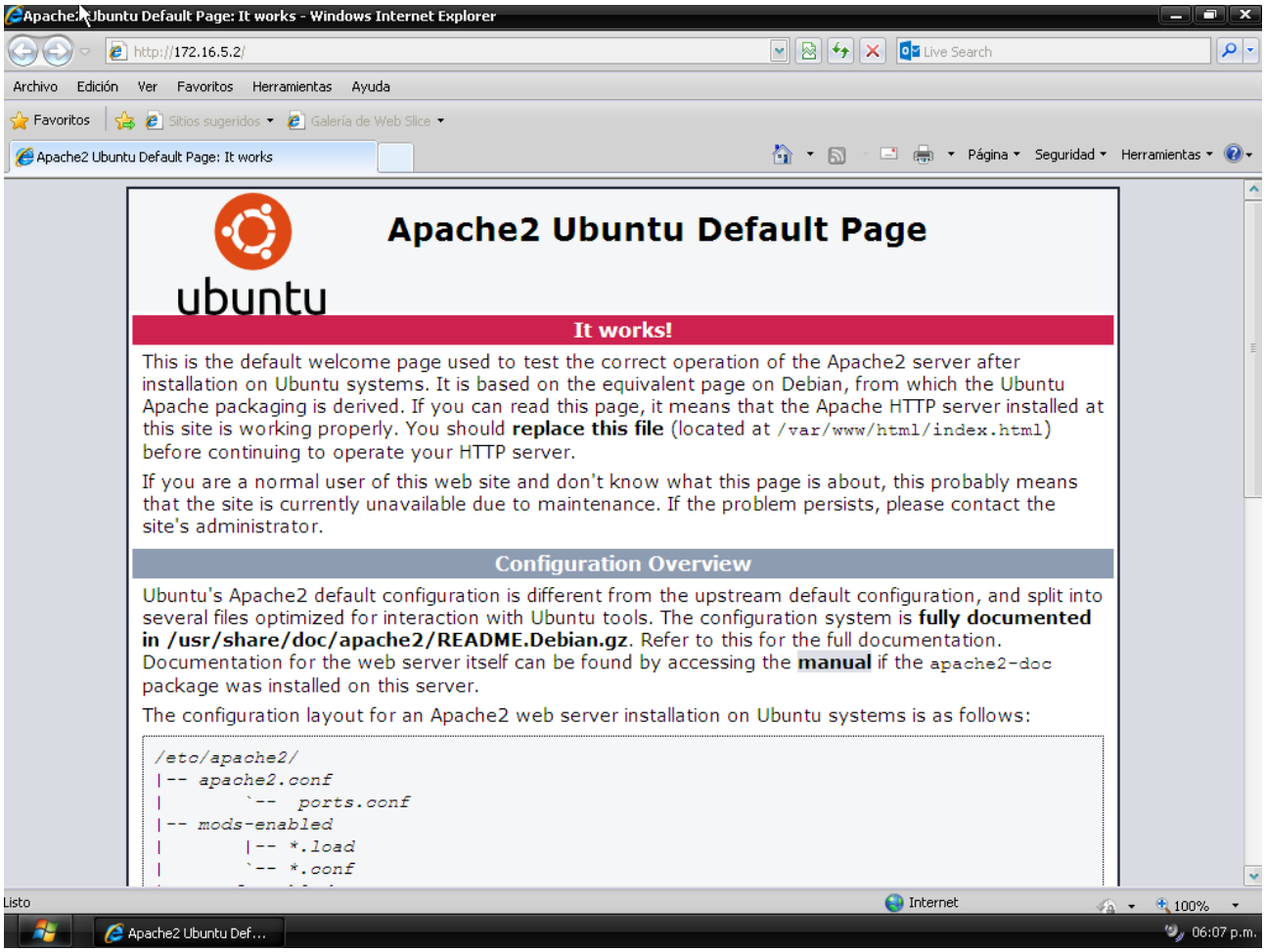
Las normas de estas iptables son:

- Poner que la política por defecto sea DROP.
- Que el router enmascare los paquetes para que se pueda navegar por internet.
- La red S1 no es segura, así que permitimos todo el tráfico de entrada y salida.
- El servidor HTTP está configurado para permitir la entrada desde el exterior u las otras redes además de responder.
- La red S2 es segura, así que permitimos todo el tráfico saliente pero el entrante solo se permite si es una respuesta a una petición previamente realizada.
- Tenemos líneas para permitir la administración del router mediante ssh desde el ordenador H1 (ordenador de administrador).
- Líneas para que funcione bien el proxy y el dansguardian.

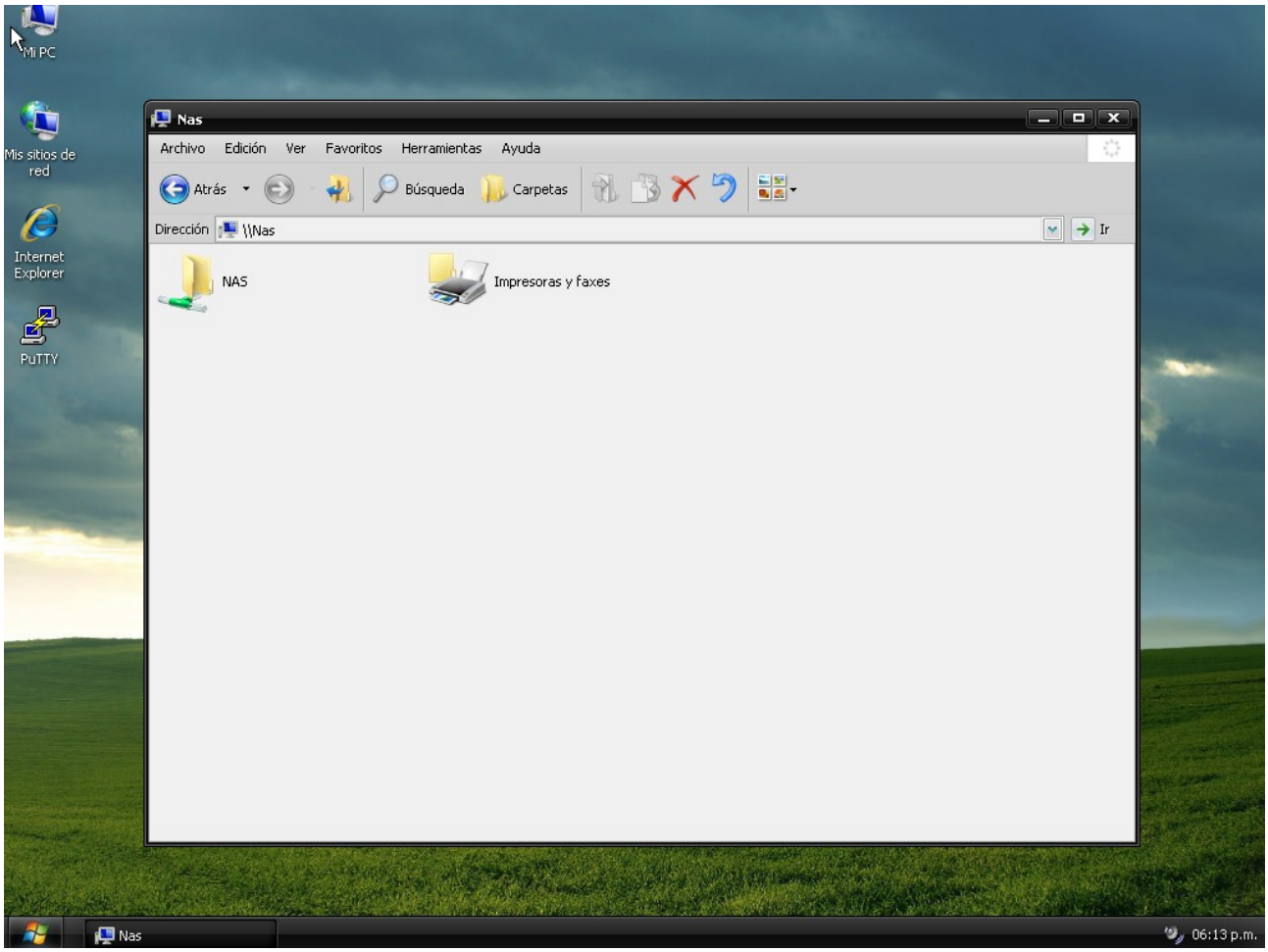
Comprobamos que funciona internet en todos los ordenadores de la red:



Comprobamos que se puede acceder a la página web del servidor HTTP:



Comprobamos que el NAS funciona:



Comprobamos que se puede acceder a través del equipo administrador a las máquinas a administrar: