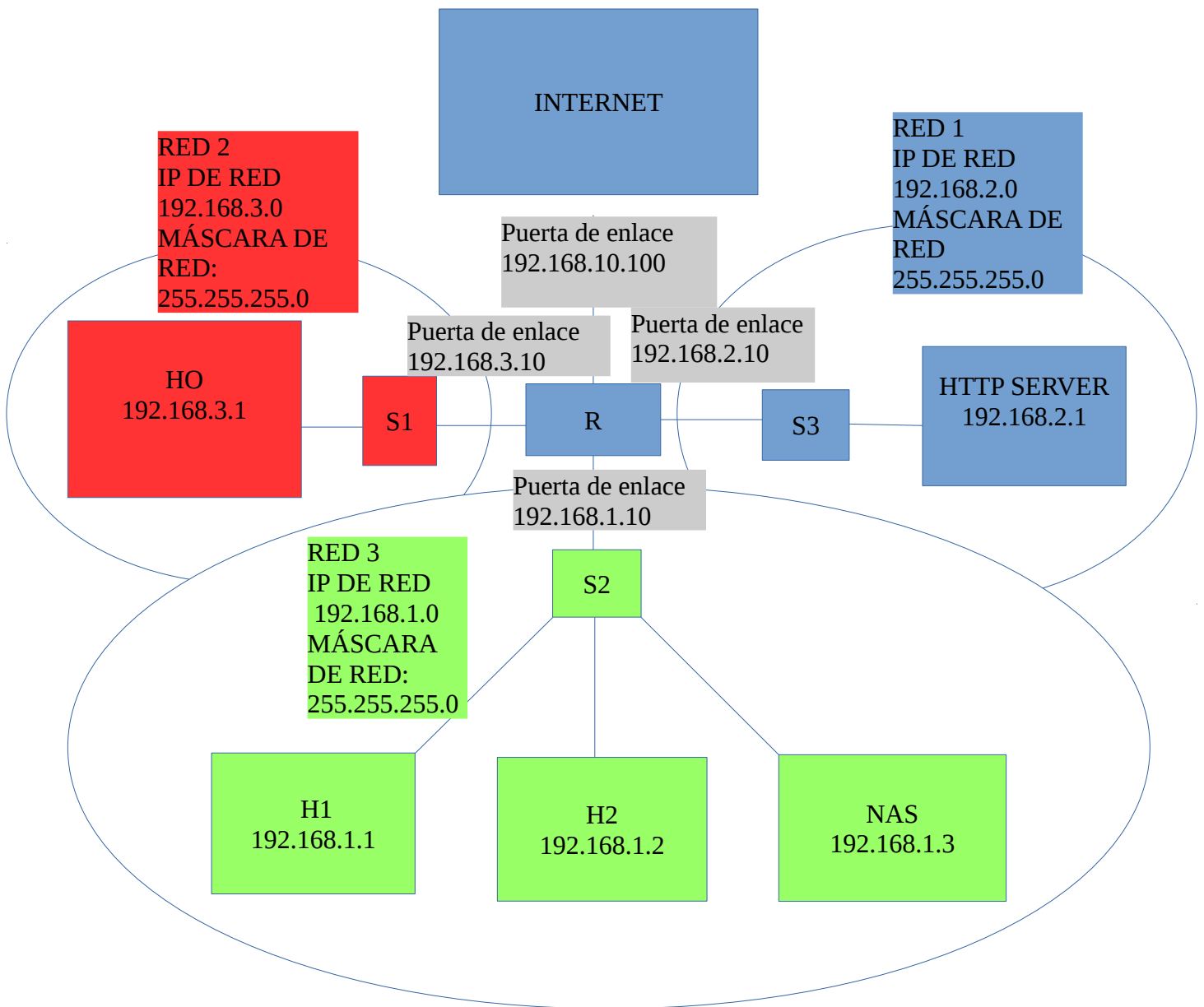


PRACTICA DE FIREWALL



DIAGRAMA DE RED



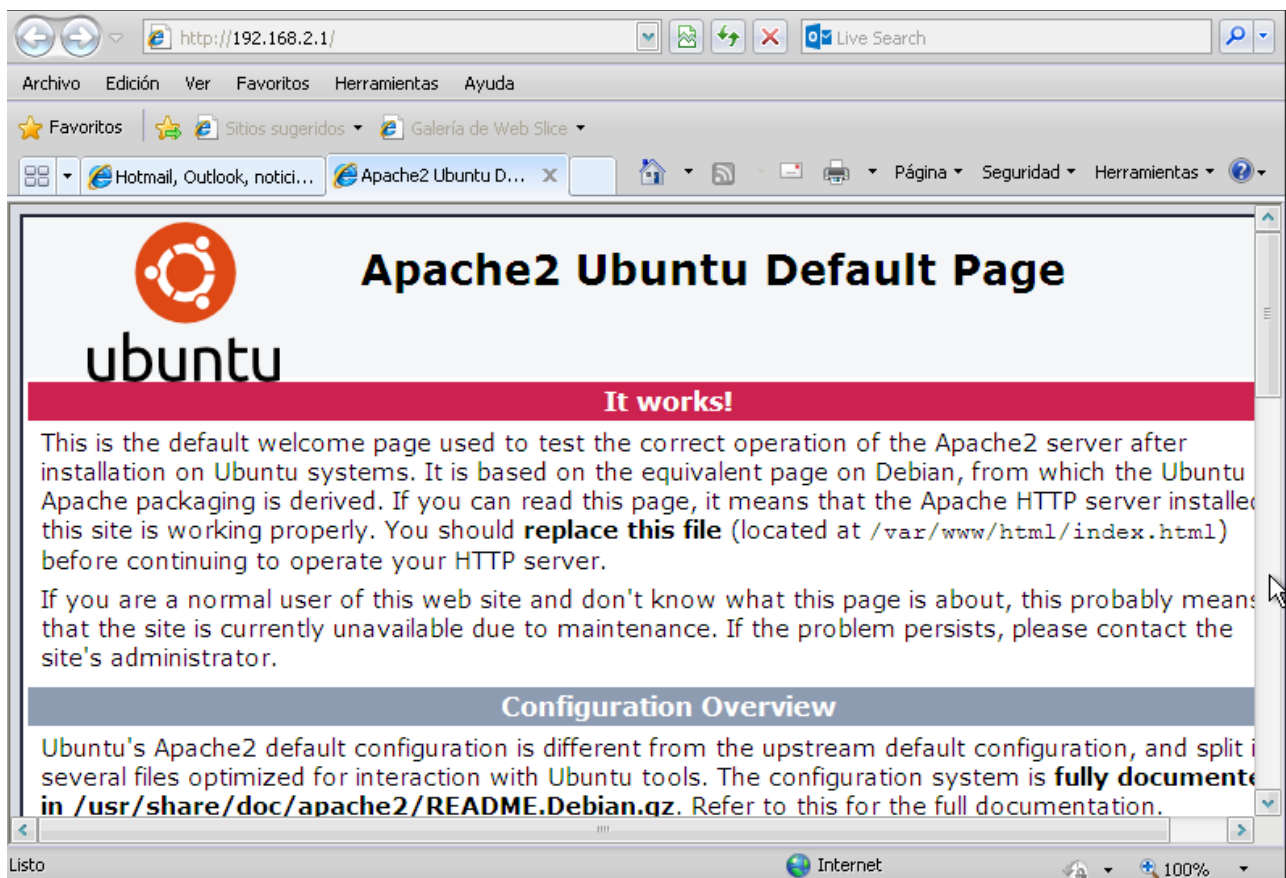
Instalación de Apache en HTTPSERVER

IP DE HTTPSERVER

```
http@httpserver:~$ ifconfig
enp0s3  Link encap:Ethernet  direcciónHW 08:00:27:3a:78:6b
        Direc. inet:192.168.2.1  Difus.:192.168.2.255  Másc:255.255.255.0
        Dirección inet6: fe80::a00:27ff:fe3a:786b/64 Alcance:Enlace
        ACTIVO DIFUSION FUNCIONANDO MULTICAST MTU:1500 Métrica:1
        Paquetes RX:3690 errores:0 perdidos:0 overruns:0 frame:0
        Paquetes TX:2751 errores:0 perdidos:0 overruns:0 carrier:0
        colisiones:0 long.colatX:1000
        Bytes RX:5043815 (5.0 MB)  TX bytes:212014 (212.0 KB)

lo      Link encap:Bucle local
        Direc. inet:127.0.0.1  Másc:255.0.0.0
        Dirección inet6: ::1/128 Alcance:Anfitrión
        ACTIVO BUCLE FUNCIONANDO MTU:65536 Métrica:1
        Paquetes RX:349 errores:0 perdidos:0 overruns:0 frame:0
        Paquetes TX:349 errores:0 perdidos:0 overruns:0 carrier:0
        colisiones:0 long.colatX:1
        Bytes RX:29614 (29.6 KB)  TX bytes:29614 (29.6 KB)
```

```
http@httpserver:~$ sudo apt-get install apache2_
```



NAS

```
Símbolo del sistema
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\admin>ipconfig

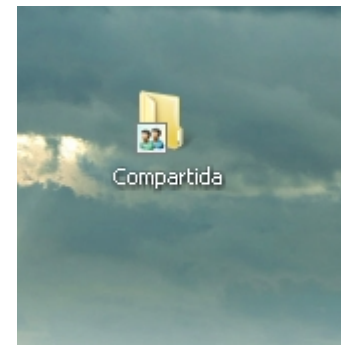
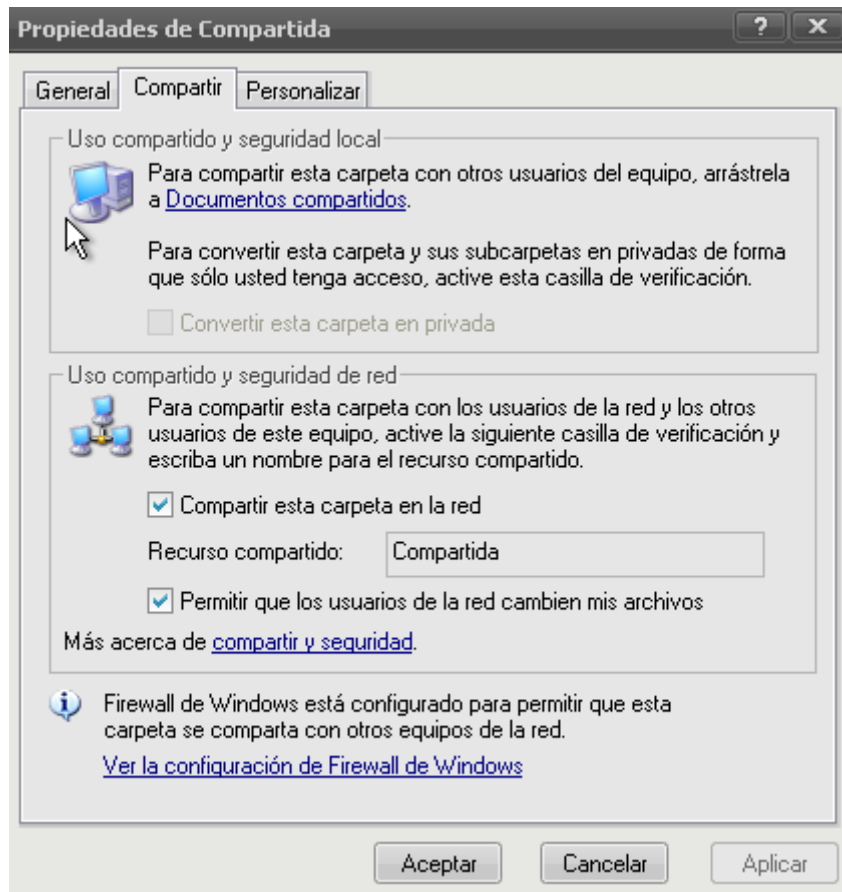
Configuración IP de Windows

Adaptador Ethernet Conexión de área local :

    Sufixo de conexión específica DNS :
    Dirección IP. . . . . : 192.168.1.3
    Máscara de subred : 255.255.255.0
    Puerta de enlace predeterminada : 192.168.1.10

C:\Documents and Settings\admin>
```

Carpeta compartida de NAS



Script

```
#!/bin/bash

echo 1 > /proc/sys/net/ipv4/ip_forward
#REINICIAR
iptables -F
iptables -X
iptables -Z

iptables -t mangle -F
iptables -t mangle -X
iptables -t mangle -Z
```

```
#POLITICAS
iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP
```

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

```
#RED 2 A INTERNET
iptables -A FORWARD -i enp0s8 -o enp0s10 -j ACCEPT
iptables -A FORWARD -o enp0s8 -j ACCEPT
```

```
#RED 2 A RED1
iptables -A FORWARD -i enp0s8 -o enp0s3 -p tcp --dport 80 -j ACCEPT
```

```
#Administrador H1 A HTTPSERVER
```

```
iptables -A FORWARD -s 192.168.1.1 -o enp0s3 -p tcp --dport 20 -j ACCEPT  
iptables -A FORWARD -s 192.168.1.1 -o enp0s3 -p tcp --dport 21 -j ACCEPT  
iptables -A FORWARD -s 192.168.1.1 -o enp0s3 -p tcp --dport 22 -j ACCEPT
```

```
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -i enp0s3 -s 192.168.1.1 -j ACCEPT
```

```
#RED 3 A RED1
```

```
iptables -A FORWARD -i enp0s9 -o enp0s3 -p tcp --dport 80 -j ACCEPT  
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -i enp0s3 -o enp0s9 -j ACCEPT
```

```
#HTTPSERVER A INTERNET (IDA Y VUELTA)
```

```
iptables -A FORWARD -i enp0s3 -o enp0s10 -j ACCEPT  
iptables -A FORWARD -i enp0s10 -o enp0s3 -p tcp --dport 80 -j ACCEPT  
iptables -A FORWARD -i enp0s10 -o enp0s3 -p udp --dport 80 -j ACCEPT
```

```
#Administrador h1 de la RED3 del router
```

```
iptables -A INPUT -s 192.168.1.2 -p tcp --dport 22 -j ACCEPT  
iptables -A INPUT -s 192.168.1.2 -p udp --dport 22 -j ACCEPT  
iptables -A OUTPUT -s 192.168.1.2 -j ACCEPT
```

```
#RED 3 A INTERNET
```

```
iptables -A FORWARD -i enp0s9 -o enp0s10 -j ACCEPT  
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -o enp0s9 -j ACCEPT
```

```
#SQUID transparente
```

```
iptables -t nat -A PREROUTING -i enp0s8 -p tcp --dport 80 -j REDIRECT --to-port 3128
```

Squid

Configuración del squid

```
# Squid normally listens to port 3128
http_port 3128 transparent

acl redroja src 192.168.3.0/24
acl redverde src 192.168.2.0/24
acl redazul src 192.168.1.0/24
acl banurl dstdomain /etc/squid/banurl.txt

http_access deny banurl

http_access allow redroja
http_access allow redverde
http_access allow redazul
```

DansGuardian

Configuración de DansGuardian

```
# Network Settings
#
# the IP that DansGuardian listens on.  If left blank DansGuardian will
# listen on all IPs.  That would include all NICs, loopback, modem, et
# Normally you would have your firewall protecting this, but if you wa
# you can limit it to a certain IP. To bind to multiple interfaces,
# specify each IP on an individual filterip line.
filterip =127.0.0.1

# the port that DansGuardian listens to.
filterport = 8080

# the ip of the proxy (default is the loopback - i.e. this server)
proxyip = 127.0.0.1

# the port DansGuardian connects to proxy on
proxyport = 3128
```

```
reportinglevel = 0

# Language dir where languages are stored for internationalisation.
# The HTML template_within this dir is only used when reportinglevel
# is set to 3. When used, DansGuardian will display the HTML file instead of
# using the perl cgi script. This option is faster, cleaner
# and easier to customise the access denied page.
# The language file is used no matter what setting however.
#
language = 'spanish'
```