Curso de Linux con Ubuntu

Configura Ubuntu en red

En esta segunda entrega del curso tu cometido es configurar tu sistema Linux para conectarlo a una red local y a Internet, bien sea a través de un router, de un módem USB, de conexión inalámbrica, etc. Tampoco puedes olvidarte de instalar un buen cortafuegos que evite conexiones poco seguras.

Guía del curso

Cap. 1 Bienvenido al mundo de Linux
Qué es Ubuntu. Instalación. Ubuntu live. Escritorio de Linux básico. PCI nº 44

Cap. 2 Configura Ubuntu en red
Configuración de red local. Internet. Configuración del Cortafuegos. Redes Windows (samba). Wireless. PCI nº 45

Cap. 3 Instala y actualiza aplicaciones
Aplicaciones empaquetadas. Añadir y quitar aplicaciones. Gestor de paquetes Synaptic. Gestión de paquetes mediante la línea de órdenes. Instalar un sólo archivo de paquete. Repositorios adicionales. Actualizaciones. PCI nº 46

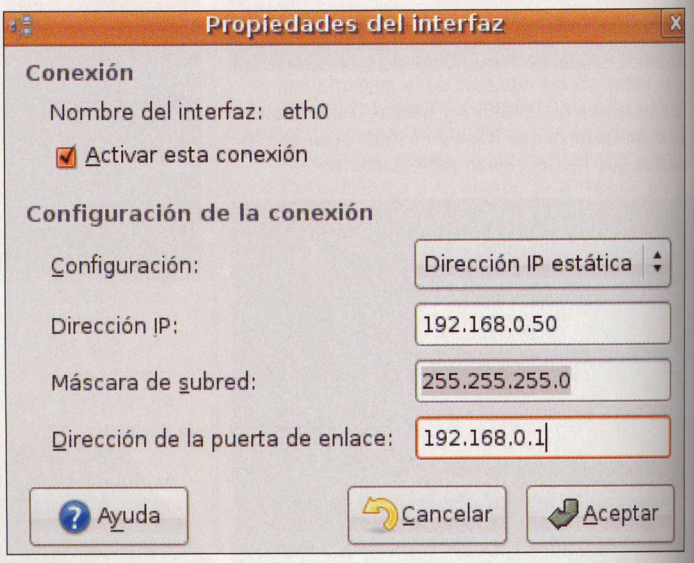
Cap. 4 Trabaja en tu PC con Ubuntu
Consejos de Escritorio. Archivos. Particiones. Arranque. Kernel. Fecha y hora. Hardware. Impresoras. PCI nº 47

Cap. 5 Disfruta del multimedia con Linux
Música. Vídeo. Formatos restringidos: códecs, MP3, DVD... Aplicaciones multimedia. Edición de imágenes. Aceleración 3D. Juegos. PCI nº 48

1 Configuración de la red local

Ubuntu es un sistema orientado a escritorio, y como tal ofrece interfaces gráficas para la mayoría de las tareas de configuración de redes. Para configurar una red local Ethernet abre la ventana de configuración de la red mediante el menú **Sistema\Configuracion\Red**.

En esta ventana se muestran las diferentes conexiones existentes. Marca la conexión Ethernet que quieras configurar, y pulsa el botón **Propiedades**. En la pantalla de Propiedades del interfaz podrás activar o desactivar la conexión, así como configurar los valores de la misma.



Cada ordenador en una red se identifica con un número al que se denomina dirección IP o simplemente IP. No puede haber dos ordenadores con la misma dirección IP en la misma red. Lo que debes hacer en la configuración de la red es, por tanto, indicar la dirección IP de tu ordenador. Puedes escoger entre tener una configuración por DHCP (el sistema solicitará a un servidor DHCP todos los datos de la configuración), o una dirección IP estática. En este último caso se habilitarán los campos para que puedas especificar la dirección IP de la máquina, la máscara de subred, y la dirección de la puerta de enlace. Todos estos valores dependen de tu red local.

Por último, en la pantalla principal de la configuración de red puedes indicar el nombre del equipo en la pestaña **General**.

2 Internet

Una de las principales necesidades actualmente es tener conexión a Internet. Configurar la conexión desde Ubuntu suele ser un proceso sencillo. Por supuesto, necesitas tener contratada una conexión a Internet con un proveedor de acceso, y que la conexión sea funcional. Existen muchos tipos de conexión diferentes, con mucho hardware diferente, y distintos proveedores de Internet. La parte buena es que Ubuntu tiene una detección de hardware bastante completa, incluye controladores para la mayor parte de los componentes más comunes, y utiliza unas configuraciones por defecto bien pensadas. ¿Qué quiere decir esto? Pues que existe una buena posibilidad de que tengas la conexión a Internet funcionando sin problemas nada más instalar Ubuntu. Haz la prueba: abre el navegador Firefox, haciendo uso del icono de acceso rápido, y trata de acceder a una página web, por ejemplo **google.com**. Si accedes es que ya tienes conexión a Internet y puedes saltarte el resto de esta sección. Si no accedes, o quieres saber cómo y por qué funciona, sigue leyendo.

La principal forma de conectarse a Internet es mediante conexiones de alta velocidad, bien ADSL, bien Cable. Y dependiendo del aparato que utilices para la conexión, los pasos a seguir son distintos. Puedes conectarte a través de un router, haciendo uso de la red local. Puedes conectarte mediante un módem USB. O puedes conectarte mediante un módem Ethernet (o cable-módem).

Problemas de los módem USB

Si te sorprende que conseguir que un simple módem funcione bajo Ubuntu sea una tarea complicada, aquí tienes la explicación.

- El estándar para las conexiones de red, ya sea con otros ordenadores de tu red local o con Internet, ha sido durante décadas el uso de una tarjeta Ethernet. Es una tecnología firme, probada y utilizada, de fiar, y fácil de configurar.
- Al contratar la conexión con un proveedor de servicios, habitualmente también obtienes el hardware necesario. Muchas veces se trata de un router o módem Ethernet, pero por cuestión de costes otras veces se proporciona un módem USB.
- La comunicación con estos módems no es ni mucho menos estándar, y los controladores los proporcionan los propios fabricantes, y habitualmente sólo funcionan en ciertas versiones específicas de MS Windows. En general, estos productos suelen dar bastantes problemas, incluso en los sistemas operativos para los que se diseñaron.
- Todo el hardware que se conecta al PC a través del puerto USB precisa un software específico para su manejo, denominado controladores (drivers). Habitualmente estos controladores son software propietario, con una licencia que prohíbe estudiarlo, modificarlo o adaptarlo a otro sistema operativo.
- Aunque algunos controladores tienen una licencia más permisiva (y se incluyen en la instalación de Ubuntu) la mayor parte de ellos no pueden incluirse por motivos legales. Por tanto, es necesario obtener los controladores directamente de los fabricantes. Y además, estos deben proporcionar controladores compatibles con Windows.

Conexión de baja velocidad mediante módem

Si aún te conectas a Internet con un módem de 56 Kb o menos, también puedes utilizarlo bajo Ubuntu. Básicamente hay dos tipos de módem:

- **Módems hardware:** suelen ser externos, conectados al puerto serie y manejan todo el funcionamiento del módem por sí mismos. Actualmente, son raros, pero están bien soportados.
- **Módems software (winmodems):** se trata de una combinación de hardware (mucho menos que en un módem hardware, lo que les hace mucho más baratos) y software (escrito para sistemas operativos Windows). Algunos de estos módems funcionan en Linux, otros no. Un módem software funcionando bajo Linux suele denominarse Linmodem.

Los módems hardware no necesitan controladores, pero los módems software sí. El sitio web especializado en módems bajo Linux es **linmodems.org**, y allí puedes obtener los controladores y las instrucciones específicas para tu modelo de módem. Además, en la documentación online de Ubuntu puedes obtener más información al respecto. La página es **help.ubuntu.com/community/DialupModemHowto**.

2.1 Conexión ADSL mediante router

Esta es, sin duda, la configuración más habitual hoy en día, y la que proporcionan la mayoría de los proveedores de Internet. Se basa en un elemento hardware, un router, que conecta una red local con Internet. Sin entrar en detalles demasiado técnicos, los router actúan como pasarelas, y toda la comunicación entre cualquier ordenador de la red e Internet circula a través del router.

Si tu conexión a Internet la realizas de esta forma, ya sea mediante cable Ethernet o Wireless, la configuración depende enteramente de tu red local. Lee las secciones sobre red local y wireless para tener más información.

Habitualmente, los routers que distribuyen los proveedores de acceso también hacen de servidor DHCP. Esto quiere decir que, en lugar de especificar una dirección IP para tu ordenador, el router le asigna una automáticamente en el momento de encenderse (además de información adicional sobre la red). Como Ubuntu por defecto solicita una dirección de este modo, si tienes un router y una red local funcionando, éste es el caso en el que es altamente probable que tu conexión a Internet se haya configurado automáticamente.

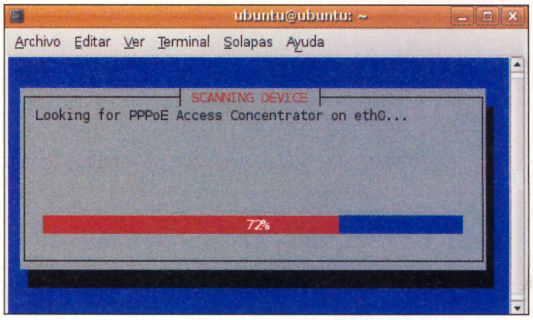
Si tu router no hace de servidor DHCP, debes configurar la IP y los parámetros de conexión de forma manual. Necesitas, por tanto, conocer la dirección IP del router. Ésta debe estar detallada en la información que te proporcionó tu proveedor de acceso al contratar el servicio con ellos. Para configurar la conexión manualmente, ve a la sección sobre la configuración de red local.

2.2 Conexión mediante módem USB

Los módem USB se popularizaron bastante en los últimos años. Aunque ahora son algo menos comunes, y su coste es mucho más reducido, muchos proveedores de Internet los han distribuido de forma masiva. USB está muy lejos de ser el medio ideal para el acceso a Internet. En general, existen muchos problemas de compatibilidades y mal funcionamiento con estos módems. Si tu módem permite la conexión vía USB y vía Ethernet, es altamente recomendable que utilices la conexión Ethernet. Y si puedes conseguir un módem Ethernet o un router, en lugar del módem USB, hazlo y te evitarás problemas. No obstante, es posible conseguir que los módem USB funcionen bajo Ubuntu, aunque dependiendo de la marca y el modelo esto puede ser bastante complejo, o incluso imposible. La mayor parte de los controladores de los módems USB son software propietario, con una licencia restrictiva, y sus fabricantes no permiten que se distribuyan con Ubuntu. Así que necesitarás descargar estos controladores de Internet desde un ordenador que tenga una conexión funcionando, y luego transferirlos a tu instalación de Ubuntu (mediante un CD, un disco extraíble, etc.).

2.3 Conexión mediante módem Ethernet

Aunque es menos común que el uso de un router, algunos proveedores precisan que se conecte directamente a un módem ADSL mediante PPPoE (Point to Point Protocolo over Ethernet, Protocolo de Punto a Punto sobre Ethernet). La configuración de la cuenta (usuario y contraseña) que suele almacenar el router, en este caso se almacenará en el PC, por lo que te hará falta para crear la



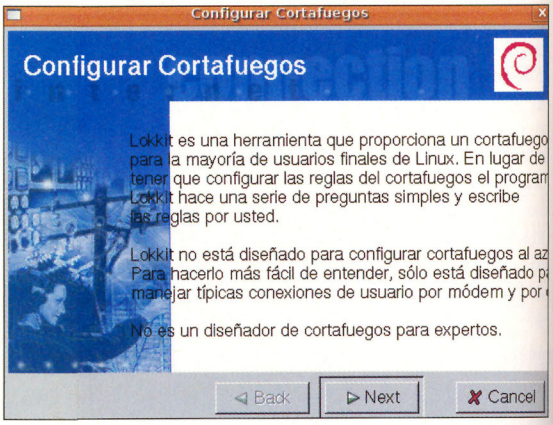
conexión. Además, antes de empezar, necesitas tener conectada tu tarjeta con el módem, mediante un cable Ethernet. Para configurar la conexión, necesitas abrir un terminal en el que introducir comandos en modo texto. Para abrirlo, utiliza el menú **Aplicaciones/Accesorios/Terminal**.
Una vez abierto el Terminal, escribe el comando **sudo pppoeconf**. El sistema te pedirá tu contraseña antes de ejecutar el comando. A continuación, un programa de menús en modo texto te guiará durante los siguientes pasos:

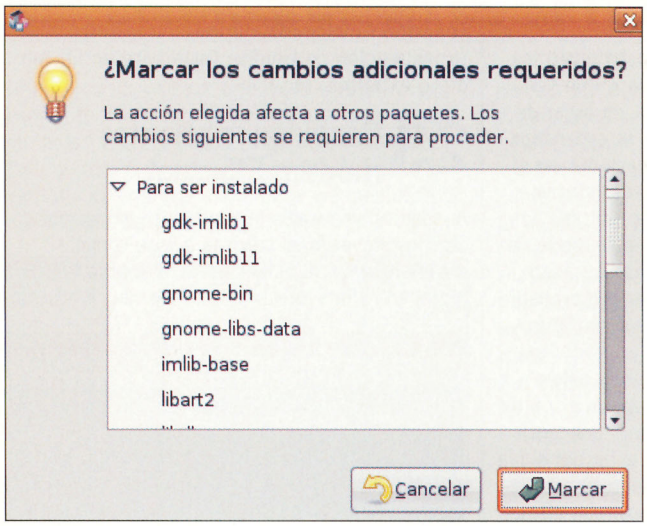
- En primer lugar, confirmar que se detecta correctamente tu tarjeta Ethernet.
- Introducir tu nombre de usuario para la conexión a Internet (que debe proporcionarte tu proveedor).
- Introducir tu contraseña para la conexión a Internet (que debe proporcionarte tu proveedor).
- Si ya tenías una conexión PPPoE configurada, debes confirmar que puede ser modificada.
- Se te preguntará si quieres activar las opciones **noauth** y **defaultroute**, y eliminar **nodetach**. Escoge **Yes**.
- A la pregunta de utilizar **peer DNS**, la respuesta que debes seleccionar es **Yes**.
- A la pregunta de **Limited MSS problem**, también tienes que señalar **Yes**.
- Cuando se te pregunte si deseas conectar al arrancar, escoge **Yes** si es lo que prefieres.
- Por último, se te ofrece la posibilidad de establecer la conexión inmediatamente.

Una vez que hayas completado todos estos pasos, deberías tener funcionando la conexión sin niingún problema.
Si no has escogido que la conexión se inicie al arrancar, o si deseas lanzarla o pararla en un momento dado, puedes hacerlo mediante unos comandos. Para iniciar la conexión utiliza **sudo pon dsl-provider** y para finalizarla escribe **sudo poff dsl-provider**.

3 Configuración del cortafuegos

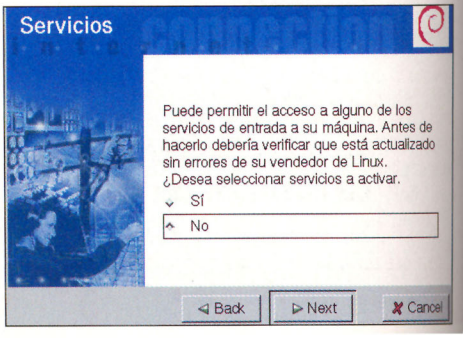
Un cortafuegos es un programa que, en un entorno de red, evita ciertas conexiones, definidas por una política de seguridad. Un cortafuegos tiene como tarea básica controlar la comunicación entre zonas con diferente nivel de confianza (como tu ordenador e Internet), de forma que haya conectividad entre las zonas, pero controlada. En el día a día, un cortafuegos impide que se establezcan conexiones no deseadas desde Internet a tu ordenador, y a la vez impide que los programas de tu ordenador accedan a Internet sin tu autorización.
La instalación por defecto de Ubuntu incluye bastante software útil para el escritorio, pero no incluye un cortafuegos por defecto. Afortunadamente, instalar y configurar uno es bastante sencillo. Como ocurre a menudo en el mundo Linux, existen multitud de cortafuegos distintos que puedes utilizar. Vamos a hablarte de dos de los principales. El primero es **Lokkit**, que mediante un asistente, te permite configurar un cortafuegos básico. Es un programa realmente sencillo de utilizar, y no requiere que tengas mucho conocimiento sobre cortafuegos. En contrapartida, ofrece pocas opciones, y no es la mejor elección si quieres configurar un cortafuegos complejo. El segundo, **Guarddog**, es un programa de configuración mucho más flexible, pero también mucho más complejo. Escoge instalar Guarddog sólo si tienes buenos conocimientos sobre cortafuegos y quieres personalizar el tuyo al máximo.
Lo primero que debes hacer es instalar el software en tu ordenador. En próximas entregas del curso te enseñaremos todo lo necesario sobre la instalación de programas, pero por ahora limítate a seguir los pasos para instalarlo. Ya que vas a descargar el programa de Internet, lo primero que necesitas es tener una conexión a Internet operativa. La instalación vas a realizarla a través del gestor de paquetes, así que ábrelo en el menú **Sistema\Administracion\Gestor de paquetes Synaptic**. Si es la primera vez que lo abres, es posible que te aparezca una ventana de introducción rápida. Por ahora puedes ignorarla, así que simplemente pulsa **Cerrar**.
Lo primero que necesitas es información actualizada sobre el software disponible. Selecciona el menú **Configuracion\Repositorios**, y en la pestaña **Soporte de la instalación** selecciona todos los canales, y pulsa el botón **Cerrar**. Acepta el aviso, pulsa el botón **Recargar**, y espera a que termine de descargarse la información de los paquetes. A continuación, pulsa el botón **Buscar**, y en el diálogo de búsqueda introduce bien **gnome-lokkit**, bien **guarddog**, dependiendo de cuál quieras instalar. Haz doble clic sobre el nombre del paquete. El instalador te preguntará si quieres marcar los cambios adicionales requeridos. Pulsa el botón **Marcar**. Por último, pulsa el botón **Aplicar** y en la pantalla de confirmación pulsa de nuevo **Aplicar**. Cuando termine la instalación puedes cerrar el gestor de paquetes.





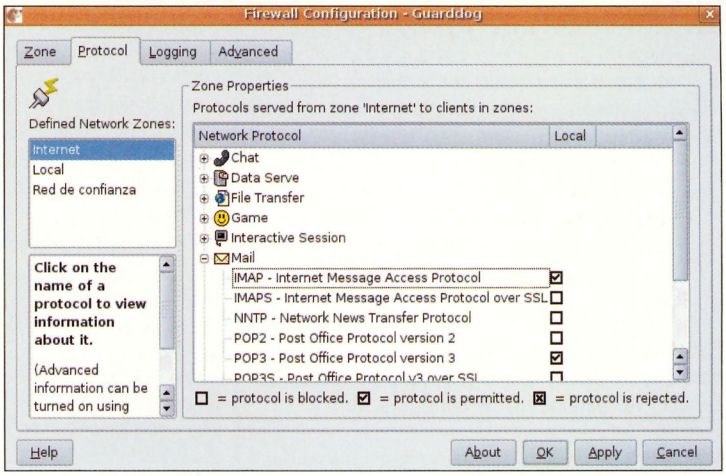
3.1 Lokkit

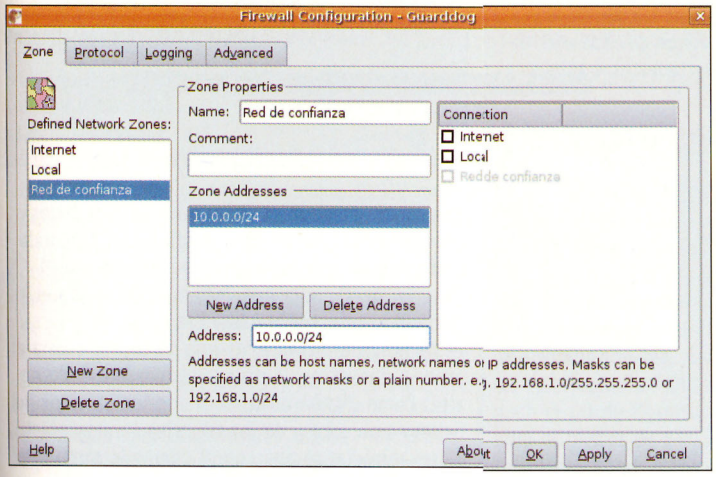
Para ejecutar Lokkit necesitas privilegios de administrador, así que abre un diálogo de ejecución mediante **Alt + F2**, y ejecuta **gksudo gnome-lokkit**. Tras introducir tu contraseña, verás un diálogo de configuración del cortafuegos.
El asistente de configuración de Lokkit es bastante autoexplicativo. Es recomendable que selecciones la opción de **Seguridad Alta**. El resto de opciones dependen de tus necesidades. Por ejemplo, si utilizas DHCP para obtener la dirección IP de tu ordenador (que es lo más seguro si tienes un cable módem o un router ADSL), deberías decir que sí cuando el asistente te pregunte si debe habilitar DHCP.
Si tu ordenador es el único en la red, lo más probable es que no necesites habilitar ningún servicio, y es seguro que digas a Lokkit que no los habilite cuando te lo pregunte.
Cuando termines la configuración, Lokkit te dirá que está preparado para activar el cortafuegos, y podrás aplicar los cambios y lanzarlo, o bien cancelar todo.
Si tras activar el cortafuegos tienes problemas con alguna de las elecciones que hiciste, siempre puedes relanzar Lokkit y seleccionar **Deshabilitar cortafuegos** para eliminar todas las reglas definidas.
Lokkit es fácil de utilizar y establece un buen conjunto de reglas para el cortafuegos. No obstante, aún bajo la configuración más restrictiva, Lokkit deja abiertos algunos de los servicios más utilizados para evitar perjudicar el funcionamiento normal (deja abiertos SSH, VNC, y permite que servicios como ping y BitTorrent funcionen). Si necesitas reglas más estrictas o una mayor personalización, puedes utilizar Guarddog.



3.2 Guarddog

Para configurar un firewall con Guarddog debes lanzarlo como súper usuario, así que ejecuta **gksudo guarddog**. La primera vez que lo ejecutes aparecerá un aviso indicando que aún no tienes definida ninguna configuración.
Este programa es mucho más complejo que Lockkit. Lo primero que verás al arrancarlo es la pestaña de zonas. Las zonas son básicamente conjuntos de direcciones IP que se utilizan para definir reglas que afecten a todas las IP de ese grupo. Por ejemplo, si tu máquina está en una red local con las direcciones IP en una red privada, puedes definir una zona para todas estas direcciones y asignarles reglas particulares.
Por defecto, Guarddog viene configurado con dos zonas. Una zona Local, para las direcciones IP en la máquina local, y una zona Internet, para todas las demás.
Para establecer una zona para tu red local, pulsa en **New Zone**, y bajo **Zone Addresses**, pulsa en **New Address**. En el campo **Address** puedes especificar una sola dirección, o una máscara de red que cubra un conjunto de direcciones. Por ejemplo, si tu red local está en el rango 10.0.0.0, y tus direcciones van de 10.0.0.1 a 10.0.0.255, puedes especificar todo el conjunto de direcciones como 10.0.0.0/24.
Definir más zonas, aparte de Internet y Local, te sirve para establecer reglas específicas para los ordenadores de estas zonas, si quieres un nivel de seguridad distinto para estas máquinas que para el del resto de ordenadores de Internet. Piensa en Internet como la zona más hostil, de la que es más probable que puedan llegar ataques de personas o programas (gusanos, virus...) que pongan en peligro tu seguridad, y por tanto la zona a la que debes permitir el mínimo tráfico posible.
Una vez que hayas configurado las zonas a tu gusto, el siguiente paso es definir las configuraciones de los protocolos. En este punto debes indicar a Guarddog exactamente qué protocolos quieres habilitar. Ten en cuenta que todo lo que no esté explícitamente habilitado estará deshabilitado. Por defecto nada (ni siquiera DNS, http, o correo POP3) está habilitado. Así que selecciona todos los protocolos que desees habilitar, para cada una de las zonas definidas en el paso previo, y pulsa **Apply**. En este momento es buena idea que compruebes si aún puedes navegar, recibir correo y cualquier cosa más que necesites, y si encuentras problemas revisa los protocolos permitidos.
Guarddog también te permite guardar informes (logs) en la pestaña **Logging**. Lo más probable es que no te interese leer la lista de todo el tráfico que ha permitido o rechazado, por lo que es recomendable que desactives los informes.
Por último, bajo la pestaña **Advanced** puedes configurar protocolos personalizados, si Guarddog no incluye reglas que encajen con un protocolo que necesites habilitar.
Aunque la configuración de este cortafuegos puede ser algo costosa, el resultado final es un sistema protegido y con reglas muy específicas del tráfico que quieres permitir entre tu máquina y el resto, por lo que el esfuerzo merece la pena.



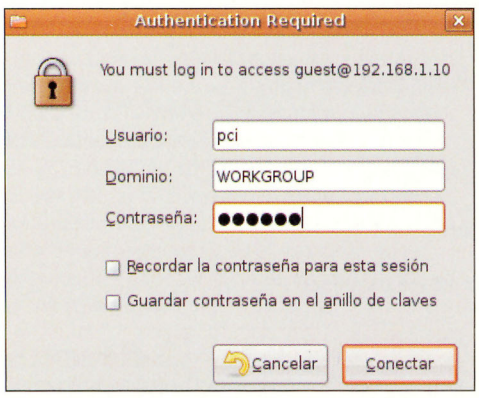


4 Redes Windows (Samba)

Cuando hay varios ordenadores en la misma red local, una de las necesidades básicas es poder compartir archivos entre ellos. E
xisten muchas formas de hacer esto, pero la más común entre ordenadores ejecutando Windows es la compartición de carpetas que ofrece este sistema operativo.
Como en muchas ocasiones, en una misma red se encuentran conviviendo ordenadores con Linux y con Windows, existe un conjunto de herramientas que permite a una máquina Linux hacer uso del sistema de compartición de Windows. A este conjunto de herramientas se las conoce como **Samba**.
Básicamente, hay dos cosas que puedes querer hacer. Bien acceder a los ficheros compartidos de un ordenador con Windows, o bien permitir a un ordenador con Windows acceder a tus ficheros compartidos.

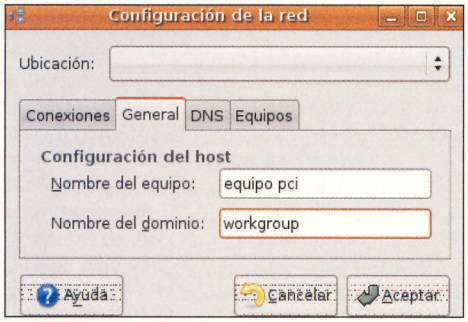
4.1 Accede a los ficheros compartidos de Windows

Por defecto, Ubuntu ya incluye la capacidad de acceder a los ficheros compartidos a través de Samba. El procedimiento es muy sencillo. Abre un navegador de archivos (utilizando, por ejemplo, la entrada de menú **Lugares\Carpeta Personal**). Selecciona el menú **Ir a\Lugar...** y en la barra de lugar especifica la dirección IP o el nombre del ordenador al que quieras acceder, precedida por **sbm://** (que indica a tu ordenador que deseas acceder mediante samba). Por ejemplo, para acceder a un ordenador con la dirección IP 192.168.1.100 la dirección sería smb://192.168.1.100.
Depende de la configuración del ordenador al que accedas, pero es probable que solicite un nombre de usuario y contraseña del ordenador destino antes de permitirte el acceso. Una vez los introduzcas, accederás a las carpetas compartidas del equipo mediante tu explorador de archivos, y podrás leer los archivos, modificarlos o añadir nuevos de acuerdo a la política de seguridad definida en el destino.



4.2 Comparte ficheros con Samba

Si lo que quieres es compartir tus archivos de forma que puedan acceder a ellos ordenadores con Windows, debes instalar y configurar la versión completa de Samba.
Ya que vas a descargar el programa de Internet, lo primero que necesitas es tener una conexión a Internet operativa. Abre el gestor de paquetes en el menú **Sistema\Administracion\Gestor de paquetes Synaptic**. En él, pulsa el botón **Buscar** y busca **samba**. Te aparecerán varios paquetes en la búsqueda, pero sólo te interesa el que se llama samba. Haz doble clic en el nombre del paquete y pulsa **Aplicar** (acepta los cuadros de confirmación que vayan saliendo).
Para acceder a la configuración de **Samba** abre el menú **Sistema\Configuracion\Red**, y accede a la pestaña **General**.



Por supuesto, para poder configurar tu máquina para que funcione en una red Windows, necesitas conocer los parámetros de configuración:

- **Nombre de equipo:** el nombre que quieres que tenga tu PC en la red.
- **Nombre del dominio:** el dominio Windows al que te quieres conectar.

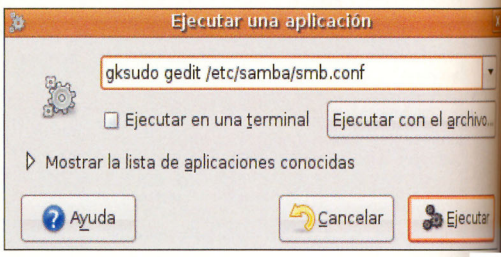
Ahora que tienes Samba configurado y funcionando, puedes definir las carpetas que quieres compartir. Por desgracia, todavía no existe una interfaz gráfica para hacer esto, por lo que la única forma de llevarlo a cabo es modificando manualmente un fichero de configuración. Debes abrir el fichero con permisos de administrador. Para ello, pulsa la combinación de teclas **Alt + F2** para obtener un diálogo de ejecución, y en él escribe la línea: **gksudo gedit /etc/samba/smb.conf**.
El fichero smb.conf se divide en varias secciones. La que te interesa es **File Sharing**. Para compartir tu carpeta home y permitir que otros usuarios puedan escribir en ella, debes localizar la entrada **[homes]** y modificar sus valores para dejarlos como muestra el **Cuadro 1**.
Por último, debes definir los usuarios a las

```
[homes]
comment = Home Directories
browseable = yes
# By default, the home directories are exported read-only. Change next
# parameter to 'yes' if you want to be able to write to them.writable = yes
# File creation mask is set to 0700 for security reasons. If you want to
# create files with group=rw permissions, set next parameter to 0775.create mask = 0775
# Directory creation mask is set to 0700 for security reasons. If you want to
# create dirs. with group=rw permissions, set next parameter to 0775.directory mask = 0775
```

Cuadro 1

Red Windows

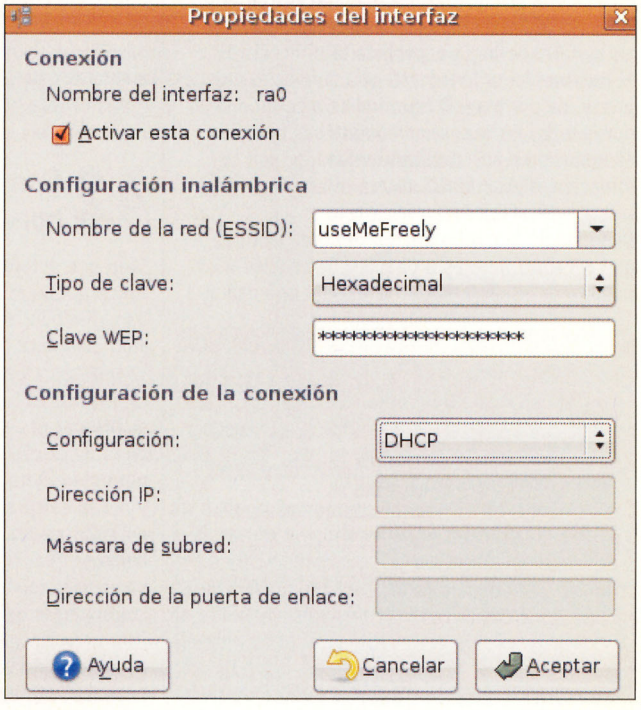
Una vez configurado Samba puedes acceder a los ficheros compartidos de otros ordenadores de la red de forma muy sencilla mediante el menú **Lugares\Servidores de red**, y haciendo uso del icono **Red de Windows**. Verás un listado de todos los dominios o grupos de trabajo de tu red, y dentro de cada uno de ellos los ordenadores que pertenezcan a ellos y estén compartiendo algo.



que vas a dar permiso de acceso a tus ficheros compartidos. Esto se hace mediante el comando **smbpasswd**. Por ejemplo, para dar de alta el usuario "axel", abre una Terminal, y escribe el comando **sudo smbpasswd -a axel**
Te pedirá que introduzcas una contraseña para el usuario dos veces, y el usuario quedará dado de alta. Como última nota, para que los cambios del fichero smb.conf y de los usuarios tengan efecto, debes reiniciar samba con el comando **sudo /etc/init.d/samba reload**.

5 Wireless

El uso de tecnología wireless está cada vez más extendido. Como al fin y al cabo sigue siendo tecnología de red, parte de su configuración es idéntica a la configuración de red local por Ethernet.
Para establecer los parámetros debes acceder al administrador de red, desde el menú **Sistema\Configuracion\Red**. En la primera pestaña, **Conexiones**, verás un listado de todos los interfaces de red que se hayan detectado. Los dispositivos wireless están claramente identificados con un icono y el título Wireless. Ubuntu incluye controladores para un alto porcentaje de las tarjetas wireless del mercado, por lo que lo más probable es que aquí veas listada tu tarjeta. Si no es así, significa que no están funcionando los controladores para tu tarjeta, por lo que tendrás que instalarlos para poder utilizarlos. Las instrucciones para esto están en el siguiente punto. Si tienes varias conexiones de red (por ejemplo, Ethernet y wireless) debes indicar en esta misma pestaña cuál de ellas es tu puerta de enlace por defecto. Debería ser la conexión que más utilices. Es más, si no es absolutamente necesario, lo más recomendable es tener sólo un interfaz de red activo al mismo tiempo. Puedes desactivar el que no utilices con el botón **Desactivar**.



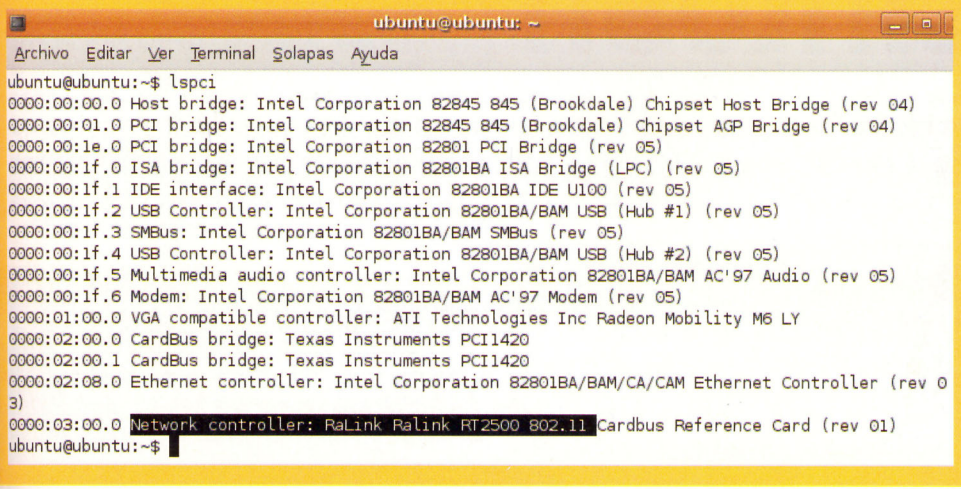
5.1 Configuración de la conexión wireless

Para utilizar la conexión wireless, primero debes configurarla. Por supuesto, necesitarás conocer los parámetros de la configuración del router, que debería haberte proporcionado tu proveedor de acceso. Selecciona la conexión wireless de la lista y pulsa el botón **Propiedades**.
Debes configurar los siguientes parámetros:

- Nombre de la red: es el ESSID de tu punto de acceso wireless. Un ESSID es simplemente un nombre identificativo. Muchos fabricantes

Tarjetas soportadas

A pesar de ser de diferentes marcas, muchas tarjetas utilizan los mismos componentes. Por tanto, para saber si tu tarjeta funciona o no, lo que debes conocer es lo que se llama **chipset**, que es el nombre de esos conjuntos de componentes.
Si no conoces cuál es el chipset de tu tarjeta, abre una ventana de Terminal (**Aplicaciones/Accesorios/Terminal**) y ejecuta el comando **sudo lspci**. Ahí verás información de gran parte del hardware de tu PC, incluyendo información de la tarjeta wireless. Una vez sepas qué chipset utiliza tu tarjeta, puedes comprobar si está soportado por Ndiswrapper en la dirección **ndiswrapper.sourceforge.net/mediawiki/index.php/List**. Aquí, además, puedes obtener consejos de instalación para tarjetas específicas, e incluso links a los controladores Windows que mejor funcionan.



dejan el nombre de la marca como ESSID por defecto (como "3Com" o "Linksys"), pero el nombre que debes indicar tú depende de la configuración de tu router. La mayor parte de las tarjetas modernas permiten buscar puntos de acceso cercanos, por lo que es probable que en el combo tengas un listado de aquellos routers wireless que se han detectado, entre los que debería estar el tuyo.

- Si utilizas encriptación WEP debes indicar el tipo de clave que utilizas (Hexadecimal o sin formato), y a continuación introducir dicha contraseña. Ten en cuenta que si utilizas una contraseña hexadecimal debes introducirla toda seguida, sin guiones ni espacios (por ejemplo, sería "0123456789ABCDEF0123" en lugar de "01-23-45-67-89-AB-CD-EF-01-23").
- Por último, debes indicar la forma en la que tu tarjeta obtendrá su dirección IP. Puede solicitarla directamente al punto de acceso (mediante DHCP), con lo que no tendrías que indicar más parámetros. O bien puedes establecer una dirección estática, para lo que tendrás que especificar la dirección IP en sí misma, la máscara de subred, y la dirección IP del punto de acceso. De nuevo, estos parámetros debe facilitártelos tu proveedor de acceso a Internet.
- Si has escogido la opción de dirección IP estática, también debes indicar la dirección IP de los DNS. Estos se indican en la pantalla principal de la **Configuración de la red**, en la pestaña **DNS**.

5.2 Ndiswrapper

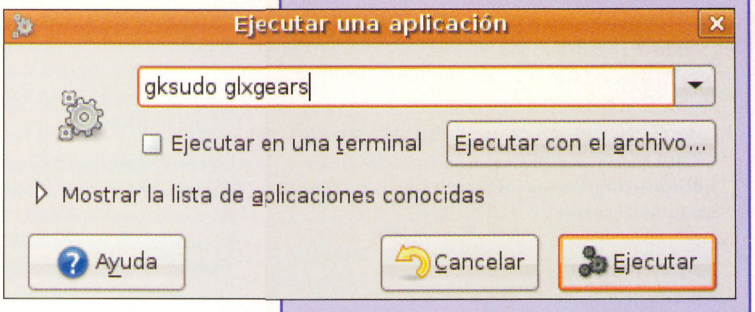
Si Ubuntu no reconoce tu tarjeta wireless lo más probable es que no existan controladores para tu tarjeta en Linux. No obstante, aunque no haya controladores nativos es muy probable que puedas hacerla funcionar utilizando Ndiswrapper. Se trata de un módulo Linux que permite a Ubuntu utilizar los controladores de las tarjetas creados para Windows. Como todos los fabricantes distribuyen controladores para Windows, mediante Ndiswrapper se puede conseguir que funcionen la gran mayoría de las tarjetas de red.
Lo primero que necesitas es instalar el paquete **ndiswrapper-utils**. Éste se encuentra en el CD de instalación de Ubuntu. Para instalarlo, introduce el CD de Ubuntu en tu PC. A continuación, abre el gestor de paquetes en el menú **Sistema\Administracion\Gestor de paquetes Synaptic**. En él, pulsa el botón **Buscar** y busca **ndis**. Haz doble clic en el nombre del paquete y pulsa **Aplicar** (acepta los cuadros de confirmación que vayan saliendo).
Una vez instalado Ndiswrapper necesitas los controladores de tu tarjeta para el sistema Windows. Así que en primer lugar, introduce el CD de los controladores o descárgalos de Internet. Localiza el archivo y ábrelo con doble clic para acceder a su contenido. Necesitarás los ficheros con extensión INF y SYS, y si los hubiese también los BIN, así que cópialos a tu directorio HOME. A continuación, instala los controladores haciendo uso de Ndiswrapper. Abre una Terminal (**Aplicaciones/Accesorios/Terminal**) y ejecuta el comando **sudo ndiswrapper –i driver.inf**. Siendo driver.inf el nombre del controlador de tu tarjeta. Recuerda que el nombre debes escribirlo exacto, incluyendo las mayúsculas y minúsculas. Con esto, el controlador ya está guardado en tu sistema. El siguiente paso es cargarlo. Para ello escribe los comandos:

sudo depmod -a
sudo modprobe ndiswrapper

Si todo ha ido bien, ya deberías tener la tarjeta funcionando, y puedes configurarla como se indica en el punto anterior. Si tienes problemas, la página de Ndiswrapper (**ndiswrapper.sourceforge.net**) tiene mucha documentación y puede serte de ayuda.
Por último, deberías indicar al sistema que cargue el controlador en el momento de arrancar (de lo contrario deberías cargarlo manualmente cada vez). Para ello ejecuta el comando **sudo ndiswrapper -m**.
El mes que viene te explicaremos cómo instalar y utilizar aplicaciones, gestionar paquetes, etc., trabajando con Ubuntu.

Root (Administrador)

En todos los sistemas Linux existe una clara división entre el administrador del sistema, conocido como root o superusuario, y los usuarios normales. La mayor parte de los programas y configuraciones que afectan a todo el sistema requieren privilegios de administrador, de forma que se evita que un usuario descuidado o malicioso pueda dañar el sistema.
En Ubuntu la política de seguridad es algo distinta al resto de distribuciones Linux. En lugar de acceder al sistema como root para realizar las tareas de administración, el usuario principal del sistema (el que se creó en el momento de la instalación) puede lanzar aplicaciones como si fuese el administrador, haciendo uso de los comandos sudo y gksudo.
Para ejecutar un programa como root, abre una Terminal mediante el menú **Aplicaciones/Accesorios/Terminal**, y ejecuta el comando sudo programa. El sistema te pedirá que introduzcas tu contraseña, y a continuación ejecutará el programa (por ejemplo, "sudo top" ejecutaría el programa top con privilegios de administrador).
Para lanzar aplicaciones gráficas, utiliza gksudo. La idea es la misma, pero en lugar de en una Terminal, puedes ejecutarlo en un diálogo de ejecución (**Alt + F2**). Igualmente, se te pedirá la contraseña (ahora de forma gráfica), y se ejecutará la aplicación con todos los privilegios de administrador.



Si eres un usuario avanzado y estás acostumbrado a acceder directamente al sistema como administrador para realizar las tareas de mantenimiento, siempre puedes habilitar la cuenta de root. Para ello, en una Terminal, escribe el comando **sudo passwd**. Con este comando podrás asignar una contraseña a la cuenta de root, y a partir de ese momento tendrás ese usuario utilizable. Ten en cuenta que al ejecutar este comando se te pedirá primero la contraseña de tu usuario. A continuación, la contraseña que deseas asignar a root. Y por último, que repitas la contraseña de root para verificarla.