



# Práctica 1 – Configuración de servicios de red (0.75 puntos)

## 1.1 Realización práctica por los alumnos del grupo FR2(turno 1):

David Suarez González

Daniel Monjas Miguélez

- 1 Compruebe las direcciones IP que tienen asignadas las diferentes interfaces de red de su equipo mediante el comando *ifconfig*, ¿cómo se llaman dichas interfaces? ¿qué direcciones de red tienen definidas?

Nombre Interfaz	PC_1	PC_2	PC_3
<b>enp0s3</b>	10.0.2.15	10.0.2.15	10.0.2.15
<b>enp0s9</b>	33.1.1.2	33.1.1.3	33.1.2.2
<b>enp0s10</b>	192.168.1.1	192.168.1.2	192.168.1.3

(En la terminal de PC\_1-Ubuntu20.04)

```
administrador@pc1:~$ ifconfig
```

```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
```

```
inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
```

```
inet6 fe80::3d00:5458:c3ab:e588 prefixlen 64 scopeid 0x20<link>
```

```
ether 08:00:27:fd:98:cc txqueuelen 1000 (Ethernet)
```

```
RX packets 31451 bytes 44402901 (44.4 MB)
```

```
RX errors 0 dropped 0 overruns 0 frame 0
```

```
TX packets 2613 bytes 210564 (210.5 KB)
```

```
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
enp0s9: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
```

```
inet 33.1.1.2 netmask 255.255.255.0 broadcast 33.1.1.255
```

```
inet6 fe80::a00:27ff:fe4d:8a84 prefixlen 64 scopeid 0x20<link>
```

```
ether 08:00:27:4d:8a:84 txqueuelen 1000 (Ethernet)
```

```
RX packets 0 bytes 0 (0.0 B)
```

```
RX errors 0 dropped 0 overruns 0 frame 0
```

```
TX packets 76 bytes 8101 (8.1 KB)
```

```
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

```
enp0s10: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.1 netmask 255.255.0.0 broadcast 192.168.255.255
    inet6 fe80::a00:27ff:fe21:6685 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:21:66:85 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 77 bytes 8182 (8.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Bucle local)
    RX packets 268 bytes 23507 (23.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 268 bytes 23507 (23.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Al usar el comando `ifconfig` accedemos a la configuración de interfaces de red del equipo. Cuando lo ejecutamos sin argumentos simplemente muestra las interfaces activas, que son las siguientes:

- ➔ `enp0s3`: Tiene dirección de red IP 10.0.2.15 y es la interfaz de red NAT (Acceso a internet).
- ➔ `enp0s9`: Tiene dirección de red IP 33.1.1.2 y es la interfaz de red Datos.
- ➔ `enp0s10`: Tiene dirección de red IP 192.168.1.1 y es la interfaz de red de Gestión.
- ➔ `lo`: Tiene dirección de red IP 127.0.0.1 y es la interfaz de red `lo` (Loop Back)

- 2 Compruebe que existe conectividad con otro equipo del laboratorio, mediante la utilidad `ping`. ¿Es posible hacer ping desde el PC\_1 al PC\_3 por la red 33.1.1.0/24? ¿Y por la red 192.168.1.0/16? Justifique su respuesta. A partir de ahora la primera de las redes la llamaremos de *datos* mientras que la segunda será la de *gestión*.

```
administrador@pc1: ~
administrador@pc1:~$ ping 33.1.2.2
PING 33.1.2.2 (33.1.2.2) 56(84) bytes of data.
^C
--- 33.1.2.2 ping statistics ---
21 packets transmitted, 0 received, 100% packet loss, time 20468ms

administrador@pc1:~$
```

```
administrador@pc1:~$ traceroute 33.1.2.2
traceroute to 33.1.2.2 (33.1.2.2), 30 hops max, 60 byte packets
 1 _gateway (10.0.2.2) 0.214 ms 0.167 ms 0.147 ms
 2 192.168.0.1 (192.168.0.1) 3.375 ms 3.346 ms 3.150 ms
 3 10.195.52.1 (10.195.52.1) 24.178 ms 24.168 ms 23.934 ms
 4 10.80.4.125 (10.80.4.125) 19.884 ms 19.835 ms 19.742 ms
```



Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

```
5 * * *
6 * * *
7 * * *
```

```
-----
30 * * *
```

Como se puede ver no hay conexión entre PC1 y PC3 por la red 33.1.1.0/24. Todos los paquetes que se transmiten se pierden. No podemos alcanzar dicha IP, pues en el encaminamiento que siguen los paquetes a través de los routers, llega un momento en que se detienen en un router específico, que podemos averiguar con “tracert”, (en este caso, el router con dirección IP 10.80.4.125 ):

```
administrador@pc1: ~
administrador@pc1:~$ ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
64 bytes from 192.168.1.3: icmp_seq=1 ttl=64 time=1.45 ms
64 bytes from 192.168.1.3: icmp_seq=2 ttl=64 time=0.830 ms
64 bytes from 192.168.1.3: icmp_seq=3 ttl=64 time=1.05 ms
64 bytes from 192.168.1.3: icmp_seq=4 ttl=64 time=0.841 ms
^C
--- 192.168.1.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3031ms
rtt min/avg/max/mdev = 0.830/1.044/1.453/0.252 ms
administrador@pc1:~$
```

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000086513	192.168.1.3	192.168.1.1	ICMP	98	Echo (ping) reply id=0x0005, seq=1
3	1.000781879	192.168.1.1	192.168.1.3	ICMP	98	Echo (ping) request id=0x0005, seq=2
4	1.000859075	192.168.1.3	192.168.1.1	ICMP	98	Echo (ping) reply id=0x0005, seq=2
5	2.002356782	192.168.1.1	192.168.1.3	ICMP	98	Echo (ping) request id=0x0005, seq=3
6	2.002426025	192.168.1.3	192.168.1.1	ICMP	98	Echo (ping) reply id=0x0005, seq=3
7	3.003251259	192.168.1.1	192.168.1.3	ICMP	98	Echo (ping) request id=0x0005, seq=4
8	3.003324529	192.168.1.3	192.168.1.1	ICMP	98	Echo (ping) reply id=0x0005, seq=4
9	4.004599826	192.168.1.1	192.168.1.3	ICMP	98	Echo (ping) request id=0x0005, seq=5
10	4.004679298	192.168.1.3	192.168.1.1	ICMP	98	Echo (ping) reply id=0x0005, seq=5
11	5.052960576	PcsCompu_57:b4:82	PcsCompu_10:27:2c	ARP	42	Who has 192.168.1.1? Tell 192.168.1.3
12	5.053739432	PcsCompu_10:27:2c	PcsCompu_57:b4:82	ARP	60	192.168.1.1 is at 08:00:27:10:27:2c
13	224561864	PcsCompu_10:27:2c	PcsCompu_57:b4:82	ARP	60	Who has 192.168.1.3? Tell 192.168.1.1
14	224593716	PcsCompu_57:b4:82	PcsCompu_10:27:2c	ARP	42	192.168.1.3 is at 08:00:27:57:b4:82
15	7.792080386	192.168.1.2	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _ipps._tcp.
16	9.478294122	fe80::a00:27ff:fe4d...	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.
17	18.792744385	fe80::a00:27ff:fe10...	ff02::2	ICMPv6	70	Router Solicitation from 08:00:27:10:

Los paquetes transmitidos por ping son recibidos como muestra la primera captura. Además la segunda captura muestra con wireshark como los recibe PC3.

- 3 Cree una cuenta de usuario en su equipo, habilite el servicio *telnet* y compruebe con algún compañero que dicho servicio es accesible.



Usaré la cuenta administrador que ya existe en los entornos virtuales, e intentaré conectar dos de estos entornos mediante telnet.

```
administrador@pc1: /etc/xinetd.d
administrador@pc1:/etc/xinetd.d$ cat telnet
service telnet
{
    disable           = no
    flags              = REUSE
    socket_type        = stream
    wait               = no
    user               = root
    server              = /usr/sbin/in.telnetd
    log_on_failure     += HOST
}
administrador@pc1:/etc/xinetd.d$
```

La opción disable = no implica que el servicio está habilitado y funciona. Ahora para comprobar que el servicio funciona se accede desde PC3 a PC1. Para que el cambio en el archivo de configuración sea efectivo se ha de realizar la orden “service xinetd restart”. Comprobamos que ahora el servicio telnet está activo y en escucha en el PC\_1 (como servidor):

```
root@pc1:/home/administrador# service xinetd restart
```

```
root@pc1:/home/administrador# netstat -ltp
```

Conexiones activas de Internet (solo servidores)

Proto	Recib	Enviad	Dirección local	Dirección remota	Estado	PID/Program name
tcp	0	0	localhost:domain	0.0.0.0:*	ESCUCHAR	557/systemd-resolve
tcp	0	0	0.0.0.0:ssh	0.0.0.0:*	ESCUCHAR	732/sshd: /usr/sbin
tcp	0	0	pc1:ipp	0.0.0.0:*	ESCUCHAR	589/cupsd
tcp6	0	0	:::http	:::*	ESCUCHAR	774/apache2
tcp6	0	0	:::ftp	:::*	ESCUCHAR	715/vsftpd
tcp6	0	0	:::ssh	:::*	ESCUCHAR	732/sshd: /usr/sbin
tcp6	0	0	:::telnet	:::*	ESCUCHAR	17158/xinetd
tcp6	0	0	ip6-localhost:ipp	:::*	ESCUCHAR	589/cupsd



Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

```
PC_3-Ubuntu20.04 [Running] - Oracle VM VirtualBox
File View Input Devices Help
Terminal 29 de oct 23:20
administrador@pc1: ~
administrador@pc3:~$ telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
pc1 login: administrador
Password:
Login incorrect
pc1 login: administrador
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-48-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

184 actualizaciones se pueden instalar inmediatamente.
86 de estas actualizaciones son una actualización de seguridad.
Para ver estas actualizaciones adicionales ejecute: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Fri Oct 23 00:57:50 CEST 2020 from 192.168.1.3 on pts/1
administrador@pc1:~$
```

Como se puede ver el servicio funciona correctamente (además se observa que se hizo un login incorrecto, ya que me equivoqué al poner la contraseña). También cree un directorio (mkdir prueba) y un archivo (archivo\_prueba.txt).

```
administrador@pc1:~$ mkdir prueba
administrador@pc1:~$ cd prueba/
administrador@pc1:~/prueba$ touch archivo_prueba.txt
administrador@pc1:~/prueba$ ls
archivo_prueba.txt
```

Y al comprobarlo en PC\_1 vemos que si que está el archivo y el directorios creados.

- 4 Configure el servicio telnet para que:
  - 4.a Sólo sea accesible desde la dirección IP de su compañero.

Este es el archivo de configuración de telnet, donde la opción `only_from = <dir_ip>` indica la dirección ip de los host remotos para los que el servicio estará disponible.



Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

```
administrador@pc1: /etc/xinetd.d
administrador@pc1:/etc/xinetd.d$ cat telnet
service telnet
{
    disable            = no
    flags              = REUSE
    socket_type        = stream
    wait              = no
    user               = root
    server             = /usr/sbin/in.telnetd
    log_on_failure     += HOST
    only_from         = 192.168.1.3
}
administrador@pc1:/etc/xinetd.d$
```

```
PC_3-Ubuntu20.04 [Running] - Oracle VM VirtualBox
ne View Input Devices Help
des Terminal 29 de oct 23:24
administrador@pc1: ~
administrador@pc3:~$ telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
pc1 login: administrador
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-48-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

184 actualizaciones se pueden instalar inmediatamente.
86 de estas actualizaciones son una actualización de seguridad.
Para ver estas actualizaciones adicionales ejecute: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Thu Oct 29 23:19:56 CET 2020 from 192.168.1.3 on pts/1
administrador@pc1:~$
```



Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

```
PC_2-Ubuntu20.04 [Running] - Oracle VM VirtualBox
Machine View Input Devices Help
es Terminal 29 de oct 23:25
administrador@pc2: ~
administrador@pc2:~$ telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
Connection closed by foreign host.
administrador@pc2:~$
```

Como se puede observar en la primera captura PC3 si puede acceder a PC1 por medio del servicio telnet. Sin embargo, PC2 no puede acceder a PC1 por medio de telnet pues su dirección IP no concuerda con la del archivo de configuración del servicio telnet de PC1.

- 1.b Se registren en el fichero `/var/log/telnet.log` los intentos de acceso con y sin éxito al servicio telnet, indicando la dirección IP del equipo que intenta el acceso.

En primer lugar añadimos la opción `log_on_success += HOST`, para que en caso de un login exitoso se guarde la dirección IP de quien la ha realizado. La opción `log_on_failure += HOST` no es necesaria añadirla pues ya estaba en el archivo de configuración. Finalmente la opción `log_type = FILE "/var/log/telnet.log"` hace que la información obtenida de un login se mande al archivo `/var/log/telnet` y en caso de que este archivo no exista se crea.

```
administrador@pc1: /etc/xinetd.d
administrador@pc1:/etc/xinetd.d$ cat telnet
service telnet
{
    disable          = no
    flags            = REUSE
    socket_type      = stream
    wait            = no
    user            = root
    server          = /usr/sbin/in.telnetd
    log_type        = FILE /var/log/telnet.log
    log_on_failure  += HOST
    log_on_success  += HOST
    only_from       = 192.168.1.3
}
```

Ahora mostramos la información que se almacena en el archivo `/var/log/telnet` tras un login exitoso y uno rechazado, pues la dirección IP no coincide con la que el archivo de configuración de telnet permite.



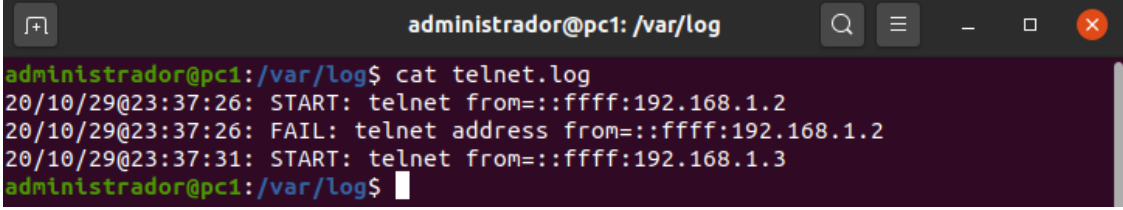
Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones



```
administrador@pc1: /var/log
administrador@pc1:/var/log$ cat telnet.log
20/10/29@23:37:26: START: telnet from=::ffff:192.168.1.2
20/10/29@23:37:26: FAIL: telnet address from=::ffff:192.168.1.2
20/10/29@23:37:31: START: telnet from=::ffff:192.168.1.3
administrador@pc1:/var/log$
```

Como se puede ver en el archivo se ha almacenado un intento fallido de conectar por medio del servicio telnet a PC1 desde PC2, y un intento exitoso de hacer login por medio de telnet desde PC3 a PC1.

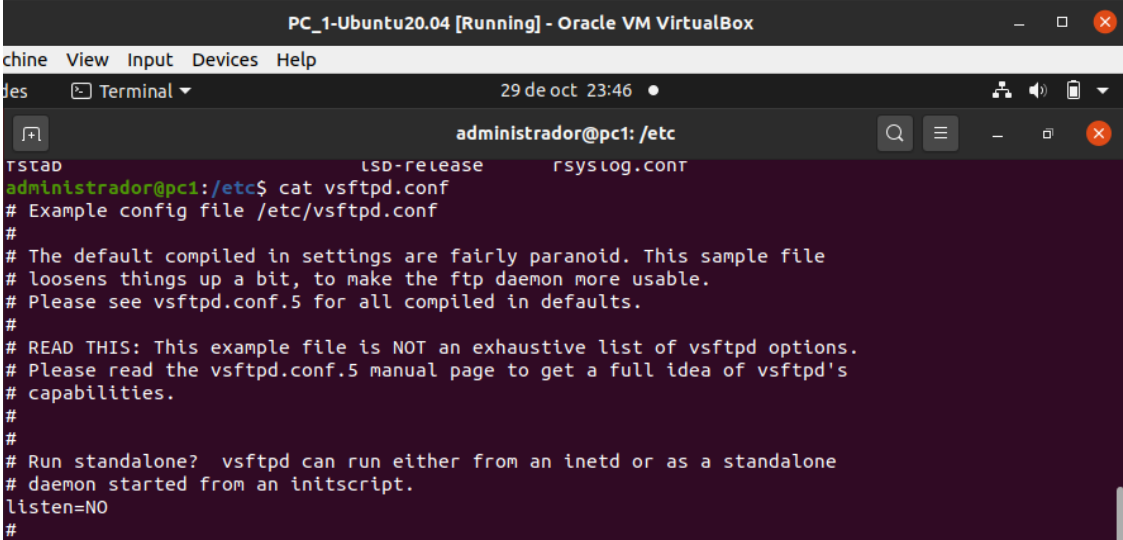
5 Habilite el servicio *ftp* en su equipo (de la “a” a la “c”).

Para habilitar el servicio ftp utilizo el comando “service vsftpd start”.

a) Para ello en el archivo de configuración del servicio vsftpd, es decir, en el archivo vsftpd.conf incluimos la siguiente línea.

listen = no

Esta opción se encarga de que vsftpd **no** funcione en modo standalone. Si la opción estuviese a yes si lo haría.



```
PC_1-Ubuntu20.04 [Running] - Oracle VM VirtualBox
chinese View Input Devices Help
des Terminal 29 de oct 23:46
administrador@pc1: /etc
rstad lsdp-release rsyslog.conf
administrador@pc1:/etc$ cat vsftpd.conf
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
```

b) Para impedir el acceso de la cuenta anonymous lo único que tenemos que hacer es añadir al archivo de configuración vsftpd.conf la siguiente línea,

anonymous\_enable=NO

Al poner esta opción a no se prohíben los login anónimos.





Universidad de Granada

Fundamentos de Redes

3º del Grado en Ingeniería  
Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

```
# Uncomment this to allow local users to log in.  
local_enable=YES  
#
```

c) Para permitir el acceso al servicio a las cuentas locales se incluye en el archivo de configuración vsftpd.conf la siguiente línea,

local\_enable=YES

Al poner esta opción a YES se permiten el acceso a las cuentas locales al servicio.

```
# Uncomment this to allow local users to log in.  
local_enable=YES  
#
```

En los tres apartados no ha sido necesario realizar cambios pues el archivo vsftpd.conf estaba correctamente configurado de forma predeterminada. Aún así se adjuntan capturas demostrando las opciones a poner.

6 Pida a un compañero que pruebe el servicio ftp. ¿Qué comandos utilizó para ello?

En este ejercicio uso ftp para conectar PC1 y PC3, para ello en primer lugar uso el comando *service vsftpd start* en ambos PC para iniciar el servicio. En este caso la conexión será desde PC3 a PC1.



Universidad de Granada

Fundamentos de Redes

3º del Grado en Ingeniería  
Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

```
PC_3-Ubuntu20.04 [Running] - Oracle VM VirtualBox
ne View Input Devices Help
des 29 de oct 23:56
administrador@pc3: ~
administrador@pc3:~$ ftp 192.168.1.1
Connected to 192.168.1.1.
220 (vsFTPD 3.0.3)
Name (192.168.1.1:administrador): administrador
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd Descargas
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r-- 1 1000 1000 190 Oct 22 19:49 default
-rw-rw-r-- 1 1000 1000 15 Oct 29 23:55 prueba_2
-rw-rw-r-- 1 1000 1000 255 Oct 22 19:49 telnet
-rw-rw-r-- 1 1000 1000 147 Oct 22 19:49 vsftpd
226 Directory send OK.
ftp> cat prueba_2
?Invalid command
ftp> get prueba_2
local: prueba_2 remote: prueba_2
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for prueba_2 (30 bytes).
226 Transfer complete.
30 bytes received in 0.01 secs (2.7352 kB/s)
ftp> exit
221 Goodbye.
administrador@pc3:~$ cat prueba_2
Este archivo pertenece al PC1
administrador@pc3:~$
```

Desde el PC3 una vez hecho el login se utilizan los comandos,

cd Descargas, para acceder al directorio Descargas de PC1.

ls para ver que archivos/directorios se encuentran en el momento en el directorio Descargas.

get <file> para descargar en PC3 un archivo de PC1, en este caso se hace get prueba\_2.

exit para finalizar la conexión entre PC1 y PC3.

Finalmente al hacer un cat sobre el archivo descargado se ve su contenido, donde pone que pertenece al PC1. El texto lo puso yo como prueba.

7 Configure el servicio ftp para que:

7.a Únicamente pueda ser utilizando a través de la cuenta de usuario que hemos creado en nuestro equipo.

En el archivo vsftpd.conf incluimos las siguientes líneas,

userlist\_deny=NO, esta opción se examina sólo si userlist\_enable está activado. Si esta opción se configura a NO, entonces se denegará el login a los usuarios que no estén especificados en el archivo userlist\_file.



Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

userlist\_enable=YES, si esta opción está activada, vsftpd cargará una lista de nombres de usuarios desde el archivo dado por userlist\_file.

userlist\_file=/etc/vsftpd.user\_list, este será el archivo que contendrá el nombre de los usuarios a los que se podrán acceder remotamente (obviamente dicho usuario deberá acceder en el sistema). Este archivo contendrá una sola línea en la que estará escrito “daniel” que es un usuario creado previamente en PC1. Ahora veamos que funciona accediendo desde PC2.

```
PC_2-Ubuntu20.04 [Running] - Oracle VM VirtualBox
chinese View Input Devices Help
des Terminal 5 de nov 02:34
daniel@pc2: /bin
daniel@pc2:/bin$ ftp 192.168.1.1
Connected to 192.168.1.1.
220 (vsFTPd 3.0.3)
Name (192.168.1.1:daniel): daniel
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```
PC_2-Ubuntu20.04 [Running] - Oracle VM VirtualBox
chinese View Input Devices Help
des Terminal 5 de nov 02:35
daniel@pc2: /bin
daniel@pc2:/bin$ ftp 192.168.1.1
Connected to 192.168.1.1.
220 (vsFTPd 3.0.3)
Name (192.168.1.1:daniel): administrador
530 Permission denied.
Login failed.
ftp>
```

Vemos que en el segundo login pone servicio denegado ya que el nombre de usuario que se ha introducido no está en el archivo vsftpd.user\_list.

#### 7.b Acepte la subida de ficheros al servidor ftp.

Para esto utilizamos la opción write\_enable=YES, la cual controla si cualquier comando de FTP tiene permitido hacer cambios en el sistema de archivos o no.



Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

```
PC_2-Ubuntu20.04 [Running] - Oracle VM VirtualBox
chine View Input Devices Help
des Terminal 5 de nov 02:41
daniel@pc2: ~
daniel@pc2:~$ cat mensaje_pc1
Mandando mensaje desde pc_2 a pc_1
daniel@pc2:~$ ftp 192.168.1.1
Connected to 192.168.1.1.
220 (vsFTPD 3.0.3)
Name (192.168.1.1:daniel): administrador
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put mensaje_pc1 ./enviado_a_pc1
local: mensaje_pc1 remote: ./enviado_a_pc1
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
35 bytes sent in 0.00 secs (229.3939 kB/s)
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 1000    1000          4096 Oct 29 23:55 Descargas
drwxr-xr-x  2 1000    1000          4096 Oct 08 09:51 Documentos
drwxr-xr-x  2 1000    1000          4096 Oct 08 09:51 Escritorio
drwxr-xr-x  2 1000    1000          4096 Oct 08 09:51 Imágenes
drwxr-xr-x  2 1000    1000          4096 Oct 08 09:51 Música
drwxr-xr-x  2 1000    1000          4096 Oct 08 09:51 Plantillas
drwxr-xr-x  2 1000    1000          4096 Oct 08 09:51 Público
drwxr-xr-x  2 1000    1000          4096 Oct 08 09:51 Vídeos
-rw-r--r--  1 1000    1000           35 Nov 05 02:41 enviado_a_pc1
-rw-rw-r--  1 1000    1000           0 Oct 25 19:59 prueba
226 Directory send OK.
```

Ahora comprobaremos desde PC1 que el archivo que hemos enviado está,

```
administrador@pc1:~$ ls Descargas Documentos enviado_a_pc1 Escritorio Imágenes
Música Plantillas prueba Público Vídeos
administrador@pc1:~$ cat enviado_a_pc1
Mandando mensaje desde pc_2 a pc_1
administrador@pc1:~$
```

Luego como se puede ver el mensaje se ha enviado desde PC2 a PC1.

8 Habilite el servicio *http* en su equipo. Abra un navegador web y pruebe a visitar la página de inicio desde su equipo (`http://localhost` o `http://127.0.0.1`). Además, realice los siguientes cambios:

8.a Modifique el contenido de la página de inicio, y compruebe con la ayuda de su compañero que la dirección de su servidor es accesible.

La siguiente captura sería la página <http://localhost> de PC1.



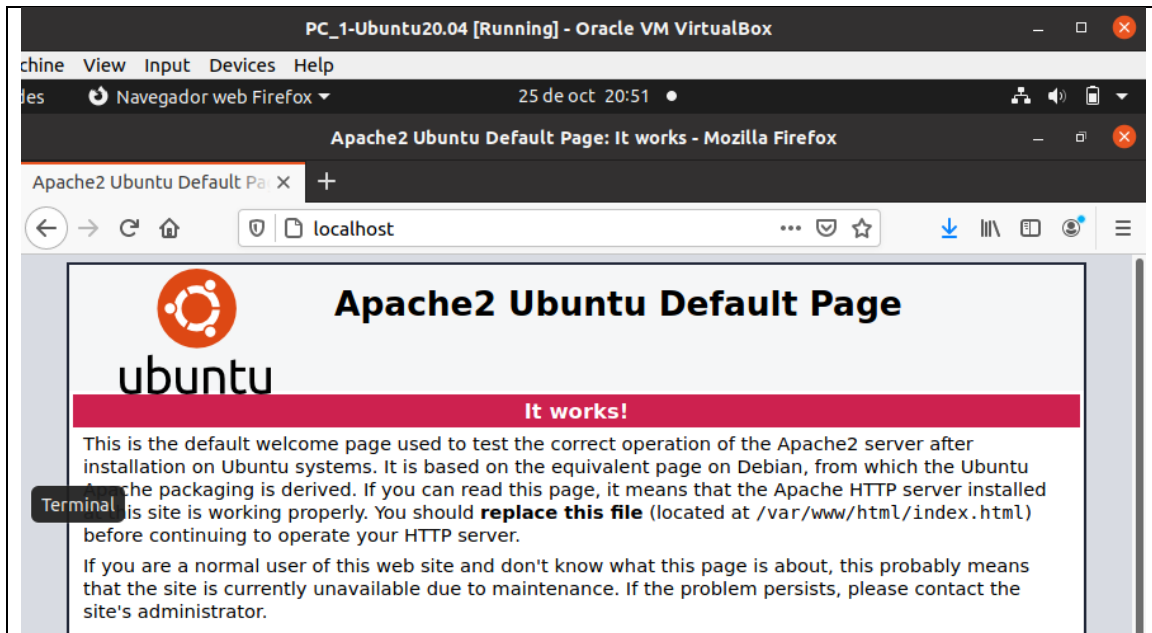
Universidad de Granada

## Fundamentos de Redes

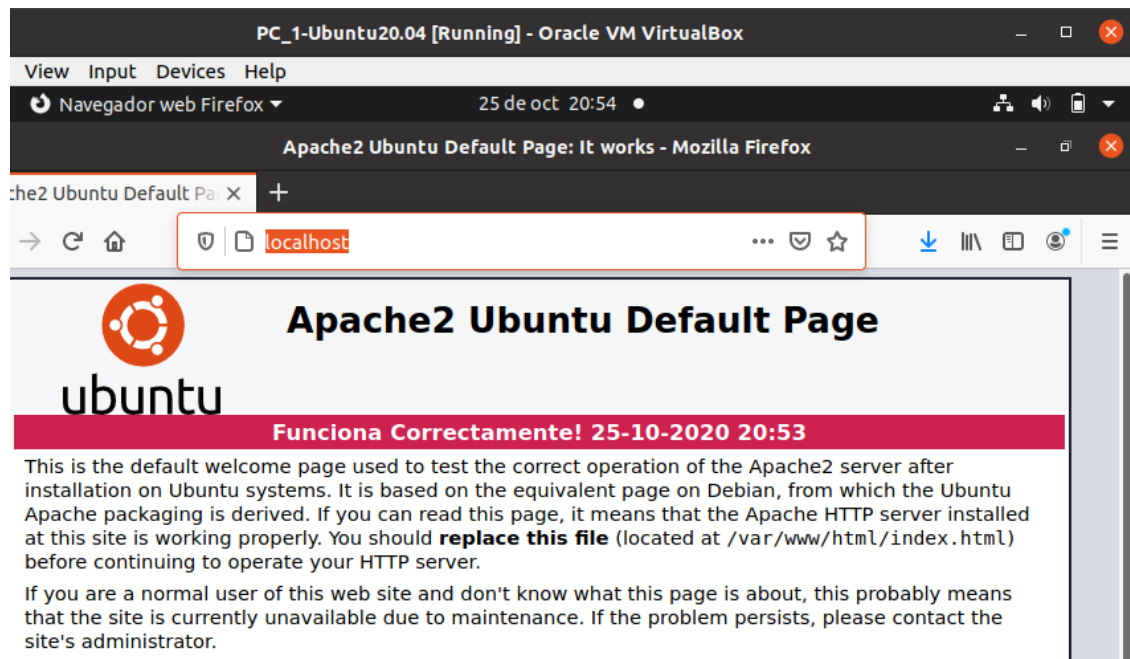
### 3º del Grado en Ingeniería Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones



Modifico el archivo “/var/www/html/index.html” para que en lugar de It works! Ponga funciona correctamente y la fecha y hora en las que modifiqué el archivo. (Como no se html simplemente cambié una línea sobre lo que ya estaba programado).



Aquí sería la página de inicio modificada. Y ahora se adjunta captura accediendo a esta página desde PC2.



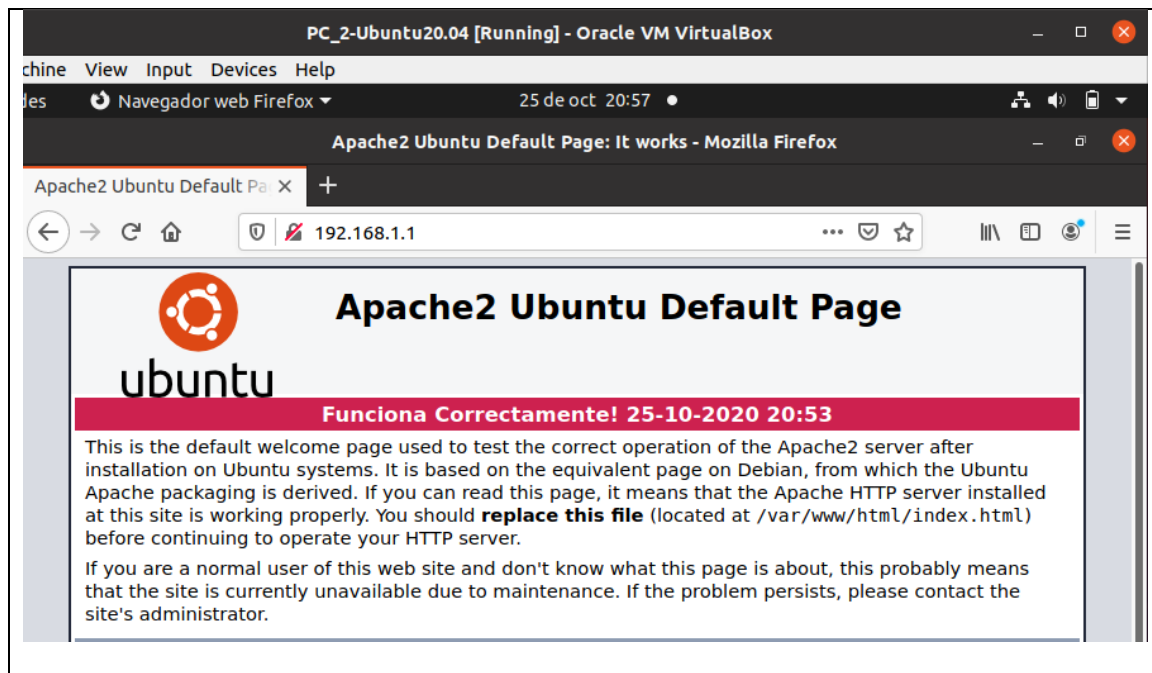
Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería Informática

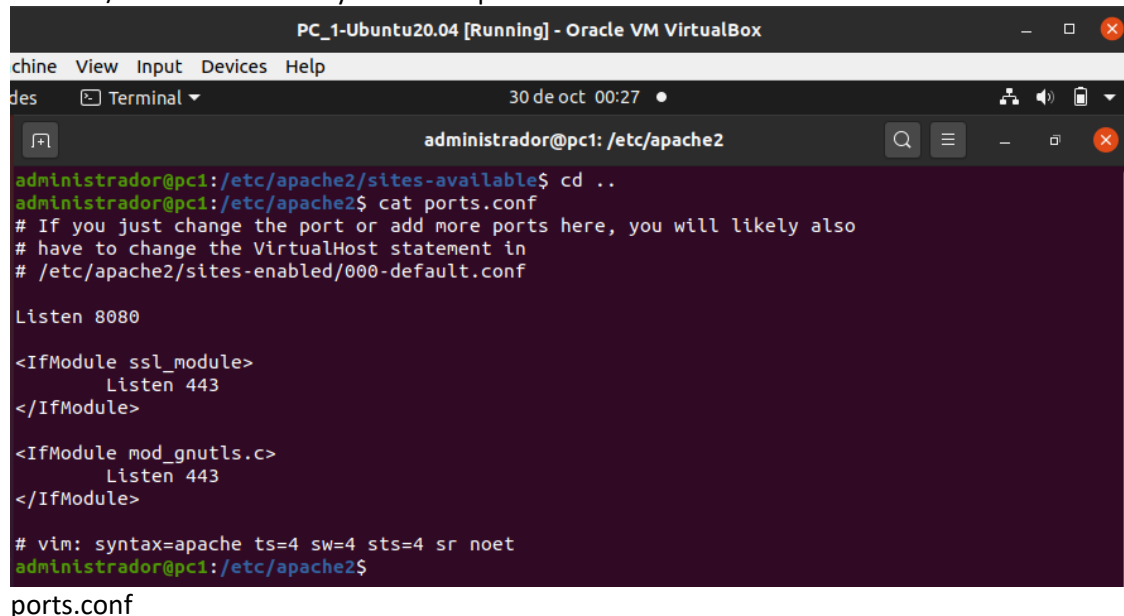


Dept. Teoría de la Señal,  
Telemática y Comunicaciones



8.b Modifique el puerto de escucha del servidor de modo que el acceso a la página de inicio se haga mediante la dirección: `http://localhost:8080`.

Para ello modifico el archivo `ports.conf` de forma que el puerto de escucha sea 8080 (para ello la primera línea será `Listen 8080`). Además modifico el archivo `"/etc/apache2/sites-enabled/000-default.conf"` y cambio el puerto a 8080.





Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

PC\_1-Ubuntu20.04 [Running] - Oracle VM VirtualBox

Machine View Input Devices Help

des Terminal 25 de oct 21:20

```
root@pc1: /etc/apache2
root@pc1:/etc/apache2# cat sites-enabled/000-default.conf
<VirtualHost *:8080>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
root@pc1:/etc/apache2#
```

000-default.conf

Ahora se adjuntan capturas demostrando que se tiene que acceder a la página de inicio del local host por medio de <http://localhost:8080>.



Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

PC\_1-Ubuntu20.04 [Running] - Oracle VM VirtualBox

Machine View Input Devices Help

es Navegador web Firefox 25 de oct 21:22

Problem loading page - Mozilla Firefox

Problem loading page x +

https://localhost

## Unable to connect

Firefox can't establish a connection to the server at localhost.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again

(la s en https se añade sola)





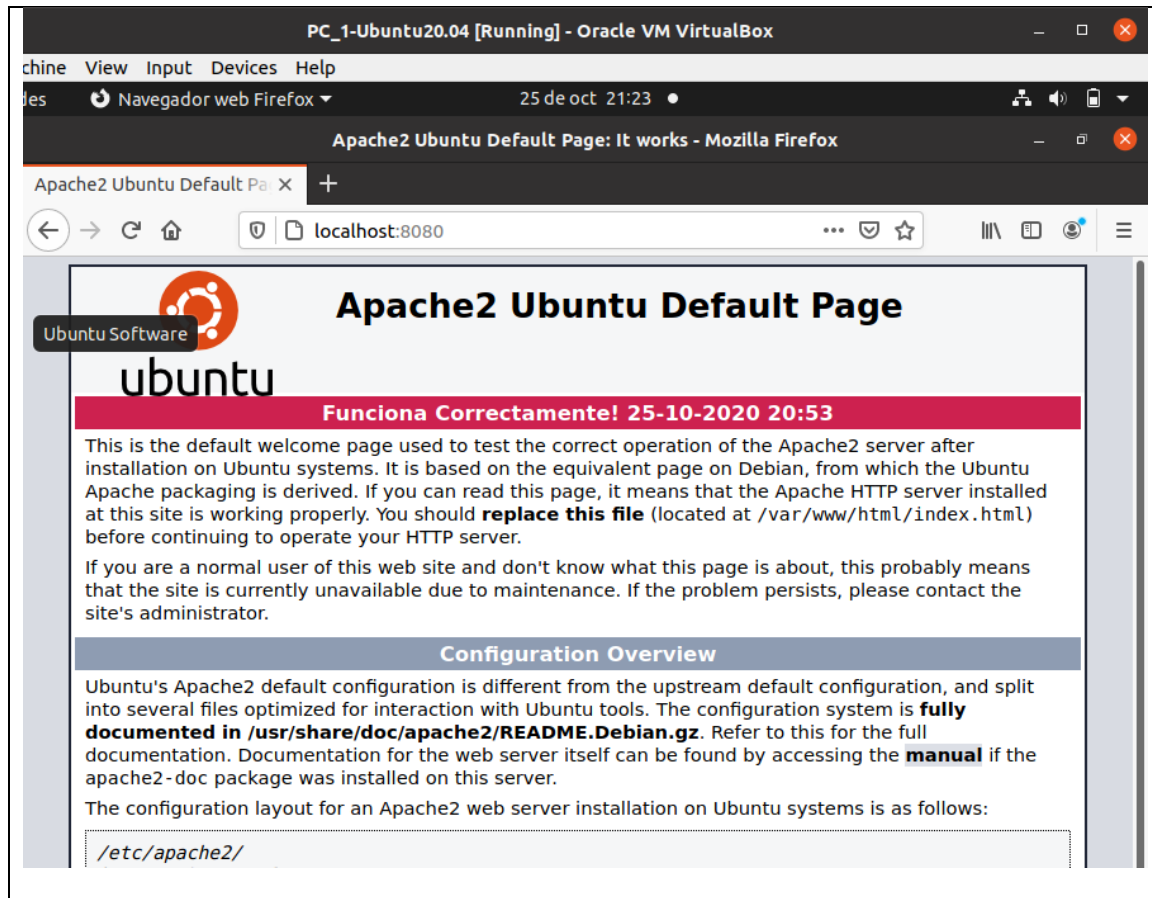
Universidad de Granada

Fundamentos de Redes

3º del Grado en Ingeniería  
Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones



8.c Cree una página de acceso restringido (es decir, que requiera usuario y contraseña antes de mostrarla) en <http://localhost/restringida/>. Utilice como credenciales de acceso el usuario *admin* y la contraseña *1234*.

En primer lugar elimino los cambios hechos anteriormente para que el puerto de escucha por defecto vuelva a ser 80.

Ahora creo la capeta restringida dentro del directorio `"/var/www/html/"`. Este será el directorio cuyo acceso sea restringido dentro de nuestro localhost. A continuación en el directorio `"/usr/local/"` uso el comando,

```
sudo htpasswd -c passwords admin
```

Que me creará el archivo que guardará encriptada la identificación para el usuario admin. Inmediatamente se pide que se introduzca contraseña y que se vuelva a introducir para confirmar, en este caso se introduce como contraseña 1234.

Ahora me voy al directorio `"/var/www/html/restringida/"`, que es el directorio al cual le queremos imponer usuario y contraseña, y en el creo un archivo `.htaccess`. Este archivo tendrá la siguiente forma,



Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

```
PC_1-Ubuntu20.04 [Running] - Oracle VM VirtualBox
Machine View Input Devices Help
es Terminal 30 de oct 00:45
administrador@pc1: /var/www/html/restringida
administrador@pc1:/var/www/html/restringida$ cat .htaccess
AuthName "Directorio Restringida -> privado"
AuthType Basic
AuthUserFile /usr/local/passwords
require valid-user
administrador@pc1:/var/www/html/restringida$
```

La opción AuthName “Name” establece el nombre del área de autorización de un directorio. Este nombre se da al usuario para que sepa que contraseña y usuario mandar.

La opción AuthType Basic selecciona el tipo de identificación de usuario para un directorio. El modo Basic establece autorización básica.

La opción AuthUserFile “file” establece el nombre del archivo textual que contiene la lista de usuarios y contraseñas para la identificación de accesos. En “file” se escribe no solo el nombre sino también la localización de este archivo.

La opción require valid-user prueba cuando un usuario es autorizado de acuerdo con unas ciertas restricciones. Valid-user permite que todos los usuarios válidos pueden acceder al recurso, en este caso, todos los usuarios que realicen un login válido de acuerdo con el archivo de autorización de la opción anterior.

Por último en el archivo de configuración de apache, apache2.conf añadimos las siguientes líneas,

```
</Directory /var/www/html/restringida/>
    AllowOverride AuthConfig
</Directory>
```

Al incluir estas líneas se hace que sobre el directorio /var/www/html/restringida se aplique la opción AllowOverride AuthConfig, es decir, en ese directorio se permite las directivas de autorización de acceso sobreponiéndose al archivo de configuración.

Finalmente se adjunta captura de que funciona correctamente.



Universidad de Granada

Fundamentos de Redes

3º del Grado en Ingeniería  
Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

