

Administración de software de base libre

Jordi Masfret Corrons

Implantación de sistemas operativos (ASX)
Sistemas informáticos (DAM)
Sistemas informáticos (DAW)

Índice

Introducción	5
Resultados de aprendizaje	7
1 Administración de usuarios y grupos en sistemas operativos libres	9
1.1 Introducción, usuarios predeterminados, archivos con información de usuarios y grupos	9
1.1.1 El shell	11
Órdenes básicas	12
1.1.3 Archivo con información de usuarios: /etc/passwd	14
1.1.4 Archivo con información de contraseñas /etc/shadow	15
1.1.5 Archivos con información de grupos: /etc/group	17
1.2 Herramientas de gestión de usuarios y grupos en modo texto	17
1.2.1 Añadir usuarios al sistema: useradd	18
1.2.2 Asignar una contraseña a un usuario: passwd	18
1.2.3 Eliminar usuarios: userdel	19
1.2.4 Deshabilitar usuarios temporalmente	19
1.2.5 Creación, eliminación y asignación de usuarios a grupos: groupadd, groupdel	20
1.2.6 Modificación del grupo de un usuario: usermod	21
1.2.7 Monitorización de usuarios: w, ac, y last	21
1.3 Herramientas de gestión de usuarios y grupos en modo gráfico	22
1.4 Perfiles de usuario locales	28
2 Configuración del protocolo de red en sistemas operativos libres	33
2.1 Parámetros básicos para la configuración de la red en sistemas libres	33
Herramientas de configuración de la red en modo texto	34
2.2.1 Herramienta de información y configuración de la red ifconfig	34
2.2.2 Herramienta de configuración del direccionamiento y rutas: route	35
2.2.3 Herramienta de configuración del nombre del nodo de la red: hostname	37
2.2.4 Herramienta de configuración de la red en sistemas Red Hat / Fedora (system-config-network)	37
2.3 Archivos de configuración de la red	38
2.3.1 Archivo de configuración de la resolución de nombres (DNS): /etc/resolv.conf	38
2.3.2 Archivo de configuración de los nombres de los nodos de la red: /etc/hosts	38
2.3.3 Archivo de configuración de los servicios: /etc/services	39
2.3.4 Archivo de configuración /etc/nsswitch.conf	39
2.3.5 Archivo de configuración /etc/host.conf	40
2.3.6 Archivo de configuración permanente de la red en sistemas Red Hat / Fedora	40
2.3.7 Archivo de configuración en sistemas Debian/Ubuntu	41
2.4 Herramientas de red en modo texto	42
2.4.1 Estado de la conexión: ping	42
2.4.2 Trazar ruta: traceroute	43
2.4.3 Estadísticas de conexiones de red: netstat	43
2.5 Herramientas de configuración y diagnóstico de la red en modo gráfico	44
2.5.1 Herramienta de configuración de la red: NetworkManager	44

2.5.2 Diagnóstico del funcionamiento de la red: aplicación Herramientas de red	48
3 Optimización del sistema en ordenadores portátiles	55
3.1 Gestión energética en sistemas GNU/Linux	56
3.1.1 Hibernar (en el disco)	57
3.1.2 Escalado de frecuencia del procesador	57
3.1.3 hdparm	58
3.1.4 Modo portátil	59
3.1.5 Programas de salvapantallas . 3.1.6	59
acpi	60
3.2 Archivos de red sin conexión	60

Introducción

Esta unidad quiere dar los conocimientos y bases del funcionamiento de la administración básica en un sistema operativo multiusuario basado en código libre, como es el GNU/Linux.

En esta unidad aprenderemos a gestionar los usuarios, configurar la red y optimizar un sistema libre para ordenadores portátiles.

Hemos escogido el sistema GNU/Linux porque, aparte de ser un sistema basado en el software libre, empieza a gozar de una gran popularidad en el ámbito universitario e industrial, y últimamente entre los usuarios personales. Lo consideramos el más representativo dentro de los sistemas operativos multiusuario. Muchos usuarios, pues, lo utilizan como herramienta de trabajo y aprendizaje de sistemas informáticos.

En el apartado “Administración de usuarios y grupos en sistemas operativos libres”, empezamos recordando las principales características de los sistemas operativos multiusuario y cómo el sistema operativo GNU/Linux se identifica con las características de estos sistemas operativos. El estudio continúa con las principales herramientas de gestión de usuarios y grupos que incorpora este sistema, tanto desde la consola en modo texto como en el entorno gráfico.

En el apartado “Configuración del protocolo de red en sistemas operativos libres”, se hace una breve descripción de los parámetros básicos para configurar una red, de cómo se configura adecuadamente en sistemas GNU/Linux, y de qué aplicación práctica podemos encontrar como, por ejemplo, la posibilidad de conectar el ordenador a Internet.

En el último apartado, “Optimización del sistema en ordenadores portátiles”, se estudian aspectos fundamentales en la utilización de sistemas portátiles, como la gestión energética, y la sincronización de directorios y archivos mediante los archivos de red sin conexión.

En esta unidad estudiaremos y utilizaremos principalmente los comandos estándar del shell BASH, que está disponible para todas las distribuciones de GNU/Linux y es el más extendido.

También cabe mencionar que no estudiaremos todas las órdenes de los sistemas GNU/Linux y UNIX en general, ni tampoco todas las posibilidades de cada orden y, por tanto, es necesario consultar continuamente los tipos diferentes de ayuda que GNU/Linux nos suministra.

Dentro del módulo profesional, esta unidad es básica para entender el funcionamiento de los sistemas operativos multiusuario. Se trata de una unidad didáctica eminentemente práctica con un contenido teórico de soporte. Es conveniente que realice las actividades y los ejercicios de autoevaluación del material web.

Resultados de aprendizaje

Al finalizar este núcleo formativo de esta unidad formativa el alumno/a:

1. Configura el software de base, atendiendo a las necesidades de explotación del sistema informático.

- Planifica, crea y configura cuentas de usuario, grupos, perfiles y políticas de contraseñas locales.
- Asegura el acceso al sistema mediante el uso de directivas de cuenta y directivas de contraseña.
- Instala, configura y verifica protocolos de red.
- Analiza y configura distintos métodos de resolución de nombres.
- Optimiza un sistema operativo libre para sistemas portátiles.

1. Administración de usuarios y grupos en sistemas operativos libres

Una de las principales características de un sistema operativo del tipo GNU/Linux es la capacidad de gestionar diferentes usuarios en un mismo sistema. De hecho, se dice que GNU/Linux es un sistema operativo multiusuario, porque incorpora todas las herramientas necesarias para llevar a cabo esta gestión.

Además, GNU/Linux tiene la capacidad de apoyar a diferentes usuarios que trabajen de forma simultánea en la misma máquina, localmente, por medio de una red de área local o, incluso, por Internet.

Cada uno de estos usuarios del sistema tiene asignado un directorio personal, dentro del cual tiene todos los permisos posibles (lectura, escritura, ejecución). Así pues, cada usuario puede tener sus documentos, archivos descargados, preferencias y aplicaciones, sin que exista ninguna interferencia entre ellos. De hecho, un usuario no puede ni leer ni modificar los archivos propios de otros usuarios.

Antes de poder trabajar directamente en un sistema Linux, necesitaremos indicar un nombre de usuario (login) y una contraseña (password); es decir, siempre deberemos identificarnos. La mayoría de sistemas Linux tienen dos modos básicos de funcionamiento, que son los siguientes:

- Modo de texto (consola de texto): modo rápido y austero que se asemeja a antiguos sistemas operativos sin pantalla gráfica, con ratón y características de multitarea y multiusuario.
- Modo gráfico, que parece ser mejor y más vistoso pero que consume muchos más recursos del sistema.

Hoy en día, el modo gráfico es el más habitual en la mayoría de ordenadores personales. Podemos saber que nos conectamos al sistema en modo gráfico porque se nos pregunta el nombre de usuario y contraseña dentro de una ventana ubicada sobre un fondo que suele incluir imágenes gráficas.

1.1 Introducción, usuarios predeterminados, archivos con información de usuarios y grupos

En todas las distribuciones de GNU/Linux modernas, siempre debemos crear al menos un usuario durante el proceso de instalación. En la mayoría de las distribuciones, este usuario no tiene derechos de administración, es decir: es un usuario que puede utilizar el

pero no puede administrarlo. En este sentido podemos decir que éste es el perfil de usuario predeterminado.

Además del usuario predeterminado, en el proceso de instalación deberemos asignar la contraseña de administrador. El nombre del usuario administrador en las diferentes variantes de UNIX y distribuciones de GNU/Linux es primario (root).

Una vez que hemos accedido al sistema con un usuario no administrador, se nos presentará el escritorio. Durante la visualización de los menús, nos daremos cuenta de que se pueden hacer muchas cosas sin tener que introducir órdenes desde el teclado: la mayoría de usuarios tendrán suficiente con el método “situate y clicla”. Pero existen operaciones de una complejidad superior que requieren que el administrador del sistema y de la red “remueva” por las interioridades del sistema. Necesitan una herramienta más potente que un ratón para manejar todas las tareas, que es el shell y que en modo gráfico lo activamos abriendo una ventana de terminal. Esta ventana de terminal también se llama consola.

Para abrir una ventana de terminal o xterm (X es el nombre del software que se encarga de hacer que el entorno gráfico pueda funcionar) es necesario ir al menú de Aplicaciones, Utilidades, Herramientas de sistema, o en el menú Internet , en función del gestor de ventanas que utilizamos. También se podría dar el caso de que hubiera iconos de acceso directo en una ventana xterm.

La ventana de terminal nos da el control del sistema, desde la que se puede realizar casi todo en el sistema. Cada ventana de terminal que se abre debería mostrar siempre un indicador de comandos (command prompt). Así pues, la presencia de este indicador es cómo el sistema indica que se encuentra preparado para recibir las órdenes del usuario y ejecutarlas.

La imagen que ofrecemos a continuación (figura 1.1) es un terminal en una sesión de trabajo en la que aparece un indicador de comandos estándar, que muestra el nombre de entrada del usuario y el directorio de trabajo actual. El directorio personal del usuario está representado por un tilde (carácter ~).

F igura 1. 1. Ventana de terminal en modo gráfico



¿Qué información muestra el indicador de mandatos?

Un indicador de órdenes puede mostrar información diversa, la cual no forma parte de las órdenes que introducimos en el sistema. El tipo de información que suele contener es el nombre de usuario con el que hemos entrado en el sistema, el nombre de la máquina, la hora, etc

1 [usuario@host decir]_

Aquí, usuario será nuestro nombre de acceso, host será el nombre de la máquina a la que hemos accedido, y decir será una indicación de nuestra ubicación actual en el sistema de archivos.

Si el indicador de mandatos se visualiza en pantalla con el carácter \$ seguido de un cursor para invitar al usuario a la introducción de mandatos, entonces el usuario todavía no tiene privilegios de administración.

En muchas distribuciones, para iniciar una sesión como usuario administrador debemos escribir en la ventana de terminal:

```
1 usuario@localhost ~ $ su -
```

Y escribir la contraseña de administrador o usuario primario.

En la distribución Ubuntu se crea un usuario que, mediante su contraseña, puede acceder a las tareas de administración. Podemos acceder a una consola como usuario primario si escribimos:

```
1 usuario@localhost ~ $ sudo su -
```

o bien:

```
1 usuario@localhost ~ $ sudo bash
```

En este caso será necesario escribir la contraseña del usuario con derechos de administración.

Hay que decir que muchas de las tareas de administración en sistemas GNU/Linux implican la modificación de una serie de archivos de configuración del sistema.

Habitualmente, estos archivos de configuración están dentro del directorio /etc, independientemente de la distribución de GNU/Linux que utilizamos.

1.1.1 El shell

Cuando iniciamos una sesión de trabajo en un servidor Linux (sesión de terminal), el sistema nos prepara un espacio de trabajo y un intérprete de órdenes.

El shell es el encargado de recibir las instrucciones introducidas por el usuario, interpretarlas y ejecutarlas. Su disponibilidad se nos muestra mediante un indicador de comandos (command prompt).

En los entornos Linux, el shell más utilizado actualmente es bash (bourne again shell), aunque se está empezando a extender la utilización del shell.

Tipo de órdenes

Clasificaremos las órdenes en dos tipos: las órdenes internas y las órdenes externas.

Buscando órdenes externas
con which

El orden muestra el camino donde se encuentra una determinada orden externa, siempre que se pueda encontrar mediante el camino de búsqueda. Por ejemplo, which ls mostrará el directorio del disco donde se encuentra el orden ls.

Las órdenes internas se encuentran implementadas dentro del mismo intérprete de órdenes y, gracias a ello, éste las reconoce de inmediato y las ejecuta al instante. Las órdenes externas, en cambio, se encuentran implementadas fuera de el shell, ubicadas en algún espacio del disco. Esto hace que el sistema tenga que dedicar un tiempo a la búsqueda de este tipo de órdenes en el disco.

El tiempo dedicado a buscar las órdenes externas en el disco es corto, gracias a un mecanismo que indica al intérprete de órdenes cuáles son los lugares en los que las que buscar. Este mecanismo se llama camino de búsqueda (search path) y es una lista de directorios que el shell utilizará para buscar los mandatos externos.

Piense que si un sistema está formado por unos dos mil directorios, el camino de búsqueda puede consistir en una lista de sólo unos siete u ocho, con lo que el tiempo de búsqueda se reduce notablemente.

Son ejemplos de órdenes internas las siguientes: cd, exec, arg, eval y exit.

Son ejemplos de órdenes externas las siguientes: ls, who, date y man.

1.1.2 Órdenes básicas

A continuación, en la tabla 1.1, tenemos las órdenes básicas, con las que es necesario empezar:

Tabla 1. 1. Órdenes básicas en Linux

Orden	Función
ls	Muestra una lista de archivos en el directorio de trabajo actual (como decir en el sistema DOS).
cd directorio	Cambia al directorio especificado.
passwd	Cambia la contraseña del usuario actual.
file nombreadarchivo	Muestra el tipo de archivo del archivo con nombre nombre-archivo.
cat archivodetext	Escribe en pantalla el contenido de archivo de texto.
pwd	Muestra el directorio de trabajo actual.
exit o logout	Cierra la sesión actual.
man orden	Muestra las páginas del manual referentes al orden.
info orden	Muestra las páginas de información referentes al orden.
acercas cadena	Buscar el texto cadena dentro de la base de datos whatis.

Las órdenes se introducen después del indicador de órdenes, dentro de una ventana de terminal en modo gráfico o en modo de texto, seguidas de la tecla de regreso.

Algunas órdenes se pueden llamar escribiendo su nombre, y dan un resultado, como por ejemplo ls. Otros permiten especificarles opciones.

Las opciones indican a un comando que tenga un comportamiento diferente al habitual. Añadir una opción a un comando es escribir detrás una letra, habitualmente precedida de un guión (-).

Por ejemplo, el comando `ls` se comporta de manera diferente a la hora de elegir qué archivos debe mostrar cuando se añade detrás la opción `-a`, formando la instrucción `ls -a`.

La opción `-a` indica a los que muestre todos los archivos para mostrar, incluso los ocultos. El mismo carácter de la opción puede tener distinto significado para otro orden. Los programas GNU también aceptan opciones largas, precedidas de dos guiones, como `ls --all` (equivalente a `ls -a`). Sin embargo, existen órdenes que no permiten opciones.

Las órdenes también permiten que se les indique sobre qué objetos debe actuar. Cada objeto especificado se llama parámetro.

Los parámetros pasados a un comando son las especificaciones del objeto u objetos sobre los que queremos que este comando actúe.

Un ejemplo de orden con un parámetro es `ls /etc`, donde el directorio `/etc` es el parámetro del mandato `ls`. Este parámetro indica a los que queremos ver qué hay dentro del directorio `/etc`, en lugar de obtener el resultado por defecto, que consistiría en ver el contenido del directorio actual, sólo introduciendo el comando `l` seguida de la tecla de retorno. Algunas órdenes requieren parámetros obligatoriamente, y para otros los parámetros son opcionales.

Cuando un parámetro es opcional, se suele escribir entre corchetes en la descripción de la sintaxis del orden. Estos corchetes no deben introducirse: sólo indican que lo que hay dentro se puede escribir o no.

Comprobando la ayuda online de un mandato, podremos saber si el mandato acepta opciones y parámetros, y cuáles de ellos son válidos. En la tabla 1.2 puede ver cómo pedir la ayuda:

Por ejemplo, `cd [directorio]` indica que la instrucción `cd` es válida, y las instrucciones `cd homejep` y `cd usrshare` también lo son.

Tabla 1. 2. Órdenes para obtener ayuda

Orden de ayuda	Descripción
<code>ls --help</code>	Muestra la ayuda (breve) del mandato <code>ls</code> .
<code>man ls</code>	Muestra el manual (más extenso) del mandato <code>ls</code> .

En un orden determinado, las opciones y parámetros se pueden combinar.

Un ejemplo de combinación dentro de la misma instrucción es `ls -a etc`, fruto de la combinación de la opción `-a` y del parámetro `etc`. También hay que mencionar que existen órdenes que aceptan opciones y parámetros múltiples. Un ejemplo sería `ls -a -l -y etc home`, en el que se combinan tres opciones y dos parámetros. Hay órdenes que admiten todas las opciones juntas y con un solo guión (o en ocasiones incluso sin guión). Así nos ahorramos el haber

de teclear en exceso! En el caso de la instrucción anterior, podría haber sido el -ali etc /hombre.

Caracteres comodín

Los shell que reciben nuestras instrucciones entienden una serie de comodines que permiten realizar abreviaciones que después expanden en listas de archivos. Por ejemplo, un asterisco (*) representa cualquier número de cualquier carácter. La instrucción ls c*.txt crearía la lista de todos los archivos del directorio actual cuyo nombre comienza por la letra c, y termina con los caracteres .txt. Cada intérprete puede tener determinados comodines propios. Los caracteres comodín más habituales son el asterisco (*) y el interrogante (?).

Por ejemplo, l?ouse mostrará archivos con el nombre house y mouse, pero no grouse.

¿El carácter ? coincide con un solo carácter.

Además, existen otras formas para refinar la especificación de caracteres en una determinada posición del nombre. Los caracteres a elegir o filtrar deben escribirse entre corchetes []. Véanse los caracteres comodín de la tabla 1.3.

Tabla 1. 3. Caracteres comodín

Carácter/s	Sustituyen
?	Cualquier carácter.
*	Cualquier secuencia de caracteres.
[abc]	Uno de los tres caracteres a, bueno c.
[^123]	Los caracteres que no son 1, 2 o 3 (también es válido el carácter ! en lugar de ^).
[ah]	Caracteres entre aih, ambos inclusive.

Se pueden combinar más de un carácter comodín. Los caracteres comodín pueden realizarse servir en instrucciones que trabajen sobre archivos y directorios, como por ejemplo ls.

1.1.3 Archivo con información de usuarios: /etc/passwd

En los sistemas GNU/Linux, la información sobre los usuarios está localizada en el archivo /etc/passwd.

Si miramos su contenido, obtendremos una lista similar a la del ejemplo 1:

Ejemplo 1. Contenido del archivo etcpasswd

```
1 $cat /etc/passwd
2 . . .
3 gdm:x:42:473::/var/lib/gdm:/sbin/nologin
4 root:x:0:0:root:/root:/bin/bash
5 angel:x:502:1001::/hombre/angel:/bin/bash
6 anna:x:503:1001::/hombre/angel:/bin/bash
```

Y describe el siguiente tipo de información:

```
1 nombre_usuario:password:UID:GID:comentarios:directorio_hombre:shell_de_acceso
```

El significado de cada elemento lo podemos ver en la tabla 1.4.

Tabla 1. 4. Elementos del archivo /etc/passwd.

Concepto	Significado
nombre_usuario	Login del usuario (nombre que utiliza el usuario para iniciar la sesión en el sistema).
password	La palabra de paso en el sistema (contraseña). De hecho, la contraseña se almacena en el archivo /etc/shadow, que es un archivo encriptado.
UID	User identification. Código de identificación del usuario.
GID	Group identification. Código de identificación del grupo al que pertenece.
Directorio_hombre	Definición del directorio personal (o por defecto) del usuario.
Shell_de_acceso	Intérprete de órdenes que utiliza el usuario en sus sesiones.

Algunos de los usuarios corresponden a servicios del sistema: podemos identificarlo porque no tienen ningún shell asociado, y no tienen un directorio personal dentro de /hombre, como el resto de usuarios.

En el ejemplo 1, el usuario gdm corresponde a un usuario asociado a un servicio del sistema (la pantalla de bienvenida o de login). Lo podemos ver porque no tiene ningún intérprete de órdenes asociado (/sbin/nologin), y su directorio personal es /var/lib/gdm, en cuentas de un subdirectorio dentro del directorio /hombre.

1.1.4 Archivo con información de contraseñas /etc/shadow

Se considera un riesgo de seguridad mantener contraseña alguna en el archivo /etc/passwd, porque cualquier persona con derechos de lectura puede ejecutar un programa y obtener las contraseñas sin mucha dificultad. Para evitar este riesgo, se utilizan contraseñas ocultas de forma que sólo aparezca una x en el campo de contraseña del archivo /etc/passwd.

Las contraseñas se guardan en el archivo /etc/shadow, al que sólo tiene acceso el usuario administrador.

Todas las distribuciones actuales de GNU/Linux permiten la utilización de contraseñas ocultas. Veamos el contenido aproximado del archivo /etc/shadow:

```
1 root@usuario~desktop:~# cat /etc/shadow
2 root!:14921:0:99999:7:::
3 daemon*:14837:0:99999:7:::
4 bin*:14837:0:99999:7:::
5 . . .
6 gdm*:14837:0:99999:7:::
7 usuario:$6$EGXuQLzP$v6fEN4db4WimengsM1ZuXNxp3gQvgz3voPNUx3BuxlotoS1D1I01THSB.
  kAZHZ
8 61WK5F27vyxrDym691GIVsH0:14921:0:99999:7:::
9 vboxadd!:14929::::
```

Hay dos algoritmos de encriptación de las contraseñas: MD5 y DES. MD5 es un método más fuerte de encriptación.

Los campos están separados por dos puntos, y están en orden:

- Nombre de usuario para iniciar la sesión
- Contraseña encriptada del usuario
- El número de días desde el 1 de enero de 1970 hasta el último cambio de contraseña. Esta fecha es conocida en el mundo de UNIX como epoch.
- El número de días que deben pasar antes de que la contraseña se pueda cambiar. Este campo indica un mínimo de días de la validez de la contraseña.
- El número de días después de los cuales la contraseña debe cambiarse. Este campo indica un máximo de días de validez de su contraseña. Puede modificarse para forzar el cambio de contraseña.
- El número de días antes de que se avise al usuario de que su contraseña expirará.
- El número de días después del cambio de contraseña y que hace que se inhabilite la cuenta de usuario.
- El número de días desde el 1 de enero de 1970 en los que la cuenta de usuario se ha deshabilitado.
- El último campo reservado, que actualmente no se utiliza para nada.

El archivo `/etc/shadow` sólo debería tener permisos de lectura y escritura para el usuario administrador; el resto de usuarios no debería tener ningún permiso de lectura ni de escritura (cadena de permisos: 600).

Por lo que respecta a la elección de las contraseñas, cabe decir que debe establecerse un compromiso entre la facilidad para recordar la contraseña y la dificultad que puede tener una persona ajena para obtenerla. Por ejemplo, contraseñas como 123456, la fecha de nacimiento, el nombre o apellidos, deben evitarse, porque facilitan muchos accesos indebidos al sistema.

También se podría tipo contraseña utilizar una serie de caracteres que han prácticamente un usuario ilegítimo accediera al sistema, pero al mismo tiempo sería muy difícil de recordar por parte del usuario. En cualquier caso hay una serie de consejos que podemos valorar a la hora de elegir y mantener una buena contraseña:

- Incluir signos de puntuación y/o cifras
- Mezclar mayúsculas y minúsculas
- Una longitud mínima de ocho caracteres
- Sustituir caracteres por otros de aspecto similar, como la letra S por el símbolo \$
- No dar nunca la contraseña a nadie

- No anotarla nunca
- No enviarla por correo electrónico
- Cambiar la contraseña a menudo.

1.1.5 Archivos con información de grupos: /etc/group

Hay un archivo llamado /etc/gshadow, que contiene información encriptada sobre los grupos de usuarios.

La información sobre los grupos del sistema, y su identificador, está localizada en el archivo /etc/group, y las contraseñas de grupo están en el archivo /etc/gshadow.

Podemos mostrar el contenido de este archivo de configuración mediante el mandato siguiente:

```
1 $ cat /etc/group
2  . . .
3  alumnos:x:1001:angel,anna
```

En este archivo aparece la siguiente información:

```
1 nombre_grupo:password:GID:lista_usuarios
```

Puede ver sus elementos y su significado en la tabla 1.5.

Tabla 1. 5. Elementos del archivo **/etc/group**.

Concepto	Significado
nombre_grupo	Nombre del grupo del sistema.
password	Contraseña de grupo.
GID	Identificador del grupo.
lista_usuarios	Todos los usuarios que pertenecen a ese grupo.

1.2 Herramientas de gestión de usuarios y grupos en modo texto

Sólo el usuario administrador del sistema (superusuario o usuario primario) puede administrar las cuentas de usuarios y grupos, creándolas de nuevo, borrando o modificando las cuentas. Los usuarios normales, que no tienen derechos de administración, no pueden utilizar ninguna herramienta de gestión de usuarios, ni pueden modificar los parámetros de su cuenta de usuario como, por ejemplo, el directorio personal o contraseña.

El shell de GNU/Linux permite llevar a cabo toda esta gestión de usuarios de una forma relativamente sencilla a la vez que potente. Estudiaremos las órdenes principales que nos permiten realizar esta gestión.

Recordemos que, para realizar estas tareas de administración, debemos autenticarnos como usuario primario; una vez hecho esto, podemos examinar y ejecutar todas las órdenes administración de usuarios y grupos. Veamos las principales con los parámetros más interesantes.

1.2.1 Añadir usuarios al sistema: useradd

La sintaxis de esta orden es:

```
1 #useradd [-d <directorio hombre> -m] [-g <grupo al que pertenece>] [-u <UID>] <login>
```

Ejemplo 2

```
1 #useradd luis
2 #useradd -d /home/marco -m marco
```

El parámetro -m fuerza a crear un directorio personal dentro de /home, y el parámetro -d especifica cuál es este directorio. En el ejemplo 2, es /home/marco/.

Utilizando la opción -D del comando useradd (#useradd -D {...}), añadiremos un usuario con las opciones por defecto.

1.2.2 Asignar una contraseña a un usuario: passwd

El mandato passwd permite al usuario administrador asignar una contraseña a cualquier usuario del sistema. Tiene un único parámetro que es el nombre de usuario del que queremos modificar la contraseña.

```
1 #passwd <login>
2 Introduzca la nueva contraseña de UNIX:
3 Vuelva a escribir la nueva contraseña de UNIX:
4 passwd: la contraseña se ha actualizado satisfactoriamente
```

Ejemplo 3

```
1 #passwd luis
2 Introduzca la nueva contraseña de UNIX:luis03
3 Vuelva a escribir la nueva contraseña de UNIX:luis03
4 passwd: la contraseña se ha actualizado satisfactoriamente
```

Seguridad de contraseña

La contraseña se genera mediante una función resumen (hash), que representa unívocamente en cada contraseña. El sistema sólo guarda la contraseña encriptada, y en jefe caso se guarda el original.

Las contraseñas son una parte integral de la seguridad de los sistemas basados en el GNU/Linux, y además son la parte más visible para el usuario.

El administrador del sistema debería seguir una política de gestión de las contraseñas, que debería incluir lo siguiente: las contraseñas permitidas y prohibidas, la

frecuencia de los cambios obligatorios de contraseñas, la recuperación o repuesto de contraseñas perdidas, y la forma de gestionar las contraseñas por parte de los usuarios.

1.2.3 Eliminar usuarios: userdel

Podemos eliminar a un usuario con userdel (#userdel login), añadiendo la opción `-r` si queremos que también nos elimine su directorio personal.

Ejemplo 4

```
1 #userdel -r alumno1
```

Esta orden eliminará al usuario alumno1 del sistema, así como su directorio personal con todos los archivos.

1.2.4 Deshabilitar usuarios temporalmente

Existe la posibilidad de deshabilitar un usuario de forma temporal, sin haberlo de borrar. Esto puede ser útil, por ejemplo, cuando el usuario no ha pagado la utilización de la máquina, o bien el administrador del sistema piensa que alguien ha obtenido su contraseña por medios poco adecuados.

La forma más sencilla de deshabilitar una cuenta es cambiar su intérprete de órdenes para un programa que escriba un mensaje que diga al usuario que contacte con el administrador del sistema para evitar más problemas.

Una forma sencilla de crear este programa sería crear un script similar al siguiente:

```
1 #!/usr/bin/tail +2
2 Esta cuenta de usuario ha sido suspendida a causa de un fallo de seguridad.
3 Avise al administrador del sistema lo antes posible.
```

Los dos primeros caracteres (#!) dicen en el núcleo del sistema que el resto de la línea es un mandato que se debe ejecutar para interpretar este archivo. El orden tail hace que se muestren por pantalla las dos últimas líneas del archivo (el mensaje).

Si, por ejemplo, el usuario que se supone que tiene un problema de seguridad se llama billg, el administrador del sistema debe hacer lo siguiente:

```
1 # chsh -s
2 /usr/local/lib/no-login/security billg
3 # su - billg
4 Esta cuenta de usuario ha sido suspendida a causa de un fallo de seguridad.
5 Avise al administrador del sistema lo antes posible.
6 #
```

Con su, el administrador podría comprobar que los cambios aplicados funcionan.

Los scripts tail deben guardarse en un directorio diferente para que su nombre no interfiera con los comandos normales del usuario.

1.2.5 Creación, eliminación y asignación de usuarios a grupos: groupadd, groupdel

La sintaxis del mandato groupadd es:

```
1 #groupadd -[g GID] <nombre del grupo>
```

Ejemplo 5

```
1 # groupadd alumnos
```

En este ejemplo, añadimos un grupo de usuarios llamado alumnos.

También podemos modificar parámetros de configuración con el mandato groupmod o eliminar grupos con el mandato groupdel.

Asignación de usuarios a grupos:

```
1 # useradd -g alumnos angel
2 # useradd -g alumnos anna
```

el resultado dentro de /etc/group:

```
1 **alumnos:x:502:angel,anna**
```

Es decir, añadimos dos usuarios llamados angel y anna, y hacemos que pertenezcan al grupo alumnos.

Hay que tener en cuenta que un usuario puede pertenecer a más de un grupo. Esto es especialmente útil para gestionar el acceso de usuarios de diferentes grupos a uno mismo recurso.

También se puede cambiar el grupo al que pertenece un usuario después de haberlo creado.

Por ejemplo, si ejecutamos el comando:

```
1 # useradd alumno
```

Veremos que el resultado dentro de /etc/passwd es:

```
1 alumno:x:501:501::/hombre/alumno:/bin/bash
```

Es decir, por defecto se crea un nuevo grupo de usuarios para cada usuario que añadamos al sistema. Si nos fijamos en la línea correspondiente dentro de /etc/group del grupo alumnos:

```
1 alumnos: x: 502:
```

Por tanto, el ID del usuario alumno es 501, la de su grupo es 501, pero la del grupo alumnos es 502.

1.2.6 Modificación del grupo de un usuario: usermod

El mandato usermod permite cambiar el grupo primario de un usuario después de haberlo creado. Si escribimos el orden:

```
1 # usermod -g alumnos alumno
```

Y ahora miramos el archivo /etc/passwd:

```
1 alumno:x:501:502::hombre/alumno:/bin/bash
```

Veremos que ha cambiado el ID de grupo, que ahora es 502, que coincide con el ID del grupo de alumnos: el usuario alumno pertenece ahora al grupo alumnos.

1.2.7 Monitorización de usuarios: w, ac, y last

La monitorización de la actividad del usuario es una tarea fundamental de el administrador del sistema para comprobar cómo se utilizan los recursos del sistema.

Monitorización de usuarios

La tarea de monitorización de los usuarios es básica para controlar cómo se utilizan los recursos del sistema informático. Un buen administrador de sistemas puede monitorear casi cualquier cosa que hagan los usuarios del sistema.

Veamos las órdenes principales de monitorización de la actividad de los usuarios:

- El comando w proporciona información sobre qué usuarios están autenticados en el sistema, desde qué momento han iniciado la sesión y qué están haciendo. Ningún usuario puede esconderse del superusuario o usuario primario. Podemos utilizar, como parámetro del comando w, el nombre de un usuario concreto para mostrar sólo qué está haciendo ese usuario.

Si ejecutamos el comando w, podemos obtener una salida similar a la siguiente:

```
1 root@usuario-desktop:~# w 18:09:10
2   up 14 min, 2 usuarios, load average: 0,05, 0,15, 0,18 USER TTY FROM LOGIN@
3   IDLE JCPU PCPU WHAT usuario tty7 :0 17 :58 1:14m 6.76s
4   0.53s gnome-session usuario pts/0 :0.0 17:58 0.00s 0.60s 1.63s gnome-terminal
5
```

- Con el comando ac, también podemos ver el tiempo total de conexión de un usuario al sistema. Si no está instalada por defecto, podemos instalarla con el mandato `# apt-get install acct`.

Si ejecutamos el comando ac desde la línea de comandos, obtendremos una salida similar a la siguiente:

```
1 $usuario@usuario-desktop:~$ ac total
2   13.86
```

El mandato `ac` accede al archivo `/var/log/wtmp` para obtener esta información.

- El mandato `last` busca en el archivo `/var/log/wtmp` y hace una lista de todos los usuarios que han iniciado y detenido la sesión desde su creación.

La salida del orden `last` sería similar a la siguiente:

```
1 usuario@usuario~$ last wtmp begins
2      Fri Dec 3 18:22:54 2010
```

Otro comando interesante es `lastb`, que muestra todos los intentos fallidos de autenticación o de iniciar sesión en el sistema. Es útil para determinar si un usuario legítimo tiene problemas para acceder al sistema o bien si un hacker está intentando acceder a él.

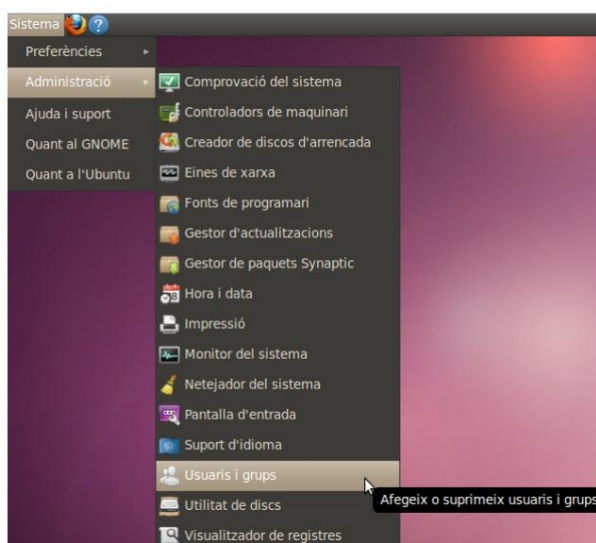
1.3 Herramientas de gestión de usuarios y grupos en modo gráfico

Además de las herramientas de gestión de usuarios, la mayoría de distribuciones de GNU/Linux disponen de herramientas de administración en el entorno gráfico. En este apartado nos fijaremos en las herramientas de administración de usuarios y grupos de que dispone uno de los entornos gráficos más extendidos: Gnome, y concretamente sobre una de las distribuciones más utilizadas, como es Ubuntu en la versión 10.04 LTS. Esta versión tiene un período de mantenimiento y actualizaciones de seguridad más largo (hasta abril de 2013).

De todas formas, las herramientas estudiadas en este apartado son similares a las que se presentan en cualquier otra distribución de GNU/Linux que funcione con el entorno Gnome.

Para acceder a las herramientas de administración de usuarios y grupos en Ubuntu 10.04 LTS, vamos al menú Sistema>Administración>Usuarios y grupos. Puede verlo en la figura 1.2.

Figura 1. 2. Acceso a las herramientas de administración de usuarios y grupos en Ubuntu



Una vez hacemos un clic en este apartado, se abre un cuadro de diálogo que nos pide la contraseña de usuario para poder realizar estas tareas de administración, y después de escribirla se abre la aplicación de gestión de usuarios y grupos, como puede ver en la figura 1.3.

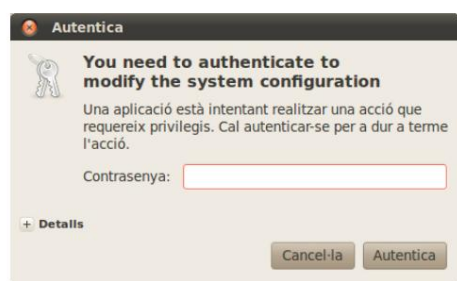
Figura 1. 3. Aplicación de gestión de usuarios y grupos de Ubuntu 10.04 LTS



Las herramientas de gestión de usuarios y grupos en modo gráfico facilitan mucho esta labor de administración.

Lo primero que podemos hacer es gestionar los parámetros avanzados sobre un usuario, en cuyo caso, lo que ha iniciado la sesión (que tiene de nombre de usuario usuario). Nos pedirá la contraseña del usuario para acceder a estos parámetros, como se muestra en la figura 1.4.

Figura 1. 4. Autenticación como usuario administrador



Petición de contraseña de administración

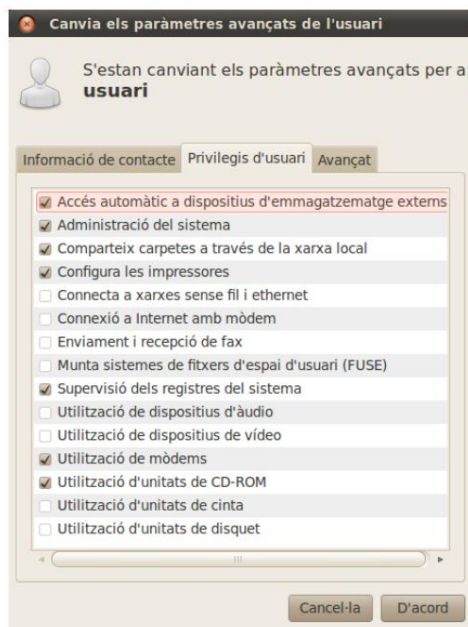
Una vez hecho esto se nos presentará un cuadro de diálogo que nos permitirá modificar la información de contacto del usuario, como se muestra en la figura 1.5.

Figura 1. 5. Información de contacto del usuario



Si hacemos un clic en la pestaña llamada Privilegios de usuario, accedemos a un cuadro de diálogo que nos permite modificar las atribuciones y los derechos del usuario, como puede ver en la figura 1.6.

Figura 1. 6. Cuadro de diálogo que permite configurar los derechos del usuario (privilegios de usuario)



Utilizando la herramienta de gestión de privilegios de los usuarios, podemos evitar que éstos realicen ningún acto que ponga en peligro el propio sistema operativo.

De estos privilegios de usuario, lo más importante es el de administración del sistema, porque a partir de éste podemos modificar y administrar el sistema.

Si hacemos un clic en la pestaña Avanzado, accedemos a un cuadro de diálogo que permite modificar el directorio personal del usuario, el shell, el grupo principal al que pertenece el usuario, y el identificador numérico de este usuario. Lo puede ver en la figura 1.7.

Figura 1. 7. Más parámetros avanzados



En esta pestaña se puede cambiar el directorio personal, su identificador, el shell y el grupo principal del usuario

Una vez modificados todos los parámetros del usuario, pulsamos Aceptar, y volvemos al cuadro de diálogo de la figura 1.3.

Como en cualquier sistema operativo multiusuario, Ubuntu 10.04 LTS nos permite añadir nuevos usuarios al sistema, además de lo que ya se ha creado durante el proceso de instalación. Basta con pulsar el botón Agregar en el cuadro de diálogo de la figura 1.3, y nos aparece un cuadro de diálogo como el de la figura 1.8.

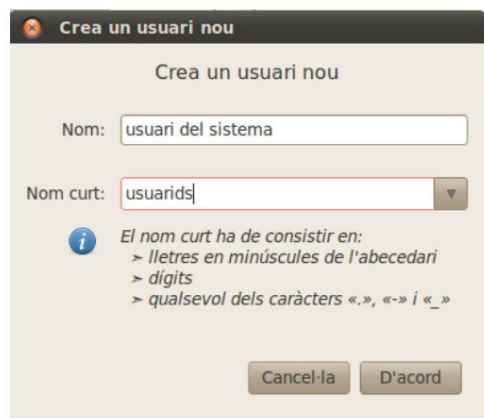
Figura 1. 8. Creación de un nuevo usuario



En este formulario podemos escribir el nombre completo del usuario y el apodo que va a utilizar para entrar en el sistema

El nombre corto se genera automáticamente cuando insertamos el nombre del usuario, pero podemos modificarlo, tal y como muestra la figura 1.9.

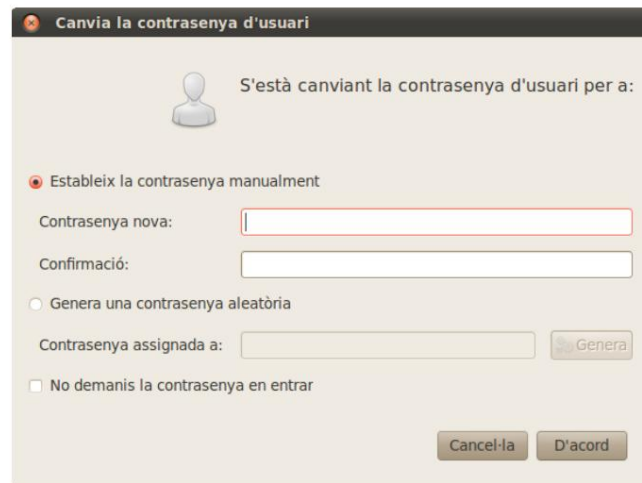
Figura 1. 9. Inserción del nombre de usuario



Nombre de usuario del sistema que queremos crear de nuevo

Una vez se ha escrito el nombre de usuario creado, pulsamos el botón Aceptar, y nos pedirá de nuevo la contraseña del usuario con el que hemos iniciado la sesión, para llevar a cabo el alta del usuario en el sistema. Hecho esto, deberemos establecer la contraseña de este nuevo usuario, o dejar que el mismo sistema genere una aleatoria. Lo puede ver en la figura 1.10.

Figura 1. 1 0. Inserción de la contraseña para el nuevo usuario



Es necesario escribir dos veces la contraseña del nuevo usuario para que sea válida

Hay que tener en cuenta que, para que la contraseña sea segura, debe contener una combinación de caracteres alfabéticos y numéricos, y debe tener una longitud mínima de seis caracteres. Opcionalmente podemos hacer que no sea necesaria contraseña para entrar en el sistema, pero esto no es muy recomendable.

Una vez terminado todo el proceso, volveremos a la pantalla de inicio de la herramienta de administración de usuarios y grupos, pero ahora, en la lista nos aparecerá un usuario adicional, como puede ver en la figura 1.11 .

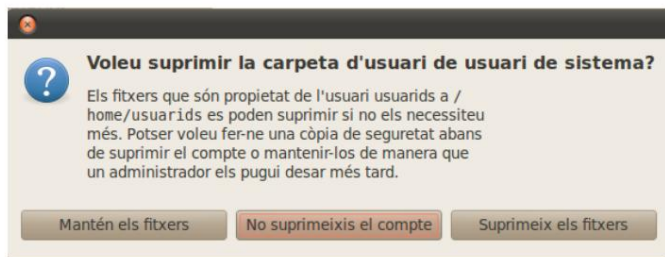
Figura 1. 1 1. Lista de usuarios del sistema



En esta lista ya aparece el usuario que hemos terminado de crear

Otra tarea básica para la gestión de usuarios es darles de baja del sistema, eliminando sus cuentas de usuario y opcionalmente sus archivos y directorios personales. Para ello, simplemente hay que seleccionar al usuario que queremos suprimir y pulsar el botón Eliminar. Si hacemos esto, el sistema nos pedirá la contraseña de un usuario administrador, y seguidamente nos mostrará el cuadro de diálogo de la figura [1.12](#).

F igura 1. 1 2. Ventana de diálogo de supresión de un usuario



Podremos escoger si eliminamos o no los archivos del usuario

En este cuadro podemos elegir no suprimir la cuenta, suprimir el usuario manteniendo sus archivos, o suprimir el usuario y sus archivos.

En cuanto a la gestión de los grupos, para acceder a ellos es necesario pulsar el botón Gestiona los grupos, desde la ventana principal de la aplicación de gestión de usuarios y grupos. Aparecerá el cuadro de diálogo de la figura 1.13.

F igura 1. 1 3. Gestión de grupos



Cuadro de diálogo con los parámetros de los grupos

Si seleccionamos uno de los grupos de la lista y hacemos clic en Propiedades, aparece un cuadro de diálogo en el que podemos asignar usuarios al grupo seleccionado. Lo puede ver en la figura 1.14.

F igura 1. 1 4. Asignación de usuarios al grupo seleccionado



Propiedades del grupo seleccionado de la lista

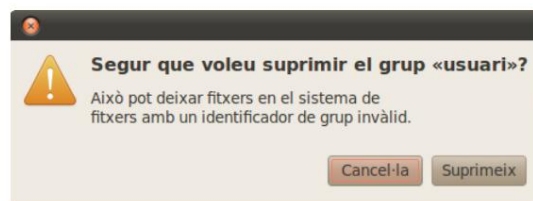
Si hacemos un clic en el cuadro de confirmación junto al nombre del usuario, haremos que éste pertenezca al grupo en cuestión. Podemos asignar tantos usuarios como queramos a un grupo determinado.

Por defecto, por cada usuario que creamos en el sistema, se crea un grupo con el mismo nombre. Esto no es muy conveniente, y es más adecuado agrupar a todos los usuarios similares en un solo grupo.

Hecho esto, es aconsejable suprimir los grupos que ya no son necesarios.

Para ello, basta con seleccionar el grupo que queremos eliminar y pulsar el botón Eliminar. Nos aparecerá un cuadro de diálogo que nos pedirá la confirmación de la supresión de este grupo, como se ve en la figura 1.15.

Figura 1. 15. Supresión de grupos de usuarios



Confirmación de la supresión de un grupo de usuarios

Si queremos, también podemos crear un nuevo grupo de usuarios pulsando el botón Agregar. El sistema mostrará el cuadro de diálogo de la figura 1.16. Podemos insertar el nombre del grupo, su identificador y asignar usuarios a ese grupo.

Figura 1. 16. Creación de grupos de usuario



1.4 Perfiles de usuario locales

Cuando se crea un nuevo usuario del sistema mediante el mandato useradd, éste lee el archivo /etc/default/useradd para definir las variables que utilizará este mandato.

Si visualizamos el contenido de este archivo, veremos algo parecido a lo siguiente:

```
1 # useradd defaults file
2   GROUP=100
3   HOMBRE=/hombre
4   INACTIVE=-1
```

```
5  EXPIRE=  
6  SHELL=/bin/bash  
7  SKEL=/etc/skel
```

En este archivo podemos modificar el valor de las variables según nos convenga:

- **HOME:** por defecto, el directorio de inicio del usuario se crea dentro del directorio /hombre. El valor de esta variable se puede cambiar si así lo desea el administrador del sistema. Por ejemplo, en el caso de un sistema que hospeda sitios de red virtuales, se puede utilizar la variable /var/www simplificando las tareas administración del sistema. En otros casos como, por ejemplo, un servidor de correo, en el que se desea aplicar una sola cuota de disco general, para el buzón de correo, y carpetas de correo en el directorio de inicio, se podría crear un directorio dentro de /var como, por ejemplo, /var/home o /var/users, de forma que al aplicar la cuota de disco sobre la partición /var esto implicaría tanto la buzón de entrada del usuario (/var/spool/mail/usuario) como las carpetas de correo en el directorio de inicio del usuario (/var/home/usuario/mail).
- **SHELL:** Define el shell que se utilizará con las nuevas cuentas de usuario. Por defecto, el sistema asigna a esta variable el valor /bin/bash, por tanto, el shell predeterminado es el BASH (Bourne Again SHell). De todas formas, si el sistema se utiliza como servidor, se puede asignar otro valor.

En este caso, fíjese en el valor /sbin/nologin, por lo que no se permite la entrada en el sistema a un usuario con este tipo de cuenta, y se muestra un mensaje que dice que la cuenta de usuario no está disponible, o el texto que hay en el archivo /etc/nologin.txt.

Se utiliza como forma de reemplazar al shell cuando las cuentas de usuario han sido deshabilitados o no se desea que accedan a un shell. Este programa almacena, en el registro del sistema, cualquier intento de acceso. Para utilizarlo como valor de la variable SHELL, basta con cambiar SHELL=/bin/bash por el valor SHELL=/sbin/nologin. De este modo, el archivo /etc/default/useradd debería quedar de la siguiente manera:

```
1 # useradd defaults file  
2  GROUP=100  
3  HOMBRE=/hombre  
4  INACTIVE=-1  
5  EXPIRE=  
6  SHELL=/sbin/nologin  
7  SKEL=/etc/skel
```

Dejando este archivo de configuración así, cualquier otro usuario que añadamos con el mandato useradd sin parámetros adicionales no podrá acceder al sistema por medio del shell, pero podrá utilizar otros servicios como el FTP, el correo, o el protocolo SAMBA.

La variable SHELL puede tener otros valores, como puede ver en la tabla [1.6](#).

Tabla 1. 6. Valores posibles para la variable de entorno SHELL.

Valor	Significado
/sbin/nologin	No deja entrar en el sistema con el shell.
/bin/false	Hace salir al usuario de forma inmediata con un mensaje de error. Se utiliza para usuarios que sólo puedan acceder a FTP o correo.
/dev/null	El dispositivo nulo, que descarta todos los datos que da el usuario, y no los redirecciona a ningún proceso para que lo lea. Se utiliza para usuarios que sólo deben acceder al correo mediante los protocolos SMTP, POP3 e IMAP, o correo web.
/bin/bash	Intérprete de órdenes más extendido en todas las distribuciones de GNU/Linux, y en Mac OS X (a partir de la versión Tiger).
/bin/sh	Versión simplificada del shell BASH.
/bin/tsh	Versión del shell que incluye instrucciones del lenguaje C.
/bin/ash	Versión del shell basado en BASH pero que utiliza menos memoria.
/bin/zsh	Versión mejorada del shell sh con funciones de los intérpretes BASH y TSH

Además de las modificaciones que podemos hacer sobre el archivo `/etc/default/useradd` por modificar la configuración por defecto del usuario, cuando se crea el directorio personal de un nuevo usuario, éste se inicializa con los archivos que hay en el directorio `/etc/skel` (skeleton, o esqueleto). El administrador del sistema puede crear archivos en este directorio, que configurarán el entorno predeterminado de los usuarios. Por ejemplo, se puede crear un archivo `/etc/skel/.profile` que especifique una variable de entorno para en el editor de textos por defecto, de modo que sea amigable para la mayoría de usuarios.

De todas formas, es recomendable que el directorio `/etc/skel` sea cuanto más pequeño mejor, porque si no, dificultamos la actualización de los usuarios existentes.

Siempre que sea posible, es mejor especificar configuraciones en archivos globales como, por ejemplo, el `/etc/profile`. De esta forma es posible actualizar información sobre usuarios sin dañar sus configuraciones.

Si, por ejemplo, queremos que cada cuenta de usuario incluya un subdirectorío para las carpetas de correo y la suscripción de las mismas por medio del servicio IMAP, se puede utilizar el siguiente procedimiento:

```
1 mkdir /etc/skel/mail/
2 touch /etc/skel/mail/Borradores
3 touch /etc/skel/mail/Enviados
4 touch /etc/skel/mail/Papelera
```

Y, después, crear con el editor de textos el archivo `/etc/skel/.mailboxlist`, que sirve para registrar las suscripciones en las carpetas de correo que se utilizarán para el servicio IMAP con un servidor UW-IMAP, utilizando el siguiente contenido:

```
1 mail/Borradores
2 mail/Enviados
3 mail/Papelera
```

También tenemos la opción de modificar el perfil de forma individual para cada usuario. Cada uno de los siguientes archivos está dentro del directorio personal de cada usuario:

- `$HOME/.bash_profile`. Es el archivo de inicialización personal, ejecutado cada vez que el usuario inicia la sesión. En este archivo se pueden añadir caminos de acceso a aplicaciones (path) o de otras variables específicas. Veamos su un ejemplo:

Ejemplo 6

```
1
2      # shell path
3      export ORACLE_HOME=/usr/lib/oracle/xe/app/oracle/product
         /10.2.0/server
4      export ORACLE_SID=XE
5      export NLS_LANG=$ORACLE_HOME/bin/nls_lang.sh'
6      export PATH=$PATH:$ORACLE_HOME/bin:$HOME/bin
7      export EDITOR=vim
8      export JAVA_HOME=/usr/lib/jvm/java-6-sun/jre
9      # load ssg keys
10     /usr/bin/keychain $HOME/.ssh/id_dsa
11     source $HOME/.keychain/$HOSTNAME-sh
12     # turn on directory spelling typos
13     shopt -s cdspell
```

- `$HOME/.bashrc`. En este archivo podemos especificar alias (variables que sustituyen órdenes), o bien funciones. Veamos un ejemplo:

Ejemplo 7

```
1
2      # shell functions
3      alias rm='rm -i'
4      alias cp='cp -i'
5      alias mv='mv -i'
6      alias vi='vim'
7      alias grep='grep --color'
8      alias update='sudo apt-get update && sudo apt-get upgrade'
9      alias dntop='dntop -l 5 eth1'
10     alias vnstat='vnstat -y eth1'
11     alias bc='bc -l'
12     genpasswd() {
13         local l=$1
14         [ "$l" == "" ] && l=16
15         tr -dc A-Za-z0-9_ < /dev/urandom | head -c ${l} |
            chargs
16     }
17     mp3(){
18         local o=$IFS
19         IFS=$(echo -en "\n\b")
20         /usr/bin/beep-media-player "$(cat $@)" &
21         IFS=o
22     }
```

- `$HOME/.bash_logout`. El archivo que se ejecuta cuando se termina la sesión de un usuario. Generalmente sirve para limpiar archivos temporales que haya podido dejar a este usuario.

2. Configuración del protocolo de red en sistemas operativos libres

Habitualmente, las redes en sistemas libres del tipo GNU/Linux se configuran con el protocolo TCP/IP. Éste es el protocolo más extendido en cuanto a la implementación en redes de área local y redes de área extensa como, por ejemplo, Internet.

Por ello, cabe remarcar que muchos de los conceptos que trataremos en este apartado son aplicables a otros sistemas operativos y, por supuesto, a las distribuciones de GNU/Linux y alguna versión de sistemas operativos basados en UNIX (por ejemplo, FreeBSD) .

2.1 Parámetros básicos para la configuración de la red en sistemas libres

Veamos los parámetros necesarios para configurar la red en un sistema GNU/Linux mediante el protocolo TCP/IP:

- IP. En las redes de área local, cada uno de los nodos que la forman debe tener asignada una dirección IP que le identifique unívocamente. En la versión actual (4), la dirección IP está formada por cuatro números de 8 bits, que, por tanto, pueden tomar valores desde cero hasta 255. De estos valores, normalmente, hay tres reservados : el 0 para indicar la dirección de subred; el 1, que se asigna al router; y el 255, que se asigna a la dirección de multidifusión (broadcast). En una red de área local del tipo C (las más habituales), las direcciones IP que se pueden utilizar por los hosts van de la 192.168.0.1 a la 192.168.0.254.
- IP enrutador. Si queremos conectar la red de área local con una otra o bien en Internet, será necesario especificar la IP del enrutador o router. Normalmente esta IP es 192.168.0.1.
- IP servidores DNS. Si hay algún servidor con resolución de nombres en nuestra red, o utilizamos una conexión a Internet y queremos navegar desde los ordenadores de la red de área local, es necesario especificar las direcciones IP de los servidores DNS.
- Nombre del host (hostname). El nombre (cadena de caracteres) que tendrá asignado el nodo dentro de la red de área local.
- Máscara de subred. Es un conjunto de cuatro números de 8 bits que sirve para saber si dos direcciones IP pertenecen a la misma subred o

no. Cada uno de los cuatro números de la subred puede tener el valor cero o 255. En el caso de las redes tipo C (las más extendidas entre las redes de áreas locales), la máscara es 255.255.255.0. En este caso las direcciones IP 192.168.0.10 y 192.168.0.11 pertenecen a la misma subred, porque si realizamos la operación y lógica (AND en inglés) entre los bits de la máscara y la IP, en ambos casos nos da 192.168 .0.0 (la misma dirección de subred). Podemos decir que si sólo pueden variar los últimos 8 bits de la IP, en este sitio la máscara tendrá el valor cero, en cambio, el resto de valores de la IP que son fijados corresponden al valor 255 de la máscara.

2.2 Herramientas de configuración de la red en modo texto

Los sistemas GNU/Linux ofrecen una serie de utilidades para diagnosticar y configurar la red desde el shell (en modo texto o modo consola), es decir, a diferencia de los sistemas Windows, no es necesario disponer de el entorno gráfico para llevar a cabo la configuración y diagnóstico del funcionamiento de la red. Para utilizar estas utilidades con todos sus parámetros, es necesario autenticarse como usuario administrador.

2.2.1 Herramienta de información y configuración de la red ifconfig

Una de las utilidades más habituales es ifconfig, que nos permite comprobar y configurar el protocolo TCP/IP desde la línea de comandos, y que nos ofrece información equivalente al comando ipconfig de la consola de Windows .

Para ver la configuración del protocolo TCP/IP, simplemente debemos escribir en una consola:

Versiones del protocolo IP La versión actual del protocolo de Internet (IPv4) será sustituida por la versión 6 (IPv6), ya que el límite de la versión 4 en el número de direcciones de red disponibles comienza a restringir el crecimiento de Internet .

```
1 $ /sbin/ifconfig
```

Con esta orden obtendremos una salida similar a la siguiente:

Ejemplo 8

```
1 ifconfig eth0 Link
2      encap:Ethernet HWaddr 08:00:27:94:65:cd inet addr:10.0.2.15 Bcast:10.0.2.255 Mask
3
4      :255.255.255.0
5      inet6 addr: fe80::a00:27ff:fe94:65cd/64 Scope:
6      Link
7      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric
8      :1
9      RX packets:10740 errores:0 dropped:0 overruns:0 frame:0
10
11     TX packets:7522 errores:0 dropped:0 overruns:0 carrier:0
12
13     colisiones:0 txqueuelen:1000 RX
14     bytes:10350281 (10.3 MB) TX bytes:1143450
15     (1.1 MB)
```

```
1  lo          Link encap:Local Loopback
2  inet addr:127.0.0.1 Mask:255.0.0.0
3  inet6 addr: ::1/128 Scope:Host
4  UP LOOPBACK RUNNING MTU:16436 Metric:1
5  RX packets:8 errores:0 dropped:0 overruns:0 frame:0
6  TX packets:8 errores:0 dropped:0 overruns:0 carrier:0
7  colisiones:0 txqueuelen:0
8  RX bytes:480 (480.0 B) TX bytes:480 (480.0 B)
```

Nos aparecen dos interfaces de red:

- eth0: que corresponde a la tarjeta de red
- lo: interfaz loopback: es una interfaz ficticia que siempre existe y que habitualmente tiene asignada la IP 127.0.0.1. Esta interfaz de red es utilizada por varios servicios del sistema.

Para comprobar la configuración del protocolo TCP/IP de la interfaz de la tarjeta de red Ethernet, escribiremos:

```
1 $ ifconfig eth0
```

Si queremos modificar la configuración de la red desde la línea de comandos, también lo podemos hacer utilizando la utilidad ifconfig, pero debemos hacerlo como usuario administrador, y además debemos tener en cuenta que esta configuración sólo será válida hasta que volvamos a iniciar el ordenador o reiniciemos los servicios de red. Por ejemplo, la siguiente línea configura la interfaz de red:

```
1 # ifconfig eth0 192.168.0.133 netmask 255.255.0.0 broadcast 192.168.255.255 up
```

en qué:

- eth0: nombre interfaz Ethernet
- 192.168.0.133: dirección IP asignada al PC
- netmask 255.255.0.0: máscara de subred
- broadcast 192.168.255.255: dirección IP de broadcast
- up: indica que se active la interfaz Ethernet.

Relacionada con el mandato ifconfig, también podemos utilizar los mandatos ifdown y ifup seguidas de la interfaz de red que queremos activar (normalmente eth0), por desactivarla o activarla. Para configurar la red con ifconfig, sería conveniente que antes la desactiváramos con ifdown.

2.2.2 Herramienta de configuración del encaminamiento y rutas: route

Además de configurar el protocolo TCP/IP de la máquina con la que estamos trabajando, si nuestra red tiene conexión a Internet, normalmente queremos configurar la dirección IP del router. Esto se hace de la siguiente forma:

```
1 # route add default gw 192.168.0.1
```

Este mandato añade la dirección IP del direccionador (default gateway).

Por lo general, el comando route sirve para construir las tablas de encaminamiento y mostrar su información. También sirve para configurar las rutas a otras redes o a otros nodos por medio del router o pasarela.

Para mostrar la tabla de direccionamiento, utilizamos el mandato route, sin ningún parámetro ni opción adicional. La salida será similar a lo siguiente:

1 \$ route

2	Kernel IP routing table						
3	Destino	Gateway	Iface	Genmask	Flags	Metric	Ref Use
4	192.168.2.0	*		255.255.255.0	U	0	0 0 eth0
5	default	.		0.0.0.0	UG	0	0 0 eth0

- En la primera columna, la dirección IP del nodo de la red de destino es:

```
1 Destino
```

La opción

```
1 default
```

es el router predeterminado de esta máquina.

- La columna que muestra la pasarela por la que los paquetes deben viajar para llegar al destino es:

```
1 Gateway
```

Cuando se muestra un asterisco, los paquetes de red viajan directamente hacia el host del destino.

- La máscara de subred es:

```
1 Genmask
```

- Lo que puede tener diferentes valores es:

```
1 Flags
```

Por ejemplo, U significa que la ruta está habilitada, y G significa que para llegar a la destino es necesario utilizar una pasarela o router.

- La columna que nos muestra la distancia al destino es:

1 Metric

- La columna que, por lo general, no se utiliza en sistemas del tipo GNU/Linux es:

1 Ref

- Por último, el nombre de la interfaz para la entrada correspondiente es:

1 Iface

2.2.3 Herramienta de configuración del nombre del nodo de la red: hostname

Para establecer el nombre del ordenador o nodo de la red (hostname), escribiremos hostname seguido del nombre del host. Por ejemplo:

1 root@usuario-desktop:~# hostname usuario-pc

Para realizar una comprobación posterior de este nombre de host, simplemente escribiremos hostname:

1 root@usuario-desktop:~# hostname usuario-pc
2

2.2.4 Herramienta de configuración de la red en sistemas Red Hat / Fedora (system-config-network)

Aparte de estas herramientas genéricas, que incorporan todas las distribuciones de GNU/Linux, Red Hat, Fedora y derivados incluyen otra utilidad que permite configurar la red utilizando un asistente, que a pesar de modo texto es muy fácil de utilizar. Para iniciarlo, es necesario ejecutar el mandato:

1 # system-config-network

Se nos presentará una pantalla en la que deberemos escribir la descripción del dispositivo, el nombre del dispositivo (normalmente eth0), si utilizará la configuración automática de la red, la IP estática, la máscara de subred y la IP de la router.

Herramientas de administración de la red

Algunas de las distribuciones de GNU/Linux incluyen herramientas específicas para administrar la red.

Además de system-config-network, en Fedora / Red Hat se encuentra el centro de control de Mandriva, o la herramienta de administración centralizada YaST de SuSE

2.3 Archivos de configuración de la red

Como es tradicional en todas las variantes de UNIX, y sistemas GNU/Linux, gran parte de la administración del sistema se lleva a cabo con la edición y modificación de archivos de configuración. En este sentido, la red no es ninguna excepción, y por tanto es necesario interpretar el contenido de los archivos de configuración para gestionar la red correctamente.

2.3.1 Archivo de configuración de la resolución de nombres (DNS): /etc/resolv.conf

Para poder navegar por Internet, o resolver direcciones IP a partir de un nombre, necesitaremos utilizar servidores DNS. Para configurarlos debemos editar el archivo resolv.conf que está situado en el directorio etc (/etc/resolv.conf), y añadir la línea nameserverip del servidor DNS.

Servidor DNS

Un servidor DNS es un ordenador que ejecuta software DNS. La mayoría de servidores DNS funcionan sobre alguna variante de UNIX o GNU/Linux, y el software más extendido para llevar a cabo esta función es BIND.

Por ejemplo, si queremos añadir el servidor DNS de XTEC, debemos editar el archivo resolv.conf y añadir la línea nameserver 213.176.161.16. Una forma alternativa es como root escribir lo siguiente desde el prompt:

```
1 root@localhost root# cat >>/etc/resolv.conf (retorno)
2     nameserver 213.176.161.16 (retorno) nameserver
3     213.176.161.18 (retorno) ctrl+d
4
```

2.3.2 Archivo de configuración de los nombres de los nodos de la red: /etc/hosts

Este archivo es especial porque almacena información sobre las IP asociadas a los nodos de la red. Es útil cuando no queremos depender de un servidor DNS para resolver determinados nombres de la red. En este archivo podemos incluir tantas líneas como nombres de nodos de la red queramos resolver estáticamente, y su sintaxis es:

```
1 ip del host nombre del host
```

Por ejemplo:

```
1 127.0.0.1          localhost
2 192.168.1.254      despensa
3 213.176.161.16     www.xtec.cat
```

En qué:

- 127.0.0.1 sería la dirección IP asociada al ordenador local (localhost).
- 192.168.1.254 sería la dirección IP de un ordenador situado en la red de área local llamado “despensa”.
- 213.176.161.16 sería la dirección IP de la página principal de XTEC.

Cabe decir que en este archivo podemos incluir nodos locales dentro de la red o servidores que están en Internet.

2.3.3 Archivo de configuración de los servicios: /etc/services

Este archivo ofrece una relación de los servicios de red activos con el puerto que tienen asociado. Su longitud puede ser bastante grande, pero las primeras líneas serán similares a las siguientes:

Ejemplo 9

```
1  # Each line describes un servicio, y está forma:
2  #
3  # service-name puerto/protocolo [aliasas ...] [# comment]
4  tcpmux 1/tcp # TCP puerto service multiplexero
5  tcpmux          1/udp # TCP puerto service multiplexero
6  rje 5/tcp # Remote Job Entry
7  rje 5/udp # Remote Job Entry
8  echo 7/tcp
9  echo          7/udp
10 discardo      9/tcp 9/          sink null
11 discardo      udp 11/          sink null
12 systat        tcp              usuarios
```

Normalmente, hay dos entradas por cada servicio, porque la mayoría pueden utilizar tanto el protocolo TCP como el UDP para las transmisiones. De hecho, una vez el sistema ha realizado una configuración inicial, el usuario no necesitará modificarlo.

2.3.4 Archivo de configuración /etc/nsswitch.conf

Este archivo fue desarrollado inicialmente por Sun Microsystems para especificar en qué orden se accede a los servicios del sistema. En este archivo hay una lista de servicios, pero la entrada que se modifica más a menudo es la línea que contiene hosts.

Una porción de este archivo tiene el siguiente aspecto:

Ejemplo 10

```
1  passwd:          compad
2  group:           compad
3  shadow:          compad
```

4	hosts:	filas dns mdns
5	networks:	filas
6	protocolos:	db filas
7	servicios:	db filas
8	ethers:	db filas
9	rpc:	db filas
10	netgroup:	nis

Este archivo indica a los servicios que deben consultar los archivos estándar de U-NIX y GNU/Linux para ejecutar los comandos `passwd`, `shadow` y `group` (`/etc/passwd`, `/etc/shadow` y `/etc/group`, respectivamente).

Para realizar búsquedas de nombres de equipos, el sistema comprueba el archivo `/etc/hosts`, y si no hay ninguna entrada, consulta el servidor DNS. Además, la línea que contiene `hosts` contiene todas las entradas posibles para nombres de hosts. Basta con modificar este archivo si el servidor de nombres se ha modificado.

2.3.5 Archivo de configuración `/etc/host.conf`

Este archivo de configuración hace una lista con el orden con el que el ordenador buscará la resolución de nombres de hosts. Veamos el contenido por defecto del archivo `/etc/host.conf`:

```
1 order hosts bind
```

En este ejemplo, primero el ordenador comprueba el contenido del archivo `/etc/hosts` y luego realiza una búsqueda utilizando el servidor DNS. La única razón para modificar éste archivo es que se utilice el protocolo NIS para el servicio de nombres, o que se necesiten servicios opcionales. La opción `nospoof` que se puede añadir en este archivo puede ser un buen método para mejorar la seguridad del sistema. Compara una búsqueda estándar DNS con una búsqueda inversa (nombre de host en IP, y luego IP en nombre de host), y da un error si ambas búsquedas no coinciden. La búsqueda de nombres puede fallar si se hace servir un servicio de proxy. Hay que tener cuidado a la hora de utilizar esta opción.

2.3.6 Archivo de configuración permanente de la red en sistemas Red Hat / Fedora

Si queremos modificar de forma permanente la IP, los DNS y el router, hemos de editar los archivos de configuración correspondientes.

En los sistemas Red Hat, y similares, es necesario editar el archivo:

```
1 /etc/sysconfig/networking/devices/ifcfg-eth*
```

En qué `*` es el número que corresponde a la interfaz de red activa que queremos configurar, y añadir las líneas tal y como muestra el ejemplo 11.

Ejemplo 11

```
1
2 IPADDR=192.168.0.101
3 DNS1=213.176.161.16
4 GATEWAY=192.168.0.1
```

En qué:

- La dirección IP que asignamos a la interfaz es:

```
1 IPADDR
```

- La dirección IP del servidor DNS es:

```
1 DNS1
```

- La dirección IP del router es:

```
1 GATEWAY
```

Hay que decir que, para que estos cambios sean efectivos, es necesario reiniciar los servicios de red. Para ello, deberíamos ejecutar la orden:

```
1 # cd /etc/init.d/
2 # ./network restart
3 Se está deteniendo la interfaz eth0: Se está [ HECHO ]
4 deteniendo la interfaz loopback: Se está activando la [ HECHO ]
5 interfaz loopback: Se está activando la interfaz eth0: [ HECHO ]
6 [ HECHO ]
```

2.3.7 Archivo de configuración en sistemas Debian/Ubuntu

Si queremos que la red se configure automáticamente mediante el DHCP, hemos de editar el archivo `/etc/network/interfaces`, y añadir las siguientes líneas:

```
1 # The primary network interface - use DHCP para find our address
2 auto eth0
3 iface eth0 inet dhcp
```

Si, en cambio, queremos configurar la red de forma manual con una dirección IP estática, deberemos editar el mismo archivo, pero añadiendo los parámetros básicos de configuración de la red:

```
1 # The primary network interface
2 auto eth0
3 iface eth0 inet static
4 address 192.168.3.90
5 gateway 192.168.3.1
6 netmask 255.255.255.0
7 network 192.168.3.0
8 broadcast 192.168.3.255
```

ifconfig

Sea cual sea la distribución del GNU/Linux que utilizamos, si no modificamos los archivos de configuración de la red y sólo utilizamos `ifconfig`, los cambios aplicados no se guardarán cuando reiniciamos el ordenador, detenemos la sesión o reiniciamos el servicio de red.

En qué:

- address: dirección IP
- gateway: dirección IP del router
- netmask: máscara de subred
- network: dirección de subred
- broadcast: dirección de multidifusión

Una vez hemos aplicado todos los cambios que queríamos, reiniciamos el servicio de red:

```
1 /etc/init.d/networking restart
```

2.4 Herramientas de red en modo texto

Además de las herramientas para configurar la red mediante el protocolo TCP/IP, los sistemas basados en GNU/Linux disponen de una gran cantidad de utilidades que nos permiten diagnosticar el funcionamiento de la red y comprobar su funcionamiento.

2.4.1 Estado de la conexión: ping

Para comprobar el estado de las conexiones, y comprobar que la red funciona de modo fiable, podemos utilizar el comando ping seguida de la IP del nodo de la red de destino. El comando es prácticamente igual que el que aparece en la línea de comandos de Windows, pero con la diferencia de que para detener su ejecución debemos pulsar Control+C.

Por ejemplo, si queremos hacer un ping en el router debemos escribir ping 192.168.0.1. Ping se ejecuta de forma indefinida, pero podemos pasar un parámetro para que sólo haga un número determinado de pings:

```
1 $ ping -c4 192.168.0.1
2   PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
3   64 bytes from 192.168.0.1: icmp_seq=1 ttl=255 time=3.74 ms
4   64 bytes from 192.168.0.1: icmp_seq=2 ttl=255 time=0.626 ms
5   64 bytes from 192.168.0.1: icmp_seq=3 ttl=255 time=0.593 ms
6   64 bytes from 192.168.0.1: icmp_seq=4 ttl=255 time=0.695 ms
7   --- 192.168.0.1 ping statistics ---
8   4 packets transmitted, 4 received, 0% packet loss, time 3003ms
9   rtt min/avg/max/mdev = 0.593/1.413/3.741/1.344 ms
```

En este caso el parámetro -c4 hace que se envíen cuatro paquetes de 64 bytes a su destino. El comando ping mide el tiempo que los paquetes de información tardan en

llegar al destino y devolver, y además muestra una estadística del tiempo mínimo, medio y máximo para realizar esta operación. También nos informa del número de paquetes enviados y de recibos, que en una red que funcione de forma fiable deberían ser los mismos con un 0% de pérdida de paquetes.

2.4.2 Trazar ruta: traceroute

Otra orden que podemos utilizar para diagnosticar el estado de la red es traceroute, que es el equivalente al orden tracert de Windows, y hace exactamente la misma función. Si, por ejemplo, queremos saber todos los hosts por los que pasan los paquetes TCP/IP hasta llegar a `www.google.com`, simplemente escribiríamos `traceroute www.google.com` desde la línea de comandos:

Ejemplo 12

```
1 $ traceroute to www.google.com (66.249.93.99), 30 hops max, 40
  byte packets
2 1 192.168.0.1 (192.168.0.1) 0.480 ms 0.473 ms 0.433 ms
3 2 10.2.242.1 (10.2.242.1) 42.955 ms 45.283 ms 45.761 ms
4 3 114.Red-80-58-123.staticIP.rima-tde.net (80.58.123.114)
  44.631 ms 43.037 ms 41.926 ms
5 4 129.Red-80-58-91.staticIP.rima-tde.net (80.58.91.129)
  53.640 ms 53.695 ms 53.759 ms
6 . . .
```

2.4.3 Estadísticas de conexiones de red: netstat

El mandato `netstat` se utiliza para mostrar el estado de la red. Tiene varios parámetros que pueden mostrar una información muy diversa. Se hace una lista de los servicios en partir del socket (conexiones aplicación-aplicación entre dos ordenadores). Veamos sus parámetros principales en la tabla 2.1.

Tabla 2. 1. Parámetros más comunes de "netstat".

Opción	Salida
-g	Muestra los grupos de multidifusión configurados.
-y	Muestra las interfaces de red configuradas con <code>ifconfig</code> .
-s	Realiza una lista resumen de la actividad para cada protocolo de red.
-v	Muestra una salida detallada haciendo una lista de los sockets activos e inactivos.
-c	Actualiza la salida cada segundo (útil para realizar pruebas y arreglar problemas).
-e	Muestra información detallada sólo para las conexiones activas.
-C	Muestra información de la memoria caché de direccionamiento. Sirve para buscar información de conexiones previas.

Su salida sería similar a la siguiente:

Herramientas de monitorización de conexiones de red (`netstat`)

Existen algunas herramientas de detección de vulnerabilidades en servidores que están conectados a una red. Hay que recordar que sólo es legítimo su uso si las aplicamos en servidores propios.

Ejemplo 13

```

1 root@usuario-desktop:~# netstat -e
2 Active Internet connections (w/o servers)
3 Proto Recv-Q Send-Q Local Addr Foreign Address      State
   User Inode
4 tcp 0      0  usuario-de... 209.85.146.101:https
   ESTABLISHED usuario 12460
5 . . .

```

2.5 Herramientas de configuración y diagnóstico de la red en modo gráfico

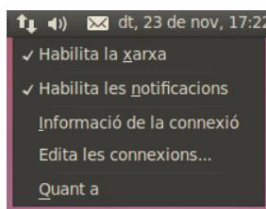
En la mayoría de distribuciones de GNU/Linux, también existe todo un conjunto de herramientas de configuración y diagnóstico del funcionamiento de la red en el entorno gráfico, además de las que funcionan sobre la consola en modo texto. Estas herramientas son específicas de cada una de las distribuciones, pero la mayoría tienen un funcionamiento similar y, en los aspectos básicos, no son muy distintos.

2.5.1 Herramienta de configuración de la red: NetworkManager

En el caso de Ubuntu 10.04 LTS, como en la mayoría de las distribuciones que funcionan sobre el entorno gráfico Gnome, la herramienta que permite visualizar y configurar la red se llama Network Manager.

Para acceder a la información sobre la red, hacemos un clic con el botón derecho sobre la icono de la conexión de red, y seleccionamos la opción Información de la conexión, como puede ver en la figura 2.1.

Figura 2. 1. Opciones del menú de conexiones de red en el Ubuntu 10.04LTS



Acceso a NetworkManager

Haciendo esto, nos aparecerá una ventana informativa con las conexiones de red activas. Esta ventana nos llama el nombre de la interfaz de red, la dirección de hardware (dirección MAC), el nombre del controlador del dispositivo de red, la velocidad de conexión y los parámetros de configuración del protocolo TCP/IP, como ahora, la dirección IP, la máscara de subred, la dirección de multidifusión (broadcast), la pasarela (gateway) y los servidores DNS. Puede verlo en la figura 2.2.

Figura 2. 2. Muestra información sobre la configuración del protocolo TCP-IP y el hardware de red



Información de la conexión

Si seleccionamos la opción Editar las conexiones, de las que aparecen en la figura 2.1, aparecerá un cuadro de diálogo que nos permitirá configurar las interfaces de red, como muestra la figura 2.3.

Figura 2. 3. Aplicación NetworkManager, que permite editar y configurar las conexiones de red



Edición de las conexiones de red

En la primera pestaña se nos muestran las conexiones alámbricas, es decir, las interfaces de red que están conectadas mediante cable. Para editar una de estas conexiones, seleccionamos el nombre de la interfaz de la lista y después pulsamos el botón Editar. Nos aparecerá la ventana de la figura 2.4.

Configuración en una red doméstica

En el ámbito doméstico, la mayoría de aparatos encaminadores o routers, disponen de servidor DHCP incorporado, por tanto, en la mayoría de casos, no será necesario llevar a cabo una configuración manual del protocolo TCP/IP de los aparatos conectados.

Figura 2. 4. Edición de los parámetros de la interfaz de red con hilo seleccionada

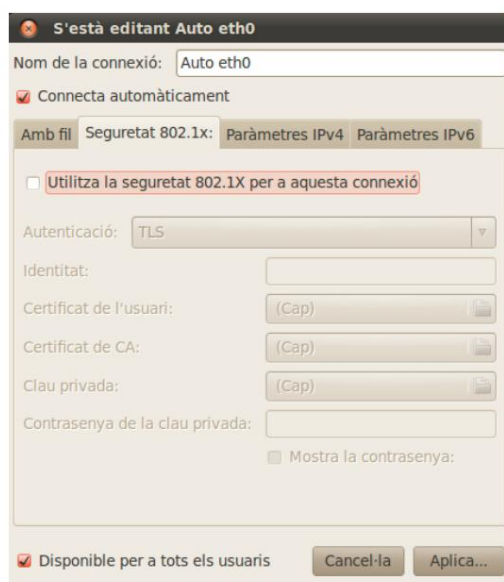


Edición de la configuración de red

En esta primera pestaña, podemos modificar el nombre de la conexión, si queremos podemos seleccionar que se inicie automáticamente al iniciar el sistema o no, podemos modificar la dirección MAC de la interfaz de red o el tamaño del MTU (el tamaño máxima que puede tener una unidad o paquete de datos para el protocolo dado). Por último, también podemos hacer que la interfaz de red esté disponible para todos los demás usuarios del sistema, aunque no sean usuarios administradores.

Si seleccionamos la pestaña Seguridad, el sistema muestra la ventana de la figura 2.5.

Figura 2. 5. Pestaña de configuración de la seguridad en la conexión de red



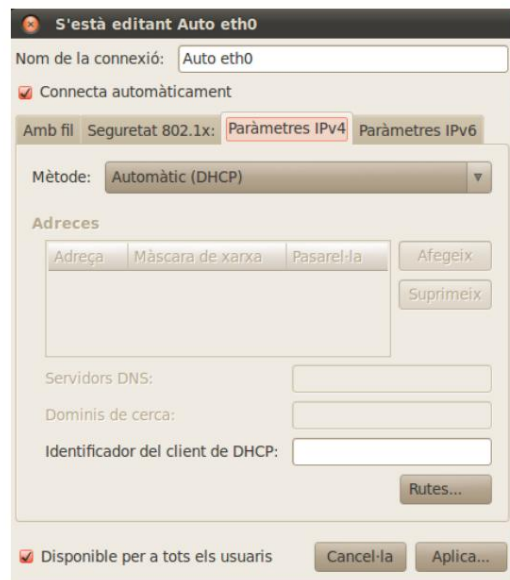
Seguridad de las conexiones

Aquí podemos habilitar el protocolo de seguridad 802.1X, que es un estándar del IEEE para el control de acceso a redes basado en el puerto, y que permite un mecanismo

de autenticación para dispositivos que desean conectarse a una red de área local o área extensa. En caso de que lo activemos, podemos elegir el método de autenticación, la identidad del dispositivo, el certificado del usuario, la clave privada y la contraseña de la clave privada.

Si hace clic en la pestaña Parámetros IPv4, el sistema muestra la ventana de la figura 2.6.

Figura 2. 6. Parámetros IPv4 de la interfaz de red



Por defecto, el sistema busca la configuración de la red automáticamente (DHCP)

Este apartado permite configurar el protocolo TCP/IP para la interfaz de red que hemos seleccionado. Por defecto, la configuración de la red es automática, lo que requiere que en la red de área local esté presente un servidor de direcciones IP, es decir, un servidor DHCP.

También podemos establecer una configuración de la red manual, para lo que seleccionaremos del desplegable la opción Manual. En ese caso, el usuario deberá insertar los parámetros básicos de la configuración del protocolo TCP/IP, es decir, la dirección IP, la máscara de subred, la pasarela, y los servidores DNS. Puede verlo en la figura 2.7

También existe una pestaña que hace referencia a la configuración del protocolo TCP/IP en la versión 6, pero de todos modos en la actualidad esto no es necesario, y sólo tendrá sentido en un futuro. De todas formas, todas las distribuciones de GNU/Linux actuales ya soportan esta nueva versión del protocolo TCP/IP.

Figura 2. 7. Configuración manual de la red



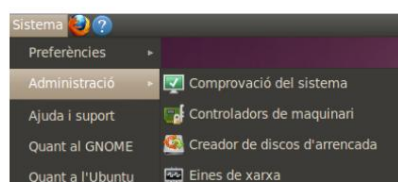
Si configuramos manualmente la interfaz de red, deberemos escribir la dirección IP, la máscara, la pasarela y los servidores DNS

Una vez hecha la configuración de la red que queremos, pulsamos el botón **Aplica**, y se guardarán los cambios que hayamos hecho sobre la red, y volveremos a la ventana de la figura 2.3. En esta ventana, podemos añadir más conexiones de red, o eliminar las configuraciones que ya no queremos utilizar.

También se pueden configurar las conexiones a redes inalámbricas, de una manera muy parecida a cómo lo haríamos en el caso de las redes inalámbricas. Sin embargo, en este caso hay que añadir dos parámetros adicionales, como son el identificador de la red inalámbrica (SSID) y la contraseña de acceso a la red (utilizando el protocolo de encriptación WEP o WPA). Esta herramienta también permite configurar dispositivos de acceso a Internet tales como módems ADSL, y dispositivos USB de conexión a Internet vía 3G.

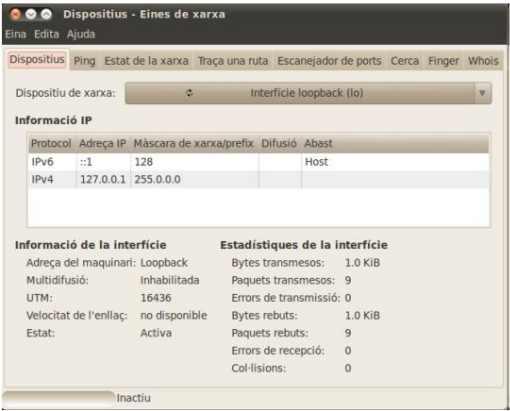
2.5.2 Diagnóstico del funcionamiento de la red: aplicación Herramientas de red

Además de la herramienta de administración llamada NetworkManager, también disponemos de otra herramienta que muestra información sobre la red, y que contiene una serie de utilidades de diagnóstico del funcionamiento de la red. Esta herramienta se llama GNOME-Network. Para acceder a esta aplicación, accedemos al menú **Sistema**, el apartado **Administración**, y seleccionamos la aplicación **Herramientas de red**, como se muestra en la figura 2.8.

Figura 2. 8. Localización de la aplicación
Herramientas de red

Una vez ejecute esta herramienta, se muestra la ventana de la figura 2.9.

F igura 2. 9. Ventana inicial de la aplicación Herramientas de red



En esta ventana inicial, por defecto, se nos muestra la información sobre la interfaz loopback, que es una interfaz ficticia que crea el sistema para algunos servicios.

Si queremos encontrar la información sobre la interfaz de red real, la seleccionamos desde el desplegable, como puede ver en la figura 2.10.

F igura 2. 1 0. Se muestran varias estadísticas sobre la interfaz de red seleccionada, e información sobre la interfaz de red eth0



Esta ventana nos mostrará información sobre la configuración del protocolo TCP/IP, dirección MAC, UTM, velocidad de conexión y estado de la conexión. También muestra estadísticas sobre el funcionamiento de la interfaz de red, como la información transmitida y recibida (medida en paquetes y bytes), el número de errores producidos en el envío y recepción de datos y el número de colisiones.

En la pestaña siguiente, Ping, se nos muestra gráficamente el resultado de la ejecución de esta orden, como puede ver en la figura 2.11.

F igura 2. 1 1. Esta pestaña muestra estadísticas del funcionamiento del comando Ping



Pestaña ping

En esta ventana, insertamos el nombre de una URL, el número de pings que queremos realizar, y una vez terminado se muestra el tiempo mínimo, máximo y medio del ping, además de información sobre la cantidad de paquetes remitidos y recibos. Esta última información es muy importante para determinar la fiabilidad y estabilidad de la conexión de la red.

Si hacemos un clic en la pestaña Estado de la red, podremos ver información sobre las conexiones de red establecidas, que corresponde a la salida del mandato netstat. Lo puede ver en la figura 2.12.

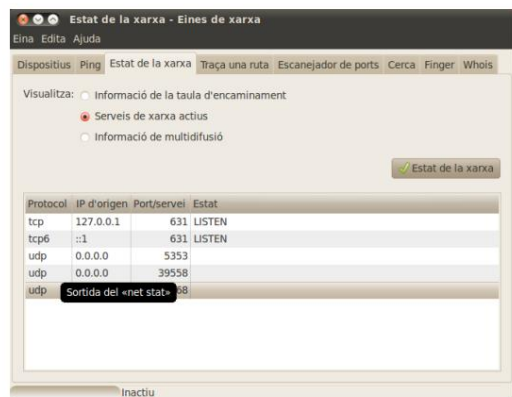
F igura 2. 1 2. Pestaña Estado de la red



Esta pestaña muestra información equivalente a la utilidad netstat cuando se ejecuta desde la consola

Haciendo clic en el botón de radio Servicios de red activos, se muestra un contenido similar al de la figura 2.13.

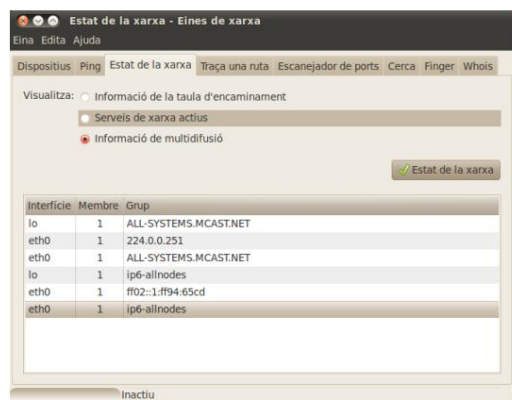
Figura 2. 1 3. Se muestra una lista de todos los servicios de red que funcionan actualmente



Servicios de red en funcionamiento

Esta pantalla nos muestra los servicios de red que están funcionando en nuestra máquina, el puerto que utilizan y el protocolo que utilizan. Si finalmente hacemos un clic en la Información de multidifusión, se muestra la ventana de la figura 2.14.

Figura 2. 1 4. Información de multidifusión

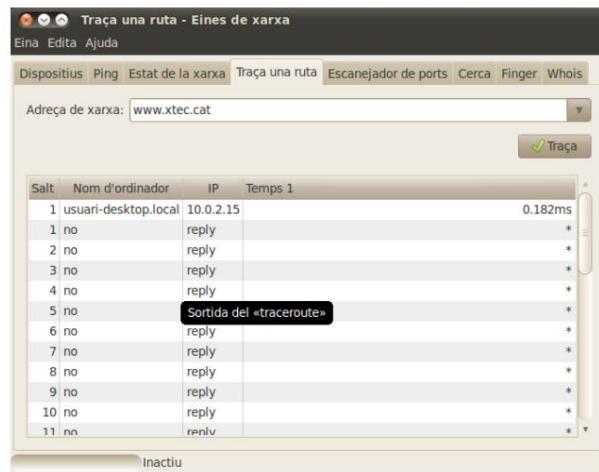


En esta ventana se muestran todas las conexiones en modo multidifusión que tienen establecidas todas las interfaces de red del sistema.

La pestaña Traza una ruta nos permite visualizar todos los saltos por las diferentes redes de área local y de área extensa (en Internet), para llegar a un determinado nodo de la red. Cabe decir que el destinatario también puede ser un servidor de Internet de cualquier tipo...

Puede ver el resultado de la ejecución en la figura 2.15.

Figura 2. 1 5. Traza de una ruta

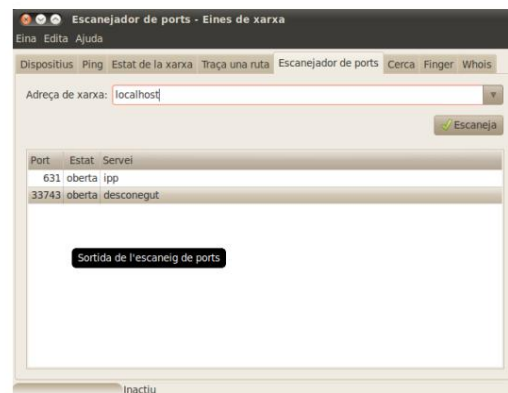


Se muestran estadísticas sobre cada paso para llegar al destino

Como puede comprobarse, la información que se muestra en esta ventana sería la misma que la que sale del mandato traceroute ejecutada desde la consola.

Si hacemos un clic en la pestaña Escaneador de puertos, e insertamos el nombre de un servidor de la red, podemos ver qué puertos tiene abiertos y podemos deducir qué servicios se ejecutan. Lo puede ver en la figura 2.16.

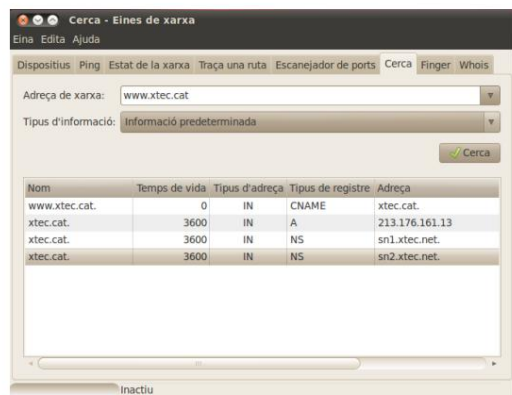
Figura 2. 1 6. Escaneador de puertos



Lista de los puertos abiertos que corresponden a servicios, en este caso del ordenador local (localhost)

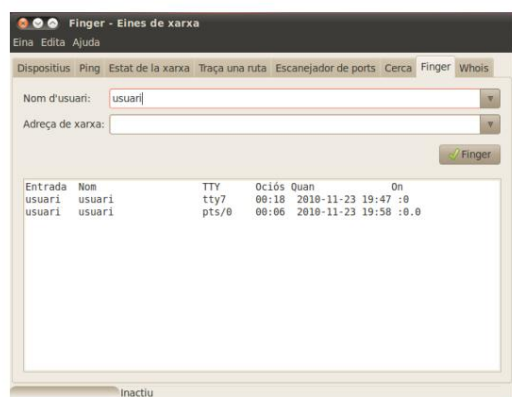
La pestaña Búsqueda nos permite obtener información de un ordenador de la red, o de un servidor en Internet. Lo puede ver en la figura 2.17.

Figura 2. 1 7. Información mostrada sobre un servidor web



Si hacemos un clic en la pestaña Finger, nos muestra un cuadro de diálogo en el que podemos buscar información sobre un usuario del sistema, podemos ver qué terminal ha iniciado la sesión, ya qué hora lo ha hecho. Se puede comprobar en la figura 2.18.

Figura 2. 1 8. Información que proporciona "Finger" sobre un usuario del sistema



Información de un usuario del sistema

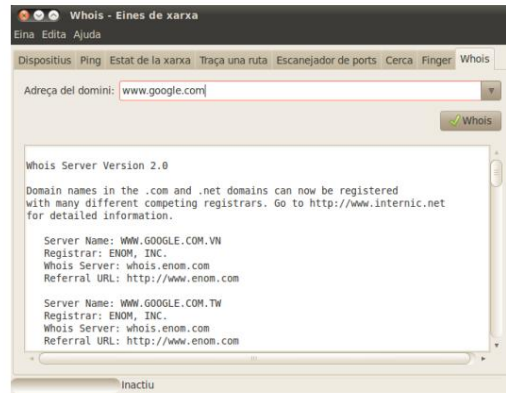
En este caso, la utilidad nos dice que el usuario llamado usuario ha iniciado la sesión en el terminal número 7, que corresponde al entorno gráfico.

Por último, si hacemos un clic en la pestaña Whois, podemos obtener información sobre un servidor web o un dominio en la red. Lo puede ver en la figura 2.19.

ICANN (Internet Corporation for Assigned Names and Numbers) Es

una organización que opera a nivel internacional, que es responsable de asignar las direcciones del protocolo IP, los identificadores de protocolo, de las funciones de gestión del sistema de dominio y de la administración del sistema de servidores raíz.

Figura 2. 1 9. Información sobre los registros de dominio de Internet



Salida del orden Whois

En este caso, podemos ver la información sobre un popular buscador de información en Internet, los distintos subdominios, y en qué servidor de whois está registrado.

3. Optimización del sistema en ordenadores portátiles

Uno de los aspectos más críticos en lo que se refiere a la utilización de un ordenador portátil es el consumo energético y la duración de la batería. Los sistemas operativos del tipo GNU/Linux ofrecen una gran cantidad de opciones y utilidades en lo que se refiere a la gestión de la energía y permite reducir el consumo energético y alargar la duración de la batería.

El soporte de hardware es vital para que la gestión de energía funcione, y el grado de gestión de energía depende del dispositivo. Algunos dispositivos como, por ejemplo, los monitores sólo soportan dos estados: abierto o cerrado. Otros, como algunos microprocesadores, soportan opciones de ahorro energético más complejas como, por ejemplo, la capacidad de funcionar a distintas frecuencias.

La gestión energética ha madurado con el tiempo, por lo que ahora existen principalmente dos estándares: APM (gestión avanzada de la energía) y ACPI (interfaz para la configuración avanzada de la gestión de la energía).

APM es un estándar propuesto por Microsoft e Intel que consiste en una o más capas de software que soportan la gestión de la energía. En este estándar, la BIOS es fundamental.

ACPI es el estándar más novedoso, propuesto por Toshiba, Intel y Microsoft. Permite una gestión más inteligente de la energía, y es gestionada por el sistema operativo, en vez de la BIOS.

En referencia al ahorro energético, como principio general, cuando existe algún dispositivo que no se utiliza, es aconsejable que éste se desconecte y, siempre que se pueda, se deje inactivo el máximo tiempo posible, lo que maximizará este ahorro.

Una forma de implementar la gestión energética es definir un diagrama de transición entre estados energéticos. Se definen diferentes estados de uso de energía del sistema, y se definen las reglas para realizar la transición entre estos estados.

Podríamos definir unos estados genéricos parecidos a éstos:

- Estado de ejecución. El sistema llega a ese estado cuando se inicia o se reinicia. El consumo energético es máximo en este estado, porque todos los dispositivos están encendidos o activos.
- Estado de espera. El sistema llega a ese estado debido a la inactividad. Es típico que el monitor se apague y que la velocidad del microprocesador se reduzca para preservar energía.
- Estado dormido. El sistema alcanza este estado debido a una inactividad continuada. La energía se preserva parando el funcionamiento de la mayoría de los

dispositivos, el microprocesador está en modo dormido, y sólo la memoria RAM consume algo de energía para refrescarse y preservar el estado de la máquina (los datos del sistema, las aplicaciones y los datos cargados en memoria). El sistema se despierta del estado dormido cuando se detecta actividad, y vuelve al estado de ejecución normal.

- Estado parado. Sólo se llega a ese estado cuando el usuario lo ordena, se detienen todos los dispositivos, y el consumo energético es mínimo. Solo funciona el reloj interno para preservar la hora del sistema.

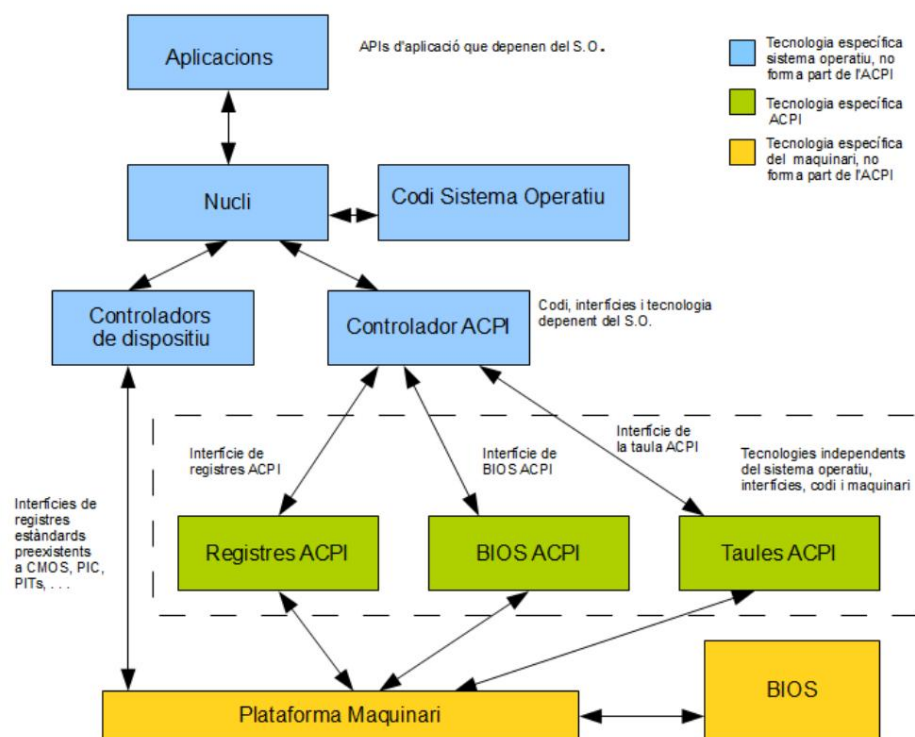
Podemos decir que la base de la gestión y el ahorro de la energía consiste en detectar la inactividad y poner los dispositivos en el modo de bajo consumo energético.

3.1 Gestión energética en sistemas GNU/Linux

La mayoría de los sistemas modernos soportan la gestión energética ACPI, y si instalamos una distribución de GNU/Linux sobre éstos, podemos obtener información completa sobre la gestión de la energía en el directorio `/proc/acpi/`. Por ejemplo, podemos encontrar información sobre la frecuencia de funcionamiento del microprocesador, medidas de temperatura, etc.

En la figura 3.1 puede ver una lista de las herramientas que nos permite GNU/Linux en cuanto a la gestión de energía.

Figura 3.1. Esquema ACPI



3.1.1 Hibernar (en el disco)

Consiste en guardar toda la información de la sesión abierta (todo el contenido de la memoria RAM) en una partición de intercambio del disco, por lo que nos ahorramos mucho tiempo de restaurar el sistema a su estado de trabajo normal, sin necesidad de reabrir todas las aplicaciones del usuario. Como consecuencia, la partición de intercambio debe ser por lo menos igual de grande que la memoria RAM del sistema.

Actualmente todas las distribuciones de GNU/Linux lo soportan, y se puede acceder a ellas como una opción más del entorno gráfico.

3.1.2 Escalado de frecuencia del procesador

Consiste en la disminución de frecuencia de funcionamiento del microprocesador para ahorrar energía. Las últimas versiones de las distribuciones de GNU/Linux soportan el escalado de frecuencia del procesador, pero no todos los microprocesadores lo soportan. En principio sólo lo soportaban los microprocesadores para ordenadores portátiles, pero actualmente también lo soportan muchos microprocesadores para equipos de mesa.

En el caso de las distribuciones de GNU/Linux, esto se implementa mediante un controlador del núcleo llamado `cpufreq`. El controlador de dispositivo `cpufreq` permite que los programas de usuario controlen la frecuencia de funcionamiento del microprocesador escribiendo archivos en el directorio `/sys/devices/system/cpu/cpufreq/`.

De hecho, lo que realmente controla la frecuencia del microprocesador es un programa que utiliza el controlador `cpufreq`.

El estándar de facto de las distribuciones de GNU/Linux es `CPUspeed`, que permite configurar el controlador de dispositivo `cpufreq` en función de criterios definidos por el usuario: carga del microprocesador, temperatura, funcionamiento con batería/enchufado, etc.

Normalmente, `CPUSpeed` se configura mediante el archivo `/etc/cpuspeed.conf`.

Veamos un ejemplo de configuración:

Ejemplo 14

```
1 VMAJOR=1
2 VMINOR=1
3 DRIVER="speedstep-centrino"
4 OPTS="-y 2
5 -t /proc/acpi/thermal_zone/THM/temperature 70 6 -a /proc/acpi/ac_adapter/
AC/state 7 -p 10 25 8 -m 600000 -M 1600000"
```

Tecnologías de escalado dinámico de frecuencia de los microprocesadores.

La mayoría de microprocesadores actuales incorpora la capacidad de modificar la frecuencia de funcionamiento sin tener que detener el sistema operativo, y reducirla cuando se necesita ahorrar energía. En el caso de los microprocesadores de Intel, esta técnica se llama `SpeedStep`, y en los de AMD se llama `Cool'n'Quiet`.

Después de realizar los cambios, será necesario reiniciar el servicio CPUSpeed con:

```
1 /etc/init.d/cpuspeed restart
```

Puede ser interesante visualizar la frecuencia de funcionamiento del microprocesador ejecutante:

```
1 cat /proc/cpuinfo
```

3.1.3 hdparm

Es una utilidad de GNU/Linux que permite controlar el tiempo que debe pasar para detener la rotación de los platos del disco duro y otros parámetros. Una forma de ahorrar energía es detener los platos del disco duro en un período de tiempo relativamente corto, lo que reduce su consumo.

Para habilitar el paro del disco, podríamos ejecutar los mandatos siguientes:

```
1 hdparm -S 5 /dev/hda hdparm
2 -K 1 /dev/hda
```

La primera orden detiene el giro. El número posterior nos indica cuántos múltiplos de 5 segundos pasan hasta que esto sucede. En este caso $5 \times 5 = 25$ segundos.

El segundo comando permite guardar los parámetros de configuración del disco, después de haber reiniciado el sistema por hardware. Por tanto, de esta manera recordará el tiempo que debe pasar hasta detener el giro de los discos, entre otros parámetros.

Otra acción que podemos llevar a cabo para ahorrar energía es ejecutar hdparm con el parámetro -B:

```
1 hdparm -B 254 /dev/sdX
```

El parámetro -B activa la gestión avanzada de energía si el disco lo soporta. El valor 255 correspondería a un disco siempre puesto en marcha, y valores bajos detendrían el funcionamiento del disco después de poco tiempo de inactividad. Es recomendable utilizar valores no inferiores a 128, porque si no, el cabezal del disco se aparca demasiado rápidamente, y esto puede dañar o acortar su vida útil.

Este valor puede ser configurado en el archivo `/etc/laptop-mode/laptop-mode.conf`, asegurándonos que el modo portátil controla hdparm

```
1 CONTROL_HD_POWERMGMT=1
```

y después cambiando los valores por defecto:

```
1 BATT_HD_POWERMGMT=254
2 LM_AC_HD_POWERMGMT=254
3 NOLM_AC_HD_POWERMGMT=254
```

Otra acción que podemos llevar a cabo para evitar que el disco duro se ponga en marcha rápidamente cuando está en reposo es desactivar el demonio hddtemp, que lee

la temperatura del disco duro cada minuto. También deberíamos tener en cuenta la configuración del demonio smartd, que controla el estado del disco duro, y que también lo hace activar, aunque en este caso esto sólo ocurre una vez cada 30 minutos en su configuración por defecto.

3.1.4 Modo portátil

El modo portátil está implementado desde la versión 2.4.23 y 2.6.6 del núcleo de GNU/Linux.

Este modo se puede activar añadiendo un “5” en el archivo `/proc/sys/vm/laptop_mode`. Cuando se configura correctamente, permite hacer girar los platos del disco sólo cuando se leen datos que están fuera de la caché. De esta forma reducimos el consumo energético del disco duro.

También existe un conjunto de herramientas de usuario que ayudan a automatizar la gestión de todos los aspectos de la configuración del modo portátil, en función del modo de operación (enchufado a la corriente alterna, o funcionamiento con batería). Se llama `laptop-mode-tools`, y se puede descargar en la mayoría de distribuciones de GNU/Linux.

Ordenadores ultraportátiles
(netbooks)

Con la aparición de los ordenadores ultraportátiles (netbook), se ha popularizado la utilización de GNU/Linux, si bien, en la mayoría de los casos, se trata de distribuciones especialmente adaptadas a este tipo de ordenadores.

3.1.5 Programas de salvapantallas

Este tipo de software se activa automáticamente después de haber detectado un tiempo de inactividad, mostrando imágenes o figuras estáticas o en movimiento en la pantalla. En función de cómo sea la imagen o las figuras se puede ahorrar una cantidad de energía importante.

Para ahorrar energía, suponiendo que la versión del servidor del entorno gráfico (las X), y el monitor, lo soporten, se pueden utilizar las opciones DPMS (display power management signaling) o señalización de la gestión de la energía del monitor). Por ejemplo, para habilitar las opciones DPMS del servidor X, podemos escribir: `xset+dpms`. También podemos cambiar manualmente el modo del monitor:

```
1 xset dpms force standby xset dpms force suspend
2
3 xset dpms force off
```

Debe tenerse en cuenta que, normalmente, las opciones `suspend` y `off` ahorran mucha más energía que el modo de espera (`standby`), sobre todo en monitores antiguos de tubo de rayos catódicos (CRT).

En el caso de los monitores LCD, también se recomienda utilizar estos modos porque no reducen su tiempo de servicio.

En los entornos gráficos modernos (como GNOME y KDE) es fácil de configurar el apagado automático del monitor dado un período de tiempo. En el caso del

GNOME, accedemos al menú Sistema>Preferencias>Ahorro de pantalla, y aparece un cuadro de diálogo en el que simplemente seleccionamos el tema del salvapantallas y el tiempo hasta que éste se active. Lo puede ver en la figura 3.2.

F igura 3. 2. Ahorro de pantalla en Ubuntu



Aquí puede seleccionar el tipo de salvapantallas, el tiempo que tarda en activarse, y si desea bloquear la pantalla cuando este ahorro se active

3.1.6 acpi

En los sistemas GNU/Linux instalados en máquinas compatibles con el estándar ACPI, utilizamos el mandato acpi con el parámetro -V, que nos mostrará toda la información que puede recoger. La salida será similar a la siguiente:

Ejemplo 15

```
1 $ acpi -V
2 Battery 1: charged, 100% Thermal
3 1: ok, 47.0 degrees C AC Adapter 1:
4 on-line
```

En este ejemplo se muestra el estado de la batería y la temperatura del microprocesador, y nos dice que la conexión a la corriente alterna está activada.

3.2 Archivos de red sin conexión

Protocolos de encriptación de datos

El protocolo SSH encripta las comunicaciones mediante una clave pública, que permite autenticar a un usuario en un ordenador remoto. SSH se utiliza para conectarse a un ordenador remoto y ejecutar comandos, pero también permite transferir archivos (mediante los protocolos asociados SCP y SFTP) y realizar sesiones remotas con entorno.

SSH utiliza el modelo cliente-servidor

Los archivos de red sin conexión se utilizan en un ordenador portátil o de mesa que a veces se conecta a una red. Utilizando este método, podemos obtener archivos de la red cada vez que el ordenador se conecta.

Los archivos seleccionados se descargan automáticamente desde carpetas compartidas en la red y se almacenan en el ordenador local. Cuando desconectamos el ordenador de la red podemos utilizar los archivos y, cuando nos volvemos a conectar,

los cambios realizados en estos archivos se añaden a los archivos disponibles en la red mediante un proceso de sincronización. Si alguien conectado a la red hace cambios en el mismo archivo, puede guardar su versión, conservar la otra versión o guardar las dos.

En los sistemas Windows, esta utilidad de sincronización de archivos ya está presente dentro del mismo sistema operativo, pero en sistemas GNU/Linux se debe instalar una utilidad adicional para poder llevar a cabo esta tarea. De todas formas, el método de transferencia de archivos cuando sincronizamos el directorio remoto y el local, es mediante el protocolo SSH (secure shell), que nos asegura la transferencia encriptada de la información por medio de la red, lo que mejora la seguridad y la privacidad del usuario.