

TRABAJO FINAL DE GRADO

INFRAESTRUCTURA GNU/LINUX

FRANCISCO JOSÉ

MÁRQUEZ BERNAL

Resumen

En este proyecto se presenta el análisis, diseño y construcción sobre cómo desarrollar una infraestructura con equipos GNU/Linux, un servidor y varios clientes, en un escenario de un centro educativo.

Se explicara el proceso de instalación del servidor así como de la configuración de los diferentes servicios que prestará. Se ha elegido la distribución Ubuntu Server 16.04 LTS, que podemos descargar de: <https://www.ubuntu.com/download/server>

Para los clientes se ha escogido la distribución Ubuntu Desktop 16.04, la cual puede ser descarga aquí <https://www.ubuntu.com/download/desktop> en este caso las aplicaciones de carácter educativo que trae de serie son escasas así que nos centraremos en la instalación de dichas aplicaciones.

Además de la parte software también explicaremos como montar la parte hardware, compuesta fundamentalmente de switches y puntos de acceso para dar conexión a las aulas y despachos de un centro educativo. En este caso obviamente todo se hace en base a unos supuestos que nos encontraremos en un centro educativo, ya sea un colegio o un instituto, puesto que no podemos replicarlo con exactitud a través de la virtualización.

Nuestra infraestructura ofrecerá varias herramientas con propósitos educativos como un Moodle, una wiki y un sistema de autenticación remota de usuarios (openLDAP). Aparte ofrecerá servicios básicos como DHCP, antivirus y filtro de contenidos para posibilitar que un profesor prohíba el acceso de determinadas páginas webs a los alumnos.

Como plataforma de virtualización se ha elegido VMWare Workstation Player, una versión gratuita de esta famosa herramienta de virtualización siempre que se use con fines educativos y no comerciales.

Aparte de los aspectos puramente técnicos también se ofrecerán pequeños manuales de incidencias más comunes que un profesor o técnico pudiera encontrarse en un centro. Hemos tenido en cuenta que estas personas pueden no tener una formación en aspectos informáticos como nosotros luego los manuales intentarán emplear una terminología más simple de lo que se pueda ver en el resto del documento.

Palabras clave: Linux, centro educativo, Ubuntu Server, Ubuntu Desktop, VMWare

Summary

This project presents the analysis, design and construction on how to develop an infrastructure with GNU / Linux computers, a server and several clients, in a setting of an educational center.

It will explain the process of installing the server as well as the configuration of the different services it will provide. We have chosen the Ubuntu Server 16.04 LTS distribution, which we can download from: <https://www.ubuntu.com/download/server>

For the clients has been chosen distribution Ubuntu Desktop 16.04, which can be downloaded here <https://www.ubuntu.com/download/desktop> In this case the applications of educational character that comes standard are scarce so we will focus on the installation of such applications.

In addition to the software part we will also explain how to assemble the hardware part, composed mainly of switches and access points to connect to the classrooms and offices of an educational center. In this case obviously everything is done based on some assumptions that we will find in an educational center, be it a school or an institute, since we can't replicate it with accuracy through virtualization.

Our infrastructure will offer several tools for educational purposes such as a Moodle, a wiki and a remote user authentication system (openLDAP). Apart it will offer basic services like DHCP, antivirus and content filter to allow a professor to prohibit the access of certain web pages to the students.

As a virtualization platform, VMWare Workstation Player has been chosen, a free version of this famous virtualization tool whenever it is used for educational and non-commercial purposes.

Apart from the purely technical aspects, there will also be small manuals of the more common problems that a teacher or technician could find in a center. We have taken into account that these people may not have the same knowledge in computers like us so the manuals will try to use simpler terminology than can be seen in the rest of the document.

Keywords: Linux, education center, Ubuntu Server, Ubuntu Desktop, VMWare

Las TIC en la educación

Preámbulo de Alvaro Marchesi, secretario general de la OEI

El desarrollo acelerado de la sociedad de la información está suponiendo retos, impensables hace unos años, para la educación y el aprendizaje. Tal vez lo más relevante sea que nos encontramos con una nueva generación de aprendices que no han tenido que acceder a las nuevas tecnologías, sino que han nacido con ellas y que se enfrentan al conocimiento desde postulados diferentes a los del pasado. Ello supone un desafío enorme para los profesores, la mayoría de ellos inmigrantes digitales, para las escuelas, para los responsables educativos y para los gestores de las políticas públicas relacionadas con la innovación, la tecnología, la ciencia y la educación.

El diseño de los nuevos currículos y la práctica de la enseñanza han de tener en cuenta a sus destinatarios. Como señala el proyecto colectivo iberoamericano para la próxima década Metas Educativas 2021: la educación que queremos para la generación de los Bicentenarios 1 , el análisis de las culturas juveniles es indispensable para afrontar los desafíos de una educación que llegue a todos los alumnos y en la que todos aprenden para integrarse de forma activa en la sociedad. Ello no quiere decir que los objetivos y los contenidos de aprendizaje deban acomodarse a los intereses de los jóvenes, sino que en su concreción es preciso tenerlos en cuenta para incrementar la motivación de los alumnos y lograr que un mayor número de jóvenes con alto riesgo de abandono se mantenga en las aulas durante más tiempo. Para el logro de estos objetivos, la incorporación innovadora de las TIC en la enseñanza es una estrategia que debe reforzarse.

La tarea principal, por tanto, es lograr que los alumnos mejoren sus aprendizajes con la utilización de las tecnologías de la información. Pero ello supone configurar un nuevo escenario en las relaciones entre los profesores, los alumnos y los contenidos de la enseñanza, y hacerlo también en la evaluación de todo el proceso de enseñanza y de aprendizaje. Si difícil es cambiar la forma de enseñar, aún lo es más modificar el sistema habitual utilizado para la evaluación. Por ello, la formación de los profesores para que dispongan de las competencias necesarias que les permitan incorporar de forma natural las TIC en su práctica pedagógica constituye la variable fundamental para garantizar el éxito del esfuerzo emprendido.

Conviene no olvidar que existen importantes diferencias entre los países iberoamericanos y los más desarrollados, pero también entre los propios países de la región e incluso dentro de cada país. Sin embargo, como algunos estudios concluyen, la presencia de ordenadores y conectividad en las escuelas está reduciendo la brecha digital que se observa en las sociedades latinoamericanas, lo que permite albergar esperanzas de que las TIC, junto con otro tipo de iniciativas sociales y educativas, aceleren el logro de las transformaciones necesarias en la educación iberoamericana.

La incorporación de las TIC a la educación exige pensar previamente cuáles son los objetivos y los retos de la educación y determinar posteriormente de qué manera y en qué condiciones la presencia de las TIC en las escuelas contribuye a ellos. Lo primero y más importante es determinar el sentido de las TIC en la educación y cuál es el modelo pedagógico con el que se puede contribuir de forma más directa a mejorar la calidad y la equidad educativa. Por ello es imprescindible establecer la relación de las TIC con el desarrollo en los alumnos de su capacidad para aprender a aprender, para buscar información de forma selectiva, para tener una posición crítica ante la información disponible en la red, para fomentar los encuentros personales entre los iguales y no solo los virtuales, para ayudar a comprender la realidad multicultural iberoamericana y para fomentar los valores de tolerancia, respeto, solidaridad y justicia.

El análisis de las condiciones que facilitan la incorporación de las TIC en los procesos de enseñanza y de aprendizaje de manera innovadora se convierte en una reflexión ineludible. Entre las principales condiciones es preciso tener en cuenta su financiación y sostenibilidad, el desarrollo de contenidos digitales significativos, pertinentes y suficientes, así como la formación de los profesores para que dispongan de las competencias necesarias para su utilización.

La administración y gestión educativa debe tener en cuenta también la penetración de las TIC en los hogares. De esta forma, no solo pueden establecerse nuevas interacciones y actividades en el seno de las familias, sino que abren un canal de comunicación entre la escuela y la familia que favorece la acción conjunta entre ambos agentes educativos.

Ante la magnitud de los retos planteados en todos los países iberoamericanos se impone la necesidad de colaboración. La tarea de la Organización de Estados Iberoamericanos para la Educación, la Ciencia y la Cultura (OEI) es precisamente contribuir a esta cooperación entre todas las instituciones públicas y privadas que tengan voluntad de aportar iniciativas y experiencias. Aprender entre todos es la mejor estrategia para acertar en el proceso de cambio educativo.

Existen ya iniciativas importantes que merece la pena reseñar. Los programas de diferentes países para que todos los niños dispongan de un ordenador; la red de portales educativos de los Ministerios de Educación que ofrece a familia, docentes y alumnos un espacio de conectividad (RELPE); los cursos de formación virtual organizados y promovidos por diferentes instituciones; el desarrollo de sistemas de indicadores a través, entre otros, del Instituto de Innovación y Desarrollo Educativo (IDIE) con sede en São Paulo; los concursos públicos para conocer las mejores experiencias y para premiar a las personas y a las instituciones más comprometidas o que mejores resultados están obteniendo, y las redes de expertos de la OEI, que estimulan la reflexión crítica y la innovación educativa, son algunos de los proyectos que se sitúan ya como una referencia en la región.

El propósito de la OEI es fortalecer estas iniciativas y promover al mismo tiempo la reflexión colectiva y el apoyo a las experiencias innovadoras en este campo. Repensar las implicaciones de la incorporación de la escuela a las TIC y de la entrada de las TIC en la escuela es tan importante como propiciar el desarrollo y la difusión de experiencias innovadoras que muestran la forma en que los nuevos entornos virtuales de aprendizaje pueden ser útiles en las aulas reales.

El impulso a la reflexión colectiva se plantea para ayudar a precisar los modelos educativos y sociales que subyacen en las políticas públicas que pretenden incorporar las TIC en la educación, para captar nuevos aliados públicos y privados en esta tarea, para analizar las condiciones que colaboran al éxito de las TIC en el proceso educativo y para contribuir a que no se pierda de vista que, al final, el objetivo es educar a más y mejores ciudadanos en sociedades más justas y dinámicas.

A su vez, el apoyo a las experiencias innovadoras pretende partir de la práctica en las aulas para identificar aquello que funciona, lo que alcanza los objetivos propuestos y lo que compromete a la comunidad educativa en el esfuerzo por una educación de mayor calidad. La difusión de los ejemplos de buenas prácticas que suponen esas experiencias innovadoras pretende ilusionar a los diferentes actores educativos en la búsqueda de nuevos caminos para mejorar la educación en los nuevos escenarios de la sociedad del conocimiento.

Sumario

1. Objetivos.....	9
2. Diseño.....	10
2.1 Sistema operativo: servidor.....	10
2.2 Sistema operativo: cliente.....	10
2.3 Nuestra red.....	10
3. Escenario.....	11
3.1 Creación de máquinas virtuales.....	11
3.2 Instalación de una máquina virtual.....	12
3.3 Redes en la MV.....	12
4. Servidor.....	13
4.1 Datos básicos.....	13
4.2 Particionado inicial de los discos.....	13
4.3 RAID software.....	14
4.4 Tarjetas de red.....	17
4.5 UFW.....	19
4.5.1 Tabla mangle.....	19
4.5.2 Tabla nat.....	19
4.5.3 Tabla filter.....	20
4.6 NTP.....	21
4.7 BIND.....	21
4.8 DHCP.....	24
4.9 SQUID + SQUIDGUARD.....	25
4.10 ClamAV.....	26
4.11 FTP con SSL/TLS.....	27
4.12 Apache.....	28
4.13 Base de datos.....	29
4.14 Email: Roundcube.....	29
4.14.1 SMTP.....	29
4.14.2 IMAP.....	31
4.14.3 Base de datos.....	32
4.14.4 Instalación de Roundcube.....	32
4.14.5 Comprar un dominio.....	34
4.13 OpenLDAP.....	34
4.13.1 Servidor LDAP.....	35
4.13.2 Configurar autenticación para clientes.....	35
4.13.3 Configurar el demonio slapd.....	35
4.13.4 Crear la estructura.....	36
4.13.5 Añadir un usuario.....	36
4.13.6 Añadir un grupo.....	37
4.14 NFS.....	37
4.14.1 Instalación.....	37
4.14.2 Configuración básica.....	37
4.15 Moodle.....	38
4.15.1 PHP.....	38
4.15.2 Instalación de moodle.....	38
4.15.3 Configuración de la base de datos.....	39
4.15.4 Instalación web.....	39
4.15.5 Últimos cambios.....	40
4.16 OurScrapbook.....	40
4.17 Radius.....	41

4.17.1	Instalación.....	41
4.17.2	Cientes permitidos.....	41
4.17.2	Añadir clientes.....	41
4.17.3	Configurar Método EAP.....	42
4.17.4	Añadir usuarios.....	42
4.17.5	Autenticación LDAP.....	42
4.17.6	Alternativas.....	43
4.18	Instalación por red (pxe).....	43
4.18.1	Primeros pasos.....	43
4.18.2	Añadir nuestros sistemas operativos.....	43
4.19	Copias de seguridad.....	44
4.19.1	Script básico para copias.....	44
4.19.2	Copia de Moodle.....	45
4.19.3	Copia de NFS.....	45
4.19.4	El cron.....	45
4.19.5	Más información.....	46
4.20	Monitorización: Munin.....	46
4.21	Script de configuración inicial.....	47
5.	Cliente.....	52
5.1	Instalación.....	52
5.2	Cliente DHCP.....	52
5.3	Cliente FTP.....	52
5.3.1	Comandos por consola.....	52
5.3.2	Cliente gráfico.....	53
5.4	Cliente LDAP.....	53
5.5	Cliente NFS.....	53
5.6	Instalar por red.....	54
5.7	Paquetería educativa: EduBuntu.....	54
6.	Hardware.....	55
6.1	Rack.....	55
6.1.1	Localización del rack.....	55
6.2	Router.....	55
6.3	Switch principal.....	56
6.3.1	Ejemplo de configuración.....	56
6.4	SAI.....	56
6.5	Elementos secundarios.....	57
6.5.1	Ejemplo: switch en un aula.....	57
6.5.1	Ejemplo: puntos de acceso wifi en la sala de profesores.....	57
6.5.2	Ejemplo: puntos de acceso wifi en un aula.....	58
7.	Clonación de imágenes.....	59
7.1	De disco a disco.....	59
7.1.1	Ventajas e inconvenientes.....	59
7.2	De disco a imagen.....	59
7.2.1	Ventajas e inconvenientes.....	59
8.	Soporte.....	60
8.1	Incidencias de red.....	60
8.1.1	No tengo internet en todo el centro.....	60
8.1.2	No tengo internet en una zona/aula.....	60
8.1.3	No tengo internet en un equipo.....	61
8.1.4	La conexión va muy lenta.....	61
8.1.5	Dejar conectado un equipo al router.....	61
8.2	Incidencias de software.....	62

8.2.1 No me deja entrar con mi usuario de LDAP.....	62
8.2.2 Quiero recuperar los datos de un usuario de LDAP que no existe.....	62
8.2.3 No se hacen las copias de seguridad.....	62
8.2.4 El sistema operativo no arranca.....	62
8.3 Incidencias de hardware.....	63
8.3.1 Un equipo no enciende.....	63
8.3.2 Un switch no enciende.....	63
8.3.3 El RACK está pitando.....	64
9. Bibliografía y referencias.....	65

1. Objetivos

El TFG (Trabajo de Fin de Grado) consiste en el diseño y construcción de una infraestructura de servicios que sirva para dar recursos que posibiliten la integración de software libre y diversos recursos a un centro educativo, ya sea un colegio o un instituto. Podemos imaginarnos este TFG como el proyecto de un profesor que quiere dotar a su colegio de una mínima infraestructura TIC que permite modernizar los métodos educativos.

La infraestructura estará creada, de forma obvia, con máquinas virtuales creadas a partir de la aplicación VMWare Workstation Player, una aplicación la cual, mientras se use para propósitos educativos como este, podemos usarla sin necesidad de pagar por ella.

Crearemos también algunos manuales básicos que expliquen las incidencias y problemas más comunes a los que tendrá que enfrentarse un profesor en su centro.

Los servicios básicos que se ofrecerán serán:

- Gestión de usuarios
- Almacenamiento remoto
- Plataformas educativas como Moodle o una wiki
- Instalación por red
- Copias de seguridad de las aplicaciones principales
- Cortafuegos y filtro de contenidos
- RAID espejo para evitar en la medida de lo posible la degradación y fallos de seguridad de los datos.

El objetivo final de este documento es crear una plantilla básica que permita a un centro tener un mínimo de servicios TIC, pero obviamente en cada centro el aprovechamiento así como el software adicional que uno quiera instalar dependerá únicamente de cada centro.

2. Diseño

2.1 Sistema operativo: servidor

El sistema operativo elegido para el servidor es Ubuntu Server 16.04 LTS. Se había previsto usar Debian, la cual es una distribución sólida como una roca a nivel de software pero resulta más sencillo encontrar funcionalidades y soporte más actualizado para Ubuntu. Se ha escogido la versión LTS puesto que ofrece un soporte a largo plazo, que habitualmente dura unos 5 años.

Para el servidor se ha decidido crear un sistema de RAID 1 o espejo, configurando los discos duros por software (no se puede hacer con virtualización por hardware, obviamente). Esto se ha decidido puesto que así es más sencillo recuperar la información frente a catástrofes y aumenta la seguridad de los datos del servidor.

La instalación inicial será bastante simple. Esta evita actualizaciones de aplicaciones no necesarias para nosotros, las cuales pueden tener riesgos y vulnerabilidades de seguridad. A excepción de la configuración del RAID, usaremos prácticamente todas las opciones por defecto.

2.2 Sistema operativo: cliente

Lo ideal sería usar la distribución EduUbuntu, una versión especial de Ubuntu con muchos paquetes educativos instalados por defecto.

Para este proyecto, por motivos prácticos, se ha decidido usar Ubuntu Desktop 16.04. Es decir, la versión “de casa” de Ubuntu, en lugar de la Server. La principal diferencia son las aplicaciones instaladas de serie así como la inclusión de un entorno gráfico por defecto.

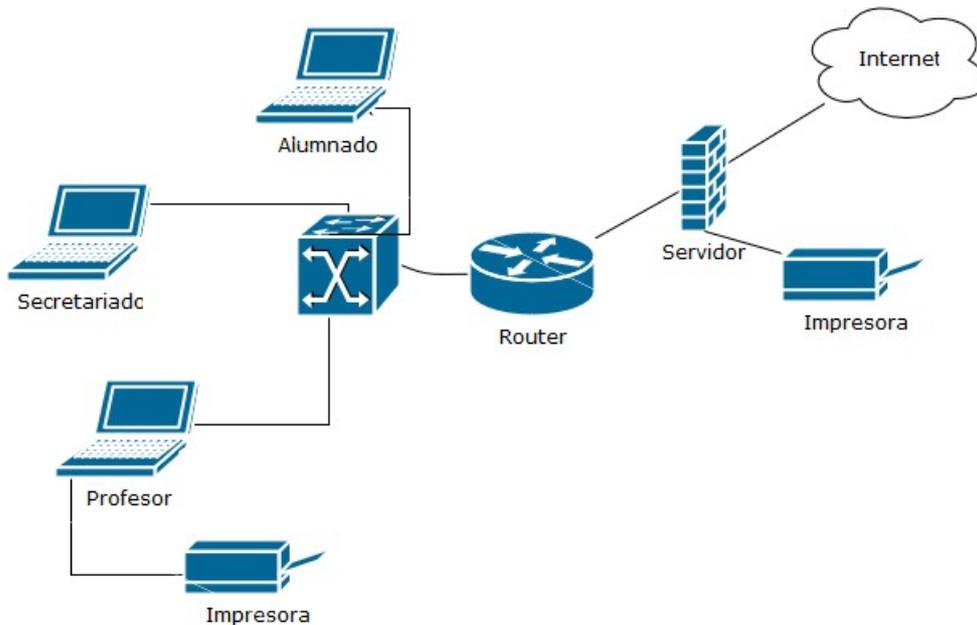
En el apartado correspondiente se explicará cómo instalar una serie de aplicaciones educativas a nuestros equipos clientes. En nuestro proyecto solo hemos usado 2 equipos cliente pero realmente en la práctica, podríamos usar los que queramos, gracias a la virtualización.

2.3 Nuestra red

Hemos desarrollado nuestra red de la siguiente manera:

- Un servidor que hará de cortafuegos y servirá el contenido de diferentes servicios.
- Equipos clientes.
- Una red VLAN para profesores
- Una red VLAN para alumnos
- Una red VLAN para el equipo de gestión (secretaría por ejemplo)

Esta vendría a ser la red de forma simple:



En el esquema además hemos puesto 2 impresoras. Una de red conectada al servidor y otra en la red de profesores.

Se ha diseñado la red de esta manera por lo siguiente:

- Un centro generalmente tiene tres partes diferenciadas: las aulas, los despachos y la zona de gestión/secretaría
- Al tener tres redes diferenciadas se hace más sencilla su administración a la hora de configurar las reglas del cortafuegos
- Aumentamos la seguridad al no tener todos los componentes en la misma red

3. Escenario

Se ha realizado todo mediante máquinas virtuales gracias a VMWARE. A continuación se describen los pasos para tener un escenario como el que se ha ejecutado en el proyecto. En nuestro caso necesitamos:

- Una imagen de Ubuntu Server 16.04
- Una imagen de Ubuntu Desktop 16.04
- La aplicación VMWare Workstation o VMWare Player
- 100G libres en nuestro disco duro aproximadamente
- 8GB de RAM como mínimo

3.1 Creación de máquinas virtuales

Necesitamos crear una máquina virtual para el servidor y otra para el cliente. En nuestro caso hemos creado dos máquinas virtuales para el cliente pero se podrían crear más, o incluso hacerlo con uno si fuera necesario.

3.2 Instalación de una máquina virtual

Para crear una máquina virtual tenemos seguir los siguientes pasos:

- Crear una máquina virtual nueva
- Instalación típica
- Elegimos Linux
- Ponemos nombre a nuestra máquina
- Seleccionamos donde estarán los archivos de la máquina
- Seleccionamos el tamaño del disco duro reservado

Debemos de tener en cuenta un aspecto en concreto para nuestro servidor: el disco duro. Usaremos una configuración RAID 1 software así que necesitamos al menos 2 discos, luego una vez realizados todos los pasos de configuración inicia la de la MV tenemos que hacer lo siguiente:

- Acceder a la configuración de nuestra MV servidor (botón derecho sobre la MV y “settings”).
- Eliminar el disco duro actual.
- Crear dos nuevos discos duros SATA con el mismo tamaño.

En nuestro caso hemos elegido 32G por cada disco duro. Esto es debido a las limitaciones de nuestra máquina real.

3.3 Redes en la MV

Necesitamos configurar nuestra red de máquinas virtuales para que estén en la misma red y que sea el servidor quien haga las veces de cortafuegos/router para que estos accedan a través de él a internet.

Nuestra MV servidor tendrá:

- Una tarjeta de red “NAT”.
- Tres tarjetas de red en una red “custom”, diferente cada una, por ejemplo vmnet1, 2, y 3.

Por ejemplo nosotros hemos hecho esta configuración:

vmnet 1: red de profesores

vmnet 2: red de gestión

vmnet 3: red de alumnos

El orden realmente no es relevante, siempre y cuando se respete la configuración DHCP y de los servicios de red de después.

Nuestras MV clientes tendrán un tarjeta de red “custom”, para la red concreto. Esto dependerá de nuestro cliente, por ejemplo si queremos 2 clientes en alumnos tendremos que poner los dos clientes con la “vmnet 2” configurada.

Es recomendable, no obstante, dejar inicialmente los clientes con la configuración de red por defecto (NAT) para que se pueda descargar las actualizaciones de seguridad de forma rápida. Tras la instalación inicial del sistema operativo ya podremos cambiar la red y trabajar con las redes creadas.

4. Servidor

4.1 Datos básicos

A la hora de instalar el servidor nos centraremos fundamentalmente en el nombre del equipo y la contraseña del super usuario.

A continuación los datos a poner durante la instalación, estos datos son los que hemos usado en el desarrollo de proyecto, pero realmente se podrían poner cualesquiera, son personalizados y no son particularmente importantes:

- Nombre de la máquina: servidor
- Nombre completo para el nuevo usuario: administrador
- Nombre de usuario para la cuenta: servidor
- Contraseña para el nuevo usuario: servidor

Por el momento ignoraremos toda configuración más avanzada como servidores dhcp y similares.

4.2 Particionado inicial de los discos

```
Método de particionado:
Guiado - utilizar todo el disco
Guiado - utilizar el disco completo y configurar LVM
Guiado - utilizar todo el disco y configurar LVM cifrado
Manual
```

Aquí vemos los dos discos duros, inicialmente, de forma obvia, no tienen particiones ni ningún tipo de configuración inicial.

```
Particionado guiado
Configurar los volúmenes iSCSI
SCSI3 (0,0,0) (sda) - 32.2 GB ATA VBOX HARDDISK
SCSI4 (0,0,0) (sdb) - 32.2 GB ATA VBOX HARDDISK
Deshacer los cambios realizados a las particiones
Finalizar el particionado y escribir los cambios en el disco
```

Elegimos los dos y le damos a crear nueva tabla de particiones

```
[!!!] Particionado de discos

Ha seleccionado particionar el dispositivo completo. Si continúa creará una tabla de
particiones en el dispositivo y se eliminarán todas las particiones que existían
previamente.

Observe que podrá deshacer esta operación más adelante si lo desea.

¿Crear una nueva tabla de particiones vacía en este dispositivo?

<Retroceder> <Sí> <No>
```

El resultado final es este

```
SCSI3 (0,0,0) (sda) - 32.2 GB ATA VBOX HARDDISK
pri/lóg 32.2 GB ESPACIO LIBRE
SCSI4 (0,0,0) (sdb) - 32.2 GB ATA VBOX HARDDISK
pri/lóg 32.2 GB ESPACIO LIBRE
```

Ahora seleccionamos el espacio libre del disco “sda” y creamos nuevas particiones. En total crearemos 4 particiones para cada disco, los cuales tendrán un esquema idéntico:

- 4G para la partición /
 - 2G para swap (área de intercambio)
 - 13.2G para la partición /home
 - 13G para la partición /var
- En todos los casos seleccionamos las siguientes opciones:

- Crear una partición nueva
- Primaria
- Volumen físico para RAID

El estado final de los discos sería el siguiente

```
[!!] Particionado de discos

Éste es un resumen de las particiones y puntos de montaje que tiene configurados
actualmente. Seleccione una partición para modificar sus valores (sistema de ficheros,
puntos de montaje, etc.), el espacio libre para añadir una partición nueva o un
dispositivo para inicializar la tabla de particiones.

Particionado guiado
Configurar RAID por software
Configurar el Gestor de Volúmenes Lógicos (LVM)
Configurar los volúmenes cifrados
Configurar los volúmenes iSCSI

SCSI3 (0,0,0) (sda) - 32.2 GB ATA VBOX HARDDISK
#1 primaria 4.0 GB K raid
#2 primaria 2.0 GB K raid
#3 primaria 13.2 GB K raid
#4 primaria 13.0 GB K raid
SCSI4 (0,0,0) (sdb) - 32.2 GB ATA VBOX HARDDISK
#1 primaria 4.0 GB K raid
#2 primaria 2.0 GB K raid
#3 primaria 13.2 GB K raid
#4 primaria 13.0 GB K raid

Deshacer los cambios realizados a las particiones
Finalizar el particionado y escribir los cambios en el disco

<Retroceder>
```

4.3 RAID software

Configuraremos un RAID 1, conocido como “raid espejo”. Seguimos los siguientes pasos:

- Elegimos “Configurar RAID por software”
- Creamos un dispositivo MD de tipo RAID 1 por cada partición
- Número de dispositivos para el array: 2
- Número de dispositivos libres para el array: 0
- Elegimos las dos particiones correspondientes, por parejas, en cada caso.

A continuación el procedimiento explicado:

- Configurar RAID por software
- Desea escribir los cambios en el dispositivo: Sí
- Crear un dispositivo MD
- RAID1
- Número de dispositivos: 2
- Dispositivos libres: 2

Este último paso es realmente importante, podemos ver como se escogen las particiones “parejas”, la sda1 con la sdb1 y así sucesivamente.

```
Ha elegido crear un array RAID1 con 2 dispositivos activos.

Por favor, escoja qué particiones son dispositivos activos. Debe seleccionar 2
particiones.

Dispositivos activos para el array RAID1:

[*] /dev/sda1 (3999MB; raid)
[ ] /dev/sda2 (1999MB; raid)
[ ] /dev/sda3 (13200MB; raid)
[ ] /dev/sda4 (13010MB; raid)
[*] /dev/sdb1 (3999MB; raid)
[ ] /dev/sdb2 (1999MB; raid)
[ ] /dev/sdb3 (13200MB; raid)
[ ] /dev/sdb4 (13010MB; raid)

<Retroceder> <Continuar>
```

El estado final de los discos sería el siguientes

```
[!] Particionado de discos

Éste es un resumen de las particiones y puntos de montaje que tiene configurados
actualmente. Seleccione una partición para modificar sus valores (sistema de ficheros,
puntos de montaje, etc.), el espacio libre para añadir una partición nueva o un
dispositivo para inicializar la tabla de particiones.

Particionado guiado
Configurar RAID por software
Configurar el Gestor de Volúmenes Lógicos (LVM)
Configurar los volúmenes cifrados
Configurar los volúmenes iSCSI

Dispositivo RAID1 #0 - 4.0 GB Dispositivo RAID por software
#1 4.0 GB
Dispositivo RAID1 #1 - 2.0 GB Dispositivo RAID por software
#1 2.0 GB
Dispositivo RAID1 #2 - 13.2 GB Dispositivo RAID por software
#1 13.2 GB
Dispositivo RAID1 #3 - 13.0 GB Dispositivo RAID por software
#1 13.0 GB
SCSI3 (0,0,0) (sda) - 32.2 GB ATA VBOX HARDDISK
#1 primaria 4.0 GB K raid
#2 primaria 2.0 GB K raid
#3 primaria 13.2 GB K raid
#4 primaria 13.0 GB K raid
SCSI4 (0,0,0) (sdb) - 32.2 GB ATA VBOX HARDDISK
#1 primaria 4.0 GB K raid
#2 primaria 2.0 GB K raid
#3 primaria 13.2 GB K raid

<Retroceder>
```

A continuación

debemos de configurar por separado cada uno de nuestros dispositivos RAID, en todos casos la configuración es la misma pero variamos solo el punto de montaje:

4G para la partición /
2G para swap (área de intercambio)
13.2G para la partición /home
13G para la partición /var

El procedimiento sería:

- Seleccionamos el primer dispositivo
- Seleccionamos “sistema de ficheros ext4 transaccional”
- Y el punto de montaje correspondiente

El estado final sería el siguiente

```
[!!] Particionado de discos

Éste es un resumen de las particiones y puntos de montaje que tiene configurados
actualmente. Seleccione una partición para modificar sus valores (sistema de ficheros,
puntos de montaje, etc.), el espacio libre para añadir una partición nueva o un
dispositivo para inicializar la tabla de particiones.

Particionado guiado
Configurar RAID por software
Configurar el Gestor de Volúmenes Lógicos (LVM)
Configurar los volúmenes cifrados
Configurar los volúmenes iSCSI

Dispositivo RAID1 #0 - 4.0 GB Dispositivo RAID por software
#1 4.0 GB f ext4 /
Dispositivo RAID1 #1 - 2.0 GB Dispositivo RAID por software
#1 2.0 GB f intercambio intercambio
Dispositivo RAID1 #2 - 13.2 GB Dispositivo RAID por software
#1 13.2 GB f ext4 /home
Dispositivo RAID1 #3 - 13.0 GB Dispositivo RAID por software
#1 13.0 GB f ext4 /var
SCSI3 (0,0,0) (sda) - 32.2 GB ATA VBOX HARDDISK
#1 primaria 4.0 GB K raid
#2 primaria 2.0 GB K raid
#3 primaria 13.2 GB K raid
#4 primaria 13.0 GB K raid
SCSI4 (0,0,0) (sdb) - 32.2 GB ATA VBOX HARDDISK
#1 primaria 4.0 GB K raid
#2 primaria 2.0 GB K raid
#3 primaria 13.2 GB K raid

<Retroceder>
```

Entonces le damos a “Finalizar el particionado y escribir los cambios en el disco”. Y luego le confirmamos que queremos escribir los cambios.

Con el servidor arrancado si ejecutamos el comando siguiente podemos ver el estado del RAID, el cual debería de ser correcto obviamente correcto

```

root@servidor:~# cat /proc/mdstat
Personalities : [raid1] [linear] [multipath] [raid0] [raid6] [raid5] [raid4] [raid10]
md1 : active raid1 sdb2[1] sda2[0]
      1951744 blocks super 1.2 [2/2] [UU]

md0 : active raid1 sdb1[1] sda1[0]
      3903488 blocks super 1.2 [2/2] [UU]

md2 : active raid1 sdb3[1] sda3[0]
      12882944 blocks super 1.2 [2/2] [UU]

md3 : active raid1 sdb4[1] sda4[0]
      12697600 blocks super 1.2 [2/2] [UU]

unused devices: <none>

```

Y el estado de los sistemas de ficheros

```

root@servidor:~# df -h
S.ficheros      Tamaño Usados  Disp Uso% Montado en
udev            981M   0      981M  0% /dev
tmpfs           201M   3,2M   197M  2% /run
/dev/md0        3,7G   1,1G   2,4G  33% /
tmpfs           1001M   0     1001M  0% /dev/shm
tmpfs           5,0M   0      5,0M  0% /run/lock
tmpfs           1001M   0     1001M  0% /sys/fs/cgroup
/dev/md2        12G    31M    12G   1% /home
/dev/md3        12G   330M    11G   3% /var
tmpfs           201M   0      201M  0% /run/user/1000
root@servidor:~#

```

4.4 Tarjetas de red

El siguiente paso será configurar las tarjetas de red de nuestro servidor. Para ello editamos el fichero `/etc/network/interfaces` de la siguiente manera.

```

#Interfaz conectada al router
auto eth0
iface eth0 inet static
    address 10.227.20.114 #Ip del router+1
    broadcast 10.227.20.127
    netmask 255.255.255.192
    network 10.227.20.64
    gateway 10.227.20.65
    ip_proxy_arp 1

#Interfaz de gestión
auto eth1
iface eth1 inet static
    address 192.168.4.1
    broadcast 192.168.7.255
    netmask 255.255.252.0
    network 192.168.4.0

#interfaz de alumnado
auto eth2
iface eth2 inet static
    address 192.168.8.1
    broadcast 192.168.15.255

```

```
netmask 255.255.248.0
network 192.168.8.0

#interfaz de profesores
auto eth3
  iface eth3 inet static
  address 192.168.0.1
  broadcast 192.168.3.255
  netmask 255.255.252.0
  network 192.168.0.0
```

Ojo, debemos de tener en cuenta que esta configuración sería en caso de tener un servidor real. En el caso de VMWare las tarjetas se nombran como “ens33” y sucesivas así que tendremos que cambiar los correspondientes “ethX” por “ensXX”.

En el caso de la eth0 directamente debe ser eliminada dado que obviamente la necesitamos para que el servidor virtual tenga conexión a través de nuestro equipo real. La configuración aquí puesta para la eth0 es solo un ejemplo.

Podemos ver como las redes se quedan así:

```
Gestión → 192.168.4-7.X
Alumnos → 192.168.8-15.X
Profesores → 192.168.0-3.X
```

La red de alumnos es la más grande puesto que se entiende que habrá mucho más alumnos que profesores en un centro.

También podemos ver que la configuración de la eth0 dependerá de nuestro router. Un ejemplo:

Ip de nuestro router: 10.227.20.113 → Ip de la eth0 del servidor: 10.227.20.114 → ip router +1

Un ejemplo de como queda la configuración con un pantallazo:

```
ens39    Link encap:Ethernet direcciónHW 00:0c:29:7a:e7:14
        Direc. inet:192.168.4.1 Difus.:192.168.7.255 Másc:255.255.252.0
        Dirección inet6: fe80::20c:29ff:fe7a:e714/64 Alcance:Enlace
        ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
        Paquetes RX:19 errores:0 perdidos:0 overruns:0 frame:0
        Paquetes TX:235 errores:0 perdidos:0 overruns:0 carrier:0
        colisiones:0 long.colaTX:1000
        Bytes RX:3150 (3.1 KB) TX bytes:38486 (38.4 KB)

ens40    Link encap:Ethernet direcciónHW 00:0c:29:7a:e7:1e
        Direc. inet:192.168.8.1 Difus.:192.168.15.255 Másc:255.255.248.0
        Dirección inet6: fe80::20c:29ff:fe7a:e71e/64 Alcance:Enlace
        ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
        Paquetes RX:19 errores:0 perdidos:0 overruns:0 frame:0
        Paquetes TX:272 errores:0 perdidos:0 overruns:0 carrier:0
        colisiones:0 long.colaTX:1000
        Bytes RX:3150 (3.1 KB) TX bytes:45322 (45.3 KB)
```

4.5 UFW

Es un cortafuegos sencillo de usar, viene instalado por defecto pero en caso de que no venga usar el comando siguiente para instalarlo:

```
apt-get install ufw
```

A continuación se describe la configuración de las iptables. Es MUY recomendable no aplicar esta configuración hasta el final de la completa instalación del servidor. Esta configuración es opcional y sujeta a las particularidades de cada centro.

4.5.1 Tabla mangle

Se encarga de modificar los paquetes.

```
*mangle
:PREROUTING ACCEPT [46313:7266649]
:INPUT ACCEPT [38608:5427585]
:FORWARD ACCEPT [4615:1844548]
:OUTPUT ACCEPT [40527:11522906]
:POSTROUTING ACCEPT [45142:13367454]
```

4.5.2 Tabla nat

Las tablas NAT (Network Address Translation), es decir, traducción de direcciones de red, serán consultadas cuando un paquete cree una nueva conexión. Permiten compartir una IP pública entre muchos equipos, por lo que resultan imprescindibles en el protocolo IPv4.

```
*nat
:PREROUTING ACCEPT [117:8697]
:POSTROUTING ACCEPT [22:1416]
:OUTPUT ACCEPT [22:1416]
:PROFESORADO_PRE - [0:0]
:PROFESORADO_POS - [0:0]
:GESTION_PRE - [0:0]
:GESTION_POS - [0:0]
:ALUMNADO_PRE - [0:0]
:ALUMNADO_POS - [0:0]
-A PREROUTING -s 192.168.0.0/22 -j PROFESORADO_PRE
-A PREROUTING -s 192.168.4.0/22 -j GESTION_PRE
-A PREROUTING -s 192.168.8.0/21 -j ALUMNADO_PRE
-A PROFESORADO_PRE ! -d 192.168.0.1 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 8080
-A GESTION_PRE ! -d 192.168.4.1 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 8080
-A ALUMNADO_PRE ! -d 192.168.8.1 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 8080
-A POSTROUTING -s 192.168.0.0/22 -j PROFESORADO_POS
-A POSTROUTING -s 192.168.4.0/22 -j GESTION_POS
-A POSTROUTING -s 192.168.8.0/21 -j ALUMNADO_POS
-A PROFESORADO_POS -o eth0 -j MASQUERADE
-A GESTION_POS -o eth0 -j MASQUERADE
-A ALUMNADO_POS -o eth0 -j MASQUERADE
```

4.5.3 Tabla filter

Las tablas de filtrado se usan por defecto para gestionar paquetes de datos. Estas son las más usadas y son responsables del filtrado de los paquetes según se ha configurado el cortafuegos o filtro. Todos los paquetes pasan a través de esta tabla.

```
*filter
:INPUT DROP [2:656]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [3627:435302]
:LOCAL_IN - [0:0]
:LOCAL_FW - [0:0]
:ALUMNADO_IN - [0:0]
:ALUMNADO_FW - [0:0]
:GESTION_IN - [0:0]
:GESTION_FW - [0:0]
:PROFESORADO_IN - [0:0]
:PROFESORADO_FW - [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -s 127.0.0.0/8 -j ACCEPT
-A INPUT -j LOCAL_IN
-A INPUT -s f0 -j ACCEPT
-A INPUT -p icmp --icmp-type echo-request -j ACCEPT
-A INPUT -s 192.168.4.0/22 -j GESTION_IN
-A GESTION_IN -p tcp -m multiport --dports
21,53,80,111,389,443,873,8080,8180,30000,50000 -j ACCEPT
-A GESTION_IN -p tcp -m tcp --sport 1024:65535 --dport 20:65535 -m conntrack
--ctstate NEW,ESTABLISHED -j ACCEPT
-A GESTION -p udp -m udp --dport 1812 -j ACCEPT
-A INPUT -s 192.168.8.0/21 -j ALUMNADO_IN
-A ALUMNADO_IN -p tcp -m multiport --dports
21,53,80,111,389,443,873,8080,8180,30000,50000 -j ACCEPT
-A ALUMNADO_IN -p tcp -m tcp --sport 1024:65535 --dport 20:65535 -m conntrack
--ctstate NEW,ESTABLISHED -j ACCEPT
-A ALUMNADO -p udp -m udp --dport 1812 -j ACCEPT
-A INPUT -s 192.168.0.0/22 -j PROFESORADO_IN
-A PROFESORADO_IN -p tcp -m multiport --dports
21,53,80,111,389,443,873,8080,8180,30000,50000 -j ACCEPT
-A PROFESORADO_IN -p tcp -m tcp --sport 1024:65535 --dport 20:65535 -m conntrack
--ctstate NEW,ESTABLISHED -j ACCEPT
-A PROFESORADO -p udp -m udp --dport 1812 -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -j LOCAL_FW
-A FORWARD -s 192.168.0.0/22 -j PROFESORADO_FW
-A FORWARD -s 192.168.4.0/22 -j GESTION_FW
-A FORWARD -s 192.168.8.0/21 -j ALUMNADO_FW
-A ALUMNADO_FW -p tcp -m multiport --dports
21,25,80,110,143,443,465,554,993,995,8080,8180,8900,9000 -j ACCEPT
-A ALUMNADO_FW -j DROP
-A GESTION_FW -j ACCEPT
-A PROFESORADO_FW -j ACCEPT
```

4.6 NTP

Es un protocolo de internet para sincronizar los relojes de los sistemas informáticos. Nos servirá para que todos los equipos, clientes y servidores, tengan la hora correcta y se sincronice de forma automática. Esto evita que un usuario cambie la hora sin motivo.

Comando de instalación: `apt-get -y install ntp`

Fichero de configuración → `/etc/ntp.conf`

En dicho fichero comentamos las líneas siguientes:

```
pool 0.ubuntu.pool.ntp.org iburst
pool 1.ubuntu.pool.ntp.org iburst
pool 2.ubuntu.pool.ntp.org iburst
pool 3.ubuntu.pool.ntp.org iburst
```

Añadimos servidores españoles

```
server 2.es.pool.ntp.org
server 1.europe.pool.ntp.org
server 2.europe.pool.ntp.org
```

Comando para reiniciar el servicio

```
systemctl restart ntp
```

Comando para ver el estado del servicio

```
ntpq -p
```

4.7 BIND

Nos permite configurar un servidor DNS. Este sistema asocia información variada con nombre de dominio asignado a cada uno de los participantes. Su función más importante es "traducir" nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.¹

Nosotros lo usaremos para que en nuestro centro podamos acceder a diversas direcciones por el nombre en lugar de la ip, lo que sería engorroso. Por ejemplo definiremos una para la red de alumnado y otra para la de profesores.

Comando para instalar: `apt-get -y install bind9 bind9utils`

Fichero `/etc/bind/named.conf` → Lo dejamos tal y como esta

En el fichero `/etc/bind/named.conf.default-zones` añadimos las siguientes líneas al inicio (tras el comentario inicial con //):

```
view "local" {
```

¹ https://es.wikipedia.org/wiki/Sistema_de_nombres_de_dominio

```
match-clients { "acl-interna"; };
recursion yes;
```

En el fichero */etc/bind/named.conf.local*

```
acl acl-interna {
    127.0.0.0/8;
    87.219.218.237/27 #Nuestra IP (en el caso de VM no coincide claro)
};

acl acl-alumnos {
    192.168.8.0/21;
};

acl acl-gestion {
    192.168.4.0/22;
};

acl acl-profesores {
    192.168.0.0/22;
};

view "interna" {
    match-clients { acl-interna; };
    recursion yes;

    // add entries for other zones below here

    zone "12345678a.12.uoc.tfg.trabajo-uoc.es" {
        type master;
        file "/etc/bind/db.red-interna";
    };

    zone "168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192.168";
    };
};

view "profesores" {
    match-clients { acl-profesores; };
    recursion yes;

    // add entries for other zones below here

    zone "12345678a.12.uoc.tfg.trabajo-uoc.es" {
        type master;
        file "/etc/bind/db.red-profesores";
    };

    zone "168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192.168";
    };
};

view "externa" {
    match-clients { any; };
    recursion no;

    // add entries for other zones below here

    zone "12345678a.12.uoc.tfg.trabajo-uoc.es" {
        type master;
```

```

        file "/etc/bind/db.red-externa";
    };
};

```

Creamos el fichero /etc/bind/db.red-alumnos

```

$ttl 86400
@      IN      SOA      ns.12345678a.12.uoc.tfg.trabajo-uoc.es
uoc\.universidad.uoc.es. (
    2012022201
    4h
    1h
    2w
    1h )

```

```
$INCLUDE /etc/bind/db.custom
```

```

ns      IN      NS      ns
ns      IN      A      192.168.8.1
dns     IN      CNAME   ns
servidor IN    CNAME   ns
ntp     IN      CNAME   ns
aptproxy IN  CNAME   c0
ldap   IN      A      192.168.8.1
      IN      A      192.168.8.2

```

Creamos el fichero /etc/bind/db.red-gestion

```

$ttl 86400
@      IN      SOA      ns.12345678a.12.uoc.tfg.trabajo-uoc.es
uoc\.universidad.uoc.es. (
    2012022201
    4h
    1h
    2w
    1h )

```

```
$INCLUDE /etc/bind/db.custom
```

```

ns      IN      NS      ns
ns      IN      A      192.168.4.1
dns     IN      CNAME   ns
servidor IN    CNAME   ns
ntp     IN      CNAME   ns
aptproxy IN  CNAME   c0
ldap   IN      A      192.168.4.1
      IN      A      192.168.4.2
switch IN      A      192.168.4.50

```

Creamos el fichero /etc/bind/db.red-profesores

```

$ttl 86400
@      IN      SOA      ns.12345678a.12.uoc.tfg.trabajo-uoc.es
uoc\.universidad.uoc.es. (
    2012022201
    4h
    1h
    2w
    1h )

```

```
$INCLUDE /etc/bind/db.custom
```

```

ns          IN      NS      ns
ns          IN      A        192.168.0.1
dns        IN      CNAME    ns
servidor   IN      IN        CNAME    ns      ns
ntp        IN      CNAME    ns
aptproxy   IN      CNAME    c0
ldap       IN      A        192.168.0.1
           IN      A        192.168.0.2

```

Creamos el fichero /etc/bind/db.red-interna

```

$ttl 86400
@      IN      SOA      ns.12345678a.12.uoc.tfg.trabajo-uoc.es
uoc\.universidad.uoc.es. (
      2012022201
      4h
      1h
      2w
      1h )

```

```
$INCLUDE /etc/bind/db.custom
```

```

router     IN      NS      ns
router     IN      A        87.219.218.1 #Nuestra IP del router
sustituir por la que sea
ns         IN      A        87.219.218.113
dns        IN      CNAME    ns
servidor   IN      IN        CNAME    ns      ns
ntp        IN      CNAME    ns
ldap       IN      A        87.219.218.113

```

Para reiniciar este servicio usamos el comando `/etc/init.d/bind9 restart`

4.8 DHCP

Comando para instalar: `apt-get -y install isc-dhcp-server`

Fichero de configuración → `/etc/dhcp/dhcpd.conf`

```

ddns-update-style none;
stash-agent-options true;
update-conflict-detection true;
option domain-name "12345678a.12.uoc.tfg.trabajo-uoc.es";

default-lease-time 15552000;      # Seis meses
max-lease-time 15552000;        # Seis meses
authoritative;
# Proporcionar hostname a los clientes
get-lease-hostnames false;
# Declaracion de la subred para Alumnos
subnet 192.168.8.0 netmask 255.255.248.0 {
    range 192.168.8.51 192.168.8.254;
    range 192.168.9.1 192.168.9.254;
    range 192.168.10.1 192.168.10.254;
    range 192.168.11.1 192.168.11.254;
    range 192.168.12.1 192.168.12.254;
    range 192.168.13.1 192.168.13.254;
    range 192.168.14.1 192.168.14.254;
}

```

```

    range 192.168.15.1 192.168.15.254;
    option routers 192.168.8.1;
    option subnet-mask 255.255.248.0;
    option broadcast-address 192.168.15.255;
    option domain-name-servers 192.168.8.1, 192.168.8.2;
    deny duplicates;
}
# Declaracion de la subred para Gestion
subnet 192.168.4.0 netmask 255.255.252.0 {
    range 192.168.4.51 192.168.4.254;
    range 192.168.5.51 192.168.5.254;
    range 192.168.6.1 192.168.6.254;
    range 192.168.7.1 192.168.7.254;
    option routers 192.168.4.1;
    option subnet-mask 255.255.252.0;
    option broadcast-address 192.168.7.255;
    option domain-name-servers 192.168.4.1, 192.168.4.2;
    deny duplicates;
}
# Declaracion de la subred para Profesores
subnet 192.168.0.0 netmask 255.255.252.0 {
    range 192.168.0.51 192.168.0.254;
    range 192.168.1.1 192.168.1.254;
    range 192.168.2.1 192.168.2.254;
    range 192.168.3.1 192.168.3.254;
    option routers 192.168.0.1;
    option subnet-mask 255.255.252.0;
    option broadcast-address 192.168.3.255;
    option domain-name-servers 192.168.0.1, 192.168.0.2;
}

#Para la instalación por red
next-server servidor;
filename "pxelinux.bin";

```

Comando para reiniciar el servicio → *systemctl restart isc-dhcp-server*

Como podemos observar determinados rangos no empiezan en el “1” si no en el 51, por ejemplo la 192.168.4.51. El motivo es que en nuestro centro tendremos elementos de red como switches, puntos de acceso, impresoras, discos duros... para que sea más sencilla su configuración reservamos las primeras direcciones para ellos. Por ejemplo:

- Una impresora con ip fija en la 192.168.0.35
- Un punto de acceso con ip fija en la 192.168.4.36

4.9 SQUID + SQUIDGUARD

Squid es un servidor proxy para web con caché.

Comando para instalar → *apt-get -y install squid*

Lo usaremos en conjunto con Squidguard, que permite listas negras para evitar que nuestros clientes entren en webs concretas.

Comando para instalar → *apt-get install -y squidguard*

Configuramos el fichero → */etc/squidguard/squidGuard.conf*

```

dbhome /var/lib/squidguard/db
logdir /var/log/squidguard
dest deny {
    # Categoria "deny" para dominios prohibidos

    domainlist deny/domains
    # En este caso es para URL, no dominios

    urllist deny/urls
}
acl {
    default {
        # permit all except 'deny' category

        pass !deny all
        # redirigimos a una página si está prohibida
        redirect www.google.es
    }
}

```

Ahora haremos lo siguiente:

```

mkdir /var/lib/squidguard/db/deny
nano /var/lib/squidguard/db/deny/domains

```

Aquí podremos escribir nuestros dominios prohibidos. Ejemplo:

direccion.es

En el caso del fichero `/var/lib/squidguard/db/deny/urls` nos sirve para URL concretas como:

www.pagina.es/loquesea/

Tras esto ejecutamos los siguientes comandos:

```

squidGuard -C all
chown -R proxy. /var/lib/squidguard /var/log/squidguard

```

Y ahora debemos decirle a “Squid” que use squidguard así que en el fichero `/etc/squid/squid.conf` añadimos la línea:

```

url_rewrite_program /usr/bin/squidGuard

```

Tras esto reiniciamos el servicio squid: `systemctl restart squid`

Observación: si tras el comando `squidGuard -C all` nos da un error debemos de revisar los ficheros de las url y los dominios para ver si hay algún fallo.

4.10 ClamAV

Es un antivirus útil para Linux.

Comando para instalar → `apt-get -y install clamav`

Fichero de configuración: `/etc/clamav/freshclam.conf`. En este fichero comentamos la línea siguiente:

```
NotifyClamd /etc/clamav/clamd.conf
```

Ahora podemos escanear si queremos, por ejemplo con el comando siguiente, en función de lo que queramos escanear varía el directorio: `clamscan --infected --remove --recursive /home`

Es posible que nos de un error, eso es debido a que se estará actualizando la base de datos y hay que esperar un poco. Para realizar este proceso de forma manual se usa el comando `freshclam` pero es muy probable que nada más instalar haya que esperarse unos minutos a que este comando funcione correctamente. El log de este servicio es: `/var/log/clamav/freshclam.log`

Para hacer una prueba nos descargamos un virus (acordarse de borrarlo después):

```
wget http://www.eicar.org/download/eicar.com
clamscan --infected --remove --recursive ./
```

4.11 FTP con SSL/TLS

Útil para la transferencia de ficheros. Actualmente está en desuso pero aquí se explica su instalación y configuración por si se quiere tener instalado. Además, es imprescindible para la instalación por red, así que en este caso concreto si que tenemos que instalarlo.

Comando para su instalación: `apt-get -y install proftpd`

Debemos de seleccionar la opción de configuración: independiente (standalone).

En el fichero de configuración podemos desactivar el uso de ipv6:

```
# Set off to disable IPv6 support which is annoying on IPv4 only boxes.
UseIPv6                                off
```

Y también tenemos que cambiar el nombre de nuestro servidor, en este caso concreto es “servidor” pero hay que poner el que convenga, si es que hemos elegido otro:

```
ServerName                               servidor
```

Comando para reiniciar el servicio → `systemctl restart proftpd`

Pero no hemos terminado, para tener seguridad extra podemos, si lo queremos, configurar SSL. Obviamente si hacemos esto en el cliente deberemos de realizar lo propio pero eso lo explicaremos más adelante.

El procedimiento en el servidor es el siguiente:

Ir al directorio → `cd /etc/ssl/private`

Crear clave → `openssl req -x509 -nodes -newkey rsa:2048 -keyout proftpd.pem -out proftpd.pem -days 365`

La configuración sería por ejemplo:

```
Country Name (2 letter code) [AU]:ES
```

```
State or Province Name (full name) [Some-State]:Sevilla
Locality Name (eg, city) []:Sevilla
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UOC
Organizational Unit Name (eg, section) []:UOC
Common Name (e.g. server FQDN or YOUR name) []:servidor
Email Address []:administrador@uoc.es
```

Dar los permisos adecuados → `chmod 600 proftpd.pem`

Ahora en el fichero siguiente `/etc/proftpd/proftpd.conf` descomentamos la siguiente línea:

Include /etc/proftpd/tls.conf

Y en el `/etc/proftpd/tls.conf` descomentamos:

```
TLSEngine                on
TLSLog                   /var/log/proftpd/tls.log
TLSProtocol               SSLv23
TLRSACertificateFile     /etc/ssl/private/proftpd.pem
TLRSACertificateKeyFile  /etc/ssl/private/proftpd.pem
```

4.12 Apache

Es un servidor web HTTP, el cual nos será muy útil para diversos servicios que montaremos después.

Comando para su instalación → `apt-get -y install apache2`

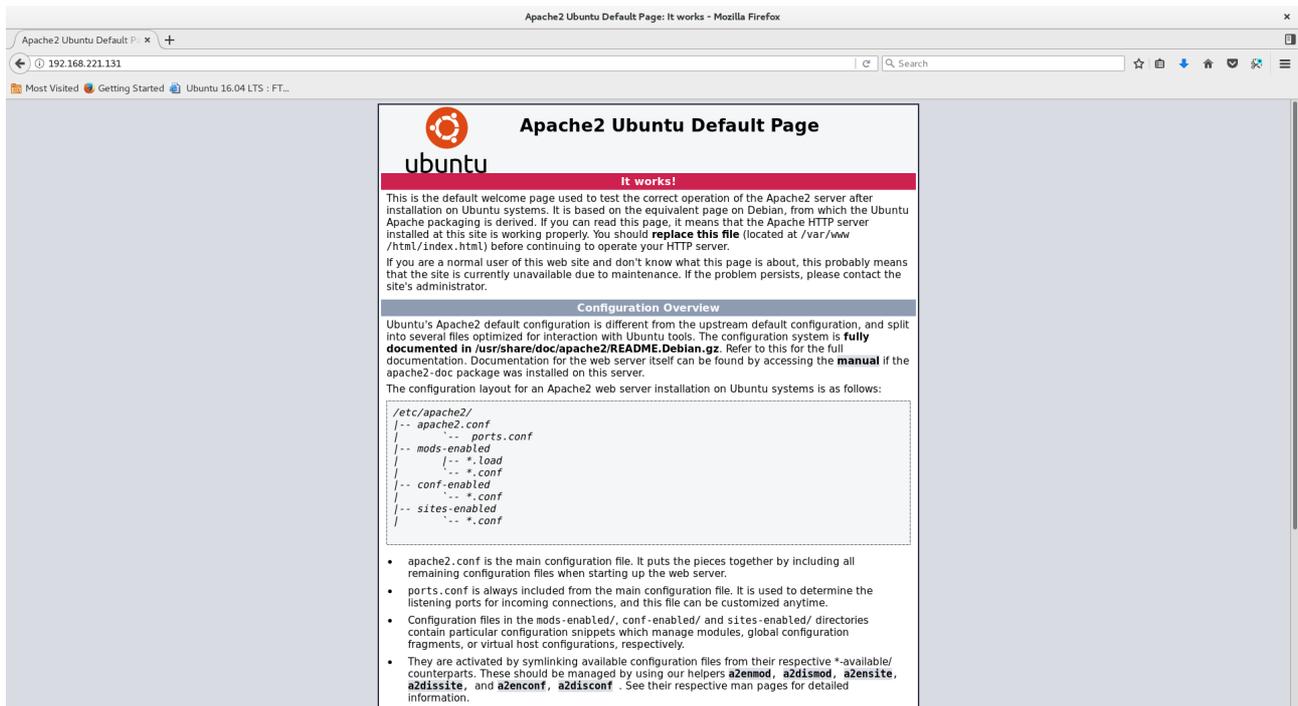
Ahora añadimos la línea siguiente al fichero `/etc/apache2/apache2.conf`

```
servername servidor
```

Entonces hacemos el comando `apache2ctl configtest` cuyo resultado debe ser el siguiente:
Syntax OK

Para reiniciar este servicio usamos `systemctl restart apache2`

Ahora para probarlo abrimos nuestro navegador web y ponemos la ip del servidor, en nuestro caso concreto es 192.168.221.131



4.13 Base de datos

Comando para su instalación → *apt-get install mysql-server*

En este caso concreto no requerimos más configuración, simplemente se nos pedirá la contraseña que queremos para nuestra base de datos.

La base de datos nos servirá, al igual que Apache, para tener instalados diversos servicios como Moodle.

4.14 Email: Roundcube

En nuestro centro necesitaremos email. Obviamente podemos usar email externo, como un típico Yahoo o Gmail pero lo ideal será tener un servidor que nuestros equipos clientes pueden usar. Al igual que otros servicios descritos no es obligatorio pero si es interesante su uso.

A continuación explicaremos todos los pasos necesarios para su configuración, siempre y cuando supongamos que usaremos el correo de forma interna y no dependeremos de un dominio externo. Para esto último incluiremos un apartado especial más abajo.

4.14.1 SMTP

Protocolo de red usado para el intercambio de mensajes. Lo necesitamos para que funcione nuestro sistema sistema de correo.

Comando para su instalación → *apt-get -y install postfix sasl2-bin* (elegimos en el menú “Sin configuración”)

A continuación copiamos el fichero `/usr/share/postfix/main.cf.dist` a `/etc/postfix/main.cf` y lo modificamos de la siguiente manera:

```
# linea 78: descomentar
mail_owner = postfix

# linea 94: descomentar y especificar nombre del equipo
myhostname = mail.srv.world

# linea 102: descomentar y especificar dominio
mydomain = srv.world

# linea 123: descomentar
myorigin = $mydomain

# linea 137: descomentar
inet_interfaces = all

# linea 185: descomentar
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain

# linea 228: descomentar
local_recipient_maps = unix:passwd.byname $alias_maps

# linea 270: descomentar
mynetworks_style = subnet

# linea 287: red local
mynetworks = 127.0.0.0/8, 10.0.0.0/24

# linea 407: descomentar
alias_maps = hash:/etc/aliases

# linea 418: descomentar
alias_database = hash:/etc/aliases

# linea 440: descomentar
home_mailbox = /var/mail

# linea 576: comentar y añadir
#smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
smtpd_banner = $myhostname ESMTP

# linea 650: añadir
sendmail_path = /usr/sbin/postfix

# linea 655: añadir
newaliases_path = /usr/bin/newaliases

# linea 660: añadir
mailq_path = /usr/bin/mailq

# linea 666: añadir
setgid_group = postdrop

# linea 670: comentar
#html_directory =

# linea 674: comentar
#manpage_directory =

# linea 679: comentar
#sample_directory =
```

```

# linea 683: comentar
#readme_directory =

# Limite del mensaje
message_size_limit = 10485760

# Limite de la bandeja de correo
mailbox_size_limit = 1234567894

# Autorizaciones
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain = $myhostname
smtpd_recipient_restrictions =
permit_mynetworks,permit_auth_destination,permit_sasl_authenticated,reject

```

4.12.2 IMAP

Es un protocolo de aplicación que permite el acceso a mensajes almacenados en un servidor de Internet. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet. IMAP tiene varias ventajas sobre POP (otro protocolo empleado para obtener correos desde un servidor).²

Comando para su instalación → *apt-get -y install dovecot-core dovecot-pop3d dovecot-imapd*

Ahora modificamos el fichero siguiente: */etc/dovecot/dovecot.conf*

```

# línea 30: descomentar
listen = *, ::

```

Y modificamos también el */etc/dovecot/conf.d/10-auth.conf*

```

# línea 10: descomentar y cambiar
disable_plaintext_auth = no

# línea 100: añadir
auth_mechanisms = plain login

```

Modificamos el */etc/dovecot/conf.d/10-mail.conf*

```

# línea 30: cambiar
mail_location = maildir:/var/mail

```

Modificamos el */etc/dovecot/conf.d/10-master.conf*

```

# líneas 96-98: descomentar y añadimos
# Postfix smtp-auth
unix_listener /var/spool/postfix/private/auth
{
    mode = 0666
    user = postfix
    group = postfix
}

```

² https://es.wikipedia.org/wiki/Protocolo_de_acceso_a_mensajes_de_Internet

Y finalmente hacemos un `systemctl restart dovecot`

4.12.3 Base de datos

Accedemos a nuestro SQL con `mysql -u root -p` y creamos la base de datos con los comandos siguientes:

```
create database roundcube;
grant all privileges on roundcube.* to roundcube@'localhost' identified by
'password';
flush privileges;
exit
```

En donde ponemos “password” tenemos que poner el que nosotros queramos que sea la contraseña del usuario roundcube.

4.12.4 Instalación de Roundcube

Comando para instalar → `apt-get -y install roundcube roundcube-mysql` donde seleccionaremos “No” cuando nos pregunten si queremos instalar con `dbconfig-common`. Y luego hacemos:

```
cd /usr/share/dbconfig-common/data/roundcube/install
mysql -u roundcube -D roundcube -p < mysql
cd
```

Ahora editamos el fichero `/etc/roundcube/debian-db.php`

```
$dbuser='roundcube ';
$dbpass='password';
$basepath='';
$dbname='roundcube';
$dbserver='localhost';
$dbport='';
$dbtype='mysql';
```

Editamos el fichero `/etc/roundcube/config.inc.php`

```
# línea 35: IMAP server (SSL)
$config['default_host'] = 'ssl://mail.srv.world';

# línea 47: SMTP server (SSL)
$config['smtp_server'] = 'ssl://mail.srv.world';

# línea 51: SMTP port (SSL)
$config['smtp_port'] = 465;

# línea 55: cambiar (usa el mismo usuario para SMTP e IMAP auth)
$config['smtp_user'] = '%u';

# línea 59: cambiar (usa el mismo pass para SMTP e IMAP auth)
$config['smtp_pass'] = '%p';

# línea 66: aquí ponemos el título de nuestro servidor. Es al gusto.
$config['product_name'] = 'UOC Webmail';

# añadir lo siguiente
```

```
$config['default_port'] = 993;
$config['smtp_auth_type'] = 'LOGIN';
$config['smtp_helo_host'] = 'uoc.email';
$config['mail_domain'] = 'uoc.email';
$config['useragent'] = 'UOC Webmail';
$config['imap_conn_options'] = array(
    'ssl' => array(
        'verify_peer' => true,
        'CN_match' => 'uoc.email',
        'allow_self_signed' => true,
        'ciphers' => 'HIGH:!SSLv2:!SSLv3',
    ),
);
$config['smtp_conn_options'] = array(
    'ssl' => array(
        'verify_peer' => true,
        'CN_match' => 'uoc.email',
        'allow_self_signed' => true,
        'ciphers' => 'HIGH:!SSLv2:!SSLv3',
    ),
);
```

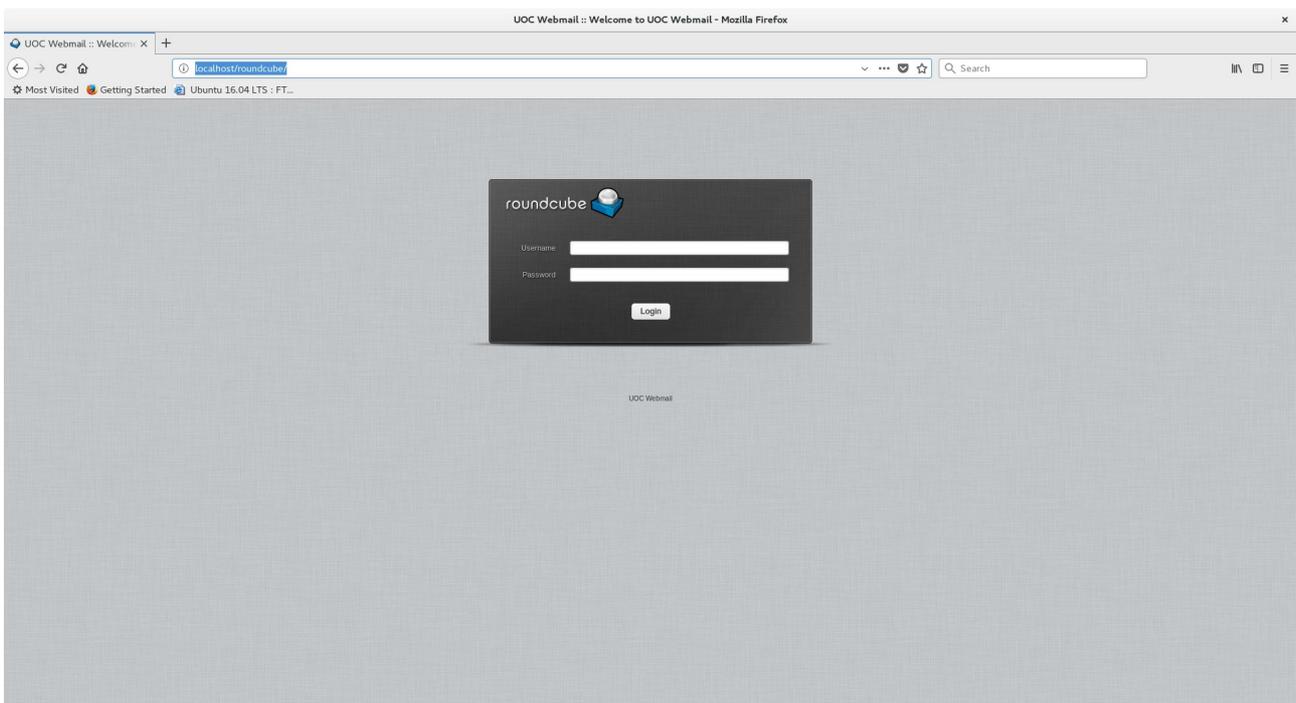
Editamos el fichero `/etc/apache2/conf-enabled/roundcube.conf` y descomentamos la línea 3:

```
Alias /roundcube /var/lib/roundcube
```

Ahora ejecutamos:

```
phpenmod mcrypt
systemctl restart apache2
```

Tras esto accedemos a nuestra web y comprobamos que funciona correctamente.



4.12.5 Comprar un dominio

Puede darse el caso de que queramos un dominio externo para el centro. En este caso concreto podemos recurrir a diversas páginas de internet como:

https://es.godaddy.com/offers/domains?isc=gdeses06&countryview=1¤cytype=eur&mkwid=sHWkiSG0Y_pcrd_196519601965_pkw_comprar%20dominio_pmt_p_pdv_c_&gclid=EAIAIQobChMIytyKienr1wIV6TLTCh2VFgnwEAAYAiAAEgKDFfD_BwE

https://www.1and1.es/dominios?ac=OM.WE.WEo42K356280T7073a&gclid=EAIAIQobChMIytyKienr1wIV6TLTCh2VFgnwEAAAYASAAEgKMFPD_BwE#stage

https://www.hostalia.com/dominios/?gclid=EAIAIQobChMIytyKienr1wIV6TLTCh2VFgnwEAAYAyAAEgKVRvD_BwE

https://www.arsys.es/correo?s=cpc&c=315843363&a=31700134203&gclid=EAIAIQobChMIytyKienr1wIV6TLTCh2VFgnwEAAAYBCAAEgJtR_D_BwE

La ventaja de esto es que, a diferencia del modelo anteriormente explicado, podemos usar nuestros correos con más facilidad fuera de nuestro centro. Tengamos en cuenta que es posible que con la configuración anterior a lo mejor el correo es por y para el centro, sin poder acceder al exterior. Es decir el uso sería interno, para profesores y alumnos.

Esto depende básicamente de la red a la que este conectado el centro. En el caso de Andalucía nos consta que todos los centros están conectados a una red concreta llamada RCJA donde mucho tráfico está bloqueado o debe de ser permitido por agentes externos. En otros casos, podemos tener nuestro centro conectado directamente a internet, a través de una conexión normal y corriente como de Jazztel o Movistar, luego este problema desaparece.

4.13 OpenLDAP

OpenLDAP es una implementación libre y de código abierto del protocolo Lightweight Directory Access Protocol (LDAP) desarrollada por el proyecto OpenLDAP. Un servidor LDAP es un servidor de datos optimizado para la realización rápida de consultas de lectura y orientado al almacenamiento de datos de usuarios a modo de directorio.

La principal utilidad de un directorio LDAP es como servidor de autenticación para los distintos servicios de un sistema informático como puedan ser: autenticación para entrar en un PC, para entrar en una aplicación web, para acceder a un servidor ftp, para acceder a servidores de correo entrante POP3 y saliente SMTP, etc.

Al igual que otros componentes a instalar es opcional. Imaginemos por ejemplo dos escenarios:

- Un centro donde los alumnos tienen sus propios portátiles: en este caso no será necesario la instalación de LDAP, cada alumno tendrá su portátil en propiedad siempre y solo lo usará este alumno.

- Un centro donde los portátiles son compartidos: un centro puede tener 20 portátiles para un aula y ser compartidos por diversos alumnos dado que no hay para todos, en este caso sería útil tener LDAP.

Obviamente podemos igualmente instalar LDAP para el primer escenario, pero lo normal es hacerlo para el segundo.

4.13.1 Servidor LDAP

Comando para su instalación → *apt-get install slapd ldap-utils*

Nos preguntará la contraseña de administración de LDAP, en nuestro caso hemos usado “admin” simplemente.

Tras esto modificaremos el */etc/host* para que cuando hagamos referencia a *ldapserver* nuestro servidor lo entienda, para esto añadimos la línea siguiente:

```
127.0.0.1 ldapserver ldapserver.example.net
```

Luego instalamos el paquete *libnss-ldap* con el comando → *apt-get install libnss-ldap -y*

La configuración que seguiremos será:

- *ldapi:///127.0.0.1*
- *dc=example, dc=net* (esto es personalizable a gusto del centro)
- Versión de LDAP: 3
- Cuenta LDAP para administración: *cn=admin, dc=example, dc=net*

El resto de opciones las dejamos por defecto.

4.13.2 Configurar autenticación para clientes

Comando → *auth-client-config -t nss -p lac_ldap*

Tras esto ejecutamos → *pam-auth-update*

Las opciones que aparezcan las dejamos por defecto. Y para finalizar con este paso modificamos el fichero */etc/ldap.conf* con el contenido siguiente:

```
host 127.0.0.1 base
dc=example,dc=net
uri ldapi:///127.0.0.1/
rootbinddn cn=admin,dc=example,dc= net
ldap_version 3
bind_policy soft
```

4.13.3 Configurar el demonio slapd

Ejecutamos → *dpkg-reconfigure slapd*

Aquí deberemos de escribir el nombre de nuestro dominio así como el nombre de la entidad. En nuestro caso sería “example.net” y “UOC” respectivamente.

El resto de opciones las dejamos por defecto.

4.13.4 Crear la estructura

Creamos primero un fichero llamado base.ldif. El directorio donde lo hagamos es irrelevante pero tenemos que acordarnos de donde está luego (obviamente no conviene crearlo en /tmp)

El contenido de este fichero será:

```
dn: ou=usuarios,dc=example,dc=net
objectClass: organizationalUnit
ou: usuarios
```

```
dn: ou=grupos,dc=example,dc=net
objectClass: organizationalUnit
ou: grupos
```

A continuación, deberemos añadir la información a la base de datos OpenLDAP. Esto se hace con el comando siguiente → *ldapadd -x -D cn=admin,dc=example,dc=net -W -f base.ldif*

4.13.5 Añadir un usuario

En este caso crearemos el fichero usuario.ldif donde el contenido podría ser algo como:

```
dn: uid=jlopez,ou=usuarios,dc=example,dc=net
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: jlopez
sn: Lopez
givenName: Juan
cn: Juan Lopez
displayName: Juan Lopez
uidNumber: 1001
gidNumber: 10001
userPassword: paas
gecos: Juan Lopez
loginShell: /bin/bash
homeDirectory: /home/nfs/jlopez
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: juan.lopez@uoc.com
postalCode: 41300
o: somebooks
initials: JL
```

Para cargar el usuario usaremos el comando *ldapadd -x -D cn=admin,dc=example,dc=net -W -f usuario.ldif*

4.13.6 Añadir un grupo

En este caso el fichero es grupo.ldif y su contenido será algo como

```
dn: cn=Nombregrupo,ou=grupos,dc=example,dc=net
objectClass: posixGroup
cn: SMR2
gidNumber: 10001
```

En nuestro caso, dado que tenemos 3 redes: profesores, gestión y alumnos podríamos pensar en crear 3 grupos, uno por cada tipo de usuario en nuestro centro. Uno para alumnos, uno para el equipo de gestión y otro para los profesores.

El comando es el mismo que antes solo que cambiamos el fichero obviamente
ldapadd -x -D cn=admin,dc=somebooks,dc=local -W -f grupo.ldif

Observación: tenemos que tener cuidado con los gid e id de cada usuario/grupo.

4.14 NFS

El Network File System (Sistema de archivos de red), o NFS, es un protocolo de nivel de aplicación, según el Modelo OSI. Es utilizado para sistemas de archivos distribuido en un entorno de red de computadoras de área local. Posibilita que distintos sistemas conectados a una misma red accedan a ficheros remotos como si se tratara de locales.³

4.14.1 Instalación

Usamos el comando siguiente:

```
apt-get install nfs-kernel-server
```

4.14.2 Configuración básica

Ahora buscaremos que los directorios “home” de los clientes en realidad estén en nuestro servidor y sean accesibles. Exportaremos el directorio “/home/nfs” de nuestro servidor, si no lo tenemos lo creamos con el comandos

```
cd /home
mkdir -P nfs
```

Configuramos el fichero “/etc/exports” con la siguiente sintaxis:

directorio a compartir cliente(opciones)

Por ejemplo si queremos compartir una de nuestras redes:

```
/home/nfs 192.168.0.0/255.255.255.242 (rw,sync,no_root_squash,no_subtree_check)
```

³ https://es.wikipedia.org/wiki/Network_File_System

O si solo queremos un equipo concreto:

```
/home/nfs 192.168.4.60 (rw, sync, no_subtree_check)
```

El significado de las opciones lo explicamos aquí:

- `rw`: da al cliente posibilidad de acceder y escribir
- `sync`: fuerza a NFS a escribir los cambios. Reduce la velocidad pero aumenta la seguridad y la integridad
- `no_subtree_check`: previene el “subtree checking”, proceso por el cual el cliente debe chequear cualquier fichero exportado disponible cada poco tiempo. Causa problemas y es muy lento así que mejor quitarlo.

Tras esto reiniciamos el servicio con el comando siguiente:

```
systemctl restart nfs-kernel-server
```

4.15 Moodle

Moodle es una herramienta de gestión de aprendizaje (LMS), o más concretamente de Learning Content Management. de distribución libre, escrita en PHP.

Está concebida para ayudar a los educadores a crear comunidades de aprendizaje en línea, Moodle es usada en blended learning, educación a distancia, clase invertida y diversos proyectos de e-learning en escuelas, universidades, oficinas y otros sectores.

Estas herramientas son de gran utilidad en el ámbito educativo, ya que permiten a los profesores la gestión de cursos virtuales para sus alumnos (educación a distancia), o el uso de un espacio en línea que dé apoyo a la presencialidad (aprendizaje semipresencial, blended learning o b-learning).

4.15.1 PHP

Ahora instalaremos PHP, necesario para Moodle.

Usamos el comando `apt-get install php libapache2-mod-php php-mcrypt php-mysql`

Ahora dejamos el fichero `/etc/apache2/mods-enabled/dir.conf`

de la siguiente manera:

```
<IfModule mod_dir.c>
    DirectoryIndex index.php index.html index.cgi index.pl index.xhtml
index.htm
</IfModule>
```

```
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

4.15.2 Instalación de moodle

Usamos el comando siguiente →

```
apt-get install aspell graphviz php7.0-curl php7.0-gd php7.0-intl php7.0-ldap  
php7.0-mysql php7.0-pspell php7.0-xml php7.0-xmlrpc php7.0-zip
```

Tras esto reiniciamos el servicio apache → `systemctl restart apache2`

Ahora descargamos moodle y lo descomprimos en el directorio correspondiente

```
apt-get install curl  
curl -L https://download.moodle.org/download.php/direct/stable32/moodle-latest-  
32.tgz > moodle.tgz  
tar -xvzf moodle.tgz -C /var/www/html
```

Ahora tenemos que crear un directorio para los datos de los cursos de moodle y dar los permisos adecuados. No es obligatorio pero si recomendable como medida de seguridad:

```
mkdir /var/moodledata  
chown -R www-data /var/moodledata  
chmod -R 0770 /var/moodledata
```

4.15.3 Configuración de la base de datos

Ahora tenemos que configurar nuestra base de datos, en nuestro caso MySQL. Hacemos lo siguiente:

Editamos el fichero de configuración siguiente → `/etc/mysql/mysql.conf.d/mysqld.cnf`

Añadiendo las líneas en el apartado “*Basic Settings*”:

```
default_storage_engine = innodb  
innodb_file_per_table = 1  
innodb_file_format = Barracuda
```

Reiniciamos el servicio: `systemctl restart mysql`

Ahora creamos nuestra base de datos y un usuario nuevo para esto. No es obligatorio pero si recomendable por motivos de seguridad, así no usamos nuestro usuario administrador de la base de datos constantemente en la plataforma.

```
mysql -u root -p
```

Dentro de mysql:

```
CREATE DATABASE moodle DEFAULT CHARACTER SET utf8 COLLATE utf8_unicode_ci;  
create user 'usuariomoodle'@'localhost' IDENTIFIED BY 'passmoodle';  
GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,CREATE TEMPORARY  
TABLES,DROP,INDEX,ALTER ON moodle.* TO 'usuariomoodle'@'localhost' IDENTIFIED BY  
'passmoodle';  
quit;
```

4.15.4 Instalación web

El último paso es entrar vía web a la página siguiente: `http://direccionIP/moodle/install.php`

(sustituir direccionIP por la de nuestro servidor)

A partir de aquí simplemente tenemos que asegurarnos de configurar correctamente determinados campos concretos como el del directorio de datos, que recordemos en nuestro caso es el siguiente:
/var/moodledata

Valores concretos a configurar, el resto pueden dejarse por defecto, o no, dependiendo de como queramos nuestra Moodle.

Directorio de datos → */var/moodledata*

Usuario de la base de datos → *usuariomoodle*

Contraseña de la base de datos → *passmoodle*

4.15.5 Últimos cambios

Un cambio de seguridad, optativo, puede ser modificar los permisos de los ficheros en */var/moodledata*. Por defecto Moodle los hace con permisos 777 así que si queremos cambiar eso editamos el fichero */var/www/html/moodle/config.php*

En la línea siguiente: `$CFG->directorypermissions = 0777;`

La cambiamos por: `$CFG->directorypermissions = 0770;`

4.16 OurScrapbook

El Libro Virtual OurScrapBook consiste como su propio nombre indica en un libro virtual donde pueden alojarse contenidos bien para leer o escribir y cuya funcionalidad es similar a la de cualquier libro convencional.

La lectura se realiza de forma sencilla accediendo a cualquier capítulo del libro y desplazándose por sus diferentes hojas, como en cualquier libro de texto. OurScrapBook tiene la característica fundamental de que cualquier persona puede escribir en el libro, editando artículos, sin necesidad de estar registrado. La potencia de esta herramienta consiste en que cualquier contenido será editado siempre que el administrador (que en la mayoría de los casos será un profesor) permita su publicación.

Se trata de una herramienta de comunicación, efectiva y muy sencilla de utilizar en la que todos pueden participar con sus aportaciones publicando sus creaciones en la red y convirtiéndola en una fuente de información adecuada para todos.⁴

No existe paquete para ninguna distribución de Linux, para instalarlo lo que tenemos que hacer es descargarlo de la web: <https://sourceforge.net/projects/ourscrapbook/> y tras esto, tenemos que descomprimir el .zip descargado en nuestro directorio de publicación de Apache, en nuestro caso */var/www/*

Recordemos que tenemos que tener instalado Apache, SQL y PHP en nuestro servidor para que funcione.

Por defecto los datos de acceso a la aplicación son los siguientes:

4 http://www.juntadeandalucia.es/educacion/cga/mediawiki/index.php/Libro_virtual_OurScrapBook

- Usuario: myscrapbook
- Contraseña: myscrapbook

4.17 Radius

Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones, motivo por el cual abrimos este puerto en la configuración previa de iptables.

Este servicio nos sirve para que un usuario tenga que autenticarse en una web antes de poder conectar a nuestros puntos de acceso wifi, añadiendo una capa extra de seguridad. Obviamente es opcional, dado que se puede poner una clave wifi común para todo el centro y que todo el mundo use la misma, pero eso no es muy seguro dado que cualquiera que conozca la clave no tiene más que acercarse al centro y conectar su portátil o móvil.

Muchos dispositivos poseen un servidor de estas características ya integrado que permite la captura del tráfico, siendo redirigido a lo que se conoce como “portal cautivo” en el que tendrá que introducir las credenciales que hemos mencionado con anterioridad.

4.17.1 Instalación

Si queremos instalar nosotros uno, lo podemos hacer con el comando siguiente:

```
apt-get install freeradius
```

Tras esto, para verificar su versión hacemos el comando siguiente y después hacemos otro comando para comprobar que la configuración inicial es correcta:

```
freeradius -v  
freeradius -CX
```

4.17.2 Clientes permitidos

Ahora deberemos de configurar nuestro servidor. Primero ajustaremos el número máximo de clientes permitidos. Esto se hace en el fichero “/etc/freeradius/radiusd.conf” con la variable siguiente:

```
max_requests = 2048
```

En este ejemplo permitimos 8 clientes (hay que multiplicar por 4 el número 256). Si quisiéramos 16 habría que poner 4096.

4.17.2 Añadir clientes

Esto se hace en el fichero “/etc/freeradius/clients.conf” y se hace de la siguiente forma:

```
client PUNTO_DE_ACCESO {  
    ipaddr = 192.168.8.20
```

```
secret = contraseña
}
```

Ojo, estos “clientes” se refieren a los puntos de acceso que usarán nuestro Radius, no nuestros portátiles o móviles.

4.17.3 Configurar Método EAP

Por defecto la autenticación de este servicio se hace con MD5, si queremos cambiarlo modificamos el fichero “/etc/freeradius/eap.conf”, concretamente la línea siguiente:

```
default_eap_type = md5
```

Son varios los métodos de autenticación soportados: tls, leap, mschapv2.... Elegimos el que consideremos oportuno (o dejamos md5 si queremos). Por regla general el que se usa cuando configuramos LDAP es “mschapv2”.

4.17.4 Añadir usuarios

Aquí podemos añadir usuarios con permisos para autenticarse en nuestro servidor RADIUS. El fichero de configuración en este caso es “/etc/freeradius/users” (notad que no tiene un .conf detrás, no es un directorio, es un fichero).

Ejemplo de usuario:

```
nombre_usuario Cleartext-Password := "12345"
```

4.17.5 Autenticación LDAP

En el caso de que tengamos configurados el servicio LDAP en nuestro servidor debemos de instalar el módulo que nos permite autenticarnos en RADIUS con nuestros usuarios creados con LDAP:

```
apt-get install freeradius-ldap ipa-server-trust-ad
```

Ahora configuraremos el módulo, cuyo fichero de configuración es “/etc/freeradius/modules/ldap” con el siguiente contenido:

```
ldap {
server = fqdn de nuestro servidor%ldap_server_fqdn%
port = puerto %ldap_server_port%
identity = "uid=%bind_user%,cn=users,cn=accounts,dc=example,dc=com"
password = contraseña%bind_user_password%
basedn = basedn de nuestro servidor "cn=users,cn=accounts,dc=example,dc=com"
filter = "(uid=%{%Stripped-User-Name}:-{%User-Name})"
authtype = ldap
groupname_attribute = cn
groupmembership_filter = "(|(&(objectClass=GroupOfNames) (member=%{Ldap-UserDn})) (&(objectClass=GroupOfUniqueNames) (uniquemember=%{Ldap-UserDn})))"
dictionary_mapping = ${raddbdir}/ldap.attrmap
set_auth_type = yes
auto_header = yes
password_header = "{ssh}"
password_attribute = userPassword
}
```

Y por último en el fichero “/etc/freeradius/sites-enabled” modificamos lo siguiente en la sección “Authenticate”:

```
Auth-Type LDAP {  
  ldap  
}
```

4.17.6 Alternativas

Existen numerosas alternativas a este servicio, los interesados pueden mirar:

- Pepper Spot: <http://pepperspot.sourceforge.net/>
- NoCatAuth: <https://sourceforge.net/projects/nocatauth/>
- Coova Chilli: <https://coova.github.io/>

4.18 Instalación por red (pxe)

Preboot eXecution Environment (PXE) (Entorno de ejecución de prearranque), es un entorno para arrancar e instalar el SO en ordenadores a través de una red, de manera independiente de los dispositivos de almacenamiento de datos disponibles (como discos duros) o de los sistemas operativos instalados.

Nos sirve para instalar el sistema operativo desde un equipo de un aula, sin necesidad de pendrive, CD de instalación o similar.

4.18.1 Primeros pasos

Primero instalaremos dos paquetes concretos con el comando siguiente: `apt-get install tftpd-hpa inetutils-inetd`

Tras esto añadiremos al fichero `/etc/default/tftpd-hpa` las líneas siguientes:

```
RUN_DAEMON="yes"  
OPTIONS="-l -s /var/lib/tftpboot"  
Ahora en el fichero /etc/inetd.conf hacemos lo mismo, añadir al final la línea:
```

```
tftp dgram udp wait root /usr/sbin/in.tftpd /usr/sbin/in.tftpd -s /var/lib/tftpboot
```

Tras resto reiniciamos el servicio → `systemctl restart tftpd-hpa`

4.18.2 Añadir nuestros sistemas operativos

Ahora deberemos de añadir a un directorio nuestros sistemas operativos. Es decir, aquellos que queramos que puedan ser instalados por red. En nuestro ejemplo haremos con una Ubuntu pero técnicamente hablando es posible hacerlo con cualquier otra distribución.

Primero, nos descargamos la ISO a nuestro servidor, en cualquier directorio, y una vez lo hagamos hacemos, en el directorio donde tenemos la ISO, los comandos:

```
cd /mnt/  
cp -fr install/netboot/* /var/lib/tftpboot/  
mkdir /var/www/html/ubuntu  
cp -fr /mnt/* /var/www/html/ubuntu/
```

Ahora añadimos las líneas siguientes al fichero: */var/lib/tftpboot/pxelinux.cfg/default*

```
label linux  
kernel ubuntu-installer/amd64/linux  
append ks=http://192.168.1.105/ks.cfg vga=normal initrd=ubuntu-  
installer/amd64/initrd.gz  
ramdisk_size=16432 root=/dev/rd/0 rw --
```

Añadimos las siguientes líneas en el fichero */etc/dhcp/dhcpd.conf*

```
allow booting;  
allow bootp;  
option option-128 code 128 = string;  
option option-129 code 129 = text;  
next-server 192.168.1.105;  
filename "pxelinux.0";
```

Y reiniciamos el servicio con *systemctl restart isc-dhcp-server*

Por parte del servidor la configuración está terminada. En el apartado del cliente, más adelante, explicaremos como configurar nuestros equipos clientes para que se pueda instalar por red.

4.19 Copias de seguridad

El sistema de copias de seguridad desarrollado se ha basado en la creación de scripts simples y el uso de la funcionalidad del cron. A continuación se explica de forma más detallada cada uno de los componentes.

4.19.1 Script básico para copias

Existen muchos scripts que pueden ser usados para copias, uno de los más básicos (y efectivos) es el creado por Hafiz Haider en 2012. Aquí lo tenemos modificado con comentarios en español:

```
#!/bin/bash  
#Purpose = Backup of Important Data  
#Created on 17-1-2012  
#Author = Hafiz Haider  
#Version 1.0  
#START  
# Añadimos la fecha al nombre del fichero de copias  
TIME=`date +%b-%d-%y`  
# Definición del nombre del fichero  
FILENAME=backup-NOMBRE- $\$$ TIME.tar.gz  
# Localización de los directorios a copiar. En este ejemplo, los datos de moodle  
SRCDIR=CARPETAAGUARDAR  
# Donde guardamos el directorio creado de copia de seguridad.  
DESDIR=/var/backups/DONDEQUEREMOSGUARDARLASCOPIAS  
tar -cpzf  $\$$ DESDIR/ $\$$ FILENAME  $\$$ SRCDIR  
#END
```

Tenemos que sustituir las variables necesarias para la realización de las copias que queramos. A continuación varios ejemplos.

4.19.2 Copia de Moodle

```
FILENAME=backup-moodledata-$TIME.tar.gz  
SRCDIR=/var/moodledata  
DESDIR=/var/backups/moodledata
```

En este caso se comprimirá el directorio “/var/moodledata” y pondrá el tar.gz en el directorio donde alojamos las copias, en este caso en /var/backups.

A este script podríamos llamarlo, por ejemplo, backup_moodle.sh.

4.19.3 Copia de NFS

Si hemos implementado NFS en nuestro sistema y queremos realizar una copia de seguridad de esto, habría que modificar las variables del script de la siguiente forma:

```
FILENAME=backup-NFS-$TIME.tar.gz  
SRCDIR=/home/nfs/  
DESDIR=/var/backups/nfs
```

4.19.4 El cron

Cron es el nombre del programa que permite a usuarios Linux/Unix ejecutar automáticamente comandos o scripts (grupos de comandos) a una hora o fecha específica. Es usado normalmente para comandos de tareas administrativas, como respaldos, pero puede ser usado para ejecutar cualquier cosa.

Aunque el fichero puede ser editado de forma manual es más fácil usar la utilidad “crontab”, con el comando siguiente: *crontab -e*

Un menú interactivo nos irá guiando hasta llegar al fichero donde podremos editar cuando queremos que se ejecute un comando concreto, en nuestro caso, backup_moodle.sh; el formato es el siguiente:

Minutos	Horas	Día del mes	Mes	Día de la semana	Comando
0-59	0-23	1-31	1-12	0-6	/bin/bash /usr/scripts/backup_moodle.sh>2&1

En nuestro caso el comando podemos ver como incluye una redirección especial hacia la salida de errores estándar, que es 2&1, básicamente debido a que no nos interesa que aparezca nada por pantalla.

Por ejemplo si ponemos

```
11 2 * * * /bin/bash /usr/scripts/backup_moodle.sh>2&1
```

Se ejecutará la copia de seguridad de Moodle a las 02:11 todos los días.

4.19.5 Más información

Si queremos usar un sistema más complejo y completo de copias de seguridad aquí tenemos unas guías prácticas. No se considera necesario puesto que el sistema de scripts creados es más que suficiente pero en caso de necesitar más información sobre otros sistemas o de copias de seguridad en general podemos mirar aquí:

- Bacula: <https://www.digitalocean.com/community/tutorials/how-to-install-bacula-server-on-ubuntu-14-04>
- Políticas de copias de seguridad: <https://infosegur.wordpress.com/unidad-3/politicas-de-copias-de-seguridad/>
- Que copia elegir: <http://searchdatacenter.techtarget.com/es/cronica/Copia-de-seguridad-completa-incremental-o-diferencial-como-elegir-el-tipo-adecuado>

4.20 Monitorización: Munin

Munin nos sirve para monitorizar el estado de nuestro servidor sin necesidad de desplazarnos físicamente a él.

Comando para instalar → *apt-get -y install munin munin-node*

Ahora en el fichero de configuración: */etc/munin/munin.conf* modificamos lo siguiente (línea 98), donde tenemos que poner el nombre de nuestro servidor:

```
[nombre_de_servidor]
  address 127.0.0.1
  use_node_name yes
```

Ahora en el fichero */etc/munin/apache.conf* en la primera línea la dejamos así:

```
# Enable this for template generation
#Alias /munin /var/cache/munin/www
Alias /munin /var/www/munin
```

Y los apartados los dejamos así:

```
<Directory /var/www/munin>
#      Order allow,deny
#      Allow from localhost 127.0.0.0/8 ::1
#      Options None

      Require all granted
      Options FollowSymLinks SymLinksIfOwnerMatch
(...)
```

```
# Enables fastcgi for munin-cgi-graph if present
ScriptAlias /munin-cgi/munin-cgi-graph /usr/lib/munin/cgi/munin-cgi-graph
<Location /munin-cgi/munin-cgi-graph>
#      Order allow,deny
#      Allow from localhost 127.0.0.0/8 ::1
```

```

        Require all granted
        Options FollowSymLinks SymLinksIfOwnerMatch
(...)

<Location /munin-cgi/munin-cgi-html>
#       Order allow,deny
#       Allow from localhost 127.0.0.0/8 ::1
        Require all granted
(...)

```

Ahora tendremos acceso a nuestro portal Munin en la web:

http://192.168.221.131/munin/

Recordad que hay que cambiar la ip por de nuestro servidor.

4.21 Script de configuración inicial

Este pequeño script configurará el servidor de forma inicial. Instalará lo básico y además configurará determinados aspectos como el nombre o la ip. Hemos supuesto que cada centro educativo tiene que tener un código, una sede y una dirección ip.

```

#!/bin/bash

# Puesta en marcha básica de servidores de centros educativos
# Autor: Francisco José Márquez Bernal

DEFAULT_DIR="`pwd`" #Directorio usado
DATA_DIR="$DEFAULT_DIR/data" #Directorio donde estan diversos ficheros de
utilidad
DOMINIO="uoc.tfg.trabajo-uoc.es" #Nuestro dominio
DESTINATION_DIR=""
FECHA="`date +%Y%m%d`" #Fecha

#Necesitamos este fichero para usar diversas funciones
. /lib/lsb/init-functions

#Nos permite saber si es un numero entero
isInteger ()
{
    x=$1
    case $x in
        *[^0-9+-]*|?*[-+]*|""|-|+)
            return 1 ;;
        *)
            return 0 ;;
    esac
}

#Obtenemos los datos de nuestro centro
obtenerDatosCentro ()
{
## CODIGO DE CENTRO
CORRECTO="N"
while [ "$CORRECTO" != "S" ];
do
    echo -e "\nIntroduzca el código de centro: "
    read CODIGO

```

```

if [ ${#CODIGO} != 8 ]; then
    echo "ERROR: el codigo de centro debe tener 8 digitos."
elif ! isInteger $CODIGO; then
    echo "ERROR: el código de centro debe ser numerico."
else
    CORRECTO="S"
fi
done

## SEDE (Si hay más de una, hemos supuesto un máximo de 2 sedes)
echo -en "\n¿Tiene el centro mas de una dotacion de datos? (s/n):"
read -n1 RESP
if [ "$RESP" == "s" ] || [ "$RESP" == "S" ]; then
    CORRECTO="N"
    while [ "$CORRECTO" != "S" ];
    do
        echo -e "\nSeleccione de qué sede se trata: "
        select SEDE in "a" "b" "c" "d" "e" "f" "g" "h" "i" "j" "k" "l";
        do
            case "$REPLY" in
                "1")
                    CODIGO=`echo $CODIGO"a"`; CORRECTO="S" ;;
                "2")
                    CODIGO=`echo $CODIGO"b"`; CORRECTO="S" ;;
                *)
                    echo -e "ERROR: la opción elegida no es correcta."
                    CORRECTO="N"
            esac
            break;
        done
    done
fi

## TIPO DE CENTRO
CORRECTO="N"
while [ "$CORRECTO" != "S" ];
do
    echo -e "\nSeleccione el tipo de centro: "
    select TIPO_CENTRO in "C.E.I.P." "C.E.P." "C.P.R." "I.E.S.";
    do
        if ! isInteger $REPLY; then
            echo -e "ERROR: la opción elegida no es correcta."
        elif [ $REPLY -lt 1 ] || [ $REPLY -gt 4 ]; then
            echo -e "ERROR: la opción elegida no es correcta."
        else
            CORRECTO="S"
        fi
        break;
    done
done

## ANHO DEL CENTRO
CORRECTO="N"
while [ "$CORRECTO" != "S" ];
do
    echo -e "\nIntroduzca el año del centro: "
    read ANHO
    if [ ${#ANHO} != 4 ]; then
        echo "ERROR: el año del centro debe tener 4 dígitos."
    elif ! isInteger $ANHO; then
        echo "ERROR: el año del centro debe tener 4 dígitos."
    else
        CORRECTO="S"
    fi
done

```

```

done

## NOMBRE, MUNICIPIO Y PROVINCIA
echo -e "\nIntroduzca el nombre del centro: "
read NOMBRE
echo -e "\nIntroduzca el municipio donde se ubica el centro: "
read POBLACION
CORRECTO="N"
while [ "$CORRECTO" != "S" ];
do
    echo -e "\nSeleccione la provincia a la que pertenece: "
    select PROVINCIA in "Almería" "Cádiz" "Córdoba" "Granada" "Huelva" "Jaén"
"Málaga" "Sevilla";
do
    if ! isInteger $REPLY; then
        echo -e "ERROR: la opción elegida no es correcta."
    elif [ $REPLY -lt 1 ] || [ $REPLY -gt 8 ]; then
        echo -e "ERROR: la opción elegida no es correcta."
    else
        CORRECTO="S"
    fi
done
done

## IP BASE
echo -en "\n\nIntroduzca la dirección de red (Ej.- 10.245.10.96): "
read RED
echo -e ""
}

verificarDatosCentro ()
{
    echo -e "\n\n\t***** Verificación de datos
*****"
    echo -e "\tCódigo de centro:\t\t"$CODIGO
    echo -e "\tTipo de centro:\t\t\t"$TIPO_CENTRO
    echo -e "\tAño del centro:\t\t\t"$ANHO
    echo -e "\tNombre del centro:\t\t\t"$NOMBRE
    echo -e "\tMunicipio:\t\t\t\t"$POBLACION
    echo -e "\tProvincia:\t\t\t\t"$PROVINCIA
    echo -e "\tDirección de red en R.C.J.A.:\t"$RED
    echo -e
"\t*****"
}

calcularVariables ()
{
    RED_:Q1Q2Q3=`echo $RED | cut -d. -f1,2,3`
    RED_Q4=`echo $RED | cut -d. -f4`

    ROUTER=$((`echo $RED_Q4` + 1))
    SERVIDOR_ETH0=$((`echo $RED_Q4` + 2))
    SWITCH=$((`echo $RED_Q4` + 5))
    BRD=$((`echo $RED_Q4` + 31))

    IP_BASE=`echo $RED_Q1Q2Q3.$RED_Q4`
    IP_ROUTER=`echo $RED_Q1Q2Q3.$ROUTER`
    IP_SERVIDOR=`echo $RED_Q1Q2Q3.$SERVIDOR_ETH0`
    IP_BROADCAST=`echo $RED_Q1Q2Q3.$BRD`
    IP_ADM_SERVIDOR=`echo $RED_Q1Q2Q3.$SERVIDOR_ADM`

    COD_PROVINCIA=`echo $CODIGO | cut -c1,2`
    HOSTNAME=`hostname`
}

```

```

}

replaceVariables ()
{
    FILE="$1"
    TEMP_FILE="`tempfile`"

    log_action_begin_msg "Actualizando $DESTINATION_DIR/interfaces.servidor"
    cat $DATA_DIR/$FILE | sed -e s/___IP_BASE___/$IP_BASE/g |\
    sed -e s/___IP_ROUTER___/$IP_ROUTER/g |\
    sed -e s/___IP_SERVIDOR___/$IP_SERVIDOR/g |\
    sed -e s/___IP_BROADCAST___/$IP_BROADCAST/g |\
    mv -b $TEMP_FILE $DATA_DIR/$FILE
    log_action_end_msg $?
}

#Configura el nombre del servidor y el host
configuraFiles ()
{
    FILES="$DATA_DIR/files"
    for FILE in `cat $FILES`
    do
        replaceVariables $FILE
    done
    echo "127.0.0.1        localhost" > /etc/hosts
    echo "$IP_SERVIDOR servidor.$CODIGO.$COD_PROVINCIA.uoc.tfg.trabajo-uoc.es
servidor" >> /etc/hosts
}

networkingRestart ()
{
    echo "Reiniciando Red"
    #service networking restart
}

#Los instalamos con el FRONTEND no interactivo para que no pregunte nada.
instalaPaquetes ()
{
    aptitude update
    DEBIAN_FRONTEND=noninteractive aptitude -f -y -o Dpkg::Options::="--
force-confnew" -o Aptitude::CmdLine::Ignore-Trust-Violations=true safe-upgrade
groupadd ftp
    echo "dash        dash/sh boolean false" > dash_answer.txt
    cat dash_answer.txt | debconf-set-selections
    DEBIAN_FRONTEND=noninteractive dpkg-reconfigure dash
    rm dash_answer.txt

    if [ "$HOSTNAME" = "servidor" ]
    then
        DEBIAN_FRONTEND=noninteractive aptitude install -f -y -o
Dpkg::Options::="--force-confnew" -o Aptitude::CmdLine::Ignore-Trust-
Violations=true apache2 apache$
        DEBIAN_FRONTEND=noninteractive aptitude install -f -y -o
Dpkg::Options::="--force-confnew" -o Aptitude::CmdLine::Ignore-Trust-
Violations=true libgd2-xpm
        aptitude install mysql-client-5.1 mysql-server-5.1 sun-java6-jre
sun-java6-bin
        aptitude install -o Dpkg::Options::="--force-confnew"
libapache2-mod-jk
        DEBIAN_FRONTEND=noninteractive aptitude install -f -y -o
Dpkg::Options::="--force-confnew" -o Aptitude::CmdLine::Ignore-Trust-
Violations=true apache2 apache$
        sed -i '/syslocation Unknown/ a \syslocation Centro $TIPO_CENTRO
$NOMBRE, $POBLACION ($PROVINCIA) $CODIGO' /etc/snmp/snmpd.conf

```

```
                DEBIAN_FRONTEND=noninteractive aptitude install -f -y -o
Dpkg::Options::="--force-confnew" -o Aptitude::CmdLine::Ignore-Trust-
Violations=true libgd2-xpm
                DEBIAN_FRONTEND=noninteractive aptitude install -f -y -o
Dpkg::Options::="--force-confnew" -o Aptitude::CmdLine::Ignore-Trust-
Violations=true libcrypt-rc4-p$
                fi
    }

CORRECTO="N"
while [ "$RESP" != "S" ] && [ "$RESP" != "s" ];
do
    obtenerDatosCentro
    verificarDatosCentro
    echo -en "\n¿Es correcto? (s/n) "
    read -n1 RESP
done
calcularVariables
configuraFiles
networkingRestart
instalaPaquetes
```

5. Cliente

5.1 Instalación

La instalación del cliente se realiza dejando todas las opciones por defecto. No se requiere usar ninguna opción en particular.

5.2 Cliente DHCP

Para que nuestros equipos tomen ip a través del servidor debemos de configurar la red. Para ello tenemos que añadir al fichero `/etc/network/interfaces` las siguientes líneas, si es que no vienen por defecto:

```
# The primary network interface
auto eth0
iface eth0 inet dhcp
```

Recordemos que esto es en un equipo real, en una MV seguramente sea `ens33` o similar.

5.3 Cliente FTP

Si se desea instalar el cliente ftp por consola en un equipo cliente debemos de usar el comando siguiente: `apt-get -y install lftp`

5.3.1 Comandos por consola

Los comandos más usados por parte de un cliente ftp son:

- `!ls`, para listar el contenido del directorio actual
- `alias`, para crear alias de comandos y parámetros a nuestra medida. Por ejemplo: `alias dir ls -la`
- `cat`, para mostrar el contenido de un archivo
- `cd`, para movernos entre las carpetas
- `get`, un comando muy importante. Nos permite descargar el archivo remoto y guardarlo en local.
- `jobs`, nos lista la lista de trabajos
- `kill`, nos permite “matar” trabajos
- `mirror`, nos permite obtener una réplica exacta de una carpeta del servidor en nuestra máquina.
- `mkdir`, permite crear directorios en el servidor remoto
- `put`, sube archivos al servidor
- `mv`, renombra archivos
- `open`, seleccionar para abrir un servidor FTP externo

5.3.2 Cliente gráfico

En el caso de que no queramos un cliente FTP por consola podemos instalar una aplicación gráfica, más sencilla de usar y que proporciona más opciones, incluso la conexión por SSH y puertos seguros más modernos que los usados por FPT.

El más usado es Filezilla, y el comando para instalarlo es:

```
apt-get install filezilla
```

5.4 Cliente LDAP

Si hemos instalado un servidor LDAP necesitaremos que nuestros equipos clientes sean capaz de autenticarse por este medio. En este caso no tenemos que instalar ningún paquete si no simplemente configurar unos ficheros.

En el fichero “/etc/nsswitch.conf” añadimos “ldap” a las siguientes líneas dejándolas así:

```
passwd:          ldap compat
group:           ldap compat
shadow:         ldap compat
```

Tras esto editamos el fichero “/etc/pam.d/common-session” añadiendo al final la línea:

```
session required pam_mkhome.so skel=/etc/skel umask=0022
```

Esto creara un directorio en el cliente cuando se autentique un usuario LDAP y no tenga directorio. Tras esto reiniciamos el servicio con el comando:

```
/etc/init.d/nscd restart
```

5.5 Cliente NFS

Si hemos configurado NFS en nuestro servidor necesitaremos configurar los clientes para que puedan usar esta funcionalidad.

Primero, creamos el punto de montaje, en nuestro caso “/home/nfs”

```
mkdir -P /home/nfs
```

Y luego debemos montar el directorio. En nuestro caso, por comodidad, lo haremos directamente en el fichero fstab para que monte siempre al iniciar el equipo. En el fichero “/etc/fstab” añadimos la línea:

```
uoc.example.com:/home/nfs /home/nfs nfs rsize=8192,wsiz=8192,timeo=14,intr
```

Y por último instalamos el paquete “nfs-common”

```
apt-get install nfs-common
```

5.6 Instalar por red

Para instalar por red un equipo debemos de configurar dicho equipo para que arranque por red. Esto se hace entrando en la BIOS y seleccionando ese arranque concreto como primera opción en el menú de arranque por red del equipo.

Dependiendo del equipo el método será ligeramente diferente pero, en general, todos los casos serán parecidos al siguiente ejemplo:

- Arrancar el equipo y pulsar SUPR para entrar en la BIOS
- Seleccionar “advance settings”
- Seleccionar “set boot priority”
- Elegir “lan”, “network”, “pxe” o similar

5.7 Paqueteria educativa: EduBuntu

Nuestro equipo cliente, si hemos elegido la versión normal de Ubuntu, tendrá instaladas unas aplicaciones por defecto pero seguramente no terminen de llegar las expectativas de los profesores para ejercer su trabajo. Existen muchos programas recomendados para el aprendizaje de los alumnos, a continuación mostramos algunos.

Para cambiar nuestra distribución de “Ubuntu” a “EduBuntu” debemos de instalar el paquete correspondiente con el comando:

```
apt-get install edubuntu-desktop
```

La instalación puede ocupar aproximadamente unos 3G así que es mejor tomarselo con calma.

6. Hardware

En este apartado describiremos el hardware necesario para interconectar las diferentes redes y elementos de un centro educativo. Obviamente todos son supuestos, puesto que no pueden ser reproducidos con VMWare.

6.1 Rack

Rack es un término inglés que se emplea para nombrar a la estructura que permite sostener o albergar un dispositivo tecnológico. Se trata de un armazón metálico que, de acuerdo a sus características, sirve para alojar una computadora, un router u otra clase de equipo.⁵

Por explicarlo de forma sencilla, el rack es el “armario” donde pondremos nuestros elementos principales. Dentro del rack un centro educativo debería de tener como mínimo, en términos de hardware para la conexión de los equipos:

- Un router.
- Un switch principal.
- Un SAI.
- Un switch por aula (o un punto de acceso).
- El servidor

Por supuesto, no todos los centros educativos podrán permitirse un elemento de estas características, así que en algunos casos este “rack” no será más que una estantería, una mesa, o cualquier soporte físico donde pongamos el switch principal, el servidor....

6.1.1 Localización del rack

Donde poner el rack es un aspecto a tener en cuenta en toda infraestructura. Lo normal es ponerlo en una sala estanca donde se nos garantice que no pueda entrar agua, así como estar bien reforzada contra elementos externos tales como el fuego o la lluvia.

No obstante, en este caso concreto tenemos que ser realistas, un centro educativo muy probablemente no podrá disponer de una habitación de estas características y terminara instalando el rack en un habitación normal y corriente, o incluso debajo de una escalera, o en secretaría donde transita mucha gente....

Para un centro educativo lo mejor sería buscar una habitación apartada y poco transitada para evitar en la medida de lo posible el ruido que genere.

6.2 Router

Conectado al servidor a través a través de la tarjeta 0 del servidor. Los centros ya suelen tener internet contratada desde hace años así que no debería de haber problemas. Modelos recomendados:

5 <https://definicion.de/rack/>

http://www.tp-link.es/products/details/cat-9_Archer-C1200.html
<https://www.netgear.com/home/products/networking/wifi-routers/R8000.aspx>

Se necesitará un modelo con al menos 2 puertos.

6.3 Switch principal

En nuestro Rack tendremos un switch, conectado al servidor, con la siguiente configuración básica:

- 1 puerto para la red VLAN 1 conectado a la tarjeta correspondiente del servidor
- 1 puerto para la red VLAN 2 conectado a la tarjeta correspondiente del servidor
- 1 puerto para la red VLAN 3 conectado a la tarjeta correspondiente del servidor
- X puertos para los switches de aulas
- X puertos para las zonas de profesores (despachos, sala de profesores)
- X puertos las zonas de gestión (secretaría)

Se considera que el switch principal estará en la red de gestión (192.168.4-) así que, ya que hemos reservado las 50 primeras direcciones podríamos darle la ip 192.168.4.40. En caso de tener más de uno serían la 4.40, 4.41, y así sucesivamente.

En caso de tener más de dos los switches se configurarían en cascada. Es muy recomendable usar switches que permitan cascada hardware, y no solo por software.

Por experiencia propia, es recomendable desactivar el STP (Spanning tree) si nuestro modelo lo permite. Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes. El problema que esto es en casos necesarios en muchos casos para garantizar la disponibilidad de las conexiones.

Más información en: https://en.wikipedia.org/wiki/Spanning_tree

Modelo recomendado: <http://www.dell.com/es/empresas/p/networking-n2000-series/pd>

Observación: en el caso de que no podamos tener un servidor con varias tarjetas y tengamos que usar virtuales (eth1.1, eth1.2... por ejemplo) deberemos de poner un cable entre la tarjeta física y un puerto del switch configurado para las tres vlans. Esto normalmente suele ser llamado configuración “tagged” en los switches.

6.3.1 Ejemplo de configuración

```
Ip: 192.168.4.20
Puerta de enlace: 192.168.4.1
Puertos 1 al 10: vlan 1
Puertos 11 al 20: vlan 2
Puertos 21 al 30: vlan 3
Puerto 31: conexión con el servidor
```

6.4 SAI

Es un dispositivo que gracias a sus baterías puede proporcionar energía eléctrica por un tiempo limitado durante un apagón a todos los dispositivos que tenga conectados. Permite que los equipos conectados a él puedan estar encendidos durante unos minutos, para así apagarlos de forma normal.

Existen muchos modelos diferentes con diferentes precios. En función del presupuesto de nuestro centro se podrán comprar uno u otro. Aquí unos modelos de ejemplo:

<https://www.dns-system.es/sai-trifasico-10000-va-10-kvas,-3f-3f-p-2220.html>
http://tienda.prosegur.es/salicru-sps-1000-soho-sistema-de-alimentacion-ininterrumpida.html?gclid=EAIaIQobChMIIm7Szje6V1wIVSTwbCh2bmQubEAQYAiABEgKNbPD_BwE

https://www.dns-system.es/sai-online-6000-va-lapara-6-kvas-p-1698.html?gclid=EAIaIQobChMIIm7Szje6V1wIVSTwbCh2bmQubEAQYBCABEgJ5CfD_BwE

6.5 Elementos secundarios

Deberemos de dividir nuestro centro en zonas, por ejemplo, imaginemos el siguiente centro:

- Tres plantas.
- En la planta 1 los despachos, la zona de secretaría...
- En la planta 2 las aulas de los alumnos.
- En la planta 3 más aulas.

En este caso concreto la planta 1 tendría un switch configurado de la siguiente manera (imaginemos que tiene 24 puertos):

- 12 bocas para la vlan de profesores
- 12 bocas para la vlan de gestión

Dos de estas bocas irían a parar al switch principal y las otras serían para los equipos de la planta.

En las plantas 2 y 3 tendríamos la misma configuración pero dado que solo hay aulas, tendremos configurados todos los puertos para la red de alumnado.

La dirección ip de los switches debería ser fija y depender de donde estuvieramos, por ejemplo si es un switch de aula tendríamos que darle una ip de la red de alumnos (192.168.8.20 por ejemplo). A continuación veremos varios ejemplos.

6.5.1 Ejemplo: switch en un aula

```
Ip: 192.168.8.21
Puerta de enlace: 192.168.8.1
Red: 192.168.8.0
Puertos 1 al 23: configuración plana para una sola vlan
Puerto 24: conexión con uno de los puertos del switch principal (de esta vlan concreta)
```

6.5.1 Ejemplo: puntos de acceso wifi en la sala de profesores

Ip: 192.168.0.21
Puerta de enlace: 192.168.0.1
Red: 192.168.0.0
Puerto 1: conexión con uno de los puertos del switch principal (de esta vlan concreta)

6.5.2 Ejemplo: puntos de acceso wifi en un aula

Ip: 192.168.8.22
Puerta de enlace: 192.168.8.1
Red: 192.168.8.0
Puerto 1: conexión con uno de los puertos del switch principal (de esta vlan concreta)

7. Clonación de imágenes

Llegados a este punto podemos clonar las imágenes de los equipos clientes y servidor para tenerlos siempre a mano. Gracias a un simple pendrive y Clonezilla tendremos a mano siempre nuestros sistemas operativos en caso de fallo de software irrecuperable.

Describiremos dos sistemas diferentes y diremos sus ventajas e inconvenientes.

7.1 De disco a disco

- Descargamos Clonezilla desde aquí: <http://clonezilla.org/downloads.php>
- Grabamos el programa en un cd o pendrive
- Insertamos un disco duro USB en nuestro equipo, sea cliente o servidor (aunque nuestro servidor tiene 2 discos y necesitaríamos 2)
- Arrancamos el equipo desde Clonezilla
- Elegir la opción “*device-device*”
- Modo experto
- Elegir “*disk to local disk*”

En este punto tendremos que elegir el disco origen y el disco de destino. Tenemos que tener MUCHO cuidado con este punto dado que podemos hacerlo al revés y clonar el disco duro usb al local, lo que es justo lo contrario de lo que queremos.

A partir de aquí todas las opciones que elijamos pueden ser las que nos da el programa por defecto.

7.1.1 Ventajas e inconvenientes

- Permite tener un disco duro idéntico, sustituible fácilmente si en lugar de USB usamos uno internet, por ejemplo un SATA o IDE
- Inutilizamos un disco para otros usos

7.2 De disco a imagen

En este caso el proceso es igual al anterior con la diferencia de que seleccionaremos la opción de clonar de disco a imagen. En este caso se guardará una imagen del disco y no una clonación completa como si nuestro disco duro usb fuera idéntico al local.

7.2.1 Ventajas e inconvenientes

- Procedimiento más rápido y no dependiente de tener más de un disco en el equipo. En nuestro caso es ideal para servidores
- Su recuperación es más lenta dado que no podemos conectar un disco duro clonado directamente al equipo

8. Soporte

En este apartado describiremos las principales incidencias a las que puede enfrentarse el personal docente de un centro y los principales responsables de la coordinación TIC así como posibles soluciones.

Se ofrece también una pequeña guía de actuación para cada tipo de incidencia. Hay que tener en cuenta que cada centro puede tener sus particularidades y esto no puede ajustarse del todo al que estemos nosotros.

8.1 Incidencias de red

8.1.1 No tengo internet en todo el centro

- Comprobar que el router está encendido
- Comprobar que el servidor está encendido
- Comprobar que el switch principal está encendido

Una vez comprobado esto se puede probar a:

- Reiniciar los servicios de dansguardian y squid en el servidor
- Comprobar que el disco duro no está lleno. Esto puede causar problemas de navegación dado que diversos servicios de red escriben en un log y si está lleno puede que no deje navegar.
- Comprobar que la tarjeta de red del servidor que va al switch principal está funcionando correctamente.
- Comprobar que la tarjeta de red del servidor que va al router está funcionando correctamente.
- Comprobar que el cable que va del router al servidor funciona correctamente
- Comprobar que el cable que va del switch principal al servidor funciona correctamente

En caso de que nada de esto resulte pasamos a realizar lo siguiente (no recomendado en primera instancia):

- Reiniciar el router, si no sirve pasar a
- Reiniciar el switch principal, si no sirve pasar a
- Reiniciar el servidor

8.1.2 No tengo internet en una zona/aula

- Comprobar si el switch del aula o de la zona (por ejemplo de la primera planta) está encendido
- Si las aulas van con wifi comprobar si el punto de acceso está encendido
- Si las aulas funcionan con wifi, comprobar la roseta del aula que está conectada al punto de acceso

Si esto no sirve tendremos que comprobar lo siguiente, ya en el armario principal:

- Comprobar que el puerto del switch principal al que va conectada esa zona funciona
- Comprobar el cable de ese puerto
- Comprobar la tarjeta de red del servidor perteneciente a esa zona.

El último punto es importante. Si por ejemplo todas las aulas fallan, pero están repartidas en diferentes plantas dependientes de diversos switches, es posible que lo que falle sea la tarjeta de red concreta del servidor. En este caso concreto podríamos actuar de la siguiente forma:

- Tirar y levantar la tarjeta
- Comprobar el cable que va de esa tarjeta al switch principal

8.1.3 No tengo internet en un equipo

- Comprobar el cable de red del equipo, si está conectado por cable
- Comprobar la tarjeta wifi del equipo, si está conectado por wifi
- Si el equipo está conectado directamente a una roseta probad en otra para descartar problemas de esa roseta
- Probar, si es posible, un equipo en esa misma roseta, para descartar algún problema de software

8.1.4 La conexión va muy lenta

En este caso el procedimiento ideal sería:

- Descargar un fichero bastante grande directamente a través del servidor
- Descargar el mismo desde un equipo de un aula

La descarga desde un equipo de aula obviamente ira más lenta pero aun así la diferencia no debe de ser mucha, en caso de que sea muy notable es posible que haya un bucle de red o que algún elemento de red no funcione correctamente.

En el caso de que la conexión sea lenta incluso desde el servidor lo ideal sería reiniciar el router o llamar directamente a la compañía que provee el servicio de Internet al centr.

8.1.5 Dejar conectado un equipo al router

Imaginemos que no tenemos servidor, pues este tiene alguna avería física que impide su uso. Nos quedaríamos sin conexión en todo el centro. El servicio técnico tardará algunas horas en resolver la incidencia pero por el momento podemos realizar el siguiente procedimiento para tener conexión temporalmente en un equipo:

- Desconectamos el cable que va del router al servidor
- Configuramos la tarjeta de red del equipo cliente como si fuera la de servidor

Así el router creerá que esta conectado al servidor y este equipo al menos tendrá conexión.

8.2 Incidencias de software

8.2.1 No me deja entrar con mi usuario de LDAP

Comprobaremos:

- Que el equipo cliente tenga conexión
- Que el servidor tenga conexión
- Si solo falla nuestro usuario concreto o es algo general
- Si el disco duro está lleno

8.2.2 Quiero recuperar los datos de un usuario de LDAP que no existe

Imaginemos que hemos perdido el acceso a un usuario de LDAP, bien por borrarlo sin querer, un fallo en la copia de seguridad o simplemente hemos perdido la contraseña y no podemos cambiarla por algún motivo.

Ahora imaginemos que la persona que usa dicho usuario quiere recuperar sus datos, pero no tenemos forma de darle acceso a su cuenta, ¿como lo hacemos?. El procedimiento sería el siguiente:

- Entramos a nuestro equipo con un usuario local
- Como *root* podemos entrar en la carpeta del usuario LDAP, generalmente */home/nfs/'nombre'*
- Copiamos el contenido de esta carpeta a un pendrive, al escritorio local, o a donde queramos

Así al menos habremos tenido acceso a los datos de usuario y recuperado, si bien no el acceso, la información de esta persona en concreto.

8.2.3 No se hacen las copias de seguridad

Si nuestro servidor no está haciendo bien las copias de seguridad podemos comprobar:

- Los scripts, para ver si tienen algún error
- Si la partición que las aloja está llena
- Si nuestro servidor está encendido en la hora programada del script

8.2.4 El sistema operativo no arranca

En este caso lo ideal sería reinstalar el sistema operativo completo. Si no es un problema físico del disco duro no habría mayores problemas.

En caso de que el usuario tenga información local en el equipo que quiera recuperar se podría intentar recuperar gracias a un cd live externo, siguiente un manual como este:

<https://gilbertsecure.wordpress.com/2012/01/11/recuperar-datos-como-un-experto-forense-uso-de-un-live-cd-de-ubuntu/>

O también podemos usar: <https://www.softzone.es/2017/02/27/4mrescuekit-live-cd-recuperacion-lo-mas-completo/>

8.3 Incidencias de hardware

8.3.1 Un equipo no enciende

- Comprobar en otro enchufe el equipo
- Comprobar si se enciende el equipo con otro cable de alimentación
- Comprobar si se enciende pero no aparece nada por pantalla, en ese caso realmente puede ser algo del monitor, y sería conveniente probar con otro

En este caso realmente el centro, aparte de comprobar el estado de los equipos, no puede hacer mucho más, y será necesario contactar con el servicio técnico proveedor de los equipos.

8.3.2 Un switch no enciende

Esta casuística puede ser más delicada que la anterior dado que el hecho de que un switch no encienda provocaría que una zona no tuviera conexión, o incluso afectar a todo el centro. En este caso, si se puede, se podría recablear temporalmente los switches para dejar con conexión la zona.

Por ejemplo, imaginemos que tenemos dos switches principales en el RACK:

- El primero entero para la red de alumnado
- El segundo, mitad profesores mitad gestión

¿Qué pasa si el segundo no funciona?. La zona de gestión y profesores no tendrá conexión, y quizás por motivos administrativos sea imprescindible tener conexión ese día en esta zona (por ejemplo por estar en período de poner las notas). Entonces, sacrificaremos la conexión en la parte de alumnos haciendo lo siguiente:

- Quitamos los cables del switch 1
- Quitamos los cables del switch 2
- Ponemos los antiguos cables del switch 2 en el 1
- Dejamos los antiguos cables del switch 1 conectados en el 2

Así tendremos conexión donde nos interesa, si bien dejaremos la parte de las aulas sin conexión. Es importante decir que la configuración de los switches deberá cambiar en consecuencia si queremos evitarnos malos mayores, dado que en el ejemplo anterior los equipos de profesores pasarán a tener ip de alumnado.

En caso de que no nos afecte da igual pero si tenemos configurada alguna regla especial de navegación podemos tener problemas. Por ejemplo con squidguard podemos prohibir la navegación de una web concreta en una red concreta.

8.3.3 El RACK está pitando

Aquí lo primero será, primero, averiguar que elemento pita. Por regla general suelen pitar los siguientes:

- El servidor de nuestro centro.
- El SAI
- El sistema de ventilación propio del armario.

En este caso es recomendable seguir un manual y/o llamar al servicio técnico.

Observación sobre el servidor: este se supone que estará integrado en nuestro armario rack, bien por ser un servidor específico diseñado para este armario o simplemente una torre de ordenador normal usado como servidor.

En el caso concreto del sistema de ventilación, este suele venir integrado dentro de los racks profesionales que podemos adquirir en distribuidores especializados. La mayoría vienen con varios ventiladores para refrigerar bien todos los elementos de su interior.

9. Bibliografía y referencias

- Comandos lftp: <https://www.ochobitshacenunbyte.com/2014/05/20/lftp-transferencia-de-archivos-desde-la-consola-de-comandos/>
- Información general sobre los servicios: <https://es.wikipedia.org/>
- Plantillas de instalación de diversos servicios: <https://www.server-world.info/>
- Las TIC en la educación: <https://es.unesco.org/themes/tic-educacion>
- Los desafíos de las TIC para el cambio educativo, de Roberto Carneiro, Juan Carlos Toscano y Tamara Díaz.
- El cron en Linux: <http://lasegundapuerta.com/index.php/informatica/linux-y-software-libre/1709-comando-cron-en-linux-ubuntu>
- Scripts: http://refspecs.linuxbase.org/LSB_3.0.0/LSB-generic/LSB-generic/iniscrptfunc.html
- Clonezilla: <http://clonezilla.org/clonezilla-live-doc.php>
- Documentación oficial de Ubuntu: <https://help.ubuntu.com/>
- Documentación oficial de EduUbuntu: <https://www.edubuntu.org/documentation>
- Manual básico de scripting en Linux: <https://www.edubuntu.org/documentation>
- Otro manual de scripting: <https://www.shellscript.sh/>
- Pitidos del ordenador (1): <http://www.ajpdssoft.com/modules.php?name=News&file=article&sid=409>
- Pitidos del ordenador (2): <https://www.adslzone.net/postt132331.html>
- Principios básicos de la administración de redes: <http://www.monografias.com/trabajos43/administracion-redes/administracion-redes.shtml>
- Iptables: <https://www.linuxadictos.com/iptables-tipos-de-tablas.html>
- LDAP, definición básica y su principal uso en la educación o la administración: <http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m6/openldap.html>
- Configuración RADIUS: <https://www.packet6.com/install-freeradius-ubuntu-server/>
- Configuración NFS: <http://nfs.sourceforge.net/nfs-howto/ar01s03.html>