



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

Gonzalo de la Torre Martínez
Javier Ramírez Pulido
Grupo B2

1.1 Realización práctica

- 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?

Las interfaces son las siguientes:

- enp0s3: red NAT, ip: 10.0.2.15
- enp0s9: red de datos, ip: 33.1.1.2
- enp0s10: red de gestión, ip: 198.162.1.1
- lo: localhost, ip: 127.0.0.1

ifconfig está ejecutado después de desactivar la red host-only (enp0s8)

```
root@pci:/home/administrador# 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 108293 bytes 156238639 (156.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6798 bytes 458662 (458.6 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:fe45:d52c prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:45:d5:2c txqueuelen 1000 (Ethernet)
    RX packets 164 bytes 17135 (17.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 126 bytes 12578 (12.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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:fe1e:f9a3 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:1e:f9:a3 txqueuelen 1000 (Ethernet)
    RX packets 166 bytes 17334 (17.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 128 bytes 12792 (12.7 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 521 bytes 47292 (47.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 521 bytes 47292 (47.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@pci:/home/administrador#
```



Universidad de Granada



- 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*.

Es posible hacer ping mediante la red de gestión:

```
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=0.963 ms
64 bytes from 192.168.1.3: icmp_seq=2 ttl=64 time=0.992 ms
64 bytes from 192.168.1.3: icmp_seq=3 ttl=64 time=0.953 ms
64 bytes from 192.168.1.3: icmp_seq=4 ttl=64 time=1.04 ms
64 bytes from 192.168.1.3: icmp_seq=5 ttl=64 time=0.993 ms
^C
--- 192.168.1.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 0.953/0.989/1.044/0.031 ms
administrador@pc1:~$
```

en cambio no se puede hacer ping mediante la red de datos:

```
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 ---
8 packets transmitted, 0 received, 100% packet loss, time 7142ms
administrador@pc1:~$
```

esto se debe a que, como podemos ver en el esquema de la práctica, la red de gestión conecta directamente las tres máquinas virtuales (pc1, pc2, pc3), en cambio la red de datos solo conecta directamente pc1 y pc2, pero no pc3.

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



Universidad de Granada

Fundamentos de Redes

3º del Grado en Ingeniería
Informática



Dept. Teoría de la Señal,
Telemática y Comunicaciones

En primer lugar creamos un nuevo usuario en pc3 (telemaco)

```
root@pc3:/home/administrador/Descargas# adduser telemaco
Añadiendo el usuario 'telemaco' ...
Añadiendo el nuevo grupo 'telemaco' (1001) ...
Añadiendo el nuevo usuario 'telemaco' (1001) con grupo 'telemaco' ...
Creando el directorio personal '/home/telemaco' ...
Copiando los ficheros desde '/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para telemaco
Introduzca el nuevo valor, o presione INTRO para el predeterminado
Nombre completo []: telemaco
Número de habitación []:
Teléfono del trabajo []:
Teléfono de casa []:
Otro []:
¿Es correcta la información? [S/n] S
root@pc3:/home/administrador/Descargas#
```

Seguidamente activamos el servicio telnet (cambiando en el archivo /etc/xinetd.d/telnet la línea "disable = yes" por "disable = no"). Reiniciamos el servicio xinetd y finalmente se puede observar como accedemos desde pc1 con el usuario root, al usuario telemaco de pc3



Universidad de Granada

Fundamentos de Redes

3º del Grado en Ingeniería
Informática



Dept. Teoría de la Señal,
Telemática y Comunicaciones

```
root@pc1:/home/administrador/Descargas# telnet 192.168.1.3
Trying 192.168.1.3...
Connected to 192.168.1.3.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
pc3 login: telemaco
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

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

Your Hardware Enablement Stack (HWE) is supported until April 2025.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

telemaco@pc3:~$
```

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

En el archivo `/etc/xinetd.d/telnet`: añadimos la siguiente sentencia,
`only_from = IP`, donde IP es la dirección de nuestro compañero

```
1 service telnet
2 {
3     disable      = no
4     flags        = REUSE
5     socket_type  = stream
6     wait         = no
7     user         = root
8     server        = /usr/sbin/in.telnetd
9     log_on_failure += USERID
10    only_from     = 192.168.1.1
11 }
```



Universidad de Granada



- 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.

Debemos añadir varias sentencias en los archivos `/etc/xinetd.d/telnet` y `/etc/xinetd.conf`

- `log_on_failure` (`log_on_success`) `+= HOST`, estos parámetros indican si se ha producido un log con éxito o fracaso, `HOST` indica la dirección de quién intenta entrar
- `log_type = FILE /var/log/telnet.log`, este parámetro indica el destino (archivo) donde se va a guardar el registro de acceso

Hay que modificar de la siguiente forma los archivos:

```
telnet
/etc/xinetd.d

1 service telnet
2 {
3     disable          = no
4     flags             = REUSE
5     socket_type       = stream
6     wait             = no
7     user              = root
8     server            = /usr/sbin/in.telnetd
9     log_on_failure    += USERID
10    only_from         = 192.168.1.1
11    log_on_success    += HOST
12    log_on_failure    += HOST
13    log_type          = FILE /var/log/telnet.log
14 }
```

```
xinetd.conf
/etc

1 # Simple configuration file for xinetd
2 #
3 # Some defaults, and include /etc/xinetd.d/
4
5 defaults
6 {
7
8 # Please note that you need a log_type line to be able to use log_on_success
9 # and log_on_failure. The default is the following :
10 # log_type = SYSLOG daemon info
11
12     log_type          = FILE /var/log/xinetdlog
13     log_on_failure    += USERID
14 }
15 }
16
17 includedir /etc/xinetd.d
```



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

Para las tres partes del ejercicio necesitaremos abrir el archivo `/etc/vsftpd.conf`

- a) Buscamos “listen”, finalmente establecemos la igualdad a “listen=NO”
- b) Buscamos “anonymous_enable”, finalmente establecemos la igualdad a “anonymous_enable=NO”
- c) Buscamos “local_enable”, finalmente establecemos la igualdad a “local_enable=YES”

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

Primero estableció conexión a través de la IP de la red de gestión con ftp

```
ades Terminal 24 de oct 22:39
administrador@pc2: ~
administrador@pc2:~$ ftp 192.168.1.1
Connected to 192.168.1.1.
220 (vsFTPD 3.0.3)
Name (192.168.1.1:administrador): javierramirezp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```



Universidad de Granada

Fundamentos de Redes

3º del Grado en Ingeniería
Informática



Dept. Teoría de la Señal,
Telemática y Comunicaciones

Probamos algún comando para comprobar que se ha establecido una conexión correcta

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 1001    1001        4096 Oct 24 22:25 Descargas
drwxr-xr-x  2 1001    1001        4096 Oct 24 22:25 Documentos
drwxr-xr-x  2 1001    1001        4096 Oct 24 22:25 Escritorio
drwxr-xr-x  2 1001    1001        4096 Oct 24 22:25 Imágenes
drwxr-xr-x  2 1001    1001        4096 Oct 24 22:25 Música
drwxr-xr-x  2 1001    1001        4096 Oct 24 22:25 Plantillas
drwxr-xr-x  2 1001    1001        4096 Oct 24 22:25 Público
drwxr-xr-x  2 1001    1001        4096 Oct 24 22:25 Videos
226 Directory send OK.
ftp> 
```

Creamos un archivo de prueba en el pc al que nos conectamos para poder comprobar a descargar algún archivo

```
javierramirezp@pc1: ~
javierramirezp@pc1:~$ touch prueba
javierramirezp@pc1:~$ 
```



Universidad de Granada

Fundamentos de Redes

3º del Grado en Ingeniería
Informática



Dept. Teoría de la Señal,
Telemática y Comunicaciones

Compruebo que se ha creado correctamente y lo descargo en mi pc con la orden "get"

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 1001      1001      4096 Oct 24 22:25 Descargas
drwxr-xr-x  2 1001      1001      4096 Oct 24 22:25 Documentos
drwxr-xr-x  2 1001      1001      4096 Oct 24 22:25 Escritorio
drwxr-xr-x  2 1001      1001      4096 Oct 24 22:25 Im??genes
drwxr-xr-x  2 1001      1001      4096 Oct 24 22:25 M??sica
drwxr-xr-x  2 1001      1001      4096 Oct 24 22:25 Plantillas
drwxr-xr-x  2 1001      1001      4096 Oct 24 22:25 P??blico
drwxr-xr-x  2 1001      1001      4096 Oct 24 22:25 V??deos
-rw-rw-r--  1 1001      1001         0 Oct 24 22:44 prueba
226 Directory send OK.
ftp> get prueba
local: prueba remote: prueba
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for prueba (0 bytes).
226 Transfer complete.
ftp>
```

Y compruebo en el cliente que efectivamente ese archivo de prueba se ha descargado

```
administrador@pc2:~$ ls
Descargas  Escritorio  Música      prueba      ruta
Documentos Imágenes   Plantillas  Público     Vídeos
administrador@pc2:~$
```

- 7) Configure el servicio ftp para que:
- Únicamente pueda ser utilizando a través de la cuenta de usuario que hemos creado en nuestro equipo.



Universidad de Granada



Modificamos como super usuario el archivo `/etc/vsftputusers`, que es donde se encuentra la lista de usuarios que tienen prohibida la entrada con ftp. Añadimos “administrador” y con estas solo podremos acceder con usuarios creados por nosotros

```
root@pc1: /home/administrador/Descargas
root@pc1:/home/administrador/Descargas# gedit /etc/vsftputusers
(gedit:5918): Tepl-WARNING **: 11:19:28.592: GVfs metadata is not
supported. Fallback to TeplMetadataManager. Either GVfs is not cor
rectly
rm. In
vfu-me
8 games
9 man
10 lp
11 mail
12 news
13 uucp
14 nobody
15 administrador
Editor de textos  altura del tabulador: 8 Ln 15, Col 14 INS
```

Probamos a acceder a “administrador” en el servidor y se nos niega el acceso



Universidad de Granada

Fundamentos de Redes

3º del Grado en Ingeniería
Informática



Dept. Teoría de la Señal,
Telemática y Comunicaciones

```
vidades Terminal 30 de oct 11:21
root@pc2: /home/administrador/Descargas
root@pc2:/home/administrador/Descargas# 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:
530 Login incorrect.
Login failed.
ftp>
```

Pero si probamos en el especificado por nosotros, el acceso es concedido

```
dades Terminal 30 de oct 11:21
root@pc2: /home/administrador/Descargas
root@pc2:/home/administrador/Descargas# ftp 192.168.1.1
Connected to 192.168.1.1.
220 (vsFTPD 3.0.3)
Name (192.168.1.1:administrador): javierramirezp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

b) Acepte la subida de ficheros al servidor ftp.

Descomentamos algunos atributos del vsftpd.conf para permitir la subida de archivos



Universidad de Granada

Fundamentos de Redes

3º del Grado en Ingeniería
Informática



Dept. Teoría de la Señal,
Telemática y Comunicaciones

```
ades  Editor de textos  25 de oct 12:54  [icon]
*vsftpd.conf  Guardar  [menu]  [minus]  [copy]  [close]
/etc
30 # Uncomment this to enable any form of FTP write command.
31 #write_enable=YES
32 #
33 # Default umask for local users is 077. You may wish to
   change this to 022,
34 # if your users expect that (022 is used by most other ftpd's)
35 #local_umask=022
36 #
37 # Uncomment this to allow the anonymous FTP user to upload
   files. This only
38 # has an effect if the above global write enable is
   activated. Also, you will
39 # obviously need to create a directory writable by the FTP
   user.
40 anon upload enable=YES
41 #
42 # Uncomment this if you want the anonymous FTP user to be
   able to create
43 # new directories.
44 #anon_mkdir_write_enable=YES
45 #
```



Universidad de Granada

Fundamentos de Redes

3º del Grado en Ingeniería
Informática



Dept. Teoría de la Señal,
Telemática y Comunicaciones

```
des  Editor de textos  25 de oct 12:54
*vsftpd.conf
/etc  Guardar
IPv4 and IPv6
19 # sockets. If you want that (perhaps because you want to
listen on specific
20 # addresses) then you must run two copies of vsftpd with two
configuration
21 # files.
22 listen_ipv6=YES
23 #
24 # Allow anonymous FTP? (Disabled by default).
25 anonymous_enable=NO
26 #
27 # Uncomment this to allow local users to log in.
28 local_enable=YES
29 #
30 # Uncomment this to enable any form of FTP write command.
31 write_enable=YES
32 #
33 # Default umask for local users is 077. You may wish to
change this to 022,
34 # if your users expect that (022 is used by most other ftpd's)
35 #local_umask=022
36 #
37 # Uncomment this to allow the anonymous FTP user to upload
files. This only
38 # has an effect if the above global write enable is
activated. Also you will
```

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

Este es el contenido original de la pagina a la que accedemos.



Universidad de Granada

Fundamentos de Redes

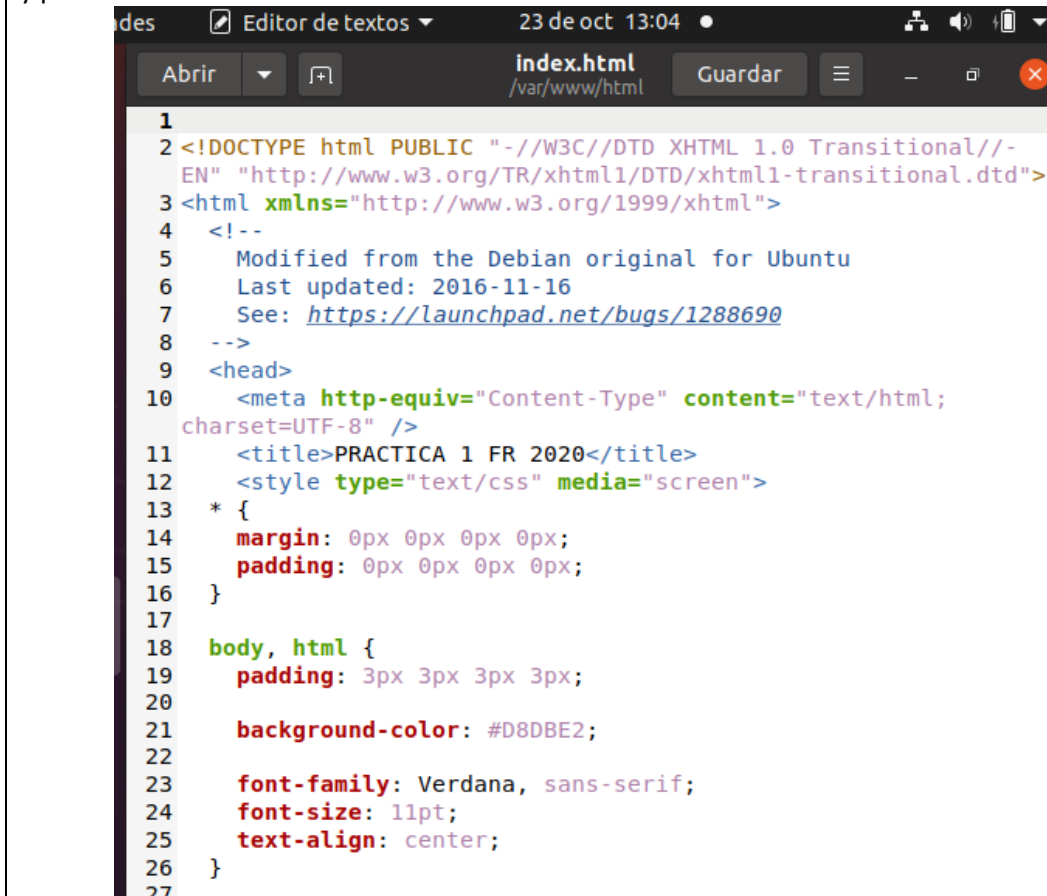
3º del Grado en Ingeniería Informática



Dept. Teoría de la Señal,
Telemática y Comunicaciones



Tras dar permisos de escritura, modificamos algo dentro del html, como por ejemplo, un título y ponemos "PRACTICA 1 FR 2020"





Universidad de Granada

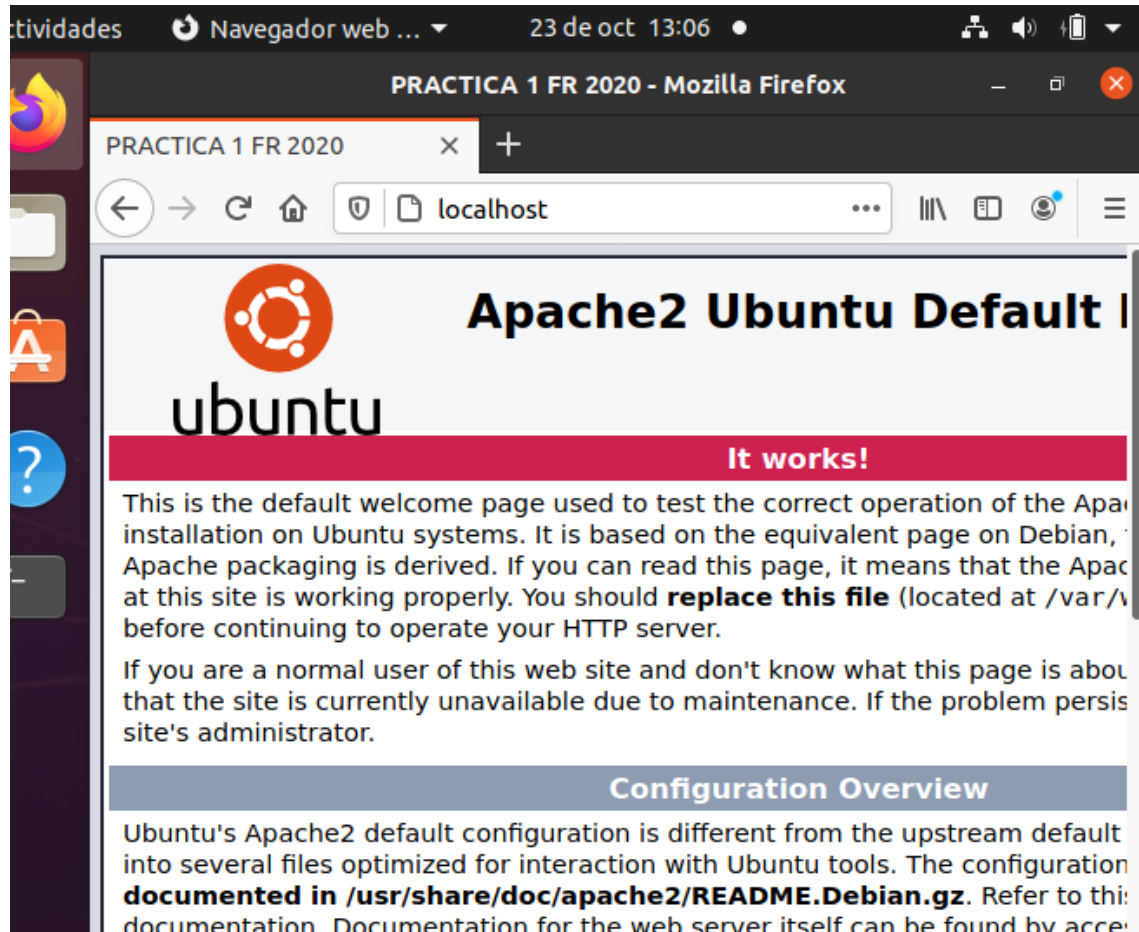
Fundamentos de Redes

3º del Grado en Ingeniería
Informática



Dept. Teoría de la Señal,
Telemática y Comunicaciones

Y al recargar vemos como los cambios se han aplicado en el nombre de la pestaña que tenemos abierta.



- 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`.



The image displays two screenshots of a text editor window, likely gedit, showing Apache configuration files. The top screenshot shows the `ports.conf` file located at `/etc/apache2`. The file contains instructions on how to change the listening port and includes configurations for SSL and mod_gnutls. The bottom screenshot shows the `default` file located at `/etc/apache2/sites-available`. It contains a `<VirtualHost>` block for `192.168.1.2:8080` with settings for `ServerAdmin`, `DocumentRoot`, and logging.

```
des Editor de textos 24 de oct 13:12
ports.conf /etc/apache2
Abrir Guardar
000-default.conf x default x ports.conf x
1 # If you just change the port or add more ports here, you will
  likely also
2 # have to change the VirtualHost statement in
3 # /etc/apache2/sites-enabled/000-default.conf
4
5 Listen 192.168.1.1:8080
6
7 <IfModule ssl_module>
8     Listen 443
9 </IfModule>
10
11 <IfModule mod_gnutls.c>
12     Listen 443
13 </IfModule>
14
15 # vim: syntax=apache ts=4 sw=4 sts=4 sr noet

ades Editor de textos 23 de oct 13:15
default /etc/apache2/sites-available
Abrir Guardar
1 <VirtualHost 192.168.1.2:8080>
2
3     ServerAdmin webmaster@localhost
4     DocumentRoot /var/www/
5
6     #Logs
7     ErrorLog ${APACHE_LOG_DIR}/error.log
8     CustomLog ${APACHE_LOG_DIR}/access.log combined
9
10 </VirtualHost>
```




Universidad de Granada

Fundamentos de Redes

3º del Grado en Ingeniería
Informática



Dept. Teoría de la Señal,
Telemática y Comunicaciones

```
1 <VirtualHost 192.168.1.2:8080>
2     # The ServerName directive sets the request scheme,
3     # hostname and port that
4     # the server uses to identify itself. This is used when
5     # creating
6     # redirection URLs. In the context of virtual hosts, the
7     # ServerName
8     # specifies what hostname must appear in the request's
9     # Host: header to
10    # match this virtual host. For the default virtual host
11    # (this file) this
12    # value is not decisive as it is used as a last resort
13    # host regardless.
14    # However, you must set it for any further virtual host
15    # explicitly.
16    #ServerName www.example.com
17
18    ServerAdmin webmaster@localhost
19    DocumentRoot /var/www/html
```

Tras modificar los atributos y archivos considerados como necesarios, reiniciamos el servicio de apache2 para asegurarnos de la aplicación de los cambios.

```
root@pc2:/home/administrador# service apache2 start
root@pc2:/home/administrador# service apache2 stop
root@pc2:/home/administrador# service apache2 restart
root@pc2:/home/administrador#
```

Y comprobamos que ahora la forma de acceder a la pagina es especificando el puerto detrás (192.168.1.2:8080)



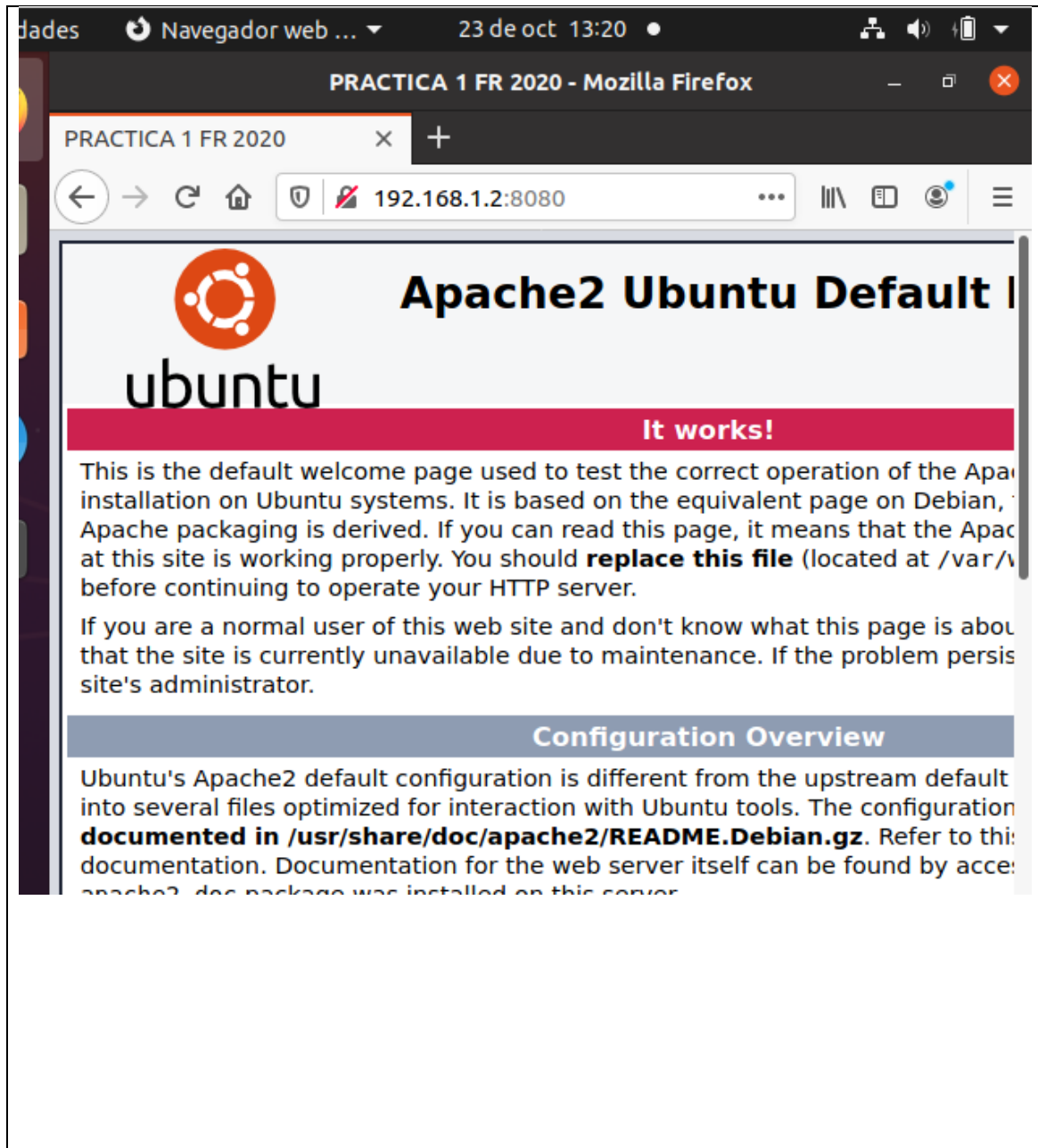
Universidad de Granada

Fundamentos de Redes

3º del Grado en Ingeniería
Informática



Dept. Teoría de la Señal,
Telemática y Comunicaciones



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*.



Borro 'index.html' como ponía en la página ("Reemplaza este archivo antes de continuar") y creo una carpeta que será a la que restringiremos el acceso. Con la orden proporcionada en el enunciado establecemos un usuario y una contraseña que, por defecto, se encriptará.

```
root@pc1: /var/www/html
root@pc1:/var/www/html# rm index.html
root@pc1:/var/www/html# mkdir restringida
root@pc1:/var/www/html# htpasswd -c /var/www/html/restringida/pass
words admin
New password:
Re-type new password:
Adding password for user admin
root@pc1:/var/www/html#
```

Creamos en el interior del directorio a restringir un archivo nuevo llamado ".htaccess" y lo rellenamos con el texto que se ve en la siguiente imagen. También pasamos index.html a la carpeta "restringida"

```
root@pc1:/var/www/html# cd restringida/
root@pc1:/var/www/html/restringida# gedit .htaccess

(gedit:21193): Tepl-WARNING **: 13:26:32.516: GVfs metadata is not
supported. Fallback to TeplMetadataManager. Either GVfs is not co
s platf
isable-

1 AuthName "Restricted Area"
2 AuthType Basic
3 AuthUserFile /var/www/html/restringida/passwords
4 require valid-user
```



Modificamos en apache2.conf el AllowOverride para que prevalezcan los cambios realizados en .htaccess

The screenshot shows a terminal window with the command `gedit /etc/apache2/apache2.conf` being executed. A text editor window titled `apache2.conf /etc/apache2` is open, displaying the following configuration lines:

```
170 <Directory /var/www/>
171     Options Indexes FollowSymLinks
172     AllowOverride All
173     Require all granted
174 </Directory>
```

The editor's status bar at the bottom indicates `texto plano`, `Anchura del tabulador: 4`, `Ln 1, Col 1`, and `INS`.

Y probamos a acceder a este directorio nuevo.



Universidad de Granada

Fundamentos de Redes

3º del Grado en Ingeniería
Informática



Dept. Teoría de la Señal,
Telemática y Comunicaciones

Index of / - Mozilla Firefox

• Index of /

192.168.1.1:8080/restringida/

Index of /

Name

Last modified

Size

Description

Authentication Required - Mozilla Firefox

http://192.168.1.1:8080 is requesting your username and password. The site says: "Restricted Area"

User Name:

Password:

Cancel

OK

Como vemos, este ya te requiere un usuario y contraseña. De tal forma, probamos a introducir la que hemos creado por defecto



Universidad de Granada

Fundamentos de Redes

3º del Grado en Ingeniería
Informática



Dept. Teoría de la Señal,
Telemática y Comunicaciones

Index of /

192.168.1.1:8080/restringida/

Index of /

[Name](#) [Last modified](#) [Size](#) [Description](#)

Authentication Required - Mozilla Firefox

http://192.168.1.1:8080 is requesting your username and password. The site says: "Restricted Area"

User Name:

Password:

Y con esto desbloqueamos el acceso como nos pedían.



Universidad de Granada

Fundamentos de Redes

3º del Grado en Ingeniería
Informática




Dept. Teoría de la Señal,
Telemática y Comunicaciones

ades Navegador web ... 26 de oct 20:58

PRACTICA 1 FR 2020 x +

192.168.1.1:8080/restringida

Apache2 Ubuntu Default I



ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache installation on Ubuntu systems. It is based on the equivalent page on Debian, and the Apache packaging is derived. If you can read this page, it means that the Apache at this site is working properly. You should **replace this file** (located at `/var/www`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, that the site is currently unavailable due to maintenance. If the problem persists, contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration. It is split into several files optimized for interaction with Ubuntu tools. The configuration is **documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this documentation. Documentation for the web server itself can be found by accessing the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/  
|-- apache2.conf
```

Y ya accedmos.