Capítulo 6

Instalación del sistema

> The whole is more than the sum of its parts.
>
> Aristóteles

Una vez acabado con el código tanto de la aplicación como del sitio web, solo nos restará finalmente el instalar la red, así como el comprobar su correcto funcionamiento.

En nuestra red podemos diferenciar entre tres elementos distintos, cada uno de los cuales necesitara de una preparación y atención diferente al resto. Éstos son: el servidor web (al que también hemos llamado PC de administración) y los PCs y conmutadores de las subredes de prácticas. Antes de llevar a cabo la instalación de cualquiera de ellos, se recomienda llevar a cabo una serie de pasos que facilitarán las tareas de configuración y administración de la red:

- **Etiquetar los elementos de la red**. Para el correcto funcionamiento del sistema es necesario que cada uno de los PCs y conmutadores que conforman la red tengan asignados un identificador único, el cual será usado posteriormente por la aplicación para diferenciarlos. Es recomendable por tanto el etiquetar físicamente todo el hardware de red con el id asignado, lo cual permitirá por ejemplo localizar el problema en caso de producirse un error.

- **Establecer la configuración de la red de administración**. Es necesario definir la IP y máscara de red que vayan a ser usados en la red de administración ya que estos datos son necesarios para configurar las interfaces reservadas para esta red. También habrá que decidir el listado de puertos de los con-

mutadores que serán asignados a la vlan de administración (se reservarán los mismos puertos en todos ellos).

- **Definir la topología y elementos de las subredes de práctica**. Deberemos tener claro cual va a ser la estructura de las subredes de prácticas.

Todas estas decisiones afectan a la configuración de la aplicación. Ésto se reflejará en el archivo `configuracion.php` y los esquemas de las subredes de prácticas creados para ser usadas en la interfaz de usuario. Para una mayor información acerca de como tratar con estos archivos ver el apéndice A.

6.1. El servidor web

6.1.1. Sistema operativo

El primer pasó consistirá en la instalación del sistema operativo en la máquina escogida para ejercer como servidor web. Tanto en el servidor web como en el resto de PCs, se usará Linux, siendo la distribución escogida Debian GNU/Linux 5.0 'Lenny'.

No explicaremos aquí el proceso completo de instalación del sistema operativo aunque sí cabe mencionar algunas de las decisiones tomadas durante el mismo.

Se ha optado por el uso del gestor de volúmenes lógicos (Logical Volume Manager ó LVM). Una de las principales ventajas del sistema LVM sobre el sistema tradicional, es que LVM nos abstrae de los discos físicos y de las limitaciones de un disco, permitiendo tener sistemas de ficheros sobre varios discos, redimensionarlos según las necesidades y por lo tanto, hacer un uso más eficiente del espacio del que disponemos, con independencia de su ubicación.

Entre las particiones creadas se ha reservado una para las tareas de respaldo del sistema. En esta partición se almacenaran las copias de seguridad realizadas periódicamente de los archivos de la aplicación, así como una copia del sistema completo una vez se halla finalizado con su puesta en marcha.

6.1.2. Configuración de red y manejo remoto vía OpenSSH

El primer paso que llevaremos a cabo una vez finalizada la instalación del sistema operativo consistirá en la configuración de red. Para ello editaremos el archivo `/etc/network/interfaces`. Habremos de establecer la configuración de las dos interfaces de red de las que deberá disponer la máquina. A la primera de ellas

le asignaremos una IP pública, la cuál será donde el servidor web permanecerá a la escucha. A la segunda le asignaremos una IP privada dentro del rango de direcciones de la red de administración. Una vez establecida la configuración reiniciaremos la red para que los cambios surtan efecto.

Para habilitar la conexión remota con el servidor instalaremos el servidor OpenSSH. Este servidor nos permitirá el acceder y administrar el PC de manera remota y segura mediante el uso del protocolo SSH. Por motivos de seguridad es recomendable desactivar el acceso remoto al usuario 'root' (`PermitRootLogin no`) y, si se considerara necesario, establecer específicamente los usuarios y host a los que permitir el acceso mediante la directiva `AllowUsers`. También cabría la posibilidad de usar pares de llaves pública y privada para autenticar el acceso a los servidores en vez de la tradicional combinación de usuario y contraseña.

6.1.3. Configuración del firewall

La opción más común y frecuente para proteger un servidor es el empleo de iptables. Sin embargo, sus reglas pueden resultar innecesariamente detalladas para una configuración básica de servidor web, acceso shell y base de datos MySQL. Uncomplicated Firewall (UFW) es una alternativa más simple de instalar, configurar y administrar que a la vez sirve de interfaz para iptables.

Para instalar Uncomplicated Firewall (UFW), bastará con ejecutar el siguiente comando:

```
sudo apt-get install ufw
```

Si el comando anterior no llevara a cabo la instalación del programa, se debería aadir el siguiente repositorio al archivo `/etc/apt/sources.list`:

```
deb http://ftp.de.debian.org/debian squeeze main
```

Deberemos permitir el acceso al puerto 22 (SSH), el puerto 80 (HTTP) y el puerto 443 (HTTPS) así como el acceso a través de la red de administración:

```
sudo ufw default deny
sudo ufw allow 22/tcp
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp
sudo ufw allow from 192.168.200.0/24
```

Una vez definidas nuestras reglas activaremos el firewall:

```
sudo ufw enable
```

Podremos verificar su estado en cualquier momento escribiendo:

```
sudo ufw status
```

6.1.4. Servidor web: Apache, PHP y MySQL

Para poner en marchar el servidor web lo primero será instalar los siguientes paquetes haciendo uso del comando `apt-get`:

- Servidor web: `apache2` y `apache2-mpm-prefork`.
- Base de datos: `mysql-server`.
- Interprete PHP: `php5`, `php5-mysql`, `php5-gd` y `php5-cli`.
- Administración la base de datos: `phpmyadmin`.

Una vez finalizada la instalación de todos ellos se llevara a cabo la configuración de los mismos. La seguridad de un servidor y los controles de acceso al mismo son temas de vital importancia. Tomaremos una serie de medidas simples que nos permitirán aumentar esta seguridad.

6.1.4.1. Configuración de Apache

El primer paso consistirá en eliminar el sitio web por defecto que sirve Apache:

```
sudo rm /var/www/index.php
sudo a2dissite default
```

Una vez hecho ésto, es el turno de copiar los archivos de nuestra propia web al servidor y crear el archivo de configuración correspondiente:

```
sudo cp -r redes /var/www/
find /var/www -type f -exec sudo chmod 664 {} \;
sudo nano /etc/apache2/sites-available/redes
```

El archivo de configuración tendrá el siguiente aspecto:

```
<VirtualHost *:80>
  # Sustituir localhost con el nombre del dominio
  ServerName localhost
  ServerAdmin admin@localhost
  DocumentRoot /var/www/redes

  <Directory />
    Options -Indexes -Includes -FollowSymLinks
  </Directory>
  <Directory /var/www/redes>
    Order allow,deny
    Allow from all
  </Directory>
  <Directory /var/www/redes/admin>
    Order allow,deny
    Deny from all
    <Files aplicacion.php>
      Order allow,deny
      Allow from all
    </Files>
    <Files proc_form.php>
      Order allow,deny
      Allow from all
    </Files>
    <Files usuario.php>
      Order allow,deny
      Allow from all
    </Files>
    <Files log.php>
      Order allow,deny
      Allow from all
    </Files>
    <Files conm_config.php>
      Order allow,deny
      Allow from all
    </Files>
  </Directory>
  <Directory /var/www/redes/include>
    Order allow,deny
    Deny from all
  </Directory>
  <Directory /var/www/redes/downloads>
    Order allow,deny
    Allow from all
  </Directory>

  ErrorLog /var/log/apache2/error.redes.log
  LogLevel warn
  CustomLog /var/log/apache2/access.redes.log combined
```

```
  RewriteEngine on
  RewriteRule ^/$ /index.php?inicio [NC]
  RewriteRule ^/configuraon/(.+)\.txt$ /home/www-data/uploads/$1\.txt [NC]
  RewriteRule ^/aplicacion/?$ /aplicacion.php [NC]
  RewriteRule ^/turnos/?$ /index.php?turnos [NC]
  RewriteRule ^/administrar/?$ /index.php?administrar [NC]
  RewriteRule ^/administrar/([^/.]+)/?$ /index.php?administrar&$1 [NC]
</VirtualHost>
```

Como podemos ver se hace uso del modulo 'rewrite' para lograr URLs amigables en nuestra página. Será necesario por tanto el activar dicho modulo:

```
sudo a2enmod rewrite
```

La aplicación web hace uso de una serie de archivos y directorios que deberemos crear con antelación y asignarles los permisos necesarios. En los siguientes comandos, 'www-data' es el usuario con que se ejecuta el servidor Apache:

```
# Carpeta para archivos de log
sudo mkdir /var/log/labredes
sudo chown www-data:www-data /var/log/labredes

# Carpetas para almacenar los archivos de configuración de los conmutadores
sudo mkdir /home/labredes
sudo mkdir /home/labredes/configuraciones
sudo mkdir /home/labredes/configuraciones/administracion
sudo mkdir /home/labredes/configuraciones/usuarios
sudo find /home/labredes -type d -exec chown www-data:www-data {} \;
```

Tras la creación de estas carpetas, podremos finalmente poner en marcha nuestro sitio web:

```
sudo a2ensite redes
sudo service apache2 restart
```

Si bien ya será posible acceder a la página web, podremos ver como ésta no se carga correctamente. Ésto es debido a que aún no habremos creado la base de datos para el sitio web y la aplicación.

En lo referente a la seguridad del servidor, llevaremos a cabo una serie de cambios en el archivo de seguridad de Apache `/etc/apache2/conf.d/security`.

Podremos restringir la información que divulga el servidor sobre su configuración para eliminar riesgos editando los valores de `ServerTokens` y `ServerSignature`, cambiándolos a:

```
ServerTokens Prod
ServerSignature Off
```

También descomentaremos las siguientes líneas con el objetivo de restringir el acceso a la raíz del sistema a través del servidor web:

```
<Directory />
  AllowOverride None
  Order Deny,Allow
  Deny from all
</Directory>
```

6.1.4.2. Configuración de MySQL

Lo primero será configurar MySQL, tras lo cual crearemos la base de datos a ser usada por la aplicación. Empezamos pues editando el archivo de configuración de MySQL `my.cnf` situado en el directorio `/etc/mysql/`. Le añadiremos la siguiente línea:

```
bind-address = 127.0.0.1
```

Esta directiva establece que el servidor solo escuchará las peticiones provenientes de la propia máquina donde se encuentra instalado. Deberemos también asegurarnos que el usuario 'root' tiene asignada una contraseña. En caso contrario podremos asignarle una mediante el siguiente comando:

```
sudo mysqladmin -u root password "newpassword"
```

Lo siguiente que haremos es crear la base de datos para nuestro sitio web y otorgarle derechos sobre la misma a un nuevo usuario. Evitaremos así el tener que acceder al servidor como usuario 'root' con los peligros que ello conlleva. Para ello bastará con ejecutar los siguientes comandos:

```
mysql -u root -p

mysql> CREATE DATABASE redes;
mysql> GRANT ALL ON redes.* TO 'user'@'localhost' IDENTIFIED BY 'password';
mysql> exit
```

Deberemos sustituir 'user' y 'password' por sus valores correspondientes e introducir estos valores en el archivo de configuración de la aplicación web. Una vez

hecho todo lo anterior, el siguiente comando terminara de crear la base de datos por nosotros.

```
sudo php /var/www/redes/admin/instala_db.php
```

Podremos volver a ejecutar dicho comando cada vez que hagamos un cambio en el archivo `configuracion.php`, si bien hay que tener en cuenta que ésto borrara todos los datos de la base de datos por lo que se recomienda precaución. Tras usar este comando será necesario vaciar la carpeta `/home/labredes/configuraciones/usuarios/`.

6.1.4.3. Configuración de PHP

Encontraremos el archivo de configuración de PHP, `php.ini`, en el directorio `/etc/php5/apache2/`. Debido principalmente a motivos de seguridad será necesario el modificar el valor de las siguientes directivas:

- `register_globals = Off`. Si se encontrara activa, esta directiva podría inyectar los scripts con todo tipo de variables, como variables de peticiones provenientes de formularios HTML.
- `allow_url_fopen = Off`. El resultado de permitir este tipo de peticiones es que si en lugar de indicar en la petición el fichero `index.php` especificamos por ejemplo, `/etc/passwd`, podríamos abrir cualquier fichero del servidor.
- `enable_dl = Off`. PHP puede cargar módulos desde programas usando la función `dl()` desde un script. Existen sin embargo complicaciones de seguridad derivadas del uso de esta función.
- `expose_php = Off`. Esto evitará el envío de información sobre PHP en las cabeceras del servidor web.
- `disable_functions` y `disable_classes`. Mediante el uso de estas directivas es posible deshabilitar el uso funciones y clases potencialmente peligrosas si estas no son usadas en nuestros scripts. Deshabilitaremos el uso de las siguientes funciones:
  - `openlog`
  - `apache_child_terminate`
  - `apache_get_modules`

- `apache_get_version`
- `apache_getenv`
- `apache_note`
- `apache_setenv`
- `virtual`

- `error_reporting = E_ALL` y `log_errors = On`. Con estas directivas activamos las opciones de registro.
- `display_errors = Off` y `display_startup_errors = Off`. Desactivamos la opción de mostrar los errores de inicialización y ejecución de PHP al usuario.
- `memory_limit = 128M`. Estableceremos un limite en la cantidad de memoria que puede consumir un script.
- `post_max_size = 8M` y `upload_max_filesize = 2M`. También podemos establecer el tamaño máximo de las peticiones POST y los archivos subidos al servidor.

6.1.4.4. Configuración de PHPMyAdmin

PHPMyAdmin es una herramienta escrita en PHP que nos permitirá administrar las bases de datos MySQL de manera remota a través de páginas web. Si bien, tendremos que tomar medidas para evitar poner en compromiso la seguridad del sistema. Estas medidas consisten en limitar el acceso a la aplicación a determinados hosts. Para ello editaremos el archivo `apache.conf` situado en el directorio `/etc/phpmyadmin/`. Añadiremos las siguientes líneas entre las etiquetas `<Directory>` y `<Directory>`:

```
Order Allow,Deny
Allow from 127.0.0.1
```

Podremos especificar múltiples direcciones IPs o redes (IP/Máscara) según nuestras necesidades.

6.1.5. Servidor TFTP

En este apartado veremos como instalar y configurar el servidor TFTP (Trivial File Transfer Protocol), el cual, en nuestro caso, será utilizado para la transferencia

de archivos desde y hacia los conmutadores.

Para realizar la instalación bastará con ejecutar el comando:

```
apt-get install tftpd-hpa
```

Después de instalar el paquete deberemos configurar los parámetros de arranque del demonio tftpd. El archivo de configuración `/etc/default/tftpd-hpa` contiene las configuraciones globales para el arranque del demonio tftpd, entre ellas la forma como será inicializado. Por defecto su contenido es el siguiente:

```
RUN_DAEMON="no"
OPTIONS="-l -s /var/lib/tftpboot"
```

`RUN_DAEMON="no"` indica que el servidor no será iniciado como un demonio standalone, ésto es porque puede ser inicializado por el superdemonio inetd o xinetd. En nuestro caso cambiaremos esta opción. El archivo resultante quedará así:

```
RUN_DAEMON="yes"
OPTIONS="-c -l -s /tftpboot"
```

Como se puede ver también hemos cambiado algunas de las opciones como por ejemplo el directorio de inicio del servidor. Deberemos por tanto crear dicho directorio y asignarle los permisos adecuados:

```
sudo mkdir /tftpboot
sudo chmod 777 /tftpboot
```

Por último, será necesario el comentar la línea correspondiente al servicio TFTP en el archivo `/etc/inted.conf`. Después no queda más que reiniciar el sistema.

6.1.6. Administración del sistema

6.1.6.1. Logs de la aplicación

La aplicación web hace uso de un archivo de log que creará por defecto en el direcotorio `/var/log/labredes/`. Haremos uso de la herramienta **logrotate** para así tener un mayor control sobre el tamaño y la antigüedad del archivo de log. El primer paso será el instalara dicha herramienta mediante:

```
sudo apt-get install logrotate
```

Su archivo estándar de configuración es `/etc/logrotate.conf`, pero se pueden especificar múltiples archivos de configuración (o directorios incluyendo archivos de configuración). En los sistemas Debian el directorio `/etc/logrotate.d` es un lugar estándar para los archivos de configuración de logrotate. Todo lo que tendremos que hacer entonces es crear en dicho directorio el archivo de configuración para nuestro archivo de log. Crearemos pues el archivo labredes el cual tendrá el siguiente aspecto:

```
/var/log/labredes/labredes.log {
  monthly
  missingok
  rotate 12
  compress
  delaycompress
  notifempty
  create 664 www-data www-data
}
```

En el se especifica que se rote el archivo de log mensualmente y se mantengan los 12 últimos creados.

6.1.6.2. Copias de seguridad

Para las tareas de respaldo del sistema se ha creado un script (`labredes_backup.sh`) que creará una copia de seguridad de la carpeta con las configuraciones de los usuarios y de la base de datos de la aplicación en el directorio `/backups/labredes/`. Haciendo uso de este script junto a **crontab** se creará una copia de seguridad semanalmente.

```
#!/bin/bash

DBUSER="user"
DBPASS="password"
DBHOST="localhost"
DBNAME="redes"

FOLDER="/home/labredes/configuraciones/usuarios/"

BACKUPDIR="/backup/labredes"
NOW=‘date +%Y-%m-%d‘
FILENAME="labredes-"$NOW.tgz

STARTDIR=‘pwd‘
```

```
cd $BACKUPDIR
mkdir temp
cd $BACKUPDIR/temp

tar cf configuraciones.tar $FOLDER

mysqldump --user=$DBUSER --host=$DBHOST --password=$DBPASS --add-drop-table $DBNAME >
     redes_database.sql

tar czf $BACKUPDIR/$FILENAME configuraciones.tar redes_database.sql

rm -r $BACKUPDIR/temp

find $BACKUPDIR -mtime +140 -type f -exec rm '{}' \;

cd $STARTDIR
```

Se he creado también un script que nos permitirá de manera sencilla restaurar la copia de seguridad que se le indique:

```
#!/bin/bash

DBUSER="user"
DBPASS="password"
DBHOST="localhost"
DBNAME="redes"

FOLDER="/home/labredes/configuraciones/usuarios/"

BACKUPDIR="/backup/labredes"
NOW=`date +%Y-%m-%d`
FILENAME="labredes-"$NOW.tgz

STARTDIR=`pwd`

if [ $# -eq 0 ]
  then
    echo ""
    echo "Uso: sh labredes_restore.sh {backupfile.tgz}"
    echo ""
    exit
fi

BACKUPFILE=$1

if [ ! -f "$BACKUPFILE" ]
  then
    echo ""
    echo "No se encuentra el archivo: $BACKUPFILE"
    echo ""
```

```
    exit
fi

cd $BACKUPDIR
mkdir temp
cd $BACKUPDIR/temp


tar xzf $BACKUPFILE

rm -f $FOLDER*

cd /

tar xf $BACKUPDIR/temp/configuraciones.tar

cd $BACKUPDIR/temp

echo "use $DBNAME; source redes_database.sql;" | mysql --password=$DBPASS --user=$DBUSER --
    host=$DBHOST

rm -r $BACKUPDIR/temp

cd $STARTDIR
```

Por último se he optado por llevar un respaldo del sistema completo haciendo uso de la herramienta Clonezilla. Esta copia nos permitirá restaurar el sistema a su estado original en caso de que fuera necesario.

6.2. Subredes de prácticas: PCs

La preparación de los PCs que conforman la subred de prácticas pasa por:

- Instalación del sistema operativo. Al igual que con el servidor web, la opción escogida es Debian GNU/Linux 5.0 'Lenny'. No detallaremos aquí este proceso de instalación.
- Configuración de la red.
- Instalación y puesta en marcha del servidor XML-RPC.
- Creación de una copia de seguridad del sistema.

A la hora de llevar a cabo la configuración de las interfaces de red, debemos recordar que estos PCs dispondrán de dos de ellas, una destinado a la administración mientras que la otra pertenecerá a la subred de prácticas propiamente dicha.

Editaremos pues el archivo `/etc/network/interfaces` para asignarle a la interfaz conectada a la red de administración los valores correspondientes. Si bien no es necesario, podemos también asignar a la otra interfaz una configuración por defecto.

Una vez configurada la red, llevaremos a cabo la instalación del servidor XML-RPC. Este servidor está escrito en python por lo que tendremos que instalar el interprete de python mediante el comando:

```
sudo apt-get install python
```

El servidor XML-RPC incluye un script que automatiza la instalación del mismo, por lo que solo será necesario llamar a dicho script mediante el comando:

```
sudo python instalacdcrpc.py
```

Deberemos eso sí asegurarnos de que el archivo `configeth.py` se encuentre dentro de la carpeta `modules` antes de realizar la instalación.

La configuración del servidor se lleva a cabo a través del archivo `cdcrpc.conf` que tras la instalación encontraremos en el directorio `/etc/`. El archivo deberá tener un aspecto como éste:

```
##############################################################################
# #
# Archivo de configuracion del metaservidor xml, indica que puertos estan#
# activos, que modulos se cargan (uno a uno), y, opcionalmente, el uid #
# de usuario con el que ejecutar ese modulo. #
# #
##############################################################################

#RUTA PARA LOS MODULOS PROPIOS
MODULEPATH = /home/centro/scripts/cdcrpc

#FICHERO DE LOGS
LOGS = /var/log/cdcrpc
#CODIFICACION EN EL ENVIO XMLRPC
ENCODING = iso-8859-15

#MI IP, PARA CASO CON VARIOS INTERFACES, ELEGIR SOLO UNA
MYIP = 192.168.200.201

#IPS PERMITIDAS
ALLOWIP = 192.168.200.1

#SERVICE = PUERTO MODULO [UID]
SERVICE = 7777 configeth
```

```
#OFF -> SIN SALIDA, ON -> MODO DEBUG
VERBOSE = OFF
```

El valor de `MYIP` es la dirección IP asignada a la interfaz conectada a la red de administración y el valor de `ALLOWIP` el de la dirección IP del servidor web. Tanto el valor introducido en `MYIP` como el número de puerto en `SERVICE` deben ser especificados en el archivo de configuración de la aplicación en el servidor web. Ésto es debido a que la aplicación necesita conocer la IP y puerto del servidor XML-RPC para llevar a cabo las peticiones.

Una vez configurado el servidor solo nos resta reiniciar el servicio:

```
sudo service cdcrpc restart
```

Al igual que hicimos con el servidor web, una vez finalizada la instalación y configuración del todo el software, utilizaremos la herramienta Clonezilla para llevar a cabo una copia de seguridad de todo el sistema.

6.3. Subredes de prácticas: Conmutadores

Los modelos de los conmutadores empleados en la red son los siguientes:

- HP ProCurve Switch serie 2510
- HP ProCurve Switch serie 2610

Cuando un usuario envíe un archivo de configuración a un conmutador, la aplicación añadirá al mismo la configuración de la red de administración para así mantener esta red siempre en funcionamiento. La aplicación necesita pues de un archivo de texto por cada uno de los conmutadores de la red que contenga su configuración de administración. Dichos archivos se almacenarán en el directorio `/home/labredes/configuraciones/administracion/` del servidor web.

Lo primero que haremos será conectarnos con el conmutador a través del puerto serie. Para ello usaremos la herramienta **minicom** que podemos instalar haciendo uso de apt-get. Para poder conectarnos al conmutador deberemos configurar los siguientes parámetros de conexión: 9600 / 8 / N / 1 / xon-xoff.

Una vez nos encontremos en la interfaz de línea de comandos del conmutador lo primero será ejecutar lo siguiente:

```
setup
```

Con este comando accederemos a un menú donde podremos establecer la contraseña del administrador. Una vez establecida configuraremos los parámetros de la red de administración de la siguiente manera:

```
config
max-vlans 64
vlan 200
  name "ADMIN"
  forbid 1-24
  untagged 25-28
  ip adress 192.168.200.101 255.255.255.0
  exit
management-vlan 200
spanning-tree 25-28 bpdu-filter
write memory
boot
```

El listado de puertos que pasamos como parámetro al comando `untagged` corresponde con los puertos reservados para la red de administración. Prohibimos que el resto de puertos sean asignados a la vlan de administración mediante el comando `forbid`. Los modelos de los conmutadores empleados en la red difieren en el número máximo de puertos siendo este valor 26 en el modelo 2510 y 28 en el modelo 2610.

A la hora de establecer que puertos reservamos y conectamos a la red de administración debemos tener en cuenta que si bien podemos seleccionar cualquier rango de puertos, se recomienda escoger el mismo rango en todos los conmutadores. Ésto se debe a que solo podremos especificar un solo rango en al archivo de configuración de la aplicación.

Como se puede ver, se ha activado el filtrado de tramas bpdu en los puertos de administración. La razón de ello es evitar que cuando un usuario active el protocolo de spanning-tree en la red, la red de administración no afecte al resultado de dicho protocolo en la subred de prácticas y viceversa.

Una vez reiniciado el conmutador nos volveremos a conectar al mismo. Podremos usar nuevamente el puerto serie, o gracias a que ya se ha definido una dirección IP para la vlan de administración, a través de telnet. Una vez conectados, ejecutamos lo siguiente:

```
copy startup-config tftp 192.168.200.1 conm11.txt
```

Esto copiará la configuración del conmutador en el archivo `conm11.txt` en el servidor TFTP. Moveremos dicho archivo al directorio `/home/labredes/configuraciones/administracion/` y lo editaremos borrando toda línea que no corresponda a la configuración de administración. El archivo resultante tendrá un aspecto similar a:

```
; J9085A Configuration Editor; Created on release #R.11.25

max-vlans 64
snmp-server community "public" Unrestricted
vlan 200
   name "ADMIN"
   forbid 1-24
   untagged 25-28
   ip address 192.168.200.201 255.255.255.0
   exit
vlan 1
   no untagged 25-28
   exit
spanning-tree 25-28 bpdu-filter
management-vlan 200
password manager
```

Las líneas eliminadas son idénticas, por lo general, en todos los conmutadores. Con estas líneas podemos crear el archivo `default.txt` que situaremos en el directorio `/home/labredes/configuraciones/`. éste tendría el siguiente aspecto:

```
hostname "ProCurve Switch"
vlan 1
   name "DEFAULT_VLAN"
   untagged 1-24
   ip address dhcp-bootp
   exit
```

Podremos usar dicho archivo como la configuración por defecto que verá el usuario para los conmutadores de la red. Es posible, si se desea, crear una configuración por defecto distinta para cada uno de los conmutadores siempre y cuando especifiquemos la ruta a los archivos correspondientes en el archivo de configuración de la aplicación.

Con este proceso estamos dividiendo la configuración inicial del conmutador en dos archivos distintos: el primero contiene solo la información de administración; el segundo es una configuración básica que será la que se muestra al usuario como

configuración 'real' del conmutador. El objetivo de todo ello es lograr que, a todos los efectos, la red de administración permanezca invisible para el usuario, el cual solo deberá tener consciencia de la subred de prácticas con la que se encuentre trabajando.