CF GRADO SUPERIOR

CICLOS FORMATIVOS

R.D. 1538/2006

Servicios de Red e Internet



FRANCISCO J. MOLINA ROBLES
EDUARDO POLO ORTEGA

Ra-Ma®

www.ra-ma.es/cf

Servicios de Red e Internet

FRANCISCO JOSÉ MOLINA ROBLES
EDUARDO POLO ORTEGA

Ra-Ma®

Índice

INTRODUCCIÓN **9**

CAPÍTULO 1. ASIGNACIÓN DINÁMICA DE DIRECCIONES **11**

1.1 FUNCIONAMIENTODE DHCP 13

1.2 PARÁMETROS DE CONFIGURACIÓNDE DHCP 15

1.2.1 Parámetros en el servidor 15

1.2.2 Parámetros en el cliente 16

1.3 CONFIGURACIÓN DE UN SERVIDOR DHCP 16

1.3.1 Configuración en Microsoft Windows 16

1.3.2 Configuración en GNU/Linux 21

1.4 CONFIGURACIÓN DE LOS CLIENTES 28

1.4.1 Configuración del cliente en Microsoft Windows 28

1.4.2 Configuración del cliente en GNU/Linux 33

1.5 PROBLEMAS ASOCIADOS A DHCP 43

1.5.1 Problemas con el cortafuegos 44

1.5.2 Problemas con Microsoft Windows Vista/7 45

RESUMEN DEL CAPÍTULO 46

EJERCICIOS PROPUESTOS 47

TEST DE CONOCIMIENTOS 48

CAPÍTULO 2. SISTEMA DE NOMBRES DE DOMINIO **49**

2.1 INTRODUCCIÓN 50

2.2 REGISTRO DE UN DOMINIO EN INTERNET 55

2.3 CUESTIONES RELATIVAS A LA SEGURIDAD 56

2.4 CONFIGURACIÓN DE UN SERVIDOR DNS 57

2.4.1 Instalación en Microsoft Windows 57

2.4.2 Instalación en GNU/Linux 63

2.4.3 Problemas del servidor DNS 76

2.5 CONFIGURACIÓN DE UN CLIENTE DNS 77

2.5.1 Configuración en Microsoft Windows 80

2.5.2 Configuración en GNU/Linux 80

RESUMEN DEL CAPÍTULO 84

EJERCICIOS PROPUESTOS 85

TEST DE CONOCIMIENTOS 86

CAPÍTULO 3. EL SERVICIO HTTP **87**

3.1 FUNCIONAMIENTO DEL SERVICIO HTTP 88

3.1.1 Acceso seguro y utilización de certificados 92

3.2 PARÁMETROS DE CONFIGURACIÓN DEL SERVICIO HTTP 93

3.2.1 Parámetros del servidor 93
3.2.2 Parámetros del cliente 93
3.3 CONFIGURACIÓN DEL SERVIDOR HTTP 94
3.3.1 Configuración en Microsoft Windows 94
3.3.2 Configuración en GNU/Linux 101
3.4 CONFIGURACIÓN DEL CLIENTE HTTP 111
3.4.1 Configuración en Microsoft Windows 112
3.4.2 Configuración en GNU/Linux 115
RESUMEN DEL CAPÍTULO 118
EJERCICIOS PROPUESTOS 119
TEST DE CONOCIMIENTOS 120
CAPÍTULO 4. EL SERVICIO DE TRANSFERENCIA DE ARCHIVOS 121
4.1 FUNCIONAMIENTO DE FTP 122
4.2 PARÁMETROS DE CONFIGURACIÓN DE FTP 124
4.2.1 Parámetros en el servidor 124
4.2.2 Parámetros en el cliente 125
4.3 CONFIGURACIÓN DE UN SERVIDOR 125
4.3.1 Configuración en Microsoft Windows 125
4.3.2 Configuración en GNU/Linux 132
4.4 CONFIGURACIÓN DE UN CLIENTE 140
4.4.1 Acceso mediante línea de órdenes 140
4.4.2 Acceso mediante navegador 144
4.4.3 Acceso mediante programas específicos 145
RESUMEN DEL CAPÍTULO 147
EJERCICIOS PROPUESTOS 148
TEST DE CONOCIMIENTOS 149
CAPÍTULO 5. TERMINAL REMOTO 151
5.1 FUNCIONAMIENTO DEL SERVICIO 152
5.1.1 TELNET (*Telematics Network*) 152
5.1.2 RLOGIN (*Remote Login*) 153
5.1.3 SSH (*Secure Shell*) 153
5.1.4 X-Terminal 154
5.1.5 Escritorio remoto VNC 154
5.1.6 Terminal Server 154
5.1.7 Acceso remoto mediante interfaz web 155
5.2 CONFIGURACIÓN DEL SERVICIO DE ACCESO REMOTO 156
5.2.1 Configuración en Microsoft Windows 156
5.2.2 Configuración en GNU/Linux 160
5.3 CONFIGURACIÓN DEL CLIENTE DE ACCESO REMOTO 163
5.3.1 Configuración en Microsoft Windows 163
5.3.2 Configuración en GNU/Linux 170
RESUMEN DEL CAPÍTULO 175

EJERCICIOS PROPUESTOS 176
TEST DE CONOCIMIENTOS 177

CAPÍTULO 6. LOS SERVICIOS DE CORREO ELECTRÓNICO 179
6.1 INTRODUCCIÓN 180
6.2 PROTOCOLOS INVOLUCRADOS 181
6.2.1 Formatos de mensajes 182
6.2.2 Transferencia de correo 184
6.2.3 Seguridad y privacidad 186
6.2.4 Protección frente a virus 188
6.2.5 Correo basura (*spam*) 189
6.3 CONFIGURACIÓN DE UN CLIENTE DE CORREO 190
6.3.1 Configuración en Windows 190
6.3.2 Configuración en Linux 193

RESUMEN DEL CAPÍTULO 194
EJERCICIOS PROPUESTOS 195
TEST DE CONOCIMIENTOS 196

CAPÍTULO 7. SERVIDORES DE CORREO ELECTRÓNICO 197
7.1 SERVIDORES DE CORREO EN MICROSOFT WINDOWS 198
7.1.1 Internet Information Services en Windows Server 2003 198
7.1.2 Microsoft Exchange Server 2007 201
7.2 SERVIDORES DE CORREO EN GNU/LINUX 206
7.2.1 Instalación y configuración del agente de transporte *Sendmail* 207
7.2.2 Instalación y configuración del agente de usuario *Cyrus* 210
7.3 PROBLEMAS Y SOLUCIONES 213
7.3.1 Problemas relacionados con el DNS 214
7.3.2 Problemas relacionados con los puertos del servidor 215
7.3.3 Problemas con *Sendmail* 216
7.3.4 Problemas con *Cyrus* 217

RESUMEN DEL CAPÍTULO 218
EJERCICIOS PROPUESTOS 219
TEST DE CONOCIMIENTOS 220

CAPÍTULO 8. MENSAJERÍA INSTANTÁNEA 221
8.1 INTRODUCCIÓN 222
8.2 TIPOS DE SERVICIOS DE MENSAJERÍA INSTANTÁNEA 222
8.2.1 IRC 223
8.2.2 XMPP 224
8.2.3 OSCAR 224
8.2.4 Yahoo Messenger y Windows Live Messenger 225
8.2.5 Skype 225
8.3 CLIENTES DE MENSAJERÍA INSTANTÁNEA 226
8.3.1 Pidgin 227
8.3.2 Google Talk 228

8.3.3 Yahoo Messenger y Windows Live Messenger 229
8.3.4 Skype 230
8.3.5 Clientes IRC 231
8.4 SERVIDORES DE MENSAJERÍA INSTANTÁNEA 232
8.4.1 Instalación y configuración de un servidor XMPP 232
8.4.2 Instalación y configuración de un servidor IRC 242
RESUMEN DEL CAPÍTULO 245
EJERCICIOS PROPUESTOS 246
TEST DE CONOCIMIENTOS 247
CAPÍTULO 9. SERVICIOS DE AUDIO 249
9.1 FUNCIONAMIENTO DEL SERVICIO 250
9.2 FORMATOSDE AUDIO 252
9.2.1 MP3 252
9.2.2 Ogg Vorbis 252
9.2.3 MIDI (Instrumento Musical de Interfaz Digital) 252
9.2.4 WAVE o WAV (*Waveform Audio Fileformat* o Formato de Fichero de Audio en forma de Onda) 253
9.2.5 AAC (*Advanced Audio Coding* o Codificación de Audio Avanzada) 253
9.2.6 WMA (*Windows Media Audio*) 253
9.2.7 Real Audio 253
9.3 STREAMING 254
9.4 SINDICACIÓN Y SUSCRIPCIÓN DE AUDIO.PODCAST 256
9.5 CONFIGURACIÓN DEL SERVIDOR 258
9.5.1 Configuración en Microsoft Windows 258
9.5.2 Configuración en GNU/Linux 261
9.6 CONFIGURACION DE UN CLIENTE 264
9.6.1 Configuración en Microsoft Windows 264
9.6.2 Configuración en GNU/Linux 265
RESUMEN DEL CAPÍTULO 266
EJERCICIOS PROPUESTOS 267
TEST DE CONOCIMIENTOS 268
CAPÍTULO 10. SERVICIOS DE VÍDEO 269
10.1 FUNCIONAMIENTO DEL SERVICIO 270
10.2 FORMATOS DE IMAGEN 271
10.2.1 Características de las imágenes de mapa de bits 271
10.2.2 Formato de los archivos de mapa de bits 272
10.2.3 Formato de los archivos de imágenes vectoriales 273
10.3 FORMATOS DE VÍDEO 273
10.3.1 MPEG (*Moving Pictures Experts Group* o Grupo de Expertos en Imágenes en Movimiento) 274
10.3.2 AVI (*Audio Video Interleave* o Audio y Vídeo Intercalado) 274
10.3.3 ASF (*Advanced Streaming Format* o Formato Avanzado de Secuencias) 274
10.3.4 WMV (*Windows Media Video*) 274
10.3.5 MKV (*Matroska Video*) 275

10.3.6 Quicktime 275
10.3.7 Real Video 275
10.3.8 Flash Video 275
10.3.9 Ogg u Ogv 275
10.3.10 DV (*Digital Video* o Vídeo Digital) 275
10.4 COMPRESIÓN DE VIDEO 276
10.5 VIDEOCONFERENCIA 276
10.5.1 Videoconferencia mediante navegador web con Dimdim 278
10.6 CONFIGURACIÓN DEL SERVIDOR 279
10.6.1 Configuración en Microsoft Windows 280
10.6.2 Configuración en GNU/Linux 282
10.7 CONFIGURACIÓN DE UN CLIENTE 285
10.7.1 Configuración en Windows 285
10.7.2 Configuración en GNU/Linux 287
RESUMEN DEL CAPÍTULO 289
EJERCICIOS PROPUESTOS 290
TEST DE CONOCIMIENTOS 291
CAPÍTULO 11. OTROS SERVICIOS 293
11.1 LISTAS DE DISTRIBUCIÓN DE CORREO 294
11.1.1 Introducción 294
11.1.2 Instalación y configuración en Microsoft Windows 296
11.1.3 Instalación y configuración en GNU/Linux 302
11.2 SERVICIOS DE REDIFUSIÓN 310
11.3 EL SERVICIO HORARIO NTP 311
11.3.1 Configuración de un servidor NTP 311
11.3.2 Configuración de un cliente NTP 313
RESUMEN DEL CAPÍTULO 315
EJERCICIOS PROPUESTOS 316
TEST DE CONOCIMIENTOS 317
CAPÍTULO 12. VOIP 319
12.1 TELEFONÍA TRADICIONAL 320
12.1.1 Pública 320
12.1.2 Privada 321
12.2 FUNCIONAMIENTO DE VOIP 322
12.2.1 Codecs 323
12.2.2 Transporte y Control de la transmisión 324
12.2.3 Señalización 324
12.2.4 Direccionamiento 325
12.2.5 QoS (*Quality of Service* o Calidad del Servicio) 326
12.3 ELEMENTOS VOIP 327
12.3.1 Redes de telefonía cableadas 327
12.3.2 Redes de telefonía inalámbricas 330

12.3.3 ATA (*Analog Telephone Adaptor* o Adaptador Telefónico Analógico) 331
12.3.4 Gateways o Pasarelas VoIP 332
12.3.5 Terminales 333
12.3.6 PBX 334
12.4 CONFIGURACION DE UN PBX 335
12.4.1 Configuración de 3CX en Microsoft Windows 335
12.4.2 Configuración de Asterisk con FreePBX en GNU/Linux 338
12.5 CONFIGURACIÓN DE UN CLIENTE VOIP 343
12.5.1 Configuración en Microsoft Windows 343
12.5.2 Configuración de un cliente en GNU/Linux 345
RESUMEN DEL CAPÍTULO 348
EJERCICIOS PROPUESTOS 349
TEST DE CONOCIMIENTOS 349
MATERIAL ADICIONAL 351
ÍNDICE ALFABÉTICO 353

Introducción

Internet es una Red que está enfocada al intercambio de información entre usuarios y equipos. Actualmente, la información disponible en los distintos ordenadores y servidores de Internet es enorme: en 2006, la corporación EMC estimó en 161 mil millones de gigabytes, lo que equivale a 3 millones de veces la cantidad total de libros escritos en toda la historia de la humanidad. Es evidente que esta ingente cantidad de información debe estar convenientemente organizada y estructurada para que sea accesible. Gracias al uso de los navegadores y los buscadores de Internet, la información se encuentra mayoritariamente estructurada en páginas de hipertexto con enlaces, imágenes, vídeos, etc., en lo que se conoce como la *Word Wide Web* (Tela de Araña Mundial).

Existen multitud de aplicaciones que los usuarios demandan para su trabajo y entretenimiento. En general, todas ellas se basan en transferencia de información, aunque se distinguen por su formato o los tipos de datos que manejan. Algunos de los servicios más importantes que incluye Internet son los siguientes:

- ✓ Transferencia de archivos.
- ✓ Correo electrónico.
- ✓ Mensajería instantánea.
- ✓ Conexión remota a equipos.
- ✓ Acceso a información de hipertexto.
- ✓ Transferencia de audio y vídeo.

La gran mayoría de los servicios ofrecidos por una red de comunicación de ordenadores se basan en el funcionamiento en modo **cliente-servidor**. Éste consiste en que el servicio podrá ser proporcionado si existe en la red, al menos, un equipo que funcione como **servidor** y que se encargue de atender las peticiones recibidas. Por su parte, el resto de equipos de la red se comportarán como **clientes**, enviando las peticiones a los servidores para que las atiendan.

En una red de comunicación, el servicio más importante que debe ofrecerse es el intercambio de información entre equipos. Sin embargo, para que este servicio pueda funcionar con todas las garantías, puede ser necesario que tengan que existir otros servicios complementarios que aporten las funciones necesarias.

La mayoría de los servicios ofrecidos en una red de comunicación se basan en el mecanismo de interacción cliente-servidor. Según este modelo, existen una serie de equipos, llamados *clientes*, que son habitualmente manejados por los usuarios, que solicitan una serie de servicios para completar sus tareas. Por otro lado, en la red también deben existir otros equipos que sean capaces de ofrecer los servicios solicitados, conocidos como *servidores*. Entre los servicios que pueden solicitar los clientes para ser atendidos por los servidores, podemos encontrar el acceso a páginas web, impresión de documentos, descarga de archivos, transferencia de correo electrónico, etc.

Cuando un equipo quiere acceder a los servicios disponibles en un servidor remoto, primero tiene que enviar un mensaje de solicitud y dirigirlo al **puerto** asociado a ese servicio. El servidor deberá tener activo ese puerto para recibir la solicitud, procesarla y enviar los resultados. En este modelo, el cliente debe conocer cuál es el número de puerto que tiene asociado ese servicio en el servidor, normalmente porque se trata de un *puerto bien conocido*.

El concepto del modelo cliente-servidor es muy amplio y en el campo de la informática se puede aplicar tanto a programas que se ejecutan en un mismo equipo como a equipos conectados a través de la red. De igual forma, este modelo no restringe la función que desempeña cada equipo en la red, de forma que un equipo se puede comportar como cliente de unos determinados servicios a la vez que comportarse como servidor de otros. Por todo ello, el modelo

cliente-servidor funciona muy bien en redes de ordenadores donde los servicios se gestionan a través de servidores centralizados y donde pueden existir varios servidores que repartan el trabajo de diferentes tareas.

En general, las características que definen a un **equipo como cliente** son:

- ✓ Requiere de una potencia de cálculo menor, aunque esto dependerá de los programas que ejecute.
- ✓ Es utilizado por los usuarios para realizar su trabajo diario.
- ✓ Es el encargado de iniciar las peticiones o solicitudes.
- ✓ Recibe las respuestas de los servidores, obteniendo la información que ha solicitado o un mensaje de rechazo.
- ✓ Puede realizar peticiones de varios servicios a diferentes servidores.

Por su parte, las características que definen a un **equipo como servidor** son:

- ✓ Suele requerir una gran potencia de cálculo y memoria principal para poder atender todas las peticiones que recibe.
- ✓ Permanece a la espera de recibir peticiones.
- ✓ Cuando recibe una petición, la procesa y envían los resultados o un mensaje de rechazo.
- ✓ Suele aceptar un gran número de peticiones, aunque este valor puede limitarse.
- ✓ Es un equipo dedicado a atender peticiones y los usuarios no suelen trabajar con él directamente.

Entre las **ventajas** del uso del modelo cliente-servidor en los servicios de red, podemos destacar:

- ✓ Se establece un mayor control de la seguridad y el acceso a servicios autorizados, ya que éste se realiza a través de cada servidor.
- ✓ Puede aumentarse fácilmente la capacidad de los equipos o su número.
- ✓ Permite un mantenimiento más sencillo y una división de responsabilidades entre los administradores, ya que los cambios solamente se deben realizar en los servidores involucrados.

El modelo cliente-servidor también tiene sus **inconvenientes**. Los más importantes son:

- ✓ Sobrecarga de los servidores cuando existen muchas peticiones.
- ✓ El mal funcionamiento de un servidor hace que no estén disponibles los servicios que ofrece.
- ✓ Los servidores requieren de sistemas operativos y programas muy estables.

1 Asignación dinámica de direcciones

OBJETIVOS DEL CAPÍTULO

- ✓ Conocer el funcionamiento de los mecanismos automatizados de configuración de los parámetros de red e identificar las ventajas que proporcionan.
- ✓ Ilustrar los procedimientos y pautas que intervienen en una solicitud de configuración de los parámetros de red.
- ✓ Instalar un servicio de configuración dinámica de los parámetros de red.
- ✓ Preparar el servicio para asignar la configuración básica a los sistemas de una red local.
- ✓ Realizar asignaciones estáticas y dinámicas.
- ✓ Integrar en el servicio opciones adicionales de configuración.
- ✓ Verificar la correcta asignación de los parámetros de red.

El servicio más importante que debe ofrecer una red de comunicación es el intercambio de información entre equipos. Sin embargo, para que este servicio pueda funcionar con todas las garantías, puede ser necesario que tengan que existir otros servicios complementarios que aporten las funciones necesarias.

Este capítulo está dedicado a explicar un servicio que, si bien no es imprescindible para que una red de ordenadores funcione correctamente, sí que resulta muy adecuado para simplificar las tareas de configuración y administración. Este servicio, denominado **DHCP** (*Dynamic Host Configuration Protocol* o Protocolo de Configuración Dinámica de Direcciones), permite a los equipos obtener su configuración de red de forma automática. De esta forma, los administradores pueden ahorrarse mucho trabajo si tienen que configurar nuevos equipos o hacer cambios en los ya existentes.

Para que un usuario pueda realizar una comunicación en una red local o en Internet, primero necesita instalar en su equipo una serie de programas. Dichos programas contienen todos los pasos que se deben seguir para establecer las conexiones, realizar transferencia de información, controlar los errores, etc. Este conjunto de normas resulta muy importante, ya que sin ellos no estarán disponibles los servicios necesarios a bajo y alto nivel. En el caso que nos ocupa de conexión a Internet, el paquete que es necesario instalar se denomina **TCP/IP** (*Transmission Control Protocol / Internet Protocol* o Protocolo de Control de la Transmisión/Protocolo de Interred) y su especificación se encuentra perfectamente definida en documentos oficiales denominados RFC (*Request for Comments* o Petición de Comentarios), definidos desde el año 1983 por el **IAB** (*Internet Activities Board* o Comité de Arquitectura de Internet).

Además de instalar todos los protocolos de TCP/IP, también es necesario configurar correctamente sus parámetros más importantes, como son la dirección IP, máscara de red, puerta de enlace predeterminada, direcciones IP de los servidores DNS, etc. Esta configuración se puede establecer de forma manual o bien se puede obtener de forma automática desde un servidor DHCP.

El funcionamiento del protocolo DHCP está basado en el documento RFC 1531 que siguen todos los fabricantes a la hora de realizar sus implementaciones. Esto permite que, en una red con equipos diferentes (diferentes sistemas operativos y diferentes versiones de los protocolos de comunicación), estos puedan utilizar el servicio DHCP sin que existan problemas de compatibilidad.

Cualquier equipo que necesite conectarse a la red e intercambiar información a través de ella, necesita disponer de una configuración correcta de TCP/IP. Sin embargo, esta configuración puede llegar a ser un poco complicada, sobre todo para aquellas personas que no están familiarizadas con los aspectos técnicos de la arquitectura TCP/IP. Este problema se agrava con el uso del formato de direcciones IP versión 6, ya que el crecimiento de Internet ha requerido de la ampliación del número de direcciones disponibles.

Para paliar este problema, en este apartado se explica cómo configurar uno o varios servidores de la red para que envíen información al resto de equipos de la red con la configuración de red que necesitan. De esta forma, los usuarios que trabajan en estos equipos pueden olvidarse de la configuración de red de sus equipos y dejar que los administradores gestionen esos servidores de configuración.

El protocolo DHCP establece una **configuración predeterminada** para el equipo que la solicita, es decir, una configuración que ha sido definida con antelación para la red o subred en la que están conectados los equipos. La utilización del protocolo IPv6 permite también otro mecanismo de **configuración automática**, en el que es el propio equipo el que decide qué dirección IP va a utilizar, en base a la información que puede obtener de la red a la que está conectado y asegurándose de que ningún otro equipo la va a utilizar. Aunque IPv6 todavía no se ha generalizado en Internet, se espera que estos dos tipos de configuraciones coexistan, e incluso se complementen, ya que IPv6 permite que un equipo pueda autoconfigurar su propia dirección a la vez que obtener el resto de los parámetros de red de un servidor DHCPv6.

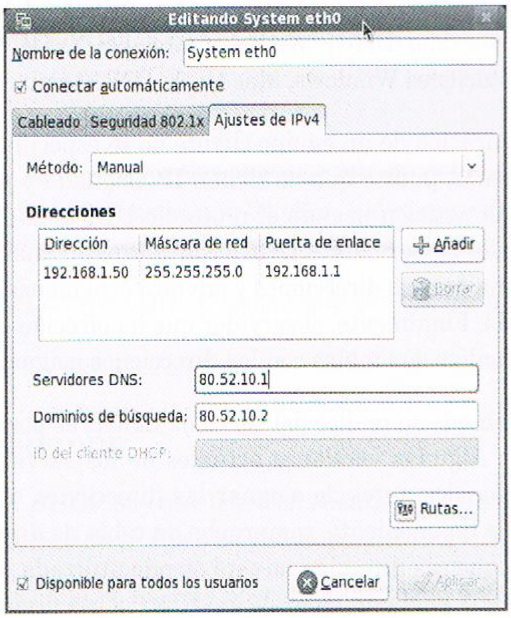


Figura 1.1. *Ventana de configuración de los parámetros de red en Linux Fedora 11. Aunque la configuración se puede realizar a través de ventanas con opciones y no es necesario tener conocimientos avanzados del sistema, los parámetros de la red son bastante complejos (dirección IP, máscara de red, etc.), sobre todo para usuarios que no tienen buenos conocimientos de informática*

1.1 FUNCIONAMIENTO DE DHCP

El protocolo **DHCP** permite que a los equipos de la red se les asigne una dirección IP automáticamente solo cuando la necesiten. DHCP apareció en la década de los noventa con el objetivo de mejorar el protocolo BOOTP que se utilizaba en máquinas Unix para asignar direcciones a ciertos dispositivos que trabajaban en pequeñas redes locales.

Dicho de esta forma, puede resultar un poco complejo describir cuál es la función del protocolo DHCP. Cualquier ordenador de esté conectado a Internet necesita una dirección IP que lo distinga del resto. Por lo tanto, deberá existir algún mecanismo que organice las direcciones y ponga de acuerdo a todo el mundo para que no exista ninguna dirección duplicada. Para ordenar este caos en Internet con cientos de millones de equipos conectados, existe una autoridad central que se encarga de asignar conjuntos de direcciones a organismos y empresas. A este grupo pertenecen las empresas proveedoras de acceso a Internet, que son las que asignan las direcciones a sus clientes. Para simplificar esta asignación, las empresas utilizan el protocolo DHCP, de forma que los usuarios finales obtienen una dirección de forma automática sin necesidad de realizar ninguna configuración en sus equipos. Por lo tanto, DHCP simplifica el trabajo de asignación de direcciones a los clientes que acceden a Internet.

DHCP puede utilizarse también dentro del ámbito de una red local y, en este caso, los ordenadores deben solicitar una dirección a una estación especial que funcione como **servidor DHCP**. Esta estación mantiene una tabla de direcciones asignadas y libres para esa red. La ventaja de este método consiste en que las estaciones solamente tienen asignadas IPs cuando realmente se conectan y hacen uso de la red y permanecen libres mientras no se necesitan, lo que ahorra direcciones que pueden asignarse a otras estaciones. Además, se reducen las tareas de los administradores de la red cuando hay que cambiar de lugar estaciones, ya que no tienen que volver a configurarlas.

El protocolo DHCP es *abierto* (no depende del sistema operativo utilizado), lo que significa que se puede utilizar sobre una red heterogénea. Así, un servidor DHCP Windows, Mac OS X, GNU/Linux, Novell, etc., puede asignar direcciones sin ningún problema a estaciones Windows, Mac OS X, GNU/Linux, etc.

Hay que recalcar que en la configuración de un equipo cliente no se especifica la dirección IP del servidor DHCP. El protocolo establece que las estaciones, puesto que no tienen IP asignada y no conocen direcciones de servidores ni máscaras de red, deben lanzar una petición usando el protocolo UDP a la dirección de difusión (la dirección de difusión IPv4 es 255.255.255.255). Todos los servidores DHCP contestan con una dirección IP, también por un mensaje UDP de difusión. El cliente tomará una de esas direcciones y enviará otro mensaje de difusión anunciando a todos los servidores DHCP cuál es la IP tomada. Finalmente, el servidor que ha ofrecido la dirección asignada envía al cliente la confirmación de la operación y actualiza sus tablas con las direcciones asignadas y libres.

Dependiendo de la implementación que se realice del servidor DHCP, es posible que su comportamiento sea algo diferente de unas versiones a otras. Algunas versiones actuales de los servidores DHCP disponibles para GNU/Linux realizan comprobaciones adicionales antes de asignar las direcciones a los clientes. En estos casos, cuando un servidor DHCP recibe una petición de un cliente, comprueba su tabla de direcciones libres (dentro del rango que puede asignar) y, para asegurarse de que esa dirección no está siendo utilizada por ningún otro equipo en la red (que haya sido configurado de forma manual), envía un mensaje *eco ICMP* a esa dirección. Si un equipo contesta, significa que esa dirección ha sido asignada de forma manual (estática) y la marca como "abandonada" para no asignarla a ningún cliente. Si no contesta ningún equipo, entonces asigna esa dirección. En caso de que no existan direcciones libres a asignar dentro del rango, el servidor vuelve a comprobar con mensajes *eco ICMP* si alguna de las direcciones abandonadas está libre.

Un mensaje **eco ICMP** se utiliza para comprobar si un equipo está conectado a la red y funciona. Si ese equipo devuelve un mensaje de respuesta, entonces sabemos que está perfectamente operativo. En caso contrario, el equipo no existe, está apagado o tiene algún problema con la red.

Es posible que exista más de un servidor DHCP en la misma red y, para que no se produzcan conflictos, cada uno de ellos debe asignar un rango de direcciones distinto. Por ejemplo, un servidor podría asignar las direcciones en el rango 192.168.0.1-192.168.0.127 y el otro las direcciones del rango 192.168.0.128-192.168.0.254.

Cuando un cliente no es capaz de conectar con un servidor DHCP para obtener su dirección IPv4, entonces utiliza la asignación **APIPA** (*Automatic Private IP Addressing* o Direccionamiento IP Privado Automático), que consiste en la utilización de las direcciones IP de la red 169.254.0.0/16. Existen algunos sistemas operativos que incluyen la posibilidad de establecer una configuración IP estática para que sea utilizada por el equipo en caso de que falle la asignación por DHCP, lo que puede resultar muy útil cuando se dispone de un equipo portátil que se usa en diferentes redes. Si un equipo quiere obtener su dirección IPv6 y no lo consigue a través de un servidor DHCPv6, entonces realiza un proceso de *autoconfiguración* (como se explica en la introducción de este capítulo) de forma análoga a como funciona APIPA, pero estableciendo su dirección de acuerdo con la información disponible y los mensajes que envían los encaminadores por la red.

Hay que tener en cuenta que los encaminadores (*routers*) filtran por defecto el tráfico generado por el protocolo DHCP, por lo que inicialmente no es posible que un servidor DHCP asigne direcciones a equipos que se encuentran al otro lado de un encaminador. Para conseguir esto, el encaminador debe soportar el reenvío de tráfico DHCP definido en RFC 1542 y hay que configurarlo para que permita el paso de mensajes de difusión DHCP de un lado a otro.

1.2 PARÁMETROS DE CONFIGURACIÓN DE DHCP

Antes de pasar a explicar cómo se configura un servidor y un cliente del protocolo DHCP, es necesario identificar cuáles son los parámetros de configuración de cada uno de ellos. Salvo contadas excepciones, estos parámetros son comunes a los diferentes sistemas operativos explicados en este libro.

Los parámetros fundamentales del servicio DHCP tienen que ver con los parámetros de la red de comunicación sobre la que van a funcionar.

1.2.1 PARÁMETROS EN EL SERVIDOR

En la configuración de un servidor DHCP hay que tener en cuenta que éste no puede asignarse direcciones IP a sí mismo (por lo que deberá tener una dirección IP fija o asignada por otro servidor DHCP).

Otra cuestión a tener en cuenta es que el sistema operativo instalado en el servidor DHCP debe tener soporte para enviar paquetes de difusión (recuérdese que el protocolo DHCP utiliza paquetes de difusión para asignar las direcciones). Todas las versiones de los sistemas operativos actuales tienen soporte nativo de esta característica.

Para que los mensajes sean enviados correctamente a través de las direcciones de difusión, es necesario que el equipo tenga también una entrada en su tabla de encaminamiento que especifique cuál es la dirección para difusión en la red (que es la IP 255.255.255.255 donde se envían las peticiones DHCP). Esta comprobación depende del sistema operativo utilizado y se explica en el apartado 1.3.

Cuando se ha comprobado que todo lo anterior está configurado correctamente, lo que hay que hacer es instalar el programa que contiene todos los archivos necesarios del proceso servidor DHCP. Este programa, que puede variar dependiendo del sistema operativo utilizado, se instala siguiendo los pasos expuestos en el apartado 1.3.

Un servidor DHCP debe incluir, en su información de configuración, los parámetros indicados en la tabla 1.1. Algunos de estos parámetros son obligatorios (como la dirección de la red o subred y la máscara), mientras que otros no lo son porque dependen de las opciones que queramos establecer y de la configuración de la red (por ejemplo, las direcciones de las subredes o las direcciones que deben asignarse siempre a los mismos equipos).

Tabla 1.1. Parámetros de un servidor DHCP

Parámetros de configuración de un servidor DHCP
Dirección IP de la red.
Máscara de red.
Direcciones IP de las subredes.
Máscaras de subred.
Puerta de enlace o pasarela predereminada (en la red o subredes).
Direcciones IP de los servidores DNS.
Nombre del dominio de la red o subredes.
Dirección de difusión de la red o subredes.
Rango de direcciones a asignar a los clientes.
Dirección IP, MAC y nombre de los equipos que tendrán siempre las mismas direcciones.

1.2.2 PARÁMETROS EN EL CLIENTE

Los parámetros necesarios para que un cliente obtenga su configuración de red son mínimos, de forma que la mayoría de ellos no tengan que ser especificados de forma manual. Precisamente por esta razón, DHCP funciona por mensajes de difusión, lo que evita tener que especificar direcciones de servidores que pueden cambiar con el tiempo.

Para que un equipo cliente pueda enviar y recibir mensajes de difusión de la red, necesita que el sistema operativo esté preparado para ello. Esta cuestión se explica en el apartado 1.4 relativo a la configuración de los equipos cliente.

1.3 CONFIGURACIÓN DE UN SERVIDOR DHCP

Evidentemente, la configuración de un servidor DHCP resulta enormemente más compleja que la de un equipo cliente por la gran cantidad de parámetros de la red que es necesario especificar, además de la utilización de técnicas complejas para poner en marcha el servicio en el ámbito del sistema operativo. Mientras que un servidor solamente podrá ser configurado por un experto que haya dedicado mucho tiempo de estudio y entrenamiento, un cliente DHCP puede ser configurado por un usuario con conocimientos de informática a nivel general. Sin embargo, para que ese usuario sin conocimientos específicos pueda configurar fácilmente su equipo, necesita que ya exista un servidor DHCP plenamente operativo.

Para evitar que los usuarios corrientes tengan que emplearse a fondo en instalar, configurar y mantener un servidor DHCP en su red doméstica, muchos fabricantes optan por incluir este servicio en muchos de sus dispositivos de interconexión de red. Así, un encaminador corriente de acceso a Internet (xDSL, Cable, etc.) puede incluir también las rutinas necesarias para funcionar como servidor DHCP en la red que conecta. Si éste además incluye ventanas de configuración amigables y con parámetros típicos y válidos para la mayoría de las redes domésticas, entonces se puede conseguir que los usuarios gestionen sus redes domésticas sin que sea necesario un entrenamiento previo.

Sin embargo, cuando las redes a administrar crecen en tamaño dentro del ámbito de medianas y grandes empresas, un simple servidor DHCP de un encaminador puede no ser suficiente para cubrir las necesidades. En ese caso, puede ser necesario utilizar ordenadores dedicados o incluir servicios DHCP en equipos servidores que realizan además otras tareas. En los apartados siguientes se explica paso a paso cómo realizar la configuración de un servidor DHCP en distintas versiones de Microsoft Windows y GNU/Linux.

1.3.1 CONFIGURACIÓN EN MICROSOFT WINDOWS

Para que un equipo con Microsoft Windows funcione como servidor DHCP, necesita de un programa que se encuentre en ejecución durante todo el tiempo (proceso demonio) y que atienda las peticiones que se reciben a través de la red. Este programa se puede obtener directamente de Microsoft, que lo incluye en algunas versiones de sus sistemas operativos o se puede obtener de otros fabricantes, ya sea con licencia libre o propietaria.

Microsoft distribuye un paquete de servidor DHCP en todas sus versiones de Windows Server, lo que permite a estos equipos configurar los clientes en la red. En otras versiones de Windows orientadas más a equipos que van a funcionar como estaciones de trabajo, como Windows XP/Vista/7, Microsoft no ofrece paquetes de servidor, aunque se pueden instalar herramientas como el Pack de Herramientas de Administración del Servidor (*ADMINPACK.MSI*) para Windows 2000/XP o las Herramientas de Administración Remota del Servidor para Windows 7, que permiten gestionar un servidor DHCP desde un equipo cliente. Si se desea configurar Windows 2000/XP/Vista/7 como servidor DHCP, se pueden instalar paquetes de otros fabricantes que permiten esta funcionalidad.

EJEMPLO 1.1

Veamos los pasos a seguir para configurar un equipo con Windows Server 2008 como servidor DHCP de una red que tiene la dirección 192.168.1.0/24:

1. Acceder a la herramienta de administración del servidor desde "Inicio || Herramientas administrativas || Administración del servidor". En el árbol de iconos de la izquierda, seleccionar "Administrador del servidor || Funciones". Aquí se muestra una ventana con todas las funciones instaladas en el servidor.
2. Pulsar en el enlace "Agregar funciones", lo que iniciará la ventana del asistente para añadir nuevas funciones a nuestro servidor. En ese momento, aparecerá la primera ventana del asistente donde se informa que es recomendable comprobar primero si el equipo tiene una configuración correcta. Hay que pulsar en el botón "Siguiente".
3. En la siguiente ventana del asistente se muestra la lista con las funciones que pueden añadirse al servidor. En ella, tenemos que activar la casilla de verificación "Servidor DHCP". En caso de que el equipo tenga asignada una dirección IP por DHCP, entonces se mostrará un mensaje advirtiendo de que esta situación no es recomendable, ya que lo mejor es que se le asigne una dirección estática. A continuación, se pulsa en el botón "Siguiente".
4. La siguiente ventana muestra algunos detalles introductorios sobre el funcionamiento del servidor DHCP en Windows Server 2008. De nuevo, pulsamos el botón "Siguiente".
5. A continuación, se especifica la configuración IPv4 del servidor DHCP, donde se puede establecer el nombre del dominio y las direcciones IPv4 de los servidores DNS (si es que queremos que nuestro servidor DHCP facilite esta información a los clientes). De nuevo, pulsamos el botón "Siguiente".
6. La siguiente ventana que aparece especifica si nuestro servidor DHCP va a enviar también a los clientes las direcciones de los servidores WINS, que se encargan de resolver direcciones NetBIOS que son utilizadas en la red Microsoft. Esta opción solamente hay que activarla en caso de que nuestra red tenga servidores WINS instalados. Como siempre, pulsamos el botón "Siguiente" para continuar con el asistente.
7. En la siguiente ventana se especifican los ámbitos, es decir, los rangos de direcciones IPv4 que el servidor DHCP puede asignar a los clientes. Para ello, se pulsa el botón "Agregar", lo que mostrará una ventana de creación de un nuevo ámbito (véase la Figura 1.2).
8. Una vez definido el ámbito de nuestro servidor, pulsamos el botón "Siguiente", lo que nos mostrará una ventana para configurar IPv6. Tenemos dos opciones:
   - **Habilitar el modo sin estado DHCPv6 para este servidor**: en este modo, el servidor DHCP también envía a los clientes que lo soliciten una configuración IPv6 *predeterminada*. Para ello, el servidor DHCP debe ser configurado siguiendo los mismos pasos anteriores, pero esta vez especificando direcciones IPv6.
   - **Deshabilitar el modo sin estado DHCPv6 para este servidor**: el servidor DHCP no va a enviar configuración IPv6 a los clientes. Todos aquellos clientes que deseen obtener esta configuración, deberán hacerlo mediante el modo *automático*.
9. Una vez establecida la configuración IPv6, la siguiente ventana nos muestra un resumen de la configuración del servidor DHCP que hemos establecido. Pulsando en el botón "Instalar" se realizará todo lo necesario para que el servicio DHCP comience a funcionar en el equipo con la configuración que hemos definido. Si todo funciona como está previsto, deberá aparecer una ventana con el mensaje "Instalación correcta", por lo que podremos pulsar en el botón "Cerrar" para finalizar el asistente. De vuelta a la ventana de administración del equipo, en la ventana "Funciones" deberá aparecer ahora "Servidor DHCP".

10. Podemos acceder a la configuración del servidor DHCP que acabamos de crear si seleccionamos "Inicio || Herramientas administrativas || DHCP". Desde esta herramienta (Figura 1.3) se puede iniciar o detener el servicio y realizar cambios en la configuración inicial definida en el asistente. También podemos realizar reservas de direcciones (para que determinados equipos tengan siempre asignadas las mismas direcciones), si seleccionamos "Reservas" en la lista de la parte izquierda y pulsamos en la opción del menú principal "Acción || Reserva nueva...". Los parámetros que hay que especificar para realizar una reserva de dirección a un equipo concreto son:
    - **Nombre de la reserva** (para identificarla).
    - **Dirección IP** (la dirección IP que se reserva a un equipo concreto).
    - **Dirección MAC** (la dirección MAC del equipo al que se le va a realizar la reserva).
    - **Descripción** (un texto que nos ayude a informar la causa de la reserva).
    - **Tipos compatibles** (protocolo utilizado para realizar la asignación).

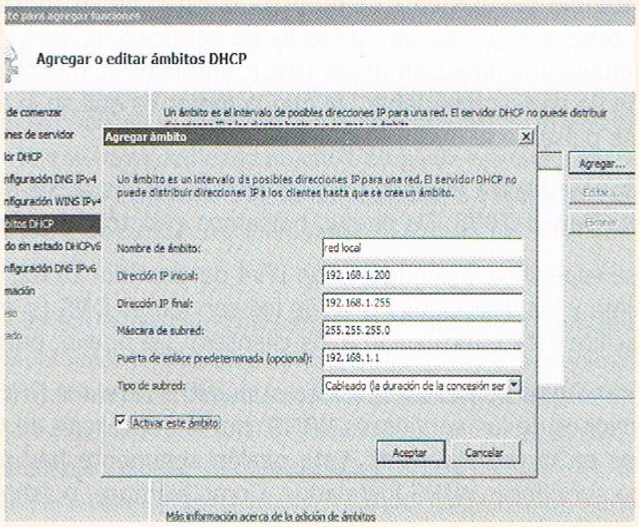


Figura 1.2. Ventana de especificación del ámbito en el asistente de creación del servidor DHCP de Windows Server 2008. Aquí se especifican los rangos de direcciones IPv4 que el servidor DHCP puede asignar a los clientes

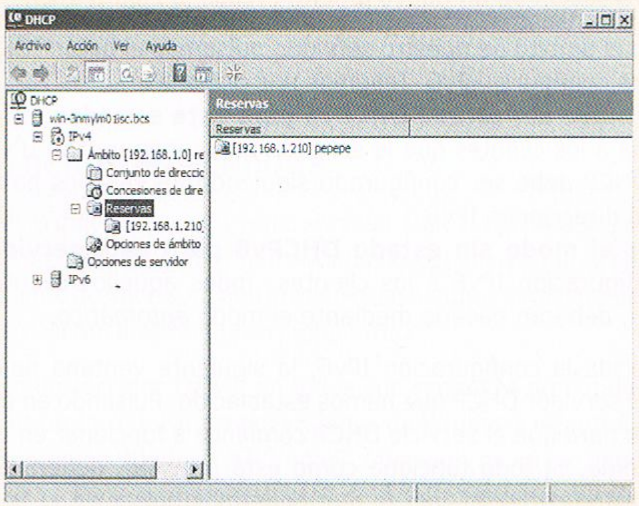


Figura 1.3. Ventana principal de gestión del servidor DHCP en Windows Server 2008. Desde esta ventana se puede controlar el funcionamiento del servicio, iniciándolo, deteniéndolo o cambiando su configuración

EJEMPLO 1.2

Veamos los pasos a seguir para configurar un equipo como servidor DHCP con Windows 7. El paquete utilizado se llama Dual DHCP DNS Server (versión 6.50) que se distribuye bajo licencia GPL.

1. En primer lugar hay que descargar e instalar el paquete Dual DHCP DNS Server en el equipo.
2. Una vez instalado el programa, éste se inicia automáticamente en el sistema como un proceso demonio, utilizando la configuración que incluye por defecto. Se puede comprobar que este proceso está en ejecución si se pulsa la combinación de teclas CTRL + ALT + SUPR, se selecciona "Iniciar el administrador de tareas", se accede a la pestaña "Procesos" y se pulsa el botón "Mostrar procesos de todos los usuarios". El proceso se llama "DUALServer".
3. En el menú de inicio de Windows 7 se crean todos los accesos directos a este programa (véase la Figura 1.4).
4. La configuración por defecto del servidor DHCP utiliza el rango de direcciones 192.168.0.1/24-192.168.0.254/24. Para cambiar esta configuración por defecto hay que seleccionar la opción del menú de inicio de Windows 7 "Todos los programas || Dual Server || Configure". Esto mostrará una ventana del programa "Editor de Textos" que abre el archivo de configuración de este servicio, que se llama *DualServer.INI* y debe estar ubicado en la misma ruta que el proceso *DualServer.EXE*.
5. La configuración de Dual Server 6.50 se almacena en un archivo de texto sin formato que está estructurado en secciones, cada una de las cuales contiene un título entre corchetes. En la sección "[SERVICES]" se especifica el servicio que se encuentra activo (si no se ha indicado ninguno se activan por defecto los servicios DHCP y DNS). Por otra parte, en "[LISTEN-ON]" se especifican las direcciones de los adaptadores de red desde donde se van a recibir las peticiones de los clientes (si no se especifica ninguna, se asumen todos los adaptadores de red que tengan direcciones estáticas asignadas manualmente).
6. La configuración del servidor DHCP se encuentra en las secciones "[DHCP-RANGE]", que especifica el rango de direcciones a asignar y "[DHCP-OPTIONS]", que contiene las opciones globales de configuración de este servicio. Los parámetros más importantes de la sección "[DHCP-RANGE]" son:
   - **DHCP_Range**: rango de direcciones a asignar.
   - **Subset_Mask**: máscara de red.
   - **DNS_Server**: dirección de un servidor DNS.
   - **Router**: dirección de la puerta de enlace o pasarela por defecto.
   - **Lease_Time**: tiempo en el que la dirección permanece asignada.
   - **Filter_Mac_Range**: rango de direcciones MAC de los equipos a los que no se les asigna la configuración de red aunque la soliciten.
7. Por su parte, algunos parámetros destacados de la sección "[DHCP-OPTIONS]", además de *Subset_Mask*, *DNS_Server*, *Router* y *Lease_Time*, pueden ser:
   - **Time_Server**: servidor de hora (protocolo NTP).
   - **Name_Server**: servidor de nombres (véase el capítulo 2).
   - **LPR_Server**: servidor de impresoras LPR.
   - **Broadcast_Address**: dirección de difusión de la red.
   - **SMTP_Server**: servidor de correo electrónico.

8. Una vez modificados los parámetros anteriores, de acuerdo con la configuración de red, es necesario detener el servicio Dual Server y volver a iniciarlo para que los cambios tengan efecto. Para ello, hay que pulsar la combinación de teclas CTRL + ALT + SUPR, seleccionar "Iniciar el administrador de tareas", acceder a la pestaña "Servicios" y pulsar con el botón derecho del ratón sobre el proceso "DUALServer". Para detenerlo se usa la opción del menú contextual "Detener servicio", mientras que para volver a iniciarlo se usa "Iniciar servicio".
9. Se puede obtener una lista actualizada con las direcciones asignadas a los clientes si se selecciona la opción del menú de inicio de Windows 7 "Todos los programas || Dual Server || View Lease Status" (Figura 1.5).

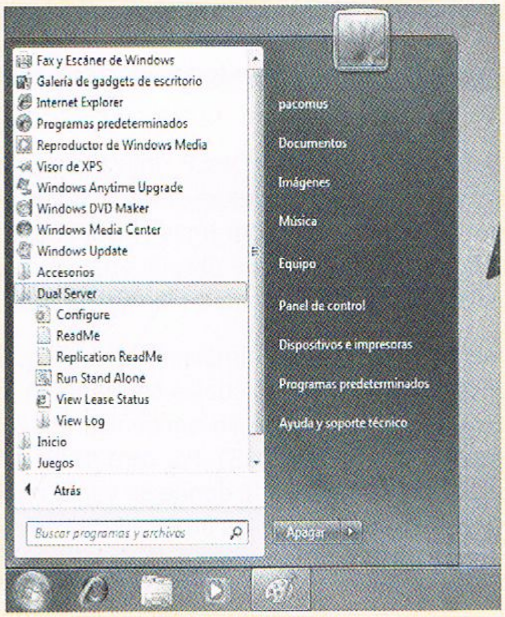


Figura 1.4. *Opciones disponibles del programa Dual DHCP DNS Server una vez instalado en Windows 7. Las opciones más utilizadas son "Configure" para configurar los parámetros del servidor y "View Lease Status" para mostrar la lista de direcciones asignadas a los clientes*

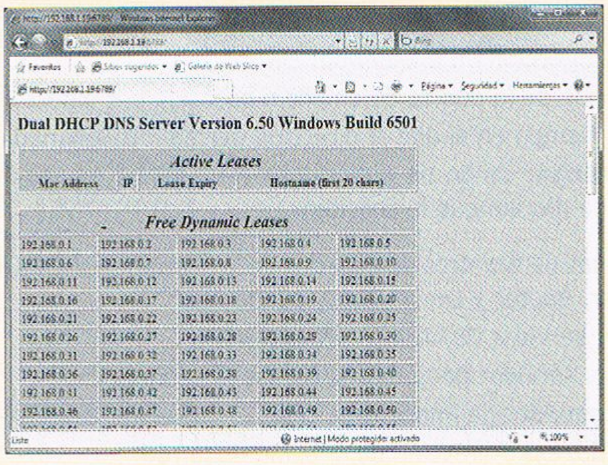


Figura 1.5. *Ventana de consulta de direcciones asignadas en el servidor DHCP Dual Server 6.50. Aquí se muestran las direcciones asignadas y libres a los equipos de la red*

1.3.2 CONFIGURACIÓN EN GNU/LINUX

La instalación y configuración de un servidor DHCP en GNU/Linux resulta bastante sencilla, sobre todo si la distribución utilizada ofrece herramientas gráficas para realizar estas tareas.

Es necesario que el núcleo de Linux que utilicemos tenga soporte para enviar paquetes de difusión (recuérdese que el protocolo DHCP utiliza paquetes de difusión para asignar las direcciones). Para comprobar si el núcleo soporta el envío de paquetes de difusión hay que ejecutar como *root* la orden *ifconfig eth0* (*eth0* es el adaptador de red que va a recibir las solicitudes DHCP) y comprobar que en la salida aparece la palabra "MULTICAST". En caso negativo, hay que utilizar otro núcleo o compilar uno con la opción "IP Multicasting" activada. Normalmente, todos los núcleos modernos de Linux están compilados para soportar esta característica.

Para que los mensajes sean enviados correctamente a través de las direcciones de difusión, es necesario que el equipo tenga también una entrada en su tabla de encaminamiento que especifique cuál es la dirección para difusión en la red (que es la IPv4 255.255.255.255 donde se envían las peticiones DHCP). Para comprobarlo, se utiliza la orden *route* sin argumentos (véase la referencia de órdenes incluida con este libro). En caso de que ya exista, deberá aparecer una entrada con la dirección 255.255.255.255 dentro de la columna "Destination". Si no aparece, hay que incluirla con la siguiente orden, que debe ser ejecutada con la cuenta de usuario *root*:

```
root@linux:~# route add -host 255.255.255.255 /dev/eth0
```

Si la orden anterior devuelve algún error, entonces hay que editar el archivo */etc/hosts*, incluir en él la línea *255.255.255.255 all-ones* (respetando los tabuladores de las líneas que ya aparecen) y ejecutar como *root* la orden:

```
root@linux:~# route add -host all -ones /dev/eth0
```

Cuando se ha comprobado que todo lo anterior está configurado correctamente, lo que hay que hacer es instalar el paquete que contiene todos los archivos necesarios del proceso servidor DHCP. Este paquete, que puede variar dependiendo de la distribución o versión de Linux, suele tener por nombre "dhcpd" o "dhcp-server" (el nombre que contenga solo "dhcp" nos puede indicar que se trata del paquete que contiene el cliente DHCP). En este apartado nos centraremos en la instalación y configuración del paquete DHCP que distribuye el ISC (*Internet Systems Consotium*) con licencia GPL y que está disponible en la mayoría de distribuciones de Linux. Siempre es recomendable instalar la última versión del paquete disponible, ya que así nos aseguramos de que se han corregido problemas y vulnerabilidades de versiones anteriores.

El servidor DHCP de Linux consta de dos partes:

- **Proceso demonio**: permanece en ejecución y atiende las peticiones que le llegan a través de la red por el puerto 547. Este proceso suele llamarse **dhcpd** o **dhcp-server** y puede ser iniciado automáticamente en la instalación del paquete, a través de una orden o configurando los niveles de ejecución del sistema.
- **Archivos de configuración**: guardan los parámetros con la información de la red y los datos que debe enviar a los clientes. El archivo más importante para la configuración de este servicio se llama *dhcpd.conf* y se explica con detalle en el apartado 1.3.2.2.

1.3.2.1 Ejemplos de configuraciones

Este apartado está dedicado a exponer algunos ejemplos de instalación y configuración de un servidor DHCP en diferentes distribuciones de Linux. Al igual que ocurre en la instalación y configuración de otros paquetes y servicios, el paquete del servidor DHCP requiere los mismos pasos y los mismos parámetros, aunque algunos de ellos pueden variar ligeramente.

EJEMPLO 1.3

Veamos cómo se instala y configura el servidor DHCP ISC sobre Linux Debian 5. El primer paso a seguir consiste en instalar el paquete *dhcp3-server* (versión 3) que se incluye con esta distribución, usando la herramienta correspondiente. También se puede hacer con la siguiente orden ejecutada con el usuario *root*:

```
root@linux:~# apt-get install dhcp3-server
```

Lo anterior instala, configura e intenta iniciar el servidor DHCP sin la necesidad de paquetes adicionales. Esta versión indica en la instalación que ha sido configurada como "no autoritaria" por defecto. Esto quiere decir que si un cliente pide una dirección que el servidor no conoce porque es incorrecta o pertenece a otra red o subred, no enviará un mensaje de tipo *DHCPNACK* (que indica al cliente que no le puede suministrar la configuración de red). Es posible cambiar este comportamiento por defecto si se indican explícitamente en el archivo *dhcpd.conf* las subredes sobre las que el servidor tiene autoridad mediante la sentencia "*autoritative*" (véase el apartado 1.3.2.2).

La instalación del paquete *dhcp3-server* en Debian ubica el archivo *dhcpd.conf* en la carpeta */etc/dhcp*. Por su parte, los mensajes de error y diagnóstico del proceso demonio del servidor DHCP se guardan en el archivo de registro del sistema */var/log/syslog*. Examinar este archivo puede ayudar a resolver problemas de funcionamiento (véase el apartado 1.5). De hecho, cuando se instala el paquete, el sistema intenta iniciar el proceso demonio, pero normalmente no podrá hacerlo porque la configuración que está grabada por defecto en el archivo *dhcpd.conf* no está adaptada a los parámetros de la red actual.

La configuración del servidor DHCP se puede realizar directamente modificando el archivo *dhcpd.conf*, según lo indicado en el apartado 1.3.2.2. También se puede instalar el paquete *gdhcpd* para configurar el servidor DHCP en el entorno gráfico, aunque la versión incluida con Debian 5 (0.4.4) está en inglés. Este paquete instala un acceso directo al programa en el menú principal del entorno gráfico que se llama "Gdhcpd" o "Gadmin-dhcpd". La Figura 1.6 muestra la ventana principal de este programa.

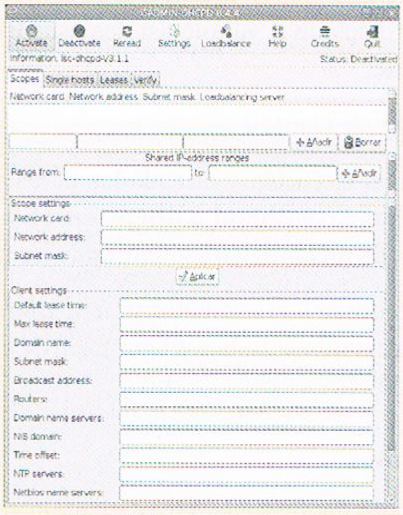


Figura 1.6. *Ventana principal del programa Gdhcpd en Debian. Este programa permite configurar los parámetros del servidor DHCP, de la misma forma que se puede hacer directamente sobre el archivo /etc/dhcp3/dhcpd.conf. La página "Scopes" muestra la configuración general del servidor DHCP (rangos de direcciones a asignar y configuración de red de cada equipo). La página "Single hosts" se utiliza para reservar direcciones a equipos individuales. La página "Leases" muestra las direcciones asignadas por el servidor en ese momento*

Para iniciar el servidor DHCP se puede utilizar un programa de gestión de servicios que permita modificar los niveles de ejecución del sistema. También se puede usar una de estas órdenes del intérprete que deben ser ejecutadas como *root*:

```
root@linux:~# /etc/init.d/dhcp3-server start
root@linux:~# dhcpd3 &
```

La orden *dhcp3-server* también acepta otros argumentos: *stop* (para el servidor), *restart* (lo vuelve a reiniciar, en caso de que se hayan hecho modificaciones en el archivo *dhcpd.conf*) y *status* (para mostrar el estado actual).

EJEMPLO 1.4

Veamos cómo se instala y configura el servidor DHCP ISC sobre Linux OpenSUSE 11.1. El primer paso a seguir consiste en instalar los paquetes *dhcp-server* (versión 3.1.1), *yast2-dhcp-server* (módulo para configurar el servidor DHCP en YaST) y *yast2-dns-server* (dependiente del paquete anterior), que se incluyen con esta distribución, usando la herramienta correspondiente.

La configuración del servidor DHCP en OpenSUSE se puede realizar de dos formas:

- Utilizando el archivo de configuración *dhcpd.conf*, que se encuentra ubicado en la carpeta */etc/dhcp* (véase el apartado 1.3.2.2).
- Utilizando el *centro de control de YaST*, en la opción "Servicios de red || Servidor DHCP" lo que muestra una ventana como la de la Figura 1.7.

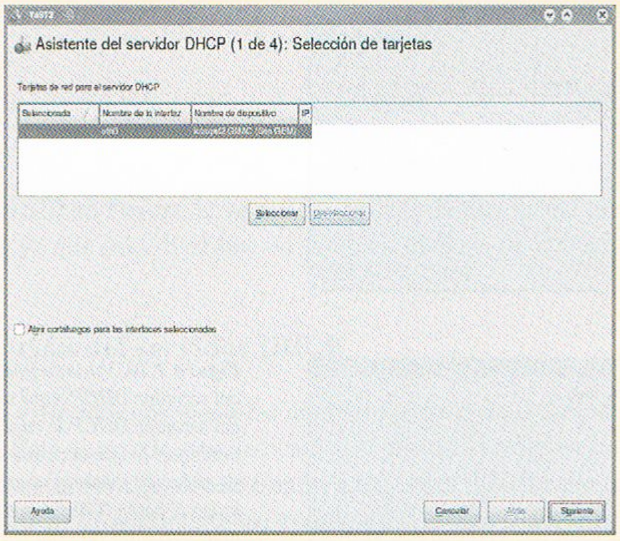


Figura 1.7. *Ventana principal del asistente de YaST para configurar el servidor DHCP. En esta ventana se selecciona el adaptador de red del equipo que va a recibir las peticiones DHCP de los clientes y las va a responder. También se utiliza para configurar el cortafuegos del sistema de forma que éste no bloquee el tráfico a través del puerto por defecto que usa el servidor DHCP*

Cuando se pincha en el adaptador de red y se pulsa en los botones "Seleccionar" y "Siguiente", puede aparecer el mensaje "El puerto en el cortafuegos no está abierto y el servidor DHCP no podrá servir a la red. ¿Desea continuar?", lo que indica que hay que marcar la casilla de verificación "Abrir cortafuegos para las interfaces seleccionadas".

En las Figuras 1.8, 1.9, 1.10 y 1.11 se muestran los pasos siguientes de configuración del servidor DHCP en YaST. Si no se establecen parámetros globales de la red, el asistente tomará los asignados actualmente al equipo.

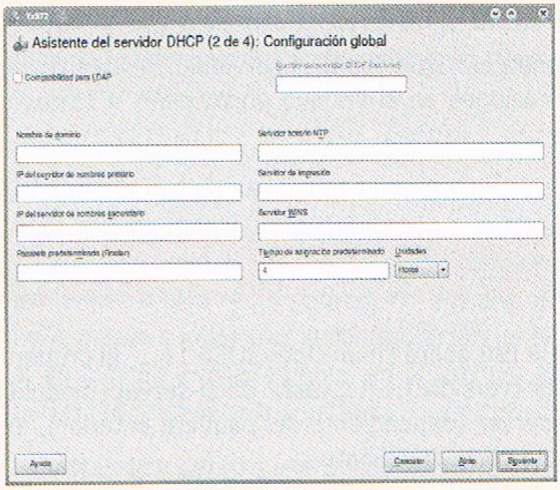


Figura 1.8. *Configuración de los parámetros globales del servidor DHCP. Aquí se indican los parámetros de la configuración de red que van a ser enviados a los clientes del servicio*

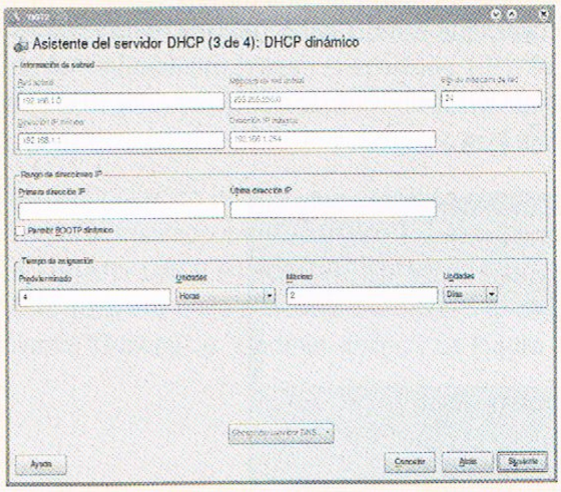


Figura 1.9. *Configuración de los rangos de direcciones a asignar por el servidor DHCP. Además de estos rangos, se puede configurar el tiempo en el que se mantienen asignadas las direcciones. Una vez pasado este tiempo, las direcciones se renuevan para los equipos que todavía están conectados*

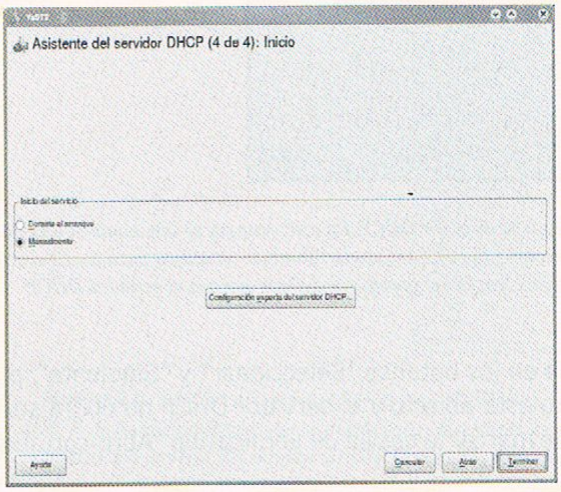


Figura 1.10. *Ventana final del asistente de configuración del servidor DHCP. Aquí se indica si el proceso demonio del servidor DHCP se va a iniciar automáticamente en el arranque, lo que hace que se configure en el editor de niveles de ejecución (véase el apartado 1.4.2 del capítulo 1). Si se pulsa el botón "Configuración experta del servidor DHCP...", aparecerá una ventana para consultar todas las opciones de configuración que se han indicado en el asistente, además de permitir editar directamente el archivo dhcpd.conf (véase el apartado 1.3.2.2)*

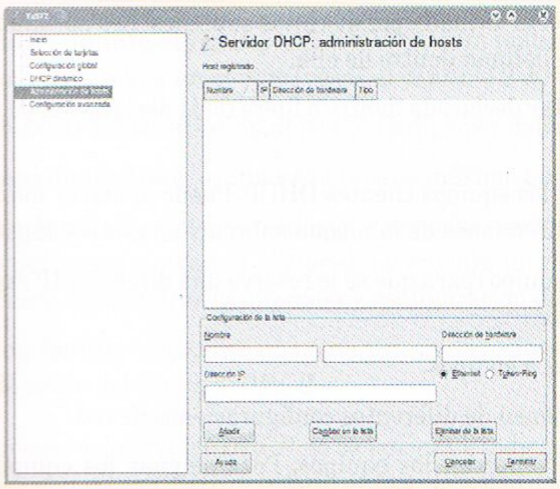


Figura 1.11. *Ventana de asignación de direcciones fijas a equipos. Esta ventana es accesible desde la ventana final del asistente (Figura 1.10) pulsando en el botón "Configuración experta del servidor DHCP..." y después en la página "Administración de hosts". En la página "Configuración avanzada" se puede realizar toda la configuración del servidor DHCP, pero en una sola ventana*

Para iniciar el servidor DHCP se puede utilizar la herramienta de gestión de los niveles de ejecución del sistema que incluye YaST. También se puede usar la siguiente orden que hay que ejecutar con los privilegios del usuario *root*:

```
root@linux:~# /etc/init.d/dhcpd start
```

Esta orden también acepta otros argumentos: *stop* (para el servidor), *restart* (lo vuelve a reiniciar en caso de que se hayan hecho modificaciones en el archivo *dhcpd.conf*) y *status* (para comprobar su estado).También se puede usar la siguiente orden para iniciar el demonio del servidor DHCP:

```
root@linux:~# dhcpd &
```

La configuración del servidor DHCP en Fedora 11 se puede realizar de una forma muy parecida a los pasos que se realizan en Debian 5 (ejemplo 1.3), ya que esta distribución también dispone de la herramienta Gdhcpd.

1.3.2.2 Archivos de configuración del servidor DHCP

En el apartado anterior se han visto algunos ejemplos de instalación y configuración de un servidor DHCP para diferentes distribuciones de Linux. Este apartado está dedicado a explicar la configuración del servidor DHCP a través de sus archivos, una técnica que tiene la ventaja de ser común a todas las distribuciones de Linux. Sin embargo, hay que tener cuidado a la hora de modificar directamente los archivos de configuración ya que, en general, la mayoría de ellos son muy sensibles en el formato y cualquier carácter no válido o fuera de lugar puede acarrear un funcionamiento incorrecto o inesperado.

Todos los parámetros del servidor DHCP del ISC se configuran a través del archivo *dhcpd.conf*, que normalmente se encuentra en la carpeta */etc* o en */etc/dhcp*. Hay que tener en cuenta que, cuando se realizan modificaciones en este archivo, es necesario reiniciar o refrescar el proceso demonio del servidor DHCP para que lea la nueva configuración.

El archivo *dhcpd.conf* está escrito en texto plano (sin formato) y contiene una serie de sentencias que pueden ser de tres tipos: *declaraciones*, *peticiones* y *parámetros*.

Las declaraciones pueden contener otras declaraciones, peticiones y parámetros, y pueden ser:

- **shared-network**: se utiliza para definir una red que está formada por distintas subredes. Los parámetros que se indican aquí se aplican a todas las subredes que se definan dentro de ella.
- **subnet**: se utiliza para definir una subred y puede estar declarada dentro o fuera de la declaración de una red (*shared-network*).
- **range**: indica el rango de direcciones que se asigna a los equipos clientes DHCP. Puede aparecer más de una declaración de este tipo siempre que sean rangos de direcciones de la misma subred y no estén solapados.
- **host**: permite definir la configuración específica a un equipo (para que se le reserve una dirección IP específica, para indicar que va a utilizar un protocolo concreto, etc.).
- **group**: se utiliza para hacer agrupaciones de subredes o equipos.
- **pool**: sirve para definir conjuntos de equipos que disponen de diferentes configuraciones de red.
- **class**: permite crear diferentes clases a las que pertenezcan los equipos. Para asignar los equipos a las diferentes clases se puede utilizar la información que el servidor recibe en una petición, especificando la cláusula "match if" para diferenciar a los equipos.

Las peticiones pueden ser aceptadas (poniendo la palabra *allow* delante) o rechazadas (poniendo la palabra *deny*) y son:

- **unknown-clients**: indica que el cliente es desconocido. Si se especifica *allow unknown-clients*, entonces el servidor DHCP asignará direcciones IP a equipos desconocidos; si se especifica *deny unknown-clients* entonces no se asignarán.
- **bootp**: especifica si se van a admitir peticiones de tipo BOOTP, que por defecto si se admiten si no se indica nada o se indica *allow bootp*.
- **booting**: al igual que *bootp*, se utiliza para indicar si se van a aceptar o no peticiones de tipo BOOTP, pero esta indicación solamente se puede realizar dentro de una declaración *host*.

Por su parte, los parámetros que se pueden indicar son los siguientes (se pueden indicar de forma global o aplicados solamente a las declaraciones de redes o subredes):

- **hardware**: se utiliza para especificar un equipo cliente a través del tipo de adaptador de red y la dirección MAC (por ejemplo, *hardware ethernet 2C:34:5E:00:5A:75*).
- **filename**: indica el archivo que va a ejecutar el cliente una vez que ha realizado la configuración de los parámetros de red.
- **server-name**: se usa para establecer el nombre del servidor DHCP.
- **next-server**: especifica cuál es el servidor (indicado con su nombre o dirección IP) que contiene el archivo especificado en *filename*.
- **fixed-address**: se utiliza para establecer una dirección IP que se va a reservar para un equipo concreto.
- **option**: establece varias opciones cuyo nombre y valores deben indicarse a continuación de la palabra *option*. Éstas pueden ser:
  - **subnet-mask**: establece la máscara de subred.
  - **routers**: especifica las direcciones de los encaminadores (o puertas de enlace).
  - **time-servers**: indica los servidores de hora que se basan en el protocolo NTP.
  - **domain-name-servers**: establece las direcciones de los servidores de nombres.
  - **host-name**: especifica el nombre del equipo.

- **domain-name**: indica el nombre del dominio.
- **broadcast-address**: establece la dirección de difusión.

- **ddns-update-style**: especifica si se intenta realizar una actualización del servidor DNS cuando se ha asignado una dirección a un equipo (véase el capítulo 2 de este libro). El valor por defecto es *none*.
- **default-lease-time**: establece el tiempo por defecto que se mantiene la asignación de las direcciones.
- **max-lease-time**: establece el tiempo máximo que se mantiene la asignación de las direcciones.
- **authoritative**: si no se indica y el servidor recibe una petición de un cliente que no conoce porque es incorrecta o pertenece a otra red o subred, no enviará un mensaje de tipo *DHCPNACK* (que indica al cliente que no le puede suministrar la dirección y configuración de red).
- **log-facility**: especifica un nombre de archivo donde se van a registrar los mensajes de error y avisos del proceso demonio del servidor DHCP.

El proceso del servidor DHCP no se iniciará e indicará un mensaje de error en caso de que el archivo */etc/dhcpd.conf* tenga algún error. Será necesario utilizar la orden de inicio del servidor DHCP, consultar los archivos de registro de errores del sistema o examinar la lista de procesos en ejecución para saber si el proceso demonio está en ejecución.

En el archivo *dhcpd.leases* que, dependiendo de la versión y distribución, puede estar ubicado en */var/state/dhcp/* o en */var/lib/dhcp/*, contiene las asignaciones de direcciones que en un momento dado realiza el servidor. Por lo tanto, se puede utilizar para consultar qué direcciones han sido asignadas y a qué equipos. También se puede consultar la configuración de red en cada equipo para comprobar qué parámetros de configuración le han sido asignados.

EJEMPLO 1.5

Supongamos que queremos instalar un servidor DHCP que asigne a los clientes los parámetros de la red, que son:

- Dirección de red: *10.0.8.0*
- Máscara de red: *255.255.255.0*
- Nombre de dominio: *localdomain*
- Servidores de nombres: *10.0.8.3*, *10.0.8.4*
- Encaminador por defecto: *10.0.8.2*

Ahora hay que editar el archivo *dhcpd.conf* para incluir lo siguiente (las líneas precedidas de "#" se consideran comentarios que el sistema ignora):

```
default-lease-time 600;
max-lease-time 7200;
# Aquí se incluye una definición de ámbito (puede
# haber más):
subnet 10.0.8.0 netmask 255.255.255.0 {
       range 10.0.8.6 10.0.8.254;
       option subnet-mask 255.255.255.0;
       option broadcast-address 10.0.8.255;
       option routers 10.0.8.2;
       option domain-name-servers 10.0.8.3, 10.0.8.4;
       option domain-name "localdomain"; }
# Si se quiere reservar una dirección IP a un equipo
# concreto cuyo nombre es ines, se pone lo siguiente:
host ines {
       hardware ethernet 00:40:33:2e:c0:03;
       fixed-address 10.0.8.10; }
```

1.4 CONFIGURACIÓN DE LOS CLIENTES

En el apartado anterior se explica cómo realizar la configuración de los servidores DHCP, es decir, aquellos equipos de la red que van a entregar la configuración necesaria a los equipos que la soliciten.

Puesto que los equipos que funcionan como clientes del servicio DHCP lo hacen para que se simplifique al máximo su configuración, es necesario que ésta no requiera de parámetros ni valores a almacenar. Si esto fuera necesario, se perdería toda la funcionalidad de DHCP, ya que su objetivo es evitar precisamente que tengan que establecerse parámetros de configuración.

Los sistemas operativos actuales se instalan por defecto con una configuración de red que se espera sea obtenida de forma *predeterminada* (DHCP) o *automática* (IPv6). Por esta razón, no es necesario cambiar ningún parámetro en la instalación por defecto del sistema operativo. Gracias a que los mensajes de DHCP se envían a una dirección de difusión que sirve para cualquier red (255.255.255.255), no es necesario indicar ni siquiera la dirección IP del equipo que va a enviar la configuración (el servidor).

Para que un equipo sea capaz de generar su propia dirección IPv6 necesita, por un lado, obtener la dirección de la red capturando los mensajes enviados por los encaminadotes donde se anuncia esta información. Para completar la dirección con la parte que identifica al propio equipo, es necesario que éste disponga de información local donde se incluyan direcciones asignadas con anterioridad y direcciones de otros equipos de la red con los que se intercambiaron mensajes en el pasado. Cuando se ha decidido finalmente la dirección a utilizar, el equipo realiza comprobaciones para detectar direcciones duplicadas en la red. Finalmente, la dirección es asignada, aunque lo será por un tiempo limitado.

Las direcciones asignadas a equipos por cualquiera de los dos mecanismos explicados anteriormente, siempre tienen un tiempo de vida limitado. Mientras ese tiempo no expira, la dirección se considera "preferida", pero cuando ese tiempo va a llegar a su fin, la dirección pasa a ser "desaprobada". En ese momento, el sistema debe generar u obtener una nueva dirección "preferida", que es la que debe utilizar, aunque puede seguir usando la dirección anterior "desaprobada" en caso de que algún programa en ejecución no haya terminado su comunicación y exista riesgo de que ésta se vea interrumpida, con la consiguiente pérdida de información.

En los apartados siguientes se explica cómo acceder a la configuración de red de un sistema operativo Microsoft Windows o GNU/Linux para comprobar que ésta será obtenida de forma automática, bien a través de DHCP o bien de forma automática mediante las condiciones establecidas para el correcto funcionamiento de IPv6.

1.4.1 CONFIGURACIÓN DEL CLIENTE EN MICROSOFT WINDOWS

En este apartado se explica con ejemplos concretos cómo establecer una configuración automática de red para equipos que trabajan con sistema operativo Microsoft Windows.

EJEMPLO 1.6

Los pasos para comprobar si un equipo con Windows XP tiene establecida una configuración automática que va a obtener por el servicio DHCP son los siguientes:

1. Pulsar con el botón derecho sobre el icono "Mis sitios de red" del escritorio o del menú de inicio y seleccionar "Propiedades". Aparecerá una ventana con los iconos asociados a cada una de las conexiones de red disponibles en el equipo.
2. Seguidamente hay que pulsar con el botón derecho del ratón en el icono "Conexión de área local" y seleccionar "Propiedades". Aparecerá una ventana con una lista que incluye todos los protocolos y servicios que funcionan sobre esa conexión de red.
3. A continuación se selecciona "Protocolo TCP/IP" y se pulsa el botón "Propiedades". En esta otra ventana se muestran los parámetros TCP/IP asociados a la conexión de red seleccionada (Figura 1.12).
4. En la página "General" (Figura 1.12) se muestran los parámetros generales de TCP/IP asociados a la conexión de red. Para que el equipo pueda obtener una dirección por DHCP deben estar marcados los botones de opción "Obtener una dirección IP automáticamente" y "Obtener la dirección del servidor DNS automáticamente".
5. En la página "Configuración alternativa" se puede seleccionar el botón de opción "Dirección IP privada automática" para que el equipo se asigne una dirección por el método APIPA, cuando no recibe ninguna por DHCP. Si se marca el botón de opción "Configurada por el usuario", se puede especificar una configuración de red manual en caso de que no se reciba ninguna respuesta por DHCP.
6. Para probar que se ha obtenido la configuración por DHCP en el arranque de Windows XP, ejecutar la orden *IPCONFIG /ALL* en el intérprete (Figura 1.13).

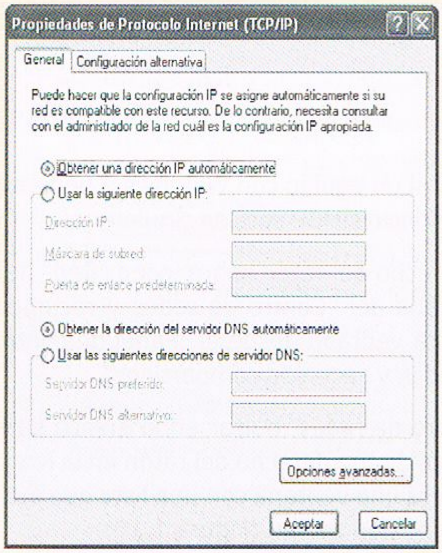


Figura 1.12. *Ventana de configuración de los parámetros TCP/IPv4 en Windows XP. Los botones de opción marcados permiten que el equipo pueda obtener toda la configuración de un servidor DHCP. En caso de que no sea posible, el equipo se asignará la configuración indicada en la pestaña "Configuración alternativa"*

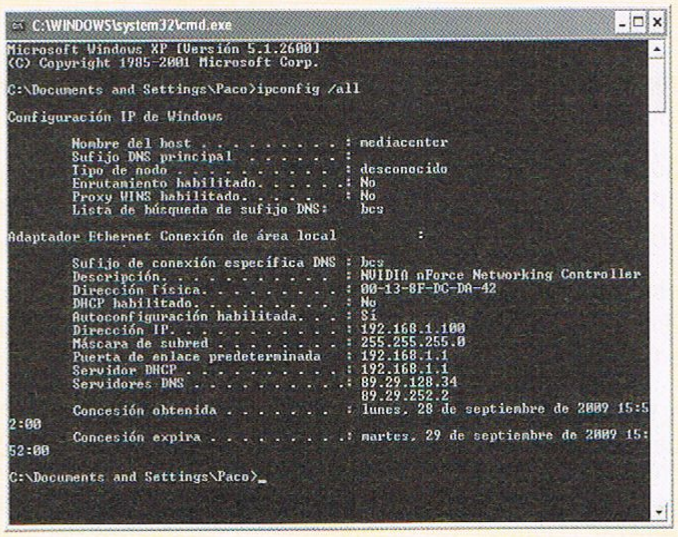


Figura 1.13. *Consulta de la configuración de red asignada a una conexión por DHCP en Windows XP. En la información titulada "Servidor DHCP" se muestra la dirección IPv4 del equipo que ha enviado todos los parámetros que se muestran*

Windows XP también permite el uso del protocolo IPv6, aunque no se instala por defecto en el sistema operativo. Es posible instalar y utilizar esta característica avanzada si se accede a la lista de servicios y protocolos disponibles para el adaptador de red (paso 2 de este ejemplo) y se pulsa el botón "Instalar...". A continuación se selecciona "Protocolo" y se pulsa en el botón "Agregar...". En la ventana que aparece, se selecciona "Microsoft TCP/IP versión 6" y se pulsa el botón "Aceptar". Hay que tener en cuenta que, cuando un equipo utiliza los protocolos IPv4 e IPv6 a la vez, siempre debe tener preferencia IPv6, a no ser que las direcciones de los equipos con los que se van a establecer comunicaciones sean IPv4.

EJEMPLO 1.7

Los pasos para comprobar si un equipo con Windows 7 tiene establecida una configuración automática que va a obtener por el servicio DHCP son los siguientes:

1. Pulsar con el botón derecho del ratón sobre icono "Red" del escritorio y seleccionar "Propiedades". Se mostrará una ventana del "Centro de redes y recursos compartidos" (Figura 1.14). También se puede acceder a esta ventana desde el "Panel de control", seleccionando "Redes e Internet" y después "Centro de redes y recursos compartidos".
2. En la ventana del centro de redes, pulsar en el enlace de la izquierda "Cambiar configuración del adaptador", pulsar con el botón derecho del ratón en el icono "Conexión de área local" y seleccionar "Propiedades". Aparecerá una ventana con una lista que incluye todos los protocolos y servicios que funcionan sobre esa conexión de red (Figura 1.15).
3. Seguidamente, seleccionar "Protocolo de Internet versión 4 (TCP/IPv4)" en la ventana de la Figura 1.15 y pulsar el botón "Propiedades". En la página "General", deben aparecer marcados los botones de opción "Obtener una dirección IP automáticamente" y "Obtener la dirección del servidor DNS automáticamente" (Figura 1.16).

4. En la página "Configuración alternativa" se puede seleccionar el botón de opción "Dirección IP privada automática" para que el equipo se asigne una dirección por el método APIPA cuando no recibe ninguna por DHCP. Si se marca el botón de opción "Configurada por el usuario", se puede especificar una configuración de red manual en caso de que no se reciba ninguna respuesta por DHCP.

5. Para probar que se ha obtenido la configuración por DHCP en el arranque de Windows 7, ejecutar la orden *IPCONFIG /ALL* en el intérprete (Figura 1.17). Si en la salida de esta orden se muestran los parámetros TCP/IP junto con la dirección del servidor DHCP desde donde se han obtenido, entonces la asignación se ha realizado correctamente.

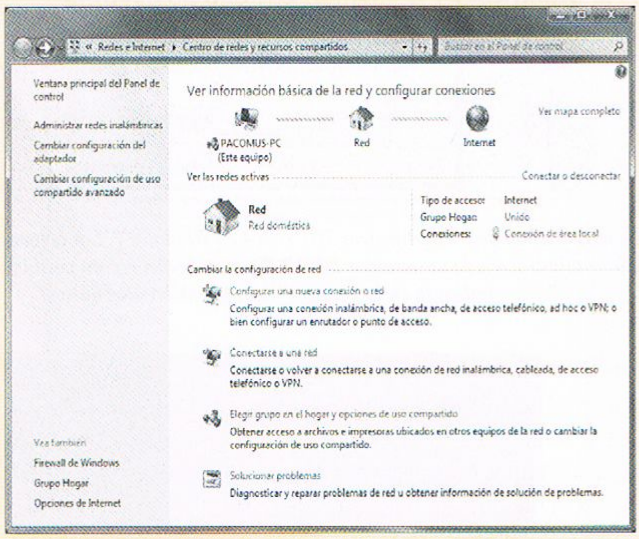


Figura 1.14. *Centro de redes y recursos compartidos de Windows 7. Desde esta ventana se pueden gestionar todas las conexiones de red disponibles en el equipo*

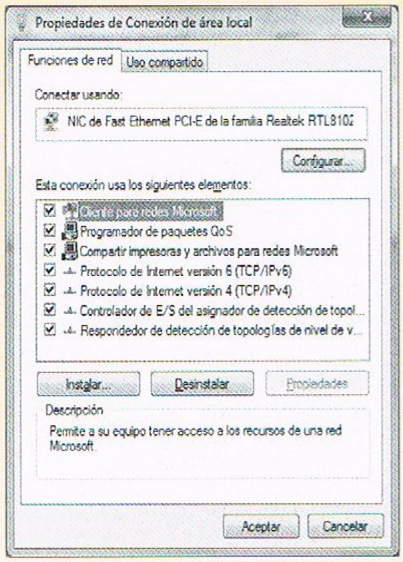


Figura 1.15. *Ventana de propiedades de la conexión de área local en Windows 7. Aquí se muestran todos los protocolos y servicios que funcionan para el adaptador de red seleccionado. Desde esta ventana se pueden instalar o desinstalar esos protocolos y servicios. Obsérvese que en Windows 7 está instalado por defecto IPv6, cuya configuración es accesible si se selecciona y se pulsa el botón "Propiedades"*

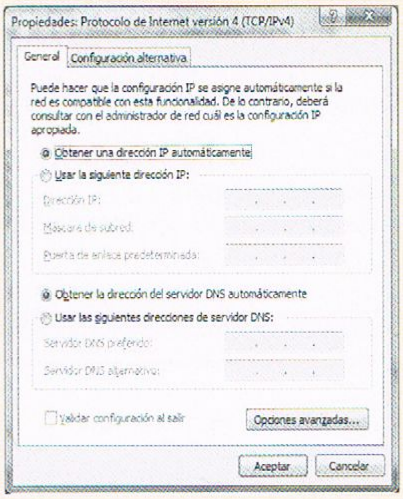


Figura 1.16. *Ventana de configuración de los parámetros TCP/IPv4 en Windows 7. Los botones de opción marcados permiten que el equipo pueda obtener toda la configuración de un servidor DHCP. En caso de que no sea posible, el equipo se asignará la configuración indicada en la pestaña "Configuración alternativa"*

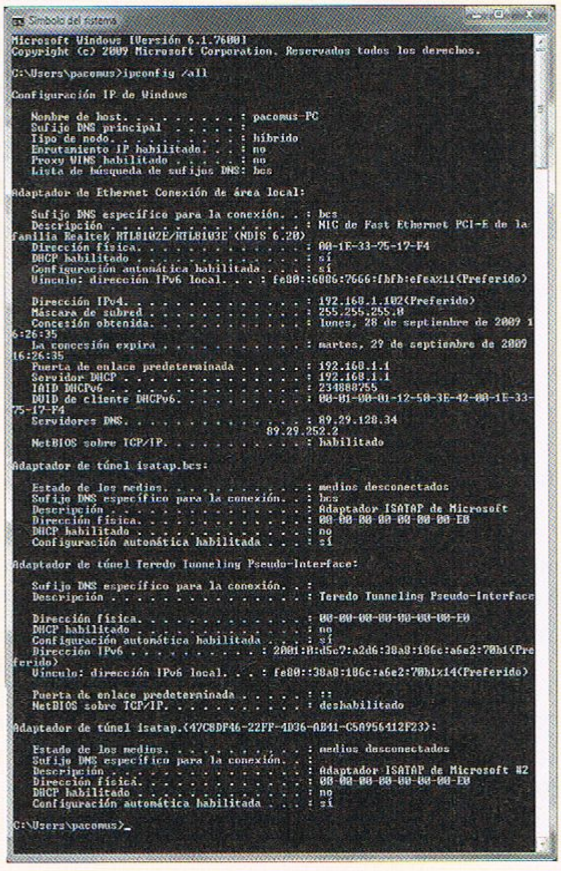


Figura 1.17. *Consulta de la configuración de red asignada a una conexión por DHCP en Windows 7. En la información titulada "Servidor DHCP" se muestra la dirección IPv4 del equipo que ha enviado todos los parámetros que se muestran. Aquí también se muestra cuándo se ha asignado esta configuración y cuándo caduca. Si comparamos la información que muestra esta ventana con respecto a Windows XP (Figura 1.13), se puede observar que aquí se incluye información sobre la configuración IPv6 que se ha obtenido automáticamente*

Windows 7 incluye IPv6 en la instalación por defecto del sistema operativo. Como se muestra en la Figura 1.17, cuando están disponibles IPv4 e IPv6 en el mismo equipo, éste obtiene la configuración necesaria para los dos protocolos, de forma que estos se encuentren activos. Hay que tener en cuenta que, cuando un equipo utiliza los protocolos IPv4 e IPv6 a la vez, siempre debe tener preferencia IPv6, a no ser que las direcciones de los equipos con los que se van a establecer comunicaciones sean IPv4.

Los sistemas operativos Microsoft Windows utilizan el sistema Teredo para permitir la coexistencia de los protocolos IPv4 e IPv6. Este sistema crea un sistema de túnel IPv6 sobre IPv4 en caso de que sea necesario conectar con un equipo IPv6 a través de una red que funciona con IPv4. Si se va a conectar con un equipo IPv4 a través de una red también IPv4, se utiliza la conexión configurada con este protocolo. Si se va a conectar con un equipo IPv6 a través de una red también IPv6, se utiliza el interfaz configurado con IPv6 para esta comunicación.

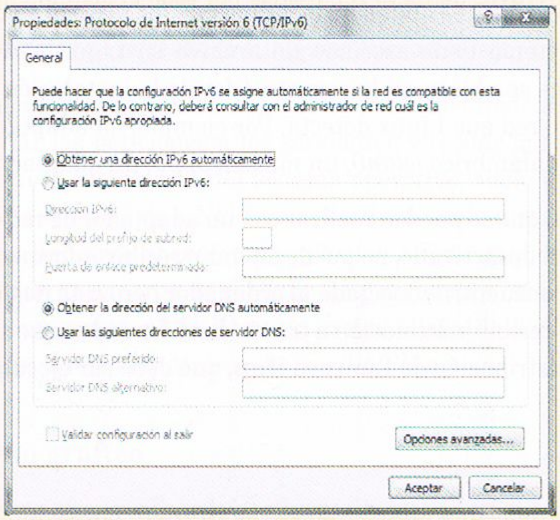


Figura 1.18. *Ventana de configuración de los parámetros TCP/IPv6 en Windows 7. Los botones de opción marcados permiten que el equipo pueda obtener toda la configuración, bien de forma predeterminada (desde un servidor DHCPv6) o bien de forma automática. Puesto que IPv6 puede generar una configuración automáticamente sin ayuda, no es necesario que exista ninguna otra configuración alternativa, como el uso de APIPA en IPv4*

1.4.2 CONFIGURACIÓN DEL CLIENTE EN GNU/LINUX

Al igual que ocurre con la configuración de un servidor DHCP en GNU/Linux, la configuración de un cliente DHCP para este sistema operativo requiere que el núcleo tenga soporte para enviar paquetes de difusión (recuérdese que el protocolo DHCP utiliza paquetes de difusión para asignar las direcciones). Para comprobar si el núcleo soporta el envío de paquetes de difusión hay que ejecutar como *root* la orden *ifconfig eth0* (*eth0* es el adaptador de red que va a recibir las solicitudes DHCP) y comprobar que en la salida aparece la palabra "MULTICAST". En caso negativo, hay que utilizar otro núcleo o compilar uno con la opción "IP Multicasting" activada. Normalmente, todos los núcleos modernos de Linux están compilados para soportar esta característica.

De igual forma, para que los mensajes sean enviados correctamente a través de las direcciones de difusión, es necesario que el equipo tenga también una entrada en su tabla de encaminamiento que especifique cuál es la dirección para difusión en la red (que es la IPv4 255.255.255.255 donde se envían las peticiones DHCP). Para comprobarlo, se utiliza la orden *route* sin argumentos (véase la referencia de órdenes incluida con este libro). En caso de que ya exista,

deberá aparecer una entrada con la dirección 255.255.255.255 dentro de la columna "Destination". Si no aparece, hay que incluirla con la siguiente orden, que debe ser ejecutada con la cuenta de usuario *root*:

```
root@linux:~# route add -host 255.255.255.255 /dev/eth0
```

Si la orden anterior devuelve algún error, entonces hay que editar el archivo */etc/hosts*, incluir en él la línea *255.255.255.255 all-ones* (respetando los tabuladores de las líneas que ya aparecen) y ejecutar como *root* la orden:

```
root@linux:~# route add -host all -ones /dev/eth0
```

La mayoría de las opciones de configuración básica de los adaptadores de red se pueden realizar sin problemas a través de utilidades en entorno gráfico y de forma parcialmente automática. Sin embargo, cuando la configuración se aleja de las situaciones normales o es necesario configurar servicios específicos, entonces el administrador no tiene más remedio que pelearse con archivos de texto repartidos por todo el sistema de ficheros.

Cualquier dispositivo del sistema tiene asociado un archivo en Linux para poder hacer referencia a él. Estos archivos de dispositivo especiales se ubican en la carpeta */dev* de la instalación del sistema. Esta situación también es aplicable a los adaptadores de red que Linux detecta. Por ejemplo, un adaptador Ethernet puede tener asociado el dispositivo *eth0*, un adaptador inalámbrico *wlan0*, un módem *ppp0*, un adaptador Token Ring *tr0*, etc.

Las operaciones más sencillas que se pueden realizar con un adaptador de red en Linux son activarlo o desactivarlo. Cuando un adaptador de red está desactivado, no puede enviar o recibir información por la red. Es un estado parecido a cuando una unidad de disco se encuentra conectada al ordenador pero está desmontada. Solamente cuando se activa el dispositivo es posible enviar o recibir información a través de él. La orden que se utiliza para activar una interfaz de red y que sirve para cualquier distribución de Linux es **ifup**, que debe ser ejecutado con privilegios de administrador (*root*). Por ejemplo:

```
# ifup eth0
```

Y la orden que permite desactivar una interfaz de red es **ifdown**, por ejemplo:

```
# ifdown eth0
```

Además de estas órdenes, también pueden existir herramientas gráficas en diferentes distribuciones de Linux que permiten activar y desactivar interfaces de red.

La configuración de red en los sistemas Linux se puede realizar, dependiendo de la distribución utilizada, de tres formas posibles:

- **Configuración de bajo nivel**: consiste en utilizar una serie de órdenes para establecer los parámetros de la red y de la arquitectura TCP/IP. Estas órdenes pueden ser **ifconfig** y **route**, que tradicionalmente han sido utilizadas desde los inicios de Linux. También se puede utilizar la orden **ip**, que es mucho más completa y potente, aunque solamente funciona con versiones del núcleo 2.2 o superior, además de que a los usuarios experimentados no les puede resultar tan familiar trabajar con ella. En el apartado 1.4.2.3 se explica cómo configurar la red en Linux con estas herramientas.
- **Configuración de alto nivel**: consiste en emplear un archivo de configuración de texto que almacena todos los parámetros de la red con un formato definido. Este archivo de configuración puede cambiar en nombre y ubicación dependiendo de la distribución y versión de Linux (por ejemplo, en Debian 5 es */etc/network/interfaces*, mientras que en OpenSUSE 11.1 es */etc/sysconfig/network/config*). El archivo de configuración de la red establece los parámetros de un adaptador "virtual" o "lógico", es decir, que no existe físicamente. Posteriormente, ese adaptador lógico debe ser asociado con el adaptador físico correspondiente (*eth0*, *eth1*,

etc.). Para establecer la configuración de red a alto nivel, se usa la orden *ifdown* para desactivar la interfaz, se modifica el archivo de configuración y finalmente se usa la orden *ifup* para activarlo. En el apartado 1.4.2.2 se explica cómo realizar una configuración de la red en Linux a alto nivel.

- **Herramientas de entorno gráfico**: algunas distribuciones de Linux permiten instalar herramientas gestionadas desde el entorno gráfico que sirven para realizar una configuración de la red de la misma forma que en otros sistemas operativos como Microsoft Windows. De esta forma, los usuarios que están más acostumbrados a trabajar con estos sistemas pueden cambiar a Linux sin sufrir un cambio brusco. Estas herramientas pueden ser YaST (OpenSUSE), Control de dispositivos de red (Fedora), NetworkManager, Webmin, Linuxconf, etc. En el apartado 1.4.2.1 se explica cómo realizar la configuración de la red utilizando estas herramientas.

La configuración de red en Linux también requiere el uso de una cuenta de usuario que disponga de los privilegios necesarios para realizar las operaciones necesarias. Normalmente, cuando se realiza una instalación típica de Linux, se crea la cuenta ***root***, que tiene privilegios para realizar cualquier operación sobre el sistema.

Para que un equipo con Linux funcione correctamente, necesita tener instalado el paquete del cliente DHCP, que contiene el proceso encargado de enviar las peticiones a los servidores y recibir la configuración. Este paquete, que normalmente se incluye por defecto en la instalación del sistema operativo, suele denominarse *dhcp*, *dhcp-client* o *dhclient*. Además, en las distribuciones actuales de GNU/Linux, también suele instalarse por defecto el paquete que contiene el cliente DHCPv6, que suele llamarse *dhcpv6* o *dhcpv6-client*. Este paquete contiene un proceso demonio, habitualmente denominado *dhclient*, que se encarga de realizar las peticiones a los servidores. Este proceso demonio guarda la configuración que recibe de un servidor DHCP en un archivo llamado *dhclient.leases* que, dependiendo de la distribución y versión de GNU/Linux, suele encontrarse en */var/lib/dhcp*.

1.4.2.1 Configuración en entorno gráfico

En los ejemplos siguientes se muestra cómo realizar la configuración de red en diferentes distribuciones GNU/Linux utilizando herramientas gráficas de configuración.



EJEMPLO 1.8

Los pasos para configurar un dispositivo de red en OpenSUSE 11.1 sobre un equipo que va a funcionar como cliente DHCP son los siguientes:

1. Acceder a YaST y seleccionar "Dispositivos de red || Ajustes de la red".
2. En la ventana que aparece, donde se gestionan los dispositivos de red instalados (Figura 1.19), seleccionar el adaptador y pulsar el botón "Editar".
3. En la pestaña "Dirección" de la Figura 1.19, seleccionar "Dirección dinámica" y en las dos listas desplegables seleccionar "DHCP" y "Solo versión 4 de DHCP" (Figura 1.20).
4. Para obtener también la configuración DNS por DHCP, hay que acceder a la página "Nombre de Host/DNS" de la Figura 1.19 y marcar la casilla de verificación "Modificar Nombre de Host mediante DHCP".

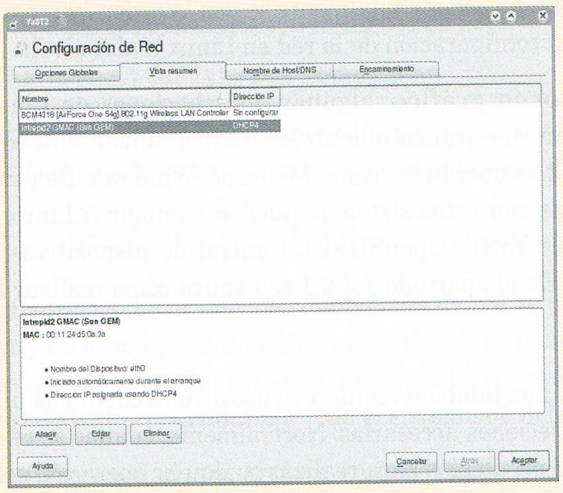


Figura 1.19. *Ventana de gestión de los dispositivos de red en YaST sobre OpenSUSE 11.1. Aquí se muestran todos los dispositivos de red instalados en el equipo. Si se selecciona cualquiera de ellos y se pulsa el botón "Editar", se puede acceder a su configuración detallada*

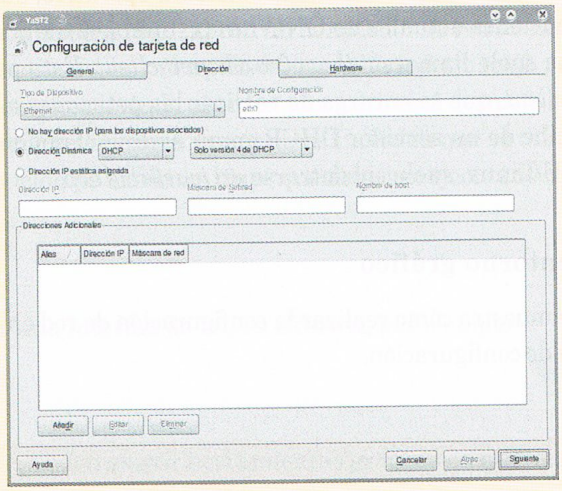


Figura 1.20. *Configuración de un adaptador de red en YaST. La página "Dirección" especifica los parámetros de red IPv4 e IPv6 y permite establecer una configuración automática (DHCP u otros métodos) o manual*

Es posible establecer también una configuración de red IPv6 para el adaptador de red si se especifica una de las siguientes opciones en la segunda lista desplegable de "Dirección Dinámica" (Figura 1.20):

- **Solo versión 6 de DHCP**: intenta asignar una dirección IPv6 al adaptador de red, bien de forma predeterminada por DHCPv6 o bien de forma automática.
- **DHCP versiones 4 y 6** (ambas): intenta asignar dos direcciones IPv4 e IPv6. La asignación de la dirección IPv4 se realizará por DHCP y, si no lo consigue, asignará una dirección APIPA. La asignación IPv6 se realizará, bien de forma predeterminada por DHCPv6 o bien de forma automática.

Cuando un adaptador de red tiene asignadas ambas direccines IPv4 e IPv6, utiliza una u otra en función de si el equipo de destino usa un esquema de direccionamiento u otro.

EJEMPLO 1.9

Las últimas versiones de los sistemas Fedora, al igual que ocurre con otras distribuciones GNU/Linux, utilizan por defecto la herramienta NetworkManager para la gestión de la configuración de los adaptadores de red. Los pasos para configurar un dispositivo de red en Fedora 11 con Gnome sobre un equipo que va a funcionar como cliente DHCP son los siguientes:

1. Acceder a NetworkManager, pulsando con el botón derecho del ratón sobre el icono de red del panel superior y seleccionar "Editar las conexiones...", lo que muestra una ventana como la de la Figura 1.21. También se puede acceder desde el menú principal del entorno en "Sistema || Preferencias || Conexiones de red".
2. Para comprobar la configuración DHCP, seleccionar el adaptador que corresponda (normalmente será "System eth0") y pulsar el botón "Editar". En la ventana que aparece, seleccionar la pestaña "Ajustes de IPv4". En la lista desplegable "Método" debe aparecer la opción "Automático (DHCP)" (véase la Figura 1.22).

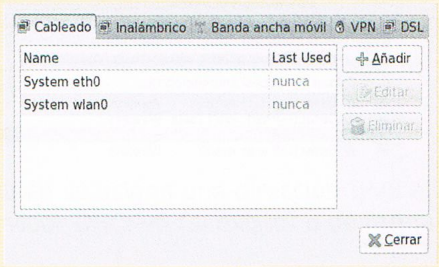


Figura 1.21. *Ventana principal de gestión de los dispositivos de red de NetworkManager sobre Fedora 11 con Gnome. Aquí se muestra una lista con los dispositivos disponibles ("System eth0" es el adaptador de red cableada, mientras que "System wlan0" se refiere al adaptador inalámbrico)*

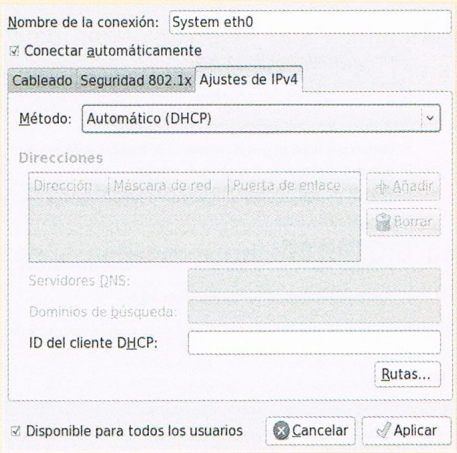


Figura 1.22. *Configuración IPv4 de un adaptador de red en NetworkManager. Aquí se especifica la configuración de red manual o automática (por DHCP)*

En Fedora 11 es posible desactivar NetworkManager y utilizar otra herramienta de configuración de red que se ha incluido por defecto en anteriores versiones del sistema. Esta herramienta, denominada **system-config-network**, permite gestionar también los adaptadores de red conectados en el equipo

y se incluye como paquete instalable en los repositorios oficiales. Los pasos a seguir para configurar la red con esta herramienta son:

1. Instalar el paquete *system-config-network*.
2. Acceder a la herramienta de configuración, seleccionando la opción correspondiente del entorno gráfico (en Gnome es "Sistema || Administración || Red" o ejecutando la orden del intérprete *system-config-network-gui*.
3. En la pantalla principal que aparece (Figura 1.23), seleccionar el adaptador a configurar y pulsar el botón "Modificar", lo que muestra una ventana como la de la Figura 1.24.
4. En la ventana de la Figura 1.24, se puede desactivar el control de NetworkManager sobre este adaptador si se desmarca la casilla de verificación "Controlado por NetworkManager".
5. La herramienta de configuración *system-config-network* también permite especificar si los adaptadores de red van a ser configurados mediante IPv6.

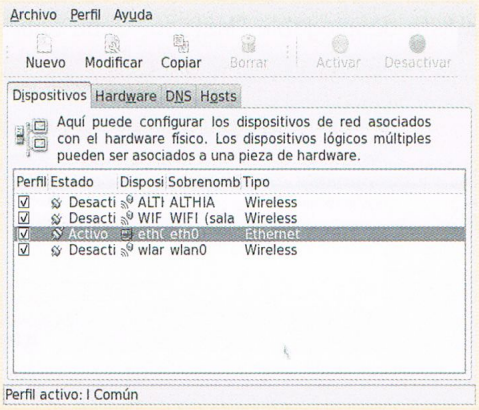


Figura 1.23. *Ventana principal de gestión de los dispositivos de red de system-config-network sobre Fedora 11. Esta ventana muestra los adaptadores conectados al equipo, de igual forma que la ventana de NetworkManager de la Figura 1.21. El adaptador eth0 es la conexión de red cableada, mientras que wlan0 hace referencia al adaptador inalámbrico*

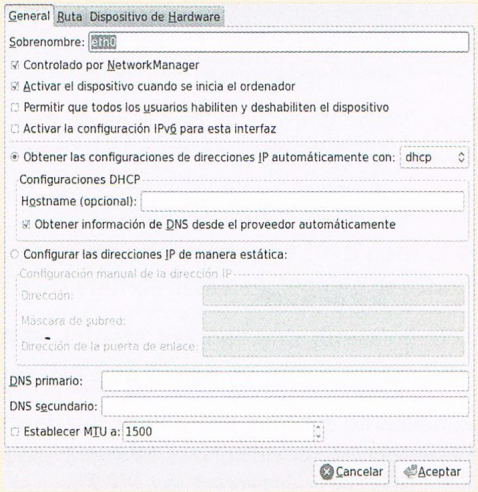


Figura 1.24. *Configuración de un adaptador de red con la herramienta system-config-network. En esta ventana se puede indicar si el dispositivo está controlado por NetworkManager. Para especificar que este adaptador va a obtener la configuración por DHCP hay que marcar el botón de opción "Obtener las configuraciones de direcciones IP automáticamente con:" y seleccionar "dhcp" de la lista desplegable. También se puede activar el uso de IPv6 en la casilla de verificación correspondiente*

Las distribuciones Debian actuales también incluyen herramientas gráficas de configuración de los adaptadores de red. Por ejemplo, en Debian 5 y en otras distribuciones se puede instalar el paquete *gnome-network-admin*, que será accesible desde la opción del menú principal de Gnome "Sistema || Administración || Red".

1.4.2.2 Configuración de alto nivel

En los ejemplos siguientes se explica cómo se establecen los parámetros de un cliente DHCP utilizando los archivos de configuración de alto nivel de la distribución GNU/Linux.



EJEMPLO 1.10

El siguiente ejemplo muestra cómo debe realizarse una configuración a alto nivel de la red sobre Debian 5 como cliente DHCP. Los pasos a seguir son los siguientes (ejecutados como usuario *root*):

1. Desactivar la interfaz de red:
   ```
   # ifdown eth0
   ```
2. Editar el archivo */etc/network/interfaces* para que contenga la siguiente información:
   ```
   iface eth0 inet dhcp
   ```
3. Activar la interfaz de red:
   ```
   # ifup eth0
   ```

En la configuración anterior también se asigna una dirección IPv6 al adaptador de red. Esta dirección podrá ser obtenida desde un servidor DHCPv6 (si existe) o de forma automática.



EJEMPLO 1.11

El siguiente ejemplo muestra cómo debe realizarse una configuración a alto nivel de la red sobre Fedora 11 como cliente DHCP, suponiendo que el adaptador de red a configurar es *eth0*. Los pasos a seguir son los siguientes (ejecutados como usuario *root*):

1. Desactivar la interfaz de red:
   ```
   # ifdown eth0
   ```
2. Editar el archivo */etc/sysconfig/network-scripts/ifcfg-eth0* para que contenga la siguiente información:
   ```
   DEVICE=eth0
   BOOTPROTO=dhcp
   HWADDR=00:11:24:D5:0A:3A
   ONBOOT=yes
   ```
3. Opcionalmente, el archivo *ifcfg-eth0* puede contener una línea con el parámetro *HWADDR*, que especifica la dirección MAC del adaptador.
4. Revisar el archivo de configuración */etc/sysconfig/network* para comprobar que contiene la siguiente línea:
   ```
   NETWORKING=yes
   ```

5. Finalmente, hay que activar la interfaz de red:

```
# ifup eth0
```

En la configuración del archivo */etc/sysconfig/network-scripts/ifcfg-eth0* se ha activado por defecto el protocolo IPv6 sobre el adaptador de red. Si deseamos desactivar IPv6 para ese adaptador de red, hay que añadir la siguiente línea:

```
NETWORKING_IPV6=no
IPV6_AUTOCONF=no
```

1.4.2.3 Configuración de bajo nivel

Otra forma de establecer la configuración de las interfaces de red en GNU/Linux es a través de las órdenes de bajo nivel *ifconfig*, *route* e *ip*. Esta forma de configurar las interfaces tiene la ventaja de que sirve para cualquier sistema Linux, incluso las distribuciones antiguas. Sin embargo, tiene el inconveniente de que requiere el aprendizaje de estas órdenes, que no resultan nada fáciles de utilizar y es necesario utilizar otros mecanismos adicionales que permitan guardar la configuración establecida para que permanezca una vez que se apaga o reinicia el equipo.

Existen dos formas de configurar una interfaz de red a bajo nivel sobre GNU/Linux: usando las órdenes **ifconfig** y **route**, tradicionalmente incluidas en todas las versiones y distribuciones de GNU/Linux o usando la orden **ip**, mucho más actual, más estandarizada y más potente, pero que no se incluye en las distribuciones antiguas. En los ejemplos 1.12 y 1.13 se muestra cómo realizar la configuración de red con estas órdenes.



EJEMPLO 1.12

El siguiente ejemplo muestra cómo debe realizarse una configuración a bajo nivel de la interfaz de red válida para cualquier distribución de GNU/Linux. Los pasos para configurar el adaptador utilizando las órdenes *ifconfig* y *route* de un equipo que va a funcionar como cliente DHCP son los siguientes:

1. Acceder al terminal de línea de órdenes como usuario *root*.
2. Suponemos que la interfaz de red cuya configuración de red vamos a modificar está inactiva. Si no es así, tenemos que desactivarla con la orden siguiente:

```
# ifconfig eth0 inet down
```

3. A continuación, especificamos que la interfaz se va a configurar por DHCP:

```
# ifconfig eth0 inet dhcp start
```

4. Se puede comprobar que la interfaz ha obtenido una configuración válida si se ejecuta la orden *ifconfig eth0*. Se puede ejecutar también la siguiente orden para comprobar el estado de configuración del cliente DHCP (si aparece la palabra "BOUND", significa que se ha obtenido la configuración de red de un servidor DHCP):

```
# ifconfig eth0 dhcp status
```

5. Finalmente, se puede comprobar que también se ha obtenido la configuración correcta de las tablas de encaminamiento del equipo local:

```
# route
Kernel IP routing table
Destination  Gateway       Genmask         Flags  Metric  Ref  Use  Iface
192.168.1.0   *            255.255.255.0    U      0       0    0    eth0
default       192.168.1.1  0.0.0.0          UG     0       0    0    eth0
```

Se puede activar el uso de IPv6 sobre la interfaz si se cambia el argumento "inet" por "inet6". Además de esta configuración, para que el sistema de red funcione a la perfección, es necesario configurar el cliente del protocolo DNS. Esta configuración se realiza incluyendo las direcciones IP de los servidores de nombres en el archivo */etc/resolv.conf*. Para más información, puede consultar el apartado 2.5.2.2 del capítulo 2 donde se explica el funcionamiento del servidor DNS.



EJEMPLO 1.13

El siguiente ejemplo muestra cómo debe realizarse una configuración a bajo nivel de la interfaz de red válida para cualquier distribución de GNU/Linux. Para realizar la configuración del ejemplo 1.12 usando la orden *ip* hay que ejecutar lo siguiente (como usuario *root*):

```
# ip link set dev eth0 down
# ip link set dev eth0 dynamic on
# ip link set dev eth0 up
eth0: Link is up at 100 Mbps, full-duplex.
eth0: Pause is enabled (rxfifo: 10240 off: 7168 on: 5632)
# ip addr show dev eth0
2: eth0: <BROADCAST,MULTICAST,DYNAMIC,UP,LOWER_UP>
    mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:11:24:d5:0a:3a brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.102/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::211:24ff:fed5:a3a/64 scope link
        valid_lft forever preferred_lft forever
# ip route show
192.168.1.0/24 dev eth0  proto kernel  scope link src
192.168.1.120  metric 1
default via 192.168.1.1 dev eth0  proto static
```

1.4.2.4 Comprobación de la configuración

Una vez que se ha configurado un equipo como cliente DHCP, éste debe obtener la configuración desde un servidor de la red o, si no hay ninguno disponible, asignarse una dirección por el método APIPA (IPv4) o de forma automática por IPv6. Si, a partir de ese momento, el equipo es capaz de acceder a los servicios de la red, entonces la configuración que ha obtenido será correcta. Sin embargo, si no puede acceder a la red, entonces la configuración que ha obtenido no es correcta o ningún servidor DHCP de la red ha podido proporcionarle ninguna.

En los equipos con Microsoft Windows, se pueden utilizar las siguientes herramientas para comprobar si el equipo ha obtenido una configuración correcta:

- **Centro de redes y recursos compartidos**: esta herramienta es la utilizada para establecer la configuración de red de los adaptadores instalados en Windows Vista/7. También se puede consultar cúal es la configuración de red actual si, desde la ventana del centro de redes, se selecciona "Conexión de área local | | Detalles", lo que muestra una ventana informativa como la de la Figura 1.25.

- **Orden** *netsh*: esta orden permite establecer o modificar la configuración de red de equipos con Windows XP/Vista/7 o Windows Server 2000/2003/2008. Cuando se inicia netsh, se muestra un indicador de órdenes específicas de esta herramienta para modificar o consultar la configuración de red. Se pueden ejecutar las órdenes *interface*, después *ipv4* (*ip* si es Windows XP) y después *show config*, lo que mostrará la configuración de red actual.

- **Orden** *ipconfig*: se trata de una orden tradicionalmente utilizada en todas las versiones de Windows. Si se ejecuta con el parámetro */all*, muestra la configuración completa para todos los adaptadores de red instalados.

- **Orden** *ping*: permite comprobar si el equipo puede conectar con otro a través de la red. Para usar esta orden, hay que especificar la dirección IP del otro equipo. Esta orden envía un mensaje (de tipo *eco ICMP*) y espera una respuesta del equipo remoto. Si se producen esas respuestas a los mensajes ICMP enviados, entonces es que la interfaz de red está correctamente configurada.

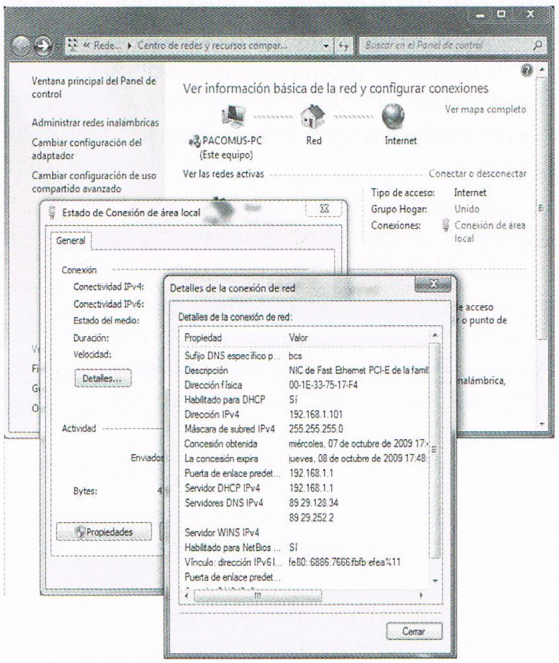


Figura 1.25. *Detalles de la conexión de red cableada en Windows 7. A esta ventana se accede desde el Centro de redes y recursos compartidos y muestra los parámetros de configuración del adaptador. Con la información que se muestra se pueden detectar y corregir posibles problemas de configuración*

Para comprobar si la configuración recibida por DHCP es correcta, se pueden utilizar una serie de herramientas incluidas en la instalación de GNU/Linux. Estas herramientas, que tienen la forma de órdenes del intérprete, son las siguientes:

- **ifconfig**: como se explica en los apartados anteriores, esta orden se puede utilizar para establecer la configuración de red a bajo nivel. También permite consultar los parámetros de configuración actuales de todos los adaptadores instalados en el equipo (o solamente del adaptador indicado), si no se indica ningún parámetro de configuración (véase la Figura 1.26).

- **route**: esta orden, que también se explica en apartados anterires, permite establecer las tablas de encaminamiento del equipo (a bajo nivel). Si se utiliza sin argumentos, muestra el estado actual de la tabla de encaminamiento con las entradas que dispone. Gracias a esta orden se puede consultar el estado de estas tablas y verificar su funcionalidad.
- **ip**: es una orden muy completa que permite mostrar o manipular dispositivos de red, tablas de encaminamiento, políticas de encaminamiento y túneles. Con la orden "ip addr show" se puede consultar el estado de configuración de las interfaces de red. Por su parte, con la orden "ip route show" se pueden consultar las entradas de la tabla de encaminamiento.
- **ping**: permite comprobar si el equipo puede conectar con otro a través de la red. Para usar esta orden, hay que especificar la dirección IP del otro equipo. Esta orden envía un mensaje (de tipo *eco ICMP*) y espera una respuesta del equipo remoto. Si se producen esas respuestas a los mensajes ICMP enviados, entonces es que la interfaz de red está correctamente configurada.

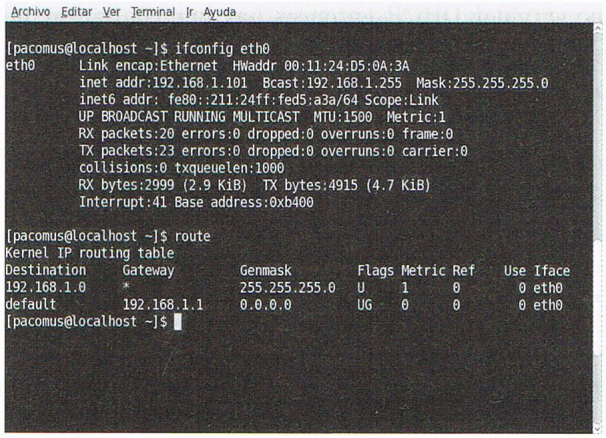


Figura 1.26. *Las órdenes ifconfig y route para consultar el estado de los adaptadores de red en GNU/Linux. La orden ifconfig muestra la configuración actual del adaptador, mientras que route muestra información sobre la tabla local de encaminamiento (es muy útil para saber si está correctamente configurada la pasarela o puerta de enlace por defecto para acceder a otras redes conectadas, como Internet)*

1.5 PROBLEMAS ASOCIADOS A DHCP

Como se explica en este capítulo, el protocolo DHCP se utiliza para asignar los parámetros de red de forma automática a los equipos. En caso de que esta asignación no sea posible, entonces el equipo cliente va a tener una configuración de red por defecto (APIPA en IPv4 o una dirección automática IPv6), por lo que a primera vista puede dar la impresión de que se trata de un problema de ese equipo y no del servidor DHCP o de la red.

Para identificar si el problema ha ocurrido a causa del servidor DHCP hay que tener en cuenta lo siguiente:

- El equipo tiene establecida en su configuración que obtendrá una dirección de forma automática por DHCP.
- El equipo tarda mucho más tiempo en arrancar de lo normal. Esto es debido a que el protocolo DHCP especifica que se realicen varios intentos si no se consigue la configuración. Si se examinan los mensajes que muestra el núcleo de Linux durante el arranque del sistema, se puede detectar esta situación.

- Una vez que ha arrancado, el equipo tiene asignada una dirección IP de la red 169.254.0.0/16 (protocolo APIPA), una dirección estática que se ha asignado en caso de que falle el protocolo DHCP o una dirección automática IPv6 (por ejemplo, la dirección privada *FEC0::*, aunque ha sido declarada obsoleta por el RFC 3879, que indica que no debe ser utilizada).

1.5.1 PROBLEMAS CON EL CORTAFUEGOS

La mayoría de los sistemas operativos actuales se instalan por defecto con un programa cortafuegos que aumenta el nivel de seguridad del equipo, evitando intrusiones o accesos no autorizados en él. Sin embargo, este mecanismo, que resulta enormemente beneficioso, puede perjudicar determinados servicios que tenemos activados en el equipo, hasta tal punto que no funcionen como se espera.

En los sistemas operativos de Microsoft, los servicios de cortafuegos que llevan instalados permiten por defecto el tráfico de mensajes como clientes DHCP, por lo que este tipo de tráfico nunca será eliminado. Sin embargo, cuando el equipo Windows funciona como servidor DHCP, entonces hay que configurar manualmente el cortafuegos para permitir la recepción de solicitudes y el envío de respuestas. Las Figuras 1.27 y 1.28 muestran cómo configurar el cortafuegos de Windows 7 para permitir el funcionamiento del servidor DHCP DualServer.

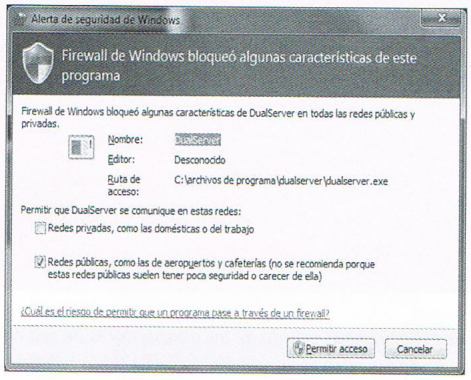


Figura 1.27. *Ventana de alerta de seguridad en Windows 7. Cuando se intenta iniciar la ejecución de DualServer, el sistema informa que este servicio está bloqueado por defecto por el cortafuegos. Se puede desbloquear si se pulsa el botón "Permitir acceso"*

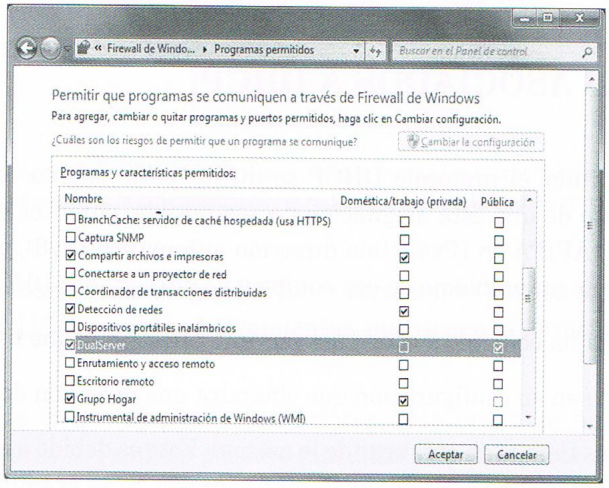


Figura 1.28. *Configuración del cortafuegos en Windows 7. En esta ventana se muestra una lista de los servicios disponibles en el equipo y si su uso está permitido por el cortafuegos las casillas de verificación están activadas para los servicios permitidos*

Por su parte, la configuración del cortafuegos en un cliente DHCP con GNU/Linux también requiere que este servicio esté permitido. Por defecto, cualquier instalación de Linux incluirá la correspondiente aceptación de este servicio, incluso será mucho más restrictivo de lo necesario. En caso de que el cortafuegos no permita el tráfico de peticiones del cliente DHCP, es necesario ejecutar esta orden como usuario *root* para permitir la comunicación DHCP (que se realiza a través de los puertos 67 y 68 mediante el protocolo UDP):

```
#iptables  -I INPUT -i eth0 -p udp --dport 67:68 \
--sport 67:68 -j ACCEPT
```

1.5.2 PROBLEMAS CON MICROSOFT WINDOWS VISTA/7

En general, los equipos con Microsoft Windows están preparados para funcionar como clientes DHCP por defecto, sin necesidad de realizar operaciones adicionales ni instalar nuevos programas. También pueden funcionar como servidores DHCP, siempre que se instale en ellos el programa gestor adecuado (véase el apartado 1.3.1).

Sin embargo, es cierto que algunas versiones de Microsoft Windows han experimentado algunos problemas con el funcionamiento del cliente DHCP. Estos problemas afectan, sobre todo, a las versiones Vista y 7 y, probablemente, serán solucionados en posteriores desarrollos de los Service Pack correspondientes o en actualizaciones en línea.

En concreto el problema detectado con Windows Vista/7 tiene que ver con la forma en la que solicita su configuración por DHCP y en el comportamiento que tiene el servidor. Si el servidor tiene reservada una dirección IP concreta para ese equipo (identificado por su dirección MAC), éste último nunca obtendrá la dirección reservada, sino que obtendrá una dirección del conjunto que el servidor asigna libremente.

Para cambiar este comportamiento por defecto de Windows Vista/7 hay que seguir estos pasos:

1. Abrir el editor del registro del sistema, escribiendo "regedit" en el cuadro de texto de búsqueda del menú de inicio.

2. Si has iniciado sesión como usuario sin privilegios de administrador, el sistema solicitará una cuenta y contraseña de administrador.

3. Buscar la siguiente clave del registro:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\Tcpip\Parameters\Interfaces\{GUID}
```

4. Pulsar con el botón derecho sobre la entrada "DhcpConnForceBroadcastFlag" y seleccionar "Modificar...".

5. En el campo "Información del valor", cambiar el valor "0" por "1" y pulsar el botón "Aceptar".

6. Cerrar el editor del registro y reiniciar el equipo para que los cambios tengan efecto.

RESUMEN DEL CAPÍTULO

Todos los equipos que se conectan a una red de comunicación basada en la arquitectura TCP/IP necesitan tener asignada una configuración que incluya una dirección única para identificarlos en ella. Muchos usuarios carecen de conocimientos avanzados en informática, por lo que no conocen los mecanismos que se utilizan a la hora de asignar la configuración a los equipos de una red. Estos mecanismos pueden complicarse mucho más cuando en la red coexisten direcciones IPv4 con direcciones IPv6.

Los equipos de una red pueden obtener su configuración a través de diferentes mecanismos:

- **Configuración manual**: consiste en asignar la configuración de red a cada equipo, de forma que ésta no variará mientras que no se cambie. A esta configuración también se le llama estática.
- **Configuración predeterminada**: consiste en asignar la configuración mediante un servidor DHCP que ya conoce los parámetros correctos.
- **Configuración automática**: es el propio equipo el que decide qué configuración de red va a utilizar, en ausencia de los mecanismos de asignación anteriores. Si se utilizan asignaciones IPv4, el mecanismo de autoconfiguración se llama APIPA, mientras que si se utiliza IPv6, el mecanismo se basa en la consulta de los parámetros utilizados en el pasado o la información que facilitan los encaminadores de la red.

El protocolo DHCP funciona en base al modelo cliente-servidor, de forma que los equipos que desean obtener su configuración de forma automática (clientes) consultan a los servidores para que se la faciliten. Puesto que los clientes no saben cuáles son los parámetros que utiliza la red, envían siempre sus peticiones a las direcciones de difusión 255.255.255.255, que son atendidas por los servidores. Los servidores, por su parte, mantienen, además de los parámetros de configuración de la red que tienen que facilitar, una tabla actualizada con las direcciones IP que se encuentran asignadas y las direcciones libres.

El funcionamiento del servicio DHCP en una red no debe verse afectado por las características de los equipos conectados a ella, el sistema operativo utilizado o la tecnología en que se basan. Esto debe ser así ya que el protocolo DHCP es abierto y está definido formalmente en documentos que se consideran estándares (fundamentalmente, RFC 1531).

Un equipo con Microsoft Windows puede funcionar como servidor DHCP si tiene instalado el paquete necesario. En las versiones de servidor (Windows 2000 Server, Server 2003 y Server 2008), este paquete se incluye por defecto con los discos de instalación que proporciona el fabricante. En versiones de cliente, será necesario instalar paquetes de otros fabricantes para disponer de esta funcionalidad (como, por ejemplo, Dual Server).

En los sistemas GNU/Linux, la mayoría de las distribuciones incluyen los paquetes de servidor DHCP. Dependiendo de la distribución y versión, estos paquetes se pueden llamar *dhcp3-server*, *dhcp-server*, *dhcpd*, etc. Estos paquetes contienen, por un lado, el proceso demonio que atiende las peticiones y contesta con las configuraciones y, por otro, los archivos de configuración necesarios.

La configuración de un cliente DHCP no requiere de la instalación de paquetes adicionales, ya que la mayoría de sistemas operativos ya instalan por defecto todo lo necesario. La configuración también resulta bastante sencilla, ya que no es necesario especificar ningún parámetro, simplemente se va a obtener la configuración por DHCP. Es posible especificar una configuración de red manual que el equipo va a utilizar en caso de que no le sea posible obtenerla por DHCP.

También existen una serie de herramientas que permiten comprobar si la configuración de red ha sido obtenida correctamente por DHCP. En los sistemas Microsoft Windows se utiliza el *Centro de redes y recursos compartidos*, además de las órdenes *netsh*, *ipconfig* y *ping*. En los sistemas GNU/Linux se usan las órdenes *ifconfig*, *route*, *ip* y *ping*.

El funcionamiento incorrecto del servicio DHCP puede ser debido a:

- Problemas de funcionamiento o configuración de la red.
- Filtrado de alguno de los cortafuegos.
- Problemas de configuración de los equipos.

EJERCICIOS PROPUESTOS

- **1.** Imagina que deseas configurar un equipo Linux como servidor DHCP de la red. Supón que tienes tres equipos cuyas direcciones MAC son 00:E0:29:64:6A:F1, 00:E0:29:64:6A:F2 y 00:E0:29:64:6A:F3, y que se desea asignar la dirección IP 192.168.0.0/16. Enumera todos los pasos que debes realizar, teniendo en cuenta que el servicio *dhcp* no está instalado en el equipo.
- **2.** Realiza el ejercicio anterior pero esta vez utiliza un equipo Microsoft Windows. Comprueba qué ocurre si mantienes funcionando los dos servidores DHCP en la misma red.
- **3.** ¿Cuáles son los parámetros de red que puede obtener un cliente de un servidor DHCP?
- **4.** Utiliza un programa que capture el tráfico de la red para obtener los mensajes que se envían un cliente y un servidor DHCP cuando el primero arranca y solicita la configuración de red. Dibuja un esquema con los mensajes enviados.
- **5.** Si dispones de conexión a Internet a través de un encaminador, accede a su configuración para comprobar si éste funciona o puede funcionar como servidor DHCP.
- **6.** Indica los pasos a seguir para realizar la configuración de alto nivel de un cliente DHCP en Linux.
- **7.** ¿Cómo puedes averiguar si un equipo ha obtenido su configuración de red por DHCP sin necesidad de acceder a a las ventanas o archivos de configuración?
- **8.** Cuando un equipo envía una petición para obtener su configuración de red, ésta puede ser recibida por varios servidores DHCP a la vez. ¿Qué control se lleva a cabo para evitar que al equipo se le reserve más de una dirección IP a la vez?

TEST DE CONOCIMIENTOS

1 La configuración automática IPv6:
a) Se obtiene siempre desde un servidor DHCPv6.
b) Se puede generar exclusivamente en base a la información de que dispone el propio equipo.
c) Se basa en el uso de APIPA.
d) Ninguna es cierta.

2 Un parámetro de red que no se envía por DHCP es:
a) Máscara de red.
b) Nombre del dominio.
c) Rango de direcciones a asignar.
d) b y c son ciertas.

3 La asignación de una dirección por el mecanismo APIPA se realiza cuando:
a) La asignación actual ha caducado.
b) Uno de los servidores DHCP de la red está sobrecargado.
c) Ningún servidor DHCP ha contestado a la solicitud de configuración.
d) a y b son ciertas.

4 Un servidor DHCP:
a) No puede funcionar si tiene Windows Vista/7.
b) No puede funcionar si tiene asignada una dirección automática.
c) No es compatible con equipos Windows si lleva GNU/Linux.
d) Necesita de la existencia de un servidor DNS.

5 Un equipo GNU/Linux podrá funcionar como servidor DHCP si:
a) Tiene asignada una dirección IP estática.
b) El núcleo es capaz de enviar mensajes de difusión.
c) El proceso demonio del servidor DHCP está en ejecución.
d) Todas son ciertas.

6 Cuando un servidor envía un mensaje *DHCPNACK* es debido a que:
a) Está demasiado ocupado atendiendo peticiones.
b) La solicitud de dirección que ha recibido es incorrecta.
c) El cliente ya ha sobrepasado el tiempo de asignación de la dirección.
d) Ninguna es cierta.

7 La declaración *host* en el archivo *dhcpd.conf* se usa para:
a) Especificar el rango de direcciones a asignar.
b) Definir conjuntos de equipos con diferentes configuraciones.
c) Especificar una dirección reservada a un equipo concreto.
d) Definir la subred a la que pertenecen los equipos.

8 El archivo *dhcpd.leases* contiene:
a) Todas las direcciones que el servidor ha asignado desde que está funcionando.
b) Todas las direcciones que están asignadas actualmente.
c) El rango de direcciones asignado por el servidor.
d) Ninguna es cierta.

9 Un cliente solicita su configuración por DHCP a la dirección:
a) Del servidor DHCP.
b) De todos los equipos encendidos que hay en la red.
c) De todos los equipos posibles que hay en la red.
d) Ninguna es cierta.

2 Sistema de nombres de dominio

OBJETIVOS DEL CAPÍTULO

- ✓ Identificar y describir los escenarios en los que surge la necesidad de un servicio de resolución de nombres.
- ✓ Clasificar los principales mecanismos de resolución de nombres.
- ✓ Describir la estructura, nomenclatura y funcionalidad de los sistemas de nombres jerárquicos.
- ✓ Instalar un servicio jerárquico de resolución de nombres en los sistemas operativos Microsoft Windows y Linux.
- ✓ Preparar el servicio para almacenar las respuestas procedentes de servidores de redes públicas y servirlas a los equipos de la red local.
- ✓ Añadir registros de nombres correspondientes a una zona nueva, con opciones relativas a servidores de correo y alias.
- ✓ Realizar transferencias de zona entre dos o más servidores.
- ✓ Comprobar el funcionamiento correcto del servidor y corregir problemas.

A los usuarios de Internet les resulta complicado trabajar con direcciones de transporte (un *conector* IPv4, por ejemplo *15.234.88.126:80* o, peor todavía, uno IPv6, como *[2001:4898::1002:20f:1fff:feff:b3a3]:80*), sobre todo porque son difíciles de recordar. A las personas nos cuesta mucho menos trabajo recordar un nombre o una palabra, puesto que nuestro cerebro está más acostumbrado a manejar el lenguaje de las palabras. Dado que no existen direcciones de nivel de aplicación de la arquitectura de red, Paul Mockapetris definió en 1986 el protocolo **DNS** (*Domain Name System* o Sistema de Nombres de Dominio). Éste se encarga de definir **direcciones de dominio** formadas por cadenas de caracteres (como, por ejemplo, *www.fsf.org*) y de convertirlas automáticamente en direcciones binarias de transporte. Mediante este sistema es posible identificar usuarios y equipos en la red con nombres, sin necesidad de utilizar engorrosas direcciones numéricas.

Gracias al uso de las direcciones de dominio, también conocidas como **URL** (*Universal Resource Locator* o Localizados Universal de Recursos) o **URI** (*Uniform Resource Identifier* o Identificador Uniforme de Recursos), los complejos formatos de direcciones IP en las versiones 4 y 6 quedan completamente ocultos a los usuarios, que pueden incluso desconocer su existencia aunque trabajen con sus equipos en red.

2.1 INTRODUCCIÓN

Las direcciones de dominio forman una clasificación jerárquica de nombres separados por puntos. A un nivel superior, se encuentran los **nombres genéricos** (también llamados *nombres de primer nivel*), que son de dos tipos: genéricos y de país. Junto a estos nombres genéricos aparece el nombre distintivo de la organización (*nombre de segundo nivel*). Dentro de la organización pueden definirse subdominios, de forma que también hay que especificarlos. Finalmente, a un nivel inferior se especifica el nombre asignado al equipo. Por ejemplo, una dirección completa de dominio puede ser *www.miweb.com*, siendo *com* el dominio de primer nivel, *miweb* de segundo nivel y *www* es el nombre del equipo. Los nombres genéricos y de país aparecen listados en las tablas 2.1 y 2.2.

Tabla 2.1. Dominios genéricos DNS

Dominio	Significado
com	Comercial.
edu	Instituciones educativas.
gov	Gobierno Federal de Estados Unidos.
int	Organizaciones internacionales.
mil	Fuerzas Armadas de Estados Unidos.
net	Proveedores de servicio de Internet.
org	Organizaciones sin carácter de lucro.

Tabla 2.2. Algunos dominios de países en DNS

Dominio	Significado
ar	Argentina.
es	España.
fr	Francia.
it	Italia.
jp	Japón.
nl	Países Bajos.
ru	Federación Rusa.

Los dominios genéricos se encuentran en el nivel más alto de la jerarquía y los nombres completos de dominio se van construyendo de derecha a izquierda. En la parte más a la izquierda se especifica el nombre de la máquina (suele ser corriente nombrar la máquina utilizando el tipo de servicio sobre el que trabaja, como *www*, *ftp*, etc., de forma que resulta más sencillo identificar el equipo). El ejemplo 2.1 muestra algunos casos de nombres de dominio completos. Hay que tener en cuenta que la división jerárquica en dominios para nombrar equipos puede no seguir la estructura física de la red subyacente, de forma que pueden existir equipos dentro del mismo segmento o subred que pertenezcan a subdominios distintos.

EJEMPLO 2.1

Supongamos que tenemos la organización jerárquica de nombres de dominio que aparece en la Figura 2.1.

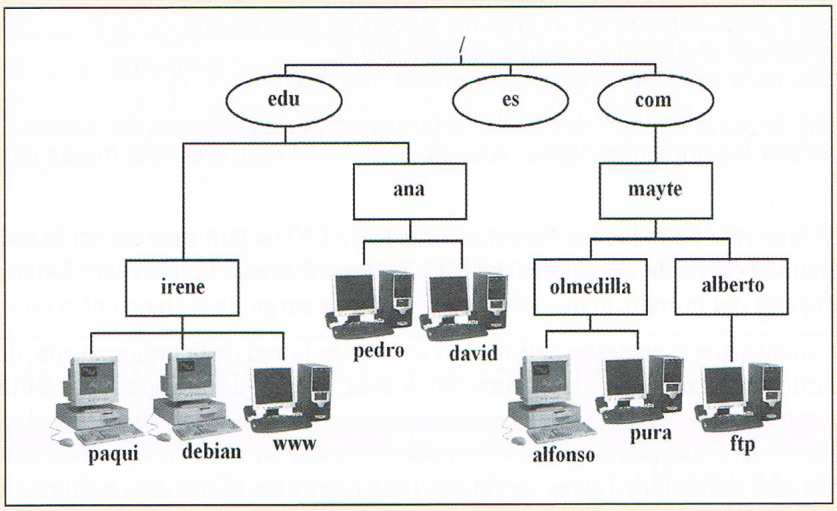


Figura 2.1. *Ejemplo de jerarquía de nombres de dominio. Los dominios de primer nivel se han representado mediante elipses, mientras que los dominios de segundo nivel y subdominios se han representado utilizando rectángulos*

Según la Figura 2.1, tenemos los siguientes nombres de dominio para los equipos:

```
paqui.irene.edu
debian.irene.edu
www.irene.edu
pedro.ana.edu
david.ana.edu
afonso.olmedilla.mayte.com
pura.olmedilla.mayte.com
ftp.alberto.mayte.com
```

A las direcciones completas de dominio se les llama **nombres totalmente cualificados** o **FQDN** (*Fully Qualified Domain Name*), y son absolutas porque especifican la ruta completa en la jerarquía hasta llegar al elemento. Cada equipo de la red tendrá un único nombre FQDN (aunque tenga más de un adaptador de red instalado). Por su parte, un **dominio** está formado por el espacio de nombres que comparten el mismo dominio de primer nivel y segundo nivel (es decir, todos los nombres que hay por debajo de un dominio de segundo nivel en la jerarquía).

Como se ha mencionado anteriormente, el sistema de nombres de dominio también permite identificar usuarios. Para ello, solamente hay que añadir su nombre en la parte izquierda de la dirección seguido del carácter "@". Siguiendo el ejemplo 2.1, podría existir un usuario llamado *ines@debian.irene.edu*.

La pregunta que surge ahora es: *¿dónde se guarda la información relativa a la organización interna de los dominios?* El modelo del DNS distribuye la información relativa a los dominios en servidores DNS de la red. Esta información almacenada constituye una **zona**, que está definida por un conjunto de dominios y/o subdominios. Esto significa que la zona *tiene autoridad sobre el dominio*, es decir, es la zona la que guarda la información relativa a la organización del dominio. Normalmente las zonas se guardan como una base de datos en determinados servidores DNS, desde donde es posible gestionarlas. El ejemplo 2.2 aclara todos estos conceptos.

EJEMPLO 2.2

Siguiendo con la estructura de la Figura 2.1, tenemos:

- *paqui*, *debian* y *www* pertenecen al dominio *irene.edu*.
- *pedro* y *david* pertenecen al dominio *ana.edu*.
- *alfonso* y *pura* pertenecen al dominio *olmedilla.mayte.com*.
- *ftp* pertenece al dominio *Alberto.mayte.com*.
- *alfonso*, *pura* y *ftp* pertenecen al dominio *mayte.com*.

La configuración de zonas puede diferir de la jerarquía por cuestiones de administración. En el ejemplo podríamos encontrar las siguientes zonas: *edu*, *es*, *com*, *irene.edu*, *ana.edu*, *mayte.com*, *alberto.mayte.com*.

La zona definida como raíz de todos los dominios de internet "/" (según aparece en la estructura de ejemplo de la Figura 2.1) está gestionada en varios servidores del ISC (*Internet Systems Consotium*). Estos servidores se encuentran ubicados en varios lugares del mundo, lo que permite repartir la carga de trabajo entre ellos.

Hay que tener en cuenta que si se desea definir una zona para la red de la organización, deberá existir al menos un servidor DNS que guarde la información de configuración de ésta. En caso de que no se defina ninguna zona, los servidores DNS existentes funcionarán como *caché de nombres exclusivamente*. Esto quiere decir que el servidor no define ninguna zona y se limita solamente a recibir peticiones de los equipos y buscar en su caché para ver si las puede resolver. Si no las puede resolver, reenvía esas solicitudes a otros servidores DNS conocidos. El uso de servidores de caché de nombres puede acelerar el acceso a una red de área extensa, ya que la resolución de nombres es mucho más rápida.

Se entiende por *caché* una tabla local de tamaño fijo que almacena correspondencias ya resueltas que se van eliminando conforme quedan anticuadas.

El establecimiento de las zonas de los dominios se basa en gran medida en cuestiones relativas al tamaño de la organización y subdominios definidos, velocidad de los enlaces que comunican los servidores DNS, tasa de tráfico esperada entre ellos, etc. Por estas razones, en muchas organizaciones grandes suele ser complicado establecer criterios concretos para la división en zonas.

EJEMPLO 2.3

Como se ha mencionado anteriormente, el concepto de *zona* y *dominio* son distintos, aunque normalmente suele coincidir una zona con un dominio. Sin embargo, puede ocurrir que una zona pueda contener varios dominios o un dominio distribuirse en varias zonas. Un ejemplo del primer caso aparece en la Figura 2.2.

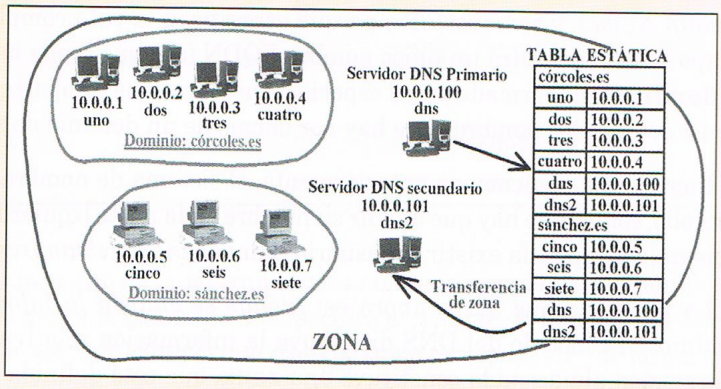


Figura 2.2. *Zona formada por varios dominios. Los dominios están definidos por la autoridad del servidor DNS primario llamado dns. En esta figura no aparece la topología física de la red porque no resulta relevante a nivel de dominios*

La información de zona está estructurada en forma de **registros de recursos** (RR), cuyos tipos aparecen expuestos en la tabla 2.3. Estos registros de recursos son entradas como las mostradas en la tabla estática de la Figura 2.2, donde se especifican las direcciones IP y los nombres de los equipos que forman el dominio. Sin embargo, en las situaciones reales, se suele incluir más información sobre un dominio (equipos que tienen más de un nombre, servidores de correo, etc.).

En algunas situaciones (como, por ejemplo, un dominio grande), puede resultar conveniente crear un subdominio en una zona distinta a la que se encuentra el dominio padre (como ocurre en el ejemplo 2.2 con el subdominio *alberto.mayte.com*). Será la zona que contiene el dominio padre la que autorice y delegue el control a la nueva zona para que gestione el subdominio de forma autónoma.

El formato de los registros de recursos y la información que contienen se explica en el apartado 2.4, donde se detalla cómo instalar y configurar un servidor DNS en Microsoft Windows y Linux.

Tabla 2.3. Tipos de registros de zona en los servidores DNS

Tipo	Descripción
A	Asocia un nombre de dominio de equipo con su dirección IP. Es el registro más utilizado.
AAAA	Asocia un nombre de dominio de equipo con su dirección IPv6 completa de 128 bits. Su nombre proviene de los registros A para IPv4, pero las direcciones IPv6 son cuatro veces más grandes.
A6	Otro registro que asocia un nombre de equipo con su dirección IPv6, pero especifica direcciones fragmentadas.
CNAME	Se utiliza para asignar otro nombre (alias) de un nombre de dominio de equipo.
HINFO	Guarda información adicional de un equipo, como el tipo de CPU que lleva o el sistema operativo instalado. No se recomienda utilizar este tipo de registro por cuestiones de seguridad en la red.
MX	Registra un servidor de correo.
NS	Es una referencia a los nombres de dominios DNS de servidores que tienen autoridad para una zona, es decir, guardan la información de los dominios de esa zona.
PTR	Asigna una dirección IP a un nombre de dominio para llevar a cabo correspondencias inversas (se verá más adelante en este apartado).
SOA	Es el primer registro o punto de partida que se crea cuando se agrega una nueva zona. Se usa para informar que el equipo especificado es el que guarda la información del dominio, es decir, la autoridad para la zona.
TXT	Se trata de un registro definido para guardar información de tipo texto que cualquier usuario puede leer. Actualmente, como especifica el RFC 1464, se utiliza para guardar otro tipo de información distinta a nombres de equipos o direcciones y que pueda resultar útil de consultar.

Hasta la fecha no existe consenso en cuanto al uso de registros *AAAA* o *A6* y muchos especialistas recomiendan que se utilicen los dos. Un registro *AAAA* especifica una dirección IPv6 completa (al igual que un registro *A* especifica una dirección IPv4 completa), por lo que si hay modificaciones en la red, los administradores tendrán que cambiarlos y actualizarlos. Este tipo de registros se han utilizado sin problemas desde los inicios de IPv6 en 1996. Un registro *A6* puede especificar una dirección incompleta, que se refiere a varios equipos a la vez o incluso direcciones que cambian. Cuando se realiza una consulta de un registro *A6* incompleto, es necesario resolverlo en varias consultas recursivas hasta obtener toda la dirección, por lo que la resolución puede tardar mucho más tiempo. BIND 9.x soporta registros *AAAA* y *A6*, mientras que las versiones anteriores solo soportan registros de tipo *AAAA*. En los RFC 3363 y RFC 3364 se comparan estos dos tipos de registros y se recomienda usar los registros *AAAA*, hasta que los registros *A6* incompletos hayan sido probados más exhaustivamente.

La base de datos de una zona está almacenada en un **servidor DNS primario**, de forma que todos los dominios que contiene ésta se gestionan desde el equipo. Sin embargo, no resulta conveniente mantener un único servidor primario para la zona, ya que en caso de fallo no se podrán resolver esas direcciones. Por lo tanto, en la organización también se pueden configurar uno o más **servidores DNS secundarios**, que se encargan de mantener copias actualizadas de la información de zona. La actualización se realiza mediante volcados totales o parciales de la información de zona, llamados **transferencias de zona**. Las transferencias parciales se llaman **transferencias de zona incrementales**, y a veces se utilizan con el propósito de reducir la cantidad de información que se transmite por la red. Así mismo, los servidores DNS primarios pueden notificar a los secundarios que se ha producido una modificación en la zona, con el fin de que actualicen sus informaciones de zona lo antes posible.

El protocolo DNS se define en los estándares RFC 1034 y 1035. Éste utiliza una base de datos distribuida por la red en ordenadores llamados *servidores DNS*, que almacenan tablas de correspondencias entre direcciones de nombres de dominio y direcciones IP. Cuando una estación desea establecer una conexión con una dirección DNS, llama a la rutina del sistema o **resolvedor** que primero comprueba si puede obtener la dirección IP a través de una tabla local o almacenada de forma temporal de una consulta anterior. Si no la encuentra en esa tabla, envía un mensaje con el protocolo UDP a la dirección del servidor DNS que tenga configurado por defecto (normalmente el más próximo). Este servidor consulta primero en sus registros de recursos de zona la dirección solicitada (en caso de ser un servidor primario o secundario) y devuelve la dirección IP si la encuentra. Si no la encuentra ahí, consultará entonces la tabla local donde están almacenadas temporalmente consultas anteriores. En caso de que tampoco la encuentre ahí, puede consultar otros servidores DNS, operación que se denomina **consulta recursiva** (véase la Figura 2.3). Finalmente, el resolvedor devuelve la dirección IP solicitada a la estación.

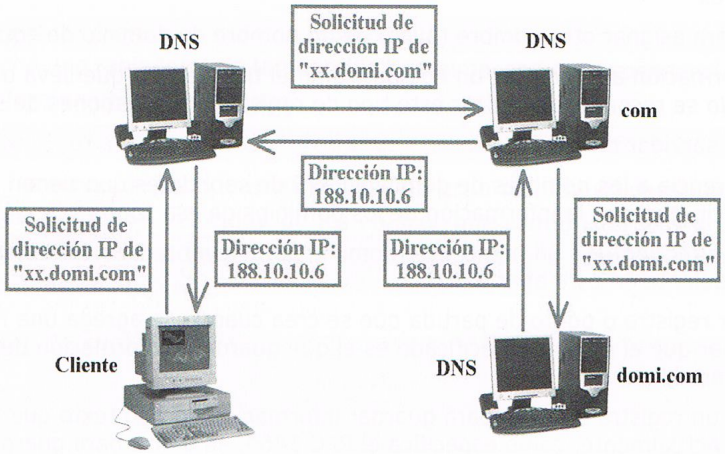


Figura 2.3. *Ejemplo de resolución recursiva a través del DNS. El cliente envía la solicitud de resolución al servidor DNS cuya dirección conoce. Éste no puede establecer la correspondencia, por lo que la pasará al servidor de nombres raíz ".", puesto que no conoce la dirección IP del servidor de la zona domi.com. El servidor raíz conoce la dirección del servidor de zona com, por lo que le envía la petición para que la resuelva. El proceso continúa hasta que el servidor DNS domi.com puede establecer la correspondencia, que es enviada de nuevo por el mismo camino por el que llegó*

Dependiendo del sistema operativo instalado, la tabla local puede estar almacenada en distintos directorios del disco duro. Por ejemplo, muchas distribuciones de Linux guardan esta tabla en el archivo */etc/hosts* y, en todos los casos, se pueden incluir entradas manualmente con direcciones de equipos bien conocidos. En la mayoría de estas tablas suele aparecer la entrada que se refiere al equipo local, como puede ser "127.0.0.1 localhost".

Los servidores DNS son capaces de resolver **correspondencias directas**, es decir, recibida una dirección de nombre, estos devuelven la dirección IP asociada (éstas son las operaciones de resolución normales y, de hecho, eran las únicas aceptadas en las primeras versiones del protocolo DNS). Así mismo, también son capaces de resolver

correspondencias inversas, devolviendo una dirección de nombre cuando reciben una solicitud con una dirección IP. Las resoluciones inversas se utilizan en situaciones determinadas, por ejemplo, cuando un servidor DNS ha solicitado una resolución directa a otro y, por seguridad, quiere comprobar que esa correspondencia es correcta.

El problema que plantean las resoluciones inversas es que, conforme se ha organizado el espacio de nombres de los dominios y estos en las zonas, estas consultas deben hacer una búsqueda en todos los dominios de la red. De este modo, las consultas inversas tardarían demasiado tiempo en resolverse. Para solucionar este problema, en el estándar de DNS se ha reservado el dominio especial *in-addr.arpa* (funciona con IPv4) o *ip6.arpa* (funciona sobre IPv6), que debe definirse en una zona tantas veces como dominios existan en ella. Para crear zonas de resolución inversa IPv6, se pueden usar los dominios reservados *ip6.arpa* o *ip6.int*, aunque el RFC 3152 declara obsoleto el uso del dominio *ip6.int*.

A diferencia de los dominios del DNS, los dominios *in-addr.arpa* (IPv4) o *ip6.arpa* (IPV6), están definidos por todos los subdominios *en orden inverso*, junto con su dirección IP asociada (también aparecen los octetos en orden inverso, ya que el nombre de un dominio se lee al revés a una dirección IP). Los registros que guardan estas correspondencias inversas son **punteros de registros de recursos** (*PTR*). Es posible que la herramienta de administración del servidor DNS cree automáticamente las resoluciones inversas, aunque a veces hay que establecerlas manualmente.

Con el fin de facilitar la administración de zonas en los servidores DNS, algunos sistemas operativos para estaciones cliente permiten la **actualización dinámica**. Ésta consiste en que la estación cliente notifica de forma automática al servidor DNS cualquier cambio en su dirección IP o nombre de dominio. Así, el administrador de la zona no tendrá que configurar ese nuevo registro en el servidor, ya que éste lo hará automáticamente cuando reciba la notificación de la estación cliente.

Cuando un determinado dominio aumenta de tamaño e incluye una gran cantidad de subdominios asociados, puede resultar demasiado complejo mantener un único servidor DNS primario para esa zona. En su lugar, se pueden crear **zonas de delegación**, que permiten llevar algunos de esos subdominios a otros servidores DNS primarios. De esta forma, cada servidor DNS primario va a funcionar como autoridad para una parte del dominio.

La configuración de un servidor DNS se encuentra definida en el RFC 1033. En el apartado 2.4 se explica con detalle la configuración de los servidores del protocolo DNS para los sistemas Microsoft Windows y Linux, mientras que la configuración de los clientes se explica en el apartado 2.5. Hay que tener en cuenta que, aunque las implementaciones de los servicios DNS se basan en las especificaciones estándares incluidas en los documentos RFC, es posible que surjan ciertas incompatibilidades entre los servidores DNS de Linux y servidores DNS implementados en otros sistemas operativos, sobre todo en versiones antiguas.

2.2 REGISTRO DE UN DOMINIO EN INTERNET

Cuando se configura un dominio en una red local y se establecen los nombres de los equipos, ésta organización puede permanecer oculta dentro del ámbito de esa red o puede difundirse a Internet para que el dominio sea conocido en el exterior.

Si el dominio va a ser visible en Internet, existe un mecanismo de reserva y asignación de dominios para evitar que se dupliquen, de la misma forma que se realizan las asignaciones de direcciones IPv4 e IPv6. El ICANN es el organismo encargado de acreditar a las empresas para que ofrezcan servicios de registro único de dominios. Estas empresas acreditadas, también denominadas *registradores de dominios*, son las que habitualmente reservan nombres de dominios a otras empresas o particulares, a cambio de una cantidad económica que puede hacerse efectiva de una

vez o mediante cuotas mensuales o anuales. En el RFC 1032 se especifica cómo registrar un nombre de dominio en Internet e incluye los formularios que son necesarios.

Si el dominio va a permanecer oculto dentro del ámbito de la red local, entonces no es necesario reservar ningún nombre de dominio de Internet, simplemente se puede utilizar el que se desee (incluso aquellos que se encuentren reservados en Internet). Hay que tener en cuenta que este dominio solamente puede ser utilizado dentro del ámbito de la red local, nunca será visible desde cualquier otra red.

Una **empresa de registro de dominios** o **registrador** es aquella que vende dominios de Internet, ya sea ".com", ".es", ".org", etc. El precio de reserva de estos dominios se paga normalmente a través de una cuota anual, que puede variar mucho de unas empresas a otras. Se recomienda mirar la letra pequeña, porque un dominio barato se puede encarecer al contratar servicios adicionales que resultan imprescindibles (como la redirección a una dirección, un servidor DNS, etc.).

Cuando se registra un dominio en Internet, también se puede contratar con la empresa proveedora un servicio DNS, de forma que éste puede ser gestionado para añadir o eliminar registros a ese dominio. En ese caso, puede no ser necesario instalar un servidor DNS en la red, aunque solamente se podrán asignar nombres a direcciones IP públicas (que no sean NAT).

2.3 CUESTIONES RELATIVAS A LA SEGURIDAD

El correcto funcinamiento del servicio DNS resulta crítico dentro del ámbito de Internet. Si este servicio falla o se interrumpe, los usuarios no podrán conectar con los servidores de Internet, puesto que no conocen sus direcciones IPv4 o IPv6 asociadas. Además, debe ser completamente seguro, para evitar los sabotajes y la suplantación de direcciones. Cuando un usuario envía una petición de resolución, tiene que tener la garantía de que la dirección que obtenga es la auténtica, porque eso puede comprometer su propia seguridad. Por ejemplo, si se conecta a un servidor de su sucursal bancaria para realizar alguna operación, debe tener la certeza de que no está accediendo a un servidor fraudulento que está suplantando la identidad del banco oficial. En el pasado, han sido muy populares los casos en los que se ha saboteado algún servidor DNS para suplantar servidores de organismos oficiales y empresas multinacionales por servidores de contenido pornográfico y de otra índole.

Para evitar todos estos problemas, los servidores DNS establecen relaciones de confianza entre ellos, utilizando técnicas de cifrado y autenticación para realizar transferencias de zona y consultas recursivas. Estas técnicas se incluyen en el **DNSSEC** (*Domain Name System Security Extensions* o Extensiones de Seguridad del Sistema de Nombres de Dominio), definido formalmente en el RFC 2535 o Active Directory, exclusivamente para los sistemas Microsoft Windows.

2.4 CONFIGURACIÓN DE UN SERVIDOR DNS

En una red local de pequeñas dimensiones se puede prescindir de un servidor DNS que resuelva los nombres y las direcciones IP. Los equipos pueden configurarse para enviar peticiones a otros servidores DNS que están disponibles en Internet. Sin embargo, cuando en la red local se utilizan direcciones privadas (NAT) y existen equipos que tienen que ofrecer una serie de servicios (por ejemplo, un servidor de páginas *web*, correo electrónico, autenticación de usuarios, etc.), entonces puede ser necesario disponer de un equipo que resuelva las direcciones. Si en estas condiciones no existe un servidor DNS en la red, entonces los usuarios tienen que utilizar directamente direcciones IPv4 (o peor, ¡direcciones IPv6!) o los administradores tienen que mantener tablas de correspondencias en todos los equipos. Mantener tablas de correspondencias en todos los equipos no es factible porque un cambio de dirección de un servidor requiere actualizar las tablas de todos los equipos de la red.

La instalación y configuración de un servidor DNS resulta mucho más compleja que otros servicios, como DHCP debido, sobre todo, a que los estándares asociados también son muy complejos y requieren de la creación de una serie de registros asociados (véase la introducción de este capítulo). Hay que tener en cuenta que un servidor DNS se puede configurar como maestro para la zona, secundario, solo caché, etc. En caso de que sea servidor de zona, hay que crear las tablas de correspondencias directas e inversas, además de otros muchos parámetros de configuración.

En los apartados siguientes se incluye la instalación y configuración del servicio DNS en una red local para los sistemas operativos Microsoft Windows y Linux.

2.4.1 INSTALACIÓN EN MICROSOFT WINDOWS

Al igual que ocurre con otros servicios, para que un equipo con Microsoft Windows funcione como servidor DNS, necesita de un programa que se encuentre en ejecución durante todo el tiempo (proceso demonio) y que atienda las peticiones que se reciben a través de la red. Este programa se puede obtener directamente de Microsoft, que lo incluye en algunas versiones de sus sistemas operativos o se puede obtener de otros fabricantes, ya sea con licencia libre o propietaria.

Microsoft distribuye un paquete de servidor DNS en todas sus versiones de Windows Server, lo que permite a estos equipos configurar los clientes en la red. En otras versiones de Windows orientadas más a equipos que van a funcionar como estaciones de trabajo, como Windows XP/Vista/7, Microsoft no ofrece paquetes de servidor, aunque se pueden instalar herramientas como el Pack de Herramientas de Administración del Servidor (*ADMINPACK.MSI*) para Windows 2000/XP o las Herramientas de Administración Remota del Servidor para Windows 7, que permiten gestionar un servidor DNS desde un equipo cliente. Si se desea configurar Windows 2000/XP/Vista/7 como servidor DHCP, se pueden instalar paquetes de otros fabricantes que permiten esta funcionalidad.

2.4.1.1 Windows Server 2008

Los sistemas operativos Microsoft Windows Server 2008 incluyen todos los paquetes necesarios para permitir que el equipo se comporte como un servidor DNS. Sin embargo, estos paquetes no se incluyen en una instalación por defecto del sistema operativo, sino que hay que instalarlos posteriormente.

EJEMPLO 2.4

Veamos los pasos a seguir para instalar un equipo con Windows Server 2008 como servidor DNS:

1. Acceder a la herramienta de administración del servidor desde "Inicio || Herramientas administrativas || Administración del servidor". En el árbol de iconos de la izquierda, seleccionar "Administrador del servidor || Funciones". Aquí se muestra una ventana con todas las funciones instaladas en el servidor.
2. Pulsar en el enlace "Agregar funciones", lo que iniciará la ventana del asistente para añadir nuevas funciones a nuestro servidor. En ese momento, aparecerá la primera ventana del asistente donde se informa que es recomendable comprobar primero si el equipo tiene una configuración correcta. Hay que pulsar en el botón "Siguiente".
3. En la siguiente ventana del asistente se muestra la lista con las funciones que pueden añadirse al servidor. En ella, tenemos que activar la casilla de verificación "Servidor DNS". En caso de que el equipo tenga asignada una dirección IP por DHCP, entonces se mostrará un mensaje advirtiendo de que esta situación no es recomendable, ya que lo mejor es que se le asigne una dirección estática. A continuación, se pulsa en el botón "Siguiente".
4. La siguiente ventana muestra algunos detalles introductorios sobre el funcionamiento del servidor DNS en Windows Server 2008. De nuevo, pulsamos el botón "Siguiente".
5. A continuación, se muestra un resumen sobre la instalación que se va a realizar. Pulsando en el botón "Instalar" se realizará todo lo necesario para que el servicio DNS instale los paquetes necesarios. Si todo funciona como está previsto, deberá aparecer una ventana con el mensaje "Instalación correcta", por lo que podremos pulsar en el botón "Cerrar" para finalizar el asistente. De vuelta a la ventana de administración del equipo, en la ventana "Funciones" deberá aparecer ahora "Servidor DNS".
6. Podemos acceder a la configuración del servidor DNS que acabamos de crear si seleccionamos "Inicio || Herramientas administrativas || DNS". Desde esta herramienta (Figura 2.4) se puede iniciar o detener el servicio y realizar cambios en la configuración por defecto que establece el asistente.

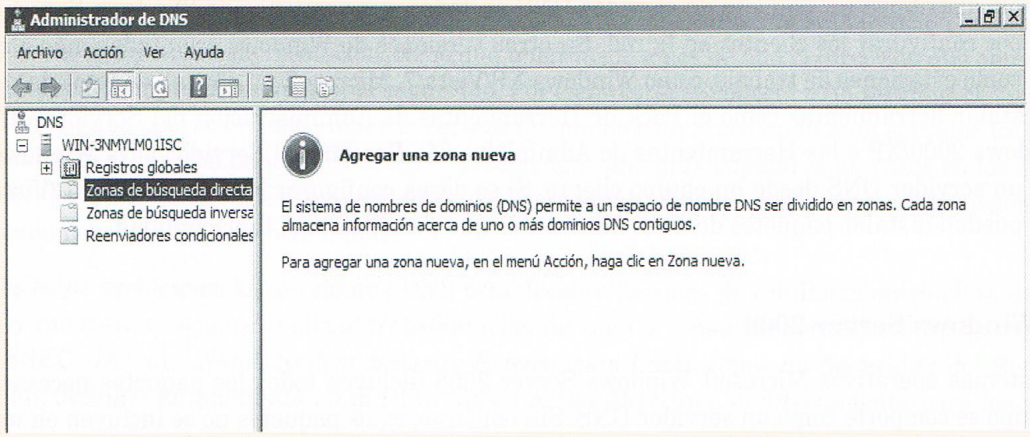


Figura 2.4. *Ventana principal del administrador del servidor DNS en Windows Server 2008. Para cada servidor DNS se muestra un árbol con las zonas de búsqueda directa e inversa definidas en él*

EJEMPLO 2.5

Veamos los pasos a seguir para configurar un equipo con Windows Server 2008 como servidor DNS primario:

1. Suponiendo que hemos seguido los pasos especificados en el ejemplo 2.4 para instalar el servicio DNS, accedemos a la herramieta de configuración, que se encuentra en "Inicio || Herramientas administrativas || DNS".
2. En el árbol de la izquierda, seleccionamos el icono "Zonas de búsqueda directa". Después, en el menú principal de la herramienta, seleccionamos "Acción || Zona nueva...". Esto nos mostrará la ventana principal del asistente para crear una nueva zona. Pulsamos el botón "Siguiente" para pasar a la siguiente ventana.
3. En la siguiente ventana del asistente, se nos pide que seleccionemos el tipo de zona que queremos crear. Ésta puede ser:
   - **Zona principal**: configura el servidor DNS como primario para la zona que vamos a crear.
   - **Zona secundaria**: configura el servidor DNS como secundario para la zona que vamos a crear.
   - **Zona de rutas internas**: configura el servidor DNS para que mantenga una copia de los registros *NS*, es decir, los nombres de los servidores que son autoridad para la zona. Este tipo de servidores resultan muy útiles a la hora de realizar consultas recursivas sin necesidad de que éstas tengan que ser consultadas en el espacio de nombres DNS de Internet.
4. Una vez seleccionado "Zona principal", pulsamos en el botón "Siguiente". Si el equipo funciona como un controlador de dominio de la red Microsoft, entonces aparecerá otra ventana donde se especifica cómo se desea que se repliquen los datos de esta zona en la base de datos de *Active Directory*. Normalmente, se seleccionará la opción "Para todos los servidores DNS de este dominio", de forma que otros servidores que pertenezcan a este dominio pueden obtener transferencias de zona.
5. A continuación, se especifica el nombre del dominio y se pulsa en "Siguiente". Si el equipo no funciona como controlador de dominio, en la siguiente ventana, se especifica el nombre del archivo que va a guardar la información sobre la zona. Tenemos dos opciones:
   - **Crear un archivo nuevo con este nombre de archivo**: crea un archivo nuevo que va a almacenar los registros de la zona.
   - **Usar este archivo**: se utiliza para especificar un archivo de zona que ha sido copiado desde otro servidor DNS. Esta opción resulta muy útil cuando tenemos una copia anterior de los archivos de zona.
6. Una vez especificado el archivo de zona, ya sea uno nuevo o uno existente, pulsamos el botón "Siguiente", lo que mostrará una ventana donde se nos pedirá configurar las actualizaciones dinámicas. Las opciones disponibles son:
   - **Permitir solo actualizaciones dinámicas seguras**: permite que se realicen actualizaciones dinámicas seguras a otros servidores DNS secundarios. Esta opción solo está disponible si el servidor forma parte de un dominio de la red Microsoft.
   - **Permitir todas las actualizaciones dinámicas**: permite que se realicen actualizaciones dinámicas, tanto seguras como no seguras. Esta opción no se recomienda ya que las actualizaciones no seguras pueden registrar información falsa en el DNS.
   - **No admitir actualizaciones dinámicas**: no permite que se realicen actualizaciones dinámicas a servidores esclavos.

7. A no ser que tengamos definido un dominio de la red Microsoft (con *Active Directory*), es recomendable marcar la opción "No admitir actualizaciones dinámicas" a no ser que estemos configurando servidores para pruebas. Pulsamos en el botón "Siguiente" y nos aparecerá una ventana con el resumen de los parámetros que hemos definido para esta zona. Si pulsamos en el botón "Finalizar", se creará la nueva zona con la configuración necesaria.
8. Una vez creada la zona, deberá aparecernos en la parte izquierda de la ventana principal de gestión del DNS, como una rama más del árbol, debajo del icono "Zonas de búsqueda directa". Al pulsar en ella, deberá aparecer una lista con los registros definidos en esta zona. En su creación se definen dos registros por defecto: *SOA* (registro de autoridad) y *NS* (servidor DNS).
9. Antes de comenzar a introducir registros en la zona, es necesario crear la zona de resolución inversa. Para ello, hay que seleccionar el icono "Zonas de búsqueda inversa" del árbol de la parte izquierda en la ventana de administración del servidor DNS y pulsar en la opción del menú principal "Acción || Zona nueva...".
10. En la primera ventana del asistente, pulsamos el botón "Siguiente" y seleccionamos el tipo "Zona principal". De nuevo pulsamos "Siguiente" y nos aparecen dos opciones:
    - **Zona de búsqueda inversa para IPv4**: crea una zona inversa *in-addr.arpa* para resolver direcciones IPv4.
    - **Zona de búsqueda inversa para IPv6**: crea una zona inversa *ip6.arpa* para resolver direcciones IPv6.
11. Seleccionamos "Zona de búsqueda inversa para IPv4" y pulsamos el botón "Siguiente".
12. A continuación, especificamos el nombre del dominio de resolución inversa, que se nos mostrará por defecto según la configuración de red que tenga nuestro servidor en ese momento, como se puestra en la Figura 2.5. Tenemos dos opciones para especificar el nombre del dominio:
    - **Id. de red**: aquí se especifica la parte de la dirección IP que corresponde a la red, sin utilizar el orden inverso. La herramienta convertirá posteriormente esa dirección en el dominio de resolución inverso correspondiente.
    - **Nombre de la zona de búsqueda inversa**: aquí se especifica el nombre completo del dominio de resolución inverso, tal y como debe ser especificado, por lo que hay que indicar "in-addr.arpa" o "ip6.arpa", según corresponda.

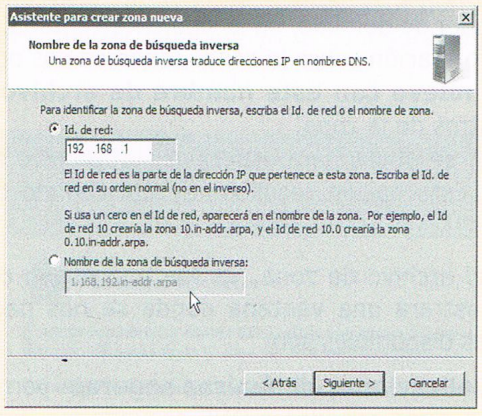


Figura 2.5. *Asistente de creación de una zona de resolución inversa en Windows Server 2008. Aquí se especifica el nombre de la zona inversa, que puede establecerse a través de su identificador de red (dirección IP* ***de la red) o el dominio de resolución inversa in-addr.arpa***

13. En la siguiente ventana, se especifica el nombre del archivo que va a guardar la información sobre la zona. Igual que ocurre para la creación de una zona de resolución directa, normalmente se seleccionará la opción "Crear un archivo nuevo con este nombre de archivo" para crear un archivo

que guarde la información de la zona. Si ya tenemos este archivo de una configuración anterior, podemos seleccionar "Usar este archivo".

14. Después de volver a pulsar el botón "Siguiente", se mostrará una ventana donde se nos pedirá configurar las actualizaciones dinámicas. En este caso, se vuelve a recomendar seleccionar "No admitir actualizaciones dinámicas", a no ser que nuestro servidor forme parte del conjunto de servicios de Active Directory en la red de Microsoft o nuestra configuración del sistema DNS sea de prueba.
15. Pulsamos en el botón "Siguiente" y nos aparecerá una ventana con el resumen de los parámetros que hemos definido para esta zona inversa. Si pulsamos en el botón "Finalizar", se creará la nueva zona con la configuración necesaria.
16. Una vez creada la zona de búsqueda inversa, deberá aparecernos en la parte izquierda de la ventana principal de gestión del DNS, como una rama más del árbol, debajo del icono "Zonas de búsqueda inversa". Al pulsar en ella, deberá aparecer una lista con los registros definidos en esta zona. En su creación se definen dos registros por defecto: *SOA* (registro de autoridad) y *NS* (servidor DNS).
17. Ahora ya podemos añadir registros a las zonas. Para añadir un registro de resolución directa, hay que seleccionar la zona de resolución directa y pulsar en la opción del menú principal "Acción || Host nuevo (A o AAAA)", lo que mostrará una ventana como la de la Figura 2.6.
18. En la creación de un registro de resolución directa hay que especificar los siguientes parámetros:
    - **Nombre**: es el nombre del equipo, sin especificar el nombre del dominio.
    - **Nombre de dominio completo (FQDN)**: es el nombre completo del equipo, incluyendo el nombre del dominio.
    - **Dirección IP**: especifica la dirección IP del equipo.
    - **Crear registro del puntero (PTR) asociado**: se utiliza para que la herramienta cree también el registro de resolución inversa de forma automática. Esta opción solamente se podrá utilizar si se ha definido previamente el dominio de resolución inversa.

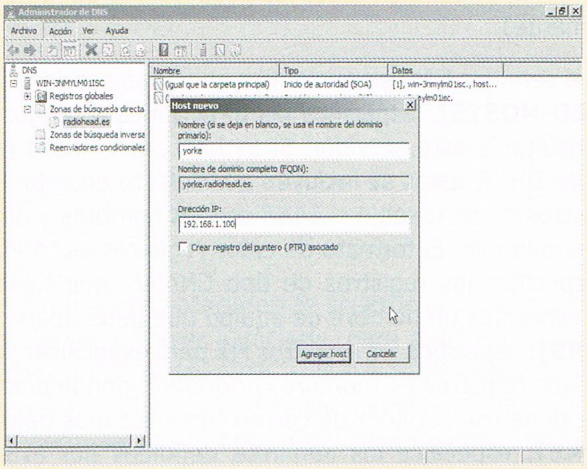


Figura 2.6. *Creación de un nuevo registro A en Windows Server 2008. Aquí se especifica el nombre del equipo y su dirección IPv4. También se puede crear de forma automática el registro PTR asociado si se marca la casilla de verificación "Crear registro del puntero (PTR) asociado"*

2.4.1.2 Windows 7

Los sistemas operativos Microsoft Windows 7 no incluyen por defecto los paquetes necesarios para permitir que el equipo se comporte como un servidor DNS. Estos paquetes tampoco son suministrados, por el momento, por Microsoft, por lo que, será necesario utilizar programas de otros fabricantes, ya sean de pago o gratuitos. Aquí recomendamos usar el paquete Dual DHCP DNS Server, ya que se distribuye bayo licencia GPL.

EJEMPLO 2.6

Veamos los pasos a seguir para configurar un equipo como servidor DNS en Windows 7, utilizando el paquete Dual DHCP DNS Server (versión 6.50).

1. En primer lugar, hay que descargar e instalar el paquete Dual DHCP DNS Server en el equipo, si es que no lo tenemos instalado ya.
2. Una vez instalado el programa, éste se inicia automáticamente en el sistema como un proceso demonio, utilizando la configuración que incluye por defecto. Se puede comprobar que este proceso está en ejecución si se pulsa la combinación de teclas CTRL + ALT + SUPR, se selecciona "Iniciar el administrador de tareas", se accede a la pestaña "Procesos" y se pulsa el botón "Mostrar procesos de todos los usuarios". El proceso se llama "DUALServer".
3. La configuración por defecto del servidor DNS establece el dominio "workgroup". Para cambiar esta configuración por defecto, hay que seleccionar la opción del menú de inicio de Windows 7 "Todos los programas || Dual Server || Configure". Esto mostrará una ventana del programa editor de textos que abre el archivo de configuración de este servicio, que se llama *DualServer.INI* y debe estar ubicado en la misma ruta que el proceso *DualServer.EXE*.
4. La configuración de Dual Server 6.50 se almacena en un archivo de texto sin formato que está estructurado en secciones, cada una de las cuales contiene un título entre corchetes. En la sección "[SERVICES]" se especifica el servicio que se encuentra activo (si no se ha indicado ninguno, se activan por defecto los servicios DHCP y DNS). Por su parte, en "[LISTEN-ON]" se especifican las direcciones de los adaptadores de red desde donde se van a recibir las peticiones de los clientes (si no se especifica ninguna, se asumen todos los adaptadores de red que tengan direcciones estáticas asignadas manualmente).
5. La configuración del servidor DNS se encuentra en varias secciones. Las más importantes:
   - **[DNS-ALLOWED-HOSTS]**: especifica las direcciones o rangos de direcciones de los equipos que pueden consultar a este servidor. Si se han especificado rangos de direcciones para que asigne el servidor DHCP, estos se incluyen por defecto en esta lista.
   - **[HOSTS]**: registros de recursos *A* o *AAAA* con los nombres y direcciones IP de los equipos que forman parte del dominio. El formato de estos registros es "*nombre=direcciónIP*".
   - **[ALIASES]**: especifica los registros de tipo CNAME, que tienen el formato "*alias=nombre*", donde *nombre* especifica un nombre de equipo que debe aparecer en la sección "[HOSTS]".
   - **[MAIL-SERVERS]**: especifica los registros MX para especificar servidores de correo electrónico. El formato de estos registros es "*nombre=prioridad*", donde *prioridad* especifica un número con la prioridad que tiene ese servidor de correo (un valor más bajo indica más prioridad).
   - **[DOMAIN-NAME]**: especifica los dominios definidos por este servidor. Si se especifica un nombre de dominio sin nada más, entonces el servidor DNS se considera no autoritario para él. En cambio, si se especifica un nombre de dominio con el formato "*nombre=xx.xx.xx*.in-addr.arpa", entonces el servidor DNS será autoritario para el dominio y le asignará también el espacio de direcciones para resolución inversa.
   - **[DNS-SERVERS]**: especifica las direcciones de los servidores DNS a los que se les van a enviar consultas recursivas.
   - **[CHILD-ZONES]**: se utiliza para especificar subdominios gestionados por otros servidores DNS.
   - **[ZONE-REPLICATION]**: especifica las direcciones de los servidores DNS primarios y secundarios para los que están permitidas las transferencias de zonas.
   - **[TIMINGS]**: especifica los intervalos de tiempo utilizados por el servidor DHCP y DNS.

6. Un ejemplo de configuración del servidor DNS puede ser el siguiente (aquí no se ha especificado ninguna configuración como servidor DHCP):

```
[SERVICES]
DNS
[LISTEN-ON]
192.168.1.1
[DNS-ALLOWED-HOSTS]
192.168.1.1-192.168.1.254
[HOSTS]
DNS=192.168.1.1
Pc1=192.168.1.101
mac=192.168.1.102
debian=192.168.1.103
linux=192.168.1.104
[ALIASES]
www=debian
secundario=debian
ines=Pc1
[MAIL-SERVERS]
debian=10
Linux=15
[DOMAIN-NAME]
midominio.com=1.168.192.in-addr.arpa
[DNS-SERVERS]
80.10.54.250
[CHILD-ZONES]
subdominio.midominio.com=192.168.1.104
1.168.192.in-addr.arpa=192.168.1.104
[ZONE-REPLICATION]
secundario=192.168.1.103
[TIMINGS]
Refresh=3600
Retry=10
Expire=360000
Minimum=20
MinCacheTime=100
MaxCacheTime=1000
```

7. Una vez modificados los parámetros anteriores de acuerdo con la configuración de red, es necesario detener el servicio Dual Server y volver a iniciarlo, para que los cambios tengan efecto. Para ello, hay que pulsar la combinación de teclas CTRL + ALT + SUPR, seleccionar "Iniciar el administrador de tareas", acceder a la pestaña "Servicios" y pulsar con el botón derecho del ratón sobre el proceso "DUALServer". Para detenerlo se usa la opción del menú contextual "Detener servicio", mientras que para volver a iniciarlo se usa "Iniciar servicio".

2.4.2 INSTALACIÓN EN GNU/LINUX

La traducción de direcciones de dominio a direcciones IP en un equipo Linux la realiza el paquete **BIND** (*Berkeley Internet Name Domain* o Dominio de Nombres de Internet de Berkeley). Dentro de este paquete se encuentra el demonio *named*, que es el encargado de recibir y atender las peticiones y actualizar las tablas de nombres de dominio. El proceso demonio *named* se inicia utilizando la orden *named*, cuya sintaxis se puede consultar en el apéndice A de referencia de órdenes que se incluye con este libro.

Existen varias versiones del paquete BIND. Actualmente se incluyen las versiones 9.x con las últimas distribuciones de Linux. Si se dispone de una configuración de BIND anterior (4.x u 8.x), los paquetes de documentación de BIND incluyen información sobre cómo actualizar todos los archivos de configuración a las nuevas versiones. Aquí nos centraremos en la versión 9 de BIND, que incluye las siguientes mejoras con respecto a versiones anteriores:

- ✓ Aumento de la seguridad en el DNS, con la utilización de zonas y solicitudes firmadas digitalmente.
- ✓ Utilización completa del protocolo IP versión 6, con la inclusión de registros de tipo *AAAA* y *A6*.
- ✓ Mejora en el protocolo con la utilización de transferencias de zona incrementales, DDNS y EDNS0.
- ✓ Gestión de vistas, que permiten ocultar determinados registros de las zonas a algunos equipos cliente.
- ✓ Soporte para equipos con múltiples procesadores.
- ✓ Arquitectura portable a diferentes sistemas operativos.

Hay dos opciones de configuración del servidor DNS en Linux (como se explica en el apartado 2.1):

- **Como caché de nombres exclusivamente**: el demonio *named* recibe las solicitudes y busca en la caché las correspondencias. Si no están, envía esas solicitudes para que otros servidores DNS las resuelvan. En este servidor no se define ninguna zona.
- **Como servidor de zona**: en el servidor se ha definido, al menos, una zona, de forma que éste resuelve las correspondencias del dominio de ella. Para otros dominios, el servidor funciona como una caché de nombres. La definición de las zonas debe realizarse en los archivos de configuración de *named*, como se explica a continuación.

La configuración general de *named* se realiza en el archivo por defecto *named.conf* que, dependiendo de la distribución y versión de Linux, puede estar ubicado en diferentes carpetas (normalmente, se encuentra en la carpeta */etc*). Se puede especificar una ubicación diferente para este archivo utilizando los argumentos *-b* o *-c* de la orden *named*.

En la instalación de BIND se crea por defecto un archivo *named.conf* que permite que el equipo se comporte como un servidor DNS que funciona como caché de nombres exclusivamente. Si la configuración del servidor DNS BIND ya resulta bastante compleja con la gran cantidad de opciones que se pueden establecer, mucho más compleja resulta si se realiza editando directamente estos archivos de configuración, ya que cualquier pequeño error de sintaxis puede hacer que el servicio no funcione como se espera.

El archivo que se crea por defecto en una instalación de BIND 9 puede incluir las siguientes zonas predefinidas:

- **Raíz**: incluye la configuración de la zona raíz de todo el sistema DNS.
- **0**: define la zona todo ceros, que está reservada por IP.
- **localhost**: especifica la zona que hace referencia al equipo local.
- **127.0.0.1**: define la zona inversa que hace referencia a la dirección IPv4 del equipo local.
- **0000::1**: define la zona inversa que hace referencia a la dirección IPv6 del equipo local.

2.4.2.1 Ejemplos de instalación de un servidor DNS

Este apartado está dedicado a exponer algunos ejemplos de instalación y configuración de un servidor DNS en diferentes distribuciones GNU/Linux. Al igual que ocurre en la instalación y configuración de otros paquetes y servicios, el paquete del servidor DNS requiere los mismos pasos y los mismos parámetros, aunque algunos de ellos pueden variar ligeramente.

EJEMPLO 2.7

Veamos cómo se instala y configura el servidor DNS BIND sobre Linux Debian 5. El primer paso a seguir consiste en instalar el paquete *bind9* (versión 9) que se incluye con esta distribución, usando la herramienta correspondiente. También se puede hacer con la siguiente orden ejecutada con el usuario *root*:

```
root@linux:~# apt-get install bind9
```

Lo anterior instala, configura e intenta iniciar el servidor DNS como caché de nombres, sin la necesidad de paquetes adicionales. El proceso demonio se inicia correctamente con el mensaje "Starting domain name service...: bind9". El archivo *named.conf*, junto con los archivos de definición de dominios, se ubican por defecto en la carpeta */etc/bind*.

Otros paquetes que resultan muy útiles para configurar el servidor DNS en Debian son *bind9-doc* (que incluye documentación adicional sobre BIND) y *gbindadmin* (herramienta de configuración del servidor DNS en el entorno gráfico). A esta herramienta se accede desde el menú principal del entorno gráfico en la opción "GBIN Admin" o "GADMIN-BIND" (véase la Figura 2.7). La primera vez que se inicia esta herramienta, puede mostrar una advertencia indicando que no se han encontrado los archivos de configuración necesarios, por lo que se pregunta si se desea crearlos en la carpeta */var/named*.

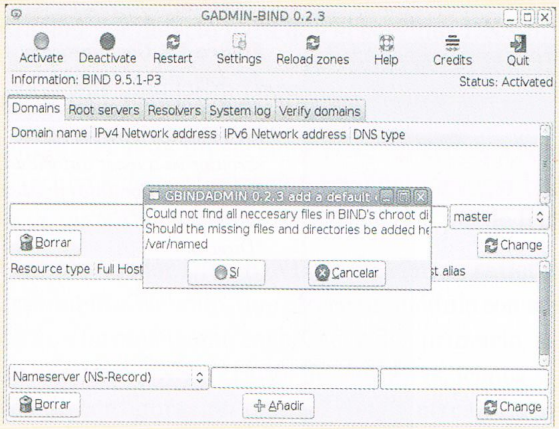


Figura 2.7. *Ventana principal de la herramienta GADMIN-BIND en Debian 5. Con esta herramienta se puede configurar un servidor DNS completo, sin necesidad de editar manualmente los archivos de configuración. También permite iniciar o detener el servicio en cualquier momento*

EJEMPLO 2.8

Veamos cómo se instala y configura el servidor DNS BIND sobre openSuSE Linux 11.1. El primer paso a seguir consiste en instalar los paquetes *bind* (versión 9.5), *yast2-dns-server* y *bind-chrootenv* (es una dependencia del paquete *bind*). Estos paquetes se incluyen con esta distribución y se pueden instalar usando la herramienta correspondiente.

La configuración del servidor DNS se puede realizar directamente sobre los archivos de configuración o a través del entorno gráfico (con la herramienta que incluye el paquete *yast2-dns-server*). El archivo *named.conf* se ubica por defecto en la carpeta */etc* e incluye una configuración por defecto para que el servidor DNS se comporte como caché de nombred.Por su parte, para acceder a la configuración del servidor DNS en el *centro de control de YaST*, hay que seleccionar "Servicios de red || Servidor DNS" lo que muestra una ventana como la de la Figura 2.8.

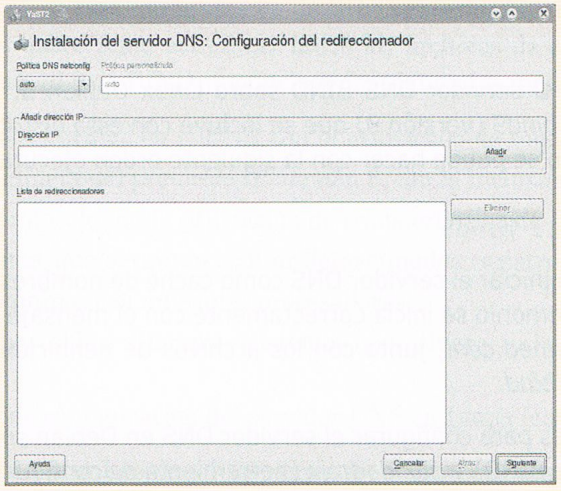


Figura 2.8. *Ventana inicial del asistente de configuración del servidor DNS en YaST. En esta ventana se configuran las direcciones de los servidores DNS a los que se les van a enviar consultas recursivas que no va a poder resolver nuestro servidor*

Los parámetros más importantes que se establecen para un servidor DNS se muestran en las Figuras 2.9 y 2.10. La Figura 2.11 muestra la ventana donde se configuran los archivos de registro del servidor DNS, que es accesible desde la ventana de la Figura 8.13 pulsando en el botón "Configuración experta del servidor DNS...".

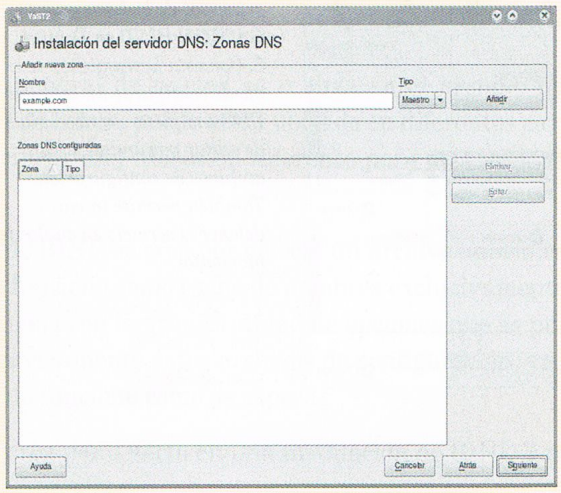


Figura 2.9. *Configuración del dominio en el servidor DNS en YaST. Aquí se indican los dominios para los que el servidor va a tener autoridad. Los tipos de dominios pueden ser "Maestro", "Esclavo" y "Directa"*

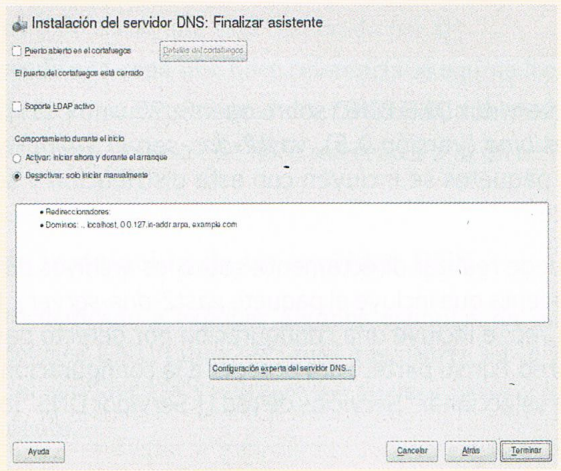


Figura 2.10. *Configuración del demonio del servidor DNS en YaST. Aquí se indica si se va a configurar el cortafuegos para permitir comunicación a través del puerto utilizado por el servidor DNS. También se indica si el demonio named se va a cargar automáticamente en el arranque*

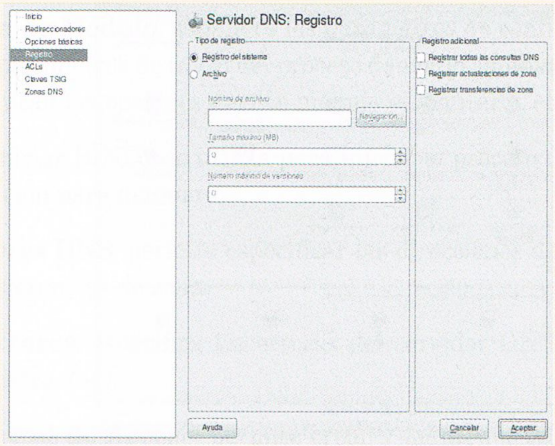


Figura 2.11. *Configuración experta del servidor DNS en YaST. Aquí se pueden indicar los archivos de registro (log) donde el proceso demonio named va a registrar los mensajes de error. Estos registros son muy útiles para resolver problemas de configuración y funcionamiento*

La instalación de BIND en Fedora 11 no difiere de los ejemplos anteriores; el paquete incluido en esta distribución se llama *bind* y los archivos de configuración por defecto se ubican en las carpetas */etc* y */etc/named*. Estos archivos contienen una configuración por defecto para que el servidor DNS funcione como caché de nombres exclusivamente.

2.4.2.2 Configuración del servidor DNS con *Webmin*

Es cierto que la configuración de un servidor DNS en Linux a través del paquete BIND no resulta nada sencilla, sobre todo porque los archivos de configuración involucrados son bastante complejos. Además, el servidor BIND es muy sensible a errores de sintaxis de estos archivos, lo que puede frustrar a más de un administrador.

Para poder configurar el servidor DNS BIND de una forma satisfactoria sin perecer en el intento, se puede utilizar como alternativa la herramienta Webmin, que ofrece un módulo con soporte completo para configurar un servidor DNS BIND en cualquiera de sus formas (como caché, servidor primario, servidor secundario, etc.). Con esta herramienta, se puede configurar un servidor DNS a través de ventanas, iconos y menús, aunque internamente guarda todos los cambios en los archivos de configuración (*named.conf* y otros). La ventaja de utilizar Webmin radica en que no es necesario conocer con detalle la sintaxis de estos archivos, además de evitar los errores no intencionados. Para poder utilizar esta herramienta de configuración es necesario instalarla.

Hay que tener en cuenta que Webmin se inicia siempre con el idioma por defecto en inglés. Para cambiar el idioma a español, hay que acceder a la ventana "Webmin || Webmin Configuration || Language".

El módulo de configuración DNS BIND de Webmin se encuentra en "Servidores | | Servidor de DNS BIND". En caso de que Webmin se haya instalado antes que el paquete BIND, entonces será necesario seleccionar "Refrescar módulos" (*Refresh Modules*) para que el módulo de configuración desaparezca de la lista de módulos no utilizados y aparezca en la sección "Servidores". La Figura 2.12 muestra la ventana principal de este módulo. Puesto que el paquete BIND y la herramienta Webmin son iguales para todas las distribuciones de GNU/Linux, los pasos para instalar y configurar un servidor DNS que se explican en este apartado sirven de igual forma para cualquier distribución de GNU/Linux. Puede haber pequeños cambios si se utilizan versiones diferentes de BIND y Webmin.

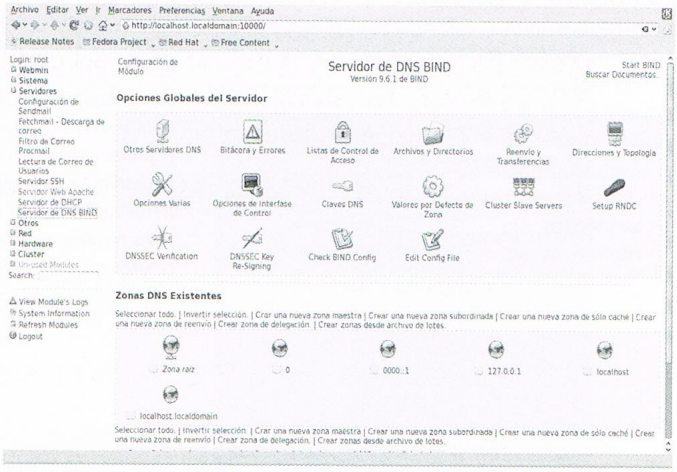


Figura 2.12. *Ventana principal del módulo DNS BIND de Webmin. Esta página aparece cuando la herramienta detecta una configuración existente. En la parte superior se muestran las opciones generales, mientras que en la parte inferior aparece la configuración actual de zonas para el servidor*

Si al iniciar el módulo DNS de Webmin se localizan los archivos de configuración del servidor DNS, entonces se mostrará una ventana como la de la Figura 2.12. Esto significa que la configuración del servidor DNS ya está definida, por lo que se muestran todas las opciones para modificarla. En caso de que no se encuentren los archivos de configuración, entonces se mostrará un asistente (Figura 2.13) para crear un archivo *named.conf*, desde el que se parte para definir toda la configuración de la zona que va a gestionar el servidor.

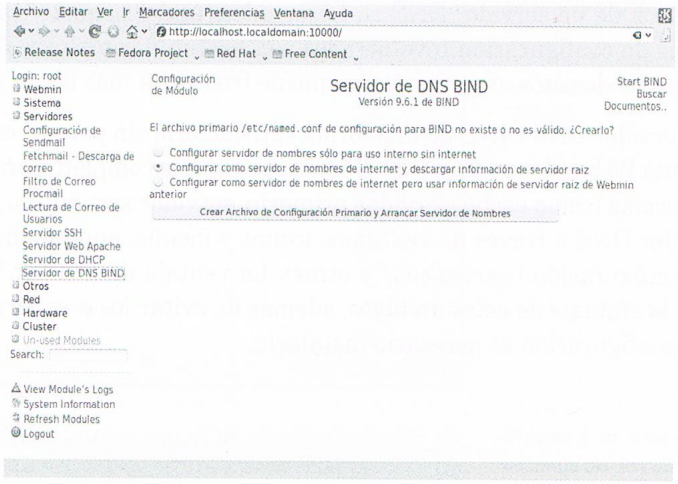


Figura 2.13. *Asistente del módulo DNS BIND de Webmin para establecer la configuración inicial. Esta página aparece cuando la herramienta no detecta ninguna configuración existente. Para crear una nueva configuración de partida, hay que seleccionar el botón de opción más adecuado y pulsar el botón "Crear Archivo de Configuración Primario y Arrancar Servidor de Nombres"*

Si sabemos que la configuración del servidor DNS existe pero Webmin no la ha encontrado, significa que el archivo *named.conf* no se encuentra en la ruta por defecto. Para especificar otra ruta, hay que acceder a la configuración del servidor DNS en Webmin pulsando en el enlace "Configuración de Módulo" de la página principal.

Las opciones disponibles en el módulo de configuración DNS BIND de Webmin son las siguientes:

- **Configuración de Módulo**: establece los parámetros de configuración del módulo DNS de Webmin. Aquí se especifican los parámetros de inicio del proceso demonio, la ubicación de los archivos de configuración, la forma en que se presentan las opciones de este módulo en pantalla, etc.
- **Start BIND** (iniciar BIND): se utiliza para iniciar el proceso demonio del servidor DNS. Si ya está iniciado, aparecerá la opción para detenerlo.
- **Otros Servidores DNS**: permite especificar las direcciones de otros servidores DNS desde los cuales se van a realizar transferencias de zona.
- **Bitácora y Errores**: especifica los errores del servidor DNS que se van a registrar y la ubicación de los archivos de registro (*log*).
- **Listas de Control de Acceso**: permite crear y mantener **ACL** (*Access Control List* o Lista de Control de Acceso), que son grupos de direcciones de equipos a los que posteriormente se les puede autorizar o denegar determinadas operaciones, como la consulta de un determinado tipo de registros o la desautorización para consultar determinadas zonas definidas en los servidores DNS.
- **Archivos y Directorios**: permite indicar la ubicación de determinados archivos que utiliza el servidor DNS.
- **Reenvío y Transferencias**: establece las direcciones de los servidores DNS a los que reenviar las consultas no resueltas.
- **Direcciones y Topología**: se utiliza para especificar las direcciones locales desde las que se van a recibir consultas, además de las direcciones de origen de los equipos cliente que las pueden realizar.
- **Opciones Varias**: establece algunas opciones del servidor DNS, como el uso de la memoria, archivos abiertos, opciones de determinados tipos de registros, etc.
- **Opciones de Interfase de Control**: especifica la configuración de la conexión con los clientes.
- **Claves DNS**: gestiona las claves de cifrado del servidor DNS que se utilizan para realizar transferencias de zona seguras.
- **Valores por Defecto de Zona**: establece los valores por defecto para las nuevas zonas que se creen en el servidor.
- **Cluster Slave Servers** (conjunto de servidores esclavos): permite crear un conjunto de equipos que van a funcionar como un único servidor DNS, repartiendo la carga de trabajo entre ellos.
- **Setup RNDC** (configurar RNDC): se utiliza para que el proceso RNDC controle al servidor DNS, de forma que no sea necesario reiniciar por completo el servidor DNS cuando se realizan cambios en una zona concreta.
- **DNSSEC Verification** (verificación de DNSSEC): establece las claves de seguridad de DNSSEC para este servidor DNS, de forma que otros servidores realicen transferencias de zona seguras con él.
- **DNSSEC Key Re-Signing** (regeneración de claves DNSSEC): especifica el intervalo de tiempo en el que se regeneran las claves de cifrado para este servidor.
- **Check Bind Config** (comprobar la configuración de BIND): nos indica si se han encontrado errores de sintaxis en los archivos de configuración actuales.
- **Edit Config File** (editar archivo de configuración): permite editar manualmente el archivo de configuración *named.conf*, de la misma forma que se podría hacer con un editor de textos.

Por su parte, las opciones disponibles para configurar la zona actual son las siguientes:

- **Seleccionar todo**: selecciona todas las zonas existentes.
- **Invertir selección**: selecciona las zonas existentes que no están seleccionadas actualmente.
- **Crear una nueva zona maestra**: crea una nueva zona maestra en el servidor, ya sea para resolución directa o resolución inversa.
- **Crear una nueva zona subordinada**: define una zona para la que el servidor DNS va a funcionar como secundario (copiando la zona de un servidor primario).
- **Crear una nueva zona de solo caché**: define una zona para la que el servidor DNS va a funcionar como caché de nombres, reenviando peticiones que no conozca y almacenándolas de forma temporal.
- **Crear una nueva zona de reenvío**: crea una zona para que el servidor reenvíe todas esas peticiones a otros servidores DNS, sin guardar después aquellas que se han resuelto.
- **Crear zona de delegación**: permite crear un subdominio basado en uno ya existente y que va a ser gestionado por otro servidor DNS. Esto significa que el servidor DNS que es autoridad para un determinado dominio no lo va a ser para un subdominio dependiente de él.
- **Crear zona desde archivo por lotes**: permite crear una zona cuya definición ha sido almacenada en un archivo.
- **Borrar seleccionados**: elimina las zonas seleccionadas.
- **Update Records in Selected** (actualizar registros en las zonas seleccionadas): cambia los valores de los registros de las zonas seleccionadas.
- **Add Record to Selected** (añadir registros en las zonas seleccionadas): añade nuevos registros a las zonas seleccionadas.
- **Crear una nueva vista**: se usa para crear nuevas vistas, de forma que los clientes solamente van a poder realizar consultas de parte de los registros de las zonas.

Por su parte, las opciones disponibles para crear una configuración básica de un servidor DNS desde cero, cuando no se encuentra ninguna configuración anterior, son las siguientes:

- **Configurar servidor de nombres solo para uso interno sin Internet**: se utiliza cuando tenemos una red local sin conexión a Internet donde el servidor DNS solamente resuelve direcciones locales.
- **Configurar como servidor de nombres de Internet y descargar información de servidor raíz**: esta es la mejor opción cuando tenemos una red local en la que necesitamos que se resuelvan tanto direcciones locales como direcciones externas. En esta opción Webmin descargará de forma automática desde *rs.internic.net* una lista actualizada de servidores DNS que serán utilizados para resolver consultas recursivas.
- **Configurar como servidor de nombres de Internet pero usar información de servidor raíz de Webmin anterior**: esta opción es igual que la anterior, salvo que no descarga de Internet una lista actualizada de servidores DNS, sino que toma la lista que incluye el propio paquete Webmin. Esta opción es útil cuando no se dispone de conexión a Internet en el momento de configurar el servidor DNS.

Finalmente, las opciones más importantes que están disponibles para editar una zona ya creada en Webmin (Figura 2.14), son las siguientes:

- **Dirección**: se usa para gestionar los registros de dirección IPv4 (*A*).
- **Servidor de Nombres**: se usa para gestionar los registros de servidores de nombres (*NS*).

- **Alias de Nombre**: se usa para gestionar los registros de alias (*CNAME*).
- **Servidor de Correo**: se usa para gestionar los registros de servidores de correo electrónico (*MX*).
- **Información de Máquina**: se usa para gestionar los registros de información de equipo (*HINFO*).
- **Texto**: se usa para gestionar los registros que guardan información textual (*TXT*).
- **Dirección Inversa**: se usa para gestionar los registros de resolución inversa (*PTR*). En estos registros solamente se especifica la última parte de la dirección IP que corresponde al número de equipo y Webmin la convertirá automáticamente al formato de dirección inversa.
- **Dirección IPv6**: se usa para gestionar los registros de dirección IPv6 (*AAAA*).
- **Todos los Tipos de Registro**: muestra todos los registros de la zona, independientemente del tipo que sean.
- **Editar Archivo de Registros**: permite editar directamente el archivo donde se guardan los registros para la zona.
- **Editar Parámetros de Zona**: se usa para gestionar los parámetros de la zona, como el servidor maestro, tiempos de refresco o expiración, etc.
- **Editar Opciones de Zona**: se usa para configurar las transferencias de zona con otros servidores.
- **Generadores de Registro**: se usa para generar automáticamente registros DNS si estos siguen un patrón numérico predeterminado para los nombres y las direcciones (por ejemplo, "pc1" es *192.168.1.100*, "pc2" es *192.168.1.101*, etc.).
- **Mirar Información de WHOIS**: permite realizar consultas a servidores DNS para comprobar el estado de funcionamiento de este protocolo.
- **Setup DNSSEC Key**: permite gestionar las claves de cifrado para evitar ataques, usando el protocolo de seguridad DNSSEC.

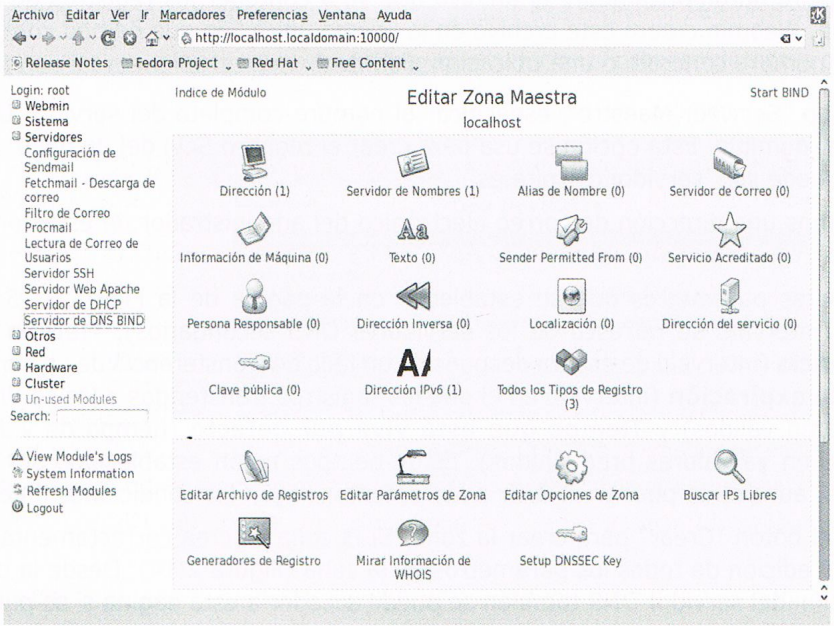


***Figura 2.14**. Ventana de edición de una zona en Webmin. Todos los iconos que aparecen en el primer grupo de opciones se utilizan para consultar, añadir, modificar o eliminar diferentes tipos de registros en la zona*

- **Freeze Zone**: permite congelar una zona para evitar que sea actualizada por una transferencia de zona.
- **Unfreeze Zone**: descongela una zona para que pueda ser actualizada mediante una transferencia.
- **Check Records**: se usa para realizar comprobaciones de los registros de la zona y encontrar posibles problemas de funcionamiento.
- **Convertir a zona subordinada**: permite convertir una zona maestra en secundaria.
- **Borrar Zona**: elimina la zona actual y todos sus registros.

EJEMPLO 2.9

Suponemos que tenemos una red local en la que hay que definir los nombres de determinados equipos que ofrecen servicios. Veamos cómo configurar a través de Webmin una zona maestra de resolución directa e inversa para un servidor DNS desde la configuración inicial que nos ofrece BIND. Los pasos a seguir son los siguientes:

1. Acceder a Webmin y seleccionar el módulo "Servidores || Servidor de DNS BIND". En la ventana principal que aparece, seleccionamos "Crear una nueva zona maestra", lo que mostrará una página como la de la Figura 8.18.
2. Establecemos el tipo de zona maestra que vamos a crear, en este caso comenzamos con la creación de la zona de resolución directa, por lo que hay que marcar el botón de opción "Reenvío (Nombres a Direcciones)".
3. Especificamos el nombre de dominio de la zona maestra en el cuadro de texto como, por ejemplo, "chispita.es". Si esta zona va a ser visible en Internet, entonces debe haber sido previamente registrada y reservada.
4. Es recomendable dejar marcado "Automático" en la opción "Archivo de Registros" para que Webmin cree y nombre automáticamente el archivo que va a contener los registros de zona. Si se marca esta opción, Webmin creará este archivo en la misma ubicación que *named.conf*, aunque se puede indicar un nombre concreto o una ubicación distinta.
5. En el campo "Servidor Maestro", especificar el nombre completo del servidor DNS, incluyendo el nombre del dominio. Esta opción se usa para crear el registro *SOA* del dominio. Siguiendo nuestro ejemplo, puede ser "servidor.chispita.es".
6. Especificamos una dirección de correo electrónico del administrador de esta zona (este campo es obligatorio).
7. Los siguientes parámetros que se establecen en la página de la Figura 2.15 son: **Tiempo de refresco** (intervalo de refresco de los servidores DNS secundarios), **Tiempo de reintento de transferencia** (intervalo de espera después de un fallo de transferencia de un servidor secundario), **Tiempo de expiración** (intervalo en el que los registros transferidos a los servidores secundarios se consideran válidos) y **Tiempo que está viva por defecto** (tiempo de vida de los registros que no tienen ya valores predefinidos). Estos tiempos están establecidos por defecto a valores razonables, aunque se pueden reducir o incrementar según las condiciones de cambio de la red.
8. Pulsar en el botón "Crear" para crear la zona. Si la zona se crea correctamente, se mostrará una ventana de edición de todos los parámetros de la zona (Figura 2.14). Desde la página principal de configuración del servidor DNS también se puede acceder a esta página si se pulsa sobre el enlace de la zona a editar.
9. Volver a la página principal del módulo DNS de Webmin y pulsar nuevamente en el enlace "Crear una nueva zona maestra", lo que mostrará de nuevo una página como la de la Figura 2.15.

10. Establecemos el tipo de zona maestra que vamos a crear, en este caso continuamos la creación de la zona de resolución inversa, por lo que hay que marcar el botón de opción "Inversas (Direcciones a Nombres)".
11. Especificamos el nombre de dominio de la zona maestra en el cuadro de texto como, por ejemplo, "192.168.1", que corresponde con el número de red de la parte de dirección IP. Webmin convertirá automáticamente esta dirección al formato utilizado en las zonas de resolución inversa.
12. Al igual que cuando se crea una zona de resolución directa, es recomendable dejar marcado "Automático" en la opción "Archivo de Registros" para que Webmin cree y nombre automáticamente el archivo que va a contener los registros de zona.
13. En el campo "Servidor Maestro", especificar el nombre completo del servidor DNS, incluyendo el nombre del dominio. Esta opción se usa para crear el registro *SOA* del dominio. Siguiendo nuestro ejemplo, debe ser "servidor.chispita.es".
14. Especificamos una dirección de correo electrónico del administrador de esta zona (este campo es obligatorio).
15. Configurar los parámetros de tiempo según sean necesarios, aunque se recomienda dejar a los valores por defecto.
16. Pulsar en el botón "Crear" para crear la zona inversa. Si la zona se crea correctamente, se mostrará una ventana de edición de todos los parámetros de la zona (Figura 2.15). Desde la página principal de configuración del servidor DNS también se puede acceder a esta página si se pulsa sobre el enlace de la zona a editar.
17. Volver a acceder a la ventana de edición de la zona maestra de resolución directa (Figura 2.15) y pulsar el icono "Dirección" para añadir un registro *A*. Esto mostrará una ventana como la de la Figura 2.16, donde se especifica el nombre del registro (por ejemplo, "ines") y valor del registro (por ejemplo "192.168.1.68"). Se puede activar la casilla "Actualizar Inversas" para crear también el registro de resolución en la zona inversa (solo se podrá hacer esto si el servidor DNS es maestro, tiene autoridad para esa zona, la dirección pertenece también a esa zona y la zona de resolución inversa ha sido creada con anterioridad). Para añadir ese registro, se pulsa el botón "Crear".
18. Para hacer que los cambios tengan efecto, hay que reiniciar el proceso demonio del servidor DNS.

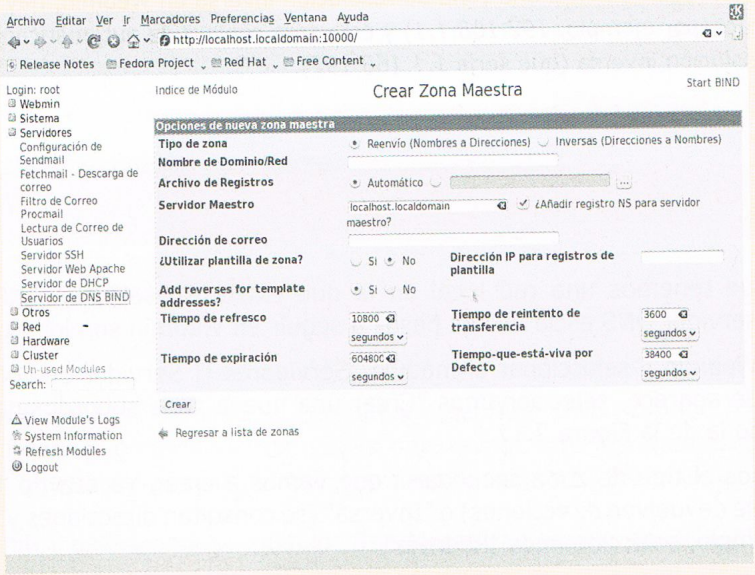


Figura 2.15. *Página de creación de una nueva zona maestra en el módulo DNS BIND de Webmin. Los parámetros principales son el tipo de zona, el nombre completo del dominio y el nombre completo del servidor, incluyendo su dominio*

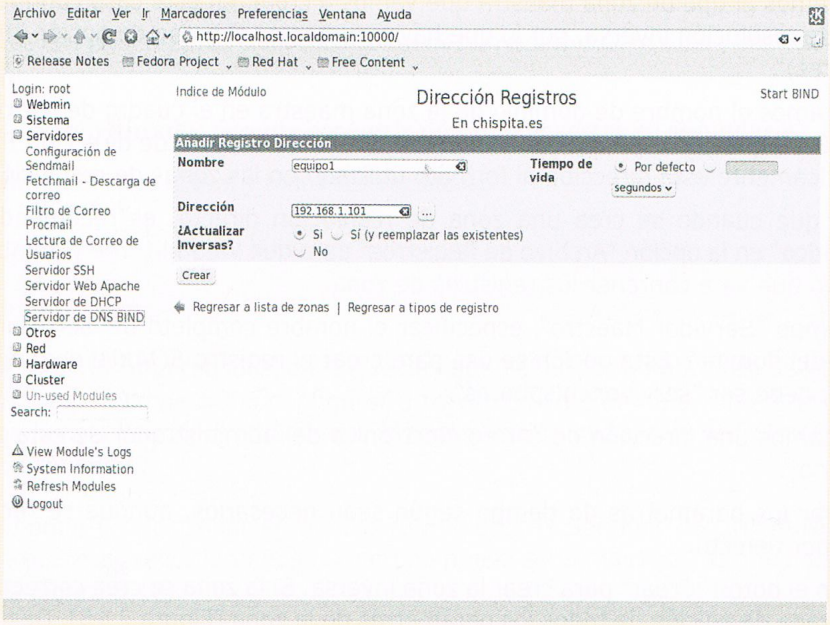


Figura 2.16. *Añadir un nuevo registro de resolución directa (A) a una zona en Webmin. Aquí se especifica el nombre del equipo (sin el dominio) y su dirección IP. Si se marca el botón de opción "Sí" en "Actualizar Inversas" entonces Webmin creará también de forma automática el registro correspondiente de resolución inversa (PTR)*

Si se va a añadir un registro *PTR* a una zona de resolución inversa en Webmin, hay que especificar la dirección IP tal cual (por ejemplo, *192.168.1.1*) y ésta será convertida automáticamente al formato utilizado para resolución inversa (que sería *1.1.168.192*).

EJEMPLO 2.10

Suponemos que tenemos una red local en la que existe un servidor DNS maestro y deseamos configurar un servidor DNS esclavo. Los pasos a seguir en Webmin son los siguientes:

1. Acceder a Webmin y seleccionar el módulo "Servidores || Servidor de DNS BIND". En la ventana principal que aparece, seleccionamos "Crear una nueva zona subordinada", lo que mostrará una página como la de la Figura 2.17.
2. Establecemos el tipo de zona secundaria que vamos a crear, ya sea de "Reenvío" (se consultan nombres y se devuelven direcciones) o "Inversa" (se consultan direcciones y se devuelven nombres). En este ejemplo, seleccionamos "Reenvío".
3. Especificamos el nombre de dominio de la zona, que tiene que coincidir con el nombre de dominio de la zona maestra, en el cuadro de texto (por ejemplo, "chispita.es").

4. Es recomendable dejar marcado "Automático" en la opción "Archivo de Registros" para que Webmin cree y nombre automáticamente el archivo que va a contener los registros de zona. Si se marca esta opción, Webmin creará este archivo en la misma ubicación que *named.conf*, aunque se puede indicar un nombre concreto o una ubicación distinta.
5. En el campo "Servidores Maestros", especificar las direcciones IP del servidor maestro (en primer lugar) y de cualquier otro servidor secundario que ya exista.
6. Pulsar en el botón "Crear" para crear la zona. Si la zona se crea correctamente, se mostrará una ventana para introducir opciones adicionales. Ahora, hay que regresar a la ventana principal de configuración del servidor DNS en Webmin.
7. Para hacer que los cambios tengan efecto, hay que reiniciar el proceso demonio del servidor DNS BIND.
8. En la configuración Webmin del servidor DNS maestro, añadir un nuevo registro a la zona de tipo *NS* con el nombre y dirección del servidor DNS secundario. Además, hay que acceder a la configuración de la zona, seleccionar el icono "Editar Opciones de Zona", activar la opción "¿Notificar los cambios a las subordinadas?" y especificar la dirección IP del servidor DNS esclavo que se ha creado en los pasos anteriores. Recordar que para hacer que los cambios tengan efecto, hay que reiniciar el proceso demonio del servidor DNS.
9. Si se han especificado otros servidores esclavos para realizar transferencias, también hay que activar en ellos la opción que se indica en el paso 8.

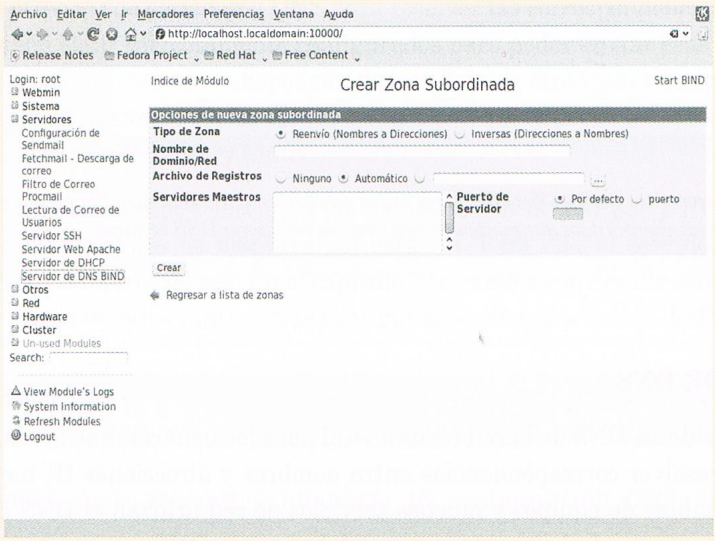


Figura 2.17. *Página de creación de una zona secundaria en Webmin. En esta ventana se especifica el tipo de zona (resolución directa o inversa), el nombre del dominio y las direcciones IP de los servidores DNS maestro o esclavos desde donde se van a transferir los registros*

EJEMPLO 2.11

Una vez que tenemos definido un dominio con nuestro servidor DNS primario (con alguno o ningún servidor DNS secundario), podemos crear vistas para evitar que los clientes puedan consultar y obtener direcciones que deben quedar ocultas. Los pasos a seguir en Webmin son los siguientes:

1. Acceder a Webmin y seleccionar el módulo "Servidores || Servidor de DNS BIND". En la ventana principal que aparece, seleccionamos "Crear una nueva vista", lo que mostrará una página como la de la Figura 2.18.

2. Establecemos el nombre de la vista (que debe ser único) y las direcciones IP de los equipos cliente que la van a tener disponible. Después, hay que pulsar el botón "Crear" para crear la vista.
3. En la ventana principal de configuración del servidor DNS en Webmin, seleccionar las zonas que van a formar parte de la vista y pulsar el enlace "Mover a la vista". También se pueden añadir directamente a la vista creada todas aquellas zonas nuevas que se creen, ya que, en la ventana de creación de la nueva zona, aparecerá una opción para especificar la vista a la que va a pertenecer.

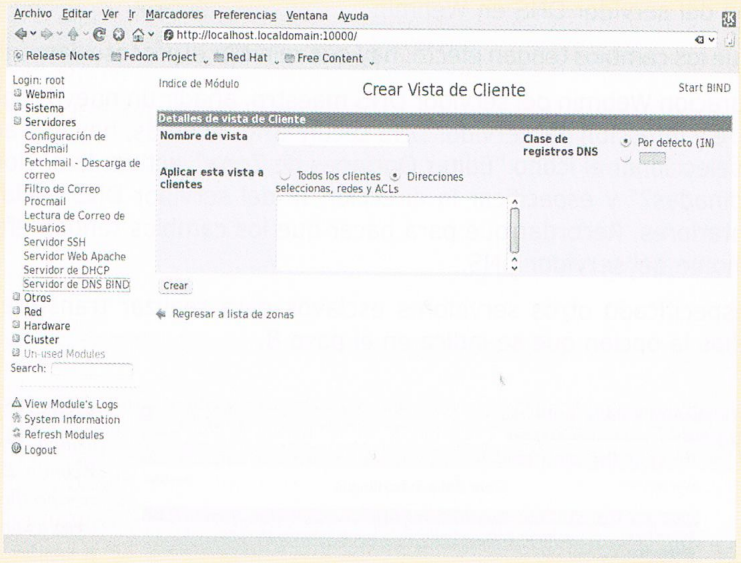


Figura 2.18. *Página para crear una nueva vista DNS en Webmin. Estas vistas pueden ser utilizadas para limitar los registros que pueden consultar los clientes o los que pueden transferirse los servidores DNS esclavos*

2.4.3 PROBLEMAS DEL SERVIDOR DNS

El correcto funcionamiento de los servidores DNS de la red resulta vital para los usuarios que la manejan. Aunque se trata de un servicio que se limita a resolver correspondencias entre nombres y direcciones IP, hay que tener en cuenta que los usuarios trabajan con nombres de equipos y muchos servicios de red utilizan el DNS para funcionar. Por ejemplo, el uso de un programa navegador de Internet requiere del sistema DNS porque los usuarios están acostumbrados a introducir direcciones de dominio y no saben lo que es una dirección IPv4 o IPv6.

La mejor forma de comprobar si el servidor DNS está funcionando correctamente es a través de las órdenes *nslookup* o *dig*. Los errores que devuelven estas órdenes pueden ser:

- **Timed out** (tiempo de espera agotado): se produce cuando el servidor no responde a una solicitud y varios reintentos en el tiempo establecido. Puede ser debido a que el servidor esté saturado, sea inaccesible o existan problemas de conectividad en la red.
- **No response from server** (no hay respuesta del servidor): se produce cuando en el servidor, aunque está funcionando, no tiene activo el servicio DNS.
- **No records** (no hay registros): se devuelve este mensaje cuando no hay información en el servidor DNS para el tipo de consulta realizada.

- **Non-existent domain** (dominio no existente): se utiliza para indicar que el equipo especificado o el dominio para el que se está intentando resolver la dirección IP no existe.
- **Connection refused** (conexión rechazada): se produce cuando no se puede realizar conexión con el servidor para realizar la consulta.
- **Server failure** (fallo en el servidor): se notifica cuando el servidor encuentra una inconsistencia en su base de datos y no puede devolver una respuesta válida. Se recomienda repasar los archivos de configuración en el servidor.
- **Refused** (rechazado): se produce cuando el servidor DNS rechaza la consulta, una situación que puede producirse cuando se han limitado las consultas por cuestiones de seguridad.
- **Format error** (error de formato): esta notificación es enviada por el servidor cuando detecta que el mensaje de solicitud no tiene el formato correcto, por lo que el problema se puede encontrar en la orden *nslookup* o en la consulta realizada por el usuario.

2.5 CONFIGURACIÓN DE UN CLIENTE DNS

Además de disponer de servidores DNS para resolver las correspondencias de direcciones, los equipos clientes de la red también deben estar correctamente configurados para poder enviar esas peticiones. Para ello, es necesario que su configuración de red sea correcta y dispongan de una lista de direcciones correspondientes a los servidores DNS que les pueden resolver las direcciones. En los apartados siguientes se explican los pasos a seguir para establecer estas direcciones en equipos con Microsoft Windows y Linux.

En caso de que los equipos obtengan su configuración de red por DHCP, también es posible que obtengan las direcciones de los servidores de nombres por esta vía. Para ello, el servidor DHCP debe facilitar esta información, además de otros parámetros de red. En el capítulo 1 se explica con detalle cómo incluir las direcciones de los servidores DNS para que sean enviadas junto con la configuración de red a través de DHCP.

EJEMPLO 2.12

Los pasos para acceder y modificar la configuración DNS de un cliente Windows XP son los siguientes:

1. Pulsar con el botón derecho sobre el icono "Mis sitios de red" del escritorio o el menú de inicio y seleccionar "Propiedades". Aparecerá una ventana con los iconos asociados a cada una de las conexiones de red disponibles en el equipo.
2. Seguidamente hay que pulsar con el botón derecho del ratón en el icono "Conexión de área local" y seleccionar "Propiedades". Aparecerá una ventana con una lista que incluye todos los protocolos y servicios que funcionan sobre esa conexión de red.
3. A continuación se selecciona "Protocolo TCP/IP" y se pulsa el botón "Propiedades". En esta otra ventana se muestran los parámetros TCP/IP asociados a la conexión de red seleccionada (Figura 2.19).
4. En la página "General" (Figura 2.19), se muestran los parámetros generales de TCP/IP asociados a la conexión de red. Para que el equipo pueda realizar consultas a través de DNS deberá disponer de, al menos, una dirección IP de un servidor de nombres especificada en los cuadros de texto titulados "Usar las siguientes direcciones de servidor DNS".

5. En caso de que esta configuración se pueda obtener de forma automática desde un servidor DHCP, se puede marcar el botón de opción "Obtener la dirección del servidor DNS automáticamente", de manera que no será necesario indicar ninguna dirección.
6. Para probar que se han obtenido direcciones de servidores DNS por DHCP en el arranque de Windows XP, ejecutar la orden *IPCONFIG /ALL* en el intérprete.

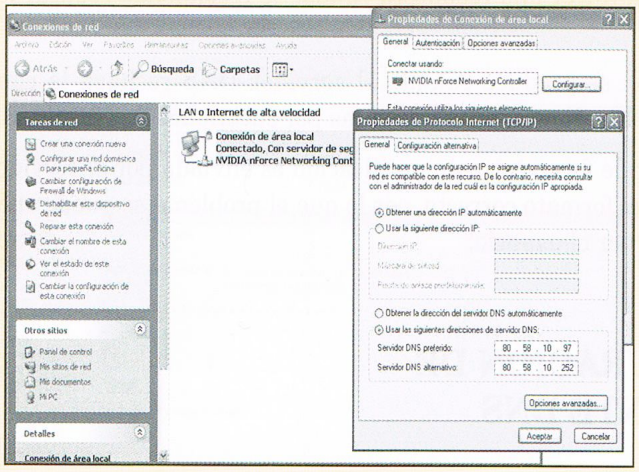


***Figura 2.19**. Configuración de red IPv4 en Windows XP. En esta ventana se especifican las direcciones de los servidores DNS, una dirección principal y otra secundaria. Se puede indicar que estos parámetros se obtengan también por DHCP si se marca el botón de opción "Obtener la dirección del servidor DNS automáticamente"*

EJEMPLO 2.13

Los pasos para acceder y modificar la configuración DNS de un cliente Windows 7 son los siguientes:

1. Pulsar con el botón derecho del ratón sobre icono "Red" del escritorio y seleccionar "Propiedades". Se mostrará una ventana del "Centro de redes y recursos compartidos". También se puede acceder a esta ventana desde el "Panel de control", seleccionando "Redes e Internet" y después "Centro de redes y recursos compartidos".

2. En la ventana del centro de redes, pulsar en el enlace de la izquierda "Cambiar configuración del adaptador", pulsar con el botón derecho del ratón en el icono "Conexión de área local" y seleccionar "Propiedades". Aparecerá una ventana con una lista que incluye todos los protocolos y servicios que funcionan sobre esa conexión de red.

3. Seguidamente, seleccionar "Protocolo de Internet versión 4 (TCP/IPv4)" y pulsar el botón "Propiedades". En la página "General" (Figura 2.20), se deben especificar las direcciones de los servidores de nombres en caso de marcar el botón de opción "Usar las siguientes direcciones de servidor DNS". Si nuestra red dispone de un servidor DHCP que puede enviar esa configuración, entonces hay que marcar el botón de opción "Obtener la dirección del servidor DNS automáticamente", para lo que ya no es necesario especificar ninguna dirección IP.

4. Para probar que se han obtenido las direcciones de los servidores de nombres por DHCP en el arranque de Windows 7, ejecutar la orden *IPCONFIG /ALL* en el intérprete.

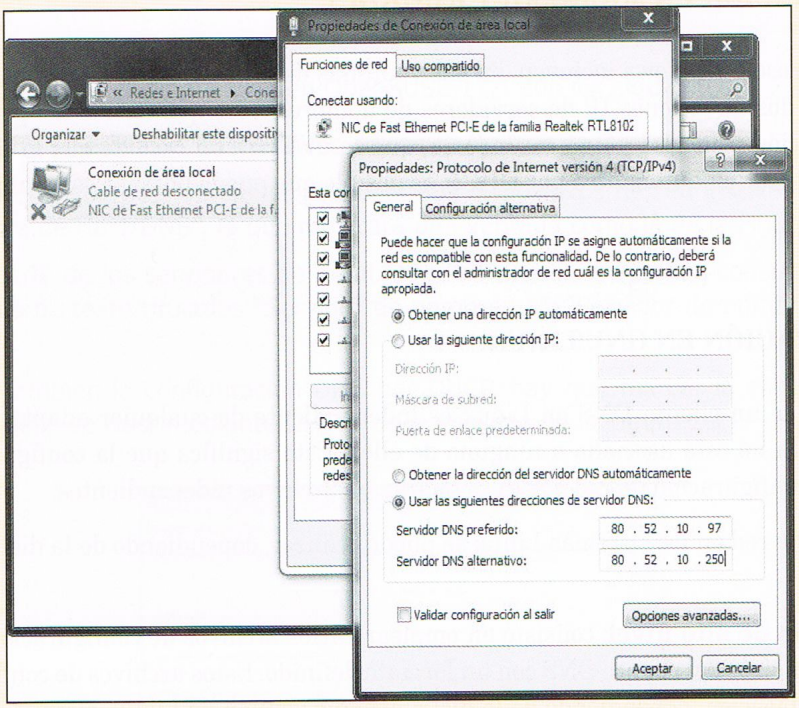


Figura 2.20. *Configuración de red IPv4 en Windows 7. En esta ventana se especifican las direcciones de los servidores DNS a los que se les van a enviar las consultas (una dirección principal y otra alternativa). Si se marca el botón de opción "Obtener la dirección del servidor DNS automáticamente", se pueden obtener estas direcciones automáticamente por DHCP*

EJEMPLO 2.14

Los pasos para comprobar que la configuración DNS en un equipo Microsoft Windows de un cliente funciona correctamente son los siguientes:

1. Acceder al intérprete de órdenes que se encuentra en "Inicio || Todos los programas || Accesorios || Símbolo de sistema". También se puede acceder desde "Inicio || Ejecutar" y escribir "CMD".
2. Dentro del interfaz de órdenes, escribir *NSLOOKUP* y pulsar INTRO. Aparecerá el símbolo ">", que indica que desde aquí se puede interrogar al DNS.
3. Escribir un nombre de equipo como, por ejemplo "es.wikipedia.org" y pulsar INTRO. En ese momento, se enviará la consulta al servidor DNS para que devuelva la dirección IP correspondiente. En caso de que no haya problemas, esta dirección IP se mostrará en pantalla.
4. También se puede realizar una consulta recursiva si previamente se introduce la orden "*SET TYPE=PTR*" de *NSLOOKUP*. Una vez introducida, se puede especificar una dirección IP para que se resuelva en su nombre correspondiente.
5. La herramienta *NSLOOKUP* también permite realizar una transferencia de zona desde el servidor DNS (si éste último también lo permite), de forma que se pueden consultar los registros disponibles en él. Para ello, se ejecuta orden *LS* seguida del nombre del dominio.

2.5.1 CONFIGURACIÓN EN MICROSOFT WINDOWS

Los sistemas Microsoft Windows incluyen, en sus ventanas de configuración de red, sendos cuadros de texto que permiten especificar dos direcciones IP de servidores de nombres a los que enviar las peticiones. Es recomendable especificar una dirección principal y una secundaria, que se utilizará en caso de que la principal no conteste. Si el equipo se configura de forma automática por DHCP, es posible que pueda obtener esta información también a través de DHCP.

2.5.2 CONFIGURACIÓN EN GNU/LINUX

La configuración de un cliente DNS en Linux es independiente de cualquier adaptador de red instalado en el equipo, por lo que ésta no está asociada a ninguno de ellos. Esto significa que la configuración del cliente DNS es independiente de la configuración de red y ésta se guarda en archivos independientes.

La configuración de red en los sistemas Linux se puede realizar, dependiendo de la distribución utilizada, de tres formas posibles:

- **Configuración de alto nivel**: consiste en emplear varios archivos de configuración de texto que almacenan todos los parámetros del cliente DNS con un formato definido. Estos archivos de configuración pueden cambiar en nombre y ubicación, dependiendo de la distribución y versión de Linux, aunque en la mayoría de los casos suelen tener los mismos nombres. En el apartado 2.5.2.2 se explica cómo realizar la configuración del cliente DNS en Linux a alto nivel.
- **Herramientas de entorno gráfico**: algunas distribuciones de Linux permiten instalar herramientas gestionadas desde el entorno gráfico que sirven para realizar una configuración del cliente DNS de la misma forma que en otros sistemas operativos como Microsoft Windows. De esta forma, los usuarios que están más acostumbrados a trabajar con estos sistemas pueden cambiar a Linux sin sufrir un cambio brusco. Estas herramientas pueden ser YaST (OpenSUSE), Control de dispositivos de red (Fedora), NetworkManager, Webmin, Linuxconf, etc. En el apartado 2.5.2.1 se explica cómo realizar la configuración de la red utilizando estas herramientas.

La configuración del cliente DNS en Linux también requiere el uso de una cuenta de usuario que disponga de los privilegios necesarios para realizar las operaciones necesarias. Normalmente, cuando se realiza una instalación típica de Linux, se crea la cuenta ***root***, que tiene privilegios para realizar cualquier operación sobre el sistema.

Todo el sistema de resolución de nombres que utiliza el cliente DNS se instala en Linux a través de las **librerías GNU de C**, también conocidas como *libc* o *glibc*. Estas librerías contienen un conjunto de funciones estandarizado para realizar operaciones básicas sobre el sistema. Estas funciones ayudan al desarrollo de programas, debido a que los programadores no tienen que desarrollarlas. Actualmente, los sistemas Linux utilizan *glibc 2.x*, también conocida como *libc6*.

2.5.2.1 Configuración en entorno gráfico

En los ejemplos siguientes se muestra cómo realizar la configuración del cliente DNS en diferentes distribuciones GNU/Linux, utilizando para ello herramientas gráficas.

EJEMPLO 2.15

Los pasos para configurar el cliente DNS en OpenSUSE 11.1 son los siguientes:

1. Acceder a YaST y seleccionar "Dispositivos de red || Ajustes de la red".
2. En la ventana que aparece, donde se gestionan los dispositivos de red instalados, seleccionar la página "Nombre de Host/DNS", lo que mostrará una ventana como la de la Figura 2.21.
3. Las direcciones IP de los servidores de nombres a los que se envían las consultas se especifican en tres cuadros de texto titulados "Servidor de nombres 1", "Servidor de nombres 2" y "Servidor de nombres 3".
4. Para obtener también la configuración DNS por DHCP, hay que marcar la casilla de verificación "Modificar Nombre de Host mediante DHCP" de la ventana de la Figura 2.21.

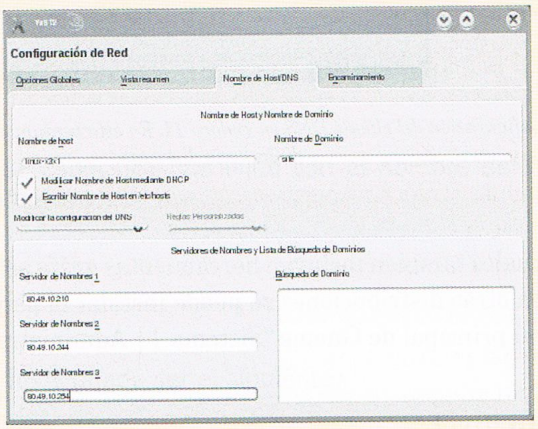


Figura 2.21. *Ventana de configuración del cliente DNS en OpenSUSE 11.1. En esta ventana se pueden especificar hasta tres direcciones distintas*

EJEMPLO 2.16

Las últimas versiones de los sistemas Fedora, al igual que ocurre con otras distribuciones GNU/Linux, utilizan por defecto la herramienta NetworkManager para la gestión de la configuración de los adaptadores de red. Sin embargo, la configuración del cliente DNS se realiza desde la herramienta de configuración *system-config-network*. Los pasos a seguir son los siguientes:

1. Selccionar "Sistema || Administración || Red" desde el menú principal de Gnome.
2. En la ventana que aparece, seleccionar la página "DNS", lo que mostrará una ventana como la de la Figura 2.22.
3. Las direcciones IP de los servidores de nombres se establecen en los cuadros de texto titulados "DNS primario", "DNS secundario" y "DNS terciario". Este es el orden a la hora de enviar las consultas.
4. El cuadro de texto "Ruta de búsqueda DNS" se utiliza para especificar un nombre de dominio por defecto. En caso de que se realice una consulta de un nombre de equipo que no incluya el nombre del dominio, éste dominio por defecto se anexará automáticamente a la consulta.

5. Si se desea obtener la configuración DNS a través de DHCP hay que configurar el adaptador convenientemente, como se explica en el capítulo 1 de este libro.

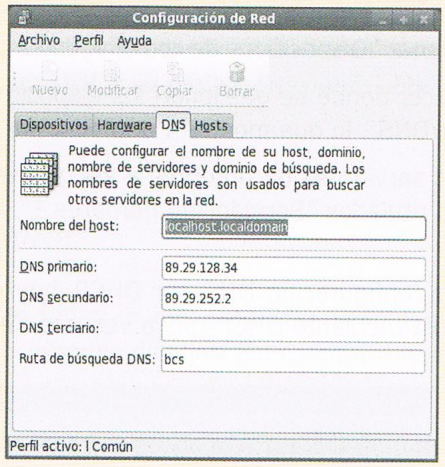


Figura 2.22. *Ventana de configuración del cliente DNS en Fedora 11. En esta ventana también se pueden especificar hasta tres direcciones distintas*

Las distribuciones Debian actuales también incluyen herramientas gráficas de configuración de los parámetros de red. Por ejemplo, en Debian 5 y en otras distribuciones se puede instalar el paquete *gnome-network-admin*, que será accesible desde la opción del menú principal de Gnome "Sistema | | Administración | | Red".

2.5.2.2 Configuración de alto nivel

Como se explica en el apartado anterior, los parámetros de configuración del cliente DNS se pueden establecer a través de ventanas y herramientas gráficas. Sin embargo, estos parámetros se guardan en archivos de configuración que, como suele ser tradicional en los sistemas Linux, tienen un formato de texto plano.

Los archivos de configuración del cliente DNS suelen ser los mismos y también pueden encontrarse en las mismas ubicaciones para las distribuciones más conocidas, aunque bien es cierto que pueden existir pequeños cambios. La tabla 2.4 enumera los archivos de configuración que guardan información sobre el funcionamiento del cliente DNS en Linux.

Tabla 2.4. Archivos de configuración del cliente DNS en Linux

Archivo	Descripción
/etc/resolv.conf	Es el archivo principal del cliente DNS que guarda las direcciones IP hacia donde se envían las consultas.
/etc/defaultdomain	Guarda el nombre del dominio al que pertenece el equipo local.
/etc/hosts	Contiene una tabla de correspondencias locales entre nombres de equipos y direcciones IP para consultar sin necesidad de enviar peticiones al DNS.
/etc/nsswitch.conf	Especifica la configuración de las bases de datos que necesita el sistema. En este archivo se especifica qué información se puede obtener y desde dónde, incluyendo el DNS.

EJEMPLO 2.17

Un ejemplo de archivo */etc/resolv.conf* puede ser el siguiente:

```
search bcs.com
nameserver 80.59.249.202
nameserver 80.59.249.254
```

Las líneas que comienzan por *nameserver* especifican las direcciones IP de los servidores DNS a los que se les van a enviar las consultas (por orden de prioridad). La línea que comienza por *search* se utiliza para especificar un nombre de dominio por defecto que es incluido cuando la consulta especifica un nombre de equipo pero ningún nombre de dominio. También se puede especificar la línea *domain* seguida del nombre del dominio al que pertenece el equipo (este nombre de cominio deberá ser el mismo que el indicado en el archivo */etc/defaultdomain*).

EJEMPLO 2.18

Un ejemplo de archivo */etc/defaultdomain* puede ser el siguiente:

```
bcs.com
```

En este archivo solamente se especifica una línea con el nombre del dominio al que pertenece el equipo, sin ningún otro parámetro.

EJEMPLO 2.19

Un ejemplo de archivo */etc/hosts* puede ser el siguiente:

```
127.0.0.1     localhost
192.168.1.101 ines
```

Cada línea de este archivo especifica una dirección IP y su correspondiente nombre de equipo. Normalmente, este archivo siempre contiene por defecto la línea correspondiente al equipo local *localhost*.

El archivo */etc/hosts* se ha utilizado tradicionalmente para resolver direcciones en pequeñas redes y conseguir un acceso rápido a través de los nombres de los equipos. Sin embargo, su uso debe limitarse a eso, ya que en redes más grandes o con dominios más complejos, es imposible realizar una gestión eficaz de este modo.

EJEMPLO 2.20

Un ejemplo de archivo */etc/nsswitch.conf* puede ser el siguiente:

```
passwd:     files nis
shadow:     files
group:      files nis
hosts:      files dns
ethers:     files
netmasks:   files
networks:   files
protocols:  files
rpc:        files
services:   files
automount:  files
aliases:    files
```

Cada línea especifica una base de datos, seguida del símbolo de dos puntos ":" y de la fuente desde donde se va a obtener la información. En el caso del DNS, la línea que nos interesa es la que comienza por la palabra *hosts*. En este ejemplo se especifican las fuentes "files" y "dns", lo que significa que, cuando se necesite obtener un nombre de equipo, primero se consultan los archivos locales (por ejemplo, */etc/hosts*) y, si no se resuelve, se consulta al DNS.

Además de los archivos de configuración anteriores, los clientes DNS Linux también pueden utilizar el **NSCD** (*Name Service Cache Daemon* o Demonio de Caché del Servicio de Nombres). Gracias a este proceso demonio, se pueden guardar las últimas consultas realizadas al DNS, de forma que si éste se vuelve a interrogar, la resolución será muy rápida. El archivo de configuración que gestiona el NSCD es */etc/nscd.conf*.

2.5.2.3 Comprobación de la configuración

Una vez se ha establecido la configuración del cliente DNS en Linux y, suponiendo que los servidores funcionan correctamente, puede ser necesario comprobar que todo funciona correctamente. Para ello, se pueden utilizar las siguientes órdenes ejecutadas desde el Terminal o interfaz de órdenes:

- **host**: permite realizar consultas al DNS si se especifica como parámetro un nombre de equipo o una dirección IP.
- **nslookup**: se utiliza para enviar consultas al DNS, tanto directas como inversas. Se puede especificar el nombre o dirección directamente como argumento de esta orden. También se puede escribir esta orden sin argumentos, lo que mostrará un símbolo ">" para introducir las consultas. Esta orden se considera actualmente obsoleta y se espera que finalmente desaparezca de las distribuciones a favor de *dig*.
- **dig**: herramienta de consulta al DNS que funciona de la misma forma que *nslookup*.

RESUMEN DEL CAPÍTULO

A los usuarios de Internet, sobre todo aquellos que no tienen conocimientos avanzados de Informática, les resulta muy difícil trabajar directamente con direcciones IPv4 o IPv6. Por esta razón, existe el protocolo DNS, que permite asignar nombres a los equipos y así son más fáciles de manejar y recordar. Este protocolo tiene que resolver las direcciones de forma automática, de forma que las direcciones IPv4 o IPv6 queden ocultas a los usuarios. Para realizar estas resoluciones, en la red deben instalarse servidores DNS que realicen estas tareas y mantengan tablas de correspondencias entre nombres de equipos y direcciones IP.

El sistema DNS está basado en una organización jerárquica en base a los equipos y no a la estructura física o topológica de la red. Esta jerarquía está organizada por los nombres genéricos en un nivel más alto, los nombres de los dominios y los subdominios en un nivel inferior y los nombres de los equipos en un nivel más bajo. Las direcciones de dominio se construyen desde el nivel inferior al superior, es decir, primero se escribe el nombre del equipo, a continuación los nombres de subdominios y dominios, para finalmente especificar el nombre genérico, todos separados por puntos.

Para cada dominio es necesario almencenar información sobre los equipos y sus direcciones IP, además de otra información como alias, servidores de correo, etc. A esta información se la conoce como registros de recursos. Un servidor DNS debe almacenar esta información para poder realizar las resoluciones de direcciones que se le piden.

Cuando se instala un servidor DNS y se crea un dominio en él, éste se convierte en la autoridad para ese dominio, es decir, es un servidor DNS primario. El servidor puede almacenar más de un dominio, en cuyo caso se dice que todos esos dominios pertenecen a la misma zona.

Un servidor DNS también puede trabajar como secundario o caché de nombres y, en ese caso, se utilizan para descargar de trabajo a los servidores primarios. Estos servidores reciben consultas y, o bien las reenvían a otros servidores (los de caché) o bien mantienen copias de los dominios almacenados en los servidores primarios (a través de transferencias de zona).

Cuando se configura un servidor DNS primario, es necesario definir en él los dominios para los que tiene autoridad (tanto para resolución directa como para resolución inversa). También se pueden definir en él dominios secundarios que están alojados en otros servidores y establecer transferencias de zonas con ellos.

Los sistemas Microsoft Windows en versión de servidor ofrecen la posibilidad de instalar todo lo necesario para que el equipo funcione como servidor DNS. En las versiones de cliente (Windows 2000/XP/Vista/7) es necesario utilizar paquetes de otros fabricantes para permitir que se comporten como servidores DNS (como por ejemplo, Dual Server). La mayoría de las distribuciones GNU/Linux también disponen del paquete BIND para instalar y configurar un servidor DNS. La configuración se puede realizar de una forma más cómoda utilizando la herramienta Webmin.

La configuración de un equipo cliente del servicio DNS se realiza de forma muy sencilla, ya que solamente es necesario especificar la dirección o direcciones IP de los servidores DNS a los que se les van a enviar las consultas. Es recomendable especificar más de una dirección, de forma que, si un servidor no contesta, se puede enviar la petición al siguiente de la lista.

Para comprobar si la configuración del servidor y el cliente DNS en Microsoft Windows es correcta, se puede utilizar la orden *nslookup*. Por su parte, en los sistemas Linux están disponibles las órdenes *host*, *nslookup* (actualmente obsoleta) y *dig*.

EJERCICIOS PROPUESTOS

- **1.** Utiliza la orden *nslookup* para obtener información del servidor DNS preferido de tu equipo. ¿Qué tipo de información te devuelve esta orden?
- **2.** En caso de que tu equipo tenga más de una dirección de un servidor DNS, ¿cuál de esos servidores es el que resuelve esas direcciones? Para contestar a esta pregunta, establece distintas direcciones de servidores DNS, algunas de ellas inexistentes (inventadas).
- **3.** Enumera todos los pasos que necesitas realizar para crear el dominio *midominio.local* en un servidor DNS Windows 2008.
- **4.** Enumera todos los archivos de configuración que necesitas y su contenido básico para crear el dominio *midominio.local* en un servidor DNS Linux.
- **5.** Descarga de Internet el programa DNS2Go que se usa para asociar una dirección IP dinámica con un dominio. Indica todos los pasos que debes seguir para configurar un dominio de prueba usando una dirección IP dinámica proporcionada por tu proveedor de acceso a Internet en Microsoft Windows.
- **6.** Repite el ejercicio anterior, pero esta vez sobre un equipo GNU/Linux, utilizando la herramienta DynDNS.
- **7.** Consulta cuál es la dirección IP asignada a tu equipo o tu red en Internet y cuál es el nombre de dominio que tiene esa dirección.

TEST DE CONOCIMIENTOS

1 Un nombre totalmente cualificado:
- a) Identifica a un dominio de Internet.
- b) Está formado por el nombre completo del dominio y del equipo.
- c) a y b son ciertas.
- d) Ninguna es cierta.

2 Una zona es:
- a) Un dominio.
- b) El conjunto de servidores DNS de una organización.
- c) Los dominios raíz.
- d) Ninguna es cierta.

3 Un registro de recursos:
- a) Se usa para almacenar información del dominio.
- b) Asocia una dirección IP a un nombre de equipo.
- c) Asocia un nombre de equipo con una dirección IP.
- d) Especifica el equipo que es autoridad para la zona.

4 Una transferencia de zona:
- a) Intercambia información entre los servidores para actualizar sus tablas.
- b) Se usa cuando hay que cambiar el servidor DNS a otro lugar.
- c) Se usa cuando el servidor DNS no conoce la dirección que se le consulta.
- d) Ninguna es cierta.

5 El identificador *ip6.arpa* se usa para:
- a) Definir un dominio de correspondencias directas.
- b) Definir un dominio de correspondencias inversas.
- c) Definir un registro de correspondencias directas.
- d) Definir un registro de correspondencias inversas.

6 Si deseamos disponer de un dominio en Internet necesitamos:
- a) Registrar el dominio en alguna empresa acreditada.
- b) Instalar y configurar convenientemente nuestro servidor DNS.
- c) Configurar los mecanismos de seguridad DNSSEC para evitar ataques e intromisiones.
- d) Todas son ciertas.

7 Para configurar correctamente un servidor DNS primario en Windows es necesario:
- a) Definir las zonas de búsqueda directa.
- b) Definir las zonas de búsqueda inversa.
- c) Crear los registros de recursos necesarios.
- d) Todas son ciertas.

8 Un registro *AAAA* especifica:
- a) Una correspondencia entre nombre de equipo y dirección IPv6.
- b) Una correspondencia entre dirección IPv6 y nombre de equipo.
- c) Una dirección IPv6 incompleta.
- d) Ninguna es cierta.

9 La opción "Crear una nueva zona subordinada" en Webmin se usa para:
- a) Definir un servidor DNS que va a funcionar como caché de nombres.
- b) Definir un servidor DNS que va a aceptar transferencias de zona.
- c) Definir un servidor DNS primario.
- d) Definir un servidor DNS secundario.

3 El servicio HTTP

OBJETIVOS DEL CAPÍTULO

- ✓ Describir el funcionamiento general del servicio HTTP.
- ✓ Describir la terminología relacionada, los principales lenguajes de creación de páginas y las variantes seguras de HTTP.
- ✓ Describir el funcionamiento de un servidor virtual.
- ✓ Describir las secciones de configuración y la función de los módulos del servidor de código abierto Apache.
- ✓ Instalar y configurar el servidor de código abierto Apache, así como la del servidor propietario IIS.
- ✓ Obtener informes de acceso al servicio HTTP.
- ✓ Conocer los elementos generales que incluye un cliente HTTP, particularizando en las características de los navegadores Internet Explorer y Konqueror.
- ✓ Configurar y utilizar las principales características de los clientes HTTP Internet Explorer y Konqueror.

La utilización de servicios como FTP (*File Transfer Protocol* o Protocolo de Transferencia de Archivos) ha posibilitado el acceso de los usuarios a información localizada en un equipo distante, aunque la forma de obtenerla resulta un tanto engorrosa, teniéndose que localizar previamente en el sistema de ficheros del equipo remoto antes de proceder a su transferencia y posterior visualización.

El protocolo HTTP (*HyperText Transfer Protocol* o Protocolo de Transferencia de HiperTexto) surgió para facilitar a los usuarios el acceso a información remota de una forma sencilla e intuitiva, dando lugar a lo que conocemos como WWW (*World Wide Web* o Telaraña Mundial). Hoy, el servicio HTTP es uno de los más utilizados y goza de gran popularidad en Internet.

3.1 FUNCIONAMIENTO DEL SERVICIO HTTP

Los usuarios que utilizan este servicio, acceden a documentos denominados **páginas** o **webs**. Además de texto, estas páginas pueden incluir otros elementos que también aportan información al usuario, como imágenes, sonido o vídeo. A veces los creadores de estas páginas, dan un carácter especial a algunos de sus elementos, permitiendo que a través de ellos se acceda a otras páginas o servicios, los cuales conocemos con el nombre de **hiperenlaces**. Estos enlaces aparecen de forma resaltada, el puntero del ratón modifica su aspecto al pasar sobre ellos (generalmente aparece en forma de mano) y permiten acceder a otra página al situar y hacer clic sobre ellos con el ratón. Al formato de estas páginas que permite incluir diversos tipos de información y referencias a otras páginas, se conoce como **hipertexto** o HTML (*HyperText Markup Language* o Lenguaje de Marcas de Hipertexto).

A priori, las **páginas estáticas** tienen un contenido que no admiten interacción por parte del usuario, simplemente se muestran y a lo sumo permiten el acceso a otras páginas mediante los mencionados hiperenlaces. Para conseguir que los usuarios interactúen con ellas, como por ejemplo, para rellenar un formulario recibiendo avisos si no se rellenaron todos los datos o por ser incorrectos, se requiere que las páginas sean programadas o **páginas dinámicas**. Algunos de los lenguajes y tecnologías utilizados para la creación de páginas dinámicas son:

- **PHP**: lenguaje cuyas instrucciones forman parte del documento HTML, se interpretan y procesan en el servidor HTTP y, posteriormente, se envía al cliente el documento HTML resultante.
- **ASP** (*Active Server Pages* o Páginas Activas de Servidor): su código se implementa mediante *scripts* y se combina con documentos HTML. Al igual que PHP, se interpreta en el servidor y el documento HTML resultante se envía al cliente. Derivado de ASP y aprovechando la tecnología .NET, surgió el lenguaje orientado a objetos ASP.NET, que permite la utilización de lenguajes soportados por el marco de trabajo .NET, como por ejemplo C#.
- **Java**: lenguaje de programación multiplataforma basado en C++ que permite incorporar animación e interacción en páginas mediante lo que se conoce como **applets**. Un applet es un pequeño programa que se obtiene y es ejecutado por el software cliente (navegador), como parte de la página solicitada. Un *servlet* también es un programa Java que se ejecuta en el servidor, cuya función es la de generar páginas en respuesta a las peticiones cliente.
- **JSP** (*Java Server Pages* o Páginas de Servidor Java): las páginas en JSP se escriben en HTML o XML, y utilizan etiquetas especiales para incluir contenido dinámico mediante código Java. El servidor interpreta o compila la página y, mediante *servlets*, genera una página en respuesta a la petición generada por el cliente. Se puede decir que JSP es utilizado como interfaz con el cliente, apoyándose en Java para aportar dinamismo a las páginas.

- **JavaScript**: lenguaje basado en Java. Sus instrucciones forman parte de una página o documento HTML y son interpretadas por el software del cliente o navegador.
- **CGI** (*Common Gateway Interfaz* o Interfaz de Pasarela Común): no es propiamente un lenguaje, sino un interfaz que permite a documentos HTML intercambiar datos, por ejemplo con programas C o Perl.
- **AJAX** (*Asinchronous JavaScript And XML* o JavaScript y XML Asíncrono): utiliza varias tecnologías como XML y JavaScript. La comunicación del cliente con el servidor la efectúa en segundo plano, facilitando la interacción con el usuario y evitándole recargas de página.

Para una visualización adecuada de las páginas, el cliente utiliza software específico denominado **navegador** o **visor**. El acceso a una página requiere que el usuario proporcione diversa información al navegador, como la página web que desea y dónde localizarla, especificando lo que se conoce como **URL** (*Uniform Resource Locators* o Localizador Uniforme de Recursos). Por tanto podríamos decir que una URL expresa la manera de acceder a un recurso utilizando un determinado servicio. Un ejemplo de URL podría ser: *http://fedoraproject.org/es/index.html*, cuyo formato se resume en la tabla 3.1.

Tabla 3.1. Descripción resumida de las partes de una URL

Parte de la URL	Descripción	Ejemplo
Servicio:	Indica el servicio o protocolo a utilizar, como *HTTP*, *HTTPS*, *FTP*, *gopher*, *telnet* o *news*.	*http:*
//	Es meramente un separador.	//
Servidor	Indica la dirección IP o nombre del servidor que contiene el recurso.	*www.opensuse.org*
Ruta_al_recurso	Indica el directorio y subdirectorios del sitio web donde reside el recurso. Puede omitirse.	*/es*
Recurso	Indica el recurso al que se quiere acceder. Si se omite el servidor buscará generalmente el fichero *index.html* o *index.htm*.	*/index.html*

Cuando un cliente indica una URL en su navegador, una vez resuelta por el servidor DNS que tenga configurado (véase capítulo 2), se estabece una conexión TCP con el puerto 80 del servidor, que permanece a la escucha de solicitudes HTTP. El navegador utiliza esta conexión para solicitar la página o recurso deseado al servidor mediante el envío de sencillas órdenes (véase ejemplo 3.1) y adjuntando la información necesaria, como el recurso solicitado y el protocolo utilizado. El servidor atiende la petición, y envía la página o el recurso solicitado, o bien un mensaje de error en forma de página web si no existe o no está disponible, mostrándose al cliente en su navegador (véase Figura 3.1).

Cuando se lleva a cabo la transferencia de información entre el cliente y servidor mediante el protocolo HTTP, no existe una conexión de control explícita para gestionar dicha transferencia, tal y como ocurre con el protocolo FTP (véase capítulo 4). Para este menester se utilizan las **líneas de encabezado**, que contienen información sobre la propia transferencia y se transmite antes del contenido en sí de la página web. Por ejemplo, cuando un cliente se autentica en un servidor web, el usuario y contraseña que ha introducido y que se transfiere al servidor, viaja en dichos encabezados. Dichas líneas de encabezado pueden incluir distintos encabezados y sus correspondientes valores.

EJEMPLO 3.1

Se desea obtener la página del servidor web con dirección IP 192.168.1.100 de nuestra red local. La forma de obtenerla será mediante la utilización de órdenes internas que emplea un navegador.

Antes de ejecutar la orden HTTP, se establece una conexión telnet con el servidor HTTP accediendo a su puerto 80:

```
[Eduardo@FedoraLnx ~]$ telnet 192.168.1.100 80
Trying 192.168.1.100...
Connected to 192.168.1.100.
Escape character is '^]'.
```

Se ejecuta la orden HTTP *GET*, que permite la obtención de una página web. En este caso se solicita la página web ubicada en el directorio raíz del sitio (/). La orden y un fragmento de la página obtenida sería el siguiente:

```
GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Mon, 09 Nov 2009 17:34:23 GMT
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 3607
Connection: close
Content-Type: text/html

<html>
<head>
<title>AppServ Open Project 2.5.10</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<style>
<!-- Hide style for old browsers
BODY          {font-family: MS Sans Serif;font-size="10"}
.headd { font-family: Helvetica,Verdana ; font-size: 13pt; text-decoration:  none; }
.app { font-family: MS Sans Serif ; font-size: 10pt; text-decoration:  none; }
A:link    {text-decoration: none; color: #0000FF}
A:visited {text-decoration: none; color: #0000FF}
A:hover   {text-decoration: none; color: #FF0000}
A:active  {text-decoration: none; color: #FF0000}
-->
</style>
</head>
<body bgcolor="#FFFFFF">
<div align="left">
  <table border="0" width="100%" height="19">
    <tr bgcolor="#FFD2F8">
      <td width="100%" height="19" valign="top"><font color="#000080">
  <span class="headd"><strong><big>  The AppServ Open Project - 2.5.10 for
  Windows </big></strong></span></font></td>
    </tr>
  </table>

</div>
<div align="left">
.
.
.
</div>
</body>
</html>
```

Las páginas que se ofrecen a los usuarios se almacenan en los servidores HTTP, localizándose en un directorio específico denominado **sitio** o **sitio web**. En este directorio, se suele establecer una jerarquía de subdirectorios para organizar las distintas páginas, así como los distintos elementos que las integran (fondos, imágenes, webs, etc). La página *index.html* o *index.htm* se situa en el directorio raíz de la jerarquía del sitio y se utiliza a modo de índice para dar acceso al resto de páginas y elementos del sitio. Esta página también se muestra por defecto cuando en la URL solo se indica el servidor al que se quiere acceder.

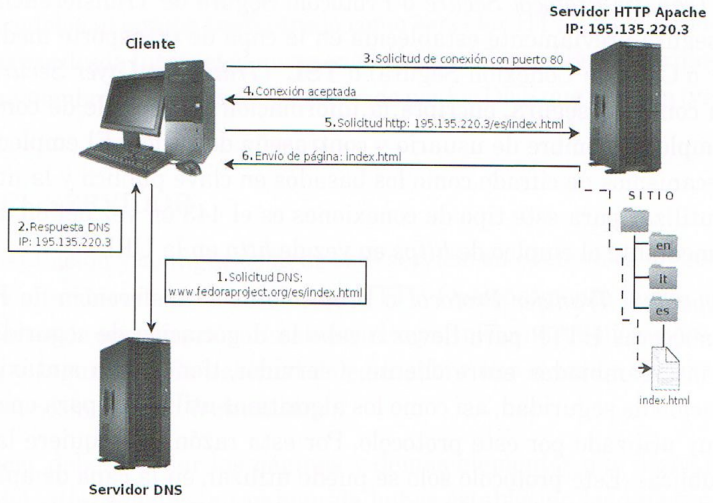


Figura 3.1. *Esquema de funcionamiento del servicio HTTP. Al indicar http://fedoraproject.org/es/index.html en el navegador, el servidor DNS resuelve la dirección IP del servidor HTTP (http://fedoraproject.org) y se establece una conexión HTTP con el servidor, el cual proporciona la página solicitada (index.html) al cliente, ubicada en el directorio es del sitio web*

Entre el cliente y el servidor se puede transfererir cualquier tipo de contenido, aunque debería estar definido por el estándar MIME (*Multipurpose Internet Mail Extension* o Extensión de Correo Multipropósito de Internet). *A priori* este estándar se definió para el envío de mensajes de correo electrónico, aunque posteriormente también se ha utilizado para transferencias de información mediante el protocolo HTTP. Este estandar define los formatos, tipo de letra y características de una página para que pueda ser visible por distintos navegadores. Si al crear las páginas no se especifica su formato, el navegador no lo reconocerá, presupondrá el tipo de contenido a visualizar y podrá mostrarlo de forma incorrecta. En el ejemplo 3.2 puede observar la siguiente línea html, que incluye una etiqueta *meta* para especificar el tipo de contenido de la página web (*text/html*).

```
<meta http-equiv="Content-Type" content="text/html;
```

La extensión al protocolo HTTP 1.1 **WebDAV** (*Web-based Distributed Authoring and Versioning* o Edición y Versionado Distribuidos sobre la Web), nos proporciona un entorno de colaboración para la elaboración y administración de los elementos del sitio de una forma remota y descentralizada. Es decir, aquellas personas encargadas de la elaboración de los diferentes elementos del sitio como webs, imágenes, vídeos o sonidos, y teniendo acceso al servidor, podrían, por ejemplo, editar los contenidos *online* o mover los ficheros de directorio dentro de la jerarquía del sitio. Para un mejor control de los cambios efectuados sobre los elementos del sitio, se lleva a cabo mediante software de control de versiones, como es el caso de **CVS** (*Concurrent Versioning System* o Sistema de Versiones Concurrentes). Paquetes ofimáticos como Open Office o Microsoft Office, ya incorporan soporte para WebDAV.

3.1.1 ACCESO SEGURO Y UTILIZACIÓN DE CERTIFICADOS

En ocasiones, el acceso a determinadas páginas puede requerir determinada información confidencial, como la referente a transacciones financieras o la autenticación en servidores de correo. Debido a que la información viaja por la red sin cifrar, puede ser interceptada por un usuario malintencionado para hacer mal uso de ella, comprometiendo la seguridad del cliente. Para paliar este problema surgieron algunos protocolos:

- **HTTPS** (*HyperText Transfer Protocol Secure* o Protocolo Seguro de Transferencia de HiperTexto): se apoya sobre una conexión segura previamente establecida en la capa de transporte mediante la utilización de **SSL** (*Secure Socket Layer* o Capa de Conexión Segura) o **TSL** (*Transport Layer Security* o Seguridad de la Capa de Transporte). Esta conexión segura, encripta la información susceptible de comprometer la seguridad del cliente, como por ejemplo su nombre de usuario y contraseña de sesión. El empleo de este tipo de conexiones seguras, requiere mecanismos de cifrado como los basados en clave pública y la utilización de certificados. El puerto que se suele utilizar para este tipo de conexiones es el 443 en vez del 80. El cliente hará referencia a este servicio seguro mediante el empleo de *https* en vez de *http* en la URL.
- **S-HTTP** (*Secure HyperText Transfer Protocol* o Protocolo de Transferencia de HiperTexto Seguro): utiliza extensiones de las cabeceras HTTP para llevar a cabo la negociación de seguridad entre cliente y servidor. Dichas extensiones intercambiadas entre cliente y servidor, tienen una sintáxis concreta donde incluyen determinada información de seguridad, así como los algoritmos utilizados para encriptar la información, como por ejemplo PGP, muy utilizado por este protocolo. Por esta razón, no requiere la utilización de certificados digitales ni claves públicas. Este protocolo solo se puede utilizar, en la capa de aplicación, y no es válido para soportar y asegurar la utilización de otros protocolos como ocurre con SSL. La extensión de los documentos utilizados con este protocolo es "*.shttp*". Este protocolo no ha tenido tanta aceptación como el anterior, de hecho existen pocos navegadores que soporten dicho protocolo.

Los certificados son utilizados para permitir que las comunicaciones sean seguras. Se basan técnicas de encriptación, como los algoritmos de cifrado asimétrico, que utilizan una clave pública conocida por el emisor y el receptor, y una clave privada solo conocida por el destintario de la información. La información a transmitir se encripta con la clave pública y solo el que posee la clave privada será capaz de desencriptar la información. Algunos de los algoritmos utilizados son el RSA, Triple DES (o TDES) y AES, así como el X.509 de la ITU-T, que se ha establecido como estándar para los certificados.

La utilización de un certificado permite que su titular se identifique y autentique a la hora de acceder a un sitio cuya información puede verse comprometida, por ejemplo cuando queremos acceder a la Agencia Tributaria para hacer la declaración de la renta *online*.

Un certificado de usuario es firmado por una entidad certificadora o CA (*Certification Authority*) como por ejemplo la Fábrica Nacional de Moneda y Timbre (FNMT) o *Verisign*, de forma que garantiza su autenticidad. Siguiendo con el ejemplo de la Agencia Tributaria, cuando accedemos mediante nuestro certificado de usuario, dicha entidad confía en la entidad certificadora, la FNMT, y por tanto nos permitirá el acceso. Cuando confiamos en una entidad certificadora, debemos instalar su certificado denominado raíz (autofirmado por la CA), de forma que los certificados que dicha entidad haya firmado significará que también son de nuestra confianza.

Cuando accedemos a un sitio web mediante el protocolo HTTPS, necesitamos conocer previamente que el servidor es realmente de la entidad a la que queremos acceder. Para demostrarlo deberá poseer un certificado, el cual debe estar firmado por una CA que sea de nuestra confianza. En caso contrario, cuando accedamos al sitio web mediante nuestro navegador, nos pedirá confirmación para proseguir con nuestos trámites.

La tramitación de la firma de certificados por entidades certificadores como *Verisign*, suelen conllevar gastos, aunque como alternativa se pueden utilizar certificados autofirmados, que se pueden generar con herramientas software como OpenSSL. Para probar la utilización de certificados, puede acceder a la página web de *Verisign* para la descarga de un certificado de carácter temporal (véase enlaces de interés de este capítulo).

3.2 PARÁMETROS DE CONFIGURACIÓN DEL SERVICIO HTTP

Como requisito previo del software cliente y servidor, necesitará tener configurado correctamente el acceso a la red TCP/IP. Para que su servidor HTTP sea accesible desde Internet y los clientes puedan utilizar este servicio, recuerde que debe habilitar el acceso al puerto HTTP (por defecto el 80) de su router. Además, las solicitudes cliente que hagan referencia a dicho servicio, deberá redirigirlas al equipo configurado como servidor HTTP. Si el servidor dispone de cortafuegos, también deberá permitir el acceso desde Internet al mencionado puerto. Si también desea que los clientes puedan acceder al servidor HTTP mediante un nombre FQDN, ha de ser conocido por los DNS que utilizan (véase capítulo 2).

3.2.1 PARÁMETROS DEL SERVIDOR

Antes de proceder a la instalación y configuración de este servicio en cualquiera de las plataformas, se debe crear o determinar el directorio donde ubicará la raíz del sitio HTTP. Opcionalmente puede establecer una jerarquía de páginas y subdirectorios a efectos de organización. Establezca los permisos adecuados sobre directorios y subdirectorios a efectos de administración y seguridad. Es habitual delegar sobre uno o varios usuarios la responsabilidad de la gestión del sitio, los cuales conocemos como **webmaster**.

Antes de iniciar el servicio, deberá alojar las páginas y demás elementos que desee ofrecer a los usuarios en el directorio correspondiente del sitio. Asegúrese también de haber establecido los hiperenlaces de manera adecuada para que hagan referencia a la página o elemento deseado. Utilice una página índice del sitio para permitir el acceso a los diferentes elementos que lo conforman.

Una vez establecido el directorio raíz del sitio, podremos configurar parámetros adicionales, como el soporte para conexiones seguras mediante HTTPS, requerir la autenticación de los usuarios para acceder al sitio, o la utilización de sitios adicionales sobre el mismo servidor.

La configuración de un acceso seguro mediante HTTPS, requerirá la instalación en el servidor de un certificado, autogenerado por el sistema operativo o firmado por una CA.

3.2.2 PARÁMETROS DEL CLIENTE

La utilización del software cliente de este servicio, básicamente consiste en indicar la URL deseada en el campo destinado a tal efecto en un navegador. Ciertos contenidos requieren la instalación de elementos adicionales o configurar el navegador de forma adecuada, activando o desactivando las opciones pertinentes. El navegador también tiene opciones propias de configuración, como las relativas al aspecto y comportamiento. Si el equipo pertenece a una organización con proxy, debe configurar el navegador indicando el equipo o dispositivo que ejerce de proxy.

No todos los navegadores permiten visualizar todas las tecnologías disponibles para documentos web, como por ejemplo distintas versiones de CSS (*Cascading Style Sheets* u Hojas de Estilo en Cascada). Por tanto, y antes de elegir un cliente para este servicio, deberá conocer la utilidad que le dará y las limitaciones de los candidatos seleccionados.

El acceso a sitios web mediante HTTPS, requerirá preceder al FQDN del sitio al que deseamos acceder de *https://*, en vez de *http://*. Al acceder el navegador mostrará una advertencia en caso de que el certificado no haya sido firmado por una CA de nuestra confianza, permitiéndonos decidir su instalación o no. La mayoría de navegadores muestran en su barra de estado el símbolo de un candado para distinguir el acceso a un sitio web seguro mediante HTTPS, advirtiéndonos de que vamos a acceder a una página segura.

3.3 CONFIGURACIÓN DEL SERVIDOR HTTP

En este apartado se aborda el software de servidor HTTP **IIS** (*Internet Information Server* o Servidor de Información de Internet), utilizado por un amplio abanico de sistemas operativos Microsoft Windows, como 2000, XP Professional, 2003, 2008, Vista y 7. Tampoco nos olvidemos del popular servidor de software libre **Apache 2**, utilizado habitualmente sobre plataformas GNU/Linux como Fedora 11, Debian 5 y OpenSuSE 11.1, y también disponible para plataformas Microsoft Windows.

3.3.1 CONFIGURACIÓN EN MICROSOFT WINDOWS

Los sistemas operativos Windows permiten la instalación de un servidor HTTP mediante la utilidad IIS incluida en los discos de instalación. Esta utilidad solamente puede instalarse en versiones Windows NT Server, 2000 Server, 2000 Advanced Server, XP Professional, 2003 Server, Vista (Business, Enterprise y Ultimate), 7 (Professional, Enterprise y Ultimate) y 2008 Server.

Para comprobar si IIS se encuentra instalado en el equipo puede consultar la tabla 3.2, donde se muestran cada uno de los pasos (iconos, accesos directos, apartados, etc) en cada uno de los sistemas operativos Windows mencionados. Tenga en cuenta que se toma como punto de referencia el *Panel de Control*.

Tabla 3.2. Pasos para la consulta de la instalación de IIS en un sistema operativo Windows

Sistema Operativo	Pasos de Consulta del Servicio FTP
NT	1. Red. 2. Protocolos. 3. Protocolo TCP/IP. 4. Servicios. 5. Microsoft Internet Information Server 2.0. 6. Detalles.
2000 y XP (Professional)	1. Agregar o quitar programas. 2. Agregar o quitar componentes de Windows. 3. Servicios de Internet Information Server (IIS). 4. Detalles.
2003	1. Agregar o quitar programas. 2. Agregar o quitar componentes de Windows. 3. Componentes. 4. Servidor de Aplicaciones. 5. Servicios de Internet Information Server (IIS). 6. Detalles.
Vista (Business, Enterprise y Ultimate) y 7 (Professional, Enterprise y Ultimate)	1. Programas. 2. Programas y Características. 3. Activar o desactivar las características de Windows. 4. Internet Information Services.
2008	1. Herramientas administrativas. 2. Administrador del servidor. 3. Resumen de Funciones. 4. Funciones.

El nombre del servidor realmente consiste en el FQDN del servidor (véase capítulo 2), compuesto por el nombre del equipo (habitualmente *www*) y el del dominio (en este caso *opensuse.org*).

Si el servicio no se encuentra instalado en nuestro equipo, en función del sistema operativo que tenga instalado y partiendo del último paso indicado en la tabla 3.2, deberá llevar a cabo las siguientes operaciones:

1 Pulse en el botón "Agregar" (Windows NT) o seleccione el componente a instalar (versiones 2000 y XP) y marque el servicio Microsoft Internet Information Server (Windows 2000) o Servicios de Internet Information Server (versión XP). En Windows 2003 seleccione el icono Servidor de Aplicaciones, pulse el botón Detalles y marque Instalar Internet Information Services (IIS). En versiones Vista o 7 despliegue "Internet Information Services" así como "Herramientas de administración web". En 2008 Server pulse sobre "Agregar funciones" en el subapartado "Funciones".

2 Durante la instalación se pedirá que seleccione los elementos de IIS a instalar. Para el servicio HTTP los más importantes son la herramienta principal de administración de IIS, el Administrador del Servicio de Internet (Consola de administración en Vista, 7 y 2008), y el propio Servicio World Wide Web (Servidor Web en 2008 y Servicios World Wide Web en Vista y 7).

3 Finalmente, en el caso de la instalación del servicio IIS en Windows NT se especificarán las carpetas que contendrán los ficheros de dicho servicio. Es recomendable que contengan solamente aquella información que queramos compartir y que el sistema de ficheros utilizado sea NTFS para un mejor control de la seguridad. En IIS de Windows 2000, XP, 2003, Vista, 7 y 2008, estas carpetas se establecen al configurar el servicio.

La principal herramienta para gestionar los servicios de IIS es el *Administrador de Servicios de Internet,* aunque recibe diferentes nombres en las distintas versiones de sistemas operativos Windows. En Windows NT y 2000 es el Administrador de Servicios de Internet, para Windows XP recibe el nombre de Servicios de IIS, para Windows 2003, 2008, Vista, 7 el de Administrador de IIS. Estas herramientas son accesibles en su correspondiente sistema operativo desde el menú de inicio del sistema en la opción "Inicio || Panel de Control || Herramientas administrativas" para versiones 2000, XP, 2003 y 2008. En versiones Vista y 7, tendrá que acceder previamente a "Sistema y Seguridad".

El primer paso es añadir el equipo que actuará como servidor a la lista del administrador de IIS, permitiéndose un equipo local o remoto. Después, y a pesar de que IIS nos ofrece un sitio web predeterminado (carpeta *\inetpub\wwwroot*), podemos crear uno nuevo mediante la opción del menú principal "Acción || Nuevo" (habiendo seleccionado el icono del servicio), o mediante la acción "Agregar sitio web" en 2008, Vista y 7. El servidor IIS de Windows 2000, 2003, Vista, 7 y 2008 permiten la administración de varios sitios web, mientras que Windows XP solamente permite la administración del sitio web predeterminado. Para alojar distintos sitios web en el servidor, ha de asociarse un puerto distinto a cada uno para poder atender las peticiones cliente. Cada uno de los sitios web podrán establecerse localmente o en un equipo remoto.

Cuando se crea un nuevo sitio web, hay que proporcionar al asistente los siguientes parámetros:

- Nombre o breve descripción del sitio para que el administrador pueda identificarlo y el grupo de aplicaciones a las que el contenido del sitio pertenece. En Windows 2008, Vista y 7, hay que indicar el parámetro "Grupo de Aplicaciones", aunque IIS crea un nuevo grupo con el mismo nombre para el sitio creado. Una aplicación es un grupo de archivos que se ofrecen como contenido del sitio web y cada una pertenece a un grupo de aplicaciones. Cada sitio tiene una aplicación predeterminada, pudiendo tener otras adicionales.

- Directorio local o remoto donde se alojará toda la jerarquía de páginas y subdirectorios del sitio web que proporcionará el servicio. Si el directorio es remoto se utilizará una nomenclatura **UNC** (*Universal Naming Convention* o Convención de Nombres Universal) para referenciarlo. Si este recurso remoto requiere usuario y contraseña para acceder a él, podremos indicarlos mediante las denominadas **credenciales**.

La nomenclatura UNC utiliza el formato *servidor**recurso_compartido* para referenciar un recurso ubicado en otro servidor.

- Direcciones IP del servidor por las que atenderá peticiones (por defecto por cualquier dirección IP), el protocolo utilizado para acceder el servicio (HTTP o HTTPS) y el puerto de acceso al sitio, estableciéndose por defecto el 80 para HTTP y 443 para HTTPS. Al seleccionar como protocolo HTTPS, se puede especificar el certificado SSL a utilizar (véase apartado 3.3.1.1). Opcionalmente se puede especificar un nombre para el servidor.
- Permisos de acceso sobre los usuarios que acceden al sitio, como lectura de su contenido y ejecución de determinadas órdenes y aplicaciones específicas como CGI (solo versiones anteriores a 2008, Vista y 7).
- Inicio inmediato o no del servicio (en versiones 2008, Vista y 7).

En Windows 2003 se pueden establecer otros parámetros seleccionando la opción "Propiedades" del menú contextual del sitio web creado. Los parámetros se agrupan en secciones, algunas de las cuales se describen brevemente a continuación:

- **Sitio Web**: permite configurar el puerto HTTP, SSL y las direcciones IP de atención de peticiones, establecer un tiempo de espera determinado para las conexiones y llevar un registro periódico de los accesos de los usuarios.
- **Rendimiento**: permite limitar el ancho de banda utilizado en el acceso al sitio, así como el número de conexiones cliente que podrá aceptar el servidor.
- **Directorio Particular**: establece un directorio local o remoto como raíz del sitio web, los privilegios (Lectura y Escritura) que los usuarios tendrán sobre él y el formato en el que se mostrará la jerarquía de carpetas y ficheros que aloja (MSDOS o UNIX).
- **Documentos**: se indican los documentos o páginas que pueden actuar como índice del sitio, como por ejemplo *index.htm*. Pulse sobre el botón "Agregar" para añadir una nueva página índice.
- **Errores personalizados**: se indican los códigos de error de acceso al servicio y la página web que contiene el mensaje de error asociado. Seleccione el error y pulse sobre "Modificar..." para asociarle otro documento con el mensaje de error.
- **Seguridad de Directorios**: permite restringir los equipos, grupos de equipos o dominios a los que se les concederá o denegará la conexión con el servidor, debiendo indicarse la dirección IP (un equipo), la máscara de red (grupo de equipos) o el nombre del dominio (un dominio). También permite habilitar o deshabilitar el acceso anónimo y exigir la autenticación a los clientes a contenidos restringidos, así como habilitar la utilización de un canal seguro SSL (véase apartado gestión de certificados y acceso seguro con HTTPS).
- **Encabezados HTTP**: entre otras cosas permite que los clientes identifiquen el tipo de contenido que el sitio proporciona en cuanto a Sexo, Violencia, Desnudez y Lenguaje.

En los sistemas operativos Windows 2008, Vista y 7, mediante el Administrador de IIS y al pulsar sobre el sitio web del panel izquierdo "Conexiones", podemos establecer parámetros adicionales mediante cada uno de los iconos que se muestran en la ventana central. Tenga en cuenta que algunos de los parámetros están asociados a la utilización de páginas dinámicas. A continuación se describen brevemente dichos parámetros:

- **Almacenamiento en caché de resultados**: permite establecer **reglas de caché**, que consisten en especificar ciertos parámetros para indicar las páginas del sitio solicitadas por los clientes que se almacenarán en caché. Por ejemplo, se puede indicar el almacenamiento de páginas con una determinada extensión, que se reemplace su contenido durante un tiempo determinado, o simplemente podemos deshabilitar el almacenamiento en caché.
- **Módulos**: permiten agregar o modificar **módulos administrados** o configurar o modificar **módulos nativos** para ponerlos a disposición del grupo de aplicaciones del sitio. Un módulo es un programa que realiza una tarea concreta al procesarse las solicitudes de los clientes, sin embargo, no genera una respuesta, delegándola en los controladores. Un módulo puede ser administrado o nativo, dependiendo si se ha creado mediante el marco de trabajo ASP.NET o no.
- **Asignaciones de controlador**: nos permite habilitar diversos controladores que darán respuesta a las solicitudes cliente. Los controladores, como los módulos, son programas administrados o nativos, pero generan respuestas a las solicitudes cliente. IIS selecciona el controlador que procesará cada solicitud en función de su tipo y de la extensión de la página solicitada.
- **Autenticación**: por defecto el acceso al sitio web es anónimo, aunque mediante esta opción se puede deshabilitar, o bien especificar un nombre de usuario registrado y su contraseña para acceder al sitio.
- **Compresión**: permite comprimir el contenido del sitio al transferirse al cliente, reduciéndose el ancho de banda empleado. Su utilización requiere la instalación del módulo correspondiente, como *StaticCompressionModule* para contenido estático.
- **Configuración de SSL**: utilizada cuando el sitio se creó para acceso mediante HTTPS. Permite o requiere conexiones SSL en las conexiones cliente, pudiendo establecerse un cifrado más eficaz de 128 bits, aunque consumirá más recursos del procesador y el tiempo en la transferencia se puede ver incrementado.

Puede importar, crear y completar una solicitud o crear un certificado de dominio o autofirmado desde *Certificados de servidor*, accesible en IIS al pulsar sobre el icono de su servidor.

- **Documento predeteminado**: nos permite indicar los archivos del sitio web que pueden ejercer como página índice (véase apartado 3.1).
- **Encabezados de respuesta HTTP**: permite personalizar los encabezados de las páginas que demandan los clientes. Por defecto, en el encabezado se proporcionan los valores de la versión del protocolo, la fecha y el tipo de contenido, pudiéndose añadir otros valores asignándoles un nombre.
- **Exámen de directorios**: permite habilitar la información que se mostrará al cliente sobre los directorios del sitio web, como la hora o la fecha.
- **Páginas de errores**: permite personalizar las páginas de error enviadas a los clientes, bien modificando el contenido de la página devuelta por defecto o indicando una URL local o remota distinta a la establecida por defecto.

- **Registro**: permite llevar un registro de las conexiones cliente mediante archivos de registro. Podemos decidir el directorio donde se ubicarán, la información que queremos registrar, su formato y el método utilizado para crear un nuevo archivo, pudiéndose crear periódicamente, cuando el fichero actual supere un determinado tamaño, o simplemente no crearlo.
- **Tipos MIME**: nos permite ver, agregar, eliminar y modificar los tipos de documentos soportados por el servidor web y que podrían solicitar los clientes mediante un navegador.

Windows XP, 2003, Vista, 7 y 2008, también nos permiten la creación de los denominados **Directorios Virtuales** en un sitio web. Un Directorio Virtual no es un directorio como tal incluido dentro del sitio y su función se asemeja a la de un acceso directo. Aunque se incluye dentro del sitio, hace referencia a un directorio local o remoto ubicado fuera de la jerarquía de directorios del sitio. Para crearlos, seleccione un sitio creado y elija la opción del menú contextual "Nuevo | | Directorio Virtual" en 2003 o XP, o "Agregar directorio virtual..." en 2008, Vista y 7. El asistente solicitará un alias o nombre para este directorio ficticio, la carpeta local o remota a la que hará referencia y los permisos de acceso (versiones 2003 y XP), o la autenticación de paso a través (versiones 2008, Vista y 7).

Desde el Administrador de Servicios de Internet se pueden parar, reanudar y reiniciar en cualquier momento el servicio para el sitio creado. En 2003 o XP puede utilizar los botones que se encuentran en la barra de herramientas de esta utilidad, o a través de la opción "Acción | | Iniciar" del menú principal. En 2008, Vista y 7 acceda al apartado "Administrar sitio web" del panel derecho para seleccionar la acción deseada. Pruebe su funcionamiento indicando como URL de su navegador *http://localhost*, debiendo mostrarse la página índice del sitio que ha creado. También podemos utilizar el panel "Acciones" para su comprobación mediante el subapartado "Examinar sitio web", pulsando sobre "Examinar *servidor:puerto (protocolo)*".

EJEMPLO 3.2

Se desea proporcionar el servicio HTTP mediante un servidor Windows 2008 Server. Este servidor dispone de dos interfaces de red configurados con las direcciones IP 192.168.0.93 y 10.0.1.93, respectivamente. Como carpeta raíz del sitio se determina *C:\www* a la que podrán acceder todos los usuarios. A efectos de organización, el sitio recibirá el nombre de "Externo" y tan solo aceptará peticiones HTTP a través de la interfaz con IP 10.0.1.93.

Suponiendo que la utilidad IIS está instalada, iniciamos el *Administrador de Servicios de Internet* ("Inicio || Herramientas administrativas || Administrador de IIS").

Creamos la siguiente jerarquía de carpetas para ubicar las páginas y los elementos que las integran:

C:\www
botones
webs
imagenes

En *C:\www* crearemos una página como índice del sitio denominada *index.html* que dará acceso al resto de páginas y elementos que se han crearse si no están creados.

Seleccionamos la acción "Agregar sitio web..." y proporcionamos al asistente los parámetros siguientes:

- **Nombre del sitio**: "Externo".
- **Grupo de aplicaciones**: El creado por defecto (Externo).
- **Ruta al directorio raíz**: *C:\www*

- **Tipo de protocolo utilizado**: HTTP.
- **Direccion IP y puerto de acceso al sitio**: Como dirección IP indicamos la 10.0.1.93. El puerto se deja el indicado por defecto (80).
- **Iniciar servicio inmediatamente**: Lo desmarcamos, ya que hay que comprobar que *index.html* puede ejercer de índice del sitio antes de iniciar el servicio y que todos los usuarios tienen permiso de lectura sobre el directorio raíz.

Seleccionaremos en el administrador del servicio el icono del sitio creado ("Externo") en el panel "Conexiones", y mediante el icono "Documento predeterminado" comprobamos que *index.html* aparece en el panel central, indicándonos que puede ejercer de página índice. Si no está utilizaremos la opción "Agregar" del panel derecho "Acciones" para añadirlo. De esta manera, conseguiremos que automáticamente aparezca esta página índice al cliente cuando indique en su navegador el nombre o dirección IP de este servidor.

Para asegurarnos que todos los usuarios tienen permiso de lectura sobre el sitio web, seleccionamos nuestro sitio del panel "Conexiones", posteriormente pulsamos sobre la acción "Editar permisos..." del panel "Acciones" y comprobamos en la pestaña seguridad que el grupo "Users" tiene permiso de lectura".

Para poner a disposición de los clientes el sitio creado, seleccionaremos en el administrador del servicio del sitio el icono "Externo" del panel "Conexiones" y elegiremos la opción "Iniciar" del apartado "Administrar sitio web" del panel "Acciones".

Para probar su funcionamiento, ejecutamos un navegador, por ejemplo Internet Explorer, e indicamos como URL *http://10.0.1.93*, no siendo válido indicar *http://localhost* debido a la restricción de acceso realizada, estando limitado el acceso al servicio HTTP a uno de las interfaces de red del servidor.

3.3.1.1 Gestión de certificados y acceso seguro con HTTPS

En las versiones del sistema opertivo Windows que soportan IIS, como Windows 2000 Server, XP Professional, 2003 Server, Vista, 7 y 2008 Server, permiten la generación de un certificado en un fichero de texto previa solicitud de determinada información por parte de un asistente. Posteriormente habrá que contactar con una CA para que firme el certificado y nos lo remita mediante un fichero con extensión "*.cer*", el cual habrá que instalar. Cuando se genera el certificado en texto, el sistema operativo crea una petición y la establece como pendiente hasta que lo recibamos firmado por la CA. En Windows 2000 Server, XP Professional y 2003 Server, puede crear dicha solicitud al seleccionar la opción "Propiedades" del menú contextual del sitio web y una vez iniciado el Administrador de IIS. En la ficha "Seguridad de directorios" apartado "Comunicaciones seguras", encontrará un botón denominado "Certificado de servidor...", el cual iniciará un asistente que le permitirá generar de forma cómoda el certificado para solicitar su firma posterior. Este asistente también está disponible en Windows Vista, 7 y 2008 Server, que requiere acceder de igual manera al Administrador de IIS y pulsar sobre el enlace "Crear una solicitud de certificado..." del panel derecho "Acciones".

En las versiones Vista, 7 y 2008, mediante IIS es posible la generación de certificados autofirmados con extensión "*.pfx*" (*Personal Information Exchange File* o Fichero de Intercambio de Información Personal), y requiere los siguientes pasos:

1 Ejecute el *Administrdor de IIS* que encontrará en las "Herramientas administrativas" del "Panel de Control".

2 Seleccione en el panel izquierdo el servidor para el que desea emitir el certificado y haga doble clic en el icono "Certificados de servidor" del apartado IIS del panel central.

3 En el panel de "Acciones", seleccione el enlace "Crear certificado autofirmado".

4 Se mostrará un cuadro de diálogo que nos solicita un nombre descriptivo para generar el certificado. Después de escribirlo pulsaremos sobre "Aceptar".

5 Tras su generación le aparecerá en el panel central. Al hacer doble click sobre él, podrá observar distintos detalles de su creación, como el algoritmo empleado para la clave pública y el número de bits.

La instalación de certificados (no solicitados previamente) requiere los siguientes pasos:

1 Acceda a las "Herramientas administativas" a partir del "Panel de Control".

2 Ejecute el Administrador de IIS.

3 Seleccione el sitio web en el que desee instalar el certificado y utilice el menú contextual para seleccionar la opción "Propiedades" (versiones anteriores a Windows Vista) o haga doble clic sobre el icono "Certificados de servidor" (versiones igual o posterior a Windows Vista).

4 En versiones anteriores a Windows Vista, acceda a la ficha "Seguridad de directorios" y pulse el botón "Certificado de servidor" que ejecutará un asistente. En versiones posteriores a Windows Vista, seleccione "Importar" del panel de "Acciones".

5 En versiones anteriores a Windows Vista, deberá escoger entre una de las siguientes opciones:

- Crear certificado nuevo: creará un certificado nuevo mediante un asistente, el cual requerirá su envío a una CA para su firma y, por tanto, tendrá que costearlo.
- Asignar un certificado ya existente: permitirá utilizar un certificado previamente utilizado.
- Importar un certificado de un archivo de copia de seguridad del Administrador de claves: permite la importación de archivos con extensión "*.key*".
- Importar un certificado desde un archivo pfx: permite la importación de archivos con extensión "*.pfx*". Si desea instalar un certificado autofirmado debe seleccionar dicha opción.

En versiones posteriores a Windows Vista indique la ruta donde tiene ubicado el certificado e indique la contraseña en caso de que previamente fuera exportado.

En Windows 2000 Server, XP Professional y 2003 Server, puede configurar el servidor para proporcionar páginas mediante HTTPS utilizando el certificado instalado. Seleccione la opción "Propiedades" del menú contextual del sitio web una vez iniciado el Administrador de IIS. En la ficha "Seguridad de directorios", apartado "Comunicaciones seguras", encontrará un botón denominado "Modificar". Marque la casilla "Requerir canal seguro" y, "Necesita cifrado de 128 bits" en caso de que el navegador del cliente lo soporte. Si quiere utilizar SSL en su versión 3, seleccione "Requerir certificados de cliente". En cambio, si quiere utilizar SSL en su versión 2, seleccione "Ignorar certificados de cliente". La configuración para soportar HTTPS en las versiones Vista, 7 y 2008 se ha expuesto en la creación de un sitio web.

3.3.2 CONFIGURACIÓN EN GNU/LINUX

Este apartado describe una sencilla forma de configuración del servicio mediante los diferentes cuadros de diálogos de diversas herramientas para distribuciones OpenSuSE 11.1 y Fedora, que nos permiten gestionar el software de servidor HTTP Apache 2. También se explican brevemente los parámetros del fichero principal de configuración que deben establecerse para instalar un servidor web básico y servidores web virtuales basados en nombre.

En Distribuciones Debian, y en general para entornos de escritorio GNOME, está disponible la herramienta **rapache**, aunque no se tratará en este capítulo ya está en desarrollo pero apenas existe documentación.

Para entender algunos aspectos del funcionamiento y configuración de Apache 2, conviene explicar previamente algunas de las características particulares de este software:

- Permite añadir nueva funcionalidad al servicio mediante la utilización de **módulos**, ofreciendo mayores prestaciones de cara a los usuarios finales. Entre otras cosas, este software permite la interpretación de lenguajes de programación de páginas como PHP (por ejemplo, para interacción con distintos sistemas gestores de bases de datos como MySQL) o para asegurar las transferencas de datos.
- Ofrece la posibilidad de configurar el servicio para permitir el acceso a diferentes sitios web ubicados en un mismo servidor HTTP, dando la impresión al cliente de estar accediendo a equipos servidores distintos. Esta característica se conoce como **máquina virtual** o **servidor virtual**. Apache admite la opción de asignar un nombre distinto a cada uno de los servidores virtuales (opción más sencilla) o bien asignarles diferentes direcciones IP a cada uno. Durante la configuración de Apache se asociará un sitio web a cada servidor virtual. Como se puede apreciar en la Figura 3.4, se utilizan los nombres *www.srvweb1.com* y *www.srvweb2.com* para acceder a diferentes sitios del servidor HTTP (*/var/www/srvweb1.com* y */var/www/srvweb2.com*), cuya dirección IP es la 195.135.220.3. Para que los clientes puedan acceder mediante las URL correspondientes, será necesario que un servidor DNS (véase capítulo 2) asocie cada uno de los nombres configurados con la dirección IP del servidor. Apache atenderá y examinará las solicitudes de los clientes, determinando el sitio web del servidor virtual a quien va dirigida la solicitud para proporcionar la página requerida al cliente. Un servidor virtual hereda las propiedades del servidor principal.

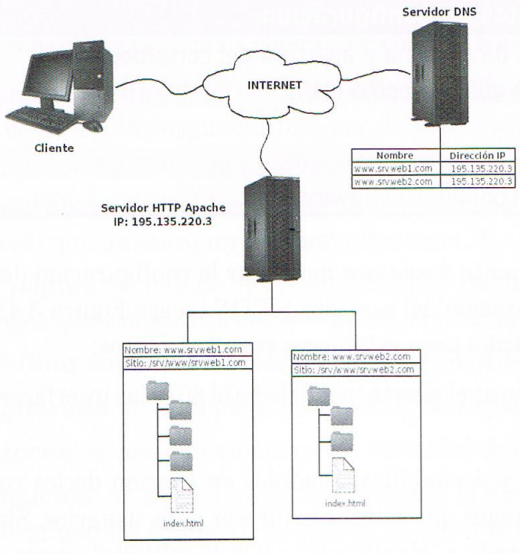


Figura 3.2. *Ejemplo de Servidor Virtual por asignación de nombre. En este ejemplo el cliente puede utilizar la URL http://www.srvweb1.com o http://www.srvweb2.com para referirse a sitios distintos del servidor HTTP. Sin embargo, a pesar de que el cliente tiene la impresión de acceder físicamente a dos servidores diferentes, los dos sitios están ubicados en un mismo equipo*

Apache 2, al igual que otros servicios en Linux, requiere la instalación de determinados paquetes para su configuración y funcionamiento. En una distribución OpenSuSE 11.1, acceda a la herramienta *Instalar software* y filtre por grupos de paquetes. Compruebe que en el grupo "Red" está marcado como instalado, o por el contrario, márquelo para que se proceda a la instalación automática de los paquetes necesarios (al menos *apache2* y *apache2-prefork*). La distribución Fedora 11 requiere la instalación del paquete estándar *httpd*, el cual podemos instalar mediante la herramienta *KPackageKit* (véase Figura 3.3). Mediante la herramienta *Synaptic* podrá hacer lo propio para instalar el paquete *apache2* en distribuciones con entorno GNOME como Debian.

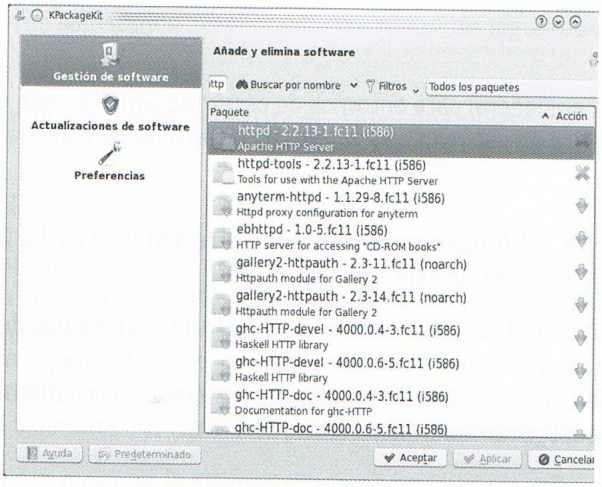


Figura 3.3. *Instalación del Servidor Web Apache en Fedora. Mediante la herramienta KPackageKit, buscaremos el paquete httpd, necesario para el servicio HTTP*

Si utiliza una distribución OpenSuSE 11.1, puede configurar este servicio mediante la herramienta *YaST2*, accediendo al apartado "Servicios de red" y pulsando sobre el icono "Servidor HTTP", requiriéndose instalar previamente el paquete *yast2-http-server*. Posteriormente, mediante el asistente, podrá configurar en cinco pasos los parámetros del servicio según se describe brevemente en la siguiente tabla.

Tabla 3.3. Pasos y elementos de configuración del servicio HTTP con YaST2

Paso	Elementos de Configuración
1	Puerto (por defecto el 80), interfaces de escucha y apertura del cortafuegos.
2	Módulos a habilitar para lenguajes de guiones como PHP.
3	Parámetros propios del servidor.
4	Servidores virtuales.
5	Tipo de inicio del servicio y acceso a configuración avanzada.

Si accedemos a la configuración avanzada o posteriormente deseamos modificar la configuración de este servicio, lo podremos hacer mediante el cuadro de diálogo "Configuración del servidor HTTP" (véase Figura 3.4). Seleccione y edite cada una de las partes de las que consta la configuración para establecer sus parámetros:

- **Puertos y direcciones de escucha**: permite configurar el puerto (por defecto el 80) y las interfaces de red por las que el servicio atenderá las peticiones HTTP.
- **Módulos del servidor**: permite añadir, habilitar y deshabilitar módulos en función de los requerimientos de las páginas que se hayan diseñado y las prestaciones que se deseen ofrecer a los usuarios. Simplemente se seleccionará el módulo deseado y se cambiará su estado a "Habilitado" o "Deshabilitado", según convenga.

- **Equipo principal**: establece los parámetros propios del servidor para el servicio HTTP, como el directorio raíz del sitio (Documento raíz) y sus parámetros (Directory), el nombre del servidor o la dirección de correo del. La opción "NameVirtualHost" permite indicar las interfaces de red utilizadas por los servidores virtuales. En el caso de servidores virtuales diferenciados por su nombre, se indicará como valor "*", cuando los servidores atiendan las peticiones indistintamente por cualquier interfaz.
- **Equipos**: este apartado permite la creación de servidores virtuales, estableciendo sus parámetros como el nombre del servidor (servidor y dominio), el directorio raíz del sitio y la forma en que se hará referencia a ellos (mediante su nombre o su dirección IP).

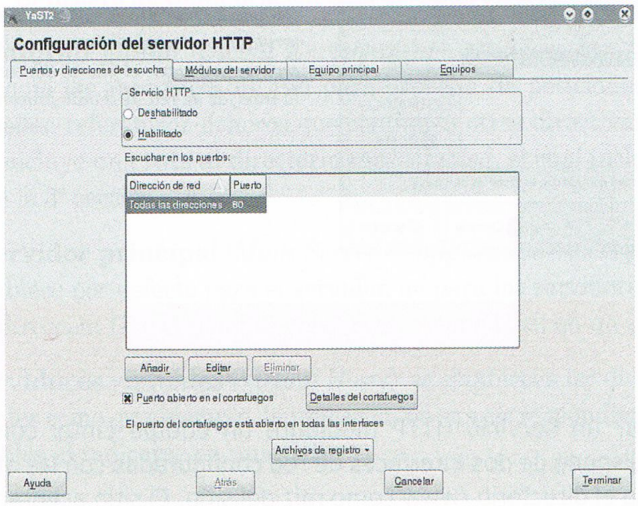


Figura 3.4. Configuración del servidor HTTP en OpenSuSE. Este cuadro de diálogo permite activar el servicio y editar cada una de las opciones de configuración, como el puerto y el directorio, que ejercerán de raíz del sitio

Si utiliza una distribución Fedora, puede instalar el paquete *system-config-httpd* para configurar de forma gráfica este servicio. Acceda mediante "Lanzador de Aplicaciones || Aplicaciones || Administración || Configuración de Servidores || HTTP" para configurar este servicio (véase ejemplo 3.3). Un cuadro de diálogo le permitirá realizar su configuración (véase Figura 3.5) a través de distintas solapas:

- **Opciones principales o básicas**: permite configurar aspectos fundamentales para poder proporcionar este servicio, como el puerto (por defecto el 80) y direcciones IP (asignadas a los interfaces de red) de escucha de atención para las peticiones cliente, así como el nombre del servidor y la dirección de correo del *webmaster*.
- **Virtual Hosts**: esta solapa permite configurar cada uno de los servidores virtuales que desee poner a disposición de los usuarios, incluyéndose uno por defecto. Mediante los botones disponibles, podrá añadir uno nuevo o modificar uno existente. Los parámetros que se configuran para cada servidor virtual se clasifican en:
  - **Generales**: se establece su nombre, directorio raíz, correo del webmaster y se indica si es un servidor virtual que utilizará un nombre o dirección IP.
  - **De página**: se indican las páginas índice que ha de buscar por defecto en el sitio (como *index.html*) y los códigos que tienen asociados cada mensaje de error generado tras una solicitud cliente.
  - **Habilitar soporte SSL**: permite admitir conexiones seguras mediante SSL.
  - **Registrado**: se establecen los archivos de registro para transferencias de páginas y errores.
  - **Entorno**: se asignan valores a las variables de entorno utilizadas por scripts CGI.
  - **Ejecución**: se asocian distintas opciones al directorio raíz del sitio para el servidor virtual. También se determinan los equipos a los que se les permite el acceso al servidor virtual.

- **Servidor**: se indica, entre otros, el fichero donde se registra el PID del demonio o proceso servidor, el usuario y grupo que pueden lanzar el demonio *httpd* y el que atiende las peticiones (por defecto *apache*).
- **Ajuste del rendimiento**: permite limitar el número de conexiones, el tiempo de duración de cada una, las peticiones para cada una de las conexiones, así como aceptar peticiones persistentes.

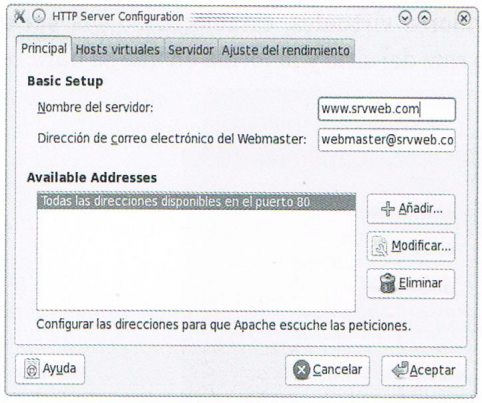


Figura 3.5. *Configuración del servicio HTTP en Fedora. Distintas solapas dividen los diferentes grupos de opciones: opciones principales, referentes a los servidores virtuales, propias del servidor por defecto y las relativas al rendimiento. En este ejemplo, se muestra la configuración principal del servidor, con nombre www.srvweb.com, y cuyo sitio será accesible por el puerto 80, con independencia de la interfaz de red de donde provenga la solicitud*

EJEMPLO 3.3

Se desea proporcionar un servicio HTTP mediante un equipo Linux con una distribución Fedora instalada. El servidor dispone de dos interfaces de red configuradas con las direcciones IP 192.168.0.93 y 10.0.1.93. Se destina el directorio */www* como raíz del sitio. El sitio aceptará peticiones por la interfaz con dirección IP 192.168.0.93.

Creamos, por ejemplo, la siguiente jerarquía de directorios para ubicar las páginas y los elementos que las integran:

```
/www
/www/botones
/www/webs
/www/imagenes
```

Suponiendo que los paquetes de este servicio están instalados, seleccionamos "HTTP" en la "Configuración de Servidores" accesible desde el botón "Aplicaciones || Administración || Configuración del sistema".

En la pestaña "Principal" indicamos como "Nombre del servidor" el mismo que el del equipo (por ejemplo *srvweb.com*). Modificaremos la aceptación desde todos las interfaces de red, seleccionando: "Available adresses", "Todas las direcciones disponibles en el puerto 80" y pulsamos sobre el botón "Modificar". Seleccionamos "Dirección", indicamos la dirección IP 192.168.0.93 y pulsamos sobre "Aceptar".

Accedemos a la pestaña "Hosts Virtuales", seleccionamos "Default Virtual Host" y pulsamos el botón "Modificar". En el cuadro de diálogo modificamos el parámetro "Directorio de Root del Documento", indicando */www* y cerrando la ventana.

Tras pulsar en el botón inferior "Aceptar", accedemos a "Aplicaciones || Administración || Administración de Servicios", buscamos el servicio "httpd", lo seleccionamos y pulsamos sobre el icono "Iniciar".

Para probar su funcionamiento, abrimos el navegador Konqueror e indicamos como URL: *http://192.168.0.93.* Deberá visualizarse la página que debemos haber establecido como índice.

Para realizar una configuración manual del servicio, debemos tener en cuenta la ubicación por defecto del directorio raíz del sitio, así como la del fichero principal de configuración para la distribución elegida según se muestra en la tabla 3.4. Generalmente, las distribuciones GNU/Linux tienden a desglosar la configuración de Apache en varios ficheros, consiguiendo que sea más sencilla. Estos ficheros se referencian unos a otros, incluyéndose las opciones de configuración del fichero referenciado en el fichero que lo referencia. El desglose de los ficheros de configuración dependerá de la distribución escogida.

Editaremos el fichero principal de configuración para modificar los parámetros de las directivas de configuración, pudiendo establecer una configuración más avanzada. Una directiva de configuración, se asemeja a una orden que se proporciona al servidor HTTP. El fichero de configuración está dividido en tres secciones:

- **Configuración del entorno global** (*Global Environment*): establece las directivas para la configuración general del servidor, como las interfaces de red para escucha de peticiones. Opcionalmente, mediante la directiva *Include* se pueden referenciar ficheros que contienen otras directivas de configuración. Por ejemplo, la distribución Debian incluye una ruta al directorio *sites-enabled*, el cual incluye ficheros con directivas de la 2ª sección (*default*) y de la 3ª sección.
- **Configuración del servidor principal** (*Main Server Configuration*): se especifican las directivas relativas al sitio web que se establece por defecto para el servidor, no para los servidores virtuales. Su página índice se mostrará al indicar la dirección IP o el nombre del servidor como URL en un navegador.
- **Configuración de servidores virtuales** (*Virtual Hosts*): se establecen las directivas que configuran cada uno de los servidores virtuales como, por ejemplo, la ubicación de sus correspondientes directorios raíz o el nombre por el que serán accesibles al indicarse en una URL.

Tabla 3.4. Ubicación de los directorios raíz por defecto del sitio web y de los principales ficheros de configuración

Distribución	Directorio Raíz por defecto	Fichero de configuración
OpenSuse	*/srv/www/htdocs/*	*/etc/apache2/httpd.conf*
Fedora	*/var/www/html/*	*/etc/httpd/conf/httpd.conf*
Debian	*/var/www/*	*/etc/apache2/apache2.conf*

Algunas de las directivas utilizadas para la configuración del servidor principal y servidores virtuales son las siguientes:

- *ServerName*: indica el nombre que se le dará al servidor web.
- *DocumentRoot*: indica el directorio raíz del sitio para el servidor.
- *ServerAdmin*: indica la dirección de correo del webmaster del sitio.
- *DirectoryIndex*: indica los ficheros que podrán actuar como página índice del sitio.

Como se ha mencionado anteriormente, conviene organizar el sitio web mediante directorios, aunque es posible que Apache pueda acceder a otros que no se encuentran en la jerarquía del sitio que se ha definido, por ejemplo, para la ejecución de un *script* de una página dinámica. Es habitual definir una estructura denominada **contenedor** para cada uno de los directorios a los que accederá Apache, incluyéndose una para el directorio raíz del sitio del servidor principal. Estas estructuras, se reconocen por una etiqueta de inicio con el formato *<Directory "Nombre_Directorio">*, y otra de fin, *</Directory>*, donde *"Nombre_Directorio"* figurará como uno de los directorios a los que tendrá acceso Apache. Como se puede apreciar en la tabla 3.5, el objeto de estas estructuras es la de definir directivas que, por lo general, establecen distintos permisos sobre el directorio que tiene asociado.

Tabla 3.5. Directivas aplicables en un contenedor Directory con algunas de sus opciones

Directiva	Opciones	Función
Options	None	No establece ninguna opción.
	All	Establece todas las opciones.
	Indexes	Permite visualizar páginas índice existentes en el directorio.
	FollowSymLinks	Permite seguir los enlaces simbólicos del directorio.
	ExecCGI	Admite la ejecución de scripts CGI.
AllowOverride	None	No establece ninguna opción.
	All	Establece todas las opciones.
	FileInfo	Muestra la información de los archivos del directorio.
Order	allow,deny	Primero aplicará los permisos de Allow y luego los de Deny.
	deny,allow	Primero aplicará los permisos de Deny y luego los de Allow.
Allow	from all	Admite cualquier acceso al directorio
	from IP	Admite cualquier acceso al directorio proveniente de la dirección IP indicada.
	from dominio	Admite cualquier acceso al directorio desde el dominio especificado.
Deny	from all	Deniega cualquier acceso al directorio.
	from IP	Deniega cualquier acceso al directorio proveniente de la dirección IP indicada.
	from dominio	Deniega cualquier acceso al directorio desde el dominio especificado.

La configuración de un sencillo servidor web, requerirá modificar la directiva de la sección 2 *DocumentRoot*, indicando el directorio que ejercerá como raíz del sitio web. Esta directiva tendrá asociada una estructura contenedora cuyo nombre del directorio coincidirá con el indicado en *DocumentRoot*.

La inclusión de los módulos necesarios para ampliar la funcionalidad del servidor, se efectúa mediante la directiva *LoadModule*, seguido del nombre del módulo y el archivo (librería) que lo contiene. Se utilizarán tantas directivas *LoadModule* como módulos distintos se vayan a utilizar. Por ejemplo, en una distribución Debian, puede observar el directorio */etc/apache2/mods-enable*, cuyos ficheros con extensión *.load* contienen una línea para la carga del módulo correspondiente. También se puede utilizar la orden *a2enmod* seguido del nombre del módulo a habilitar.

La utilización de servidores virtuales mediante nombre (sección 3), requiere utilizar la directiva *NameVirtualHost*. Esta directiva, se incluirá en el fichero de configuración por cada dirección de red diferente que utilicen los servidores virtuales para atender las solicitudes cliente. Cuando no importe la dirección de red para atenderlas, su valor se establecerá a "*".

Para cada servidor virtual, se debe crear un contenedor donde se incluirán sus correspondientes directivas (*ServerName*, *DocumentRoot*, *ServerAdmin*, *DirectoryIndex*). Cada contenedor, generalmente, está delimitado por las etiquetas con formato *<VirtualHost Dirección_De_Red:N.º del Puerto>* y *</VirtualHost>*, por tanto, se deberán crear tantos contenedores de este tipo como servidores virtuales se necesiten. Como valor *Dirección_De_Red* se indicará uno de los valores previamente definidos con las directivas *NameVirtualHost* ("*" o una dirección IP), dependiendo por donde queremos que el servidor virtual atienda las solicitudes. Opcionalmente, se puede especificar el puerto por el que se atenderán las peticiones para el sitio, escribiendo a continuación de la *Dirección de Red*, dos puntos y el *N.º del Puerto*. En el ejemplo 3.4 pueden observar los contenedores utilizados y los parámetros de configuración de los servidores virtuales de la Figura 3.2 para una distribución Debian 5 Lenny.

EJEMPLO 3.4

Disponemos de un equipo con una distribución Debian instalada y cuyo nombre es *srvweb.com*. Se desea configurarlo como servidor web, permitiendo el acceso a dos sitios diferentes. Para posibilitar el acceso a cada sitio, se utilizarán nombres distintos para este servidor:

- Se utilizará el nombre *www.srvweb1.com* cuyo directorio raíz se ubicará en */var/www/srvweb1.com*.
- Se utilizará el nombre *www.srvweb2.com* cuyo directorio raíz se ubicará en */var/www/srvweb2.com*.

Aprovechamos la inclusión del fichero de configuración */etc/apache2/ports.conf* en */etc/apache2/apache2.conf*, para añadirle la directiva *NameVirtualHost*.

```
#Fichero: /etc/apache2/ports.conf
NameVirtualHost *
```

En el directorio */etc/apache2/sites-availabe crearemos* un fichero para cada uno de los servidores virtuales y le daremos su mismo nombre. Estos ficheros contendrán los siguientes contenedores y parámetros para habilitar cada uno de los servidores virtuales:

```
#Fichero: /etc/apache2/sites-available/www.srvweb1.com
<VirtualHost *>
ServerName www.srvweb1.com
DocumentRoot /var/www/srvweb1.com
ServerAdmin webmaster@srvweb1.com
</VirtualHost>

#Fichero: /etc/apache2/sites-available/www.srvweb2.com
<VirtualHost *>
ServerName www.srvweb2.com
DocumentRoot /var/www/srvweb2.com
ServerAdmin webmaster@srvweb2.com
</VirtualHost>
```

Posteriormente habilitamos cada sitio para que estén disponibles en el servidor virtual mediante la orden *a2ensite*, el cual crea un enlace en */etc/apache2/sites-enabled*, a los ficheros de configuración creados en directorio */etc/apache2/sites-available/* previamente.

```
srvweb.com$ sudo cd /etc/apache2/sites-available
srvweb.com$ sudo a2ensite www.srvweb1.com
srvweb.com$ sudo a2ensite www.srvweb2.com
Finalmente iniciamos o reiniciamos el servicio mediante la sguiente orden:
srvweb.com$ sudo /etc/init.d/apache2 restart
```

Probaremos su funcionamiento indicando en el navegador del cliente los nombres asignados a cada sitio.

Apache nos permite varios modos de autenticarnos en el sitio web, de manera que solo usuarios autorizados puedan acceder al contenido. El modo de autenticación básico, es decir, sin encriptación del usuario ni de la contraseña, requiere previamente que Apache cargue el módulo *mod_auth*. Además, tendremos que crear un fichero con las contraseñas y los usuarios a los que se les permitirá el acceso, pudiendo valernos de la orden *htpasswd*. Finalmente, en el contenedor *<Directory>* del sitio, incluiremos las directivas para indicar a Apache el tipo de autenticación utilizado, el nombre del dominio de autenticación, el fichero con los usuarios y contraseñas y los usuarios que se pueden autenticar. En el ejemplo 3.5, se ilustra este método sencillo de autenticación.

EJEMPLO 3.5

Disponemos de un equipo con una distribución Debian instalada y cuyo nombre es *srvweb.com*. El directorio raíz del sitio será el utilizado por defecto por Debian. Solamente tendrán acceso al sitio aquellos usuarios que se autentiquen como el usuario *angel*.

Suponiendo el módulo *mod_auth* cargado por Apache, crearemos el directorio para albergar el fichero con las contraseñas.

```
srvweb.com$ sudo mkdir /usr/local/apache
srvweb.com$ sudo mkdir /usr/local/apache/etc
```

Creamos el fichero *passwords* en el directorio creado para gestión de los usuarios y contraseñas. Incluiremos, por tanto, al usuario *angel* con su contraseña.

```
srvweb.com$ sudo htpasswd -c /usr/local/apache/etc/passwords angel
```

Editaremos el fichero con la configuración por defecto del sitio */etc/apache2/sites-availabe/default*.

```
srvweb.com$ sudo nano /etc/apache2/sites-avilable/default
```

Finalmente le añadimos las directivas correspondientes al modo básico de autenticación (*AuthType*, *AuthName*, *AuthUserFile*, *Require*), quedando de esta manera el contenedor *<Directory>* del sitio por defecto:

```
<Directory /var/www/>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride none
        Order allow,deny
        allow from all
        AuthType Basic
        AuthName "Zona Privada"
        AuthUserFile /usr/local/apache/etc/passwords
        Require user angel
</Directory>
```

En las distribuciones utilizadas, puede activar el servicio mediante las herramientas de configuración descritas con anterioridad o las utilizadas para iniciar servicios en cada una de las distribuciones, como la herramientas "Servicios" de Debian para su entorno GNOME. También puede hacerlo mediante la orden *rcapache2 start* en OpenSuSE, *service httpd start* en Fedora y */etc/init.d/apache2 start* en Debian.

Para probarlo, y suponiendo alojadas las páginas y sus elementos en el sitio web, abra un navegador en el servidor e indique como URL *http://localhost*. Deberá aparecerle la página que estableció como índice de su sitio web. Si dejó como directorio raíz del sitio el utilizado por defecto, se mostrará una página indicativa de que la instalación fue satisfactoria y el funcionamiento de Apache es el correcto, como por ejemplo, mediante la expresión "It Works!". Si configuró servidores virtuales y los servidores DNS conocen su dirección IP, indique en el navegador del cliente la URL que referencie a cada uno de los servidores.

Puede monitorizar la actividad de su servidor Apache mediante generación de informes con la herramienta **Webalizer**, cuya instalación requiere la instalación del paquete *webalizer*. En una distribución Debian, podemos utilizar su configuración por defecto, que utiliza el directorio */var/www/webalizer/* para almacenar los informes en forma de página web. *Webalizer* examina los ficheros de log o registro ubicados en */var/log/apache2/* para generar dichos informes. Para utilizarlo, ejecute la oren *webalizer*, acceda a la carpeta indicada anteriormente y abra la página *index.html* con un navegador web para observar las visitas efectuadas a su sitio web, tal y como se muestra en la Figura 3.6.

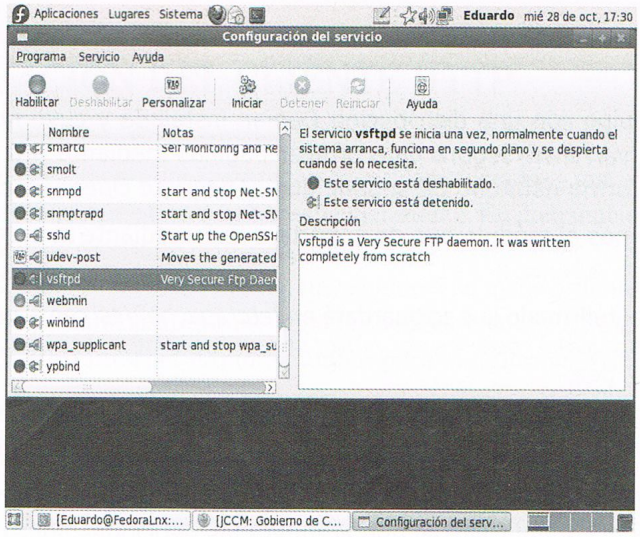


Figura 3.6. *Generador de informes Webalizer. Permite generar informes a modo de gráfico, representando parámetros como el número de visitas recibidas al sitio, la tasa de transferencia entre el servidor y cliente o el mes en el que se efectuaron las visitas*

3.3.2.1 Gestión de certificados y acceso seguro con HTTPS

Si deseamos utilizar conexiones seguras mediante el protocolo HTTPS para acceso a determinadas páginas de seguridad comprometida, tendremos que configurar Apache para que cargue el módulo *mod_ssl*, aunque en algunas versiones de Apache 2 suele venir integrado. Además, necesitaremos tener instalado el paquete *OpenSSL*, que se encarga de la implementación de SSL para llevar a cabo transferencias seguras. Este módulo no se recomienda en configuraciones con más de un servidor virtual que utilicen el mismo puerto de escucha, ya que la conexión SSL del cliente se establece con una dirección IP y un puerto determinado del servidor. Apache no sabrá con qué servidor virtual debe utilizar SSL, escogiendo el primero que encuentra, y no utilizará conexiones seguras para el resto de servidores virtuales. Para paliar este problema se utiliza la extensión de TSL denominada **SNI** (*Server Name Indication* o Indicación por Nombre de Servidor), necesitando tener instalado el paquete *libapache2-mod-gnutls* (para cargar el modulo *mod_gnutls* en vez de *mod_ssl*). También se puede utilizar el módulo *mod_ssl* para implementar SSL con un servidor virtual para el sitio principal y que atienda las peticiones por el puerto 80, y otro servidor virtual para el sitio seguro que atienda las peticiones por el puerto 443 (véase ejemplo 3.6).

Para ofrecer páginas de forma segura para un único sitio web es necesario que el servidor disponga de un certificado que pruebe su autenticidad. La generación de un certificado autofirmado requiere la ejecución de la orden *make-ssl-cert*, pudiendo solicitarnos información sobre la que basará la generación del certificado. Tendremos que indicarle como parámetro el fichero con extensión "*.pem*" que obtendremos tras su ejecución, que contiene las claves para efectuar el cifrado asimétrico por el servidor.

Es necesario habilitar el puerto de escucha mediante la directiva *Listen 443* e indicar que el puerto de escucha del servidor virtual es el 443. Además, se deberán utilizar las siguientes directivas (véase ejemplo 3.6):

- *SSLRequireSSL*: utilizado en el contenedor *<Directory>* fuerza la utilización de SSL del sitio, evitando su desactivación.
- *SSLEngine*: habilita SSL (valor on) en un servidor virtual si en el servidor principal se desactivó.
- *SSLCertificateFile*: indica en el servidor virtual la ruta al fichero (.pem) que contiene el certificado.

EJEMPLO 3.6

Disponemos de un equipo con una distribución Debian instalada y cuyo nombre es *srvweb.com*. Se utilizará el directorio */var/www/segura* para ofrecer páginas mediante SSL, y */var/www/segura* para ofrecer páginas de la forma habitual. Se supone que el paquete *OpenSSL* está instalado.

En primer lugar añadimos el módulo que da soporte a SSL mediante la orden:

```
srvweb.com$ sudo a2enmod ssl
```

Creamos el certificado autofirmado que se guardará en */etc/apache2/ssl* con el nombre *certificado.pem*.

```
srvweb.com$ sudo make-ssl-cert /usr/share/ssl-cert/ssleay.cnf \ /etc/apache2/
ssl/certificado.pem
```

Al ejecutarse nos pedirá el nombre del servidor, el cual indicaremos.

Habilitamos el puerto de escucha en */etc/apache2/ports.conf*, aunque puede venir por defecto habilitado. También añadiremos una línea para el servidor virtual que atenderá las peticiones por el puerto 80, y otra para el servidor virtual que atenderá las peticiones por el puerto 443.

```
NameVirtualHost srvweb.com:80
Listen 80
NameVirtualHost srvweb.com:443
Listen 443
```

En el directorio */etc/apache2/sites-availabe* crearemos un fichero con la configuración de los servidores virtuales. Este fichero contendrá los siguientes contenedores y parámetros para habilitar cada uno de los servidores virtuales:

```
#Fichero: /etc/apache2/sites-available/www.srvweb.com
<VirtualHost srvweb.com:443>
        SSLEngine on
SSLCertificateFile /etc/apache2/ssl/certificado.pem
        DocumentRoot /var/www/segura
</VirtualHost>
<Directory /var/www/segura>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride none
        Order allow,deny
        allow from all
SSLRequireSSL
</Directory>

<VirtualHost srvweb.com:80>
DocumentRoot /var/www/insegura
</VirtualHost>

<Directory /var/www/insegura>
        Options Indexes FollowSymLinks Multiviews
        AllowOverride none
        Order allow,deny
        Allow from all
</Directory>
```

Posteriormente habilitamos el sitio para que esté disponible mediante la orden *a2ensite*, el cual crea un enlace en */etc/apache2/sites-enabled* al fichero de creado en directorio */etc/apache2/sites-available/* previamente.

```
srvweb.com$ sudo cd /etc/apache2/sites-available
srvweb.com$ sudo a2ensite www.srvweb.com
```

Finalmente iniciamos o reiniciamos el servicio mediante la siguiente orden:

```
srvweb.com$ sudo /etc/init.d/apache2 restart
```

3.4 CONFIGURACIÓN DEL CLIENTE HTTP

En este apartado se abordan brevemente dos navegadores gráficos utilizados e instalados por defecto en plataformas Windows y Linux, como Internet Explorer y Konqueror, respectivamente. En distribuciones GNU/Linux encontraremos navegadores asociados al entorno de escritorio utilizado, como Epiphany y Galeon para entornos GNOME, o el propio Konqueror para entornos KDE, aunque también existen navegadores en modo órdenes como Lynx o Links2. Varios de los navegadores que conocemos son multiplataforma como Opera, Seamonkey o Mozilla Firefox, mientras que otros son monoplataforma, como Chrome e Internet Explorer, ambos para plataformas Windows.

La utilización del software cliente de este servicio se basa en indicar la URL deseada en el campo destinado a tal efecto, pudiendo utilizar un protocolo seguro reemplazando HTTP por HTTPS en la URL. También podremos configurar otros parámetros, como habilitar el navegador para ejecutar páginas dinámicas o la instalación de complementos para la visualización de determinados contenidos, cuya configuración dependerá del navegador utilizado. Además, cada navegador permite establecer ciertos parámetros de configuración propios, como los relativos al aspecto, comportamiento, registro de páginas visitadas, información almacenada temporalmente o aspectos de seguridad. Algunas características y elementos comunes a gran parte de los navegadores son los siguientes:

- **Barra de título**: muestra el título de la página web, habitualmente en la parte superior del navegador.
- **Barra de direcciones**: permite indicar la URL para acceder al sitio web deseado.
- **Barra de menú**: permite acceder a las distintas opciones que el navegador ofrece al usuario.
- **Barra de botones básicos**: permite el acceso a los botones estándar de detención de carga de la página, página atrás, página adelante, actualizar la página o ir a la página configurada como de inicio.
- **Barra de estado**: muestra información al usuario del proceso de transferencia de la página entre el servidor y el propio navegador.
- **Pestañas**: mediante la utilización de pestañas se pretende que el usuario, en la misma ventana del navegador, acceda a distintas páginas, cada una de ellas accesible en su correspondiente pestaña.
- **Buscador**: el usuario utiliza dicho elemento para realizar búsquedas en Internet sobre la información que desea sin necesidad de indicar la URL de la página de un buscador. Habitualmente permite al cliente seleccionar el buscador de Internet que por defecto que suele utilizar.
- **Área del documento**: es donde se muestra el contenido de las páginas a las que se accede.
- **Paneles laterales**: permiten mostrar en uno de los laterales del navegador elementos del navegador. Su objetivo es que dichos elementos permanezcan visibles y sean de fácil acceso debido a su alto grado de utilización.
- **Redifusión o sindicación web**: permite visualizar información actualizada de aquellos sitios web a los que nos hemos suscrito. Se suele utilizar por ejemplo para lectura actualizada de noticias en formato **RSS** (*Really Simple Syndication* o Sindicación Realmente Simple).
- **Gestión de ventanas emergentes o *pop-ups***: permiten el bloqueo de ventanas emergentes o **pop-ups**, utilizados principalmente con fines propagandísticos.
- **Gestión de descargas**: algunos navegadores incorporan un programa para gestionar las descargas, evitando que la descarga de cualquier tipo de archivo de un servidor web se interrumpa.

- **Seguridad y Privacidad**: permite establecer una serie de parámetros de seguridad para asegurarnos, por ejemplo, de la legitimidad el sitio que estamos visitando, evitar *phishing* y *malware* o habilitar el acceso mediante ssl.
- **Complementos**: también denominados **Plugins** o **Add-ons**, su instalación nos permiten ampliar la funcionalidad del navegador, por ejemplo, para visualizar páginas con animaciones Flash o vídeos e incluso conocer el tiempo en tu localidad.
- **Páginas favoritas**: permite almacenar la URL y una descripción de páginas que nos resultan de interés para su posterior visita.
- **Historial de navegación**: permite conocer los sitios y las páginas visitadas con anterioridad por si deseamos de nuevo acceder a ellos.
- **Gestión de contraseñas**: permite recordar la contraseña para aquellos sitios que nos resulte más comodo que volver a introducirlas de nuevo.
- **Aspecto y apariencia**: permite la configuración de ciertos aspectos de la interfaz del navegador con el usuario, como la definición del tamaño de la fuente que se muestra en el Área del documento.
- **Eliminar información temporal**: permite la eliminación de aquellos elementos que se almacenan con carácter temporal durante la navegación como *cookies*, el historial o contraseñas guardadas.

Previo a la utilización de un cliente HTTP, recuerde configurar correctamente la red TCP/IP, para que a través de la interfaz de red o módem tenga acceso a los servidores web a los que desee acceder, tanto locales a su red como los disponibles en Internet. Si el equipo pertenece a una organización con proxy consulte el apéndice H.

3.4.1 CONFIGURACIÓN EN MICROSOFT WINDOWS

En plataformas Windows es conocido su navegador **Internet Explorer**, incorporado en cada una de las versiones de este sistema operativo y en el que en su versión 8 apreciamos algunas novedades relevantes:

- **Aceleradores**: son servicios utilizados de forma contextual, como por ejemplo, el envío de texto previamente seleccionado de una web mediante correo electrónico a través de Windows Live o la traducción del texto seleccionado.
- **WebSlices**: permite acceder a un sitio web visualizando parcialmente su contenido. Su creación se asemeja a marcar una página como favorita y a la redifusión web.
- **Crash Recovery**: permite la recuperación del navegador ante el bloqueo de una pestaña.
- **Cross Site Scripting**: permite hacer frente a páginas dinámicas con código malicioso, bloqueando de forma automática su ejecución.
- **Filtro SmartScreen**: permite evitar la suplantación de identidad en nuestra visita a diferentes sitios web y la protección frente a software malicioso o *malware*. Su activación se aplica a las pestañas de la ventana donde se ha activado.
- **Filtrado InPrivate**: al activarlo permite la navegación evitando dejar rastros de los sitios que hemos visitado.

Su utilización se basa en indicar en la barra de direcciones la URL del sitio web al que se quiere acceder, aunque brevemente comentaremos algunas de las partes principales que lo integran tal y como se muestran en la Figura 3.7.

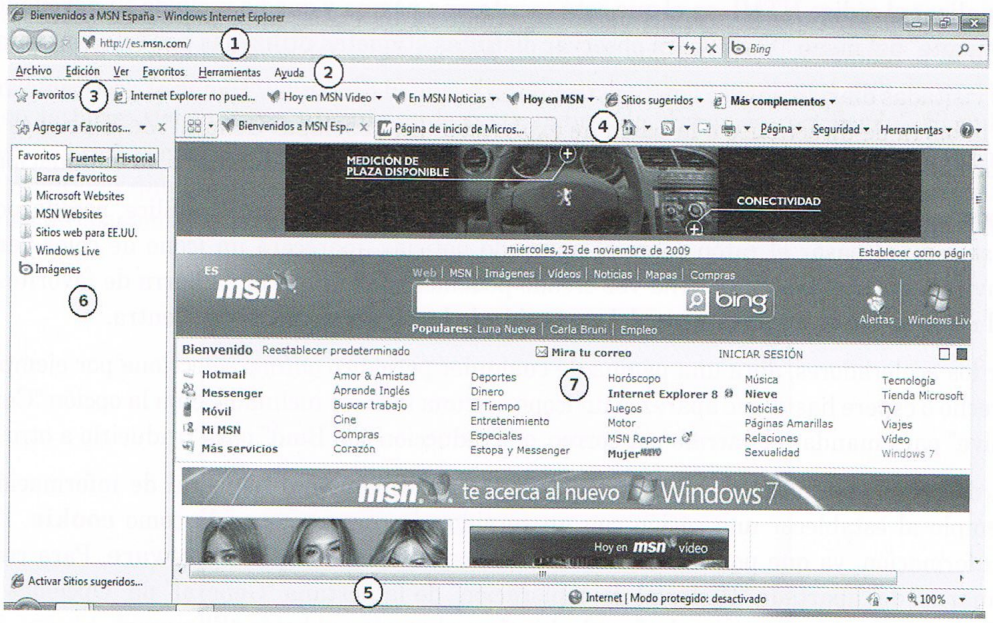


Figura 3.7. Navegador Internet Explorer 8. En esta figura aparecen numerados los elementos principales de dicho navegador según el párrafo previo

- **Barra de direcciones**: formada por los iconos básicos de navegación actualizar, detener, regresar y adelante, la barra de Dirección donde se indica la URL y el buscador integrado *Bind*.
- **Barra de menús**: permite acceder a las distintas opciones que ofrece a los clientes. Destacar el menú "Herramientas", cuya opción "Opciones de Internet..." nos permite configurar diversos parámetros como la forma de conexión a Internet o el nivel de seguridad que se desea.
- **Barra de favoritos**: permite agregar WebSlices y páginas visitadas con frecuencia para su posterior acceso a modo de acceso directo.
- **Barra de órdenes**: mediante listas desplegables e iconos permite un acceso rápido a acciones utilizadas con frecuencia, como la lectura del correo electrónico mediante Windows Live o la configuración del navegador mediante las distintas herramientas.
- **Barra de estado**: permite que este navegador muestre diversos mensajes al usuario referente a su actividad, como la finalización de la carga de una página o que se está realizando la transferencia de información entre el servidor y su navegador.
- **Barra del explorador**: muestra en su parte izquierda una nueva ventana, en la que se puede visualizar, entre otros, el Historial de sitios visitados diariamente o los sitios considerados como Favoritos.
- **Área del documento**: en esta área se visualiza la página indicada en la URL, así como todos sus elementos una vez obtenida del servidor. El usuario utiliza esta área para interactuar con la página, por ejemplo, para acceder a otra página mediante los hiperenlaces, reproducir sonidos, vídeos, etc. Si la página no pudo encontrarse se mostrará una página con un mensaje y un código de error.

Al abrir este navegador aparece una página por defecto, denominada de inicio. Esta página se puede cambiar accediendo a "Opciones de Internet...". Seleccione la pestaña "General", indique una nueva página en "Página principal" y pulse sobre "Aceptar". Esta página suele estar representada en la barra de herramientas mediante un icono con una casa, que al pulsar sobre él, se accede a la citada página.

Si desea visualizar el código HTML en el que está escrita una página y que ha recibido su navegador, seleccione la opción "Código fuente" del menú "Ver". Podrá observar distintas etiquetas utilizadas por este lenguaje.

Las páginas visitadas diariamente se van registrando en lo que se denomina "Historial", accesible mediante la lista desplegable de la barra de direcciones o la barra de explorador. En la solapa "General" de "Opciones de Internet...", apartado "Historial de navegación", puede configurar su caducidad así como proceder a su eliminación.

También podemos utilizar la novedosa tecnología WebSlices. Para crear un WebSlice, acceda por ejemplo a la página *www.msn.com*, al pasar el ratón sobre el apartado noticias aparecerá un icono de color verde, al pulsarlo Explorer nos invita a crear el WebSlice. Una vez creado podemos consultarlo en la barra de favoritos, comprobando que al pulsar el ratón sobre él, aparece parte del contenido de la página donde se encuentra.

Para probar los aceleradores, abra una página de cualquier periódico *online*, seleccione por ejemplo un párrafo y pulse botón derecho o espere hasta que aparezca un icono con una flechita inclinada, elija la opción "Correo electrónico con Windows Live" para mandar el párrafo por correo, o "Traducción con Bind" para traducirlo a otro idioma.

El acceso a determinadas páginas, a veces requiere el almacenamiento temporal de información en el equipo cliente (por ejemplo al establecer una sesión con un servidor de correo), conocida como **cookie**. Puede interesar eliminar esta información, ya que podrían incluir entre otros **software espía** o **spyware**. Para realizarlo, acceda al botón "Eliminar..." del apartado "Historial de exploración" de la pestaña "General" de "Opciones de Internet...". Marque al menos sobre "Archivos temporales" y "Cookies" y pulse sobre el botón "Eliminar".

A veces resulta útil registrar aquellas páginas que resultan de interés y que desea volver a visitarlas con posterioridad. La opción de menú "Favoritos", nos permite agregar una página visitada y marcarla como favorita. Opcionalmente, pueden organizalas mediante la creación de carpetas y subcarpetas.

Independientemente de la configuración TCP/IP establecida en un equipo, hay veces que resulta conveniente especificar la forma de acceso a Internet e indicar a Internet Explorer si se va a utilizar una conexión telefónica, una red de área local, VPN, o un servidor Proxy. Acceda a "Opciones de Internet..." y elija la pestaña "Conexiones" para determinar la forma de acceso a Internet (véase Figura 3.8).

Puede establecer distintos niveles de seguridad cuando accede a su Intranet e Internet, indicando los sitios que son de su confianza. Seleccione la solapa "Seguridad" de las "Opciones de Internet...". Para determinar el contenido que el cliente puede visualizar en este navegador acceda a la solapa "Contenido". Si quiere utilizar seguridad mediante SSL elija la solapa "Opciones avanzadas" de las "Opciones de Internet...", y para la gestión de certificados utilizados con SSL acceda al apartado "Certificados" de la pestaña "Contenido".

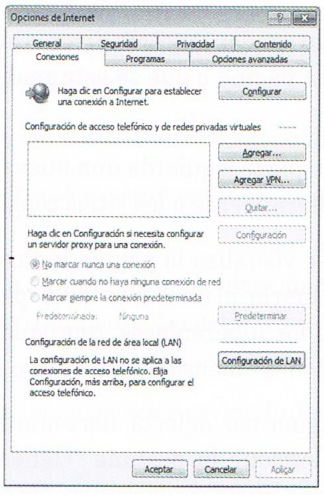


Figura 3.8. *Opciones de Internet del navegador Internet Explorer. Mediante las distintas solapas se pueden configurar distintos aspectos del navegador como la página mostrada en su inicio, la forma de conectarse a Internet, el nivel de seguridad que se quiere o restringir el contenido de las páginas que puede visitar*

Cuando efectuamos un acceso a un sitio web mediante protocolo HTTPS, si el certificado no está firmado por una entidad de nuestra confianza, Internet Explorer nos mostrará una advertencia similar a la de la Figura 3.9, indicándonos que proviene de un sitio no confiable. La decisión de acceder o no al sitio web dependerá de nosotros, mostrándonos en la barra de dirección un cuadro de texto indicando "Error de certificado". Si pulsa sobre dicho mensaje, se mostrará una pequeña ventana donde pulsaremos sobre el enlace "Ver certificados", informándole entre otras cosas de la entidad que lo emitió y su validez. Pulse el botón "Instalar certificado..." para instalar en pocos pasos y mediante un asistente dicho certificado, preguntándonos al finalizar si confiamos en la CA que generó el certificado.

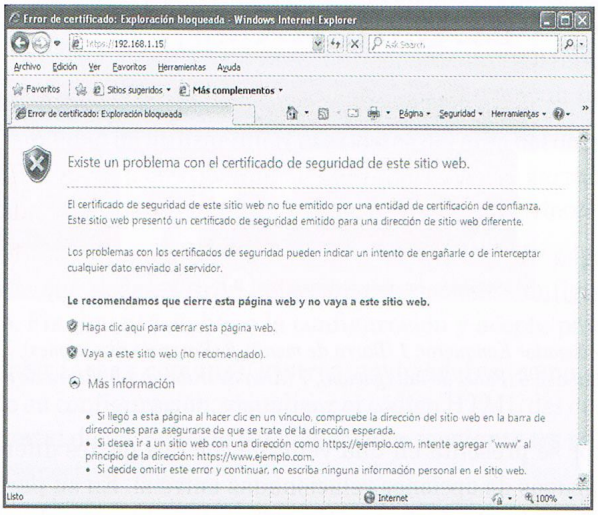


Figura 3.9. Mensaje de advertencia de Internet Explorer 8. Este mensaje se muestra al acceder a un sitio mediante HTTPS cuyo certificado no está recogido en el navegador de confianza

3.4.2 CONFIGURACIÓN EN GNU/LINUX

Konqueror es uno de los navegadores comúnmente utilizado en distribuciones Linux. Su utilización requiere el inicio de una sesión gráfica en el entorno gráfico KDE, incluyéndolo por defecto. Este navegador no solo se emplea en el acceso a páginas y servidores web, sino que también es utilizado como navegador sobre el sistema de archivos local, incluso permite el acceso remoto a otros equipos mediante **SSH** (véase capítulo 5). Esta capacidad de este navegador se consigue gracias a unos programas denominados **KIO slave**, que implementan protocolos locales o de Internet, como el indicado SSH.

Tal y como se muestra en la Figura 3.10, comprobamos que tiene elementos comunes a otros navegadores, como la utilización de barra de herramientas, barra de menú, barra de estado y área del documento. Al lado de la barra de dirección incluye un caja de texto enlazada por defecto con Google, que permite la búsqueda acerca de las palabras tecleadas sin necesidad de acceder a la página de este famoso buscador. El buscador o motor de búsqueda se puede cambiar, eligiendo "Seleccionar motor de búsqueda..." de la lista desplegable que nace en la parte inferior del icono.

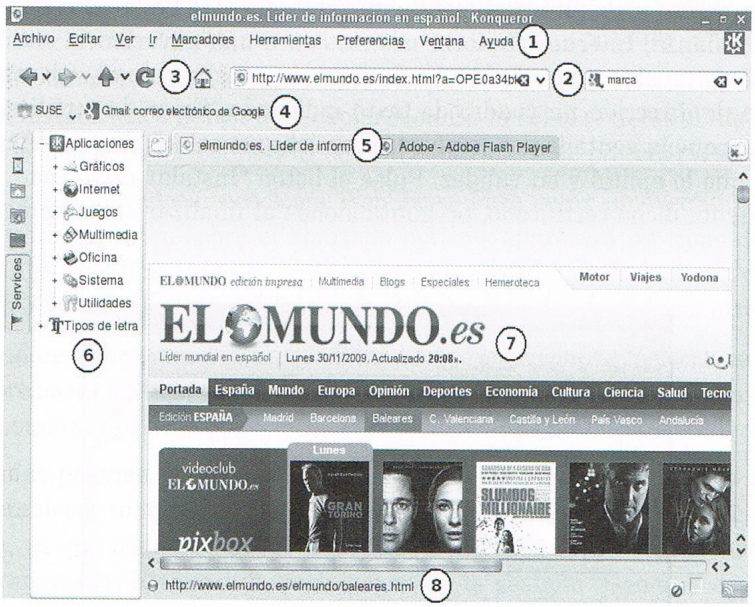


Figura 3.10. *Elementos principales del navegador Konqueror. 1 (Barra de menú), 2 (Barra de direcciones), 3 (Barra de herramientas), 4 (Marcadores), 5 (Pestañas), 6 (Panel de navegación), 7 (Área de trabajo) y 8 (Barra de estado)*

La configuración de Konqueror se presenta en una ventana con dos partes diferenciadas. En su parte izquierda, se representan mediante iconos grupos de opciones relacionadas entre sí. En su parte derecha se muestra un cuadro de diálogo con los diferentes parámetros de configuración referentes al icono seleccionado (véase Figura 3.11). Esta ventana de configuración es accesible mediante la opción "Configurar Konqueror..." del menú "Preferencias".

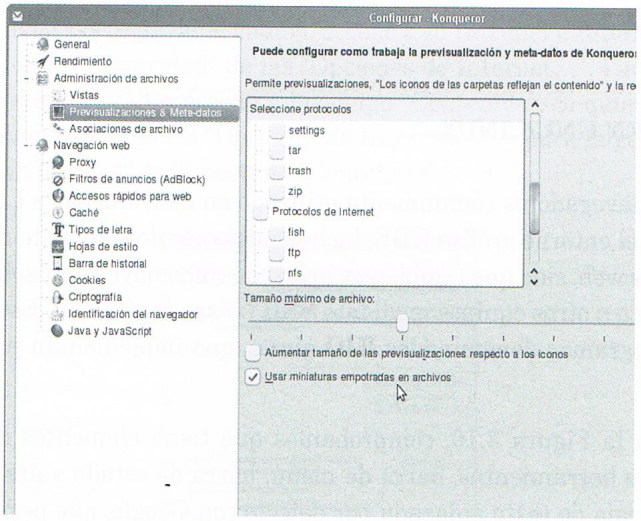


Figura 3.11. *Configuración del navegador Konqueror. En su parte izquierda se muestran grupos de opciones relacionadas y representadas por iconos. Esta figura muestra los KIO slaves que podemos instalar para poder utilizar los protocolos mostrados mediante este navegador*

Konqueror puede utilizar una serie de complementos mediante la instalación del paquete *kdeaddons*. Posteriormente podemos acceder a ellos mediante la opción de menú "Herramientas". Entre otras utilidades nos permite la traducción de la página visitada, la validación de páginas HTML o CSS, crear una galería de imágenes con las imágenes en miniatura que vemos en el área del documento o filtrar los elementos a visualizar de una carpeta. Para activar uno de estos complementos, acceda a la opción "Configurar extensiones" del menú "Preferencias".

Mediante el "Panel de navegación" (véase Figura 3.9), Konqueror nos brinda la posibilidad de navegar por las páginas marcadas como favoritas, por el historial de navegación, por la carpeta personal, por la red o por las aplicaciones que tenemos instaladas gracias a los KIO slaves. Estas diferentes opciones de navegación se nos muestran en forma de iconos a la izquierda de dicho panel y su contenido, en el interior del panel. Por ejemplo, en la Figura 3.10 puede comprobar las categorías de aplicaciones instaladas y al pulsar sobre una de ellas, en el área del documento se mostrarían las aplicaciones.

Para añadir un KIO slave, acceda a la ventana "Configurar Konqueror" y seleccione el apartado "Previsualizaciones & Meta-datos" (véase Figura 3.11). En la parte de la derecha se mostrarán los protocolos a nivel local y remoto que queremos utilizar. A nivel local, por ejemplo, podemos marcar el protocolo *zip* para visualizar el contenido de ficheros comprimidos en dicho formato. A nivel remoto, podemos marcar el protocolo FTP para permitirnos el acceso a un servidor FTP. Una vez instalado el KIO slave, en el área del documento podemos realizar acciones asociadas al protocolo. Por ejemplo al utilizar el protocolo local *zip*, podremos descomprimir un fichero en dicho formato.

Este navegador nos ofrece la posibilidad de utilizar diferentes vistas del área del documento, dividiéndolo en una parte superior e inferior, o izquierda y derecha. Para utilizarlas, activaremos "Barra de herramientas extra" de la opción "Barra de herramientas" del menú "Preferencias". Los diferentes iconos nos permitirán seleccionar la vista deseada.

Mediante la herramienta *AdBlock*, Konqueror nos permite el filtrado de páginas, bloqueando los elementos indeseados. Para indicar las URL que desea filtrar, seleccione la opción "Configurar..." e indíquela en el campo "Expresión" del cuadro de diálogo. Finalmente, aplique la configuración y acepte para cerrarlo.

Konkeror permite llevar a cabo tareas comunes a otros navegadores, como establecer una página de inicio mediante el apartado "General" de su configuración, visualizar el código HTML del documento mediante el menú "Ver" o el borrado y eliminación del historial de navegación y de las *cookies* mediante los subapartados de "Navegación web" "Barra de historial" y "Cookies", respectivamente.

Mediante el menú "Ver" podemos activar la previsualización de archivos, de manera que, en vez de mostrarse su icono representativo del tipo de archivo o carpeta, se mostrará una imagen en miniatura de su contenido. Por ejemplo, si el icono representa un archivo de imagen, se mostrará la imagen reducida. Si es un archivo de sonido, al pasar el ratón comenzará a reproducirse. Además, la opción "Modo de vista" del menú "Ver" nos permite conmutar entre un modo de vista navegador (KHTML) o editor de texto avanzado para edición de documentos web.

Para registrar los sitios que se han visitado para su posterior acceso, se utilizan los denominados "Marcadores" o "Bookmarks". Para registrar un sitio visitado ha de acceder a la opción "Añadir marcador" del menú "Marcadores", el cual se visualizará en la barra del mismo nombre para un fácil acceso. Una vez creados los marcadores los puede organizar agrupándolos en carpetas.

Este navegador, hace tiempo que incorpora una característica de gran utilidad implementada por varios navegadores, como son las **pestañas** o **tabs**, que permiten el acceso a varias páginas con una única ventana del navegador. Estos elementos nos permiten conmutar de una página a otra de una forma rápida y sencilla, seleccionando la solapa o pestaña correspondiente a la página deseada.

Cuando accedemos a un sitio web seguro mediante HTTPS, puede ser que el certificado no está firmado por una CA en la que confiemos, en cuyo caso mostrará un mensaje como el de la Figura 3.12, mostrándonos dicha advertencia. Si pulsa sobre el botón "Detalles" podrá comprobar entre otras cosas la entidad emisora del certificado. Si decidimos continuar, Konqueror preguntará al usuario si desea aceptar para siempre el certificado o tan solo para la sesión actual.

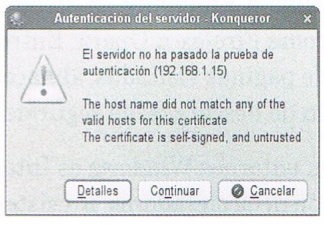


Figura 3.12. *Mensaje de advertencia de Konqueror. Este mensaje indica que el certificado es autofirmado y que se desconfía en él*

RESUMEN DEL CAPÍTULO

El servicio HTTP facilita el acceso a información de distinta naturaleza (texto, sonido, imágenes, vídeo, etc.) almacenada en páginas de servidores remotos, permitiendo también el acceso a otras páginas del mismo servidor o de otros mediante hiperenlaces. Las páginas dinámicas utilizan diversos lenguajes (PHP, ASP, Java, JavaScript, etc.) para permitir la interacción con los usuarios. Los documentos web se almacenan en el servidor en un directorio denominado sitio, utilizando una página a modo de índice para acceder al resto de los elementos.

Los clientes acceden a este servicio mediante un navegador, indicando en él la URL a la que quiere acceder. El servidor atiende la petición de la página solicitada y se la entrega al navegador del cliente para su visualización, siempre y cuando el contenido siga el estándar MIME. El diálogo para la petición y entrega de documentos se lleva a cabo mediante las líneas de encabezado de los documentos web. Cuando se desea mantener la privacidad de la información transmitida, se pueden utilizar protocolos seguros y alternativos a HTTP como S-HTTP, que utiliza extensiones a las líneas de encabezado para gestionar la seguridad, o HTTPS, que se basa en una conexión segura mediante SSL. Los usuarios pueden colaborar en el desarrollo del sitio web utilizando una extensión al protocolo HTTP 1.1 denominada WebDAV.

La configuración de este servicio requiere indicar al menos, el directorio o sitio donde se ubicarán las páginas y sus diferentes elementos (imágenes, fondos, sonidos, etc). Tambien conviene establecer los permisos sobre los directorios que forman la jerarquía del sitio. Adicionalmente, podremos requerir la autenticación de los usuarios, configurar sitios adicionales, asegurar las transferencias cliente-servidor, o establecer un entorno de colaboración.

Los sistemas operativos de Microsoft requieren la instalación de la utilidad IIS para la instalación del servicio, así como la del *Administrador de Servicios de Internet* para gestionarlo. Entre otras posibilidades, permite la configuración de directorios virtuales, autenticación de usuarios, comprensión de información transmitida o la utilización del protocolo seguro HTTPS.

Los sistemas operativos GNU/Linux requieren la instalación del software Apache 2 para proporcionar dicho servicio. Su configuración puede realizarse mediante herramientas gráficas que nos ofrezca la distribución, o de forma manual editando los ficheros de configuración y modificando los valores de sus parámetros. Apache 2, permite añadir nueva funcionalidad al servicio mediante módulos y ejercer como un servidor virtual alojando varios sitios en un mismo equipo para los clientes, siendo accesibles mediante distintas URL o distintas direcciones IP.

Los clientes pueden utilizar navegadores propietarios como Internet Explorer para sistemas operativos Microsoft Windows, o Konqueror, Nautilus o Epiphany en sistemas operativos Linux. También pueden utilizar navegadores multiplataforma como Firefox u Opera. Entre algunas de sus utilidades que ofrecen son la de proporcionar un recordatorio de páginas visitadas, almacenar la URL de aquellas que resulten de interés, utilización de pestañas o gestión de descargas, de seguridad y de ventanas emergentes.

Uno de los navegadores utilizados en entornos Windows es Internet Explorer, cuya versión 8 incorpora tecnologías como WebSlice o la utilización de aceleradores. En sistemas GNU/Linux puede utilizar Mozilla Firefox, que permite incorporar una amplia gama de complementos que amplían su funcionalidad.

EJERCICIOS PROPUESTOS

1. ¿Cómo se podría configurar un servidor con GNU/Linux instalado para utilizar como directorio raíz el utilizado por un servidor Windows? ¿Y cómo se podría configurar un servidor Windows para utilizar como directorio raíz el utilizado por un servidor GNU/Linux? Realiza las indicaciones pertinentes.

2. Configura un servidor HTTP con Windows 2008 instalado para que proporcione un servicio seguro a los clientes. Se utilizará como directorio raíz del sitio la carpeta compartida *share* del equipo denominado *srvfiles*. Además se desea que el sitio contenga el directorio *far* de otro equipo distinto de la red denominado *anothersrv*.

3. Implemente el supuesto del ejemplo 3.6 en una distribución GNU/Linux.

4. Implemente el supuesto del ejemplo 3.6 en Windows 2008, autogenerando también el certificado. Cree solamente el sitio web seguro y ubique la carpeta en el directorio raíz.

5. Configura un servidor Windows 2008 para incluir el directorio virtual denominado *virtualdir*, el cual es el sitio raíz de un servidor GNU/Linux denominado *lnxsrv*. Realice los supuestos que cree oportunos.

6. Configura un servidor GNU/Linux como servidor virtual para dar acceso a tres sitios. El primero se ubicará en el directorio */var/www/first.com*, el segundo en */var/www/second.com* y solo permitirá el acceso al usuario *curri*. Finalmente, el tercero se ubicará en el directorio */var/www/third.com*, pero hará referencia a modo de directorio virtual a una la carpeta compartida *sharefiles* del servidor Windows de nuestra red local *srvfiles*.

7. Indica los pasos a seguir con el navegador Internet Explorer 8 para acceder al servidor del ejercicio 3.

8. Indica los pasos a seguir para instalar el KIO slave *smb*. Utilízalo para acceder a una carpeta compartida en un equipo con sistema operativo Microsoft Windows instalado.

9. *Lynx* es un navegador muy peculiar de Linux. Instale el paquete correspondiente y compruebe su funcionamiento. ¿Qué característica hace particular a este navegador respecto a otros más conocidos como Internet Explorer o Mozilla Firefox?

TEST DE CONOCIMIENTOS

1 Las líneas de encabezado:
- a) Se utilizan para mostrar un encabezado en todas las páginas.
- b) Solamente se utilizan en páginas dinámicas.
- c) Con los valores de los encabezados se controla la transmisión.
- d) Ninguna de las anteriores.

2 Un sitio web:
- a) Suele estar formado por una jerarquía de directorios.
- b) Almacena los elementos de las páginas.
- c) Solamente almacena páginas web.
- d) a y b son correctas.

3 La extensión de HTTP, WebDAV:
- a) Está orientada a la filosofía de la Web 2.0.
- b) Solo permite mantener una versión de las páginas en el sitio.
- c) Solo permite la manipulación de páginas.
- d) Ninguna de las anteriores es correcta.

4 Las credenciales se utilizan en Windows 2008 Server:
- a) Para autenticación de los usuarios.
- b) Restringe el acceso a un directorio local como raíz del sitio.
- c) Solamente con referencias UNC.
- d) a y c son ciertas.

5 El webmaster:
- a) Solamente puede haber uno.
- b) En servidores con WebDAV puede haber varios.
- c) Se encarga de elaborar las páginas y sus contenidos.
- d) Todas las anteriores son ciertas.

6 Un GNU/Linux, un Servidor Virtual:
- a) Alberga directorios virtuales como los servidores Windows.
- b) Alberga varios sitios bajo diferente dirección de red.
- c) Permite referenciar el mismo sitio con diferentes nombres.
- d) b y c son ciertas.

7 Los módulos de Apache:
- a) Al cargar uno nuevo requiere reiniciar el servidor.
- b) No pueden cargarse *a posteriori*.
- c) Hay que parar el servicio para cargar uno nuevo.
- d) Al cargar uno nuevo requiere reiniciar el servicio.

8 Los complementos:
- a) Proporcionan versatilidad a mi navegador.
- b) Solo Internet Explorer permite su instalación.
- c) Los mantenemos actualizados mediante RSS.
- d) Evitan el almacenamiento de *cookies*.

9 Una WebSlice:
- a) Permite la navegación privada sin dejar rastros.
- b) Solamente es una página catalogada como favorita.
- c) Es un acelerador para previsualizar una página favorita.
- d) Ninguna de las anteriores.

4 El servicio de transferencia de archivos

OBJETIVOS DEL CAPÍTULO

- ✓ Describir el funcionamiento de FTP.
- ✓ Identificar sus ámbitos de aplicación.
- ✓ Diferenciar la utilización de FTP y TFTP.
- ✓ Identificar sus carencias para saber suplirlas.
- ✓ Conocer los parámetros más relevantes de un servidor.
- ✓ Instalar y configurar un servidor FTP.
- ✓ Conocer los parámetros más relevantes de un cliente.
- ✓ Instalar y configurar un cliente FTP.

De todos es conocida la forma en la que como usuarios interaccionamos con los sistemas de archivos de nuestro equipo local, realizando diversas operaciones sobre ellos como es la creación y borrado de carpetas, copia de archivos, cambio de ubicación de un archivo o conjunto de ellos, acceso a un subdirectorio perteneciente a una carpeta, etc. En una red, estas operaciones también se han hecho necesarias para los usuarios, de manera que puedan utilizar una red a modo de un gran sistema de ficheros, o sistema de ficheros virtual.

Algunos ejemplos de este servicio los tenemos al actualizar un programa a una nueva versión, o incluso el sistema operativo mediante parches de seguridad, al realizar descargas de información y software, al efectuar una instalación remota de un sistema operativo, al alojar y realojar páginas web en un sitio web o al clonar discos duros o particiones en red.

Para operar con este gran sistema de archivos, es necesario un protocolo que haga transparente estas operaciones al usuario sin necesidad de conocer las características de los sistemas de ficheros utilizados por los equipos de la red, dándole la impresión de hacerlo localmente. El protocolo FTP (*File Transfer Protocol* o Protocolo de Transferencia de Archivos) es el encargado de esta tarea.

4.1 FUNCIONAMIENTO DE FTP

Para lograr su objetivo, el protocolo FTP establece una doble conexión TCP (véase Figura 4.1) entre el cliente y el servidor:

- **Conexión de control**: suele utilizar el puerto 21 del servidor y es la que sirve para acceder a éste e indicarle las operaciones que el cliente desea realizar.

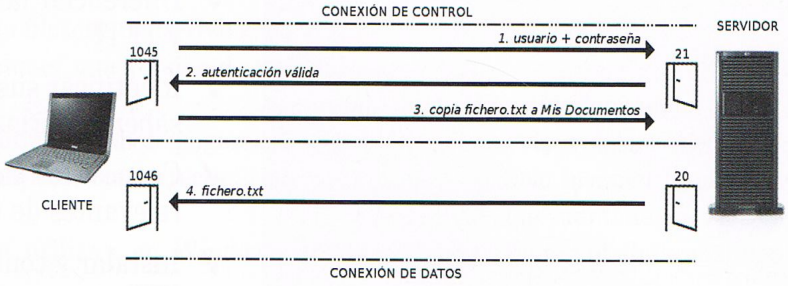


Figura 4.1. *Esquema de funcionamiento del servicio FTP. Se establece una conexión de control (puerto 21) para autenticación de usuarios y envío de operaciones. Se establece también una conexión de datos (puerto 20) para realizarse la transferencia de información*

- **Conexión de datos**: habitualmente se utiliza el puerto 20 del servidor y es la que sirve para la transferencia de archivos hacia o desde el servidor. El cliente puede negociar con el servidor un puerto distinto para establecer esta conexión, distinguiéndose dos modos:
  - **Modo Activo**: el cliente establece una conexión con el puerto habitual de datos para realizar la transferencia. Es el modo por defecto.
  - **Modo Pasivo**: el cliente utiliza la conexión de control para solicitar al servidor la utilización de un puerto distinto al habitual para la transferencia de datos. El servidor comunicará al cliente el puerto por encima del 1024 por donde atenderá la conexión de datos (véase Figura 4.2).

El cliente utiliza un puerto aleatorio para establecer la conexión de control y habitualmente el puerto inmediatamente superior para establecer la conexión de datos. Por ejemplo el cliente podría utilizar su puerto 1045 para la conexión de control con el puerto 21 del servidor, y el 1056 para la conexión de datos con el puerto 20 del servidor, siempre y cuando el cliente no requiera un modo pasivo.

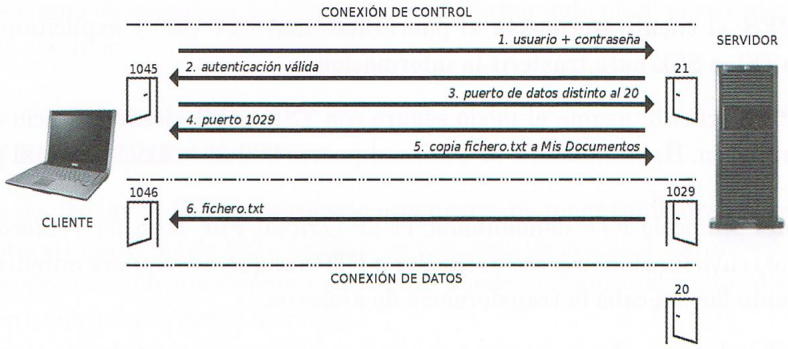


Figura 4.2. Esquema de funcionamiento del servicio FTP en modo pasivo. El cliente solicita un puerto diferente para la transmisión a través de la conexión de control. El servidor le responde con el número de puerto para poder hacer efectiva la transferencia de datos

Un servidor FTP nos permite dos formas de acceso:

- **Mediante acceso privado**: requiere que el cliente se autentique para poder acceder a él. Es decir, necesitará introducir su nombre de usuario y contraseña. Previamente la cuenta del usuario se deberá haber creado en el servidor.
- **Mediante acceso público**: el cliente no dispone de usuario ni contraseña en el servidor y utiliza una cuenta de tipo genérico denominada "anonymous". Como contraseña suele indicarse la dirección de correo electrónico, no siendo obligatorio.

Establecida la conexión entre el cliente y el servidor, el cliente tendrá acceso al sistema de ficheros del servidor mediante cualquiera de los siguientes métodos: línea de órdenes, navegador o programas específicos. Las partes del sistema de ficheros a las que el usuario tendrá acceso y las operaciones que podrá realizar en él, dependerá de los privilegios que al usuario se le hayan otorgado al configurar el servicio FTP, así como de los privilegios que el usuario tenga sobre cada una de las partes del sistema de ficheros en el servidor.

Para transferir un archivo puede determinarse su tipo: texto o binario. Esto evitará, por ejemplo, que al obtener un fichero ejecutable (binario) transferido como texto, no se ejecute. Si no lo indicamos, la transferencia se realizará según la configuración por defecto del servidor. Hoy en día, la utilización de programas específicos autodetectan el tipo de fichero a transmitir y no requiere que se especifique su tipo.

La jerarquía de ficheros y subdirectorios que se pone a disposición de los usuarios, se localiza en un directorio específico del servidor FTP, denominado **sitio** o **sitio FTP**. Conviene organizar la información del sitio de forma adecuada para facilitar al usuario el obtenerla.

Tenga en cuenta que este es un servicio no seguro, ya que tanto la autenticación del usuario como la transferencia de información se realizan sin encriptar, pudiendo ser interceptada por usuarios malintencionados y hacer mal uso de ella. Para realizar transferencias de información que comprometan la seguridad, es recomendable utilizar servicios más seguros como **SSH** (véase el capítulo *Acceso Remoto*), el cual implementa el protocolo **SFTP** (*Secure Shell File Transfer Protocol* o Shell Seguro para Protocolo de Transferencia de Ficheros) proporcionando un canal seguro en la transferencia de ficheros entre cliente y servidor.

Otra forma de asegurar la transferencia de ficheros es utilizar el servicio FTP apoyándose sobre una conexión segura, como por ejemplo mediante la utilización de **SSL** (*Secure Socket Layer* o Capa de Conexión Segura) o **TSL** (*Transport Layer Security* o Seguridad de la Capa de Transporte). Requiere mecanismos de cifrado, como por ejemplo de clave pública y la utilización de certificados. La utilización conjunta del protocolo FTP y SSL o TSL tiene dos modos de funcionamiento:

- **Explícito** o **FTPES**: el cliente se conecta al puerto habitual FTP (21) y explícitamente cambia a un modo seguro utilizando TSL o SSL para trasferir la información.
- **Implícito** o **FTPS**: el cliente asume el modo seguro con TSL o SSL desde el inicio de la conexión, antes de transferir la información. Habitualmente se utiliza el puerto 990 en vez del habitual puerto 21.

Existe una versión del protocolo FTP denominada TFTP (*Trivial File Transfer Protocol* o Protocolo Trivial de Transferencia de Archivos) cuyo funcionamiento es similar a FTP aunque no requiere autenticación del usuario antes de la conexión, simplemente lleva a cabo la transferencia de archivos.

Este protocolo es utilizado para clonar equipos en una red, para una instalación por red o para obtener los archivos del sistema operativo de un servidor en estaciones sin disco duro. Algunos ejemplos donde TFTP es utilizado lo tenemos en proyectos como TCOS (*Thin Client Operating System* o Sistema Operativo de Cliente Ligero) o LTSP (*Linux Terminal Server Project* o Proyecto de Servidor de Terminales Linux) para la obtención el sistema operativo en equipos antiguos con pocos recursos hardware. Otro ejemplo lo tenemos con WDM (*Windows Deployment Services* o Servicios de Despliegue de Windows), anteriormente RIS (*Remote Installation Services* o Servicios de Instalación Remota), utilizado en sistemas operativos Windows de servidor como 2008 ó 2003 para instalaciones desatendidas de sistemas operativos cliente Windows. Como se ha mencionado anteriormente, TFTP se limita a la transferencia de información, por tanto para lograr dicho objetivo, se debe utiliza de forma conjunta con otros protocolos, como por ejemplo:

- UDP (*User Datagram Protocol* o Protocolo de Datagramas de Usuario): permite a la máquina cliente enviar un mensaje de petición a los equipos de la red solicitando una dirección IP.
- DHCP o BOOTP (*Bootstrap Protocol* o Protocolo Autosuficiente): permiten a la máquina cliente obtener su dirección IP del servidor que alberga el núcleo o los ficheros de instalación del sistema operativo. Consulte el capítulo 1 para obtener mayor información.
- IP (*Internet Protocol* o Protocolo de Interred): para establecer comunicación con el servidor a través de la red.

El software que implemente estos protocolos deberá ser utilizado por el cliente mediante un disco de arranque o la tarjeta de red de su equipo, siempre y cuando ésta tenga soporte PXE (*Preboot eXecution Environment* o Entorno de Ejecución de Prearranque).

4.2 PARÁMETROS DE CONFIGURACIÓN DE FTP

4.2.1 PARÁMETROS EN EL SERVIDOR

La instalación y configuración de este servicio tiene gran similitud con la del servicio HTTP (véase capítulo 3). Principalmente consiste en determinar el directorio que ejercerá de raíz del sitio y establecer toda la estructura de

ficheros y directorios a ofertar a los clientes. También podremos establecer otros parámetros adicionales como aquellos que determinen la forma de acceso al sitio FTP por los usuarios (público o privado), determinar los privilegios que estos tendrán sobre el sitio FTP, si cada usuario tendrá restringido el acceso a su directorio particular o si tendrá acceso al sitio de otros usuarios, limitaciones respecto a la tasa de transferencia, número de conexiones o el tiempo de conexión e incluso asegurar la conexión mediante conexiones seguras. La gestión de espacio en disco o cuotas suele gestionarse a través del sistema de operativo, estableciéndose de forma individual para cada usuario del servicio que necesite alojamiento en el servidor.

4.2.2 PARÁMETROS EN EL CLIENTE

Previo a la utilización de un cliente FTP, es necesario asegurarse de tener configurada correctamente la red TCP/IP para que, a través de nuestro interfaz de red o módem, se disponga de acceso a distintos servidores de Internet. Si el equipo pertenece a una organización que dispone de proxy, se puede configurar el equipo del usuario o su navegador para indicar el dispositivo o equipo que ejerce de proxy.

La configuración de los parámetros del cliente consistirá básicamente en indicar el servidor al que se quiere acceder, bien con su dirección IP o mediante su nombre FQDN (véase capítulo 2). En función del tipo de usuarios que acepte el servidor, podremos autenticarnos como usuario anónimo o usuario del servidor. Indicaremos si el modo de transferencia que deseamos realizar es activa o pasiva, así como el tipo de ficheros que deseamos transferir. Adicionalmente podemos establecer otros parámetros como el directorio local y remoto por defecto. El establecimiento de estos parámetros del cliente se realizará dependiendo de la forma escogida para acceder al servidor remoto.

4.3 CONFIGURACIÓN DE UN SERVIDOR

Su puesta en práctica se ejemplifica sobre sistemas operativos Microsoft Windows, OpenSuSE 11.1, y Fedora Core 11 (derivada de Red Hat) y Debian 5 Lenny.

4.3.1 CONFIGURACIÓN EN MICROSOFT WINDOWS

Similar a la instalación del servicio HTTP, el software para FTP se puede instalar sobre Microsoft Windows NT Server, 2000 Server, 2000 Advanced Server, XP (Professional), 2003 Server, Vista (Business, Enterprise y Ultimate), 7 (Professional, Enterprise y Ultimate) y 2008 Server mediante la utilidad **IIS** (*Internet Information Server* o Servidor de Información de Internet), incluida en los discos de instalación. Antes de proceder a su instalación no olvide configurar previamente el acceso a la red TCP/IP.

4.3.1.1 Instalación del software

La tabla 4.1 le muestra los pasos (iconos, accesos directos, apartados, etc.) a seguir para consultar en los sistemas operativos que se muestran, si el servicio FTP incluido en IIS se encuentra instalado. En todos los sistemas operativos Windows expuestos anteriormente, se considera como punto de partida el *Panel de Control*.

En el caso de que el servicio no se encuentre instalado en nuestro equipo, en función del sistema operativo que tenga instalado y partiendo del último paso indicado en la tabla 4.1, deberá realizar las siguientes operaciones:

1 Pulse en el botón "Agregar" (Windows NT) o seleccione el componente a instalar (Windows 2000 y XP) y marque el servicio Microsoft Internet Information Server (Windows 2000) o Servicios de Internet Information Server (Windows XP). En Windows 2003 seleccione el icono Servidor de Aplicaciones, pulse el botón Detalles y marque Instalar Internet Information Services (IIS). En Windows Vista y 7 despliegue Internet Information Services así como Servidor FTP y Herramientas de administración web. En 2008 Server pulse sobre "Agregar funciones" en el subapartado "Funciones".

2 Deberá seleccionar los elementos de IIS a instalar. Para este servicio los más importantes son la conocida herramienta *Administrador del Servicio de Internet* (*Consola de administración* en Vista, 7 y 2008) y el *Servicio FTP* (*Servidor Web* en Vista, 7 y 2008).

3 Finalmente, en el caso de la instalación del servicio IIS en Windows NT se especificarán las carpetas que contendrán los ficheros de dicho servicio. Es recomendable que contengan solamente aquella información que queramos compartir y que el sistema de ficheros utilizado sea NTFS para un mejor control de seguridad. Para IIS de Windows 2000, XP, 2003, Vista, 7 y 2008, estas carpetas se establecen al configurar el servicio.

Tabla 4.1. Pasos para la consulta de la instalación de IIS en un sistema operativo Windows

Sistema Operativo	Pasos de Consulta del Servicio FTP
NT	1. Red. 2. Protocolos. 3. Protocolo TCP/IP. 4. Servicios. 5. Microsoft Internet Information Server 2.0. 6. Detalles.
2000 y XP (Professional)	1. Agregar o quitar programas. 2. Agregar o quitar componentes de Windows. 3. Servicios de Internet Information Server (IIS). 4. Detalles.
2003	1. Agregar o quitar programas. 2. Agregar o quitar componentes de Windows. 3. Componentes. 4. Servidor de Aplicaciones. 5. Servicios de Internet Information Server (IIS). 6. Detalles.
Vista (Business, Enterprise y Ultimate) y 7 (Professional, Enterprise y Ultimate)	1. Programas. 2. Programas y Características. 3. Activar o desactivar las características de Windows. 4. Internet Information Services.
2008	1. Herramientas administrativas. 2. Administrador del servidor. 3. Resumen de Funciones. 4. Funciones.

4.3.1.2 Configuración del servicio

Recuerde que la herramienta que permite la gestión de los servicios de IIS es el *Administrador de Servicios de Internet*, aunque recibe diferentes nombres en los distintos sistemas operativos Windows. En Windows NT y 2000 es el *Administrador de Servicios de Internet*; en Windows XP recibe el nombre de *Servicios de IIS*; para Windows 2003, Vista, 7 el de *Administrador de IIS* y el de *Administrador de IIS 6.0* para Windows 2008. Estas herramientas son accesibles en su correspondiente sistema operativo desde el menú de inicio del sistema en la opción "Inicio || Panel de Control || Herramientas administrativas" para Windows 2000, XP, 2003 y 2008. En el caso de Windows Vista y 7 tendrá que acceder además a "Sistema y Seguridad".

La configuración de dicho servicio resulta sencilla al igual que se trató en el servicio HTTP. En primer lugar, hay que añadir el servidor a la lista del administrador de IIS, permitiéndose un equipo local o remoto. Después, aunque IIS nos ofrece un sitio FTP predeterminado (directorio *\inetpub\ftproot*), se puede crear otro sitio FTP mediante la opción del menú principal "Acción || Nuevo" (manteniendo el icono del servicio FTP seleccionado). El servidor IIS de Windows 2000, 2003, Vista, 7 y 2008 son capaces de administrar varios sitios FTP, mientras que Windows XP solamente permite la administración del sitio FTP por defecto. Para alojar distintos sitios FTP en el servidor, ha de asociarse un puerto distinto a cada uno para atenderse las peticiones cliente. Cada uno de los sitios FTP podrá establecerse localmente o en un equipo remoto.

Al crear un nuevo sitio FTP, hay que especificar al asistente los siguientes parámetros:

- Breve descripción del sitio (para que el administrador pueda identificarlo).
- Dirección IP del servidor y puerto por el que se atenderán las solicitudes cliente. Por defecto se atenderán por cualquier dirección IP asignada al servidor y a través del puerto 21 que es el estándar para el servicio FTP.
- Utilización o no de aislamiento de usuarios (solo en Windows 2003 y 2008 Server), es decir, se indicará si los usuarios podrán tener acceso o no al directorio de otros usuarios ubicados en el sitio FTP. Las opciones posibles que proporciona el asistente son:
  - **No aislar usuarios**: los usuarios locales al servidor, tendrán acceso a los directorios de otros usuarios.
  - **Aislar usuarios**: los usuarios locales al servidor solo tendrán acceso a su propio directorio, el cual debe ser creado previamente por el administrador del sistema en el directorio raíz del sitio FTP y dentro de un directorio específico que se denominará *Localuser* (véase ejemplo 4.1).
  - **Aislar los usuarios mediante Active Directory**: los usuarios de Active Directory solo tendrán acceso a su propio directorio, el cual deberá tener el mismo nombre que la cuenta de usuario y se tendrá que crear dentro de un directorio que estará nominado con el nombre de dominio al que pertenece el usuario, y siempre dentro del directorio por defecto que establece IIS.
- Directorio del servidor que se utilizará como raíz del sitio y donde se ubicará toda la jerarquía de directorios, subdirectorios y ficheros a ofertar mediante este servicio.
- Permisos de acceso de los usuarios al sitio FTP (normalmente suele ser solamente *Lectura*).

Además de los parámetros anteriormente facilitados al asistente para la creación de un nuevo sitio FTP, se pueden establecer otros parámetros que aparecen con unos valores por defecto. En Windows 2003 y 2008 Server los podemos modificar seleccionando la opción "Propiedades" del menú contextual del sitio FTP elegido. Los parámetros se encuentran agrupados en las siguientes secciones:

- **Sitio FTP**: establece la dirección IP y el puerto por el que el servidor atenderá las solicitudes FTP cliente, pudiéndose restringir el número y el tiempo de duración de las conexiones que se establezcan. También permite el registro periódico de las operaciones realizadas por los usuarios, así como listar los que están conectados y

proceder a su desconexión (botón "Sesiones actuales"). Adicionalmente se puede ampliar la información que se desea registrar, así como cambiar la ubicación y el formato del fichero donde se almacena dicho registro.

- **Cuentas de Seguridad**: habilita el acceso anónimo y establece la cuenta del usuario local o remoto que tendrá dicha condición. Además, permite restringir la conexión exclusivamente a estos usuarios.
- **Mensajes**: en esta sección se determinan los mensajes a mostrar a un usuario cuando se conecta, desconecta o supera el límite de conexiones establecido.
- **Directorio Particular**: establece un directorio local o remoto como raíz del sitio FTP, los privilegios (Lectura y Escritura) que los usuarios tendrán sobre él y el formato en el que se mostrará la jerarquía de carpetas y ficheros que aloja (MSDOS o UNIX).
- **Seguridad de Directorios**: permite indicar los equipos o grupos de equipos a los que se les concederá o denegará la conexión con el servidor. Por tanto deberá indicar la dirección IP en caso de tratarse un solo equipo, o una máscara de red en caso de tratarse de un grupo de equipos o red.

En Windows 7 y Vista, al acceder al Administrador de IIS y al pulsar sobre un sitio FTP, podemos modificar parámetros adicionales mediante cada uno de los iconos que se muestran y que a continuación se describen brevemente (véase Figura 4.3):

- **Aislamiento de usuario FTP**: ya se ha explicado con anterioridad.
- **Autenticación FTP**: habilita el modo de acceso de los clientes al contenido del sitio FTP, permitiendo un acceso anónimo, un acceso básico mediante una cuenta de usuario en el servidor o en dominio. Por defecto los modos de acceso se encuentran deshabilitados. Mediante la acción "Proveedores personalizados" situada en el panel derecho, se permiten cuentas de usuarios .NET y de administradores de IIS.
- **Compatibilidad con el firewall FTP**: permite indicar la dirección IPv4 externa del firewall así como el intervalo de puertos que utiliza para las conexiones de datos.

Recuerde que al crear un sitio con Aislamiento de usuarios, debe crear una carpeta *Localuser* que contendrá una subcarpeta por cada usuario local y una subcarpeta *Public* si se permite el acceso a usuarios anónimos.

- **Configuración SSL de FTP**: utilizada para permitir o requerir conexiones SSL en las conexiones de control y datos, pudiendo personalizarlas de forma individualizada e indicar el certificado SSL a utilizar. Además, se puede establecer un cifrado más eficaz de 128 bits, aunque consumirá más recursos del procesador y el tiempo en la transferencia se verá incrementado. La utilización de certificados se realiza de forma similar a la del capítulo 3.
- **Examen de directorios FTP**: permite decidir el formato con el que se mostrará al cliente el listado con la jerarquía de archivos y directorios del sitio FTP, así como la información asociada a ellos.
- **Filtrado de solicitudes de FTP**: permite restringir aquellas solicitudes cliente en cuya petición incluyan ficheros con determinadas extensiones, utilicen URL que incluyan ciertos secuencias de texto, una serie de órdenes FTP (véase tablas 4.4, 4.5 y 4.6), e incluso ocultar en la lista del sitio que se muestre al cliente aquellos elementos que incluyan un determinado segmento de texto en la URL.

- **Mensajes de FTP**: establece los mensajes que le aparecerán a los clientes, permitiendo determinar la aparición del texto del titular, la utilización de variables de usuario o detallar el mensaje ante peticiones locales.
- **Registro de FTP**: permite llevar un registro de las conexiones clientes mediante archivos de registro. Podemos decidir el directorio donde se ubicarán, la información que queremos registrar, su formato y el método utilizado para crear un nuevo archivo, pudiéndose crear periódicamente, cuando el fichero actual supere un determinado tamaño, o simplemente no crearlo.
- **Reglas de autorización de FTP**: permite establecer los usuarios que tendrán acceso al sitio FTP, así como los permisos que tendrán sobre su contenido.
- **Restricciones de direcciones IPv4 y de dominios**: permite indicar las direcciones IP, intervalos de direcciones IP junto con su máscara de red y nombres de dominio, que tendrán acceso al sitio FTP. Hacer notar que la restricción mediante nombres de dominio requerirá un servidor DNS asociado con posibilidad de resolución inversa (véase capítulo 2).
- **Sesiones actuales de FTP**: permite monitorizar las conexiones que tienen establecidas los clientes con el servidor, mostrando información adicional como su dirección IP, las operaciones realizadas, el tiempo de conexión o la cantidad de información transferida.

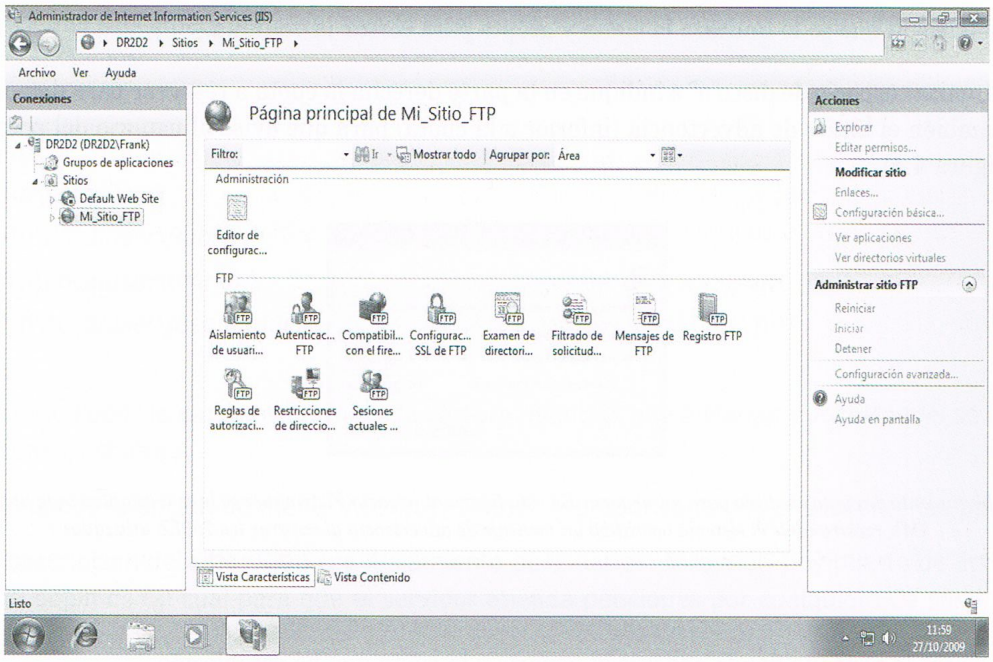


Figura 4.3. *Ventana de configuración del Administrador de IIS en Windows 7. En el panel de la izquierda distinguimos los diferentes sitios a administrar. En el panel central se encuentran diferentes iconos que nos permiten configurar los diferentes aspectos del servicio para el sitio seleccionado. Finalmente el panel izquierdo muestra las diferentes acciones a llevar a cabo*

Windows XP, 2003, Vista, 7 y 2008, también nos permiten la creación de "Directorios Virtuales" en el sitio FTP (véase capítulo 3). Para crearlos, se selecciona un sitio y se elige la opción "Nuevo || Directorio Virtual" del menú contextual en 2003 y 2008. En Vista y 7, la opción aparece directamente en el menú contextual como "Agregar directorio virtual". El asistente solicitará un alias o nombre para el directorio, la carpeta local o remota a la que hará referencia y los permisos de acceso.

La administración de cuotas en disco para los usuarios es posible gracias al sistema operativo, cuyo procedimiento es muy similar en la mayoría de sus versiones y atiende a los siguientes pasos:

1 Tenga visible la unidad de disco (por ejemplo accediendo desde "MiPC") sobre la que quiere establecer las cuotas.

2 Pulse botón derecho sobre la unidad y acceda a la pestaña "Cuota".

3 Marque la casilla "Habilitar la administración de cuota" para activar el control de cuotas.

4 Opcionalmente puede denegar espacio en disco a aquellos usuarios que superen la cuota establecida. También puede indicar que el sistema reproduzca un aviso sonoro cuando supere su cuota o el límite de advertencia.

5 Para establecer cuotas individualizadas, pulse el botón "Valores de cuota", apareciendo una ventana con los usuarios y las cuotas asignadas.

6 Acceda al menú "Cuota" y seleccione "Nueva entrada de cuota...".

7 Indique el usuario al que se le limitará la cuota y acepte para cerrar la ventana.

8 Seleccione "Limitar espacio de disco a" e indique en la parte derecha la cuota a reservar para dicho usuario. Puede establecer también el límite de advertencia (inferior a la cuota) para que avise al usuario del poco espacio que le quede (véase Figura 4.4).

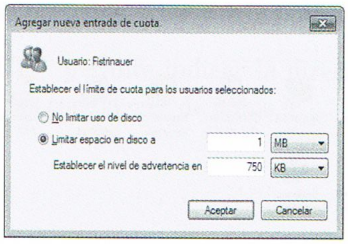


Figura 4.4. *Establecimiento de cuota en disco para un usuario. En esta figura al usuario Fistrinauer se le está estableciendo un límite en disco de 1Mb, mostrándole el sistema operativo un mensaje de advertencia al superar los 750Kb utilizados*

9 Finalmente cierre la ventana donde aparece el usuario y la cuota que ha establecido.

10 Aplique y acepte en el cuadro de diálogo previo para que los cambios surtan efecto.

4.3.1.3 Iniciar el servicio

Desde el *Administrador de Servicios de Internet* se pueden parar y reanudar en los servicios configurados y los sitios creados. Puede utilizar los botones que se encuentran en la barra de herramientas de esta utilidad o a través de la opción "Acción" del menú principal o del panel "Acciones" en Windows 7 y Vista.

EJEMPLO 4.1

Se desea proporcionar un servicio FTP mediante un servidor Windows 2008 Server que permita el acceso público y de usuarios con cuenta en el servidor. Se requiere que se muestre un mensaje de bienvenida a los usuarios. A los usuarios anónimos solamente se les permitirá la descarga. Solamente se permitirá el acceso a los usuarios locales josemanuel y marian. Se destinará la carpeta FTP para alojar el sitio FTP. El tiempo de acceso no superará los 5 minutos.

Suponiendo que la utilidad IIS está instalada, iniciamos el Administrador de Servicios de Internet ("Inicio || Herramientas administrativas || Administrador de Servicios de Internet").

Creamos la siguiente jerarquía de carpetas:

Recuerde que al crear un sitio con Aislamiento de usuarios, debe crear una carpeta *Localuser* que contendrá una subcarpeta por cada usuario local y una subcarpeta *Public* si se permite el acceso a usuarios anónimos.

C:\ftp
C:\ftp\Localuser
C:\ftp\Localuser\Public
C:\ftp\Localuser\marian
C:\ftp\Localuser\josemanuel

Al directorio *Public* le daremos permiso de Lectura mientras que a *Marian* y *JoseManuel* se los daremos de Lectura y Escritura.

Seleccionamos la opción de menú "Acción || Nuevo" y proporcionamos al asistente los parámetros:

- Descripción del sitio: Sitio con Aislamiento de usuarios. Dirección IP y puerto de acceso al sitio: lo dejamos tal cual para que el servidor atienda peticiones por cualquiera de sus interfaces de red.
- Marcamos Aislar usuarios: Carpeta: *C:\ftp*
- Permisos de acceso: Lectura y Escritura.

Complementamos los parámetros seleccionando la opción *Propiedades del menú contextual* del sitio FTP creado y nos desplazamos por cada una de las solapas:

- Sitio FTP:
  Tiempo de espera de conexión: 3000 (segundos).
- Mensajes:
  Bienvenida: Bienvenido al servidor FTP Windows 2008

4.3.2 CONFIGURACIÓN EN GNU/LINUX

En este apartado se explica cómo proporcionar el servicio FTP mediante el demonio **vsftpd** (*Very Secure Ftp Daemon* o Demonio Ftp Muy Seguro), incluido en Open SuSE 11.1, Fedora Core 11 y Debian 5 Lenny. En estas distribuciones el procedimiento a seguir para su puesta en funcionamiento es similar, el cual se expone a continuación.

La instalación del software se basa en la del paquete *vsftpd*, disponiendo de cualquiera de las siguientes alternativas:

- Si dispone de la distribución en soporte físico junto con sus paquetes, puede utilizar órdenes para acceder al medio donde se encuentra e instalar el paquete deseado, por ejemplo, mediante la orden *rpm* o *dpkg*.
- Mediante una orden, para descargarlo de los repositorios de la distribución e instalarlo, como por ejemplo mediante *apt-get*, *yum* o *aptitude* (véase ejemplo 4.4).
- Utilizar una utilidad gráfica como el *Administrador o Gestor de Software*, perteneciente a la herramienta *YaST2* de OpenSuSE, el gestor de paquetes *Synaptic*, integrado en entornos de escritorio *GNOME*, o *KPackageKit*, utilizado en entornos *KDE*.

Una vez instalado el paquete, y para configurar el servicio, se ha de editar el fichero *vsftpd.conf* situado en el directorio */etc* en OpenSuSE y Debian, y en */etc/vsftpd* en Fedora. Puede utilizar el fichero *vsftpd.conf* que se instala a modo de ejemplo y descomentar (suprimir el símbolo #) aquellos parámetros que se deseen habilitar o bien consulte la tabla 4.2 donde se muestran algunos de los parámetros más relevantes. Observará que algunos parámetros tienen como valor predeterminado 'YES' y otros tienen un valor numérico que podremos modificar. Los parámetros que encontrará en el fichero de ejemplo se encuentran agrupados en las siguientes secciones:

- **General Settings**: establece las opciones de carácter general de dicho servicio. Por ejemplo, permite habilitar la escritura en el servidor FTP o establecer el mensaje de bienvenida a los usuarios que accedan al servidor.
- **Local FTP user Settings**: establece las opciones para aquellos usuarios que poseen una cuenta en el servidor FTP. Por ejemplo, permite o deniega su acceso desde un cliente remoto, restringe el acceso de estos usuarios a su directorio personal o les permite el acceso a toda la jerarquía del sitio FTP en el servidor, pudiendo limitar su tasa de transferencia.
- **Anonymous FTP user Settings**: establece las opciones para aquellos usuarios que no poseen cuenta en el servidor FTP, es decir, los usuarios anónimos. Por ejemplo, podremos permitir o no su acceso, así como otorgarles el privilegio de escritura, creación de directorios, renombrado o limitar su tasa de transferencia.
- **Log Settings**: establece las opciones necesarias para el registro de toda interacción de los clientes con el servidor. Por ejemplo, se podrían registrar las peticiones al servidor y sus respuestas, así como las transferencias realizadas.
- **Transfer Settings**: establece las opciones relativas al proceso de transferencia. Por ejemplo, podría configurar el puerto por el que se realizan las transferencias, indicar el número máximo de clientes que se pueden conectar e incluso por dirección IP, establecer el *timeout* tras el cual un usuario que no interacciona con el servidor, es desconectado, o bien indicar la utilización de una conexión segura con SSL.
- **Modo de operación standalone**: permite que el demonio se ejecute con autonomía propia con independencia del demonio *xinetd*, o si por el contrario dependerá de éste último.

Tabla 4.2. Descripción de algunos de los principales parámetros de configuración del fichero vsftpd.conf

Parámetro	Utilidad
write_enable	Permite la escritura en el sitio.
dirmessage_enable	Permite mostrar mensajes a un usuario al acceder a los directorios.
ftpd_banner	Establece el mensaje de bienvenida del servidor.
local_enable	Debe habilitarse para permitir el acceso FTP para usuarios con cuenta en el servidor.
local_root	Especifica el directorio raíz del sitio. Cada distribución tiene uno establecido por defecto.
local_umask	Establece la máscara de creación de archivos y directorios para usuarios con cuenta en el servidor.
chroot_list_file	Indica la ruta del fichero *vsftpd.chroot_list*, que contiene un listado de usuarios con cuenta en el servidor. Se suele utilizar conjuntamente con *chroot_list_enable*.
chroot_local_user	Restringe a su directorio personal a los usuarios con cuenta en el servidor.
chroot_list_enable	Cambia el directorio raíz del sitio FTP por el directorio personal, a aquellos usuarios locales del servidor que se indiquen en el fichero referenciado en el parámetro *chroot_list_file*. Si el parámetro *chroot_local_user* también está activo, los usuarios tendrán acceso a su directorio personal así como al de los demás usuarios.
local_max_rate	Indica la tasa de transferencia expresada en bytes para los usuarios con cuenta en el servidor.
anonymous_enable	Habilita el acceso FTP para usuarios sin cuenta en el servidor.
anon_world_readable_only	Permite descargar ficheros del servidor a los usuarios sin cuenta en él.
anon_upload_enable	Permite alojar ficheros en el servidor a los usuarios sin cuenta en él.
anon_umask	Establece la máscara de creación de archivos y directorios para usuarios sin cuenta en el servidor.
anon_mkdir_write_enable	Permite crear directorios en el servidor a los usuarios que carecen de cuenta en él.
anon_other_write_enable	Permite borrar y actualizar en el servidor a los usuarios sin cuenta en el servidor.
anon_max_rate	Indica la tasa de transferencia expresada en bytes para los usuarios sin cuenta en el servidor.
log_ftp_protocol	Habilita el registro de todas las peticiones al servidor y sus respuestas.
vsftpd_log_file	Indica la ruta del fichero que contendrá la información de registro.
syslog_enable	Se delega en el demonio *syslog* la gestión del registro de peticiones.
connect_from_port_20	Habilita el puerto 20 del servidor para efectuar transferencias de información.
idle_session_timeout	Establece el timeout para usuarios que permanecen inactivos con el servidor.

data_connection_timeout	Establece el timeout para usuarios que permanecen activos con el servidor.
pasv_enable	Habilita el método pasivo para la conexión de datos.
ssl_enable	Permite la utilización de FTP mediante SSL. Requiere que *vsftpd* se haya instalado con soporte OpenSSH.
rsa_cert_file	Indica la ruta al fichero *vsftpd.pem* que contendrá el certificado RSA para la utilización de conexiones SSL.
rsa_private_key_file	Indica la ruta al fichero que contendrá la clave privada RSA para conexiones SSL.
allow_anon_ssl	Habilitar SSL para los usuarios anónimos. Puede tomar los valores YES o NO.
ssl_tlsv1	Se prefiere la utilización de la versión 1 de TLS. Admite los valores YES o NO.
force_local_data_ssl	Obligatoriedad o no en la utilización de SSL en todas las operaciones. Admite los valores YES o NO.
force_local_logins_ssl	
ssl_sslv2	Se prefiere la utilización de la versión 2 de SSL. Admite los valores YES o NO.
ssl_sslv3	Se prefiere la utilización de la versión 3 de SSL. Admite los valores YES o NO.
listen	Habilita el modo de trabajo *standalone* para *vsftpd*.
listen_port	Indica el puerto de escucha para el demonio *vsftpd* en modo *standalone*.
listen_address	Indica la dirección IP de escucha. Solo utilizado en modo *standalone*.
max_clients	Indica el número máximo de clientes que se pueden conectar en modo *standalone*.
max_per_ip	Indica el número máximo de conexiones por dirección IP en modo *standalone*.
pam_service_name	Indica el nombre del programa **PAM** (*Pluggable Authentication Modules* o Módulos Instalables de Autenticación) que gestiona la autenticación para el demonio vsftpd. Es recomendable utilizarla para evitar rechazo en las conexiones.

En función del servicio que deseemos prestar a los clientes, podemos utilizar dos ficheros para establecer una serie de restricciones, el fichero *vsftpd.chroot_list* que contiene la lista de usuarios locales a los que se les restringirá a su directorio personal, y *ftpusers*, que contiene la lista de usuarios que no podrán acceder al servicio.

Antes de iniciar el servicio, deberá crear la jerarquía de directorios y ficheros del sitio FTP. El directorio raíz por defecto del sitio es el directorio *ftp*, situado en */srv* en OpenSuse, */home* en Debian y */var* en Fedora. Si decide restringir los usuarios con cuenta local en el servidor a su directorio personal, podrá cambiar el directorio raíz por defecto del sitio a cada usuario local que desee, por su directorio. Por tanto, será el directorio *ftp*, o bien el directorio personal de los usuarios locales, donde crearemos dicha jerarquía para que el demonio *vsftpd* accederá a la información a proporcionar o alojar por los usuarios. Para restringir el acceso a esta información estableceremos los permisos pertinentes sobre directorios y ficheros en función de los usuarios y las operaciones a realizar sobre ellos mediante la orden *chmod*.

Vsftpd carece de la posibilidad de establecer cuotas de disco para los usuarios del servicio, siendo necesarias gestionarlas desde el sistema operativo, requiriendo la instalación del paquete *quota*. En GNU/Linux antes de poder gestionarlas es necesario editar el fichero */etc/fstab*, y añadir *usrquota* (cuota de usuario) o *grpquota* (cuota de grupo) como parámetro del punto de montaje del sistema de ficheros en el que queramos utilizar cuotas. Para que este cambio

se haga efectivo es necesario reiniciar el equipo o volver a montar los sistemas de ficheros afectados mediante la orden *mount –o remount PuntoDeMontaje*. Será necesario crear los ficheros de cuotas (*aquota.user* y *aquota.group*) mediante la orden *touch PuntoDeMontaje/aquota.user PuntoDeMontaje/aquota.group*, estableciendo los permisos para que solo puedan ser accedidos por el administrador (orden *chmod*). También es necesario crear la tabla con la información del espacio en disco de los sistemas de ficheros afectados por la utilización de cuotas mediante la orden *quotacheck -avgum*. La asignación de cuotas se realiza mediante la orden *equota -u NombreUsuario* o *equota -g NombreGrupo*, dependiendo si se establece para un usuario o grupo de ellos (véase ejemplo 4.2). Al ejecutarlo se abrirá el editor establecido por defecto para que se puedan establecer los siguientes parámetros:

- **Blocks**: indica el número de bloques utilizados por el usuario.
- **Soft**: expresado en Kb, indica el máximo espacio en disco que la cuota de usuario puede utilizar en esa partición antes de recibir una advertencia, la cual puede superar en un período conocido como de gracia.
- **Hard**: solo se utiliza cuando el tiempo de gracia se ha configurado. Expresado en Kb, indica el límite absoluto de espacio en disco que no puede superar el usuario.
- **Inodes**: indica el número de ficheros que puede utilizar el usuario.

Para iniciar el servicio de cuotas hay que ejecutar la orden *quotaon –vaug*, y para detenerlo mediante la orden *quotaoff –vaug*.

EJEMPLO 4.2

Deseamos establecer una cuota de disco en una distribución OpenSuSE para el usuario *fistrinauer*, de forma que no exceda de 5Mb para el sistema de ficheros de la partición */dev/hdb1*. Supondremos que el paquete *quota* se encuentra instalado.

En primer lugar editaremos el fichero */etc/fstab* e incluiremos en la línea relativa al sistema de ficheros */dev/hda1* el parámetro *usrquota*.

```
/dev/hdb1    /     ext2 defaults,usrquota        0       1
/dev/hdb2  none    swap sw                       0       0
```

Volvemos a montar el sistema de ficheros y creamos los ficheros de cuotas con los correspondientes permisos. También ejecutaremos la orden para crear la tabla con la información del espacio en disco utilizado por el sistema de ficheros afectado.

```
#mount -o remount /
#touch /aquota.user /aquota.group
#chmod 600 /aquota.*
#quotacheck -avgum
```

Ejecutamos la orden *equota* para asignar la cuota al usuario *Fistrinauer*.

```
#equota -u fistrinauer
```

Tras abrirse el editor, estableceremos el parámetro *hard* a 5120 (5Mb equivalen a 5120Kb).

```
Filesystem     blocks       soft       hard     inodes
/dev/hdb1          12          0       5120          3
```

Finalmente iniciamos el servicio.

```
#quotaon -vaug
```

Si utilizamos un entorno GNOME, podemos administrar la configuración del servicio utilizando la herramienta *FTP Administration* instalando el paquete *system-config-vsftpd*. OpenSuSE también nos lo permite mediante su herramienta *YaST2*, accediendo a los "Servicios de red" y pulsando sobre "Servidor FTP", requiriéndose el paquete *yast2-ftp-server* previamente instalado. En el panel de la izquierda nos aparecen las opciones de configuración agrupadas como se muestra en la parte izquierda de la Figura 4.5 y que se describen brevemente a continuación:

- **Inicio**: permite establecer el demonio que se hará cargo del servicio, así como guardar la configuración y reiniciar el servicio indicándonos su estado.
- **General**: establece el mensaje de bienvenida, la máscara de creación de archivos y directorios para usuarios locales y anónimos, permite la restricción de los usuarios a su directorio personal, así como indicar el directorio raíz del sitio para los usuarios anónimos y autenticados.
- **Rendimiento**: permite establecer un límite para el tiempo de la conexión, el número de conexiones por dirección IP, el número de clientes conectados y la velocidad de transmisión en Kbps para usuarios locales y anónimos.
- **Autenticación**: permite indicar el tipo de usuario que utilizará el servicio y si se les habilita para la subida de archivos.
- **Ajustes avanzados**: permite soportar el modo pasivo así como el rango de puertos utilizados para que el cortafuegos los habilite, habilitar el soporte para conexiones SSL, TSL y la utilización de certificados. Además permite configurar el cortafuegos para no rechazar las peticiones en las interfaces de red que indiquemos.

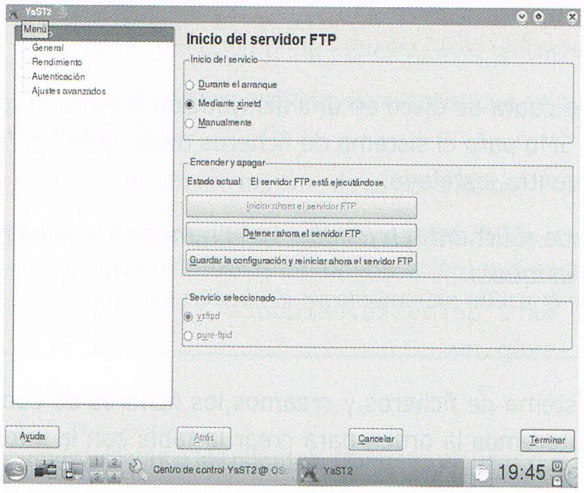


Figura 4.5. *Configuración del servicio FTP en OpenSuSE mediante YaST2. En el menú izquierdo se encuentran los diferentes grupos de parámetros de configuración, mientras que en la parte central se encuentran los parámetros del elemento del menú elegido*

El inicio del servicio dependerá de la configuración que hayamos dado en *vsftpd.conf*. Si hemos optado por una configuración **standalone**, será el demonio *vsftpd* el que se encargue de responder las peticiones FTP. Para iniciar el demonio *vsftpd* lo haremos con privilegios de superusuario ejecutando la orden *service vsftpd start* en Fedora, *rcvsftd start* en OpenSuSE y */etc/init.d/vsftpd start* en Debian. Sin embargo, si hemos optado por una configuración no *standalone*, será el demonio *xinetd* el que responda las peticiones FTP. Para ello, pare el demonio *vsftpd* si lo inició en modo *standalone*, edite el fichero */etc/xinetd.d/vsftpd*, establezca la opción *disable* con valor *no* y posteriormente reinicie el demonio *xinetd*. Alternativamente podemos activar el demonio *vsftpd* utilizando *YaST2* mediante la opción "Servicios de red || Servicios de red (xinetd)" o "Sistema || Servicios del sistema (niveles de ejecución)" en OpenSuSE, mediante "Lanzador de aplicaciones || Administración || Administración de servicios" en un entorno KDE, o mediante "Sistema || Administración || Servicios" en un entorno GNOME (véase Figura 4.6).

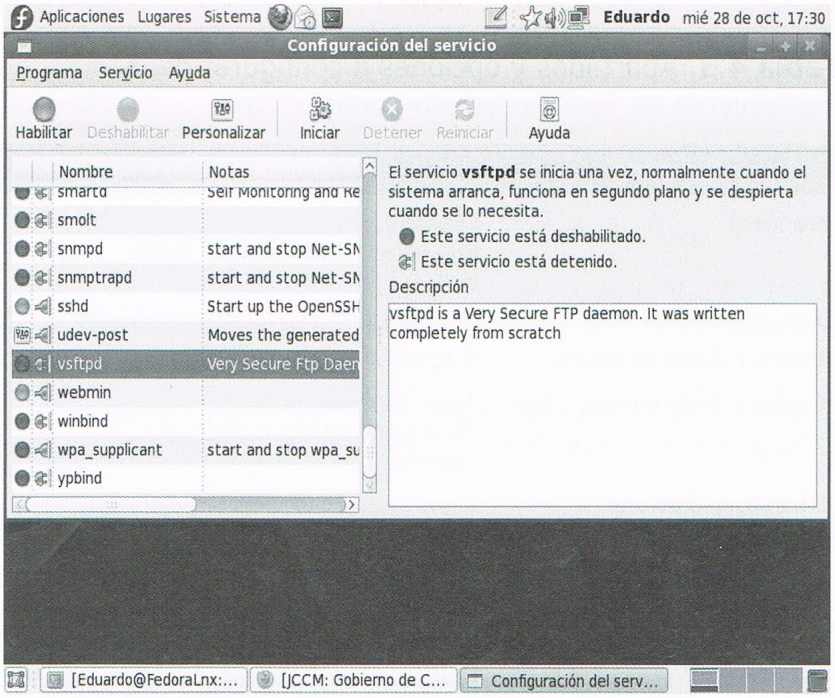


Figura 4.6. Administración de servicios de GNOME. En la parte izquierda se muestran el estado de los servicios (habilitados en verde o deshabilitados en rojo). Mediante los iconos podremos cambiar su estado e incluso iniciarlos

La utilización de un FTP seguro se realiza de forma similar a la expuesta en el capítulo 3, siendo necesaria la generación de un certificado que se ubicará en un directorio con privilegios de administrador. Las opciones correspondientes a FTP seguro las puede consultar en la tabla 4.2, como la localización del certificado, su activación o si se quieren utilizar todas las operaciones con SSL. Otra forma de realizar transferencias seguras es mediante la utilización del servicio SSH, que requiere la instalación del paquete *OpenSSH* (véase capítulo 5).

4.3.2.1 Ejemplos de configuraciones



EJEMPLO 4.3

Queremos proporcionar un servicio FTP mediante un servidor Fedora 11 en el que se permita solamente el acceso público mostrando un mensaje de bienvenida. Se permitirán solamente un acceso simultáneo de 5 usuarios y en modo pasivo. A los usuarios anónimos se les permitirá tanto leer como ver la lista de ficheros, así como subirlos al servidor. Dicho servicio dependerá de su demonio *vsftpd*.

Suponiendo instalado el paquete *system-config-vsftpd*, accedemos a "Sistema || Administración || FTP Administrator" y marcamos en el apartado correspondiente las opciones indicadas en la siguiente tabla:

Tabla 4.3. Apartados y opciones a configurar de la herramienta de Fedora system-config-vsftpd

Apartado	Opciones a activar
General	Enable download files. Run server in standalone mode. Protocol settings: IPv4.
Access Control	Use string: Bienvenido a FTP Fedora.
Users / System users	Ninguna.
Users / Anonymous user	Allow anonymous user. Allow upload files. Allow to download world-readable files.
Directory Options	Allow to users to view directory list.
Logging	Ninguna.
Network Options	Run vsftpd with ... Maximum number of simultaneous client ...: 5. Enable passive connections.
Transfer Log	Se deja en sus valores por defecto.

Pulse sobre "Archivo || Guardar" para establecer las opciones elegidas en el fichero de configuración y pulse sobre "OK".

Acceda al apartado "Server Control" y pulse el botón "Start FTP Server" para iniciar el servicio.

EJEMPLO 4.4

Queremos proporcionar un servicio FTP mediante un servidor Debian 5 en el que se permita el acceso público y a usuarios con cuenta en el servidor. Deseamos que se dé un mensaje de bienvenida a los usuarios. A los usuarios anónimos solamente se les permitirá la descarga, se limitará su tasa de transferencia a 7,2 Kb y solamente se les permite 5 minutos de acceso. Para los usuarios locales *josemanuel* y *marian* además, se restringirá su acceso a su directorio personal. Dicho servicio dependerá de su demonio *vsftpd*.

Comprobamos si tenemos instalado el paquete *vsftpd*:

```
dpkg -l | grep vsftpd
```

Suponemos que no está instalado. Utilizamos la orden *apg-get* para descargarlo de los repositorios e instalarlo:

```
apt-get install vsftpd
```

Las opciones habilitadas en */etc/vsftpd.conf* serían las siguientes:

```
#
#Fichero de configuración del servicio FTP /etc/vsftpd.conf
#
# General Settings
#-----------------
ftpd_banner="Bienvenido al servidor FTP Debian 5"
#
```

```
#Local FTP user Settings
#-----------------------
local_enable=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd.chroot_list
#
#Anonymus FTP user Settings
#-------------------------
anonymous_enable=YES
anon_world_readable_only=YES
anon_max_rate=7200
#
#Transfer Settings
-----------------
connect_from_port_20=YES
data_connection_timeout=300
#
#Modo standalone
#--------------
listen=YES
#
#Nombre del servicio PAM para autenticacion con vsftpd
#-----------------------------------------------------
pam_service_name=vsftpd
```

En el fichero */etc/vsftpd.chroot_list* añadiríamos los siguientes usuarios:

```
#
#Fichero de configuración vsftpd.chroot_list
#
#Usuarios restringidos a su directorio personal
#---------------------------------------
josemanuel
marian
```

Iniciamos el demonio *vsftpd*:

```
/etc/init.d/vsftpd start
```

EJEMPLO 4.5

El mismo supuesto del ejemplo 4.4 mediante SSL, incluiría en el fichero de configuración */etc/vsftpd.conf* las opciones adicionales que en este ejemplo se muestran en la sección de ajustes avanzados. Se ha supuesto que el certificado se encuentra en */etc/ssl/certificado* y se denomina *cert_vsftpd.pem*:

```
#Modo standalone y configuracion para TSL/SSL
#--------------------------------------------
listen=YES
#Habilitar TLS/SSL
ssl_enable=YES
#Permitir la utilización de TLS/SSL a usuarios anónimos
allow_anon_ssl=YES
#Obligar a utilizar TLS/SSL en todas las operaciones
force_local_data_ssl=YES
force_local_logins_ssl=YES
#Indicar la preferencia de SSLv2 sobre SSLv3
ssl_sslv2=YES
ssl_sslv3=NO
#Ruta al certificado
rsa_cert_file=/etc/ssl/certificado/cert_vsftpd.pem
```

4.4 CONFIGURACIÓN DE UN CLIENTE

Los usuarios del servicio FTP disponen de varias posibilidades para el acceso y posterior transferencia de ficheros entre su ordenador y un servidor remoto. En este apartado se tratan tres formas diferentes de hacerlo: mediante línea de órdenes, mediante un navegador o bien mediante programas específicos.

Previo a la utilización de un cliente FTP, es necesario asegurarse de tener configurada correctamente la red TCP/IP para que, a través de nuestro interfaz de red o módem, se disponga de acceso a distintos servidores de Internet. Si el equipo pertenece a una organización que dispone de proxy, debe configurar el equipo correctamente para indicar el dispositivo que ejerce de proxy.

4.4.1 ACCESO MEDIANTE LÍNEA DE ÓRDENES

En sistemas operativos Windows, simplemente se ha de utilizar el programa denominado "Símbolo del sistema", accesible desde "Inicio | | Accesorios | | Símbolo del sistema" o bien ejecute ("Inicio | | Ejecutar") *cmd.exe*.

En sistemas operativos GNU/Linux, para utilizar la línea de órdenes se puede abrir una consola de terminal en cualquier distribución. En un entorno KDE, por ejemplo es accesible mediante "Lanzador de Aplicaciones | | Aplicaciones | | Sistema", mientras que en GNOME es accesible mediante "Aplicaciones | | Herramientas del sistema". También puede utilizar los Terminales Virtuales (Alt + Tecla de Función).

Desde cualquiera de las consolas citada anteriormente, podrá conectarse al servidor mediante la orden genérica *ftp <Servidor>[/<Directorio>]*. Podrá realizar también diversas operaciones sobre la jerarquía de directorios del sitio FTP, como por ejemplo descarga de ficheros (véase ejemplo 4.6). Gran parte de estas órdenes las encuentra resumidas en las tablas 4.4 a 4.9.

Tabla 4.4. Órdenes para iniciar o terminar una sesión FTP

Orden	Utilidad
BYE	Termina la sesión FTP y sale del programa.
CLOSE	Termina la sesión FTP, pero no sale del programa.
DISCONNECT	Termina la sesión FTP, pero no sale del programa.
OPEN *<servidor>*	Inicia una sesión FTP con un servidor remoto, especificado por su dirección IP o nombre DNS.
PASSIVE	Activa o desactiva el modo pasivo para la transferencia de fichero.
QUIT	Termina la sesión FTP y sale del programa.
USER *<nombre>*	Inicia una sesión FTP con el nombre de usuario indicado.

Tabla 4.5. Órdenes para manejo de archivos en FTP

Orden	Utilidad
APPEND <*arch1*> <*arch2*>	Anexa el contenido del archivo <*arch1*> de la estación local al archivo <*arch2*> que se encuentra en el servidor FTP.
DELETE <*archivo*>	Elimina el archivo situado en el servidor remoto.
GET <*arch1*> <*arch2*>	Copia el archivo <*arch1*> que está situado en el servidor remoto a la estación local con el nombre <*arch2*>.
PUT <*arch1*> <*arch2*>	Copia el archivo <*arch1*> de la estación local al servidor remoto con el nombre <*arch2*>.
RECV <*arch1*> <*arch2*>	Copia el archivo <*arch1*> del servidor remoto a la estación local con el nombre <*arch2*>.
RENAME <*arch1*> <*arch2*>	Cambia el nombre del archivo <*arch1*> situado en el servidor remoto por <*arch2*>.
SEND <*arch1*> <*arch2*>	Copia el archivo <*arch1*> de la estación local al servidor remoto con el nombre <*arch2*>.

Tabla 4.6. Órdenes para manejo de múltiples archivos en FTP

Orden	Utilidad
MDELETE <*archiv*>	Elimina los archivos especificados en el servidor remoto.
MGET <*archivos*>	Copia los archivos desde el servidor FTP a la estación local.
MPUT <*archivos*>	Copia los archivos desde el cliente al servidor remoto.

Tabla 4.7. Órdenes para manejo de carpetas en FTP

Orden	Utilidad
CD <*carpeta*>	Cambia la carpeta actual del servidor remoto.
DIR <*ruta*>	Muestra el contenido de la carpeta actual o la ruta especificada en el servidor remoto.
LCD <*carpeta*>	Cambia la carpeta actual del equipo local.
LS <*ruta*>	Muestra el contenido de la carpeta actual o la ruta especificada en el servidor remoto.
MDIR <*ruta*>	Muestra el contenido de la carpeta actual o la ruta especificada en el servidor remoto. Admite caracteres comodín.
MKDIR <*carpeta*>	Crea la carpeta indicada en el servidor remoto.
MLS <*ruta*>	Muestra el contenido resumido de la carpeta actual o de la ruta especificada en el servidor remoto.
PWD	Muestra la carpeta actual en el servidor remoto.
RMDIR <*carp*>	Elimina la carpeta especificada en el servidor remoto.

Tabla 4.8. Órdenes para cambiar el estado de la conexión FTP

Orden	Utilidad
ASCII	Indica que los archivos a transferir son de texto ASCII.
BELL	Activa o desactiva la opción para que se emita un sonido cada vez que la orden introducida se complete.
BINARY	Indica que los archivos a transferir son binarios.
DEBUG	Activa o desactiva el modo de depuración.
GLOB	Activa o desactiva el uso de comodines (? y *) para especificar nombres de archivos.
HASH	Activa o desactiva la aparición del signo # por cada bloque de información transferido.
PROMPT	Activa o desactiva la aparición de mensajes de confirmación cuando se completan las órdenes.
STATUS	Muestra el estado actual de la sesión FTP.
TRACE	Activa o desactiva la inspección de paquetes enviados.
TYPE <*tipo*>	Establece el tipo de archivos que se enviarán: ascii o binary.
VERBOSE	Activa o desactiva la visualización de todas las respuestas.

Tabla 4.9. Otras órdenes utilizadas en FTP

Orden	Utilidad
! <*orden*>	Ejecuta la orden del DOS indicado en la máquina local.
? <*orden*>	Muestra la ayuda de una orden.
HELP <*orden*>	Muestra la ayuda de las órdenes.
REMOTEHELP <*orden*>	Muestra la ayuda de la orden especificada y enviada por el servidor remoto.



EJEMPLO 4.6

El usuario Fistrinauer desde lu equipo Linux, desea acceder como usuario *marian* al servidor local de su empresa cuya dirección IP es la-192.168.1.5. Desea obtener todos los ficheros en pdf y dejar el documento *CartaSociosElectos.doc*. Percibiéndose de un error en el nombre del fichero que ha dejado en el servidor, decide renombrarlo como *CartaSociosHonorarios.doc*.

Suponiendo que ya estamos en una consola de órdenes, ejecutaríamos las siguientes órdenes para conectarnos al servidor:

```
[Fistrinauer@Linux ~]$ ftp
ftp> open 192.168.1.5
Connected to 192.168.1.5 (192.168.1.5).
220 "Bienvenido al servidor FTP Fedora 11.1"
```

Accedemos al servidor con el usuario y su contraseña:

```
Name (192.168.1.5:Eduardo): marian
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Utilizamos la orden *help* para obtener las órdenes disponibles:

```
ftp> help
Commands may be abbreviated.  Commands are:

!          debug          mdir       sendport   site
$          dir            mget       put        size
account    disconnect     mkdir      pwd        status
append     exit           mls        quit       struct
ascii      form           mode       quote      system
bell       get            modtime    recv       sunique
binary     glob           mput       reget      tenex
bye        hash           newer      rstatus    tick
case       help           nmap       rhelp      trace
cd         idle           nlist      rename     type
cdup       image          ntrans     reset      user
chmod      lcd            open       restart    umask
close      ls             prompt     rmdir      verbose
cr         macdef         passive    runique    ?
delete     mdelete        proxy      send
```

Activamos el modo pasivo de transferencia:

```
ftp> passive
Passive mode on.
```

Listamos la información disponible en el servidor remoto:

```
ftp> dir
227 Entering Passive Mode (192,168,1,5,249,47).
150 Here comes the directory listing.
drwxrwxr-x    2 501      501          4096 Oct 31 17:09 bin
drwxrwxr-x    2 501      501          4096 Oct 31 17:16 doc
226 Directory send OK.
```

Cambiamos al subdirectorio remoto *doc*:

```
ftp> cd doc
250 Directory successfully changed.
```

Listamos su contenido:

```
ftp> ls
227 Entering Passive Mode (192,168,1,5,240,235).
150 Here comes the directory listing.
-rw-rw-r--    1 501      501           29 Oct 31 17:16 CartaJuntaAccionistas.doc
-rw-rw-r--    1 501      501           56 Oct 31 17:16 InformeEconomico_2009.pdf
-rw-rw-r--    1 501      501           27 Oct 31 17:11 InformeVentas_2009.pdf
226 Directory send OK.
```

Obtenemos todos los ficheros con extensión *pdf* confirmando su copia al equipo local:

```
ftp> mget *.pdf
mget InformeEconomico_2009.pdf? y
227 Entering Passive Mode (192,168,1,5,149,218).
150 Opening BINARY mode data connection for InformeEconomico_2009.pdf (56 bytes).
226 File send OK.
56 bytes received in 0,000133 secs (421,05 Kbytes/sec)
mget InformeVentas_2009.pdf? y
227 Entering Passive Mode (192,168,1,5,39,128).
150 Opening BINARY mode data connection for InformeVentas_2009.pdf (27 bytes).
226 File send OK.
27 bytes received in 0,000151 secs (178,81 Kbytes/sec)
```

Dejamos el fichero local *CartaSociosElectos.doc* en el servidor remoto:

```
ftp> put CartaSociosElectos.doc CartaSociosElectos.doc
local: CartaSociosElectos.doc remote: CartaSociosElectos.doc
227 Entering Passive Mode (192,168,1,5,204,163).
150 Ok to send data.
226 File receive OK.
32 bytes sent in 0,000161 secs (198,76 Kbytes/sec)
```

Renombramos el fichero del servidor remoto *CartaSociosElectos.doc* por *CartaSociosHonorarios.doc*:

```
ftp> rename CartaSociosElectos.doc CartaSociosHonorarios.doc
350 Ready for RNTO.
250 Rename successful.
```

Cerramos sesión como usuario *marian*:

```
ftp> close
221 Goodbye.
```

Salimos de la orden *ftp*:

```
ftp> quit
```

4.4.2 ACCESO MEDIANTE NAVEGADOR

Tan solo necesitará la utilización de cualquiera de los que disponga en su sistema operativo, como Internet Explorer, Mozilla FireFox, Opera o Chrome en sistemas operativos Windows, o Mozilla Firefox, Konkeror, Nautilus o Epiphany en el caso de distribuciones GNU/Linux.

El procedimiento para acceder al servidor FTP consiste en indicar en la barra de dirección la URL del recurso al que desea acceder. No siempre el navegador responde de la manera esperada y requiere la instalación de algún complemento para un mejor acceso al servicio, como es el caso de "FireFTP" para Mozilla Firefox, permitiéndonos establecer algunos parámetros en las opciones de este complemento, así como una cómoda navegación mediante una ventana dividida en dos partes, el sitio remoto y el local. A modo de ejemplo, supongamos que quiere conectarse al servidor FTP de SuSE, en la barra de dirección debería indicar como URL: *ftp://ftp.suse.com* para obtener el resultado que se muestra en la Figura 4.7.

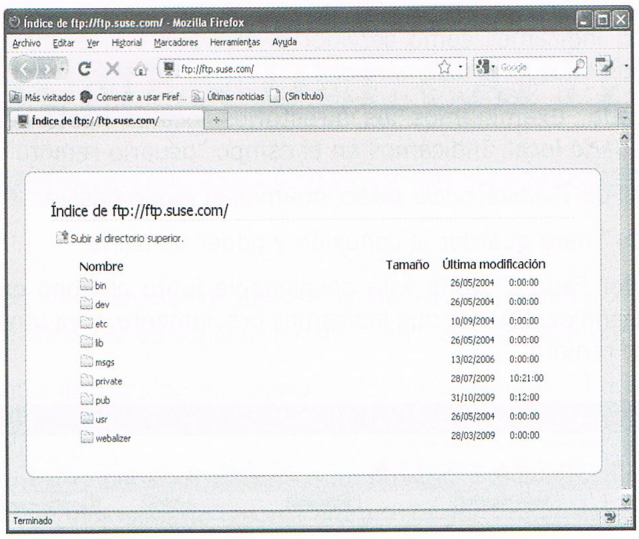


Figura 4.7. Ejemplo del navegador Mozilla Firefox como cliente FTP. La mayoría de navegadores son capaces de actuar como cliente FTP indicando en la barra de dirección la URL del servidor remoto y opcionalmente el recurso al que se quiere acceder

4.4.3 ACCESO MEDIANTE PROGRAMAS ESPECÍFICOS

En el mercado existe una amplia variedad de software para llevar a cabo la transferencia de ficheros. Podemos destacar, entre otros, CuteFTP, FileZilla o WinSCP en el caso de Windows y FileZilla o gFtp en distribuciones GNU/Linux. El acceso y las operaciones a realizar, dependerán de la interfaz del programa, siendo habitual la utilización de barras de herramientas, menús y ventanas que muestran la jerarquía de directorios del cliente y servidor por separado, facilitando al usuario su trabajo. A la hora de su elección, tenga en cuenta la documentación aportada por su fabricante para comprobar si cubre los aspectos que le interesen, como por ejemplo el soporte para SSL o TSL, modo activo y pasivo o la gestión de varios sitios. En el ejemplo 4.5 puede observar la utilización del programa Filezilla, muy completo en cuanto a sus posibilidades de configuración.



EJEMPLO 4.7

Deseamos acceder desde nuestro equipo al servidor Fedora con IP 192.168.1.5 del ejemplo 4.4 mediante la aplicación FileZilla, instalada recientemente en nuestro equipo y que nos facilitará la labor de envío y recepción de ficheros con el servidor. Nos han indicado que han creado una cuenta para nosotros cuyo nombre es *josemanuel* y su contraseña es la misma que la del equipo local. Nos han sugerido que utilicemos un modo pasivo de transferencia, que guardemos dicha conexión como "Servidor Fedora" ya que la utilizaremos en futuras ocasiones y que predeterminemos como directorio local "Mis documentos" y como directorio remoto "informes". Además, se aconseja que siempre nos pregunte la contraseña antes de efectuar la conexión.

Suponiendo que tenemos instalado un sistema operativo Windows XP, ejecutamos FileZilla seleccionando "Inicio || Programas || Filezilla FTP Client || Filezilla".

Para guardar el acceso al servidor remoto para futuras conexiones, accedemos a "Archivo || Gestión de sitios" y pulsamos sobre el botón "Nuevo sitio", escribiendo un nombre significativo, como el que nos han indicado, "Servidor Fedora".

En la pestaña *General*, indicamos como servidor el 192.168.1.5, el modo de acceso "Preguntar la contraseña" e indicamos el usuario *josemanuel*.

En la pestaña *Avanzado*, examinamos los directorios locales hasta seleccionar la carpeta "Mis documentos" de mi usuario local. Indicamos en el campo "usuario remoto" el directorio "/informes".

En la pestaña *Opciones de Transferencia* seleccionamos el modo pasivo.

Seleccionamos "Aceptar" para guardar la conexión y poder utilizarla.

Seleccionamos "Servidor Fedora" de la lista desplegable junto al icono que representa un servidor, introducimos la contraseña del usuario que indicamos previamente, y ya tendremos acceso al directorio "informes" del servidor remoto.

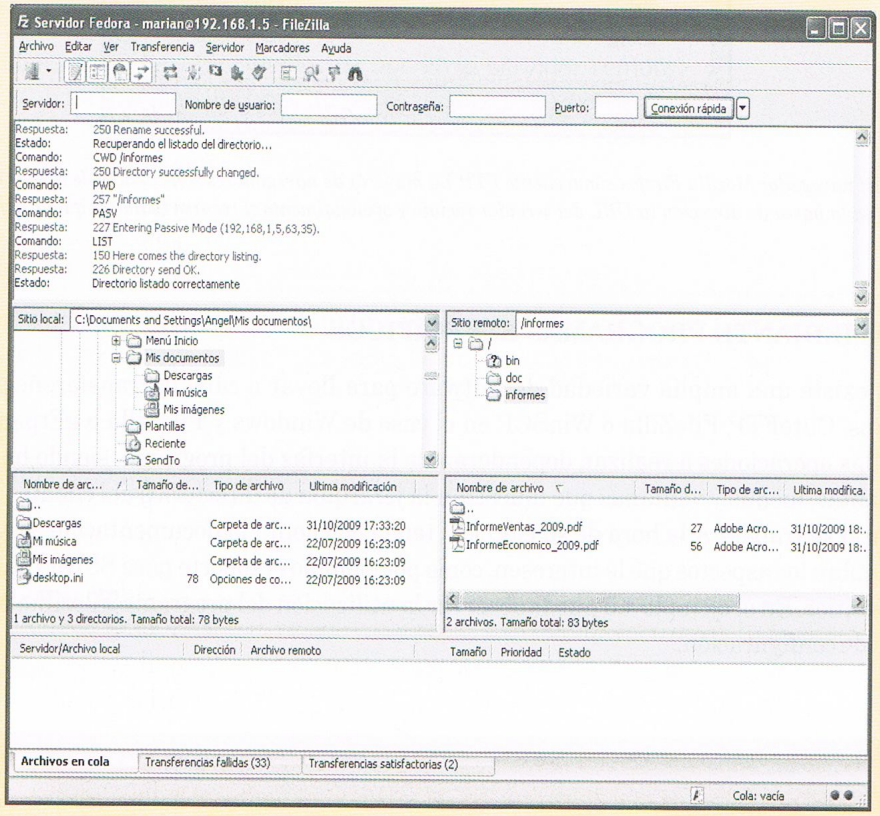


Figura 4.8. *Cliente FTP Filezilla. Ejemplo de acceso un servidor FTP (192.168.1.5), mostrándonos la jerarquía local y la del sitio remoto mediante este sencillo e intuitivo software de libre distribución*

RESUMEN DEL CAPÍTULO

El servicio FTP permite la utilización de un sistema de ficheros remotos como si fuera local mediante el protocolo FTP, el cual utiliza una conexión de control y otra para transferencia de los datos.

El cliente puede acceder al servidor sin negociar el puerto de datos al que acceder para realizar la transferencia de información (modo activo), o bien negociarlo con el servidor (modo pasivo).

Los archivos y directorios remotos se ubican en un directorio denominado sitio FTP, lugar donde se ponen a disposición de cualquier usuario (acceso público), o para unos determinados usuarios (acceso privado).

Al ser un servicio no seguro, suele utilizarse para la lectura de información, empleándose otros servicios de acceso remoto como SSH para obtener mayor seguridad, o utilizando FTP mediante el establecimiento de conexiones SSL o TSL de forma explícita o implícita.

El protocolo TFTP, variante del protocolo FTP, prescinde de la conexión de control. Es utilizado para instalaciones o arranque de un sistema operativo mediante red, requiriéndose protocolos adicionales mediante discos de arranque o tarjetas con soporte PXE.

La configuración del servicio requiere como mínimo establecer el directorio del servidor que ejercerá como raíz del sitio. Adicionalmente se pueden modificar los parámetros por defecto como el puerto de escucha, o indicar otros parámetros como la restricción a los usuarios a un directorio particular.

La instalación de este servicio en Windows requiere la instalación del *Administrador de Servicios de Internet* y el *Servicio* FTP de la utilidad IIS. La configuración en versiones Server respecto a versiones cliente como 7 y Vista, difieren tanto en su aspecto como en las posibilidades de configuración. Un parámetro interesante es la creación de sitios virtuales utilizando directorios remotos.

La instalación de este servicio en Linux requiere la instalación del paquete *vsftpd*. Su configuración se basa principalmente en la adecuación de los parámetros del fichero de configuración *vsftpd.conf*, donde se determina la ubicación del sitio FTP, el tipo de acceso que se permite (público o privado) y se indica si se restringe el acceso a los usuarios a su directorio personal.

El acceso al servicio por un equipo cliente en sistemas operativos Windows y Linux requiere especificar, al menos, el servidor al que se quiere acceder. Adicionalmente se pueden establecer otros parámetros como el modo de transferencia, el tipo de autenticación, o el tipo de ficheros a transferir.

El cliente tiene tres formas de acceder al servicio:

- Mediante órdenes.
- Navegadores, aunque dependiendo del navegador puede necesitar de la instalación de algún complemento para utilizar el protocolo FTP.
- Programas específicos como FileZilla.

EJERCICIOS PROPUESTOS

Para la realización de los ejercicios se partirá de la Figura 4.9, que se muestra a continuación. Tenga en cuenta que se han omitido routers, módems u otros dispositivos para conexión a Internet.

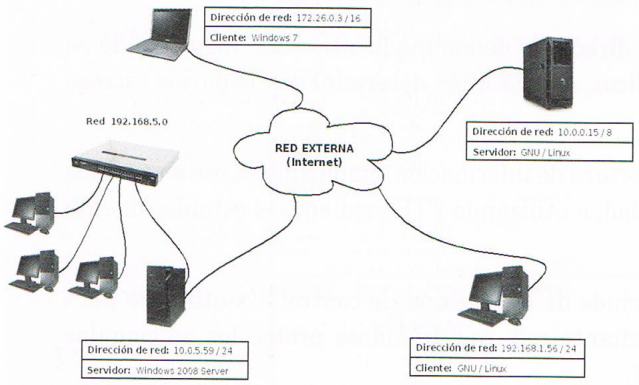


Figura 4.9. *Varios equipos y redes locales conectadas a Internet*

- **1.** Configure un servicio FTP en Windows para proporcionar el servicio FTP de solo lectura para usuarios de tipo público. El directorio raíz del sitio estará ubicado en *C:\ftp*.
- **2.** Configure dos sitios distintos FTP en un equipo con sistema operativo Windows. Si intenta tener los dos sitios disponibles para los clientes, ¿qué sucede?
- **3.** Configure el ejemplo 4.1 en un sistema operativo Windows 7 y añada un directorio virtual para acceder al sitio del ejercicio 1 suponiendo que el servidor se denomina *ftp.denos.com*.
- **4.** Configure un servidor GNU/Linux para proporcionar el servicio FTP que se iniciará en modo no *standalone*. Únicamente se tendrá acceso al directorio personal del usuario *privado* y se permitirá la escritura en el sitio FTP.
- **5.** Configure el servidor del ejercicio 3 para utilizar una conexión segura mediante SSL.
- **6.** Realice la configuración del ejercicio 5 mediante la herramienta *YaST2* en una distribución OpenSuSE pero únicamente para permitir conexiones pasivas.
- **7.** Indique cómo se podría configurar un servidor GNU/Linux para utilizar el sitio FTP de otro servidor, similar a como lo hace Windows con los directorios virtuales.
- **8.** Configure el cliente con el programa Filezilla instalado para la utilización de la conexión segura del ejercicio 5 suponiendo que se denomina *ftp.chimichami.com*, así como la conexión al sitio del ejercicio 1, suponiendo que se denomina *ftp.denos.com*.
- **9.** Utilice una consola de órdenes para obtener el fichero *PresupuestoA&F.xls* del directorio *presupuestos* del usuario *josemanuel* del ejemplo 4.1 y dejarlo en el sitio del usuario del ejercicio 4.
- **10.** Configure el navegador Mozilla Firefox con su complemento *FireFTP* para conectarnos a los mismos sitios indicados en el ejercicio 7.

TEST DE CONOCIMIENTOS

1 En un servidor, los protocolos FTP y TFTP:
- a) Ambos utilizan el mismo puerto de conexión de control.
- b) Utilizan distinto modo de transferencia.
- c) Ambos emplean la conexión de datos.
- d) Ambos utilizan el mismo puerto de conexión de datos.

2 Un servidor configurado en modo pasivo y un servidor TFTP:
- a) Utilizan el mismo puerto para la conexión de datos.
- b) Utilizan distinto puerto para la conexión de datos.
- c) Utilizan el mismo puerto para la conexión de control.
- d) Utilizan distinto puerto para la conexión de control.

3 Un cliente FTP al recibir la información:
- a) Utiliza los mismos puertos que el servidor.
- b) Negocia los puertos para que sean los mismos que el servidor.
- c) No requiere la utilización de puertos.
- d) Utiliza sus propios puertos.

4 El modo activo respecto al modo pasivo:
- e) Es menos seguro ya que obliga al cliente a escuchar todo lo que le viene del puerto 20 del servidor.
- f) Es igual de seguro ya que el servicio FTP es un servicio no seguro.
- g) Es más seguro porque el cliente sabe el puerto del servidor del que recibirá la información.
- h) Es más seguro porque el cliente utiliza un puerto distinto al del servidor.

5 En un servidor Windows al realizar aislamiento de usuarios:
- a) Cada usuario solo tendrá acceso a su directorio dentro del sitio.
- b) Requiere que la función Active Directory esté instalada junto con los usuarios.
- c) Los usuarios acceden a su directorio y al de otros usuarios.
- d) Los usuarios solo tienen acceso a su carpeta "Mis documentos".

6 En un servidor GNU/Linux con *vsftpd* instalado y activo, con permiso de acceso a usuarios locales y con las opciones *chroot_local_user* y *chroot_list_enable* activas:
- a) Los usuarios locales solo tienen acceso a su directorio personal.
- b) Los usuarios locales solo tienen acceso si están en *chroot_list_file*.
- c) Los usuarios locales que no estén en *chroot_list_file* tienen acceso al sitio de los demás.
- d) Ninguna de las anteriores.

7 En un servidor GNU/Linux, el modo *standalone* del demonio *vsftpd* significa:
- a) Que el demonio *vsftpd* se hace cargo de las peticiones FTP de los clientes.
- b) Puede ejecutarse junto con el demonio *xinetd*.
- c) No puede ejecutarse a la vez que el demonio *xinetd*.
- d) a y b son ciertas.

8 La ejecución de la orden *ftp 192.168.0.9/public*:
- a) Nos permite el acceso al servidor 192.168.0.9 desde el directorio local public.
- b) No haría nada ya que no se permite dicho formato de orden.
- c) Es lo mismo que ejecutar la orden *cd public*, más la orden *ftp* y la orden *open 192.168.1.9*.
- d) Es lo mismo que ejecutar la orden *ftp*, más la orden *open 192.168.0.9* y la orden *cd public*.

9 Al configurar un sitio remoto al que queremos acceder con Filezilla:
- a) Podemos establecer la carpeta por defecto del sitio remoto.
- b) Tenemos siempre que indicar el servidor al que queremos acceder.
- c) Siempre nos preguntará al menos la contraseña.
- d) Todas son verdaderas.

5 Terminal remoto

OBJETIVOS DEL CAPÍTULO

- ✓ Describir el funcionamiento general del servicio de acceso remoto.
- ✓ Describir los distintos modos de acceso remoto.
- ✓ Introducir a la utilización de herramientas, órdenes y protocolos para acceso remoto.
- ✓ Aprender a establecer conexiones sobre un sistema remoto para desempeñar tareas administrativas.

Habitualmente, los usuarios desarrollan su labor interaccionando con su equipo local pero, cuando este equipo forma parte de una red, a veces se requieren diversas tareas que exigen el acceso a otro equipo distante. Por ejemplo, un usuario podría acceder a un equipo remoto para utilizar un recurso cuya adquisición le supone un elevado coste económico (aplicación informática), bien para ejecutar aplicaciones muy exigentes en requerimientos hardware de los que su equipo carece o, simplemente, realizar tareas de administración sobre él.

El servicio de terminal remoto, permite al usuario acceder desde su equipo local a otro remoto, salvar la distancia geográfica que los separa y evitar su desplazamiento, dándole la impresión de estar situado frente al equipo distante. Independientemente de la forma de interacción que permita el servidor y utilice el cliente, el usuario que accede desde el cliente, previamente ha de autenticarse, aunque encontramos excepciones. Para conseguir esta interacción entre equipos remotos, se utiliza un protocolo de entre los varios existentes y que proporcionan este servicio, cada uno con características que le diferencian del resto, aunque de similar funcionamiento. El protocolo escogido dependerá de la utilidad que le queramos dar.

Dadas las diferentes formas de acceso remoto a un equipo, este capítulo trata de cubrir un amplio abanico de todas ellas. Este servicio se enfoca principalmente desde la perspectiva de la administración remota.

5.1 FUNCIONAMIENTO DEL SERVICIO

En este apartado se exponen, uno por uno, los protocolos más utilizados para proporcionar este servicio, aunque primero conozcamos de forma general las formas de interacción entre equipos distantes de un entorno cliente-servidor:

- **Mediate orden**: el cliente tras autenticarse en el servidor, recibe en su terminal una consola como si estuviera delante del servidor, en la que tecleará las órdenes a ejecutar. Estos son enviados al servidor remoto, donde se procesan, y cuyo resultado se remite al cliente (véase Figura 5.1).
- **Mediante interfaz gráfico**: el cliente accede al servidor remoto como si estuviera delante de él para iniciar una sesión gráfica. El cliente se autentica mediante una ventana inicial que recibe del servidor. Posteriormente, obtiene su escritorio, con el que podrá interactuar utilizando su teclado y ratón. El servidor remoto procesa las interacciones efectuadas por el cliente, cuyos efectos, se hacen visibles en su terminal.

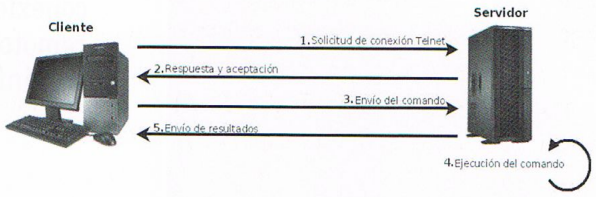


Figura 5.1. *Ejemplo de Terminal Remoto mediante Telnet. El cliente solicita a servidor la conexión Telnet, tras ser aceptada, envía una orden al servidor para su ejecución, cuyos resultados son remitidos al cliente*

5.1.1 TELNET (*TELEMATICS NETWORK*)

Telnet es un servicio proporcionado por el protocolo que lleva su mismo nombre, Telnet, el cual establece una conexión TCP entre los equipos remotos. La flexibilidad de este protocolo no solo permite un acceso remoto a un servidor, sino que se utiliza como soporte de otros servicios (FTP o HTTP). Este servicio es soportado por sistemas operativos Microsoft Windows y GNU/Linux.

El servicio Telnet atiende el establecimiento de sesiones y solicitudes de clientes a través del puerto 23. Previo al inicio de una sesión del cliente con el servidor, se suele efectuar un intercambio de parámetros adicionales como, por el ejemplo, el tipo de terminal utilizado por el cliente. Posteriormente, se requiere el ingreso de un nombre de usuario y una contraseña para el inicio de sesión. Tras comprobar su validez en el servidor, queda establecida la conexión entre cliente y servidor.

Una vez iniciada la sesión, el servidor recibe las pulsaciones emitidas por el cliente, el servidor las reenvía y se muestran al cliente (*eco*). El servidor interpreta esas pulsaciones (por ejemplo, la ejecución de una orden) y devuelve su resultado visible para el cliente.

La interacción con el servidor se puede efectuar mediante la orden *telnet* (habitual en sistemas Linux) o bien utilizar programas **emulador de terminal**, que simulan al cliente la utilización del terminal (teclado, pantalla y dispositivo de comunicación) del servidor.

Este es un servicio inseguro, ya que la autenticación de los usuarios se transmite por la red sin encriptar pudiendo ser interceptada. Además, este servicio incrementa el tráfico de la red debido al reenvío de pulsaciones o *eco*.

5.1.2 RLOGIN (*REMOTE LOGIN*)

Su funcionamiento es similar a Telnet con la salvedad de que los usuarios no tienen que introducir una contraseña para autenticarse antes de iniciar la sesión. Esta característica impide que las contraseñas sean capturadas por otros usuarios en la red. Este tipo de conexión es utilizada en sistemas Linux, cuyo puerto utilizado por defecto es el 513.

5.1.3 SSH (*SECURE SHELL*)

Al igual que Telnet, este servicio es soportado por el protocolo que lleva su nombre, SSH. El funcionamiento de dicho servicio es parecido a Telnet aunque incluye mejoras importantes en cuanto a seguridad, funciones adicionales como la copia y transferencia de archivos, así como la posibilidad de ejecución de aplicaciones en el entorno gráfico del servidor (X-Window). Además, otros servicios menos seguros como POP, Telnet, VNC, FTP o el sistema gestor de bases de datos MySQL, se pueden beneficiar de SSH estableciendo un *túnel seguro*, asegurando la utilización de estos servicios.

El servicio SSH atiende el establecimiento de sesiones y solicitudes de clientes a través del puerto 22. También requiere que el usuario se autentique en el servidor aunque, a diferencia de Telnet, tanto el nombre de usuario como su contraseña, viajan cifrados por las redes intermedias que separan al cliente del servidor. Una vez iniciada la sesión, la información intercambiada entre ambos circula encriptada. SSH utiliza mecanismos de clave pública y privada para el cifrado de información, basados en algoritmos RSA (versión 1) y DSA (versión 2).

RSA son las siglas de los apellidos de sus autores Rivest, Shamir y Adleman.

La forma de interacción del cliente con el servidor, puede realizarse mediante las órdenes (*ssh*, *scp* o *sftp*) o como Telnet, mediante emuladores de terminales. Gracias a la implementación que OpenSSH hace de SSH, se puede utilizar de forma abierta y gratuita en sistemas operativos Microsoft Windows y GNU/Linux.

5.1.4 X-TERMINAL

Este servicio se proporciona entre equipos GNU/Linux gracias al protocolo XDMCP (*X Display Manager Control Protocol* o Protocolo de Control de Administrador de la Pantalla X), que utiliza los puertos 177 (UDP) y el 6000 + N (TCP), siendo N el número de display. Para entender este servicio, necesitamos conocer sus modos de funcionamiento:

- **Sesión X Window remota**: permite a un equipo GNU/Linux iniciar una sesión gráfica en un equipo remoto desde su máquina local, visualizando la pantalla de inicio de sesión remota. Una vez iniciada la sesión, el cliente tiene acceso al escritorio y aplicaciones del equipo remoto.
- **Aplicaciones X Window remotas**: permite a un servidor GNU/Linux poner a disposición de un equipo cliente sus recursos hardware, de manera que pueda ejecutar aplicaciones gráficas. El servidor utiliza su gestor de pantalla o *X Display Manager* (por ejemplo *gdm* en entornos GNOME) para facilitar sus aplicaciones al cliente. El cliente ejecuta un *servidor X*, cuya función es la de proporcionarle un terminal, es decir, pantalla, teclado y ratón, para visualizar e interactuar con las aplicaciones remotas del servidor.

5.1.5 ESCRITORIO REMOTO VNC

El servicio de escritorio remoto permite controlar en modo gráfico otro equipo tanto de una red local como de otra externa, como Internet. El usuario tiene la impresión de estar sentado delante del equipo remoto, suponiéndole grandes ventajas. Para su utilización, se requiere la instalación de este servicio en el equipo que vaya a ser controlado de forma remota (normalmente un servidor), y software cliente que suele ser de fácil manejo y de bajo consumo en recursos, en el equipo local. Algunos de los protocolos más utilizados para proporcionar el servicio de escritorio remoto son RDP (véase siguiente apartado) y VNC (*Virtual Network Computing* o Computación en Red Virtual).

El protocolo VNC, permite establecer varias sesiones con el equipo remoto y no requiere sistemas operativos similares en los equipos local y distante. El servidor VNC atiende las peticiones por el puerto 5900, aunque también se suele utilizar el puerto 5800 para accesos vía web mediante navegador. El software servidor requiere establecer una contraseña que los clientes deberán conocer e indicar en cada uno de sus accesos. Para establecer varias sesiones con el servidor, cada cliente debe indicar el número de terminal y puede configurar diversos parámetros, como los referentes a la transmisión y a las características del escritorio. VNC es software con licencia GNU/GPL, existiendo versiones para distintas plataformas, entre ellas GNU/Linux y Microsoft Windows.

5.1.6 TERMINAL SERVER

Es software que las versiones de servidor Windows 2000 Server, 2003 Server y 2008 Server incluyen (en NT se distribuía de forma separada), y que admite, dos modos de funcionamiento:

- **Modo de administración remota**: permite a los clientes mediante la utilización de software ligero, iniciar sesiones en modo gráfico a modo de emulador de terminal, tomando el control del escritorio del servidor remoto para su administración. Los recursos del servidor (procesador, memoria, disco duro, etc.) se ponen a disposición de los clientes para ejecutar los terminales gráficos. El servidor envía cada interfaz de usuario al cliente correspondiente para que interactúe con su teclado y ratón, cuyas pulsaciones son procesadas por el servidor. Este servicio utiliza el protocolo RDP (*Remote Desktop Protocol* o Protocolo de Escritorio Remoto), permitiendo a equipos con Windows XP, 2003, Vista, 7 y 2008 instalado, el control de un escritorio remoto. Estos sistemas operativos incorporan tanto el software cliente como servidor. Además, en el CD de instalación algunos de estos sistemas operativos incorporan una herramienta para conexión a escritorio remoto desde sistemas operativos

Windows 95, 98, NT 4.0 y 2000. En Windows 2000 Server, este software necesario se incluye con Terminal Server. El puerto utilizado por este servicio para aceptar las conexiones remotas es el 3389. En Windows 2003 y 2008 Server, el software para este modo se instala de forma predeterminada, denominándose *Escritorio Remoto para Administración*. Aunque Microsoft suministra el software cliente para sus sistemas operativos Windows, otras plataformas como GNU/Linux también disponen de software cliente.

- **Modo de servidor de aplicaciones**: permite al cliente ejecutar aplicaciones instaladas en el servidor. Las aplicaciones a utilizar con *Terminal Server* deben instalarse posteriormente a este servicio. Recomendable cuando los requerimientos hardware del cliente sean insuficientes para la ejecución de aplicaciones.

Windows 2003 Server y 2008 Server incorporan software separado para cada uno de estos modos. Sin embargo, Windows 2000 Server utiliza el mismo software para habilitar ambos modos de funcionamiento.

5.1.7 ACCESO REMOTO MEDIANTE INTERFAZ WEB

- **Escritorio remoto VNC**: el servicio VNC además de utilizar un puerto determinado para atender sus peticiones, permite habilitar el puerto 5800 para que mediante un navegador web, un cliente pueda acceder a este servicio.
- **Escritorio remoto RDP (Windows XP, 2003 y 2008)**: Microsoft Windows XP Professional, 2003 Server y 2008 Server, brindan a equipos clientes la posibilidad de acceder mediante acceso web a otro equipo remoto. Para ofrecer dicho servicio, se requiere que el servicio HTTP esté instalado y activo mediante IIS (véase capítulo 3 para mas información), ya que se utiliza uno de los componentes de IIS para proporcionar este servicio. Tras su instalación, el sistema operativo crea en el sitio web por defecto la carpeta *tsweb* (XP y 2003) o *ts* (2008), con las páginas necesarias y un control *ActiveX* disponible para los navegadores de los clientes que deseen utilizar este servicio.
- **Administración remota (Windows 2003)**: Windows 2003 Server también admite la instalación de un componente de IIS denominado *Administración remota (HTML)*, que permite administrar mediante el navegador web de un cliente, un servidor con este sistema operativo instalado, permitiendo configurar desde las interfaces de red, usuarios y grupos de usuarios, hasta el propio servicio HTTP o FTP. La instalación de este servicio consiste en la creación de un nuevo sitio web (Administración), donde se ubican una serie de páginas y carpetas necesarias para su administración remota mediante web. Este nuevo sitio por defecto se configura para atender conexiones seguras cliente mediante la utilización de SSL a través del puerto 8098. En la versión Web Server de este sistema operativo, esta herramienta aparece por defecto instalada. Su principal utilidad es la de administrar un servidor web IIS Windows 2003 Server.
- **Dispositivos de red**: otra de sus áreas de aplicación en la que ha tenido un gran auge, es la configuración de dispositivos de red tales como switches, routers, puntos de acceso, etc., presentándose como una alternativa más amigable que la utilización de órdenes, ya que no es necesario conocer cada una de las órdenes ni su sintáxis.

5.2 CONFIGURACIÓN DEL SERVICIO DE ACCESO REMOTO

5.2.1 CONFIGURACIÓN EN MICROSOFT WINDOWS

5.2.1.1 Servicio de Telnet

En los sistemas operativos Microsoft Windows NT, 2000, XP y 2003, la activación del servicio Telnet, requiere que se acceda a los "Servicios" a través del menú "Herramientas Administrativas". Seleccione el icono "Telnet", edite sus propiedades y pulse sobre el botón "Iniciar". Puede indicar que se active de forma automática al iniciarse el sistema seleccionando previamente como "Tipo de inicio", "Automático". En Windows Vista y 7 además requieren su instalación mediante el acceso directo "Activar o desactivar las características de Windows" del apartado "Programas" del "Panel de Control". Windows 2008 también requiere su instalación; acceda a la herramienta administrativa "Administrador del servidor", pulse en el panel izquierdo sobre "Características" y en el panel derecho sobre el icono o enlace "Agregar características", marque la casilla "Servidor Telnet" y complete la instalación mediante el asistente.

5.2.1.2 Servicio SSH

La instalación del servicio SSH en sistemas operativos Windows (NT, 2000 y XP), requiere la descarga del software libre OpenSSH (consulte enlaces de interés) para Windows. Los pasos para realizar su configuración son los siguientes:

1 Descomprimir el software y ejecutar el programa *setupssh*.

2 Procedemos a su instalación aceptando los términos de la licencia, seleccionar al menos el componente "Server", indique la carpeta donde desea realizar su instalación y complete la instalación.

3 Ejecutaremos la consola de órdenes y nos situaremos en la carpeta donde hemos instalado OpenSSH.

4 Agregamos al archivo *group* del directorio *etc*, el grupo de trabajo o el dominio al que pertenece nuestro equipo mediante las respectivas órdenes:

```
C:\Program files\OpenSSH> mkgroup -l >> .\etc\group
C:\Program files\OpenSSH> mkgroup -d >> .\etc\group
```

5 Agregaremos al archivo *passwd* del directorio *etc* los usuarios locales o de dominio mediante las respectivas órdenes:

```
C:\Program files\OpenSSH> mkpasswd -l -u usuario >> .\etc\passwd
C:\Program files\OpenSSH> mkpasswd -d -u usuario >> .\etc\passwd
```

6 Opcionalmente podemos editar manualmente el archivo *passwd* mencionado en el paso anterior, para modificar la carpeta a la que accederá cada cliente cuando se conecte. Encontrará dicha carpeta hacia el final de la línea y con el formato */home/usuario*. Para indicar la unidad C: lo haremos mediante la notación */cygdrive/c/* y, a continuación ,indicaríamos la ruta deseada. Un ejemplo para que la carpeta de inicio del usuario *Angel* fuera *Mis documentos*, podría ser el siguiente:

```
/cygdrive/c/Documents and Settings/Angel/Mis documentos
```

7 Estableceremos los permisos necesarios sobre la carpeta a la que accederá cada cliente al conectarse, además del permiso de lectura sobre la carpeta donde se instaló el servicio.

8 Iniciaremos el servicio identificado como "OpenSSH Server" mediante la herramienta administrativa "Servicios". Recuerde abrir el puerto 22 del cortafuegos de Windows para aceptar las conexiones entrantes.

5.2.1.3 Servicio de Escritorio Remoto VNC

Podemos encontrar distinto software para servidores VNC de carácter libre como: TighVNC, UltraVNC o RealVNC 4.1. Su instalación es sencilla, tan solo requiere aceptar la licencia GNU GPL y proporcionar al asistente diversa información, como la carpeta donde se instalará, el tipo de instalación (solo servidor o Server), el nombre de la carpeta del menú de inicio e indicarle si quiere que forme parte de los servicios de Windows. Posteriormente, podrá configurar diversos parámetros de este servicio como la contraseña de usuario remoto, los puertos de escucha y el comportamiento del terminal del servidor cuando el cliente tome su control. El puerto por defecto utilizado por este servicio es el 5900 y su inicio consiste en lanzar o ejecutar el programa.

5.2.1.4 Servicio de Terminal Server

- **Modo administración remota** (**Escritorio Remoto**): la configuración de un equipo Windows XP, 2003, Vista, 7 y 2008 para actuar como servidor de escritorio remoto es muy simple, aunque es posible que deba configurar adecuadamente algunas directivas relacionadas con el inicio de sesión mediante Terminal Server. Recuerde que Windows XP, 2003, Vista, 7 y 2008 incorporan por defecto el software para este modo. La configuración de este servicio requiere los siguientes pasos:
  - Aceda al panel de control mediante "Inicio | | Panel de Control".
  - Haga doble clic sobre el icono "Sistema" si dispone de XP ó 2003. Si utiliza Vista, 7 y 2008, deberá pulsar previamente sobre "Sistema y Seguridad" y, una vez en "Sistema", sobre el acceso directo "Configuración de Acceso remoto" del panel izquierdo.
  - Seleccione la solapa "Remoto" y active la opción "Permitir que los usuarios se conecten de manera remota a este equipo" para equipos con XP ó 2003 instalado. Si dispone de Vista, 7 ó 2008, le permitirá seleccionar una de entre tres opciones disponibles (véase Figura 5.2):
    - **No permitir las conexiones a este equipo**.
    - **Permitir las conexiones desde equipos que ejecuten cualquier versión de Escritorio remoto** (**menos seguro**): utilizado cuando desconocemos la versión de la aplicación "Escritorio remoto" que utilizarán los clientes.
    - **Permitir solo las conexiones desde equipos que ejecuten Escritorio remoto con Autenticación a nivel de red** (**más seguro**): utilizado cuando sabemos con certeza que el cliente utiliza una versión de la aplicación "Escritorio remoto" compatible con la autenticación a nivel de red (NLA).
  - Utilice el botón "Seleccionar usuarios remotos" (XP y 2003) o "Seleccionar usuarios..." (Vista, 7 y 2008) para indicar los usuarios a los que desea permitir el acceso remoto al servidor.
  - Pulse sobre "Aceptar" en cada uno de los cuadros de diálogo desplegados para aplicar la configuración.

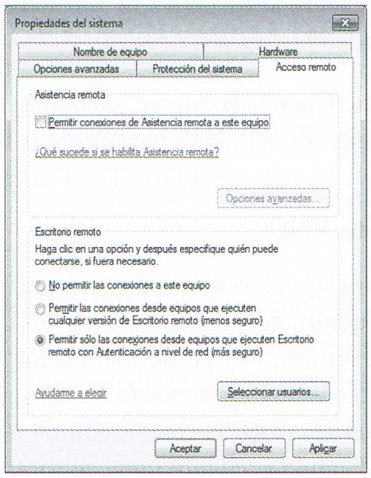


Figura 5.2. *Escritorio Remoto de Windows. Podemos seleccionar cualquiera de las dos opciones para permitir la conexión de usuarios, siendo la segunda la que nos asegura que el cliente se autenticará en red. También podemos elegir los usuarios a los que permitiremos conectarse al equipo mediante el botón "Seleccionar usuarios..."*

Las versiones de servidor Windows 2000, 2003 y 2008 Server, permiten configurar el perfil de los usuarios locales o de dominio para controlar de forma remota las sesiones de escritorio remoto iniciadas por los clientes. Para efectuarlo, acceda mediante el menú "Herramientas administrativas" a "Usuarios y grupos locales" o "Usuarios y equipos de Active Directory" si su equipo actúa como controlador de dominio. Seleccione el usuario a configurar su perfil, pulse sobre el icono "Propiedades" y seleccione la pestaña "Control remoto". Nos permitirá habilitar el control remoto sobre dicho usuario, si deseamos requerir su permiso y ver o interactuar con su sesión.

- **Modo servidor de aplicaciones**: en versiones 2000 Server y 2003 Server, puede comprobar si tiene instalado este servicio accediendo a "Inicio || Panel de Control || Agregar o quitar programas" y pulse sobre el icono de "Agregar o quitar componentes Windows". Si la casilla de "Terminal Server" no está activa, márquela y siga los pasos del asistente. Le indicará que las aplicaciones se reinstalarán tras instalar este servicio. Indique el tipo de seguridad que desee; total o media. Elija *total* si quiere alta seguridad pero menor compatibilidad con plataformas anteriores. Seleccione *media* si desea menos seguridad pero mayor compatibilidad con plataformas anteriores. Finalmente deberá reiniciar el equipo.

  En Windows 2008 Server, instalar la función "Terminal Server", para ello acceda a "Inicio || Herramientas administrativas || Administrador del servidor", pulse sobre el icono "Agregar funciones", marque la casilla "Terminal Services". El asistente nos permitirá seleccionar los siguientes componentes:

  - **Terminal Server**: permite a los clientes la ejecución de aplicaciones instaladas en el servidor.
  - **Administrador de licencias TS**: administra las licencias necesarias de las aplicaciones instaladas en el servidor, para que los clientes de Terminal Server accedan a dicho servidor y puedan ejecutarlas.
  - **Agente de sesiones de TS**: equilibra de forma homogénea la carga de sesiones entre varios servidores de nuestra red con el servicio Terminal Server activo con equilibrio de carga.
  - **Puerta de enlace de TS**: permite a los clientes la conexión de forma remota a través de otras redes como Internet, encapsulando el protocolo RDP mediante HTTPS.
  - **Acceso web de TS**: permite el acceso al servicio mediante HTTP (véase ejemplo 5.1).

Para habilitar la ejecución de aplicaciones remotas, previamente ha de instalar el servicio de *Licencias de Terminal Server*, mediante el asistente de componentes Windows, o el componente *Administrador de licencias TS* (2008) añadiendo dicha función.

El servidor de Licencias de Terminal Server no es objeto de este libro.

Las versiones de servidor Windows 2000, 2003 y 2008 Server, permiten configurar el perfil de los usuarios locales o de dominio para Terminal Server. Para efectuarlo, acceda mediante el menú "Herramientas administrativas" a "Usuarios y grupos locales" o "Usuarios y equipos de Active Directory" si su equipo actúa como controlador de dominio. Seleccione el usuario a configurar su perfil, pulse sobre el icono "Propiedades" y seleccione la pestaña "Perfiles de Servicios de Terminal Server" para establecer las opciones necesarias.



EJEMPLO 5.1

Disponemos de un equipo con Windows 2008 Server instalado cuya dirección de red es la 192.168.1.5, y deseamos compartir la aplicación *Paint* para clientes con Windows XP, ya que la versión instalada en los clientes es más antigua y ofrece menos posibilidades.

Para la instalación del servicio utilizaríamos el "Administrador del servidor" accesible desde "Herramientas administrativas", para agregar la función "Terminal Server" junto con el componente "Acceso web de TS", para poder ejecutar aplicaciones a través de un navegador.

Para compartir la aplicación *Paint*, seguiríamos los siguientes pasos:

- Accedemos a la herramienta *Administrador de RemoteApp de TS*, mediante "Inicio || Herramientas administrativas || Terminal Services".
- En el panel derecho pulsamos sobre "Agregar programas RemoteApp".
- Mediante el asistente marcamos el programa *Paint* de la lista de programas RemoteApp que nos ofrece Windows 2008.
- Finalizamos el asistente.

5.2.1.5 Servicio de acceso Remoto mediante interfaz Web

- **Escritorio remoto VNC**: permite la administración de un servidor mediante interfaz web, ya que también puede utilizar el puerto 5800 para este tipo de accesos. Por tanto, deberemos asegurarnos que en las opciones del software VNC instalado, este parámetro esté habilitado.
- **Escritorio remoto RDP (XP, 2003 y 2008)**: para la instalación del componente de IIS necesario y si utiliza XP Professional ó 2003, utilice el *Asistente de componentes Windows*. Seleccione el "Servicio *World Wide Web*" correspondiente a *Internet Information Server* (véase capítulo 3) y pulse sobre el botón "Detalles". Aparecerá un componente denominado "Conexión web a Escritorio remoto" que deberá marcar y, posteriormente, pulsar el botón "Aceptar" en cada uno de los cuadros de diálogo que ha desplegado hasta encontrarse en el primero, donde tras pulsar en "Siguiente" se instalará esta utilidad. El control mencionado anteriormente también se puede descargar de forma gratuita desde la URL:

www.microsoft.com/windowsxp/downloads/tools/rdwebconn.mspx

Si el sistema operativo instalado es Windows 2008 Server, tendremos que instalar el componente "Acceso web de TS" del servicio *Terminal Server* (véase ejemplo 5.1), creándose en el sitio web por defecto la carpeta *ts* (*Terminal Services*).

- **Administración remota (2003)**: para instalar el componente de IIS *Administración remota* tendremos que utilizar el "Asistente para componentes de Windows", marcar la casilla "Servidor de aplicaciones" y pulsar sobre "Detalles". Activaremos la casilla referida a IIS y haremos clic en "Detalles", marcaremos la casilla "Servicio *World Wide Web*" y haremos nuevamente uso de "Detalles para marcar Administración remota (HTML)".

Windows 2008 incluye un paquete de herramientas de administración de servidor remoto, que permite administración remota de servicios como Active Directory, DHCP, DNS o HTTP (IIS). Requiere la instalación de la característica *Herramienta de administración remota del servidor*.

5.2.2 CONFIGURACIÓN EN GNU/LINUX

5.2.2.1 Servicio de Telnet, RLogin y SSH

Deberá instalar el paquete *telnet-server* para proporcionar el servicio telnet (OpenSuSE 11.1 y Fedora 11) o *telnetd* (Debian 5 Lenny) y *rsh-server* para *rlogin*. El servicio SSH ya viene preinstalado gracias al paquete *openssh* (servidor y cliente) en una distribución OpenSuSE 11.1, teniendo que instalar el paquete *openssh-server* en una distribución Fedora 11 o Debian 5 Lenny. En OpenSuSE, para iniciar el servicio, acceda a los servicios de *xinetd* mediante la opción "Servicios de red" de *YaST2*, seleccione *telnet*, *rsh* según desee y actívelo. Para iniciar el servicio SSH, acceda al editor de niveles de ejecución para activarlo en el arranque o bien ejecute la orden *rcsshd start* para levantar el demonio correspondiente. En Fedora o Debian puede utilizar la herramienta *Servicios* para activar cualquiera de estos servicios o utilizar la orden *service sshd start* (Fedora) o */etc/init.d/ssh start* para activar el servicio SSH. Tenga en cuenta que los servicios *telnet* y *rlogin* dependen de *xinetd*.

5.2.2.2 Servicio X-Terminal

- **Sesión X Window remota**:

  Este servicio se puede ofertar de dos formas según se muestra a continuación, donde se indican los diferentes pasos a seguir:

  - **Mediante entorno gráfico GNOME**:
    - Acceder a "Sistema | | Administración | | Preferencias de la ventana de Entrada", pestaña "Remota".
    - Seleccionar como estilo "Igual que la entrada local".
    - Pulsar sobre el botón "Configurar XDMCP..." y activar "Confiar en las solicitudes indirectas".
  - **Mediante consola de órdenes**:
    - Editar el fichero de configuración del gestor de pantalla del entorno de escritorio como administrador del sistema. Por ejemplo, en una distribución Debian donde el entorno de escritorio utilizado sea GNOME, el gestor de pantalla es *gdm*, cuyo fichero de configuración es */etc/gdm/gdm.conf*.

      ```
      $sudo nano /etc/gdm/gdm.conf
      ```

- Establecer el valor del parámetro "Enable" a "true" en la sección [xdmcp] y guardar los cambios.

```
[xdmcp]
Enable=true
```

En ambos casos debemos reiniciar el gestor de pantalla. Siguiendo con el supuesto y considerando *gdm* como el gestor de pantalla y Debian como distribución, ejecutaríamos como administrador la orden:

```
$sudo /etc/init.d/gdm restart
```

- **Aplicaciones X Window remotas**:

La preparación del servidor es muy sencilla, ya que solo requiere modificar y exportar la variable de entorno DISPLAY, indicando el nombre o dirección de red del cliente y el número de display donde se mostrarán las aplicaciones gráficas que se ejecuten en el servidor. Suponiendo que el equipo cliente tiene asignada la dirección IP 192.168.1.15 y que el display utilizado es el 1, ejecutaríamos la siguiente orden:

```
$export DISPLAY=192.168.1.5:1.0
```

Lo habitual no es ejecutar esta orden desde el servidor, sino establecer una conexión remota con el servidor mediante Telnet o SSH desde el cliente, para ejecutar la orden anterior y ejecutar la aplicación deseada (véase ejemplo 5.6).

5.2.2.3 Servicio de Escritorio Remoto VNC

En GNU/Linux se utiliza el protocolo VNC para el acceso a un escritorio remoto. En distribuciones como OpenSuSE 11.1, Fedora 11 o Debian 5 Lenny, se disponen de varios modos de compartir el escritorio, entre ellos los siguientes:

- **Activando la administración remota mediante VNC**: en una distribución OpenSuSE acceda a la Configuración de Servicios de red de *YaST2* y seleccione la opción de "Administración remota (VNC)". Active la opción "Permitir administración remota" y abra el puerto correspondiente del cortafuegos. La activación de este servicio y sus demonios también es posible utilizando el editor de niveles de ejecución de *YaST2*.

- **Entorno KDE**: la herramienta *krfb* requiere la instalación del paquete *kde4-krfb* en OpenSuSE y *kdenetwork* en Fedora, que incluye esta aplicación de red entre otras. En OpenSuSE, es accesible mediante el grupo de aplicaciones "Sistema", y en Fedora, desde "Aplicaciones | | Internet | | Escritorio Compartido". Esta herramienta nos permite hacer invitaciones a otros equipos, generando automáticamente una contraseña de conexión que el cliente ha de conocer, permitiendo su envío mediante correo electrónico (véase Figura 5.3). Mediante el botón de configuración, se pueden configurar parámetros de red, como anunciar el servicio en la red local o establecer el puerto que tiene asociado, y de seguridad, como permitir conexiones no invitadas o permitir el control del escritorio. El servidor puede recibir noticia cada vez que un cliente se conecta y aceptar o no la conexión.

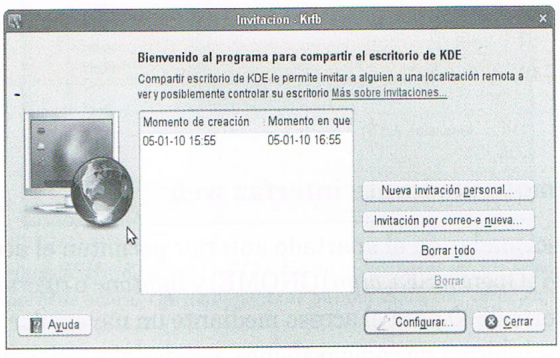


Figura 5.3. Escritorio compartido de KDE mediante la herramienta krfb. Mediante esta herramienta, un equipo GNU/Linux puede crear invitaciones para la conexión remota de otros equipos, incluso su envío por email. Mediante el botón de "Configuración" pueden establecerse parámetros adicionales

5.3 CONFIGURACIÓN DEL CLIENTE DE ACCESO REMOTO

5.3.1 CONFIGURACIÓN EN MICROSOFT WINDOWS

5.3.1.1 Cliente de Telnet, RLogin y SSH

En el mercado se encuentra disponible diferente software que permite establecer una conexión Telnet, RLogin o SSH. Uno de los más populares es el emulador de terminal PuTTY, software libre que podrá descargarse de Internet.

Su instalación resulta sencilla, tan solo requiere indicar la carpeta donde lo quiere instalar, el nombre de la carpeta del menú de inicio, si desea crear un acceso directo en el escritorio y si lo va a utilizar el usuario que lo está instalando o todos.

Previo a iniciar una sesión con un equipo remoto, permite establecer una serie de parámetros referentes a la propia sesión, el tipo de terminal, las características de la ventana de terminal y de la conexión, así como las conexiones X-Window.

Para establecer una conexión con el cliente ha de indicar el tipo de conexión (Raw, Telnet, RLogin, SSH o Serial), teniendo establecido su puerto por defecto. Indicaremos el nombre del equipo remoto o su dirección IP y pulsaremos el botón "*Open*", tras el cual le pedirá que ingrese su nombre de usuario y contraseña (véase Figura 5.4). PuTTy nos permite guardar la sesión con un servidor, si una vez indicados los parámetros de la conexión, pulsamos sobre el botón "*Save*" antes que "*Open*" para establecerla. La primera vez que lo utilicemos con SSH para conectarnos a un determinado servidor, nos preguntará si deseamos aceptar la clave pública de éste.

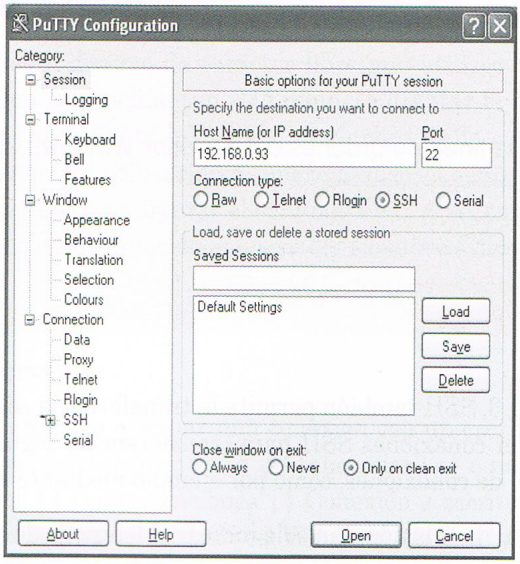


Figura 5.4. *Inicio de sesión con cliente de Telnet, SSH y RLogin (PuTTY). Ha de indicarse el equipo remoto al que se quiere acceder, el servicio que se quiere utilizar y el puerto de acceso. Opcionalmente se pueden establecer otros parámetros adicionales*

- **Entorno GNOME**: herramienta *vino*: en Debian 5 Lenny, requiere la instalación del paquete del mismo nombre. Para utilizarlo puede ejecutar la orden *vino-preferences* como administrador desde una consola de terminal para establecer los parámetros del servicio. En la pestaña "General" debe marcarse "Permitir a otros usuarios ver mi escritorio" y "Permitir a otros usuarios controlar tu escritorio". Podemos requerir confirmación del servidor antes de establecer la conexión, así como introducir una contraseña. Mediante la pestaña "Avanzado" se pueden establecer otros parámetros, como un puerto alternativo o bloquear la pantalla al desconectarse el cliente remoto.

- **Mediante línea de órdenes**: de forma alternativa y en las distribuciones mencionadas, se admite una sucesión de órdenes que inician el servicio VNC, previamente instalado el paquete *tightvnc* en OpenSuse y *tigervnc-server* en Fedora y *tightvncserver* en Debian. Para cada usuario que inicia el servicio VNC, se crea el directorio *.vnc* en su directorio personal con la configuración del mismo. Mediante el siguiente ejemplo se explican las órdenes implicadas y la forma de utilizarlas para iniciar y proporcionar este servicio.



EJEMPLO 5.2

Disponemos de un equipo GNU/Linux con una distribución OpenSuSE instalada, cuya dirección IP es la 10.0.1.93 y con el usuario con el que estamos conectamos actualmente, queremos iniciar el servicio VNC para que otro usuario de un equipo GNU/Linux acceda de forma remota. Los pasos a seguir son los siguientes:

Creamos una nueva sesión en el servidor denominada *remota* que utiliza una resolución de 800 x 600, con profundidad de 16 bits y accesible desde el terminal 1:

```
$ vncserver :1 -name remota -depth 16 -geometry 800x600
```

Posteriormente establecemos la contraseña de conexión:

```
$ vncpasswd
  Password:
  Verify:
```

Opcionalmente se puede acceder al directorio *.vnc* de su directorio personal para editar el fichero *xstartup* e indicar el gestor de ventanas a utilizar en la última línea:

```
$ cd .vnc
$ joe xstartup
      . . .
  #Entorno de ventanas utilizado: twm
    twm &
```

Para detener la sesión se ejecutaría la orden *vncserver* indicando junto con la opción -kill, el número de terminal:

```
$ vncserver -kill :1
```

5.2.2.4 Servicio de acceso remoto mediante interfaz web

No todas las herramientas mencionadas en el apartado anterior permiten el acceso web mediante el puerto 5800. Lo permiten *Administración remota* (OpenSuSE), *vino* (GNOME) y *tightvnc* o *tigervnc* mediante *vncserver*. Por defecto, estas herramientas habilitan el puerto 5800 para el acceso mediante un navegador web. De hecho la herramienta *vino* mediante su pestaña "General", nos informa de cómo podemos acceder al servicio mediante navegador.

Tabla 5.1. Formatos de conexión remota

Acción	Formato
Conexión Telnet	*telnet [Usuario@]Servidor*
Conexión RLogin	*rlogin [Usuario@]Servidor*
Conexión SSH	*ssh [Usuario@]Servidor*
Copia SSH	*scp FicheroLocal [Usuario@]Servidor[:Directorio]*
Transferencia SSH	*sftp [Usuario@]Servidor*

El acceso al servicio Telnet en sistemas operativos Windows también se puede utilizar mediante la consola de órdenes, aunque versiones como Windows Vista, 7 y 2008, requieren activar dicha característica, ya que por defecto no está activado. Para conectarse utilice la orden *telnet*, cuyo formato puede observar en la tabla 5.1, así como ilustrarse mediante el ejemplo 5.3.

EJEMPLO 5.3

Disponemos de un equipo Windows XP, cuya dirección IP es la 192.168.1.100. Deseamos realizar tareas administrativas como Administrador en un equipo Windows 2008 cuya dirección IP es la 192.168.1.5.

Para ejecutar la consola de órdenes, pulsaríamos en "Inicio || Ejecutar" y tecleamos "*cmd*". Una vez en la línea de órdenes, teclearíamos lo siguiente:

```
C:> telnet 192.168.1.5
```

Nos solicitaría el usuario y posteriormente la contraseña:

```
login: Administrador
password: *******
```

Finalmente nos aparecería la línea de órdenes del servidor Windows 2008:

```
*=======================================
Microsoft Telnet Server.
*=======================================
C:\Users\Administrador> telnet 192.168.1.5
```

Como se indicó en el apartado 5.1.3, SSH también permite la transferencia segura de archivos. Uno de los clientes más conocidos que permite establecer conexiones SSH para transferencias seguras es el programa *WinSCP*, el cual permite también establecer otro tipo de conexiones, como por ejemplo mediante FTP.

No se requiere gran esfuerzo en su instalación, tan solo indicar el lenguaje de instalación, aceptar la licencia GNU, indicar el directorio donde instalarlo, los componentes a instalar (deje los que vienen por defecto), el nombre de la carpeta del menú de inicio, el usuario o usuarios que lo utilizarán y finalmente, el tipo de interfaz.

Para establecer una conexión con un servidor remoto, ha de indicar su nombre o dirección IP, el número del puerto (22 para SSH y 23 para FTP), un nombre de usuario, su contraseña y pulsar sobre el botón "Login". Nos aparecerá una doble ventana con la jerarquía de ficheros y directorios local y remota. Su manejo resulta muy sencillo e intuitivo, utilice el ratón para arrastrar y copiar los ficheros entre los equipos remotos (véase Figura 5.5). Además, dispone de

barra de herramientas y menús con ayuda contextual. Al igual que PuTTY, la primera vez que lo utilicemos nos pedirá si deseamos aceptar la clave pública del servidor.

En Windows (NT, 2000 y XP) también puede utilizar el software de OpenSSH para instalar el cliente del servicio SSH. Para instalarlo, siga los pasos 1 y 2 del apartado 5.3.1.2, seleccionando al menos el componente "*Client*" en el paso 2. Posteriormente puede utilizar una consola de órdenes para efectuar una conexión mediante la orden *ssh* (véase tabla 5.1), o copiar archivos mediante las órdenes *scp* o *sftp*. Puede consultar el ejemplo 5.5 (configuración en GNU/Linux) para ilustrarse sobre la utilización de estas órdenes.

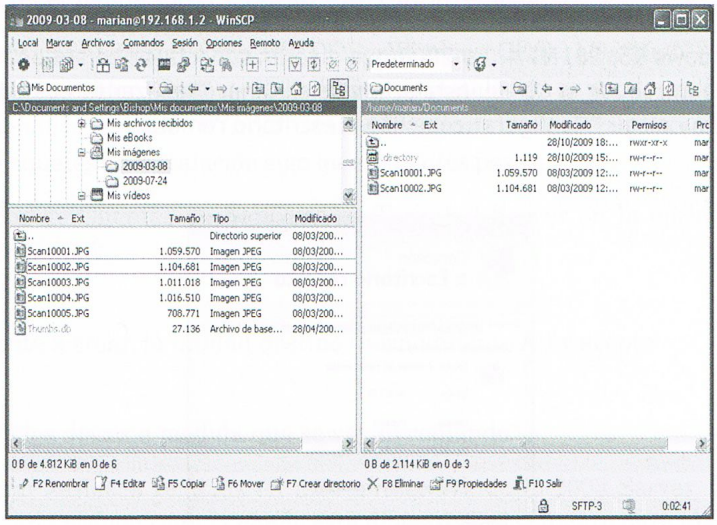


Figura 5.5. *Cliente de FTP y SSH WinSCP. Permite la transferencia segura de información entre equipos remotos. Su interfaz gráfica resulta muy intuitiva para el usuario. En el ejemplo de la figura, la ventana local hace referencia al directorio raíz de la unidad F:, mientras que la venta remota hace referencia al directorio /home/habitual*

5.3.1.2 Cliente de Escritorio Remoto VNC

Podemos encontrar software cliente diverso de carácter libre que utilizce VNC, como es el caso de TightVNC, UltraVNC o RealVNC. Su instalación es sencilla, tan solo requiere aceptar la licencia GNU GPL, la carpeta donde se instalará, el tipo de instalación (solo cliente o Viewer), el nombre de la carpeta del menú de inicio y si desea asociarle los ficheros con extensión *vnc*. Su utilización requiere indicar el servidor al que desea conectarse, así como la contraseña que se estableció al instalar o configurar el servidor VNC. A veces debe indicarse el número de terminal remoto que está utilizando, indicando a continuación del servidor (nombre o dirección de red) dos puntos seguidos del número de terminal.

5.3.1.3 Cliente de Terminal Server

- **Acceso a Escritorio Remoto**: para efectuar una conexión con un escritorio remoto con Windows XP, Vista, 7, 2003 Server ó 2008 Server, primeramente ha de tener claro el equipo de la red al que quiere acceder. Acceda a "Inicio || Accesorios || Comunicaciones || Conexión a escritorio remoto" en XP ó 2003, o a "Inicio || Accesorios || Conexión a escritorio remoto" en Windows Vista, 7 y 2008 para establecer los siguientes parámetros (véase Figura 5.6):
  - Indique el nombre o dirección IP del equipo o despliegue la lista y búsquelo seleccionando "Examinar más...".
  - Puede establecer opciones adicionales como el dominio o el usuario y contraseña pulsando sobre el botón "Opciones".

- Pulse el botón "Conectar", tras el cual se le solicitará que introduzca un nombre de usuario y contraseña perteneciente al equipo remoto si no lo hizo previamente. Si accede a un servidor con 2008 instalado, puede requerirle la aceptación de un certificado si no puede verificar la identidad de su equipo cliente.
- Tras su comprobación tendrá delante el escritorio deseado, mostrándonos en la parte superior del escritorio un indicativo de la conexión establecida, permitiéndonos alternar entre nuestro escritorio local y el remoto.

Para equipos con Windows 95, 98, NT 4.0 o 2000 que quieran conectarse en sesión remota a un equipo con Windows XP, debe introducir el CD de instalación, seleccionar "Realizar tareas adicionales" tras la ventana de bienvenida y elegir "Configurar conexión a escritorio remoto".

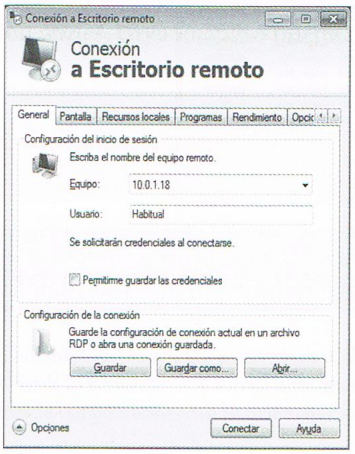


Figura 5.6. Cliente de Escritorio Remoto de Windows Vista/7/2008. Indicamos el equipo remoto al que queremos acceder y pulsamos el botón "Conectar". Mediante el botón "Opciones >>", se pueden establecer parámetros adicionales como el tamaño del escritorio

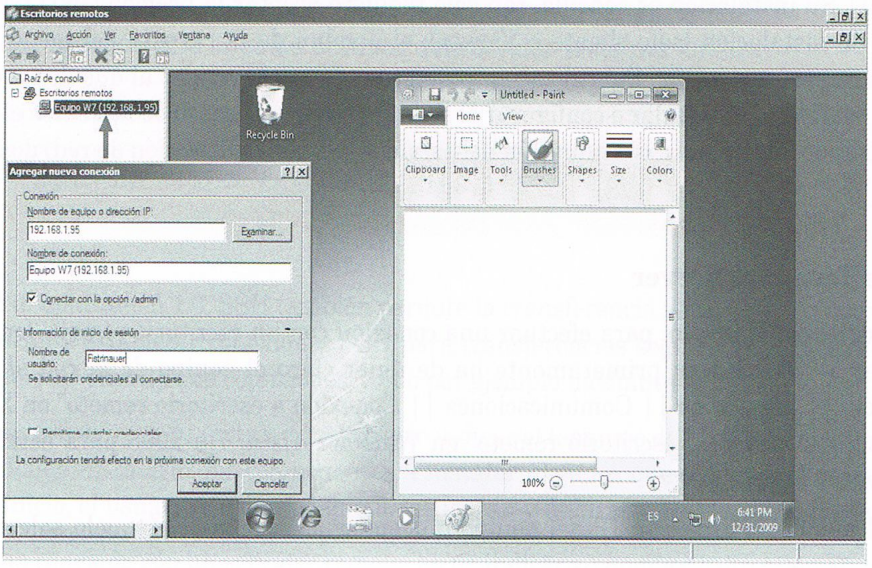


Figura 5.7. Ventana principal de gestión de conexiones de escritorio remoto de Windows Server 2008. En esta ventana se aprecian los datos (usuario, contraseña y dominio) utilizados para la conexión al equipo remoto con dirección IP 192.168.1.95. En la parte derecha de la ventana se puede observar el escritorio del equipo remoto

Windows 2003 y 2008 también nos permiten el control y acceso a distintos equipos remotos a través de la herramienta *Escritorios remotos* del menú "Herramientas administrativas" (en 2008 despliegue Terminal Services). La Figura 5.7 muestra su ventana principal junto con la ventana para establecer una conexión con un equipo remoto, que se obtiene al utilizar el menú contextual del ratón y pulsar en "Agregar conexión". Se pueden modificar las características de cada conexión, utilizando el menú contextual sobre una conexión y seleccionando la opción "Propiedades". Mediante una ventana con solapas se pueden alterar las propiedades de la conexión (como la dirección IP del equipo remoto), así como modificar otros parámetros como la configuración de la pantalla donde se visualizará el escritorio remoto y otras características en las que se puede especificar, por ejemplo, el programa a ejecutar al inicio de la conexión remota. Recuerde que para acceder a los equipos remotos, deben tener habilitado el servicio de escritorio remoto.

Para otros sistemas operativos Microsoft como MS_DOS y Windows CE/3.11/9x/Me/NT/2000, desde los que se desee iniciar sesiones remotas con un servidor Windows 2000 Server, su instalación se puede realizar mediante disquetes, o de forma alternativa, compartiendo la carpeta *\WINNT\system32\clients\tsclient* para acceder al software de clientes de 16 y 32 bits. Para crear los disquetes de instalación siga los siguientes pasos:

1. Abrir la utilidad Creador de Clientes de Servicios de Terminal Server en la opción "Inicio || Programas || Herramientas administrativas".
2. Seleccione el tipo de cliente a crear, la unidad destino (normalmente A:) y acepte.
3. El programa le solicitará los discos a medida que se vayan copiando.

Si lo que quiere es iniciar sesiones remotas en un servidor Windows 2003 Server, puede compartir la carpeta *\WINDOWS\system32\clients\tsclient\win32* donde está disponible el software para instalar en los clientes (fichero *setup.exe*). Para iniciar sesiones remotas en un servidor Windows 2008, debe descargarse el software de Microsoft, el cual está disponible para Windows XP y 2003.

- **Acceso a aplicaciones remotas**: puesto que este capítulo se centra en la administración remota, tan solo se incluye el siguiente ejemplo que se complementa con el ejemplo 5.1.

EJEMPLO 5.4

Deseamos acceder desde un equipo con Windows XP instalado al servidor del Windows 2008 del ejemplo 5.1 para ejecutar la aplicación *Paint*.

Los pasos para ejecutar la aplicación serían los siguientes:

1. Abrir un navegador web.
2. Indicar como URL: *http://192.168.1.5/ts*
3. El servidor nos solicita un usuario y contraseña para la conexión remota vía web.
4. Mediante el botón "Programas RemoteApp" observaríamos que la aplicación *Paint* está a su disposición.
5. Al hacer doble clic nos muestra un mensaje de advertencia antes de la conexión. Pulsamos sobre el botón "Conectar".
6. Finalmente nos solicita un usuario y contraseña para la ejecución de la aplicación.

5.3.1.4 Cliente de acceso remoto mediante interfaz Web

- **Escritorio remoto VNC**: si el servidor se configuró adecuadamente también podrá acceder mediante cualquier navegador que esté habilitado para ejecución de applets de Java, además de tener instalado en su equipo la utilidad **JRE** (*Java Runtime Environment*). Para realizar el acceso remoto indique como URL del navegador el nombre o dirección de red del servidor seguida de dos puntos y el número de puerto (véase la Figura 5.8). El servidor le pedirá una contraseña válida para el servicio VNC antes de interactuar con él. Mediante el botón "Options" podrá establecer previamente diversos parámetros. También dispone de los botones "Disconnect" para finalizar la conexión remota y el botón "Send Ctrl-Alt-Del", utilizado en el caso de acceder a un equipo que requiera esta combinación de teclas antes de auntenticarse.

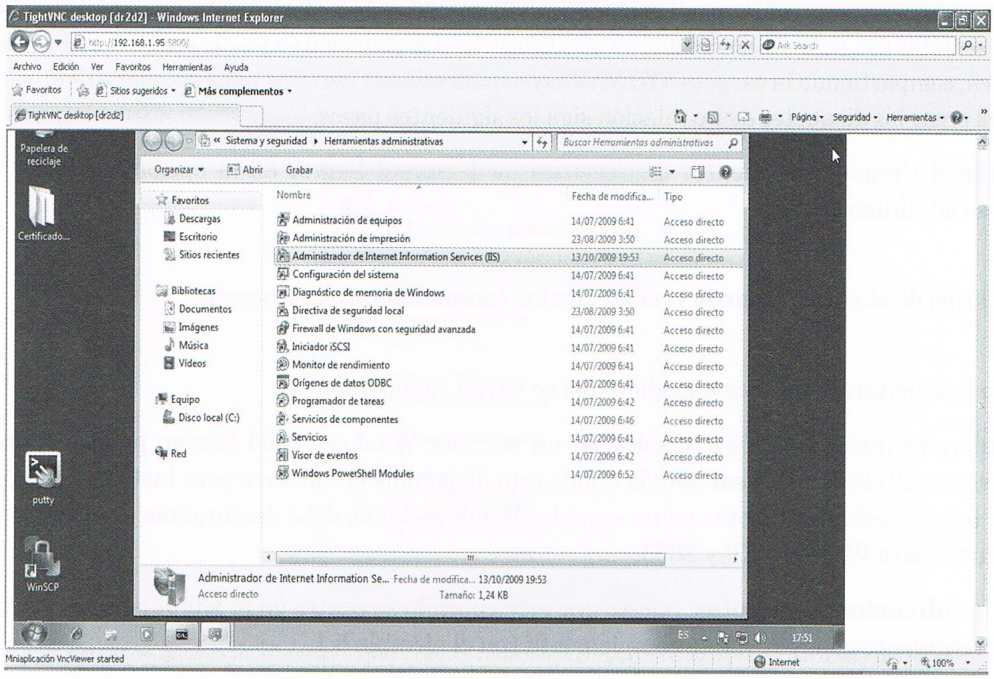


Figura 5.8. *Ejemplo de acceso remoto mediante VNC vía web. En este ejemplo se aprecia el acceso remoto desde el navegador Internet Explorer a un equipo Windows 7 con dirección IP 192.168.1.95. Se ha indicado como puerto el 5800, correspondiente al puerto VNC para este tipo de acceso a escritorio remoto*

- **Escritorio remoto RDP (Windows XP, 2003 y 2008)**: para acceder a este servicio utilizaremos un navegador (recomendable Internet Explorer) para indicar como URL *http://Servidor/tsweb* si el sistema operativo del equipo que proporciona el servicio es XP Professional ó 2003 Server, o *http://Servidor/ts* si tiene instalado 2008 Server. Como *Servidor* se indicará el nombre del equipo con alguno de los sistemas operativos mencionados instalados, o bien su dirección de red. Nos solicitará un usuario autorizado y contraseña para la conexión, tras los cuales aparecerá una página similar a la que se muestra en la Figura 5.9, donde nos pedirá autorización para la instalación del control *ActiveX*. Si el sistema operativo Windows 2008 es el que aloja dicho servicio, tendremos que pulsar sobre el botón "Escritorio remoto" del menú superior (véase Figura 5.9). Tendremos que indicar el equipo remoto al que queremos acceder (nombre o dirección de red) y el tamaño que tendrá la ventana. Al pulsar sobre "Conectar", nos mostrará un aviso de inicio de conexión remota, permitiendo marcar los recursos a los que tendremos acceso.

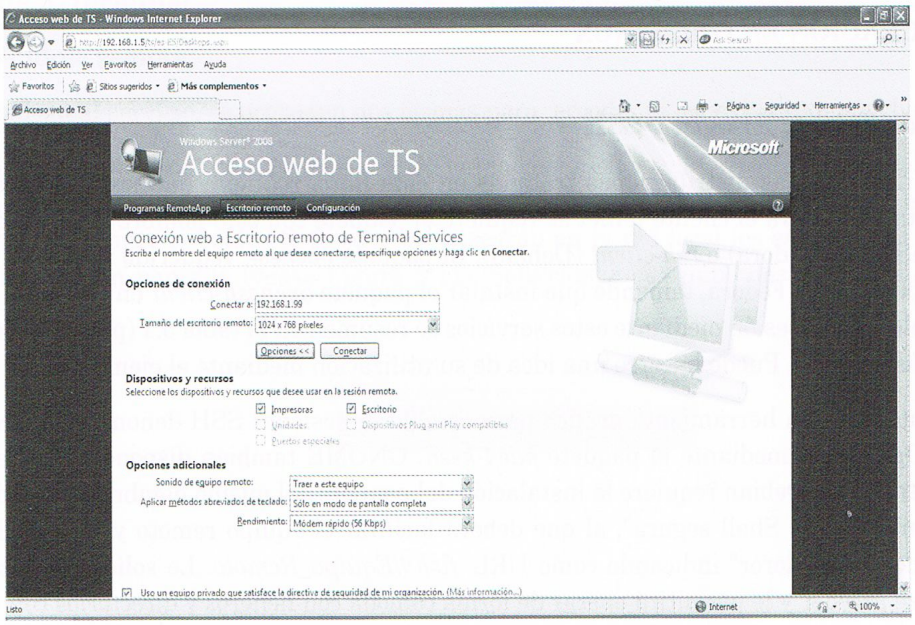


Figura 5.9. Acceso remoto a un equipo Windows mediante un navegador. En este ejemplo se ha utilizado Internet Explorer para que, a través del servidor 192.168.1.5, se pueda acceder al equipo remoto. Debe indicarse el equipo remoto (192.168.1.99) y opcionalmente, seleccionar el tamaño de la ventana, así como determinar los recursos a utilizar del equipo remoto y otras opciones adicionales

- **Administración remota (Windows 2003)**: para acceder a la herramienta *Administración remota* de Windows 2003 Server, tendremos que indicar en el navegador como URL *https://Servidor:8098* donde *Servidor* es el equipo con este sistema operativo instalado. Nos aparecerá una barra de menú y otra de submenú para configurar diversos parámetros del sistema operativo (véase Figura 5.10).

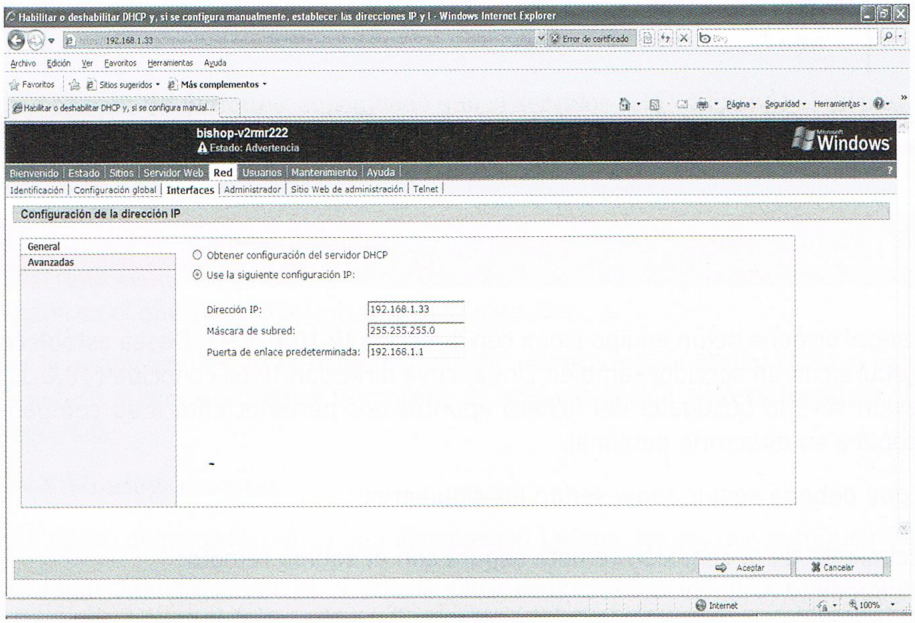


Figura 5.10. Herramienta de administración remota mediante interfaz web. En este ejemplo se aprecia el acceso remoto al equipo con dirección IP 192.168.1.33. En la página abierta se muestra la configuración de red de una de sus interfaces, mostrándose el parámetro dirección IP, máscara de subred y puerta de enlace predeterminada

5.3.2 CONFIGURACIÓN EN GNU/LINUX

5.3.2.1 Cliente de Telnet, RLogin y SSH

Su utilización mediante las distribuciones tratadas en este libro, requiere que los paquetes clientes de estos servicios estén instalados. Para el cliente telnet se requiere el paquete con este nombre y, para rlogin, se requiere el paquete *rsh* (OpenSuSE y Fedora) o *rsh-client* (Debian). El paquete *openssh* requerido para SSH, viene por defecto preinstalado en OpenSuSE y Fedora, teniendo que instalar el paquete *openssh-client* en Debian. Los formatos de las órdenes para establecer una sesión mediante estos servicios se resumen en la tabla 5.1 (para conocer el resto opciones consulte las páginas de *man*). Puede hacerse una idea de su utilización mediante el ejemplo 5.5.

KDE permite utilizar una herramienta gráfica para establecer sesiones SSH denominada *KSSH*, disponible en una distribución OpenSuSE mediante el paquete *kde4-kssh*. GNOME también dispone de la herramienta gráfica *hotssh*. En una distribución Debian requiere la instalación del paquete del mismo nombre y la tendrá accesible desde "Aplicaciones || Internet || Shell segura", al que deberá facilitar el equipo remoto y el usuario. También puede utilizar el navegador "Konqueror" indicando como URL: *fish://Equipo_Remoto*. Le solicitará autenticación para el equipo al que quiere acceder y le permitirá operar de forma comoda con ficheros y directorios con tan solo arrastrar-soltar y utilizando el menú contextual del botón derecho del ratón (véase Figura 5.11).

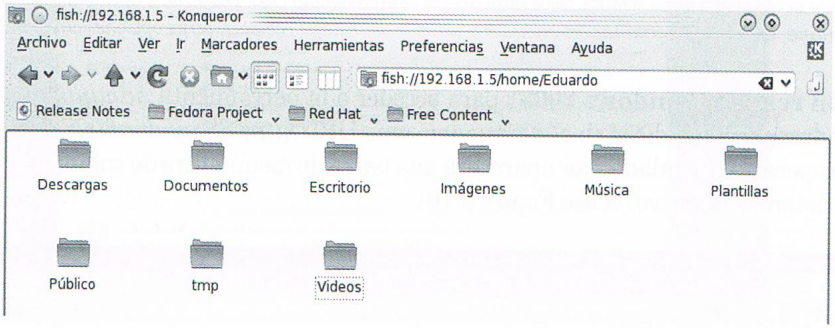


Figura 5.11. *Ejemplo de conexión SSH mediante Konqueror. Se ha utilizado como URL en este navegador: fish:/ / 192.168.1.5, donde 192.168.1.5 es la dirección IP del equipo remoto al que se desea acceder, el cual solicitará un nombre de usuario y una contraseña*

EJEMPLO 5.5

El usuario *angel* dispone de un equipo Linux con dirección IP 10.0.1.93. Desea establecer una conexión remota y segura con un servidor también Linux, cuya dirección IP es conocida (10.0.1.39). El objetivo de la conexión será la búsqueda del fichero *apuntes.doc* perteneciente a su compañero *ruben* y su posterior copia a su directorio personal.

Los pasos que debería seguir *angel* serían los siguientes:

1. Establecimiento de la conexión remota segura con el equipo remoto:
   ```
   $ ssh ruben@10.0.1.39
   ```
2. Procede a la busqueda del fichero *apuntes.doc*:
   ```
   $ find .  -name apuntes.doc
   ```
3. Suponiendo que lo ha encontrado en el directorio *apuntes*, procede a su copia segura:
   ```
   $ scp ./apuntes/apuntes.doc angel@10.0.1.93
   ```

5.3.2.2 Cliente de X-Terminal

- **Sesión X Window remota**:

De forma análoga al servicio, se proponen dos formas para acceder al servicio desde un cliente.

- **Mediante entorno gráfico GNOME o KDE**: al iniciar sesión con GNOME, KDE, pulsar sobre el botón "Opciones" y seleccionar "Entrada remota por XDMCP..." para indicar el servidor en el queremos iniciar la sesión X. Mediante el botón "Refrescar" se buscarán en la red local los equipos que ofrecen el servicio y se mostrarán en pantalla (véase Figura 5.11). Seleccionar el equipo deseado y pulsar sobre el botón "Conectar".



Figura 5.12. Ejemplo de conexión mediante XDMCP. El cliente desea iniciar una sesión gráfica, y su equipo ha detectado mediante un servidor web www.srvweb1.com en la red cuya dirección IP es la 192.168.1.5. Seleccionando dicho servidor y pulsando sobre "Conectar" aparecerá la ventana de inicio de sesión

- **Mediante consola de órdenes**: suponiendo que el servidor está utilizando el display 0 para ejecutar su sesión X, ejecutaríamos la orden:

```
$ sudo X :1.0 -query Servidor
```

El parámetro 1 indica el número de display del servidor que el cliente utilizará para la sesión X y el parámetro 0 representa la pantalla local del cliente. Como "Servidor" indicaremos el nombre o dirección de red del equipo en el que queremos iniciar la sesión gráfica.

Para finalizar la sesión gráfica en la máquina remota, cerraríamos la sesión como si estuviéramos en local ("Sistema || Salir"), y tras mostrarnos la ventana de inicio de sesión, seleccionaríamos "Desconectar" de las "Opciones" sugeridas.

- **Aplicaciones X Window remotas**.

Suponiendo un gestor de pantalla *gdm* y una distribución Debian, los pasos a seguir serían los siguientes:

- En primer lugar se debe preparar al cliente para poder recibir las aplicaciones que se ejecuten en el servidor. Para ello, editar el fichero de configuración */etc/gdm/gdm.conf* y establecer el valor del parámetro "DisallowTCP" a "false" en la sección [security] guardando los cambios. Otra posibilidad la encontramos mediante la pestaña "Seguridad" de "Sistema || Administración || Ventana de entrada" para desmarcar la opción "Denegar conexiones entrantes".
- Reiniciar el gestor de pantalla para actualizar su configuración con el anterior cambio.

- Dar permiso al servidor X mediante la orden *xhost* para visualizar e interactuar con aplicaciones remotas del servidor. El formato de esta orden es *xhost + Servidor*, donde "Servidor" es el nombre o dirección IP de la máquina que ejecuta las aplicaciones. Si no se indica éste último parámetro, indicamos que el cliente aceptará aplicaciones de cualquier máquina remota.
- Posteriormente iniciaríamos una sesión remota con el servidor para ejecutar la aplicación deseada.

Un ejemplo completo de este servicio lo tiene a continuación, mediante el ejemplo 5.6, donde el cliente además de prepararse para recibir las aplicaciones remotas, se conecta al servidor mediante SSH para ejecutar las órdenes que permitan redirigir las aplicaciones hacia el cliente y ejecutar una aplicación.

EJEMPLO 5.6

Disponemos de dos equipos GNU/Linux, un servidor cuya dirección IP es la 192.168.1.5, y un cliente cuya dirección IP es la 192.168.1.15, cuyos recursos hardware son escasos para la ejecución de aplicaciones gráficas. En ambos casos suponemos un gestor de pantalla *gdm*.

En la máquina cliente, abrimos un terminal de consola y editamos el fichero de configuración */etc/gdm/gdm.conf*. Estableceremos el parámetro *DisallowTCP* con valor *false*, de manera que permitamos la recepción de aplicaciones:

```
$sudo nano /etc/gdm/gdm.conf
[security]
DisallowTCP=false
```

Reiniciamos el gestor de pantalla para actualizar la anterior modificación:

```
$ sudo /etc/init.d/gdm restart
```

Iniciamos sesión en el entorno de escritorio GNOME y abrimos un terminal de órdenes para dar permiso al servidor para visualizar e interactuar con sus aplicaciones remotas:

```
$ xhost + 192.168.1.5
```

Nos conectamos al servidor mediante SSH:

```
$ ssh $ ssh eduardo@192.168.1.5
eduardo@192.168.1.5's password: *******
```

Redirigimos la salida por pantalla al display 1 de nuestra máquina cliente y ejecutamos la aplicación Mozilla Firefox:

```
$ export DISPLAY=192.168.1.15:1.0
$ firefox &
```

Minimizamos el terminal de órdenes y ya podemos utilizar el navegador Mozilla Firefox, el cual visualizamos en nuestro escritorio.

5.3.2.3 Cliente de Escritorio Remoto Windows y VNC

- **Entorno KDE**: herramienta *krdc*: permite acceder a un escritorio remoto perteneciente a un sistema operativo Microsoft Windows o GNU/Linux. Por ejemplo, si desea utilizarlo en OpenSuSE requerirá la instalación del paquete *kde4-krdc* y podremos acceder a ella mediante el grupo de aplicaciones "Sistema". En Fedora se instala con el paquete *kdenetwork* y se accede mediante "Aplicaciones | | Internet | | Cliente de escritorio remoto". En el campo "Escritorio remoto" seleccionaremos de la lista el protocolo a utilizar (*rdp* para escritorio Windows o *vnc* para escritorio Linux), el equipo remoto con el que se quiere. Posteriormente nos permitirá modificar parámetros adicionales como la calidad de la conexión mediante un cuadro de diálogo. Finalmente requerirá una nombre de usuario y una contraseña para autenticarnos en el equipo remoto y mostrar su escritorio (véase Figura 5.13).

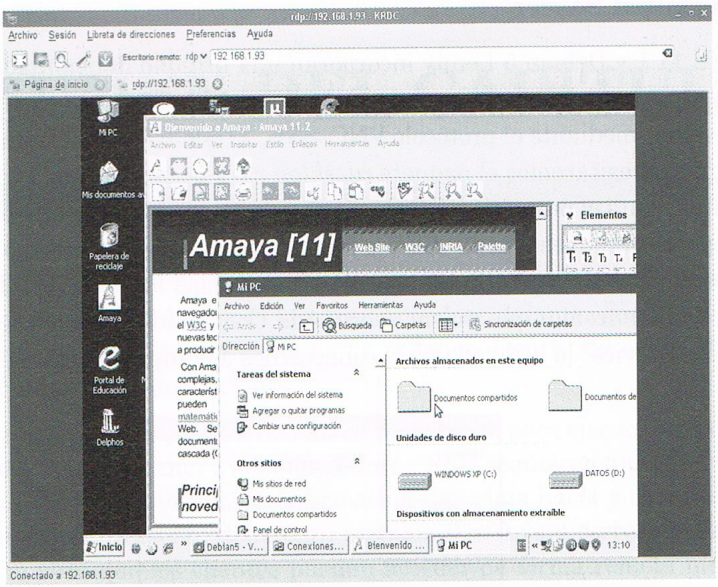


Figura 5.13. *Cliente de Terminal Server Linux tsclient. En este ejemplo se aprecia el acceso del usuario habitual al equipo con dirección IP 10.0.1.93, y se autenticará en dominio.com. En este caso la conexión se realiza utilizando el protocolo RDP, aunque también admite otros protocolos*

- **Entorno GNOME**: herramienta *gnome-rdp*: en Debian 5 Lenny requiere la instalación del paquete del mismo nombre. La podremos utilizar accediendo a "Aplicaciones || Internet || Gnome-RDP" y pulsaremos sobre el botón "New" para indicar mediante el grupo de parámetros "General", el nombre de la conexión, el protocolo a utilizar (RDP, VNC o SSH), el equipo, usuario y su contraseña. Además, mediante el grupo de parámetros "RDP", podremos configurar una conexión con un equipo Microsoft Windows, especificando el tamaño del escritorio remoto, la profundidad de colores o el tipo de teclado. También existen otras herramientas gráficas para el acceso a un servicio VNC para entornos GNOME, como por ejemplo *Vinagre*.
- **Mediante línea de órdenes**: como alternativa a las herramientas gráficas podemos utilizar la orden *vncviewer* tal y como se ilustra en el ejemplo 5.7, para acceder al escritorio de un equipo remoto. Para utilizarlo se requiere el paquete *tightvnc* en OpenSuSE, *tigervnc* en Fedora y *xtightvncviewer* en Debian.

EJEMPLO 5.7

Deseamos utilizar un cliente VNC para acceder a un servidor GNU/Linux cuya dirección IP es la 10.0.1.93.

Desde una consola de terminal, ejecutaremos la orden:

```
$ vncviewer
```

Se solicitará el host remoto con el que queremos conectar. Indicaremos el 10.0.1.93 y el nº de terminal el 1. A continuación introducimos la contraseña de conexión:

```
Host: 10.0.1.93:
Password: *******
```

Aparecerá una ventana desde la que veremos el escritorio del usuario remoto y con el cual podremos interactuar.

5.3.2.4 Cliente de Terminal Server

Fedora 11, OpenSuSE 11.1 y Debian 5 Lenny incorporan una utilidad denominada "Cliente de Terminal Server" para inicio de sesiones remotas gráficas con un servidor Windows utilizando el protocolo RDP, aunque también permite establecer conexiones mediante el protocolo VNC, SSH, XDMCP o HTTP. Esta herramienta requiere instalar el paquete *tsclient*, además necesitaremos el paquete *rdesktop* para poder acceder a sistemas operativos Windows de forma remota, ya que implementa el protocolo RDP. Puede acceder a esta herramienta desde "Aplicaciones | | Internet" en Fedora y desde el grupo "Sistema" en OpenSuSE. La información que se proporciona a esta herramienta se asemeja a la proporcionada a un cliente de Escritorio Remoto Windows (véase Figura 5.14). Previamente nos aparecerá un cuadro de diálogo, en el que tendremos que pulsar sobre "Add Connection" e indicar el protocolo a utilizar, siendo la opción "Windows Terminal Service" la utilizada para conectarnos a equipos Windows.

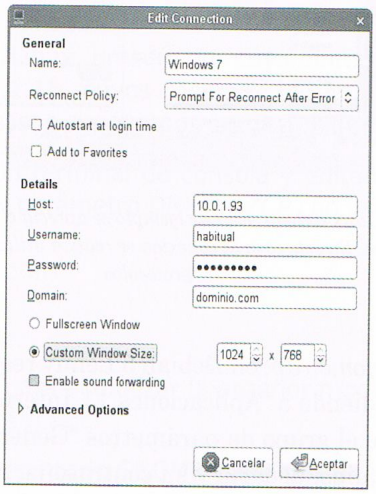


Figura 5.14. *Ejemplo de conexión remota de escritorio en Linux. En este ejemplo se aprecia el acceso a un sistema operativo Windows desde un sistema operativo Linux. En este caso se ha utilizado el protoco RDP mediante la herramienta krdc*

5.3.2.5 Cliente de acceso remoto mediante interfaz Web

Al igual que se vio en el apartado correspondiente para Microsoft Windows, desde GNU/Linux también se puede tener acceso a un servidor remoto mediante VNC utilizando un navegador HTTP. Como requisito, debe tener activa la ejecución de applets de Java en el navegador, además de tener instalada el plugin para JRE para el navegador a utilizar.

Para acceder al equipo remoto se indicará como URL el servidor al que quiere acceder, seguido de dos puntos y el puerto de acceso, sumándole en su caso el número de terminal. Por ejemplo si queremos utilizar el terminal número uno, indicaríamos como URL *http://Servidor:5801*. También se puede utilizar la herramienta *tsclient*, seleccionando de la lista el protocolo "Web" al crear la nueva conexión mediante el botón "Add connection".

RESUMEN DEL CAPÍTULO

El servicio de Terminal Remoto mediante diversos tipos de software, permite el acceso a un equipo distante para que el usuario interactúe con él como si estuviese delante. Distinguimos dos modos de hacerlo, mediante entorno gráfico, y mediante línea de órdenes. Dentro de este servicio encontramos diversos protocolos que lo implementan, a destacar:

- **Telnet, Rlogin y SSH**: permiten el acceso a un equipo remoto para ejecución de órdenes. Requieren utilizar un usuario para la conexión y, además, *Telnet* y *SSH* requieren una contraseña. A diferencia de *Telnet* y *Rlogin*, *SSH* encripta toda la información que viaja hacia y desde el servidor, incluido el nombre de usuario y contraseña. Requieren instalar el software correspondiente en el servidor y activar el servicio para que los clientes puedan acceder de forma remota mediante un usuario del servidor. Los clientes pueden acceder al servidor mediante línea de órdenes, aunque existen programas que también lo permiten emulando una consola de terminal, como el programa PuTTy para Windows. También encontramos software cliente que nos permiten las transferencias seguras mediante SSH, como es el caso de WinSCP para Microsoft Windows, o el navegador Konqueror en GNU/Linux mediante el kioslave *fish*.
- **X-Terminal**: utiliza el protocolo XDMCP para pemitir a un cliente GNU/Linux el acceso a otro equipo remoto GNU/Linux e interaccionar con él mediante el inicio de una sesión en el entorno gráfico, o bien ejecutar aplicaciones gráficas en un servidor remoto, pero visualizadas en el equipo cliente para interactuar con ellas.
- **Escritorio remoto mediante VNC**: permiten el acceso a un escritorio de un equipo remoto utilizando el protocolo VNC. Existe una amplia variedad de sofware de carácter carácter libre para distintas plataformas, que permite ofrecer este servicio así como utilizarlo. Tal es el caso de *tightvnc* o *Vino*. Este protocolo es ampliamente utilizado para el acceso a escritorios remotos de equipos GNU/Linux para su administración.
- **Terminal Server**: este servicio es proporcionado por equipos Microsoft Windows, especialmente las versiones Server, y admite dos modos de funcionamiento. El de *administración remota*, que utiliza el protocolo RDP para que los clientes tomen el control del escritorio del servidor remoto, habitualmente para realizar tareas administrativas. El de *servidor de aplicaciones*, disponible solo en versiones Server, permite compartir aplicaciones instaladas en el servidor con clientes, cuyo hardware es insuficiente para ejecutarlas. Las versiones Server disponen de una herramienta administrativa para la gestión de escritorios remotos y, además, permiten la configuración de los perfiles de usuario para ver o interactuar con su sesión. GNU/Linux dispone de la herramienta *Terminal Server Client* que permite el acceso a escritorios remotos de equipos Microsoft Windows mediante el protocolo RDP, aunque también admite otros protocolos como HTTP o SSH para accesos remotos.
- **Acceso remoto mediante interfaz web**: algunos de los protocolos anteriormente mencionados como VNC, permiten el acceso al servicio mediante el protocolo HTTP. VNC además del puerto que utiliza por defecto, abre otro para atender las solicitudes vía web mediante navegador. Los sistemas operativos Windows XP, 2003 y 2008, permiten instalar un componente adicional al servicio HTTP, depositando un control *ActiveX* en el sitio web. Los clientes que accedan al servidor web de los mencionados sistemas operativos, lo instalarán en sus navegadores (Internet Explorer) para acceder a equipos remotos. Windows 2003 Server también permite un modo de configuración para su administración remota mediante web, permitiendo la modificación de diversos parámetros de configuración.

EJERCICIOS PROPUESTOS

Para la realización de los ejercicios se partirá de la Figura 5.15. Tenga en cuenta que se han omitido routers, módems u otros dispositivos para conexión a Internet.

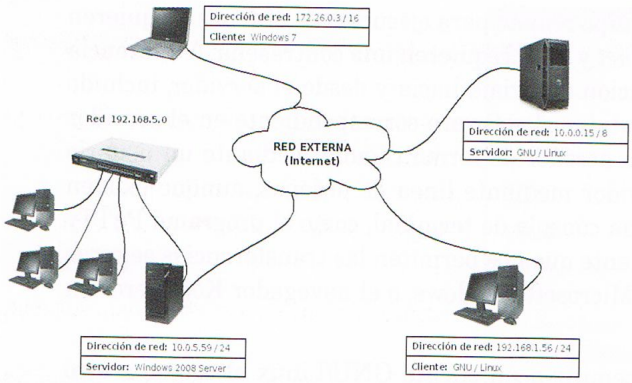


Figura 5.15. *Varios equipos y redes locales conectadas a Internet*

1. Suponiendo que el cliente Windows dispone de un archivo denominado *noticias.pdf* que quiere ubicar en el servidor Linux para su publicación mediante FTP, indique los pasos a seguir teniendo en cuenta las siguientes consideraciones:

- El cliente Windows dispone de las herramientas PuTTy y WinSCP.
- Tanto en el servidor como en el cliente Linux tienen habilitado el servicio SSH.
- El servidor Linux solo permite el acceso desde el cliente Linux, a pesar de que el cliente Windows conoce la contraseña del administrador del servidor Linux.
- El usuario Windows dispone del usuario *remoto* para acceder al cliente Linux.
- El usuario Windows deberá copiar el fichero desde el directorio *C:\upload*.

2. Respecto al ejercicio anterior, imagine que se encuentra sentado delante del cliente Linux en el cual se ha autenticado como el usuario *remoto*. Desea acceder al servidor Linux, ¿cómo hubiera copiado el citado fichero sin utilizar órdenes a su directorio personal? Enumere dos alternativas posibles.

3. Deseamos administrar de forma remota el servidor Linux. Indique alguna forma de conseguirlo. ¿Qué podría hacer para que la administración remota fuera segura?

4. Utilice VNC desde cualquier cliente para establecer una conexión remota con el servidor GNU/Linux.

5. Utilice el cliente de Terminal Server de GNU/Linux para poder acceder de forma remota al servidor Windows mediante el usuario *remoto*.

6. El cliente GNU/Linux necesita acceder al servidor Microsoft Windows para realizar tareas administrativas, pero no dispone de ninguna herramienta para acceder a un escritorio Microsoft Windows ni GNU/Linux. Sin embargo, dispone de acceso al servidor GNU/Linux mediante SSH a través del usuario *remoto*, y el servidor GNU/Linux dispone de la herramienta Krdc. Indique los pasos a seguir para administrar el servidor Microsoft Windows sabiendo que se dispone del usuario *mantenimiento* cuya contraseña conocemos.

7. Los equipos Microsoft Windows de la red 192.168.5.0 necesitan realizar tareas administrativas sobre el servidor Microsoft Windows, pero su versión de sistema operativo impide utilizar el software cliente de escritorio remoto y solicitan al administrador del sistema la gestión del servidor mediante interfaz web. Suponiendo que el administrador se encuentra en el cliente Microsoft Windows realizando tareas de mantenimiento, indica los pasos que se han de seguir para que se pueda administrar el servidor mediante un navegador.

8. El servidor Microsoft Windows se ha configurado como servidor web y las páginas y archivos necesarios los alojan los clientes mediante FTP. Puesto que el servicio FTP no es seguro, se decide reemplazarlos por el servicio SSH. Indica los pasos para instalarlo desde el cliente GNU/Linux suponiendo que el servidor tiene activado el acceso a su escritorio de forma remota.

9. El servidor GNU/Linux utiliza un entorno de escritorio GNOME y está configurado para admitir inicio de sesiones gráficas remotas mediante XDMCP. Suponiendo que nos encontramos en el cliente GNU/Linux, indica los pasos a seguir para permitir el acceso mediante VNC al servidor mencionado.

10. ¿Cómo demostrarías que las aplicaciones X-Window de un servicio de X-Terminal se ejecutan en el servidor a pesar de visualizarse en el cliente? Pon un ejemplo.

TEST DE CONOCIMIENTOS

1 Ordena de menor a mayor el grado de seguridad de los protocolos Telnet, SSH y RLogin.
- a) Telnet, SSH y RLogin.
- b) Telnet, RLogin y SSH.
- c) RLogin, Telnet y SSH.
- d) SSH, RLogin y Telnet.

2 El protocolo SSH:
- a) Solo se utiliza para conexiones remotas.
- b) Solo se puede utilizar mediante la herramienta PuTTy.
- c) Siempre requiere el paquete OpenSSH para su funcionamiento.
- d) Sirve de soporte a otros protocolos para proporcionarles seguridad.

3 En el modo de aplicaciones X Window remotas del servicio X-Terminal, las aplicaciones:
- a) Se ejecutan en el servidor y se visualizan en el cliente.
- b) Se ejecutan en el cliente y se visualizan en el cliente.
- c) Las ejecuta el cliente en el servidor pero se visualizan en el cliente.
- d) a y c son correctas.

4 El acceso a un escritorio mediante VNC:
- a) También se puede realizar a Microsoft Windows.
- b) Solo permite el acceso a equipos GNU/Linux.
- c) Necesita instalar software que requiere el pago de licencia.
- d) Ninguna de las anteriores.

5 El software de Terminal Server:
- a) Solo permite el acceso a un escritorio remoto mediante RDP.
- b) Viene preinstalado en las versiones Server de Microsoft Windows.
- c) Solo permite la ejecución de aplicaciones.
- d) Suele venir preinstalado el software de escritorio remoto.

6 El acceso remoto a escritorios Windows Interfaz Web:
- a) Requiere equipos intermediarios que proporcionen el servicio HTTP.
- b) Requiere la apertura de puertos especiales, además del utilizado por RDP.
- c) Requiere instalar en el navegador del servidor un control ActiveX.
- d) Ninguna de las anteriores.

7 La herramienta PuTTy es:
- a) Un emulador de terminal que solamente permite iniciar y guardar sesiones Telnet.
- b) Un emulador de terminal solamente para establecer sesiones SSH.
- c) Un emulador de terminal multiprotocolo que no permite guardar sesiones.
- d) Ninguna de las anteriores.

8 Las herramientas asociadas al protocolo VNC son:
- a) Vino, Tightvnc y Krfb.
- b) TSclient, Tightvnc y Gdm.
- c) Vino, Krdc y Gnome-rdp.
- d) Vino, Vinagre y Tightvnc.

9 Las herramientas GNU/Linux asociadas al protocolo RDP son:
- a) Vino, Krfb y Krdc.
- b) Krdc, TSClient y Gnome-rdp.
- c) Krdc, Krfb y TSClient.
- d) KSSH, HotSSH y Gnome-rdp.

6 Los servicios de correo electrónico

OBJETIVOS DEL CAPÍTULO

- ✓ Describir los diferentes protocolos que intervienen en el envío y recogida del correo electrónico.
- ✓ Conocer los mecanismos que se pueden utilizar para mantener la privacidad de los mensajes.
- ✓ Describir los métodos para filtrar y eliminar los virus y el correo basura.
- ✓ Usar clientes de correo electrónico para enviar y recibir correo.

El sistema de gestión de correo electrónico se ha convertido hoy en día en un servicio imprescindible para los usuarios de Internet. Gracias a él, es posible distribuir mensajes de correo de forma masiva y a nivel mundial.

Este capítulo está dedicado a explicar el funcionamiento del sistema de gestión de correo electrónico y los protocolos involucrados. También incluye una descripción detallada de cómo se realiza el acceso a este servicio desde los sistemas operativos Microsoft Windows y GNU/Linux.

El servicio de correo electrónico (*e-mail*) consiste en el envío y recepción de mensajes de texto (además de un conjunto de *archivos adjuntos*) desde un usuario origen a otro destino, sin necesidad de que el destinatario se encuentre conectado y disponible para su recepción. Aunque el servicio de correo electrónico se puede diseñar como un sistema de transferencia de archivos, éste último carece de algunas características que lo diferencian del anterior:

- Es posible transmitir un mensaje a un grupo de usuarios a la vez.
- La información de un mensaje está bastante estructurada y se incluye el nombre y dirección del emisor y el destinatario y la fecha y hora de envío. Las direcciones suelen tener el formato siguiente: *nombre_usuario@nombre_equipo.dominio*.
- Es más fácil de utilizar por los usuarios, ya que todo el programa de envío de correo está integrado en una sola aplicación.

6.1 INTRODUCCIÓN

El sistema de gestión de **correo electrónico** (*e-mail*) funciona desde la aparición de las primeras redes de comunicaciones con el propósito de permitir que los usuarios puedan intercambiar mensajes de texto. Los primeros sistemas resultaban muy simples, difíciles de utilizar y ofrecían unas funciones bastante pobres. Posteriormente aparecieron nuevos protocolos que facilitaban la interacción con los usuarios y ofrecían funciones adicionales.

La función principal de un sistema de correo electrónico consiste en el envío de mensajes entre usuarios, de forma que son recibidos en el momento en el que se conectan a la red. Otras características que ofrecen la mayoría de los protocolos de gestión de correo electrónico que funcionan hoy en día son:

- Es posible enviar un mismo mensaje a un grupo de usuarios. Esto se puede hacer de dos formas distintas: especificando varias direcciones en el campo de destino del mensaje o utilizando el sistema de **listas de correo**, que envían los mensajes a todos los usuarios que pertenecen a ellas.
- Existen mecanismos que informan al emisor si el receptor ha recibido correctamente el mensaje o incluso si lo ha leído.
- Los mensajes tienen una estructura interna bien definida, con campos que incluyen la dirección del destinatario, título del mensaje, cuerpo (texto), etc.
- Se han diseñado interfaces de usuario para facilitar el envío y recepción del correo.
- El mensaje puede incluir información no textual, como imágenes o sonidos.
- Los usuarios pueden reenviar a otros usuarios los mensajes que reciben.
- Es posible que los usuarios puedan consultar el correo eletrónico desde cualquier lugar y equipo, a través de la utilización de los **buzones de correo**.

Los pasos básicos que se realizan cuando se envía un mensaje de correo desde un origen a un destino son los siguientes:

1. Composición del mensaje con sus diferentes partes.
2. Transferencia del mensaje desde el origen al destino.
3. Generación de una confirmación del envío, indicando si llegó correctamente a su destino.
4. Presentación del mensaje al usuario receptor.
5. Tratamiento del mensaje una vez leído.

Existen varios estándares de servicios de gestión de correo electrónico **X.400** y **X.500** del antiguo CCITT (ahora ITU), **MOTIS** de OSI (basado en los protocolos anteriores) o **MHS** (*Message Handling Service* o Servicio de Gestión de Mensajes) incluido en las redes Novell NetWare. Sin embargo, los protocolos de gestión de correo electrónico que más se utilizan hoy en día son los incluidos en la arquitectura TCP/IP de Internet.

En este capítulo se explican los protocolos de la arquitectura TCP/IP involucrados en la gestión de correo electrónico porque son los que más se utilizan hoy en día con diferencia. Los protocolos definidos por el CCITT o ISO han dejado de utilizarse porque su especificación resultó demasiado compleja como para ser llevada a la práctica. Otros protocolos como MHS han quedado reducidos al ámbito de las redes locales, por lo que su uso no se ha extendido.

6.2 PROTOCOLOS INVOLUCRADOS

El sistema de gestión de correo electrónico de Internet se basa en la utilización de dos tipos de agentes que gestionan los mensajes de correo:

- **MUA** (*Mail User Agent* o Agente de Usuario de Correo): se encargan de interaccionar con los usuarios para enviar o recibir sus mensajes. Normalmente tienen la forma de servicios y programas con menús y opciones. Ejemplos de agentes son el programa Outlook de Microsoft y *mail* de Linux.
- **MTA** (*Mail Transfer Agent* o Agente de Transferencia de Correo): su tarea es la de enviar los mensajes desde el origen hasta el destino a través de la red de comunicación. Suelen ser programas de tipo *demonio* que ejecutan los protocolos de envío de correo.

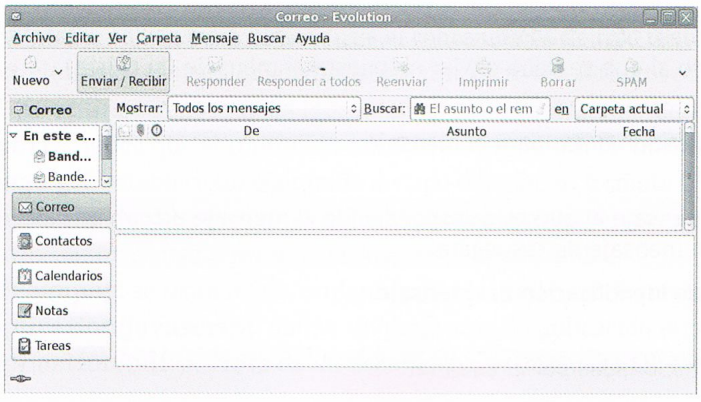


Figura 6.1. *Ejemplo de agente de usuario Evolution. Este agente de interfaz gráfica, distribuido bajo licencia GPL, facilita enormemente la interacción con los usuarios*

Los dos agentes de correo que gestionan los mensajes funcionan de una forma análoga a como trabaja el sistema de correo convencional por carta. Por un lado, se encuentra la infraestructura de transporte de correo a larga distancia, que actúa como el MTA. Por otro lado, funciona el reparto de correo local a cada buzón, que actúa como el MUA.

Son varios los protocolos involucrados en la transferencia de correo en Internet, todos ellos definidos en los documentos RFC. Los más importantes se explican en los apartados siguientes.

6.2.1 FORMATOS DE MENSAJES

El formato de los mensajes de correo electrónico está definido en el estándar RFC 822. Básicamente, un mensaje de correo electrónico está dividido en dos partes: la **cabecera** y el **cuerpo**. El cuerpo contiene el mensaje de texto, mientras que la cabecera está dividida en varios campos, todos ellos se explican en la tabla 6.1.

Tabla 6.1. Campos que forman la cabecera de un mensaje según RFC 822

Campo	Descripción
From: (De)	Nombre del usuario creador del mensaje.
To: (A)	Nombre de los usuarios receptores (separados por comas). Tienen la forma *usuario@equipo.dominio*.
Cc: (Copia al Carbón)	Nombres de otros usuarios secundarios que también recibirán el mensaje. Se trata de un sistema anticuado de "copia al carbón" que indicaba que los receptores recibirían una "copia en sucio" y que todavía se sigue utilizando.
Bcc: (Copia al Carbón Ciega)	Nombres de otros usuarios que van a recibir el mensaje. Se utiliza para que el resto de usuarios receptores del mensaje no sepan que también se van a enviar a estos. Cuando se envía un mensaje con varios destinatarios en el campo *To*, los que lo reciben también pueden ver la lista completa de destinatarios.
Sender: (Desde)	Nombre del usuario que envía el mensaje. Normalmente coincide con el campo *From*, pero puede tratarse de un usuario diferente.
Received: (Recibido)	Campo añadido por cada agente de transferencia en la ruta desde el origen al destino. Normalmente no se utiliza.
Return-Path: (Ruta de Regreso)	Se puede utilizar para establecer una ruta de regreso al remitente.
Subject: (Sujeto)	Resumen corto del mensaje para exhibir al usuario receptor. Los programas de gestión de correo suelen mostrar este campo junto con el nombre del usuario emisor en la lista de mensajes de correo entrante. Por esta razón, este campo es muy importante ya que es lo primero que lee el usuario receptor.
Date: (Fecha)	Fecha y hora de envío del mensaje.
Reply-To: (Responder a)	Nombre del usuario al que se debe enviar respuesta al mensaje (si existe).
Message-Id: (Identificador)	Número de identificación único para el mensaje.
In-Reply-To: (En Respuesta A)	Identificador del mensaje al que está respondiendo el mensaje actual, en caso de que se trate de un mensaje de respuesta.
References: (Referencias)	Otra información de identificación del mensaje.
Keywords: (Palabras Clave)	Palabras clave seleccionadas por el usuario.

Los campos que utilizan nombres de usuario utilizan el sistema DNS para identificarlos, que consiste en la composición de un nombre de usuario, nombre de equipo y dominio, todo ello separado por el carácter "@". Esto quiere decir que el correo electrónico no puede funcionar sin el apoyo del sistema de nombres de dominio. Un ejemplo de dirección de correo eletrónico puede ser el siguiente:

usuario@equipo.dominio

Los campos *From* y *Sender* se utilizan para poder distinguir al usuario que creó el mensaje del usuario que lo envió, pero suele ocurrir que se trate de la misma persona. Los campos *Received* y *Return-Path* pueden ser completados por los distintos agentes de transferencia por donde pasa el mensaje, pero muchas veces no lo hacen y solamente aparece el nombre del emisor. El campo *Reply-To* se usa para indicar el nombre de usuario que debe recibir la respuesta, que puede ser distinto del usuario que redactó el mensaje o el que lo envió.

Según el estándar RFC 822, los usuarios también pueden crear sus propias cabeceras de uso personal. Estas cabeceras deben nombrarse anteponiendo los caracteres "X-" y se incluyen con el texto del mensaje. En caso de que el programa cliente del usuario receptor no sepa interpretarlas, entonces las mostrará como parte del cuerpo del mensaje.

Para permitir el uso de mensajes con diferentes códigos de caracteres y contenidos no textuales (imágenes y sonidos), se desarrolló el estándar RFC 1341, se actualizó en RFC 1521 y, posteriormente, se volvió a actualizar en RFC 2045 y RFC 2046. A estos estándares se les conoce comúnmente como **MIME** (*Multipurpose Internet Mail Extensions* o Extensiones Multipropósito de Correo de Internet). Mediante este sistema, los mensajes siguen teniendo la estructura definida en el RFC 822, pero se añaden nuevos campos al cuerpo del mensaje. De esta forma, los agentes de transferencia de correo siguen siendo válidos, aunque es necesario modificar los agentes de usuario para poder manejar estas extensiones. En la tabla 6.2 se explican los nuevos campos que añaden las extensiones MIME.

Tabla 6.2. Campos de las extensiones MIME

Campo	Descripción
MIME-Version:	Se usa para identificar la versión MIME utilizada.
Content-Description:	Describe el contenido del cuerpo del mensaje.
Content-Id:	Se usa como identificador único del contenido.
Content-Transfer-Encoding:	Indica el sistema utilizado para codificar el texto del mensaje. Puede ser ASCII, base64, etc.
Content-Type:	Se usa para describir la naturaleza del mensaje. Puede ser *Text*, *Image*, *Audio*, *Video*, *Application*, *Message* o *Multipart*. A su vez, estos tipos se dividen en distintos subtipos.

Algunos ejemplos del contenido del campo *Content-Type* son:

- **text/plain**: se usa para indicar que el contenido es de tipo texto sin formato.
- **text/richtext**: se trata de un contenido tipo texto con formato e incluye tipos, tamaños, sangrías, justificaciones, etc. Se utilizan unas marcas iguales a las utilizadas por el metalenguaje HTML.
- **text/rtf**: indica que el contenido es texto en formato RTF (formato de texto enriquecido).
- **image/gif**: establece un contenido de tipo imagen en formato GIF.
- **image/jpg**: establece un contenido de tipo imagen en formato JPG.
- **audio/basic**: se usa para indicar un contenido de audio.
- **video/mpeg**: se trata de un contenido de tipo vídeo con formato MPEG.
- **application/javascript**: define un programa de aplicación escrito en código JavaScript.
- **application/pdf**: se trata de un documento en formato PDF de Adobe.

6.2.2 TRANSFERENCIA DE CORREO

En general, el sistema de transferencia de correo se encarga de enviar el mensaje desde el origen al destino utilizando para ello los protocolos de transporte definidos (por ejemplo, TCP). Sin embargo, en algunas circunstancias pueden ser necesarios protocolos adicionales para facilitar la gestión por los usuarios. En los siguientes apartados se explican los protocolos usados en Internet.

6.2.2.1 Protocolo sencillo de transferencia de correo (SMTP)

Para transmitir el correo a través de la red se utiliza un protocolo bastante sencillo que se limita a establecer una conexión entre el equipo origen y el destino, enviar los datos y desconectar. Este protocolo se llama **SMTP** (*Simple Mail Transfer Protocol* o Protocolo Simple de Transferencia de Correo) y está definido en RFC 821.

Para que esa transferencia sea posible, los dos equipos deben ejecutar un programa de tipo *demonio* que se encargue de controlar todo el proceso. La Figura 6.2 muestra un diagrama simplificado de los mensajes que se envían un emisor y un receptor de correo electrónico.

El diagrama de transmisión especificado en la Figura 6.2 se repetirá tantas veces como equipos intermedios existan entre el emisor y el receptor. También puede ocurrir que el mensaje se envíe a múltiples destinatarios, por lo que existirán varios mensajes "Para ...". Algunos de estos destinatarios pueden ser rechazados si sus nombres no son correctos o no existen en el destino.

En caso de que se produzca algún error durante la transmisión del mensaje, el sistema de correo puede enviar un mensaje de respuesta al usuario que lo envió indicando los posibles problemas. Cuando los sistemas de correo están correctamente instalados y configurados, estos mensajes suelen ser debidos a nombres incorrectos o a que los buzones de los destinatarios han superado el tamaño máximo de almacenamiento permitido. Sin embargo, cuando se instala un nuevo sistema de correo, estos mensajes resultan de mucha utilidad para depurar errores de configuración.

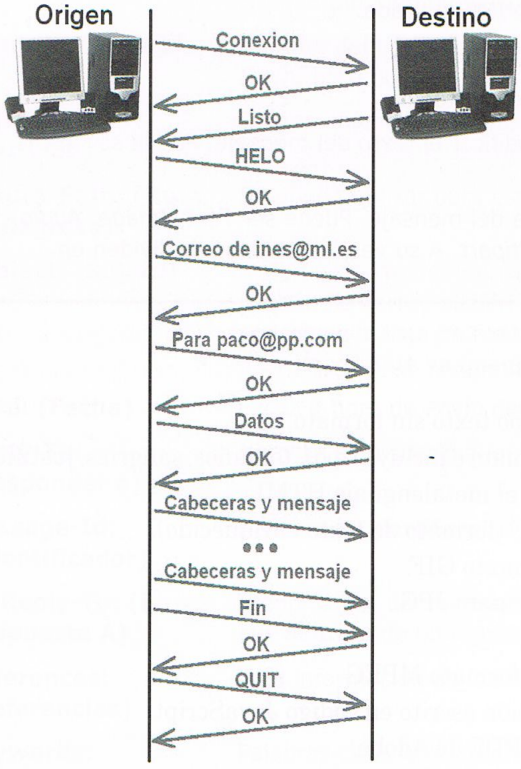


Figura 6.2. *Esquema de transferencia de correo entre dos equipos usando SMTP. Como se puede observar, el equipo emisor es el que establece la conexión, pero es el equipo receptor el que establece cuándo puede comenzar la transmisión del mensaje. Los mensajes titulados "Cabeceras y mensaje" son los que realmente contienen la información del correo enviado*

Si deseamos que nuestro servidor de correo electrónico esté disponible en Internet, entonces será necesario asignarle un dominio válido (contratado a alguna empresa que ofrezca estos servicios). También es necesario que el puerto número 25 (utilizado por el protocolo SMTP) esté abierto en el servidor, por lo que hay que permitir las conexiones en el cortafuegos o encaminador.

Este sistema de transferencia de correo funciona bien cuando los usuarios consultan el correo directamente en los equipos que ejecutan los procesos *demonio* de correo. Sin embargo, esta situación no resulta práctica debido a que resulta complejo instalar y configurar el sistema de correo en los equipos, deben tener conexión permanente con Internet y los usuarios no pueden consultar el correo desde cualquier otro lugar con un equipo distinto. Para solucionar estos problemas, se han diseñado otros protocolos de entrega de correo que permiten transferir los mensajes desde un equipo que envía y recibe mensajes con SMTP (servidor de correo) a otros equipos de usuario que no entienden este protocolo y solo necesitan conectarse con ese servidor de forma esporádica. Estos protocolos se explican en el apartado siguiente.

6.2.2.2 Entrega a los usuarios finales

Aunque no es estrictamente necesario, resulta muy común que las organizaciones trabajen con equipos dedicados al envío y recepción de correo electrónico (denominados comúnmente servidores de correo electrónico). Cuando los usuarios desean consultar su correo o enviar un mensaje, pueden hacerlo desde sus equipos de escritorio (clientes de correo) realizando una conexión con el servidor de correo. De esta forma, pueden consultar su correo desde cualquier equipo y lugar (siempre que puedan conectarse con el servidor).

Los programas agentes de usuario pueden trabajar directamente sobre el servidor de correo o también lo pueden hacer en un equipo cliente utilizando los protocolos de entrega final para acceder al servidor. Por ejemplo, el programa Microsoft Outlook u otros programas similares (Figura 5.1), se instalan en un equipo cliente y son capaces de conectar con un servidor para descargar el correo en los equipos de los usuarios.

Para que los clientes puedan establecer una conexión con el servidor de correo son necesarios otros protocolos de comunicación. Los protocolos más utilizados que realizan esta función son **POP3** (*Post Office Protocol* o Protocolo de Oficina Postal) e **IMAP** (*Interactive Mail Access Protocol* o Protocolo Interactivo de Acceso a Correo). POP3 funciona transfiriendo los mensajes de correo desde el buzón del equipo servidor al cliente, mientras que IMAP no lo hace, de forma que el buzón central permanece en el servidor y los mensajes pueden consultarse desde distintos equipos. POP3 está definido en el estándar RFC 1225 y funciona sobre el puerto 110, mientras que IMAP está definido en RFC 1064 y funciona sobre el puerto 143. Tenga en cuenta que debe activar estos puertos si dispone de un cortafuegos o encaminador entre el servidor de correo y los clientes.

Además de estos protocolos, muchos sistemas de gestión de correo electrónico incluyen la posibilidad de consultar el correo utilizando un navegador de hipertexto. Esto se consigue ya que existen algunos lenguajes de diseño de páginas dinámicas que incluyen funciones para el acceso a los buzones de correo. De esta forma, los usuarios tienen todo el sistema de gestión de correo instalado y configurado en el servidor y solamente deben preocuparse de acceder a él a través de un programa navegador de Internet, por lo que no necesitan realizar ninguna configuración en su equipo.

6.2.3 SEGURIDAD Y PRIVACIDAD

Existen problemas de seguridad y privacidad en los mensajes de correo electrónico por dos razones fundamentales:

- Los mensajes circulan libremente por la red de un origen a un destino y pueden ser interceptados en su camino.
- Los protocolos de transferencia de correo envían los mensajes en texto claro, es decir, sin cifrar.
- El nombre de origen puede ser manipulado, de forma que a veces no se puede comprobar la identificación de la persona que envía un mensaje.

Para solucionar los problemas de seguridad y privacidad de los mensajes, se pueden utilizar algunas herramientas disponibles con los programas cliente de correo electronico o paquetes auxiliares que son capaces de trabajar con los protocolos de gestión de correo que se han explicado en los apartados anteriores.

Uno de los paquetes más utilizados en el correo electrónico para ofrecer seguridad y privacidad es **PGP** (*Pretty Good Privacy* o Bastante Buena Confidencialidad). Este sistema fue diseñado por Phil Zimmermann, que lo distribuyó de forma gratuita en Internet (incluso el código fuente). PGP es multiplataforma (Windows, Linux, etc.) y está definido en RFC 1991, RFC 2015 y RFC 2440. Actualmente, la versión oficial de PGP no se distribuye libremente, pero se puede obtener una versión libre denominada **GPG** o **GnuPG** (*GNU Privacy Guard* o Guardián de Privacidad GNU), que está basado en el estándar OpenPGP del IETF.

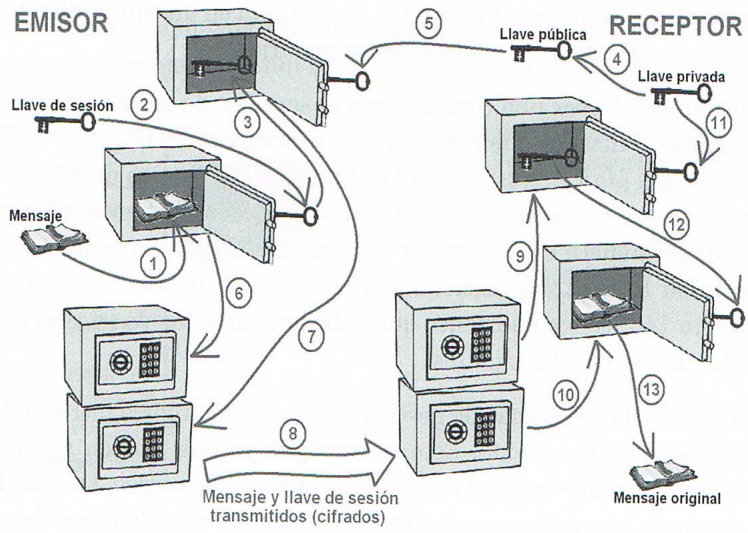


Figura 6.3. *Funcionamiento del protocolo PGP de cifrado de mensajes de correo. Los números indican el orden de las operaciones. Obsérvese que el cifrado de la llave de sesión es asimétrico, lo que significa que se usa una clave para el cifrado (usando la llave pública) y otra clave distinta para el descifrado (con llave privada)*

Como se muestra en la Figura 6.3, PGP envía el mensaje cifrado junto con la clave de cifrado (*llave de sesión*) también cifrada. La operación de cifrado de la llave de sesión se realiza con una *clave pública* suministrada por el receptor, mientras que el descifrado de esta llave se realiza con una *clave privada*, que solamente conoce el receptor y que no debe distribuir a nadie.

EJEMPLO 6.1

Veamos cuáles son los pasos a seguir para instalar GnuPG sobre un equipo GNU/Linux y generar las claves privada y pública. Estos son:

1. El primer paso consiste en instalar el paquete correspondiente, que se llama *gnupg*. En la mayoría de las distribuciones actuales, este paquete ya viene instalado por defecto.
2. A continuación, el usuario tiene que generar sus claves, para lo que tiene que ejecutar la siguiente orden en el intérprete de órdenes:
   ```
   $ gpg --gen-key
   ```
3. La orden anterior inicia un asistente para contestar a varias preguntas. Los parámetros a introducir son:
   - **Tipo de clave**: especifica el algoritmo que se va a utilizar para el cifrado. El tipo "DSA y ElGamal" es el preferido por tratarse de una versión libre.
   - **Tamaño de la clave**: el valor preferido es 2048 bytes y, si se pone un valor mayor, entonces la clave es más segura, pero requiere más tiempo para generarla, además de para cifrar y descifrar los mensajes.
   - **Validez de la clave**: tiempo en el que la clave que se va a generar es válida.
   - **Nombre y apellidos**: se usa para identificar al propietario de la clave.
   - **Dirección de correo electrónico**: dirección del propietario de la clave.
   - **Comentario**: un comentario que describe la clave.
   - **Contraseña**: se especifica una contraseña para la clave, que solamente debe conocer el propietario.
4. Durante la fase de generación de la contraseña es recomendable abrir otras ventanas y trabajar con otros programas, así el sistema puede generar números aleatorios con un mayor desorden (entropía). Si todo va bien, al final se mostrará el mensaje "Claves pública y secreta creadas y firmadas". En caso de que las claves creadas no se hayan firmado, hay que ejecutar las siguientes órdenes, donde *dirección* especifica la dirección de correo electrónico que hemos indicado al generarlas:
   ```
   $ gpg --edit-key dirección
   > sign
   ```
5. Se pueden consultar las claves disponibles usando la siguiente orden:
   ```
   $ gpg --list-keys
   ```

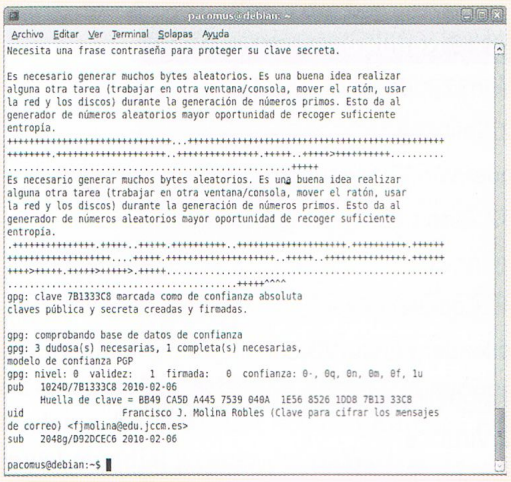


Figura 6.4. *Generación de las claves privada y pública con la orden gpg en Debian 5. Aunque estas claves se han generado a modo de prueba, no es recomendable facilitar la información que aquí aparece si se van a utilizar para enviar mensajes comprometidos*

Si queremos distribuir nuestra clave pública para que otras personas puedan enviarnos correos cifrados, tenemos que seguir estos pasos:

1. Abrimos el archivo *options* que se encuentra dentro de la carpeta *.gnupg*, a su vez ubicada dentro de la carpeta personal del usuario (habitualmente es */home/usuario*).
2. En el archivo *options*, añadimos la siguiente línea, que corresponde a un servidor gratuito de Internet donde podemos alojar nuestra clave pública:
   ```
   keyserver pgp.rediris.es
   ```
3. Ejecutamos la siguiente orden desde el intérprete para enviar la clave pública, donde *dirección* especifica la dirección de correo electrónico que hemos especificado cuando hemos generado la clave:
   ```
   $ gpg --send-keys dirección
   ```
4. La orden anterior debe devolver un mensaje como el siguiente, para indicar que el envío se ha realizado correctamente:
   ```
   $ gpg: envío correcto a 'pgp.rediris.es' (estado=200)
   ```

El estándar oficial en Internet que ofrece privacidad y seguridad en el correo electrónico se llama **PEM** (*Privacy Enhanced Mail* o Correo con Confidencialidad Mejorada) y está definido en RFC 1421, RFC 1422, RFC 1423 y RFC 1424.

6.2.4 PROTECCIÓN FRENTE A VIRUS

El correo electrónico es un mecanismo de transmisión de información muy eficiente, ya que los mensajes se pueden enviar o reenviar a varios destinatarios o a través de listas de correo. Actualmente, la cantidad de mensajes de correo electrónico enviada a través de Internet es enorme, por lo que se produce un enorme tráfico de información entre zonas geográficas remotas. Esta situación facilita también la propagación de virus, por lo que ya no nos extraña que en los medios de comunicación aparezca de vez en cuando alguna noticia relacionada con la propagación de alguno de ellos. En la tabla 6.3 se enumeran los 10 virus, troyanos u otros programas maliciosos, más extendidos, según los datos facilitados por Kaspersky Lab en mayo de 2009.

Tabla 6.3. Estadísticas de los virus más extendidos en mayo de 2009, por Kaspersky Lab

Posición	Nombre
1	Net-Worm.Win32.Kido.ih
2	Virus.Win32.Sality.aa
3	Trojan-Dropper.Win32.Flystud.ko
4	Trojan.Win32.Autoit.ci
5	Trojan.JS.Agent.xy
6	Exploit.HTML.CodeBaseExec
7	Trojan-Downloader.Win32.VB.eql
8	Trojan.Win32.Chifrax.a
9	Virus.Win32.Virut.ce
10	Virus.Win32.Sality.z

Tal y como están las cosas actualmente, resulta impensable instalar cualquier sistema de gestión de correo electrónico sin las herramientas necesarias para detectar y eliminar todos los programas perjudiciales que se adjuntan con los mensajes. Estas herramientas deben instalarse, tanto en los servidores de correo electrónico que gestionan los agentes MUA y MTA, como en los equipos clientes que descargan y abren los mensajes.

Existen muchos programas antivirus y antiespías que impiden o eliminan los virus que se introducen a través de los mensajes de correo electrónico. Algunos de los más conocidos son Panda, Kaspersky o SpyWare Doctor, todos ellos distribuidos bajo licencia. Por su parte, también existen otras herramientas no menos potentes que se distribuyen libremente a usuarios, como Avast Home, ClamWin, AVG, etc.

6.2.5 CORREO BASURA (SPAM)

Se conoce como **correo basura** o spam todos aquellos mensajes no solicitados por los usuarios, que habitualmente contienen información de carácter publicitario y que son enviados masivamente. Estos mensajes pueden perjudicar a los usuarios que los reciben, desbordando sus buzones o dificultando la consulta de mensajes legítimos.

El origen del término *spam* se remonta a la Segunda Guerra Mundial, cuando los soldados se alimentaban con esta marca de carne enlatada. Más adelante, el grupo Monty Pitón realizó, en 1970, un programa en la BBC donde se burlaba del exceso de carne enlatada que se importaba de otros países, repitiendo una y otra vez "SPAM, SPAM, SPAM, ...".

Se considera que la primera distribución de correo basura se realizó en 1978 cuando Digital Equipment Corporation (DEC) envió un mensaje a 393 destinatarios, a través de ARPANET, informando de la comercialización de un nuevo producto. Actualmente, la mayoría de los mensajes de correo enviados son considerados de tipo *spam* (véase la tabla 6.4), estimándose entre un 80% y un 85% del total de mensajes de correo enviados.

Tabla 6.4. Distribución geográfica del origen del correo basura en 2009, según un estudio realizado por Cisco Systems

Posición	País	Trillones de mensajes de spam al año
1	Brasil	7.7
2	Estados Unidos	6.6
3	India	3.6
4	Corea del Sur	3.1
5	Turquía	2.6
6	Vietnam	2.5
7	China	2.4
8	Polonia	2.4
9	Rusia	2.3
10	Argentina	1.5

El correo basura también supone enormes costes que deben afrontar las empresas y las organizaciones, tanto para instalar los equipos necesarios que filtren y eliminen los mensajes, como la pérdida de productividad que supone entre los trabajadores. En 2001, la Comisión Europea estimó en 10 billones de euros las pérdidas que se producen anualmente a nivel mundial a causa del correo basura.

En muchas ocasiones, los mensajes de correo basura se identifican por especificar direcciones de remitentes falsas o inexistentes. En algunos casos, los sistemas de filtrado de correo pueden identificar estas direcciones falsas, realizando consultas directas e inversas al DNS para comprobar si los nombres de los equipos y sus correspondientes direcciones IP coinciden. En otros casos, estas comprobaciones no detectan el correo basura y el mensaje es entregado al buzón del destinatario. Esta situación no es muy distinta cuando se especifican direcciones falsas de remitentes en el correo postal, práctica que no evita que las cartas lleguen a los destinatarios.

Existen mecanismos que evitan en gran medida la recepción de correo basura. Entre ellos, podemos destacar:

- Consulta al DNS de las direcciones IP y los nombres de los equipos remitentes.
- Inclusión de firmas digitales de los remitentes.
- Análisis de los mensajes enviados para detectar palabras como "sex" o "sexo", "viagra", etc.

6.3 CONFIGURACIÓN DE UN CLIENTE DE CORREO

Este apartado se centra en la configuración de un cliente de correo a través de los protocolos POP3 e IMAP. No aborda cuestiones relativas a la configuración de un cliente *web* de correo ya que en ese caso no es necesario seguir ningún procedimiento especial; simplemente hay que especificar la dirección o nombre del servidor de correo desde un programa navegador de Internet. La Figura 6.4 muestra un ejemplo de este tipo de sistemas de gestión de correo vía web.

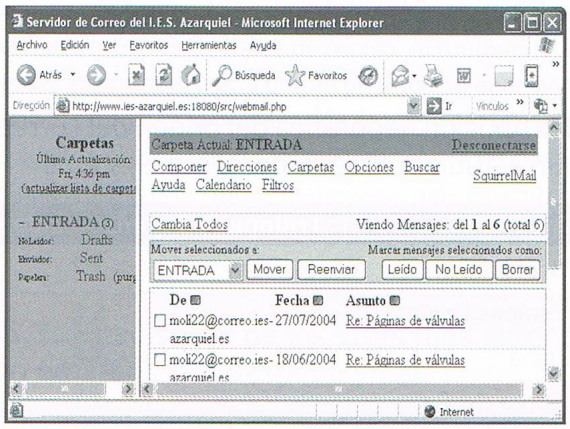


Figura 6.5. *Cliente de correo web squirrelmail. Este cliente de correo web está diseñado mediante código PHP y está disponible de forma gratuita. El propio código PHP de esta página accede al correo electrónico mediante un conjunto de funciones definidas en este lenguaje para los protocolos POP3 e IMAP*

6.3.1 CONFIGURACIÓN EN WINDOWS

La configuración de un cliente de correo en Microsoft Windows se puede realizar de forma sencilla utilizando el programa Outlook disponible en el paquete ofimático Microsoft Office. También se pueden utilizar otros programas cliente que se distribuyen de forma libre, como Mozilla Thunderbird, IncrediMail, etc.

La configuración de los parámetros del servidor de correo se puede realizar en Outlook 2007 utilizando el asistente que aparece al seleccionar la opción "Herramientas | | Configuración de la cuenta..." del menú principal. La Figura 6.6 muestra la ventana con la lista de cuentas de correo configuradas con este asistente.

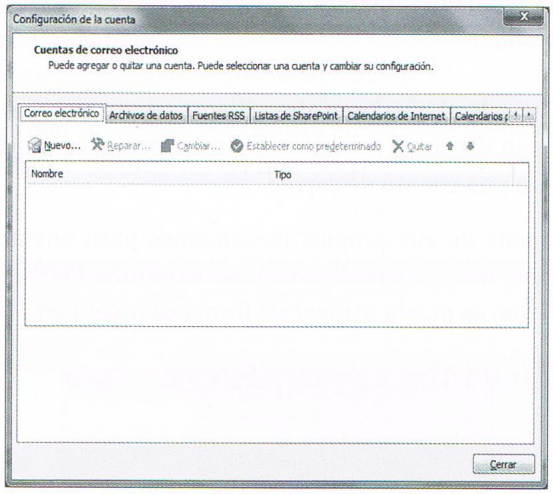


Figura 6.6. Ventana principal del gestor de cuentas de correo en Outlook 2007. Aquí se puede especificar más de una cuenta de correo para acceder a sus buzones. Si se pulsa en el botón "Nuevo..." se pueden añadir más cuentas de correo

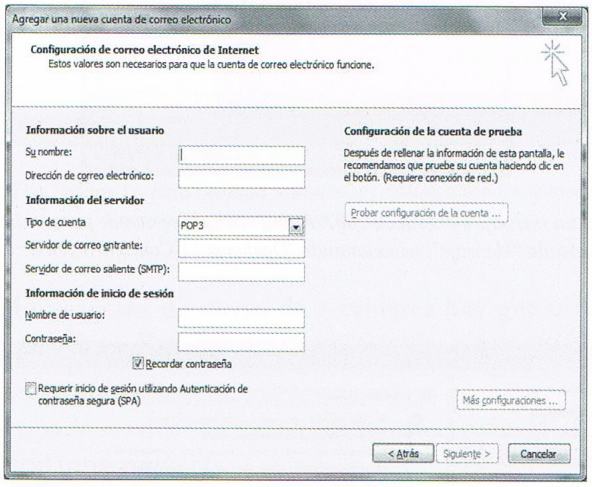


Figura 6.7. Ventana de configuración de una cuenta de correo en Outlook 2007. A esta ventana se accede pulsando el botón "Nuevo..." de la ventana de gestión de cuentas y activando la casilla "Configurar manualmente las opciones del servidor o tipos de servidores adicionales". Si no se activa esta casilla, Outlook 2007 intentará conectar con el servidor de correo cuya dirección obtiene desde la propia dirección de correo

Los parámetros necesarios para configurar el cliente Outlook 2007 son los siguientes:

- **Nombre**: especifica el nombre de la cuenta de correo, utilizado para identificarla en el programa Outlook.
- **Dirección de correo electrónico**: la cuenta debe especificarse con el nombre de dominio competo (*usuario@dominio*).
- **Tipo de cuenta**: especifica el protocolo para intercambiar mensajes con el servidor. Puede ser POP3, IMAP, Exchange, etc.
- **Servidor de correo entrante**: es el nombre del servidor que trabaja como agente MUA, es decir, el que devuelve los mensajes entrantes a través de los protocolos POP3, IMAP, etc.

- **Servidor de correo saliente (SMTP)**: es el nombre del servidor que trabaja como agente MTA, es decir, el que envía los mensajes de correo a través del protocolo SMTP.
- **Nombre de usuario y contraseña**: es el nombre de la cuenta de correo y la contraseña para autenticación. Normalmente, el nombre de la cuenta suele coincidir con el nombre especificado en la dirección de correo electrónico, aunque puede cambiar.

El cliente de correo Microsoft Outlook, al igual que otros clientes de su clase, es capaz de gestionar varias cuentas de correo de distintos servidores y con distintos dominios. De esta forma, se puede resolver el problema que tienen algunos usuarios que utilizan más de una cuenta de correo.

Microsoft Outlook también dispone de sus propios mecanismos para enviar mensajes cifrados. En versiones anteriores a la 2007 (de la 2003 hacia atrás) es posible utilizar el cifrado PGP, pero en el momento de escribir este libro, no existe una versión de PGP que se pueda utilizar de forma completa en Microsoft Outlook 2007.

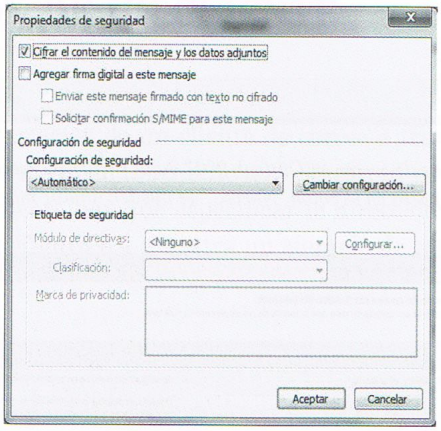


Figura 6.8. *Configuración de cifrado de un mensaje en Outlook 2007. A esta ventana se accede para indicar que el mensaje se va a enviar cifrado desde la pestaña "Mensaje", seleccionando "Opciones \|\| Configuración de seguridad"*

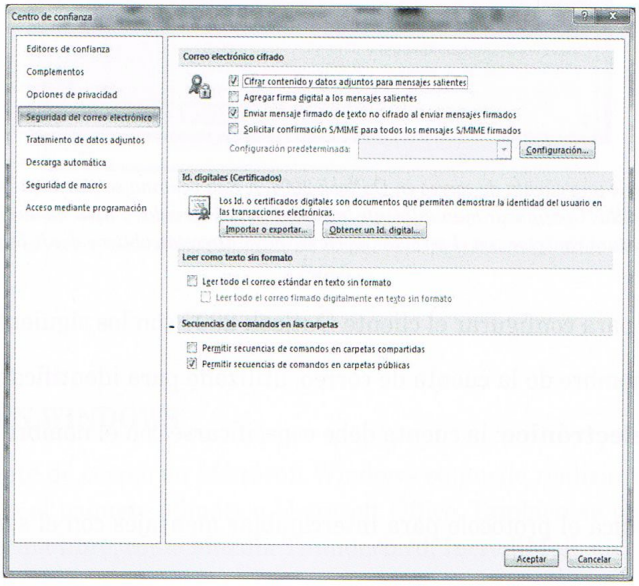


Figura 6.9. *Ventana de seguridad del correo electrónico en Outlook 2007. A esta ventana se accede desde el menú principal "Herramientas \|\| Centro de confianza..." y seleccionando la página "Seguridad del correo electrónico"*

6.3.2 CONFIGURACIÓN EN LINUX

Los sistemas Linux también pueden utilizar una gran variedad de programas cliente de correo electrónico, muchos de ellos distribuidos de forma gratuita. El cliente más conocido que utiliza la línea de órdenes es *mail* y ha sido utilizado durante muchos años por usuarios que trabajaban en modo texto. Otros clientes gráficos más amigables para los usuarios se incluyen en algunos paquetes ofimáticos, como StarOffice u OpenOffice.

Una aplicación cliente de correo que se instala por defecto en muchas distribuciones GNU/Linux es KMail. Este programa funciona en entorno gráfico y es muy parecido a Microsoft Outlook. La Figura 6.10 muestra la ventana principal de esta aplicación.

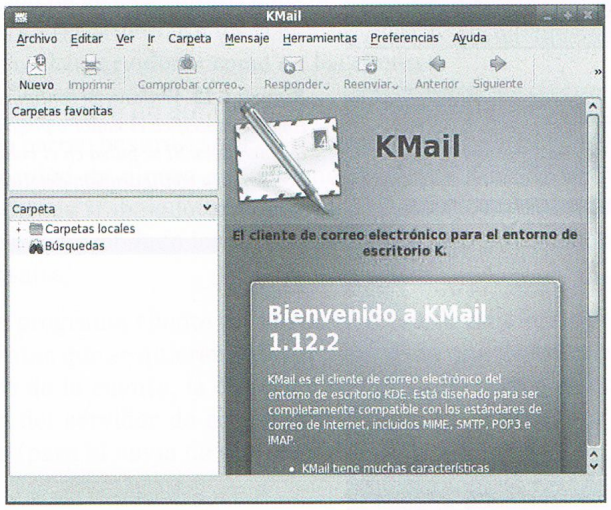


Figura 6.10. *Ventana principal de KMail en Fedora 11. Esta ventana muestra un resumen con los mensajes de correo enviados y recibidos para los servidores indicados en su configuración*

Para poder configurar en KMail cuentas de correo de servidores hay que utilizar la opción "Herramientas || Asistente de cuentas" del menú principal. Esto mostrará un asistente para configurar nuevas cuentas, siguiendo estos pasos:

- **Tipo de cuenta**: indica el tipo de servidor de correo que funciona como MUA. Se puede seleccionar un servidor POP3, IMAP, de entrega local (*procmail*), etc.
- **Información de la cuenta**: especifica el nombre del usuario, su dirección de correo electrónico y el dominio en el que se ubica.
- **Información de inicio de sesión**: define el nombre de usuario y la contraseña para el acceso del cliente. Normalmente, el nombre de usuario coincide con el nombre especificado en la dirección de correo electrónico, aunque puede cambiar.
- **Información del servidor**: especifica el nombre del servidor entrante (el agente MTA que gestiona SMTP) y el servidor saliente (el agente MUA que gestiona POP3 o IMAP).

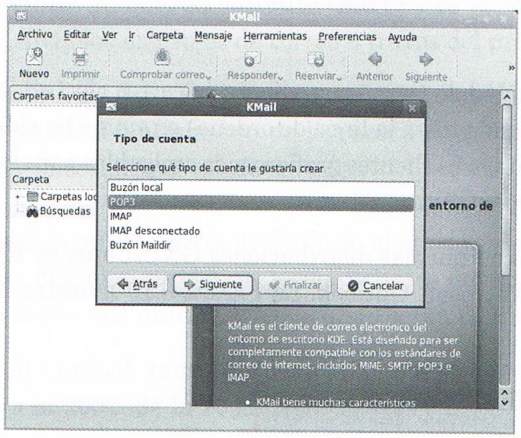


Figura 6.11. *Selección del servidor de correo que recibe los mensajes en KMail. Esta ventana aparece pulsando en el botón "Añadir" de la página "Recibiendo"*

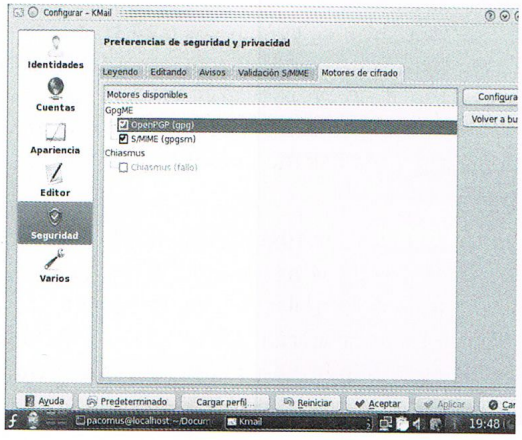


Figura 6.12. *Ventana de configuración de cifrado en KMail. Aquí se especifica el motor o programa a utilizar para cifrar los mensajes. Si se pulsa en el botón "Configurar" se puede acceder a la configuración detallada del tipo de cifrado seleccionado*

RESUMEN DEL CAPÍTULO

El sistema de **correo electrónico** permite el intercambio de mensajes entre usuarios, sin necesidad de que estos se encuentren conectados en el momento de realizar el envío. El sistema de correo electrónico requiere de un agente que intercambie los mensajes entre los servidores, llamado MTA, agentes de descarga de correo a los equipos cliente, llamados MUA y la gestión de los buzones de correo donde se almacenan los mensajes.

El protocolo SMTP es un agente MAT encargado de transportar los mensajes de correo desde el servidor donde se encuentra el buzón del usuario emisor hasta el servidor donde se encuentra el buzón del receptor. Para realizar estas transferencias, el servidor que envía realiza una conexión con el servidor que recibe, según el modelo de funcionamiento del sistema cliente-servidor.

Los protocolos POP3 e IMAP son agentes MUA que permiten la transmisión de los mensajes de correo almacenados en los buzones de los usuarios hacia los ordenadores que estos utilizan. Los equipos cliente realizan esta descarga de los mensajes utilizando programas cliente de correo electrónico, como Microsoft Outlook, KMail o Evolution.

Un mensaje de correo electrónico está formado por dos campos: la cabecera y el cuerpo. La cabecera, contiene las direcciones de origen y destino, el tipo de información que contiene, el título del mensaje y cierta información de control. Por su parte, el cuerpo contiene el texto del mensaje y todos los archivos adjuntos a él.

Tradicionalmente, el sistema de correo electrónico no ha tenido definido ningún mecanismo de control de la seguridad y el envío de la información se ha realizado como texto plano sin cifrar. Actualmente, una buena gestión de la seguridad y la privacidad en los mensajes es fundamental, por lo que se han establecido mecanismos para proteger las contraseñas y cifrar aquellos mensajes comprometidos. Uno de los mecanismos más conocidos es PGP, que permite enviar los mensajes de correo cifrados.

La detección y eliminación de virus adjuntos a los mensajes de correo también resulta importante, dada la facilidad con la que estos se extienden. En los sistemas de correo electrónico, es recomendable mantener programas antivirus tanto en los servidores como en los clientes.

Actualmente se estima que entre un 80% y un 85% de los mensajes de correo electrónico que circulan por Internet se clasifican en correo basura o *spam*. Filtrar y eliminar estos mensajes es de vital importancia para evitar la enorme cantidad de dinero que supone a las empresas y organizaciones en cuanto a la pérdida de productividad de sus trabajadores. Para ello, existen programas que son capaces de eliminar gran parte de estos correos, comprobando las direcciones de origen y buscando palabras específicas en el título o el texto de los mensajes.

La configuración de un programa cliente de correo electrónico requiere del registro de los parámetros asociados a la cuenta o cuentas que se quieren utilizar. Para cada una de estas cuentas, el programa cliente necesita conocer el nombre de la cuenta, la dirección completa de correo electrónico, el tipo de protocolo MUA utilizado, el nombre del servidor de correo entrante (para la descarga del correo), el nombre del servidor de correo saliente (para el envío de correo por SMTP) y el nombre de usuario y contraseña para autenticarse al servidor.

EJERCICIOS PROPUESTOS

- **1.** Crea una cuenta de correo gratuita en Gmail y enumera los pasos que has seguido para conseguirlo. Indica también qué pasos debes seguir para acceder a la cuenta de correo que has creado.
- **2.** Sobre la cuenta de correo que has creado en el ejercicio anterior, configura el cliente de correo Microsoft Outlook 2007 para acceder a ella. ¿Qué parámetros del servidor debes especificar?
- **3.** Repite el ejercicio sobre la cuenta creada en Gmail, pero ahora configura el acceso desde un programa cliente de GNU/Linux como KMail o Evolution.
- **4.** Indica todos los pasos que sigue un mensaje de correo desde que es escrito y enviado por el remitente hasta que es abierto y leído por el destinatario. Ambos usuarios acceden a su correo a través del protocolo POP3.
- **5.** Comprueba si en tu sistema GNU/Linux dispones del paquete GPG instalado; en caso negativo, instálalo. Anota todos los pasos que realizas.
- **6.** Indica los pasos a seguir para enviar un mensaje de correo cifrado a través de Microsoft Outlook 2007.
- **7.** Sobre lo realizado en el ejercicio anterior, indica los pasos a seguir para recibir y descifrar un correo cifrado desde Outlook 2007.
- **8.** Indica los pasos a seguir para enviar un mensaje de correo cifrado a través de Evolution.
- **9.** Sobre lo realizado en el ejercicio anterior, indica los pasos a seguir para recibir y descifrar un correo cifrado desde KMail.

TEST DE CONOCIMIENTOS

1 Un agente MUA se utiliza para:
a) Enviar los mensajes desde el origen al destino.
b) Filtrar el correo basura.
c) Enviar los mesnajes a los equipos de los destinatarios.
d) Todas son ciertas.

2 El estándar MIME define:
a) El formato de los mensajes de correo.
b) El contenido de los mensajes de correo.
c) El formato de las direcciones de correo.
d) Ninguna es cierta.

3 El protocolo SMTP:
a) Se utiliza para entregar los mensajes a los usuarios finales.
b) Es un agente MUA.
c) Define el método de cifrado de los mensajes.
d) Ninguna es cierta.

4 El protocolo IMAP:
a) Se usa para entregar los mensajes en los buzones de los usuarios.
b) Se usa para transferir los mensajes a los equipos de los clientes.
c) Transfiere copias de los mensajes a los clientes.
d) Todas son ciertas.

5 El correo basura se identifica por:
a) Mensajes con dirección de origen falsa.
b) Mensajes no solicitados por los usuarios.
c) Mensajes publicitarios.
d) Todas son ciertas.

6 Un programa cliente de correo:
a) Debe ejecutarse siempre en el ordenador del usuario.
b) Puede ejecutarse en un servidor de correo.
c) Gestiona los buzones de todos los usuarios.
d) Ninguna es cierta.

7 Un parámetro que no se especifica en la configuración de la cuenta del cliente de correo es:
a) Contenido y formato de los mensajes a enviar.
b) Nombre del servidor de correo entrante.
c) Nombre del servidor de correo saliente.
d) Dirección de correo electrónico de origen.

8 Un programa cliente de correo IMAP:
a) Copia los mensajes desde el servidor y los elimina de éste.
b) Copia los mensajes desde el servidor pero no los elimina de éste.
c) Crea las cuentas de correo en el servidor.
d) Ninguna es cierta.

9 El programa PGP:
a) Se instala en los servidores de correo para cifrar los mensajes.
b) Se instala junto con los programas cliente de correo.
c) Lo tiene que instalar el usuario que envía los mensajes, pero no lo necesita el que los recibe.
d) Ninguna es cierta.

7 Servidores de correo electrónico

OBJETIVOS DEL CAPÍTULO

- ✓ Instalar un servidor de correo electrónico.
- ✓ Crear cuentas de usuario y verificar el acceso de las mismas.
- ✓ Definir alias para las cuentas de correo.
- ✓ Aplicar métodos para impedir usos indebidos del servidor de correo electrónico.
- ✓ Instalar servicios para permitir la recogida remota del correo existente en los buzones de usuario.

Como se explica en el capítulo 6, el sistema de correo electrónico funciona en base al modelo cliente-servidor. Esto significa que un mensaje de correo es enviado primero desde un equipo cliente hasta un servidor (usando un agente MUA, como POP3 o IMAP). Después, el servidor reenvía el mensaje, si es necesario, a otro servidor que distribuya el correo local (del dominio al que pertenece la cuenta) a través del agente MTA que ejecuta SMTP. Finalmente, a través de otra conexión de cliente POP3 o IMAP, el mensaje se envía desde el servidor al cliente destinatario.

El sistema de correo electrónico requiere de unos conocimientos avanzados para poder ponerlo en marcha, por varias razones:

- Existen muchos protocolos involucrados en el envío de correos electrónicos que interactúan entre dos servidores o entre un servidor y un cliente (SMTP, POP3, IMAP, etc.). Además de estos, también son necesarios otros mecanismos para gestionar las cuentas y los buzones de correo, como son Active Directory, Cyrus, Mysql, etc.
- En caso de que se disponga de la posibilidad de acceder a los buzones de correo a través del protocolo de transferencia de hipertexto, entonces el equipo debe funcionar también como servidor HTTP con soporte para páginas dinámicas (ASP, PHP, JSP, etc.).
- El sistema de correo electrónico interactúa con otros servicios de red, como el DNS, ya que no utiliza direcciones IP sino nombres de equipos. Antes de configurar un servidor de correo, es necesario configurar correctamente el servidor DNS.

Este capítulo está dedicado a explicar cómo se realiza la instalación y configuración de un servidor de correo electrónico para los sistemas operativos Microsoft Windows y Linux.

Un requisito indispensable para poder instalar y configurar un servidor de correo electrónico en nuestra red es que exista un servidor DNS que sea capaz de resolver direcciones. Este servidor puede instalarse en el mismo equipo que el servidor de correo o puede ser un servidor independiente y debe tener un registro de tipo *MX* que especifique el nombre del servidor de correo (véase el capítulo 2).

7.1 SERVIDORES DE CORREO EN MICROSOFT WINDOWS

7.1.1 INTERNET INFORMATION SERVICES EN WINDOWS SERVER 2003

Los sistemas Microsoft Windows ofrecen la posibilidad de instalar y configurar un servidor de correo electrónico en sus versiones 2000 Server y Server 2003 a través del paquete **IIS** (*Internet Information Services*) que se incluye con los discos de instalación del sistema operativo. Este servidor es compatible con otras plataformas, como *Sendmail* para GNU/Linux.

A diferencia de otros sistemas como Linux, en Windows no es necesario instalar y configurar diferentes paquetes para disponer de un servidor de correo electrónico. El propio paquete IIS ya dispone de todo lo necesario para instalar los protocolos SMTP, IMAP y POP3 sobre el sistema, además de los protocolos necesarios para ofrecer seguridad y privacidad.

Para instalar IIS es necesario acceder a la herramienta de instalación de componentes o al asistente de configuración del servidor. Hay que recalcar que es necesario seleccionar la opción "Servicios SMTP" en la instalación de IIS. Una vez instalado, se puede acceder a su herramienta de configuración desde el menú de *Herramientas administrativas* en la opción "Administrador de Internet Information Services (IIS)". La Figura 7.1 muestra la ventana principal de esta herramienta.

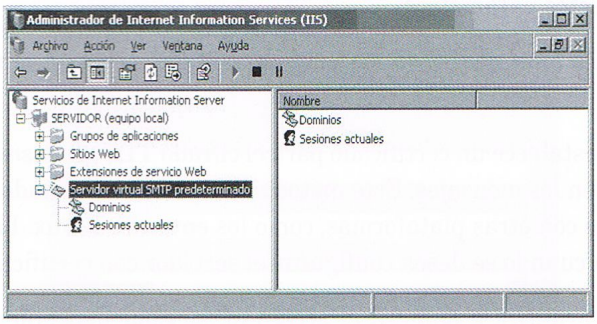


Figura 7.1. *Ventana principal de administración de IIS en Windows Server 2003. El paquete IIS permite que el equipo se comporte como un servidor web, FTP, etc. El icono titulado "Servidor virtual SMTP predeterminado" indica que el equipo también funciona como un servidor de correo*

Para que el servicio SMTP funcione correctamente en un servidor Microsoft Windows Server 2003 es necesario instalar también el protocolo POP3. Esto se puede hacer a través del asistente de configuración del servidor.

El servicio SMTP de Microsoft Windows permite manejar distintos servidores virtuales. Cada uno de estos servidores virtuales está asociado con una dirección de dominio distinta y gestiona todos los usuarios pertenecientes a ese dominio.

Para iniciar los servicios SMTP hay que pulsar con el botón derecho del ratón sobre el icono "Servidor virtual SMTP predeterminado" de la ventana de administración de IIS y seleccionar la opción "Iniciar". Otras opciones son "Detener" para pararlo o "Pausar" para suspenderlo temporalmente.

La configuración de un servidor SMTP virtual se realiza seleccionando su icono y pulsando en la opción "Propiedades" de su menú contextual (usando el botón derecho del ratón). La ventana que aparece muestra distintas opciones agrupadas por páginas.

La página "General" de propiedades del servidor virtual establece los siguientes parámetros (Figura 7.2):

- **Dirección IP**: especifica la dirección IP desde donde el servidor puede responder a las peticiones de conexión para transferir correo.
- **Limitar el número de conexiones a**: se puede establecer un número máximo de conexiones simultáneas.
- **Tiempo de espera de conexión (en minutos)**: es el tiempo que el servidor espera para cerrar una conexión si está inactiva.

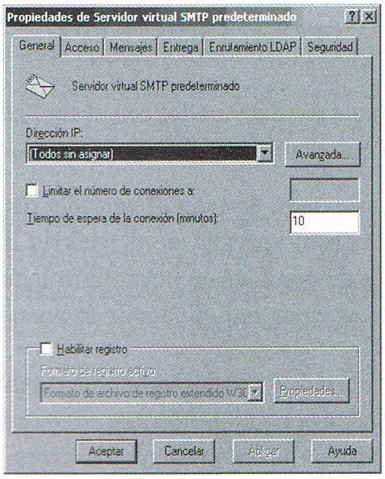


Figura 7.2. *Página "General" de la ventana de propiedades del servidor virtual en Windows Server 2003. Aquí se establece la dirección IP desde donde se van a aceptar las conexiones para transferir los mensajes desde otros servidores*

La página "Acceso" contiene estos parámetros:

- **Control de acceso**: indica si es necesario realizar una autenticación en el momento de establecer conexión con el servidor.
- **Comunicación segura**: establece un certificado para el cifrado **TLS** (*Transmisión Layer Security* o Seguridad en Capa de Transmisión) en los mensajes. Este método de cifrado está basado en el estándar de Internet PEM que a su vez es compatible con otras plataformas, como los entornos Linux. La Figura 7.3 muestra la ventana del asistente que se inicia cuando se desea configurar el servidor con certificados seguros TLS.
- **Control de conexión**: garantiza o deniega el acceso al servidor dependiendo de las direcciones IP de los equipos o sus nombres.
- **Restricciones de retransmisión**: permite configurar la transmisión de mensajes no deseados a través del servidor.

La página "Mensajes" limita algunos parámetros de los mensajes, como tamaño, número por conexión, número de destinatarios, etc. También establece una carpeta donde se registran los mensajes erróneos.

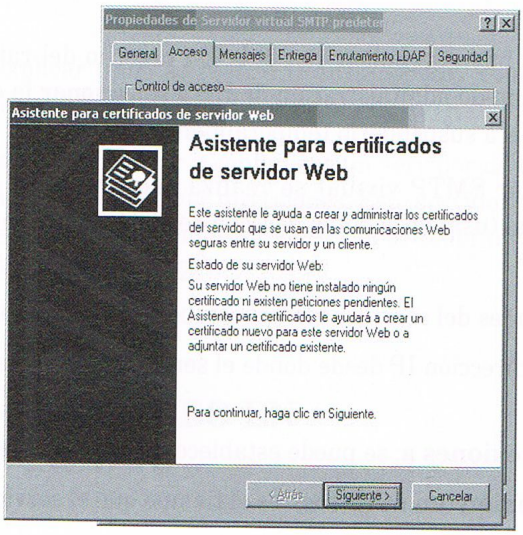


Figura 7.3. *Ventana del asistente para crear certificados TSL en Windows Server 2003. Es necesario crear estos certificados antes de activar la comunicación segura del servidor*

La página "Engrega" contiene los parámetros relacionados con el envío de correo a otros servidores, como el tiempo de reintento en las conexiones o el tiempo que transcurre para enviar una notificación de entrega.

En la página "Enrutamiento LDAP" se puede activar el servicio de pasarela para que el servidor de correo pueda gestionar los usuarios registrados en el servicio de directorio de Microsoft Windows (que usa nombres LDAP). La Figura 7.4 muestra las opciones disponibles en la configuración del enrutamiento LDAP. Como se puede observar, el sistema puede enlazar con un servidor remoto donde se encuentran las cuentas de usuario del servicio de directorio.

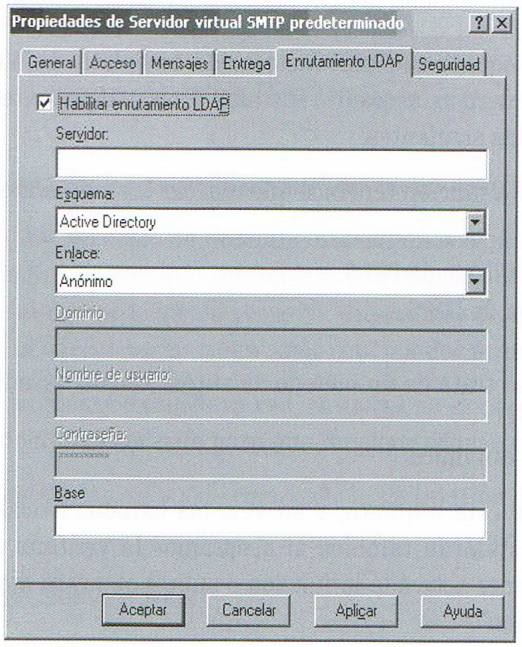


Figura 7.4. *Página "Encaminamiento IP" de las propiedades del servidor de correo en Windows Server 2003. Con esta ventana se puede integrar los usuarios del directorio activo para la gestión del correo electrónico*

Finalmente, en la página "Seguridad" es pueden establecer cuentas de usuario y grupos del sistema con privilegios para gestionar el servidor de correo electrónico, tanto de forma local como remota. Por defecto, los usuarios administradores del servidor de correo ya disponen de privilegios para gestionar todas las características del sistema de correo electrónico.

Una vez configurados todos los parámetros del servidor de correo electrónico en Microsoft Windows, el sistema será capaz de enviar y recibir correo a través de su agente de transporte (SMTP). También será capaz de enviar y recibir correo de los clientes a través de los protocolos POP3 e IMAP. Se puede utilizar un programa de exploración de puertos para comprobar que los puertos correspondientes a estos servicios están activos.

7.1.2 MICROSOFT EXCHANGE SERVER 2007

Con la aparición en el mercado de las versiones Microsoft Windows Vista/7/2008, se ha puesto de manifiesto la imposibilidad de instalar y configurar un servidor de correo completo, ya que el paquete *Internet Information Services* (IIS) ya no incluye soporte para protocolos MUA, como POP3 o IMAP. Solamente se puede utilizar IIS como un servidor de correo MTA, gracias al paquete SMTP.

En estos sistemas se pueden instalar servidores de correo electrónico de otros fabricantes o bien utilizar Microsoft Exchange Server, un paquete completo que incluye todo lo necesario para instalar y configurar un servidor de correo electrónico, aunque esta herramienta debe adquirirse por separado. En este apartado nos centraremos en la instalación y configuración de Microsoft Exchange Server 2007 sobre Windows Server 2008.

Aunque Microsoft Exchange Server debe obtenerse con licencia de uso, ya que no se trata de un programa libremente distribuido, sí que es posible obtenerlo gratuitamente desde la página oficial de Microsoft con una licencia de evaluación que expira en unos días. Mientras tanto, se puede instalar y configurar el paquete completo, de forma que podemos evaluar su funcionamiento y comprobar las posibilidades que ofrece.

7.1.2.1 Requisitos previos

Si suponemos que tenemos un equipo con una instalación completa de Windows Server 2008, para instalar Exchange Server 2007 sobre él, primero es necesario instalar otros componentes adicionales. Las funciones o roles que hay que añadir al servidor son las siguientes:

- **Servidor Web (IIS)**: para esta función tenemos que marcar las siguientes subfunciones o subroles:
  - Extensiones ISAPI.
  - Compatibilidad con la metabase de IIS 6.
  - Consola de administración de IIS 6.
  - Autenticación basica.
  - Autenticación implícita (se trata de un método de autenticación basado en el algoritmo Digest).
  - Autenticación de Windows.
  - Compresión de contenido dinámico.
- **Servidor de aplicaciones**: éste requiere, a su vez, las caracteristicas "Microsoft .NET Framework 3.0" y "Servicio WAS", que se instalarán también si aceptamos la ventana que aparece cuando se marca esta función. En este caso, dejaremos activada la función o subrol que está marcada por defecto y cuyo nombre es "Application Server Foundation".

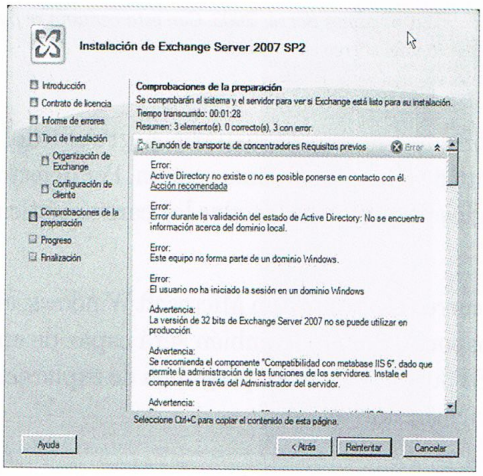


Figura 7.5. *Errores en la instalación de Microsoft Exchange Server 2007. Estos errores son debidos a que el programa requiere de la instalación de otros componentes adicionales. Si se pulsa en los enlaces que aparecen con el título "Acción recomendada", se accede desde el navegador de Internet a determinadas páginas de información de Microsoft donde se puede obtener información sobre cómo corregir los problemas detectados*

Además de las funciones anteriores, para instalar Exchange Server 2007 sobre Windows Server 2008, es necesario instalar también la característica "Windows Power Shell". De igual forma, también es necesario instalar y configurar convenientemente el *Directorio Activo* de Microsoft (*Active Directory*). Hay que tener en cuenta que las cuentas de correo electrónico que se definen en Exchange Server son las mismas que las cuentas de usuario definidas en el directorio activo correspondiente al dominio definido para la red de Microsoft.

Un dominio de la red de Microsoft está formado por un conjunto de equipos que comparten el mismo modelo de seguridad. Esto significa que todos esos equipos pueden ser utilizados a través de unas cuentas de usuario que se han definido con una serie de permisos y derechos. Toda esta información de seguridad asociada al dominio se almacena y se gestiona a través del servidor, también conocido como *Controlador de dominio*.

Para instalar y configurar convenientemente el *Directorio Activo*, tenemos que seguir estos pasos:

1 Agregamos la función "Servicios de dominio de Active Directory".

2 Ejecutamos el programa *DCPROMO*, en la opción "Ejecutar" del menú de inicio.

3 En el asistente de configuración del servidor de dominio, necesitamos especificar "Crear un nuevo dominio en un bosque nuevo", escribir el nombre de dominio totalmente cualificado o FQDN (por ejemplo, "midominio.es"), activamos la opción "DNS" para que el equipo también resuelva direcciones de dominio y aceptamos todos los datos introducidos. Después de un tiempo, el equipo ya funciona como controlador primario de dominio.

4 Si ya disponemos de un dominio existente en nuestra red, entonces no es necesario crear un dominio nuevo, sino que hay que añadir el equipo al dominio existente para que funcione como controlador de reserva de dominio.

Con todas estas características instaladas, se puede comenzar la instalación de Exchange Server 2007.

7.1.2.2 Instalación de Exchange Server 2007

Para instalar Microsoft Exchange Server 2007 hay que seguir estos pasos:

1 Ejecutar el programa de instalación que se encuentra en los discos o en el paquete que contiene esta herramienta. En la primera ventana del asistente se muestran una serie de pasos para instalar componentes adicionales. Si estos ya estuvieran instalados, entonces solamente estará activo el paso 5 "Instalar Microsoft Exchange Server". Pulsamos en esta opción y continuamos a la ventana siguiente.

2 La siguiente ventana muestra una introducción al servicio Exchange Server y las nuevas características de la versión. Pulsamos el botón "Siguiente".

3 En la siguiente ventana aceptamos los términos del contrato de licencia del producto.

4 A continuación, indicamos si deseamos que el programa envíe los informes de los errores a Microsoft para mejorar el producto.

5 Lo siguiente que se nos pide es seleccionar el tipo de instalación que deseamos. Tenemos dos opciones: **instalación típica** (con los componentes comunes para el funcionamiento del servidor) e **instalación personalizada** (para seleccionar componentes concretos). Se recomienda utilizar la instalación típica para disponer de una funcionalidad plena.

6 En la siguiente ventana se especifica el nombre de la organización para la que Exchange va a distribuir el correo.

7 A continuación se indica si en la organización existen equipos cliente que van a consultar el correo mediante Microsoft Outlook 2003 o versiones anteriores. Si es así, el servidor necesita crear una base de datos de carpetas públicas que necesitan estos programas.

8 La siguiente ventana muestra las comprobaciones previas a la instalación, donde se muestra si falta algún componente necesario para el buen funcionamiento de Exchange Server. Si es así, el programa de instalación no permitirá continuar. En caso contrario, se activará el botón "Instalar" para continuar con el proceso.

9 Una vez realizado el proceso de instalación se pide que se reinicie el equipo para que los cambios tengan efecto.

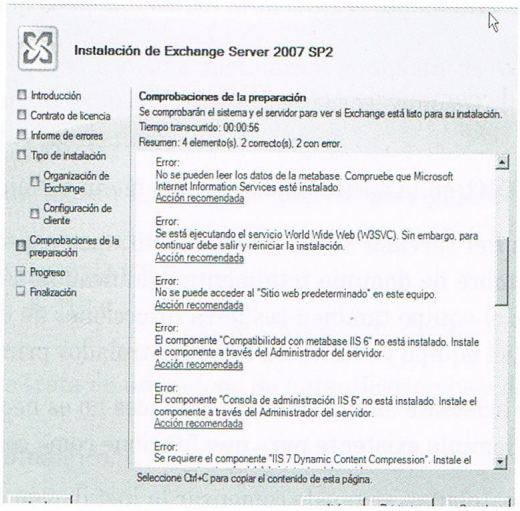


Figura 7.6. *Ventana de comprobación de requisitos de instalación para Exchange Server 2007. Si alguno de los componentes necesarios no se han instalado, el asistente no puede continuar con la configuración*

7.1.2.3 Gestión de cuentas en Exchange Server 2007

Para crear una cuenta de correo en Exchange Server 2007 hay que seguir estos pasos:

Si no existe la cuenta de usuario en *Active Directory*, entonces hay que crearla de la siguiente forma:

1 Acceder a la herramienta "Usuarios y equipos de Active Directory" dentro del menú "Herramientas administrativas".

2 En el árbol de objetos de la parte izquierda, seleccionar el contenedor "Users" (usuarios) y pulsar en la opción del menú principal "Acción || Nuevo || Usuario".

3 En la ventana que aparece, especificar el nombre de usuario y su nombre de inicio de sesión. Después, pulsar el botón "Siguiente".

4 Especificar la contraseña del usuario y desmarcar la casilla "El usuario debe cambiar la contraseña al iniciar una sesión de nuevo". A continuación, pulsar en el botón "Siguiente".

5 Una vez creada la cuenta del usuario, es necesario crear su cuenta de correo electrónico, para lo que seguiremos estos pasos:

6 Acceder a la "Consola de administración de Exchange", disponible en el grupo de opciones "Microsoft Exchange Server 2007" del menú de inicio.

7 En el árbol de objetos de la parte izquierda, seleccionar el elemento "Microsoft Exchange || Configuración de destinatarios || Buzón". Después, seleccionar "Buzón nuevo..." del menú "Acciones".

8 En la ventana que aparece, se selecciona el tipo de buzón que se va a crear, en nuestro caso será "Buzón de usuario". Después, pulsamos el botón "Siguiente".

9 A continuación se selecciona para quién se va a crear el buzón, seleccionamos "Usuarios existentes" y pulsamos el botón "Agregar".

10 En la siguiente ventana, seleccionamos el usuario y pulsamos el botón "Aceptar", así volvemos a la ventana anterior. En ella, pulsamos el botón "Siguiente".

11 A continuación, especificamos el nombre o alias del buzón de correo. También hay que seleccionar la base de datos donde se va a almacenar todo el contenido del buzón, pulsando en el botón "Examinar" (lo que muestra una ventana para seleccionarla). Pulsamos de nuevo el botón "Siguiente".

12 En la última ventana del asistente, se muestra un resumen con los parámetros especificados. Pulsamos el botón "Nuevo" para crear el buzón.

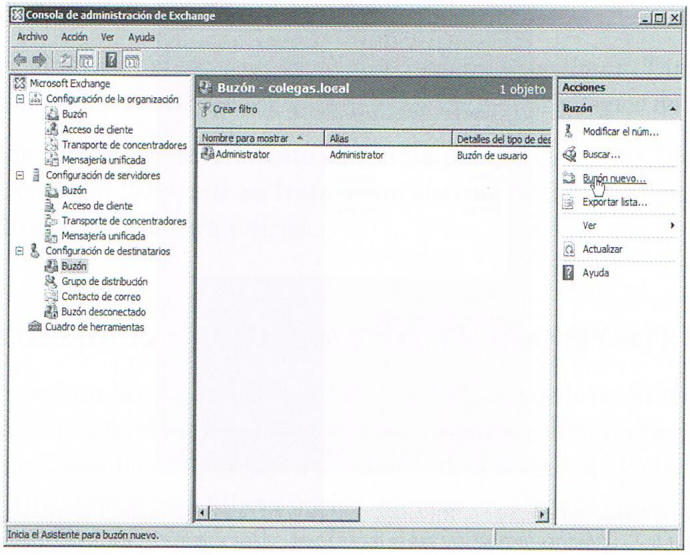


Figura 7.7. Ventana principal de la consola de administración de Exchange Server 2007. Desde esta herramienta se gestionan todos los servicios disponibles, las cuentas de correo, etc.

7.1.2.4 Acceso a los buzones de los usuarios

La instalación por defecto de Microsoft Exchange Server 2007 permite el acceso a los buzones de los usuarios a través de un programa cliente POP3 o IMAP. También permite la consulta del correo electrónico a través de un navegador de Internet, especificando la dirección del servidor de la siguiente forma:

```
https://dirección_servidor/owa
```

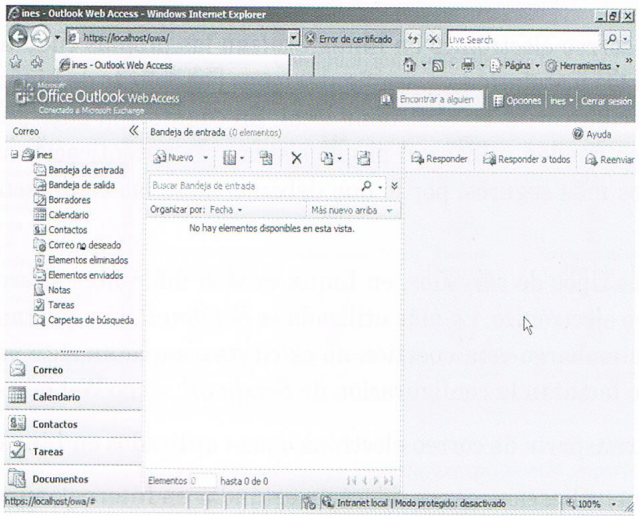


Figura 7.8. Ventana principal de consulta de correo Web a través de Exchange Server 2007. Esta herramienta permite la consulta del correo sin necesidad de que los usuarios tengan que instalar y configurar un programa cliente

El servicio **OWA** (*Outlook Web Access* o Acceso Web de Outlook) es un programa cliente de correo que se ejecuta directamente en el servidor que funciona con Exchange Server 2007. Cuando se crea una cuenta de correo en Exchange Server, es posible especificar a través de qué protocolos se puede consultar el correo. Para ello, se puede acceder a las propiedades de una cuenta desde la consola de administración de Exchange y seleccionar la página "Características de buzón" (véase la Figura 7.9).

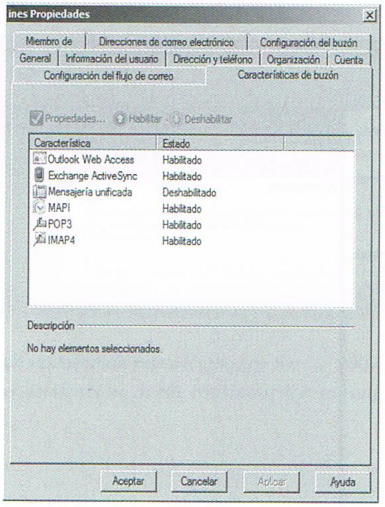


Figura 7.9. *Clientes disponibles para el buzón del usuario en Exchange Server 2007. A esta ventana se accede desde las propiedades de una cuenta de correo y permite establecer si un usuario puede consultar su correo con alguno de los agentes de usuario disponibles*

7.2 SERVIDORES DE CORREO EN GNU/LINUX

Además de estos agentes, el servidor de correo también necesita gestionar el protocolo POP3 o IMAP para que los clientes puedan descargar el correo. Se pueden utilizar varias alternativas, pero quizás la más flexible sea el paquete *cyrus*, que está disponible de forma gratuita para todas las distribuciones de Linux y agentes de transporte de correo.

Los sistemas de gestión de correo electrónico en Linux utilizan las propias cuentas de usuario del sistema como cuentas de correo. De hecho, en las instalaciones y configuraciones por defecto de Linux cualquier usuario que se crea en el sistema puede enviar o recibir correo en el sistema local. En cuanto a la autenticación de los usuarios, hay que decir que los sistemas de correo pueden utilizar el propio sistema de autenticación usado por el sistema operativo y pueden utilizar otros métodos más seguros, por lo que deben crearse las contraseñas de los usuarios con alguna herramienta u orden.

Como es habitual para otros tipos de servicios, en Linux existen diferentes alternativas a la hora de instalar y configurar un servidor de correo electrónico. La más utilizada es *Sendmail*, aunque también es la que tiene más fama de ser difícil de configurar. Sin embargo esta cuestión no es cierta completamente ya que existen herramientas de administración del sistema que facilitan la configuración de *Sendmail*, como Webmin.

Algunos de los agentes de transporte de correo electrónico mas utilizados en Linux son:

- **Sendmail**: por su amplia utilización, se considera un estándar en Internet, aunque se ha ganado la reputación de ser difícil de configurar. Esto es debido a que su archivo de configuración principal, llamado *sendmail.cf*, se diseñó para que el sistema fuera capaz de procesarlo con rapidez y no para facilitar la lectura y modificación a

los usuarios. Existen diferentes herramientas que ayudan enormemente en la configuración de los parámetros del archivo *sendmail.cf*, aunque no hay que negar que la gran cantidad de estos parámetros suele complicar a veces la configuración.

- **Postfix**: se trata de un sistema eficiente diseñado por Wietse Venema de IBM. Al contrario que *Sendmail*, este sistema es fácil de configurar y está más optimizado para un funcionamiento eficiente. Aunque todavía no se ha extendido ampliamente su uso, se considera que en el futuro será el sustituto de *Sendmail* en los servidores de correo electrónico de Internet.
- **QMail**: se trata de otra alternativa más sencilla de configurar que *Sendmail*. También tiene menos problemas de seguridad debido a que los procesos demonio no se ejecutan con privilegios de *root*.
- **Exim**: es otro agente de correo que actualmente se instala por defecto en las Distribuciones Debian. Aunque no tienen tanta tradición como *Sendmail*, se trata de un sistema de fácil configuración, flexible a los cambios y con opciones para filtrar correo basura y virus.

7.2.1 INSTALACIÓN Y CONFIGURACIÓN DEL AGENTE DE TRANSPORTE SENDMAIL

Este apartado se centra en explicar la configuración de *Sendmail* que se puede realizar de tres formas: manualmente a través del archivo *sendmail.cf*, usando el módulo M4 que crea el archivo *sendmail.cf* a partir de otro archivo llamado *sendmail.mc* (este último es más sencillo de manejar) o utilizando la herramienta Webmin que facilita enormemente esta tarea. Por simplicidad, utilizaremos esta última opción, aunque en algunos casos deberemos echar mano de los archivos de configuración ya que Webmin no permite realizar ciertas operaciones.

Antes de comenzar, se recomienda repasar los contenidos sobre la herramienta Webmin. Esta herramienta incluye un módulo de configuración de los parámetros del servidor *Sendmail* (véase la Figura 7.10). Hay que tener en cuenta que el paquete *sendmail* tiene que estar instalado en el sistema para que este módulo esté activado. Para instalar *Sendmail* en Debian 5, hay que seleccionar los paquetes *sendmail* y *sendmail-bin* (en otras distrbuciones, los nombres pueden cambiar), además de otros paquetes que se instalan automáticamente como dependencias. Esta acción eliminará del sistema el agente MTA que se encuentre instalado por defecto (puede ser Postfix, Exim, etc.).

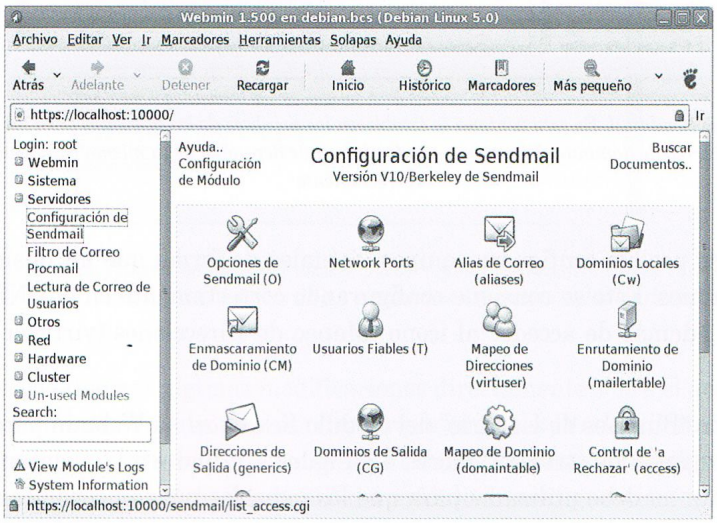


Figura 7.10. *Ventana principal del módulo de configuración de Sendmail en Webmin. La opción más importante es "Dominios Locales (Cw)" ya que en ella se especifican los dominios para los que vamos a recibir el correo electrónico. En el icono "Alias de correo (aliases)" se pueden crear alias que hagan referencia a usuarios de correo existentes*

Una vez instalado *Sendmail*, solamente son necesarias unas cuantas operaciones para que el equipo pueda enviar y recibir correo. El primer paso consiste en permitir que el correo sea recibido desde otros equipos o redes para el dominio en el que se encuentra, operación que se realiza en el icono "Dominios Locales (Cw)" del módulo *Sendmail* de Webmin. Por ejemplo, si el dominio de nuestra organización se llama "chispita.es", entonces tenemos que especificarlo para que nuestro servidor acepte el correo destinado a este dominio.

El siguiente paso consiste en permitir que los usuarios puedan enviar correo a través del servidor. Esto se realiza en el icono "Control de 'a Rechazar' (access)" de Webmin, donde se establecen las direcciones IP de las redes a las que está conectado el servidor. Por ejemplo, en una red local donde en servidor tiene la dirección *192.168.10.1*, hay que especificar la dirección *192.168.10* en el campo "Fuente de correo", marcar la opción "Aceptar" y pulsar en el botón "Crear". La nueva dirección aparecerá en la lista situada debajo del formulario con la propiedad "Acción" asignada a "RELAY" o "Permitir retransmisión".

Una vez establecidos todos los valores, hay que pulsar en el botón "Parar Sendmail" de la ventana principal del módulo de Webmin (se encuentra en la parte inferior de la Figura 7.10). Ese mismo botón cambiará al mensaje "Arrancar Sendmail". Hay que pulsar de nuevo este botón para iniciar el servidor *Sendmail* (todos sus programas *demonio*). Al realizar esta operación de parada e inicio de *Sendmail*, se consiguen aplicar todos los cambios realizados sobre la configuración de este servidor de correo.

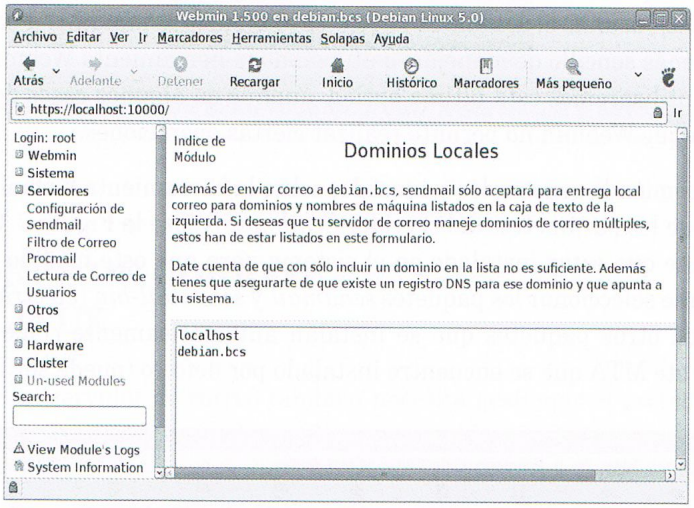


Figura 7.11. *Dominios locales en Sendmail. En esta ventana se establecen los nombres de los dominios para los que el servidor acepta correo. El servidor Sendmail puede recibir correo de dominios diferentes o subdominios que dependen de la misma raíz, siempre que el DNS esté configurado correctamente*

En *Sendmail* también es posible configurar equipos virtuales de forma que un mismo servidor pueda manejar el correo de diferentes dominios. Esto se consigue configurando correctamente en el DNS todos los registros *MX* de los dominios involucrados, además de acceder al icono "Mapeo de Direcciones (virtuser)" del módulo *Sendmail* de Webmin.

Se puede utilizar el icono "Buzones de Usuario" del módulo *Sendmail* en Webmin para realizar pruebas de envío de correo entre usuarios o a través de otros servidores. La Figura 7.12 muestra la ventana de esta utilidad. Hay que indicar que esta herramienta no debe utilizarse para que los usuarios puedan consultar su correo, ya que Webmin no tiene ningún sistema de gestión de permisos para el acceso de usuarios no administradores (Webmin es una herramienta de configuración y administración, no de explotación de sistemas). *Sendmail* realiza una gestión muy sencilla de los buzones de correo de los usuarios utilizando las cuentas de usuarios del sistema y el programa de línea de órdenes *mail*, por lo que si se desea una gestión más avanzada, entonces es necesario instalar algún programa de gestión de buzones.

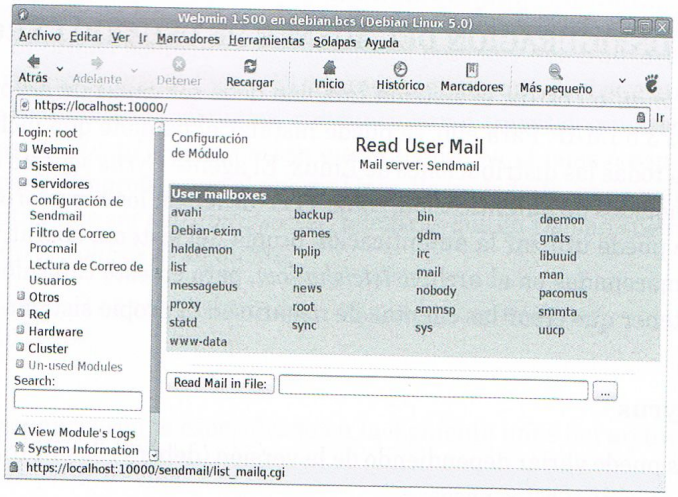


Figura 7.12. *Ventana de consulta del correo de los usuarios en el módulo Sendmail de Webmin. Con esta herramienta se pueden realizar pruebas de funcionamiento del servidor de correo, aunque no sirve para una gestión normal. En esta ventana aparecen todos los nombres de las cuentas de usuario en el equipo local*

Una vez configurado y reiniciado *Sendmail*, se puede comprobar si el puerto 25 de SMTP acepta recibir correo mediante una conexión Telnet, según se muestra en la Figura 7.13 (*localhost* se puede sustituir por el nombre o dirección del servidor de correo). El envío del mensaje simulado a través de Telnet se realiza escribiendo las órdenes reconocidas por SMTP, tal y como se muestra en el esquema del apartado 6.2.2.1 del capítulo 6.

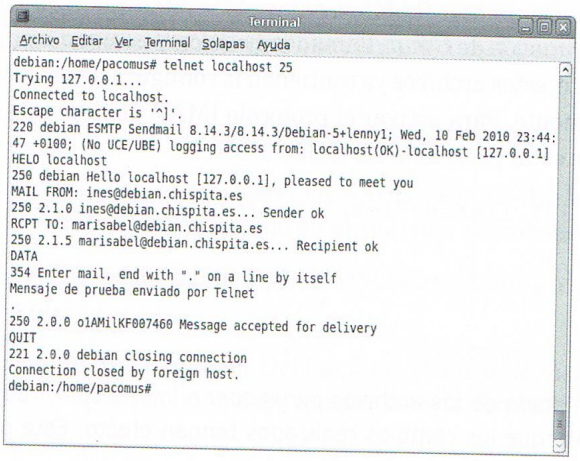


Figura 7.13. *Prueba de Sendmail a través de Telnet. Con este programa se puede simular la transferencia de correo a través de SMTP. Como se puede observar, se realiza una conexión al puerto 25 y a continuación se envían todos los datos del mensaje*

En caso de que sea necesario realizar algunas modificaciones directamente sobre el archivo *sendmail.mc*, hay que tener mucho cuidado para no cometer errores de sintaxis, porque entonces *Sendmail* no funcionará. Cada vez que se realicen modificaciones sobre este archivo, hay que pulsar en el botón "Reconstruir configuración de Sendmail", que se encuentra en la página "Configuración M4 de Sendmail" del módulo de configuración de *Sendmail* en Webmin, para generar el archivo *sendmail.cf*. Si no se muestra ningún error, entonces hay que parar y volver a iniciar el proceso demonio de *Sendmail*, usando los botones "Parar Sendmail" y "Arrancar Sendmail", que se encuentran en la página principal del módulo de configuración de *Sendmail* en Webmin. También se pueden activar los cambios reiniciando el proceso demonio *sendmail* a través de un programa editor de niveles de ejecución.

7.2.2 INSTALACIÓN Y CONFIGURACIÓN DEL AGENTE DE USUARIO CYRUS

Además del servidor *Sendmail* o Postfix, el sistema también debe ser capaz de aceptar peticiones de los clientes a través de los protocolos POP3 o IMAP. Para ello, se puede instalar el paquete que incluya estos protocolos, como el agente **Cyrus** disponible para todas las distribuciones de Linux. El agente *Cyrus* soporta distintos servidores de correo y permite utilizar distintos métodos de autenticación, como TLS (usado en los servidores Microsoft Windows), SASL, MD5 o Kerberos. También se puede utilizar la autenticación propia del sistema operativo a través de las cuentas de usuario y las contraseñas almacenadas en el archivo */etc/shadow*, pero en este capítulo nos vamos a decantar por el uso de SASL y así evitamos tener que crear las cuentas de usuario en el propio sistema operativo.

7.2.2.1 Instalación de Cyrus

La configuración de *Cyrus* puede variar dependiendo de la versión (deberá consultar la documentación que incluye el paquete) pero, en general, se siguen estos pasos:

1 Instalar los paquetes de *Cyrus* en el sistema, preferiblemente aquellos que se incluyen con la distribución de GNU/Linux utilizada. Se recomienda instalar el archivo binario (*rpm*, *deb*, etc.) ya que la configuración resultará más sencilla, teniendo en cuenta que muchas opciones por defecto estarán establecidas a sus valores apropiados. En el caso de Debian 5, necesitaremos los siguientes paquetes: *cyrus-common-2.2*, *cyrus-imapd-2.2*, *cyrus-admin-2.2*, *cyrus-doc-2.2* y *cyrus-clients-2.2* (son necesarios más paquetes, pero estos se instalarán automáticamente para resolver las dependencias).

2 Acceder a la documentación del paquete, normalmente ubicada en la carpeta */usr/share/doc*. Deberá existir una carpeta cuyo nombre comience por "cyrus" que contendrá varios archivos de ayuda con todos los pasos para la instalación.

3 Acceder a los archivos de configuración de *Cyrus*, llamados *cyrus.conf* e *imapd.conf*, que normalmente se encontrarán en la carpeta */etc*. Habitualmente, estos archivos ya contienen la configuración básica necesaria para que los protocolos IMAP y POP3 funcionen correctamente. Para activar el protocolo IMAP, no debe estar comentada la siguiente línea del archivo *cyrus.conf*, es decir, no debe estar precedida del símbolo "#":

```
imap      cmd="imapd -U 30" listen="imap" prefork=0 maxchild=100
```


Cualquier cambio en el contenido de los archivos *cyrus.conf* o *imapd.conf*, requiere del reinicio del proceso demonio *cyrus*, para que los cambios realizados tengan efecto. Este proceso se puede reiniciar usando un programa editor de niveles de ejecución.

4 De igual forma, para activar el protocolo POP3, no debe estar comentada la siguiente linea del archivo *cyrus.conf*:

```
pop3      cmd="pop3d -U 30" listen="pop3" prefork=0 maxchild=50
```


Si se quiere activar el agente de usuario POP3 de *Cyrus*, también hay que instalar el paquete correspondiente, que en Debian 5 es *cyrus-pop3d-2.2*.

5 La comunicación entre *Sendmail* y *Cyrus* se puede configurar de dos formas: usando un *socket* o *conector TCP* o usando un *conector Unix*. El primer método es más complejo, pero hay que utilizarlo cuando el agente *Sendmail* está instalado en un equipo distinto al agente *Cyrus*. El segundo método, que es el que utilizamos aquí, es más sencillo y se basa en crear puertos de comunicación virtuales, que funcionan a través de un archivo, aunque este mecanismo solo funciona si los programas *Sendmail* y *Cyrus* están ejecutándose en el mismo equipo. Es conveniente echar un vistazo al archivo *cyrus.conf* para comprobar que el puerto Unix, llamado *lmtp*, se encuentra en la ubicación correcta. En sistemas OpenSUSE, la ruta suele ser */var/lmtp/socket*, mientras que en Debian suele ser */var/run/cyrus/socket*. La línea que hay que revisar en *cyrus.conf* es la siguiente:

```
lmtpunix      cmd="lmtpd" listen="/var/run/cyrus/socket/lmtp"
prefork=0 maxchild=50
```

6 Lo anterior debe ir en consonancia con lo especificado en la siguiente línea del archivo *imapd.conf*:

```
lmtpsocket: /var/run/cyrus/socket/lmtp
```

7 Indicar a *Sendmail* que envíe el correo a los buzones de *Cyrus*. Para ello, hay que añadir las siguientes líneas al final del archivo de configuración M4. Esto se puede hacer a a través de *Webmin* o directamente editando el archivo *sendmail.mc*. Las siguientes líneas pueden variar dependiendo de la versión de *Sendmail* o *Cyrus*, por lo que es recomendable consultar la documentación instalada con estos paquetes:

```
define(`confLOCAL_MAILER',`cyrusv2')
MAILER(`cyrusv2')
```

8 Una vez configurado *Sendmail*, se genera el archivo *sendmail.cf* y se reinicia este programa demonio. En este punto, también es recomendable reiniciar el proceso demonio de *Cyrus*, habitualmente llamado *cyrus2.2*, para que los cambios tengan efecto. Después, se comprueba si el protocolo IMAP está funcionando correctamente, utilizando un programa explorador de puertos (*nmap*, por ejemplo). Hay que consultar si el puerto 143 está abierto.

7.2.2.2 Instalación de SASL

A continuación, debemos asegurarnos de que el servicio **SASL** (*Simple Authentication and Security Layer* o Autenticación Simple y Capa de Seguridad) está instalado en el sistema. Seguiremos estos pasos:

1 Comprobar que se encuentran instalados los paquetes *libsasl2-2* y *sasl2-bin*, en caso negativo, hay que instalarlos con la herramienta correspondiente.

2 Editar el archivo de configuración de SASL, que en Debian 5 es */etc/default/saslauth* y poner el valor "yes" en el parámetro "START", lo que significa que esa línea debe quedar de esta forma:

```
START=yes
```

3 Reiniciar el proceso demonio de SASL, que normalmente se llama *saslauth*, usando alguna herramienta de gestión de los niveles de ejecución. En Debian 5 se puede hacer con esta orden:

```
# /etc/init.d/saslauth restart
```

4 A continuación, establecemos la contraseña SASL del usuario *cyrus*, que es la cuenta que se utiliza para crear y gestionar cuentas y buzones de correo. Para ello, tenemos que ejecutar la orden *saslpasswd2*, que es la que se utiliza para establecer las contraseñas de autenticación en SASL:

```
# saslpasswd2 -c cyrus
```

Después se puede usar la siguiente orden para comprobar si se establece una conexión por IMAP al equipo usando el usuario *cyrus* (con la contraseña indicada anteriormente). Deberá mostrar un mensaje como "L01 OK User logged in"):

```
# imtest -m login -u cyrus localhost
```

Si lo anterior no funciona correctamente, es posible que la configuración de *Cyrus* todavía no tenga efecto. Para aplicar todos los cambios realizados, es recomendable reiniciar el proceso demonio de *Cyrus*.

7.2.2.3 Gestión de los buzones

Una vez comprobado que el servicio está operativo, entonces hay que crear los buzones de correo de los usuarios. Como se explica en los apartados anteriores, *Cyrus* se instala por defecto con soporte para SASL, por lo que no es necesario crear una cuenta de usuario en el equipo para crear una cuenta de correo. Para crear los buzones de correo se usa la orden *cyradm*, que acepta las órdenes explicadas en la tabla 7.1. En la Figura 7.14 se muestra un ejemplo de inicio de sesión en la herramienta *cyradm*, que se realizará usando el usuario *cyrus* de la siguiente forma (se puede acceder también desde otro equipo, sustituyendo *localhost* por el nombre o dirección IP del servidor):

```
# cyradm -u cyrus localhost
```

Tabla 7.1. Órdenes que reconoce cyradm

Orden	Abreviatura	Descripción
createmailbox	cm	Crea un buzón de correo para el usuario especificado.
deleteaclmailbox	dam	Elimina una lista de control de acceso de un buzón especificado.
deletemailbox	dm	Elimina un buzón de correo de un usuario. Versiones antiguas de *Cyrus* no permiten eliminar buzones de correo.
help		Muestra ayuda.
listaclmailbox	lam	Muestra la lista de control de acceso del buzón de correo especificado.
listmailbox	lm	Muestra una lista de los buzones de correo existentes.
listquota	lq	Muestra la cuota asignada a un buzón de correo existente.
listquotaroot	lqr	Muestra la cuota asignada al buzón de correo del usuario *root*.
quit		Sale de *cyradm*.
renamemailbox	renm	Cambia el nombre de un buzón de correo.
setaclmailbox	sam	Establece la lista de control de acceso de un buzón de correo existente.
setquota	sq	Establece la cuota de disco para un buzón de correo.

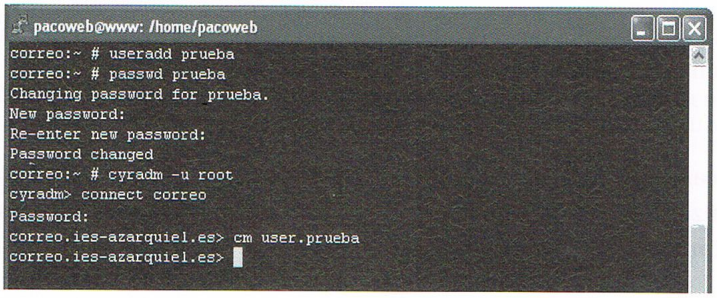


Figura 7.14. Ejemplo de inicio de sesión de la orden cyradm. En este ejemplo se ha accedido a la herramienta utilizando la cuenta de administrador root sobre el equipo denominado "correo" (es el equipo que tiene instalado el sistema de correo). Habitualmente, se usa la cuenta cyrus para acceder a esta herramienta. Se puede observar que se ha creado una cuenta de usuario llamada "prueba" y también su buzón de correo asociado

El agente *Cyrus* necesita que todos los buzones de correo de los usuarios cuelguen de un buzón primario llamado "user". Por esta razón, cuando se especifica un nombre de un buzón de correo asociado a un usuario, éste debe tener la forma "user.*nombre*", donde *nombre* es el nombre del buzón del usuario.

Como se puede observar en la tabla 7.1, la orden *cyradm* permite establecer **cuotas de disco** para los buzones de correo. De esta forma el administrador puede establecer restricciones de espacio de los buzones y así impedir que puedan crecer hasta ocupar todo el disco del servidor. También se pueden establecer **listas de control de acceso**, que son permisos que se pueden establecer para que los usuarios puedan realizar ciertas operaciones sobre los buzones de correo (por ejemplo, leer el buzón de otro usuario, crear o eliminar un buzón, crear carpetas para clasificar el correo, etc.). Puede obtener una descripción detallada de las listas de control de acceso de *cyrus* con la siguiente orden:

```
# man cyradm
```

En el apartado 7.3.4 de este capítulo se incluye una ayuda ante problemas de configuración con *Cyrus*.

Una vez creados los buzones de correo de los usuarios, es necesario establecer las contraseñas para poder autenticarse en una conexión a través del agente IMAP. Para ello, se usa la orden *saslpasswd2*, seguida del nombre de la cuenta de correo. Esta orden pedirá que se introduzca dos veces la contraseña del usuario:

```
# saslpasswd2 -c usuario
```

Una vez creadas las cuentas y establecidas sus contraseñas, se puede comprobar si se puede establecer una conexión por IMAP al equipo usando éstas. Para ello, se puede utilizar un programa cliente de correo o la orden *imtest*, de la misma forma que se ha comprobado para el usuario *cyrus* en el apartado anterior. Recordar que la conexión se realiza correctamente si después de escribir la contraseña del usuario aparece el mensaje "L01 OK User logged in"):

```
# imtest -m login -u usuario localhost
```

La comprobación de conexión con la orden *imtest* también se puede realizar desde otro equipo para saber si es posible acceder desde la red. Para ello, en los parámetros de la orden *imtest* hay que sustituir *localhost* por el nombre o dirección IP del servidor de correo.

7.3 PROBLEMAS Y SOLUCIONES

Los sistemas de transferencia de correo electrónico utilizan protocolos de comunicación bastante simples para el envío de los mensajes. Sin embargo, dada la existencia de otros protocolos adicionales que interaccionan con el sistema de correo y que son de gran complejidad (por ejemplo, el sistema DNS), la solución de los problemas planteados en las configuraciones suele resultar difícil. En este apartado nos dedicaremos a exponer los problemas más comunes que se pueden plantear a la hora de instalar y configurar un sistema de transferencia de correo electrónico.

Cuando un usuario o administrador envía un correo electrónico a través de su sistema de transferencia, éste puede ser devuelto a su origen en caso de que se produzca algún tipo de error. Esta devolución se realiza normalmente utilizando una cuenta de correo especial llamada *MAILER-DAEMON* que se corresponde con el sistema que lleva a cabo la transferencia de correo. Esto quiere decir que esta cuenta es la que aparece como emisora del mensaje, además del nombre del dominio al que pertenece el servidor que lo generó. Normalmente, junto con el mensaje, se incluye información adicional indicando el tipo de error producido. Por lo tanto, la mejor forma de investigar las causas de posibles errores en nuestro sistema de correo consiste en consultar los mensajes de correo devueltos y los mensajes de error insertados por el sistema. En el ejemplo 7.1 se muestra un fragmento de mensaje de correo devuelto con error.

EJEMPLO 7.1

Lo siguiente muestra un fragmento de mensaje de correo devuelto con error (los puntos suspensivos indican que el mensaje continúa):

```
De: MAILER-DAEMON@smtp.email.es (Mail Delivery System)
Para: marisabel@correo.es
Tema: Undelivered Mail Returned to Sender
Fecha: 12 Jan 2005 18:36:26 +0000

Texto del mensaje:
This is the Postfix program at host smtp.email.es.
I'm sorry to have to inform you that the message returned
Below could not be delivered to one or more destinations.
For further assistance, please send mail to <postmaster>
If you do so, please include this problem report. You can
Delete your own text from the message returned below.
The Postfix program

<marisabel@correo.es>: Name service error for correo.es:
Host found but no data record of requested type
[...]
```

En el fragmento de mensaje anterior se incluye la siguiente información:

- Nombre del servidor de correo al que iba destinado el mensaje.
- Usuario destinatario del correo.
- Agente de transporte de correo del servidor (en este ejemplo es *Postfix*).
- Mensaje de error (en el ejemplo es "Host found but no data record of requested type").
- Contenido del correo enviado (se ha omitido en el ejemplo).

El mensaje de error que se incluye con este correo devuelto indica que el servidor destinatario del correo se ha encontrado, pero no existe un registro DNS de tipo *MX* asociado a él.

7.3.1 PROBLEMAS RELACIONADOS CON EL DNS

Uno de los problemas más habituales en la instalación y configuración de un sistema de correo consiste en la interacción con el sistema DNS. Puesto que las direcciones de correo están formadas por nombres de equipos y dominios, es necesario que el sistema de correo sea capaz de resolver direcciones a través del DNS.

Para que un servidor de correo pueda funcionar correctamente necesita que se definan dos registros DNS:

- Un registro tipo *A* para que se pueda asociar el nombre del equipo con su dirección IP (correspondencia directa).
- Un registro *PTR* para que se pueda asociar la dirección IP del equipo con su nombre (correspondencia inversa).
- Un registro de tipo *MX* para indicar que el equipo es un servidor de correo electrónico.

No es obligatorio que un servidor de correo tenga asociado un registro de tipo *PTR*. Sin embargo, algunos servidores de correo no aceptan ningún mensaje que provenga de un servidor que no tenga perfectamente establecidas sus correspondencias directas e inversas. Así, estos servidores comprueban las correspondencias directas e inversas de los correos que reciben y realizan un filtrado del correo basura o *spam* (aquel en el que no coincide la dirección IP y el nombre de dominio de origen).

En caso de que no se haya establecido correctamente el registro *MX* de correo, los mensajes pueden incluir errores de tipo *Host found but no data record of requested type* (se ha encontrado el equipo pero no hay registro de datos del tipo solicitado). Si no se ha establecido ningún registro de tipo *A*, entonces el mensaje de error puede ser *Host not found* (no se ha encontrado el equipo).

7.3.2 PROBLEMAS RELACIONADOS CON LOS PUERTOS DEL SERVIDOR

El servidor de correo necesita una "puerta de acceso" por donde enviar o recibir los mensajes de correo. Por defecto, en una instalación de un sistema de correo solamente está permitida la *entrega local*, es decir, solamente se permiten los mensajes que van desde y hasta el equipo local. Para poder enviar y recibir mensajes de correo con el exterior, es necesario abrir una puerta que permita la comunicación.

Los protocolos de transporte de correo electrónico utilizan el puerto número 25 (SMTP) a través del cual se envían y se reciben los mensajes desde y hacia los servidores. Si ese puerto no está abierto o tiene problemas (normalmente porque hay un cortafuegos o encaminador o porque la configuración no es correcta), entonces no será posible establecer una comunicación para transferir el correo. El ejemplo 7.2 muestra esta situación.



EJEMPLO 7.2

Un ejemplo de fragmento de correo devuelto con error cuando el puerto 25 del servidor no está abierto es el siguiente (los puntos suspensivos indican que el mensaje continúa):

```
De: MAILER-DAEMON@smtp.email.es (Mail Delivery System)
Para: marisabel@correo.es
Tema: Undelivered Mail Returned to Sender
Fecha: 12 Jan 2005 18:36:26 +0000

Texto del mensaje:
This is the Postfix program at host smtp.email.es.
I'm sorry to have to inform you [...]

<marisabel@correo.es>: connect to 80.95.34.86[80.95.34.86]:
connection timed out
[...]
```

El mensaje de error *connection timed out* (tiempo de conexión agotado) se produce porque el equipo no puede establecer una conexión con el puerto 25 del servidor destinatario de correo. El sistema realiza una serie de reintentos, hasta que finalmente desiste y devuelve el mensaje con esta notificación.

En caso de que el servidor de correo deba transferir también mensajes a los equipos clientes, entonces deben estar activos y abiertos los puertos relacionados con los protocolos POP3 (110) e IMAP (143). En caso contrario, los clientes no podrán descargar ni consultar su correo.

Una forma sencilla de comprobar si están abiertos los puertos necesarios consiste en utilizar un programa de exploración de puertos, como puede ser *nmap* para Linux o *Languard* para Windows. La exploración se debe hacer sobre la dirección IP del equipo, ya que los puertos pueden estar abiertos solo para las conexiones locales (dirección *localhost* o 127.0.0.1) y no estar abiertos a otros equipos de la red.

7.3.3 PROBLEMAS CON SENDMAIL

Si *Sendmail* muestra errores al compilar el archivo *sendmail.mc* y generar el archivo *sendmail.cf*, es posible que exista algún error de sintaxis. Hay que tener cuidado al escribir directamente sobre el archivo *sendmail.mc*, ya que cualquier pequeño error de sintaxis nos puede dar quebraderos de cabeza. Es habitual encontrar errores en los caracteres entrecomillados (hay que usar ` para abrir comillas y ' para cerrarlas) o en la posición de las tabulaciones (en vez de usar varios espacios en blanco). Si se produce algún error al generar el archivo *sendmail.cf*, éste se guarda en el archivo *sendmail.cf.errors*, que es recomendable consultar para saber qué es lo que está ocurriendo. La ubicación de estos archivos puede variar y en Debian 5 es */etc/mail*.

Otra fuente de información que resulta muy útil consultar para detectar errores son los archivos *mail.log*, *mail.warn* y *mail.err*, que en Debian 5 están ubicados en la carpeta */var/log*. En estos archivos se registran todas las incidencias que se producen mientras el servidor de correo electrónico está en funcionamiento.



EJEMPLO 7.3

En muchas ocasiones es posible que el agente de correo *Sendmail* devuelva mensajes como *User Unknown* (usuario desconocido), haciendo referencia a que no encuentra el buzón del usuario destinatario del mensaje. Esto puede ser debido a que el destinatario especificado no existe o bien la configuración del agente MUA no es correcta, lo que hace que *Sendmail* no conozca los buzones definidos a través de ese agente. En este segundo caso, es recomendable revisar que la configuración de agente MUA es correcta (véase el apartado 7.2.2.1), que el archivo *sendmail.cf* ha sido generado correctamente y que el proceso demonio de *Sendmail* se ha reiniciado para aplicar los cambios.

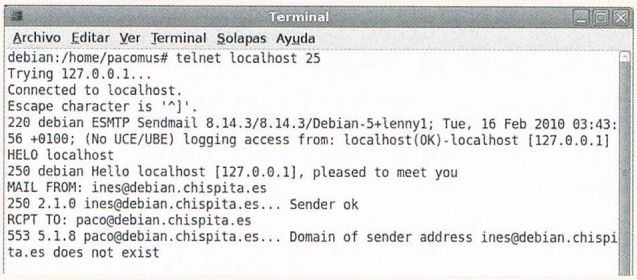


Figura 7.15. *Ejemplo de mensaje de error devuelto por Sendmail cuando no encuentra el buzón del usuario. Esta situación se produce debido a que la cuenta del destinatario no ha sido creada o bien las directivas del agente MUA no han sido especificadas correctamente*



EJEMPLO 7.4

También resulta frecuente encontrar errores de tipo *No such file or directory* en el archivo mail.err. Esto suele ser debido a que no se ha instalado algún paquete necesario. Por ejemplo, puede aparecer este error:

```
Jan 4 15:52:39 debian sendmail[5011]: p04EqdE5005009: SYSERR(root): Cannot exec
/usr/sbin/sensible-mda: No such file or directory
```

Esto significa que es necesario instalar el paquete *sensible-mda* para que *Sendmail* funcione correctamente.

7.3.4 PROBLEMAS CON CYRUS

La mayoría de los problemas a los que nos enfrentamos cuando nuestra configuración del agente *Cyrus* no funciona correctamente tienen que ver con dos cuestiones fundamentales:

- La interacción con el agente de transporte de correo: estos problemas suelen producirse debido a que la configuración del agente (*Sendmail*, Postfix, etc.) tiene establecidos unos parámetros diferentes a los del agente *Cyrus* y, por lo tanto, la transferencia de correo de un agente a otro no se produce.
- El método utilizado para la autenticación de los usuarios: el agente *Cyrus* permite distintos métodos de autenticación de usuarios, algunos de ellos bastante complejos de configurar. Se recomienda comenzar con la autenticación básica SASL y depués realizar configuraciones más avanzadas.

Cuando se va a realizar una instalación del agente *Cyrus*, a no ser que ya se disponga de conocimientos avanzados, se recomienda instalar el paquete binario (*rpm*, *deb*, etc.) para la distribución y versión concreta de GNU/Linux. De esta forma, instalaremos un paquete que está preparado para funcionar en la versión concreta del sistema y la mayoría de opciones de configuración se habrán establecido a sus valores adecuados. De todas formas, es recomendable repasar las opciones de configuración del agente de transporte (Sendmail, Postfix, etc.) y las opciones de *Cyrus* (archivos de configuración */etc/cyrus.conf* y */etc/imapd.conf*) para comprobar que concuerdan y son consistentes unas con otras. Para comprobar que todas las modificaciones se llevan a efecto, también es recomendable reiniciar el proceso demonio de *Cyrus*.

Por ejemplo, es posible que *Sendmail* y *Cyrus* utilicen una configuración por defecto distinta para ubicar el conector *lmtp* (es el que se utiliza para que *Sendmail* y *Cyrus* puedan comunicarse). Para comprobar este extremo, hay que accerder a la configuración de *Sendmail* (archivo */etc/sendmail.cf*) y buscar todas las refernencias a *lmtp*. Después deberán establecerse a la misma ruta que indiquen los arhivos de configuración de *Cyrus*.

Otra ayuda importante a la hora de localizar y resolver errores es el registro de *log* del sistema, que se guarda en la carpeta del sistema */var/log*. En él, podemos encontrar archivos que guardan los mensajes de error que se producen cuando algún servicio no funciona correctamente.

Cuando se instala *Cyrus* también hay que tener cuidado con la configuración que éste incluye por defecto. En concreto, algunas versiones de *Cyrus* no reconocen al usuario *cyrus* como administrador de los buzones de los usuarios. Esto impide que se puedan crear cuentas de correo usando esta cuenta de usuario. El error común que puede aparecer es el siguiente:

```
# cyradm -u cyrus localhost
Password:
localhost> cm user.ines
createmailbox: Permission denied
localhost>
```

Este problema se soluciona incluyendo al usuario *cyrus* como administrador de los buzones. Para ello, hay que editar el archivo *imapd.conf*, escribir la siguiente línea de esta forma (si aparece con el símbolo # delante, hay que quitarlo) y reiniciar el proceso demonio *cyrus*:

```
admins: cyrus
```

RESUMEN DEL CAPÍTULO

La instalación y configuración de un servidor de correo electrónico es una compleja tarea, sobre todo por la gran cantidad de protocolos y servicios involucrados, además de la necesidad de que estos funcionen de forma coherente.

Para configurar un servidor de correo electrónico es necesario, en primer lugar, configurar correctamente el DNS para que se resuelvan correctamente los nombres de equipo y dominios en las direcciones de correo. También es necesario definir un registro de tipo *MX* que especifique la dirección IP del equipo que va a funcionar como servidor de correo electrónico.

En segundo lugar, el equipo necesita ejecutar un agente de correo MTA que le permita reenviar el correo destinado a otros servidores, además de aceptar el correo para el dominio asociado a él. Algunos de los agentes de correo más conocidos actualmente son: IIS de Microsoft Windows Server 2003, Microsoft Exchange Server 2007 y *Sendmail*.

En tercer lugar, el equipo también necesita ejecutar un agente de usuario MUA para que el correo se pueda distribuir a los ordenadores de los usuarios. Los sistemas Microsoft IIS y Exchange Server ya disponen de estos agentes, mientras que en los sistemas GNU/Linux es necesario instalar un agente como *Cyrus*.

Para configurar un servidor de correo electrónico con Microsoft Windows Server 2003 es necesario, en primer lugar, instalar el componente *Internet Information Services* (IIS), con soporte para SMTP y POP3.

Por su parte, para configurar un servidor de correo con Microsoft Exchange Server 2007 es necesario instalar previamente los componentes IIS, servidor de aplicaciones, *Power Shell* y el *Directorio Activo*, este último configurado como controlador de dominio. Una vez hecho esto, se realiza la instalación de Exchange Server, ejecutando el programa desde los discos de instalación o desde un archivo comprimido descargado. Una vez instalado, se pueden asociar cuentas de correo electrónico a los usuarios definidos en el *Directorio Activo*. Además, para cada una de estas cuentas, se puede especificar el agente MUA a utilizar (POP3, IMAP, Outlook Web, etc.).

En los sistemas GNU/Linux se disponen de muchas alternativas a la hora de instalar y configurar un servidor de correo electrónico, tanto para el agente MTA (*Sendmail*, Postfix, etc.) como para el agente MUA (*Cyrus*, Procmail, etc.). Sin embargo, es necesario disponer de unos conocimientos más avanzados para poder llevar a cabo con éxito la instalación y configuración del sistema.

Para instalar *Sendmail* en GNU/Linux es necesario, en primer lugar, instalar el paquete *sendmail* y desinstalar cualquier otro agente instalado por defecto (normalmente es Exim). A continuación, se accede al módulo de configuración de *Sendmail* en Webmin y se establecen los dominios locales para los que se va a aceptar el correo entrante. También hay que establecer las direcciones IP de los adaptadores de red desde donde se va a recibir el correo exterior.

Por su parte, la instalación del agente *Cyrus* requiere, en primer lugar, de la instalación de los paquetes asociados. Después, hay que comprobar que se ha activado el servicio IMAP en *cyrus.conf*. A continuación se comprueba que es correcta la configuración de conector *lmtp* Unix indicada en los archivos *cyrus.conf* e *imapd.conf*. Finalmente, es necesario añadir la configuración correspondiente en el archivo *sendmail.mc* para indicar a *Sendmail* que el correo entrante debe ser entregado a *Cyrus*. Para que esta configuración se lleve a efecto, hay que generar el archivo *sendmail.cf* y reiniciar los procesos demonio *sendmail* y *cyrus*.

La autenticación de los usuarios en *Cyrus* se lleva a cabo por defecto utilizando SASL, para lo que hay que instalar también este paquete e indicar que debe activarse en el archivo *saslauth*. Finalmente, para crear los buzones de correo y asociarles las contraseñas de autenticación, hay que utilizar las órdenes *saslpasswd2* y *cyradm*, ésta última ejecutada con el usuario *cyrus*.

EJERCICIOS PROPUESTOS

- **1.** Indica todos los pasos a seguir para configurar un servidor de correo en GNU/Linux usando *Sendmail* y *Cyrus*.
- **2.** Sobre el servidor creado en el ejercicio 1, especifica los pasos a seguir para crear tres cuentas de correo y permitir que se pueda acceder a éstas desde un programa cliente de correo.
- **3.** Sobre el servidor creado en el ejercicio 1, especifica los pasos a seguir para configurar el programa cliente de correo Microsoft Outlook y acceder a una de las cuentas creadas en el ejercicio anterior.
- **4.** Repite el ejercicio anterior pero esta vez usando otro cliente de correo GNU, como Evolution o KMail.
- **5.** Si creas una cuenta de usuario para iniciar sesión en GNU/Linux, ¿es posible enviar correo a esa cuenta? ¿Cómo se puede consultar el correo recibido? ¿Cómo gestiona *Sendmail* este tipo de cuentas con respecto a las cuentas creadas con *Cyrus*?
- **6.** Para las cuentas de correo creadas en el ejercicio 2, establece cuotas de disco para limitar el espacio disponible en los buzones. Indica los pasos que has seguido para conseguir esto.
- **7.** Instala un servidor de correo con IIS o Exchange Server e indica los pasos que debes seguir para establecer cuotas de disco y limitar el tamaño de los buzones de los usuarios.

TEST DE CONOCIMIENTOS

1 Para que un servidor de correo funcione correctamente necesita que se haya definido un registro DNS de tipo:
a) *MX*.
b) *A*.
c) *TXT*.
d) a y b son ciertas.

2 Un servidor de correo virtual en IIS gestiona:
a) Buzones que no están asociados a cuentas de usuario.
b) Varios dominios simultáneamente.
c) Varios servidores POP3 simultáneamente.
d) Ninguna es cierta.

3 Microsoft Exchange Server 2007 permite gestionar:
a) Multitud de cuentas de correo diferentes.
b) Varios dominios simultáneamente.
c) Varios agentes MUA.
d) Todas son ciertas.

4 Para instalar Exchange Server 2007 es necesario que el equipo funcione como:
a) Controlador primario de dominio.
b) Controlador de reserva de dominio.
c) Servidor web.
d) a y b son ciertas.

5 Para establecer los correos que va a recibir un servidor *Sendmail* hay que especificar:
a) Los nombres de los dominios locales.
b) Las cuentas de usuario del equipo.
c) Las direcciones IP de los equipos que van a enviar los mensajes.
d) Ninguna es cierta.

6 Un servidor *Sendmail* no va a aceptar correo desde otros servidores si no se especifica:
a) Las direcciones de los adaptadores de red por donde se reciben.
b) Las direcciones de los servidores que envían.
c) Los dominios de los servidores en los que confía.
d) Todas son ciertas.

7 La comunicación entre *Sendmail* y Cyrus se puede realizar por:
a) Un conector TCP/IP.
b) Un conector Unix.
c) El archivo *lmtp*.
d) Todas son ciertas.

8 El servicio SASL se usa para:
a) Autenticar a los usuarios que acceden a su correo.
b) Cifrar los mensajes de correo.
c) Autenticar a otros servidores de correo.
d) Crear los buzones de los usuarios.

9 En *cyradm* se usa la siguiente orden para crear una cuenta de correo:
a) *cm*.
b) *lm*.
c) *dm*.
d) *lq*.

8 Mensajería instantánea

OBJETIVOS DEL CAPÍTULO

- ✓ Describir los servicios de mensajería instantánea.
- ✓ Explicar los diferentes protocolos utilizados en los servicios de mensajería instantánea.
- ✓ Instalar y configurar el servicio de mensajería instantánea.
- ✓ Utilizar clientes gráficos y de texto de mensajería instantánea.
- ✓ Crear cuentas de usuario y verificar el acceso a los servicios de mensajería instantánea.

Los servicios de mensajería instantánea están orientados al envío de mensajes de texto entre usuarios, aunque algunos también permiten el envío de archivos adjuntos. Estos servicios se diferencian fundamentalmente del correo electrónico en que, para que los usuarios puedan recibir los mensajes, estos deben estar conectados y "en línea".

Este capítulo está dedicado a explicar los servicios de mensajería instantánea más utilizados en la actualidad, además de los procedimientos a seguir para instalarlos, configurarlos y acceder a ellos. Existen muchos sistemas de mensajería instantánea que funcionan actualmente en Internet, como IRC, Google Talk u otros servicios de *chat* ofrecidos a través de páginas *web* dinámicas.

8.1 INTRODUCCIÓN

La **mensajería instantánea**, también conocida como *chat* o *cibercharla*, es una forma de comunicación basada en texto que se realiza en tiempo real, mientras los intervinientes se encuentran conectados. En esta comunicación, los mensajes son redactados a través del teclado del ordenador y enviados al destino mediante la red de comunicación que los conecta. De la palabra inglesa *chat* ha surgido el verbo *chatear* en los países de habla hispana y, desde 2007, ha sido reconocido en la Real Academia Española.

Para que el servicio de mensajería instantánea funcione correctamente, es necesario que exista un programa adecuado en los equipos de los usuarios que se comunican. Dependiendo del tipo de protocolo utilizado en la comunicación, es posible que también sea necesaria la intervención de otro equipo que funcione como servidor.

El servicio de mensajería instántánea puede ofrecer, además del envío de mensajes entre usuarios, las siguientes funciones:

- **Aviso de presencia**: permite avisar a los usuarios cuando estos se encuentran conectados.
- **Buzón de mensajes**: es el lugar donde se almacenan los mensajes de aquellos usuarios que no están conectados.
- **Transferencia de archivos**: para permitir el intercambio de archivos entre el origen y el destino.
- **Comunicación de voz**: para que los usuarios puedan comunicarse a través de un micrófono sin necesidad de teclear los mensajes.

Actualmente existen multitud de servicios de mensajería instantánea disponibles a través de Internet. Algunos de ellos utilizan programas y protocolos propietarios, mientras que otros utilizan protocolos más estandarizados, como XMPP (véase el apartado 8.2.2). La ventaja de utilizar un protocolo estandarizado radica en que no está bajo el control de una única organización y además se posibilita la comunicación utilizando diferentes programas.

8.2 TIPOS DE SERVICIOS DE MENSAJERÍA INSTANTÁNEA

Actualmente en Internet coexisten multitud de servicios de mensajería instantánea, algunos de ellos propiedad de empresas u organizaciones y otros basados en protocolos estándares como XMPP (véase el apartado 8.2.2). Los más importantes se explican en los apartados siguientes.

8.2.1 IRC

IRC (*Internet Relay Chat* o Conversación Retransmitida por Internet) es un protocolo de comunicación entre ordenadores a través de una red de transmisión de datos como puede ser Internet. Se usa como un sistema de conversación en tiempo real, es decir, los usuarios pueden enviar o recibir mensajes mientras están conectados. El servicio IRC nació en 1988 en Finlandia y, aunque tuvo una gran difusión en Internet, actualmente se está quedando obsoleto con respecto a otros sistemas más modernos. Las características más importantes que tiene el servicio IRC son:

- En cada conversación puede intervenir más de dos personas.
- Las conversaciones se pueden realizar mediante canales que son una especie de salones virtuales donde conversan los usuarios.
- Los usuarios pueden ocultar su identidad.

El servicio IRC esta basado en el **modelo cliente-servidor**. Esto quiere decir que para que los usuarios puedan enviar o recibir mensajes debe existir al menos un ordenador que trabaje como servidor, cuyas funciones son las de reunir todos los mensajes que envían los usuarios, procesarlos y enviarlos a sus destinatarios. Por lo tanto, los mensajes no son enviados directamente del usuario de origen al destinatario sino que pasan previamente por el servidor, que ejecuta los programas necesarios para procesarlos. Así mismo los usuarios tienen que establecer una conexión con el servidor para poder enviar sus mensajes a otros usuarios utilizando para ello un programa cliente de IRC cuyas funciones son:

- ✓ Conectar y desconectar con el servidor.
- ✓ Enviar los mensajes tecleados por el usuario al servidor.
- ✓ Recibir los mensajes del servidor y mostrarlos en pantalla.

Para poder instalar un servidor IRC necesitamos un programa que contenga el proceso demonio del servidor IRC. Este proceso debe estar en ejecución en todo momento en el servidor ya que es el que se encarga de recibir los mensajes de los usuarios y reenviarlos a sus correspondientes destinos. También se encarga de autenticar a los usuarios cuando se conectan a través de un nombre de usuario y una contraseña.

Los usuarios que desean conectarse a un servidor IRC deben darse de alta inicialmente en el servidor antes de que puedan conectarse y enviar mensajes. De igual forma, las conversaciones se organizan en canales, cada uno de ellos identificados por un nombre único (precedido del símbolo #) y lo que se conoce como *topic* que es una descripción de ese canal. En las conversaciones, los usuarios también están identificados por un nombre, denominado *nick* o apodo.

Cuando un usuario se conecta a un canal, cualquier texto que escriba que no sea una orden será enviada a todos los demás usuarios que están conectados en ese canal, junto con el apodo o el *nick* que lo envió. La recepción de los mensajes es automática, ya que aparecen en pantalla cuando son enviados. Dependiendo del programa cliente, también es posible que el usuario se conecte a varios canales a la vez.

Además de escribir mensajes, los usuarios pueden escribir también *órdenes* en su cliente IRC. Estas órdenes son enviadas al servidor para que realice todas las operaciones que tienen que ver con esa orden. Las órdenes suelen ir precedidas de la barra inclinada / para indicar al servidor que se trata de una orden y no de un mensaje.

Actualmente, los servicios de comunicación IRC tienen mucho menos éxito entre los usuarios, debido a la expansión de otros tipos de servicios que ofrecen más funciones o que permiten un manejo más sencillo. Sin embargo, muchos de los servicios de mensajería instantánea que se utilizan actualmente (véase los apartados siguientes) están basados en gran medida en las mismas ideas de diseño de IRC.

8.2.2 XMPP

XMPP (*Extensible Messaging and Presence Protocol* o Protocolo Extensible de Mensajería y Presencia), anteriormente conocido como **Jabber**, es un protocolo abierto para la transmisión de mensajería instantánea. Puesto que su código se distribuye libremente, existen multitud de implementaciones diferentes que habitualmente son compatibles entre sí (muchos programas de mensajería instantánea, como Google Talk o iChat). XMPP está definido formalmente en los documentos RFC 3920, RFC 3921, RFC 3922 y RFC 3923.

El protocolo XMPP está basado en el modelo cliente-servidor, por lo que, para que los mensajes puedan ser difundidos correctamente, es necesario que existan servidores que los redirijan. Entre las ventajas más importantes de uso de XMPP podemos destacar:

- Se trata de un servicio que no depende de un único servidor central, por lo que ofrece una mayor fiabilidad y tolerancia ante fallos.
- Está basado en estándares abiertos, por lo que no está ligado a ninguna empresa u organización.
- Es una tecnología que lleva utilizándose más de diez años, por lo que está muy desarrollada y probada.
- Ofrece mecanismos de seguridad y protección para su uso en redes privadas y cifrado de los mensajes.
- Permite el desarrollo de nuevas funciones adaptadas a las necesidades de cada usuario.
- No existe ningún servidor central y cada grupo u organización puede instalar el suyo. De esta forma, se evita una sobrecarga de trabajo en los servidores.

Sin embargo, este protocolo también tiene un inconveniente importante, que seguramente será solucionado en el futuro y es que existe una gran sobrecarga del tráfico que se utiliza para notificar la presencia de los usuarios. Este tráfico aumenta enormemente conforme crece el número de servidores.

Cada usuario de XMPP está identificado de forma única con un **JID** (*Jabber Identificator*), que está formado por una dirección de correo electrónico. A esta dirección se le añade un nombre que identifica el programa o equipo desde donde se conecta el usuario, por ejemplo:

```
ines@midominio.com/oficina
```

Los pasos que se siguen en el envío de un mensaje son los siguientes:

1. El usuario escribe el mensaje y lo envía al servidor al que está directamente conectado, usando un programa cliente (véase el apartado 8.3).
2. El servidor recibe el mensaje y lo reenvía al servidor en el que está conectado el usuario destinatario. Si ese servidor no contesta, el mensaje es descartado.
3. El servidor de destino recibe el mensaje y comprueba si el cliente está conectado. En caso afirmativo, le envía el mensaje; si no es así, lo guarda para su entrega posterior.

8.2.3 OSCAR

El protocolo **OSCAR** (*Open System for Communication in Realtime* o Sistema Abierto para la Comunicación en Tiempo Real), creado en 1990 por la empresa israelí Mirabilis, que en 1998 fue adquirida por AOL. Este protocolo es utilizado por los clientes de mensajería instantánea AIM e ICQ (véase el apartado 8.3). A pesar de su nombre, se trata de un protocolo cerrado y propietario, por lo que no se puede integrar con otras tecnologías de mensajería instantánea.

Sin embargo, en 2002, AOL llegó a un acuerdo con Apple, de forma que este protocolo se ha integrado con el servicio de mensajería instantánea iChat.

El protocolo OSCAR establece cómo se realiza la comunicación para el envío de los mensajes además de su formato. Estas cuestiones de diseño no han sido publicadas, por lo que muchas empresas y particulares han tenido que utilizar ingeniería inversa para dar soporte en sus propios programas. En el apartado 8.3 se enumeran algunos programas cliente que soportan el protocolo OSCAR.

8.2.4 YAHOO MESSENGER Y WINDOWS LIVE MESSENGER

Otros sistemas propietarios de mensajería instantánea muy utilizados actualmente son Yahoo Messenger y Windows Live Messenger. Estos sistemas, aunque se han desarrollado de forma completamente independiente, se encuentran integrados actualmente en la red de mensajería más grande del mundo.

Entre los servicios más importantes que ofrece este sistema se encuentran el intercambio de mensajes, transmisión de voz, transferencia de archivos, visualización en tiempo real (a través de una cámara instalada) y llamadas a teléfonos.

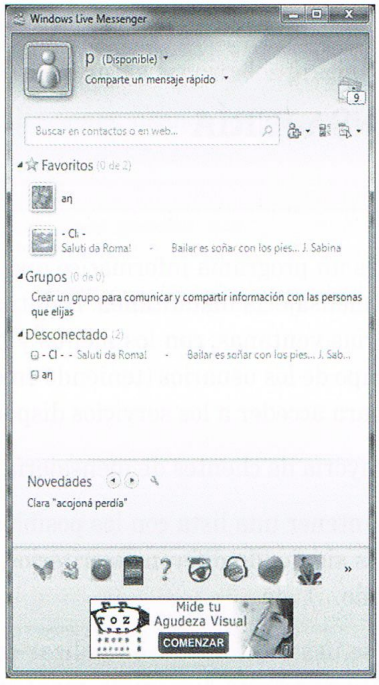


***Figura 8.1**. Programa de mensajería instantánea Windows Live Messenger. En esta ventana principal se muestran los usuarios disponibles y su estado*

8.2.5 SKYPE

Skype es un sistema orientado al intercambio de mensajes instantáneos y comunicación de voz a través de Internet. Fue desarrollado por Janus Friis y Niklas Zennström en 2003 y su tecnología de funcionamiento es completamente cerrada y propietaria. Mediante Skype se pueden mantener conversaciones de texto y voz a través de equipos (actualmente es un servicio gratuito) o teléfonos (mediante el pago de cuotas).

Skype soporta también el uso de cámaras para videoconferencia y el intercambio de archivos. Su funcionamiento está basado en el uso de multitud de servidores que comprimen la información y la envían a su destino.

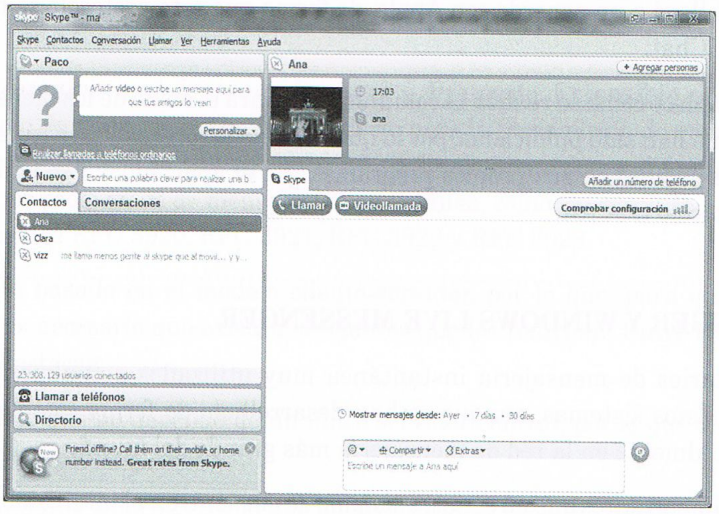


Figura 8.2. *Programa de mensajería instantánea Skype. En la ventana principal aparece la lista de usuarios disponibles con su estado. Cuando se selecciona uno de ellos, se puede enviar un mensaje de texto (parte derecha inferior de la ventana)*

8.3 CLIENTES DE MENSAJERÍA INSTANTÁNEA

Un cliente de mensajería instantánea es un programa informático que los usuarios utilizan para acceder a todas las funciones ofrecidas por los sistemas de mensajería instantánea. Habitualmente tienen la forma de una aplicación del entorno gráfico, formada por una o varias ventanas, con los menús y botones necesarios. Los programas cliente están preparados para ejecutarse en el equipo de los usuarios (teniendo en cuenta el sistema operativo que utilicen) y contienen todos los protocolos necesarios para acceder a los servicios disponibles por el sistema de mensajería.

Las funciones básicas que ofrecen la mayoría de clientes de mensajería instantánea son:

- **Gestión de contactos**: permite mantener una lista con los posibles destinatarios, mostrar su estado (si está disponible, ausente, etc.), agruparlos siguiendo diferentes criterios, asignarles información adicional que los identifique (nombre, fotografía, sonido...), etc.
- **Gestión de las conversaciones**: se usa para iniciar o finalizar conversaciones, enviar mensajes de texto o voz, enviar avisos cuando el destinatario no está disponible, mantener conversaciones entre varios usuarios a la vez, etc.
- **Transferencia de archivos**: envío de archivos entre los usuarios conectados.
- **Soporte de videoconferencia**: permite ver al otro usuario a través de una cámara que tenga instalada.

En los apartados siguientes se explican algunos de los clientes de mensajería instantánea más utilizados en la actualidad.

8.3.1 PIDGIN

Pidgin es un cliente de mensajería instantánea que es compatible con muchos protocolos de mensajería como IRC, XMPP, OSCAR y Messenger. También se puede instalar en muchas plataformas, como Microsoft Windows, GNU/Linux y Mac OS X. Pidgin se distribuye de forma libre ya que está registrado con la licencia GPL.

En 1999, Mark Spencer desarrolló el cliente **GAIM** (*GTK + AOL Instant Messenger*) como una alternativa libre al cliente de mensajería AIM de AOL. Para este desarrollo se contó con la ayuda de AOL, aunque un tiempo después esta empresa registró este sistema de comunicación y GAIM pasó a denominarse Pidgin. A partir de ese momento, las nuevas versiones del cliente comenzaron a ofrecer soporte para otros sistemas de mensajería instantánea.

Pidgin tiene la forma de una aplicación de entorno gráfico que ofrece todas las funciones necesarias para un cliente de mensajería instantánea (véase la Figura 8.3). Entre sus características principales podemos destacar:

- ✓ Es posible mantener varias comunicaciones al mismo tiempo usando diferentes sistemas de mensajería.
- ✓ Cada comunicación se muestra en una pestaña diferente.
- ✓ Mantiene un registro de las conversaciones mantenidas.
- ✓ Muestra avisos cuando los usuarios cambian de estado (de desconectado a conectado o al revés).
- ✓ Soporte para transferencia de archivos y cámaras de vídeo.
- ✓ Aumento de funciones y sistemas de mensajería soportados gracias a la instalación de complementos.
- ✓ Soporte para el cifrado de las comunicaciones, usando algunos complementos disponibles.

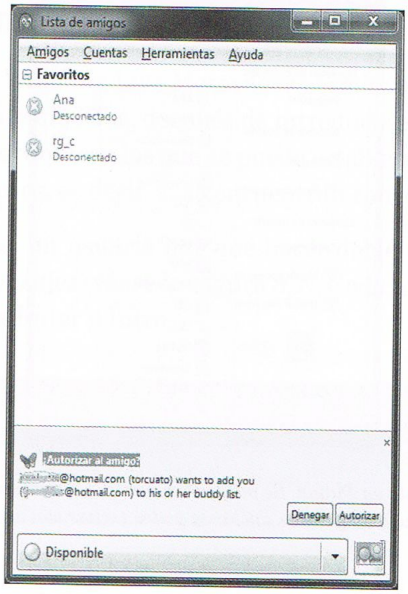


Figura 8.3. *Ventana principal del cliente Pidgin. Cuando nos conectamos con un sistema de mensajería instantánea, aparece una lista de los usuarios a los que les podemos enviar mensajes. En la parte inferior se muestran los usuarios que desean añadirse en nuestra lista de contactos*

Para configurar una nueva cuenta en Pidgin hay que seguir estos pasos:

1. Accedemos al programa y, si no tenemos configurada ninguna cuenta todavía, nos aparecerá una ventana donde se indica esto. Pulsaremos en el botón "Añadir...".
2. En caso de que ya tengamos alguna cuenta configurada en Pidgin, seleccionamos "Cuentas | | Gestionar cuentas" del menú principal. Esto mostrará una ventana como la de la Figura 8.4, donde pulsaremos el botón "Añadir...".

3 En la ventana que aparece (Figura 8.5), especificamos los siguientes parámetros:

- **Protocolo**: es el sistema de mensajería utilizado.
- **Nombre de usuario**: es la cuenta utilizada para autenticarse en el sistema de mensajería.
- **Contraseña**: es la contraseña de esa cuenta de usuario.

4 Pulsamos en el botón "Añadir" y después en el botón "Cerrar" para volver a la ventana principal de Pidgin.

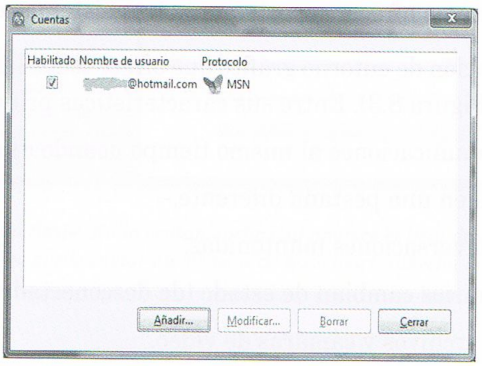


Figura 8.4. *Ventana de gestión de cuentas en Pidgin. Aquí se especifican las cuentas de usuario y los sistemas de mensajería que se van a utilizar*

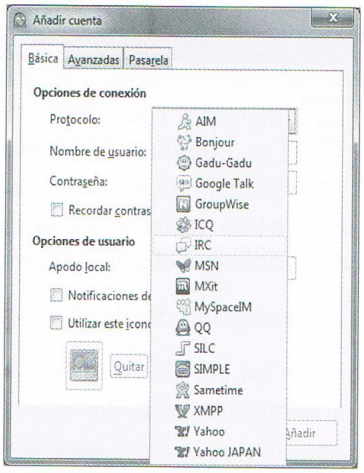


Figura 8.5. *Ventana para añadir una nueva cuenta en Pidgin. Se puede observar que Pidgin es compatible con una gran cantidad de sistemas de mensajería. Si alguno no está disponible, quizás se podrá incluir con algún complemento adicional*

Para enviar mensajes en Pidgin, simplemente hay que hacer doble clic con el ratón sobre el usuario destinatario. En ese momento, aparecerá una ventana donde se pueden empezar a introducir los mensajes de texto.

8.3.2 GOOGLE TALK

Google Talk es un cliente de mensajería instantánea que funciona sobre el protocolo XMPP (véase el apartado 8.2.2). Cualquier usuario que tenga una cuenta de correo electrónico en Gmail (Google Mail), también puede utilizarla para enviar mensajes instantáneos en Google Talk. La Figura 8.6 muestra la ventana principal de este programa.

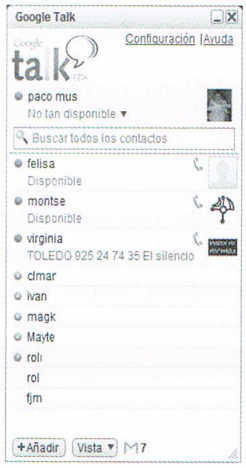


Figura 8.6. *Ventana principal del cliente de mensajería instantánea Google Talk. Aquí se muestran los usuarios con los que se puede hablar y si están conectados*

Para añadir usuarios a nuestra lista de conversación basta con pulsar en el botón "+Añadir" que aparece en la parte inferior izquierda de la ventana (Figura 8.6). En la ventana que aparece, hay que especificar la dirección de correo electrónico de esos usuarios. Si queremos hablar con un usuario, solamente tenemos que hacer doble clic con el ratón sobre él y aparecerá una ventana donde podemos escribir los mensajes.

8.3.3 YAHOO MESSENGER Y WINDOWS LIVE MESSENGER

El cliente de mensajería instantánea Windows Live Messenger permite a los usuarios la comunicación a través de las redes de Yahoo y Microsoft. Este cliente muestra, después de introducir el nombre de usuario y la contraseña, una ventana con los usuarios y los grupos favoritos (con los que se puede establecer una conversación inmediata). También se muestra el estado actual de esos usuarios, es decir, si se encuentran conectados o no (véase la Figura 8.1).

Para establecer una comunicación con un usuario hay que hacer doble clic sobre él, lo que mostrará una nueva ventana que nos permitirá escribir los mensajes (véase la Figura 8.7). Cada mensaje es enviado al destinatario cuando el usuario que lo escribe pulsa en la tecla Enter o Intro.

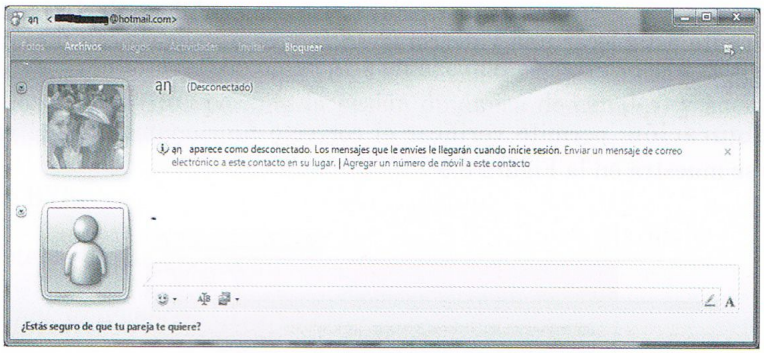


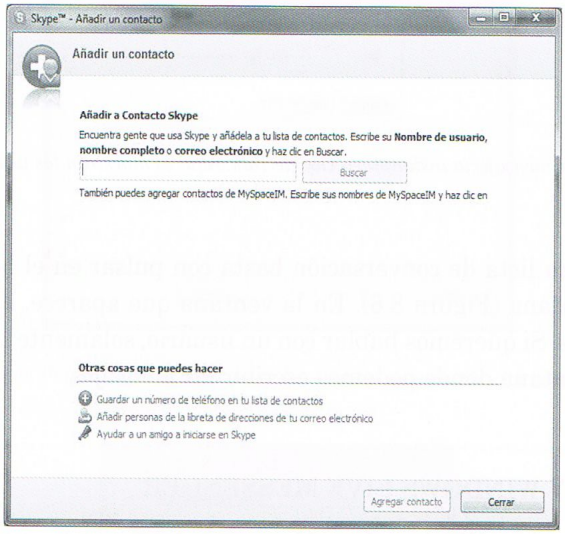
Figura 8.7. *Ventana de envío de mensajes del cliente Windows Live Messenger. Los mensajes se escriben en el cuadro de texto de la parte inferior, mientras que en la parte superior de la ventana se muestran todos los mensajes enviados por los dos usuarios*

El cliente Windows Live Messenger soporta también la videoconferencia, de forma que cuando nos comunicamos con otro usuario que tiene cámara, también nos aparecerá su imagen en tiempo real.

8.3.4 SKYPE

El cliente de mensajería instantánea de la red Skype permite a los usuarios tanto el envío de mensajes de texto como la conversación de voz en tiempo real, incluyendo el soporte a videoconferencia. En la Figura 8.2 se muestra la ventana principal de esta herramienta.

La ventana principal del cliente Skype está dividida en varias partes. En la parte de la izquierda se muestra una lista con los usuarios preferidos, es decir, aquellos con los que podemos establecer una conversación. Pulsando en el botón "Nuevo" podemos añadir más usuarios a esta lista (véase la Figura 8.8).



Figurea 8.8. *Ventana para añadir más usuarios a Skype. Una vez que un nuevo usuario ha sido añadido, éste debe confirmar que desea pertenecer a nuestra lista preferida*

Por su parte, en la parte derecha de la ventana principal de Skype se muestran las opciones necesarias para entablar conversación con uno de los usuarios seleccionados de la lista de preferidos. Algunos de los botones más importantes de los que disponemos son:

- **Llamar**: permite establecer una conversación de voz con otro usuario.
- **Videollamada**: permite establecer una videoconferencia (voz e imagen) con otro usuario, si disponemos de una cámara instalada.
- **Comprobar configuración**: permite verificar el correcto funcionamiento del micrófono, el volumen, la cámara, etc., como se muestra en la Figura 8.9.

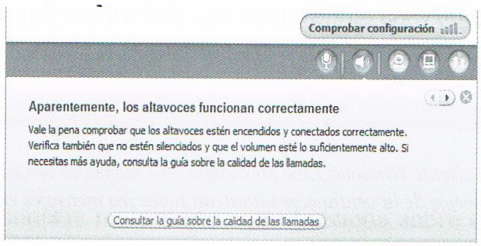


Figura 8.9. *Ventana de comprobación de medios en Skype. Aquí se comprueba el buen funcionamiento de los elementos utilizados para entablar una comunicación*

También se dispone de un cuadro de texto en el que se puede leer "Escribe un mensaje al usuario aquí". Gracias a este cuadro podemos enviar mensajes de texto a los usuarios, tanto si se encuentran conectados como si no.

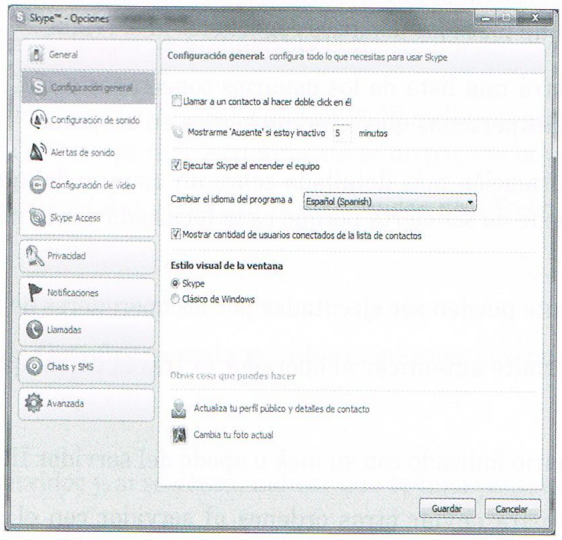


Figura 8.10. *Ventana de configuración de Skype. Esta ventana, que es accesible desde el menú principal seleccionando "Herramientas || Opciones...", permite establecer todos los parámetros de configuración de las comunicaciones, el aspecto visual, los usuarios, etc.*

8.3.5 CLIENTES IRC

La mayoría de los programas cliente IRC funcionan sobre el entorno gráfico del sistema, como puede ser Pidgin (véase el apartado 8.3.1). Sin embargo, todos ellos utilizan una serie de órdenes para que los usuarios puedan interaccionar de una forma más completa. Las órdenes se diferencian de los mensajes en que llevan una barra inclinada al principio. Las más importantes son:

- **/AWAY**: se usa para anunciar que, sin abandonar el servidor, vamos a estar unos minutos sin atender la conversación.
- **/BYE**: abandona la conversación. Si se añade un texto detrás de la orden, entonces éste es enviado al resto de usuarios como mensaje de despedida.
- **/CHANNEL** *#nombre_canal*: introduce al usuario en el canal especificado. Si este canal no existe y tenemos privilegios para ello, se crea (IRC permite la gesión dinámica de canales) y además confiere al usuario el privilegio de ser el operador del canal.
- **/EXIT**: es igual que BYE.
- **/HELP**: permite obtener ayuda.
- **/JOIN** *#nombre_canal*: es igual que CHANNEL.
- **/NICK** *nuevo_nick*: permite cambiar el *nick* o apodo del usuario.
- **/MSG** *nick mensaje*: envía un mensaje al usuario especificado por su *nick* o apodo sin que el resto pueda verlo.
- **/QUERY** *nick*: invita al usuario especificado por su *nick* o apodo a participar en una conversación privada. Si el receptor responde con una orden similar, el diálogo particular dará comienzo.

- **/QUIT**: es igual que BYE.
- **/TOPIC** *cadena*: cambia el *topic* o descripción del canal (si tenemos privilegios para poder hacerlo).
- **/USERS**: muestra una lista de todos los usuarios conectados al servidor.
- **/WHO** *nombre_canal*: muestra una lista de los usuarios conectados a IRC. Si se indica un nombre de canal, restringe el listado a todas las personas que estén presentes en ese canal.
- **/WHOIS** *nick*: muestra información más detallada sobre un usuario del que conocemos su *nick* o apodo. Sin embargo, la información puede no ser cierta porque es la facilitada por la persona.

Las siguientes órdenes solamente pueden ser ejecutadas por los operadores de los canales:

- **/OPER** *nick contraseña*: permite autenticar al operador (a través de su apodo y contraseña) para concederle sus privilegios.
- **/KICK** *nick*: expulsa al usuario indicado con su *nick* o apodo del servidor IRC.
- **/QUOTE** *orden*: se utiliza para enviar otras órdenes al servidor con el propósito de realizar operaciones privilegiadas.

Existen más órdenes reconocidas por IRC e incluso se pueden realizar programas complejos.

8.4 SERVIDORES DE MENSAJERÍA INSTANTÁNEA

En este apartado se explican los procedimientos necesarios para instalar y configurar servidores de mensajería instantánea, lo que nos permitirá disponer de este servicio en nuestra red local.

8.4.1 INSTALACIÓN Y CONFIGURACIÓN DE UN SERVIDOR XMPP

Como se explica en el apartado 8.2.2, el servicio de mensajería instantánea XMPP funciona gracias a la existencia de servidores que se encargan de autenticar a los usuarios (comprobar su nombre y contraseña) y enviar los mensajes a los destinatarios. El protocolo XMPP permite la instalación de cualquier servidor para el intercambio de mensajes en una red local o en Internet.

Existen muchos paquetes disponibles en el mercado que implementan el funcionamiento de un servidor XMPP, tanto libres como propietarios. En este libro vamos a explicar el paquete Openfire, ya que está disponible en diferentes plataformas (Microsoft Windows, GNU/Linux y Mac OS X) y además se distribuye libremente bajo licencia GPL. Otras características importantes de Openfire son las siguientes:

- Está desarrollado en lenguaje Java, lo que le permite funcionar en multitud de plataformas.
- Incluye una interfaz de configuración amigable basada en páginas web, por lo que se puede administrar de forma remota.
- Permite instalar *plugins* para añadir nuevas funciones.

- Puede integrarse con otras redes de mensajería como Yahoo Messenger, Windows Live Messenger, Google Talk y AOL.
- Soporta el envío de mensajes fuera de línea y la transferencia de archivos.
- Permite el envío cifrado de los mensajes mediante SSL/TLS.

Openfire es muy estable y robusto y prueba de ello es que en 2006 recibió el premio ServerWatch Product por ser el mejor servidor de comunicaciones en tiempo real. Actualmente se distribuye la versión 3.6.4.

En general, los pasos a seguir para instalar y configurar un servidor XMPP con Openfire son los siguientes:

1. Instalar el paquete necesario.
2. Establecer la base de datos donde Openfire necesita guardar la información (puede ser una base de datos interna u otra externa, como MySQL).
3. Iniciar el proceso demonio del servidor y, si se desea, indicar que se inicie automáticamente en el arranque.
4. Acceder a la página web de configuración de Openfire para comprobar que el servicio se ha iniciado correctamente.
5. Desde la página web de configuración de Openfire, establecer los parámetros necesarios para que el servicio funcione como deseamos.

8.4.1.1 Instalación de Openfire

En los ejemplos 8.1, 8.2 y 8.3 se explica con detalle cómo instalar Openfire en diferentes plataformas.



EJEMPLO 8.1

Para instalar el servidor Openfire en Windows XP/Vista/7 hay que seguir estos pasos:

1. Descargar el paquete de instalación desde la página oficial, pulsando en el enlace "Download", después seleccionando la plataforma "Windows" y finalmente pulsando sobre el archivo que nos interese. Hay dos opciones: descargar el paquete ejecutable que incluye Java JRE (esta opción debe ser la seleccionada cuando no tengamos instalado Java en nuestro equipo) o descargar el paquete comprimido que no incluye Java (si ya tenemos Java instalado).
2. Si hemos seleccionado el ejecutable con Java lo iniciamos y aparecerá un asistente que nos guiará en todo el proceso. Por defecto, Openfire se instalará en la carpeta *C:\Archivos de programa\Openfire*.
3. Si hemos seleccionado el archivo comprimido sin Java, lo descomprimimos en la ruta donde queramos ubicarlo y ejecutamos el archivo *openfired.exe* que se encuentra dentro de la carpeta *bin*. En Windows 7 aparecerá un mensaje del cortafuegos indicando si se permite que Openfire tenga acceso a la red (pulsaremos el botón "Permitir acceso", como se muestra en la Figura 8.11). Esta opción inicia el servidor Openfire de forma manual.

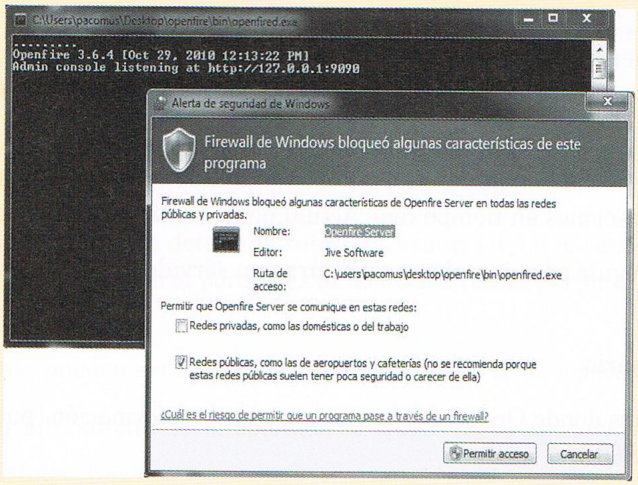


Figura 8.11. *Mensaje de notificación del cortafuegos de Windows 7. Aquí se indica que el cortafuegos está bloqueando el tráfico en los puertos utilizados por Openfire*

4. Otra forma de iniciar el servidor Openfire en Windows consiste en ejecutar el archivo *openfire.exe* que también se encuentra en la carpeta *bin*. Esto inciará una ventana como la de la Figura 8.12, donde están disponibles los botones "Start" (para iniciar el servidor), "Stop" (para pararlo) y "Launch admin" (para acceder a la ventana de configuración).
5. También podemos iniciar de forma automática el servicio Openfire ejecutando la siguiente orden (accediendo a la carpeta *bin* de instalación):
   `openfire-service /install`
6. Accedemos al asistente de instalación desde un navegador, especificando la siguiente dirección:
   `http://localhost:9090`
7. Para continuar el proceso de configuración de Openfire hay que seguir los pasos indicados en el apartado 8.4.1.2.

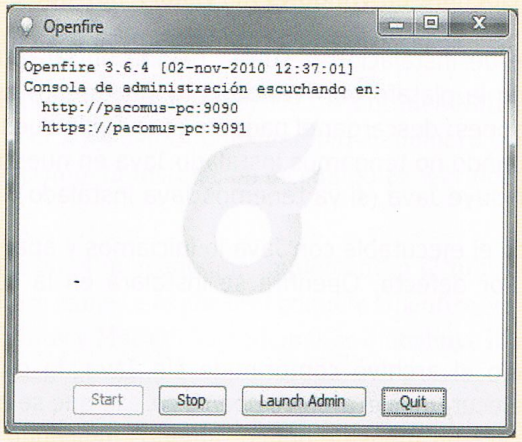


Figura 8.12. *Consola de control del servidor Openfire. Aquí se puede iniciar o parar el servidor, además de acceder a la página de configuración (a través de un navegador)*

EJEMPLO 8.2

Para instalar el paquete Openfire en Debian, Fedora u OpenSUSE hay que seguir estos pasos:

1. Descargar el paquete de instalación desde la página oficial, pulsando en el enlace "Download", después seleccionando la plataforma "Linux" y finalmente pulsando sobre el archivo que nos interese (será el paquete RPM para Fedora y OpenSUSE o el paquete DEB para Debian).
2. A continuación, instalamos el paquete descargado con la herramienta correspondiente.
3. Para iniciar o parar el servidor Openfire hay que ejecutar estas órdenes, respectivamente (como usuario *root*):

```
# /etc/init.d/openfire start
# /etc/init.d/openfire stop
```

4. Podemos hacer que el servidor Openfire se inicie automáticamente en el arranque si configuramos convenientemente los niveles de ejecución del sistema.
5. Accedemos al asistente de instalación desde un navegador, especificando la siguiente dirección:

```
http://localhost:9090
```

6. Para continuar el proceso de configuración de Openfire, hay que seguir los pasos indicados en el apartado 8.4.1.2.

EJEMPLO 8.3

Para instalar el paquete Openfire en cualquier otra distribución hay que seguir estos pasos:

1. Descargar el paquete de instalación desde la página oficial, pulsando en el enlace "Download", después seleccionando la plataforma "Linux" y finalmente pulsando sobre el archivo *TAR.GZ*.
2. Comprobar que está instalado el paquete Java.
3. A continuación, instalamos el paquete descargado con estas órdenes (ejecutadas como usuario *root* dentro de la carpeta donde se encuentre):

```
# tar -xzvf openfire_3_6_4.tar.gz
# mv openfire /opt
```

4. Para iniciar o parar el servidor Openfire hay que ejecutar estas órdenes desde la carpeta donde se encuentre descomprimido, respectivamente (como usuario *root*):

```
# ./openfire start -
# ./openfire stop
```

5. Podemos hacer que el servidor Openfire se inicie automáticamente en el arranque si configuramos convenientemente los niveles de ejecución del sistema.
6. Accedemos al asistente de instalación desde un navegador, especificando la siguiente dirección:

```
http://localhost:9090
```

7. Para continuar el proceso de configuración de Openfire, hay que seguir los pasos indicados en el apartado 8.4.1.2.

8.4.1.2 Configuración de Openfire

Una vez instalado el paquete Openfire (véase el apartado anterior), es necesario configurar algunos parámetros importantes para que el servidor pueda funcionar. Para ello, hay que seguir estos pasos, que son los mismos independientemente de la plataforma utilizada (Microsoft Windows, GNU/Linux o Mac OS X):

1 En la ventana que aparece (Figura 8.13), seleccionamos el idioma "Español (es)" y pulsamos el botón "Continue".

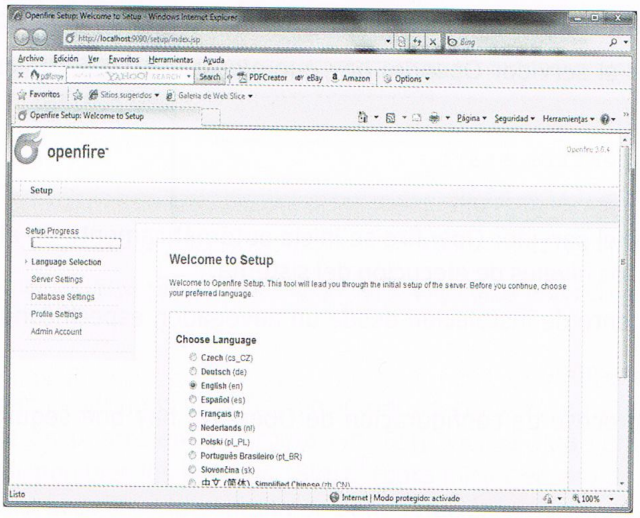


Figura 8.13. *Ventana principal del asistente de configuración de Openfire. Aquí se especifica el idioma utilizado para configurar este servidor.*

2 En la siguiente ventana del asistente (Figura 8.14), especificamos el nombre del dominio asociado con el servicio de mensajería, el puerto de la consola de administración (por defecto es el 9090) y el puerto seguro (9091). Pulsamos en el botón "Continuar".

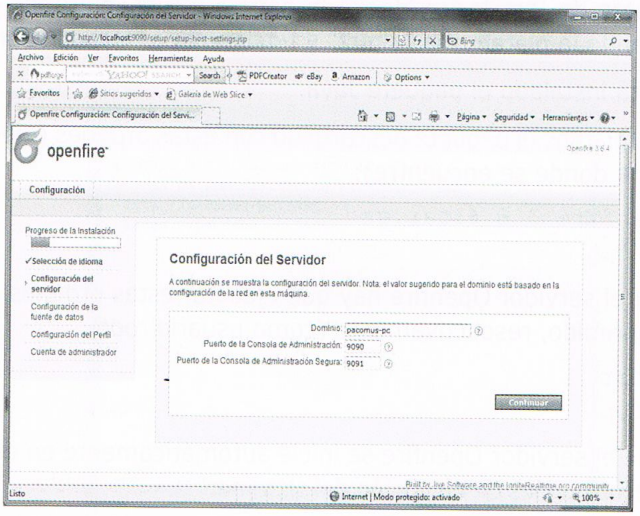


Figura 8.14. *Configuración del servidor Openfire en el asistente. En esta ventana se especifica el dominio y los puertos utilizados para administración y transmisión de los mensajes*

3 A continuación, especificamos la base de datos donde Openfire va a almacenar la información (véase la Figura 8.15). Tenemos dos opciones:

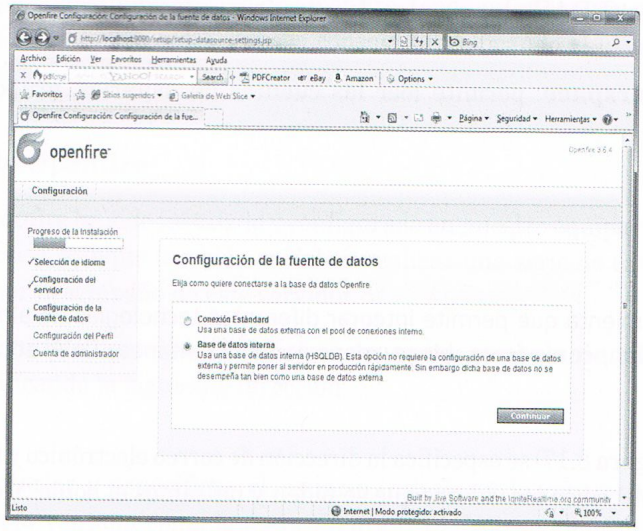


Figura 8.15. *Configuración de la fuente de datos en Openfire. Aquí se indica la base de datos que va a almacenar la información*

- **Conexión estándar**: permite especificar una base de datos externa donde almacenar la información (como por ejemplo MySQL). Esta opción hace que Openfire funcione mejor, pero requiere de un paso previo de instalación del gestor de bases de datos correspondiente.
- **Base de datos interna**: se usa para indicar que la información de Openfire se guarde en una base de datos propia de este servidor. Esta opción no requiere de la instalación de ningún paquete adicional, pero es mucho menos eficiente y no se recomienda en un entorno de producción real.

4 En la siguiente ventana se especifica la fuente desde donde se van a obtener las cuentas de usuarios y grupos que se autentican en el servidor (Figura 8.16). Tenemos tres opciones:

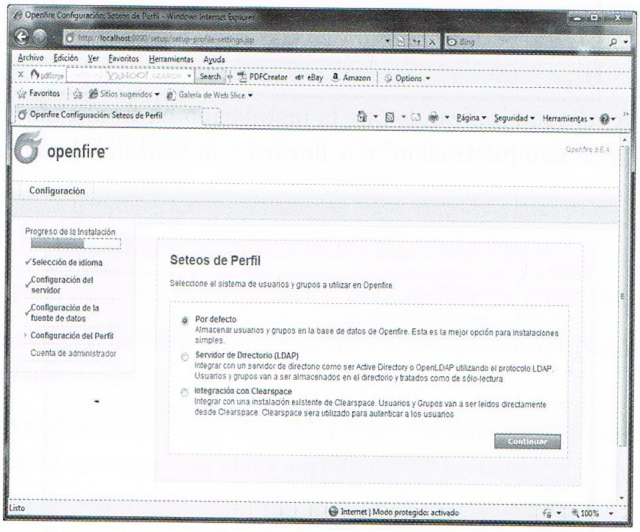


Figura 8.16. *Ventana de configuración de cuentas del asistente de Openfire. Aquí se indican las cuentas de usuario y grupos que van a tener acceso al servidor para intercambiar mensajes*

- **Por defecto**: las cuentas de usuario y grupos se crean y se almacenan directamente en este servidor. Esta opción es la más simple y permite el funcionamiento sobre una red local.

- **Servidor de directorio (LDAP)**: las cuentas de usuario y grupos se obtienen a través de un servidor LDAP existente.
- **Integración con Clearspace**: permite leer las cuentas de usuarios, grupos y contraseñas a través de Clearspace.

Clearspace es una herramienta que permite integrar diferentes tecnologías de almacenamiento y transmisión de información, como foros, blogs, mensajería instantánea, VoIP, etc.

5 En la siguiente ventana (Figura 8.17) se especifica la dirección de correo electrónico y la contraseña para administrar el servidor Openfire. Establecemos los valores que se piden y pulsamos el botón "Continuar".

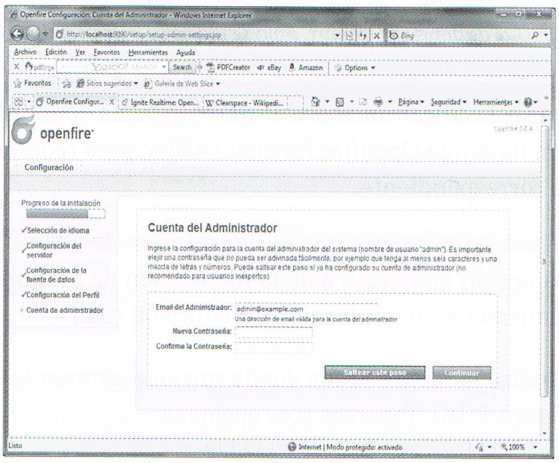


Figura 8.17. *Especificación de la dirección de correo electrónico y la contraseña de administrador en el asistente de Openfire*

6 Finalmente, se mostrará una ventana indicando que la instalación ha finalizado (Figura 8.18). Si pulsamos en el botón "Conéctese a la consola de administración" nos llevará a la ventana de administración del servidor (véase el apartado 8.4.1.3).

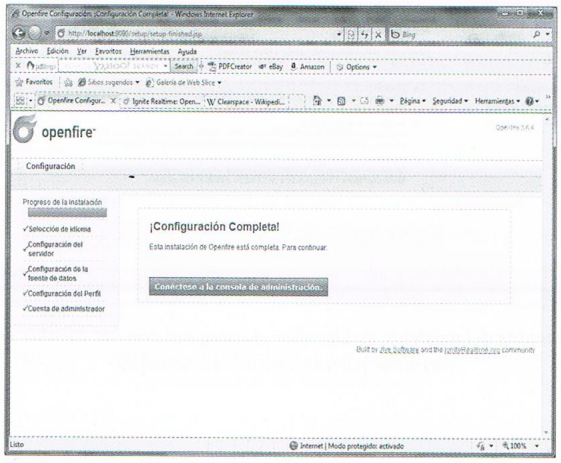


Figura 8.18. *Ventana final del asistente de instalación de Openfire*

7 Antes de acceder a la consola de administración de Openfire, tenemos que parar y volver a iniciar el proceso o de lo contrario es posible que no podamos acceder a esa consola especificando el usuario *admin* y la contraseña que hemos establecido en el paso 5.

8.4.1.3 Administración de Openfire

Una vez que el servidor Openfire ha sido instalado y configurado en nuestro equipo (véase los apartados anteriores), ya podemos comenzar a utilizarlo, aunque también se deben realizar una serie de tareas de mantenimiento que nos permitan llevar a cabo un mejor desempeño de este servidor.

La herramienta para configurar el servidor Openfire se denomina **consola de administración** y es accesible a través de un navegador especificando la siguiente dirección:

```
http://localhost:9090
```

Al indicar la dirección anterior y especificar el usuario (*admin*) y la contraseña establecidos en la fase de configuración, nos mostrará una ventana como la de la Figura 8.19. Nótese que ésta es la misma dirección que se indicó para realizar la configuración inicial de Openfire (véase el apartado 8.4.1.2) pero, como esta configuración ya se ha realizado, ahora nos aparecerá la consola de administración.

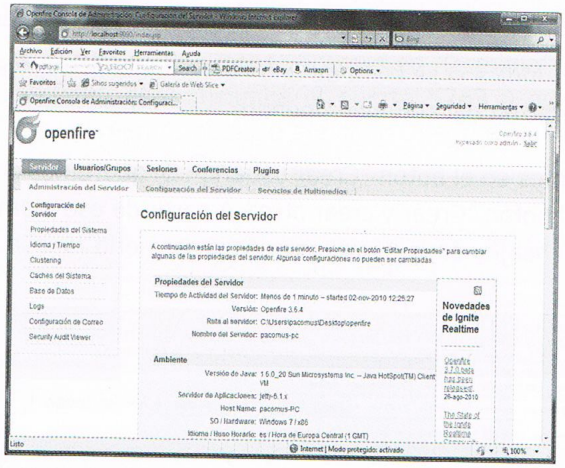


Figura 8.19. *Ventana principal de la consola de administración de Openfire. Desde esta ventana se pueden configurar todas las características de este servidor de mensajería*

Las opciones disponibles en la consola de administración son las siguientes:

- **Servidor**: establece los parámetros de configuración del servidor de mensajería. Existen varias páginas.
- **Administración del servidor**: permite establecer los valores de configuración del servidor, como los puertos, el dominio, el idioma, la base de datos, etc.
- **Configuración del servidor**: especifica determinados parámetros de configuración, como el método de autenticación de usuarios, la conexión con otros servidores de mensajería, actualizaciones de *plugins*, registro de conexiones, certificados de seguridad, etc.
- **Usuarios/Grupos**: permite gestionar las cuentas de usuario que tienen acceso al servidor de mensajería.
- **Sesiones**: gestiona los usuarios que se han autenticado en el servidor y, por lo tanto, pueden enviar mensajes.
- **Conferencias**: permite gestionar conferencias, que son conversaciones entre más de dos usuarios a la vez.
- **Plugins**: gestiona los componentes que se pueden instalar en el servidor para aumentar las funciones disponibles.

EJEMPLO 8.4

Suponemos que tenemos una instalación de un servidor Openfire plenamente operativo y deseamos crear cuentas de usuario para los clientes de mensajería. Los pasos a seguir son los siguientes:

1. Accedemos a la herramienta de administración del servidor a través de un navegador, especificando la siguiente dirección:
   `http://localhost:9090`

2. Especificamos el usuario y la contraseña y seleccionamos "Usuarios/Grupos || Crear nuevo usuario". Esto nos mostrará una ventana como la de la Figura 8.20.

3. Especificamos los siguientes parámetros:
   - **Usuario**: es el nombre de la cuenta (debe ser único).
   - **Nombre**: es el nombre completo.
   - **E-mail**: dirección de correo electrónico del usuario.
   - **Contraseña**: contraseña de autenticación del usuario. Hay que escribirla dos veces.
   - **Is Administrator**: indica si se trata de una cuenta de administrador que tiene privilegios para cambiar la configuración del servidor Openfire.

4. A continuación, pulsamos en el botón "Crear usuario". Si queremos crear varios usuarios, entonces tenemos que pulsar el botón "Crear y crear otro". A partir de ese momento, ya podemos utilizar esa cuenta para enviar mensajes desde un cliente de mensajería (véase el apartado 8.3).

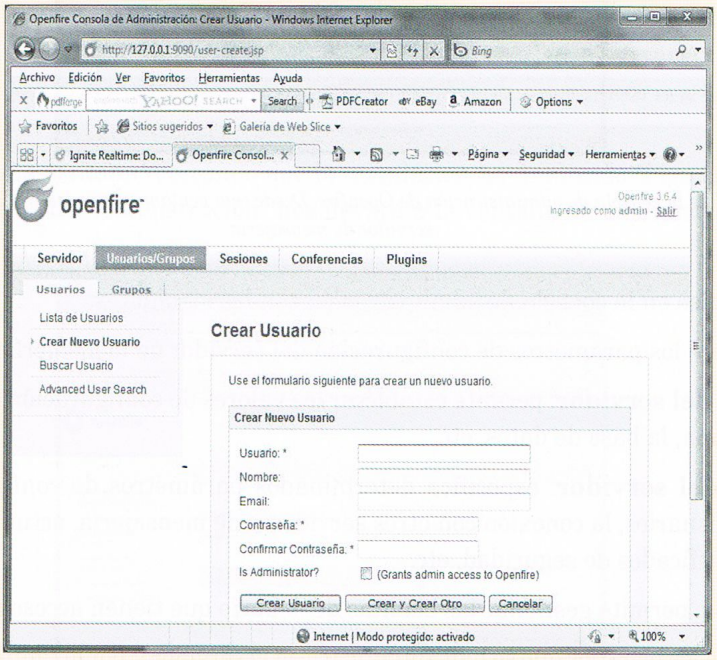


Figura 8.20. *Ventana de creación de un usuario nuevo en Openfire. Esta cuenta de usuario puede ser utilizada posteriormente para enviar mensajes a otros usuarios*

EJEMPLO 8.5

Veamos cuáles son los pasos que hay que seguir para que nuestro servidor Openfire sea capaz de validar cuentas de usuario definidas en el servicio Google Talk. Estos son:

1. Comprobar que nuestro servidor Openfire tiene asociado un registro de tipo SVR en el sistema de nombres de dominio de Internet (véase el capítulo 2). Este registro debe especificar el mismo nombre de dominio que el indicado en la configuración inicial de Openfire (véase el apartado 8.4.1.2).
2. Accedemos a la herramienta de administración del servidor a través de un navegador, especificando la siguiente dirección:
   `http://localhost:9090`
3. Seleccionamos "Servidor || Configuración del servidor || Servidor a servidor". Esto nos mostrará una ventana como la de la Figura 8.21.
4. En la sección "Servidor habilitado" marcamos el botón de opción "Habilitado" y especificamos el puerto 5269 que es el utilizado por el servidor Google Talk para conectarse con otros. Hay que tener en cuenta que el puerto 5269 debe estar abierto en el cortafuegos o encaminador y también debe haber sido redirigido hacia nuestro servidor Openfire.
5. En la parte inferior de la misma página, especificamos en "Dominio" el nombre del servidor Google Talk, que es *talk.google.com*, especificamos el puerto 5269 y pulsamos en el botón "Agregar servidor". A partir de ese momento, nuestro servidor Openfire también será capaz de autenticar conexiones de cuentas creadas para Google Talk.

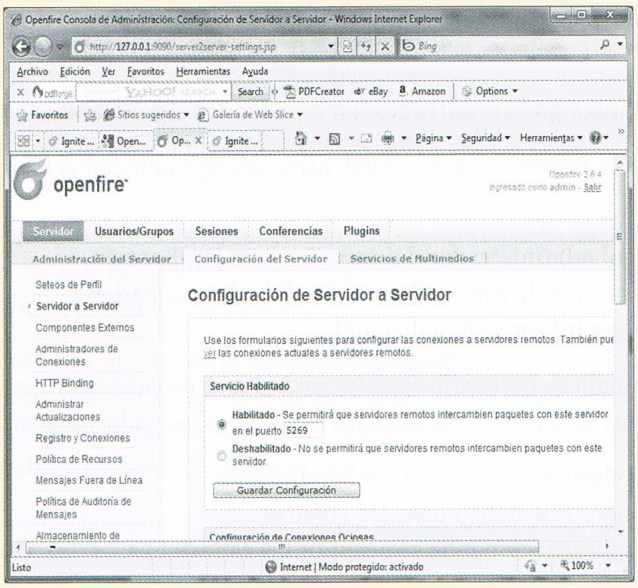


Figura 8.21. *Ventana de gestión de conexiones entre servidores de Openfire. Gracias a esta configuración, nuestro servidor se puede conectar con otras redes de mensajería*

Hay que tener en cuenta que Google Talk y Openfire utilizan el mismo protocolo de mensajería XMPP, por lo que su conexión e intercambio de mensajes es sencilla. Sin embargo, Openfire también se puede conectar con otros servidores de mensajería, como Windows Live Messenger, pero para ello es necesario configurar una pasarela en Openfire.

8.4.2 INSTALACIÓN Y CONFIGURACIÓN DE UN SERVIDOR IRC

La instalación y configuración de un sistema IRC resulta mucho más sencilla que otros servicios (por ejemplo el DNS o el correo) ya que existen muy pocos protocolos involucrados y la interacción se realiza a través de un equipo que actúa como servidor y el resto lo hacen como clientes.

Existe en el mercado multitud de programas servidores IRC, por lo que resulta muy complicado incluirlos todos en este libro. Sin embargo, la gran mayoría de ellos utilizan los mismos parámetros de configuración para funcionar. En este apartado nos centraremos en explicar cómo se realiza la instalación del paquete *ircd*.

El paquete *ircd* se puede obtener de dos formas: en código fuente y en binario. Se recomienda obtener el paquete binario ya que no es necesario compilarlo en Microsoft Windows o Linux, una tarea que puede resultar bastante ardua. En cuanto a la instalación del binario, la única diferencia entre Windows y Linux radica en la utilización de una herramienta de instalación diferente (en Windows hay que ejecutar el programa de instalación, mientras que en Linux se instala el paquete).

Para que el servidor IRC funcione correctamente es necesario que el programa demonio *ircd* esté en ejecución. En sistemas Windows se consigue ejecutando una orden, mientras que en sistemas Linux se accede al editor de niveles de ejecución.

El servidor IRC solamente necesita de un archivo de configuración que es independiente del sistema operativo y versión del equipo. Se llama *ircd.conf* y se encuentra en la carpeta de instalación del paquete o en */etc/ircd/* (en el caso de los sistemas Linux).

El archivo de configuración *ircd.conf* está construido en texto claro y se puede modificar con un editor de textos normal. Está formado por diferentes líneas, cada una de las cuales comienza por una letra mayúscula. Esa letra mayúscula establece un registro de configuración y va seguida de un conjunto de parámetros asociados y separados por el carácter dos puntos "**:**".

Los registros más importantes que encontramos en *ircd* son los siguientes:

- **A**: se usa para establecer información administrativa del servidor con el formato "A:nombre:email:otros::". Los campos son:
  - *Nombre*: identifica al administrador del servidor y su localización.
  - *Email*: indica la dirección de correo electrónico del administrador.
  - *Otros*: puede incluirse información adicional.
- **B**: resulta muy útil cuando es necesario realizar un balance de carga porque algunos servidores se encuentran saturados de conexiones de clientes. Su formato es "B:clase::servidor:puerto:", donde:
  - *Clase*: identifica la clase de conexión (C) o los clientes.
  - *Servidor*: es el servidor que deben usar los clientes.
  - *Puerto*: número de puerto por donde se aceptan las conexiones.
- **C**: se utiliza para configurar conexiones con otros servidores, puede existir más de una línea de este tipo y tiene el siguiente formato "C:dirección:contraseña:nombre:puerto:clase", donde:
  - *Dirección*: es la dirección IP del servidor con el que conectar.
  - *Contraseña*: es la contraseña de acceso al otro servidor.
  - *Nombre*: es el nombre del servidor.
  - *Puerto*: es el número de puerto por donde se va a conectar.
  - *Clase*: establece los parámetros de conexión (opción "Y").

- **I**: nos da información de los clientes que se pueden conectar a nuestro servidor, por lo que puede haber más de una entrada de este tipo. Las opciones que tiene son "I:dirección:contraseña:cliente:puerto:clase", donde:
  - *Dirección*: es la dirección IP del equipo cliente.
  - *Contraseña*: es la contraseña para conectar al servidor.
  - *Cliente*: es el nombre del equipo.
  - *Puerto*: es el número de puerto por el que va a conectar.
  - *Clase*: establece los parámetros de conexión (opción "Y").
- **K**: se usa para eliminar usuarios incontrolados del sistema. El formato de este registro es "K:nombre:tiempo: usuario:puerto:", donde:
  - *Nombre*: nombre o IP desde donde conecta el usuario.
  - *Tiempo*: intervalo de activación de la operación de eliminación.
  - *Usuario*: nombre del usuario a eliminar del servidor.
  - *Puerto*: es el número de puerto por el que se conecta.
- **M**: se usa para definir los parámetros mas importantes de nuestro servidor que siguen la forma "M:nombre: dirección:comentario:puerto", donde:
  - *Nombre*: es el nombre de nuestro servidor.
  - *Dirección*: es su dirección IP.
  - *Comentario*: se trata de un texto aclaratorio sobre el servidor.
  - *Puerto*: es el puerto por el que va a aceptar conexiones.
- **O**: se usa para definir administradores del servidor IRC. Los parámetros son "O:cliente:contraseña:nick: puerto:clase", donde:
  - *Cliente*: es el nombre del equipo desde donde se va a conectar.
  - *Contraseña*: es la contraseña de acceso que debe especificar.
  - *Nick*: es el apodo o nombre de pila.
  - *Puerto*: es el número de puerto por donde se va a conectar.
  - *Clase*: establece los parámetros de conexión (opción "Y").
- **P**: permite definir diferentes puertos de comunicación con el servidor. El formato puede ser de dos tipos, a saber, puertos de transporte, con el formato "P:dirección::máscara:puerto:" o puertos Unix, con el formato "P:ruta:::puerto:". Los parámetros son los siguientes:
  - *Dirección*: es la dirección IP desde donde se aceptan conexiones.
  - *Máscara*: es la máscara de red que se aplica a la dirección.
  - *Puerto*: número de puerto por donde se reciben las conexiones.
  - *Ruta*: es la carpeta y archivo Unix que maneja el puerto.
- **Y**: se utiliza para definir clases de conexiones. Esas clases definen parámetros de conexión y son las que se especifican en las opciones que se han visto. Los parámetros de esta opción son "Y:número:tiempo:frecuencia:conexiones: sendQ:clientes:global", donde:
  - *Número*: es el identificador numérico de esa clase.
  - *Tiempo*: frecuencia de envío de un eco al cliente que está inactivo.
  - *Frecuencia*: es la frecuencia de reintentos en las conexiones.
  - *Conexiones*: número de conexiones máximas por cliente.
  - *SendQ*: establece este parámetro sobre el tamaño de los mensajes.
  - *Clientes*: número de clientes que se pueden conectar a la vez.
  - *Global*: es el número máximo de clientes en conexión por la red.

La mayoría de los registros se pueden repetir más de una vez dentro del archivo de configuración, exceptuando los registros *M* y *A*. Por ejemplo, si nos vamos a conectar a varios servidores necesitaremos especificar varias líneas que comiencen por *C*, si necesitamos especificar mas de un usuario administrador entonces tendremos que poner varias líneas que comiencen por la letra *O*, etc.

Dentro de cada parámetro de las opciones, se puede poner un símbolo asterisco "*" que significa "cualquier valor". Si se deja en blanco algún parámetro, entonces el servidor utilizara el valor por defecto. Se puede utilizar el nombre "localhost" para especificar el nombre de nuestro equipo local dentro del parámetro que corresponda.

EJEMPLO 8.6

Veamos un ejemplo de archivo de configuración *ircd.conf*:

```
M:chat.moli.es::Ciudad Real, España:6667:
A:Javi Molina - Alcázar de San Juan:INET javi@moli.es UUCP:
¿Que hay de nuevo, viejo?::
P:192.168.1.194:::6664:
Y:23:120:300:5:100000:0:0:
Y:2:60:0:50:20000:2.1:5:
I:x::chat.moli.es::1
O:admin.azarquiel.es:panceta:Moli2::1
K:veteasaber.com::bush:0:
C:molidos.es::molidos.es:6667:1
B:2::irc.moli.es:6660:
```

Comentemos qué significa cada línea del archivo:

- La línea *M*, se lee: "Mi equipo se llama *chat.moli.es* y está localizado en Ciudad Real, España".
- La línea *A* ha sido dividida en líneas porque ocupa más espacio, pero en el archivo debe aparecer como una sola.
- La línea *P* establece que el servidor recibirá los mensajes desde la dirección IP 192.168.1.194 y el puerto 6664.
- Las líneas *Y* define dos clases: la clase 23, para permitir 5 conexiones, que son chequeadas cada 300 segundos y pueden estar inactivas 120 segundos sin ser comprobadas; también define la clase 2 para 50 usuarios.
- La línea *I* se ha añadido para indicar que los equipos clientes del propio dominio también pueden conectar con el servidor.
- La línea *O* define un operador del sistema que está ubicado en otro lugar, tiene la contraseña de acceso "panceta" y el apodo "Moli2".
- La línea *K* indica que si el usuario "bush" accede al servidor IRC desde la dirección "veteasaber.com", entonces hay que eliminarlo inmediatamente.
- La línea *C*, se lee "Conectar al equipo 'molidos.es' sin contraseña a través del puerto 6667.
- La línea *B* indica que los clientes de la clase 2 están advertidos para utilizar el servidor "irc.moli.es" en el puerto 6660.

RESUMEN DEL CAPÍTULO

Los servicios de **mensajería instantánea** permiten la comunicación entre usuarios a través de texto o voz, además de la transferencia de archivos. Se diferencia del correo electrónico en que, habitualmente, los mensajes no se almacenan para que los usuarios los consulten *a posteriori*, sino que estos se envían a aquellos usuarios que se encuentran conectados o en línea en ese momento.

Uno de los servicios de mensajería instantánea más utilizado en Internet ha sido IRC que, aunque se ha convertido en un estándar, actualmente está en desuso por la utilización de otros servicios que ofrecen una mayor cantidad de funciones. Uno de los servicios más extendidos actualmente es XMPP, sobre todo porque se basa en un protocolo abierto que no depende de ninguna empresa o tecnología concretas. Otros servicios de mensajería muy utilizados en la actualidad son AOL, iChat, Yahoo Messenger, Windows Live Messenger y Skype, aunque estos se basan en protocolos cerrados que son propiedad de determinadas empresas.

Un **cliente de mensajería instantánea** es un programa que permite el acceso a los usuarios de este tipo de servicios. Estos programas disponen de herramientas que permiten el envío y recepción de mensajes, además de otras funciones no menos útiles, como la gestión de los contactos habituales, la transferencia de archivos y el soporte para las conversaciones de voz o videoconferencia. Ejemplos de programas clientes de mensajería son Pidgin (distribuido con licencia libre y que soporta multitud de protocolos), Google Talk (que funciona sobre XMPP), Yahoo Messenger, Windows Live Messenger o Skype (enfocado fundamentalmente a conversaciones de voz).

Openfire es un paquete de programas que permite convertir a un ordenador en un potente servidor de mensajería instantánea. Se distribuye bajo licencia libre y está basado en XMPP. Además, funciona en multitud de plataformas porque está desarrollado en lenguaje Java, se gestiona a través de páginas web, soporta tecnologías de cifrado y puede integrarse con otros servicios de mensajería existentes en Internet. En general, los pasos a realizar para instalar y configurar un servidor de mensajería con Openfire son los siguientes:

1. Instalar el paquete necesario.
2. Establecer la base de datos donde Openfire necesita guardar la información.
3. Iniciar el proceso demonio del servidor y, si se desea, indicar que se inicie automáticamente en el arranque.
4. Acceder a la página web de configuración de Openfire para comprobar que el servicio se ha iniciado correctamente.
5. En esa misma página de configuración, crear las cuentas de usuario de las personas que van a utilizar el servicio de mensajería. Se pueden crear manualmente o de forma automática a través de un servidor LDAP o ClearSpace.
6. Desde la página web de configuración de Openfire, establecer otros parámetros necesarios para que el servicio funcione como deseamos.

Para instalar un servidor de mensajería instantánea de tipo IRC hay que seguir estos pasos genéricos:

1. Instalar el paquete necesario, que en los sistemas GNU/Linux se suele llamar *ircd*.
2. Modificar la configuración del servidor, que se establece en base a los siguientes tipos de registros:

   A: información administrativa.
   B: balance de carga.
   C: conexiones con otros servidores.
   I: clientes que se pueden conectar al servidor.
   K: eliminar usuarios incontrolados.
   M: definir los parámetros de funcionamiento del servidor.
   O: definir usuarios administradores del servidor.
   P: establecer los puertos de comunicación.
   Y: definir clases de conexiones.

3. Reiniciar el proceso demonio para que los cambios tengan efecto.

EJERCICIOS PROPUESTOS

1. Indica los pasos a seguir para crear una cuenta que permita acceder al servicio de mensajería instantánea Google Talk.

2. Explica los pasos a seguir para que tu equipo Windows funcione como servidor de mensajería instantánea Openfire.

3. Indica los pasos a seguir para configurar el cliente de correo Pidgin de forma que pueda acceder al servidor de mensajería instalado en el ejercicio anterior. ¿Qué diferencia existe entre instalar Pidgin en el mismo equipo que ejecuta Openfire o instalarlo en otro equipo? ¿Y si se instala en un equipo GNU/Linux?

4. Indica los pasos a seguir para instalar otro servidor de mensajería Openfire sobre un equipo GNU/Linux. ¿Cómo se puede configurar este servidor para que los usuarios que se conectan a él puedan intercambiar mensajes con usuarios conectados al servidor instalado en el ejercicio 2?

5. ¿Es posible configurar un servidor Openfire de forma que los usuarios se puedan dar de alta en él sin la intervención del administrador? ¿Es posible permitir conexiones al servidor Openfire de forma anónima, es decir, sin necesidad de especificar un usuario y una contraseña?

6. Indica los pasos a seguir para instalar y configurar un servidor IRC en GNU/Linux.

7. Configura un cliente en Windows para que se conecte al servidor creado en el ejercicio anterior.

8. Configura el cliente Pidgin para que se conecte al servidor creado en el ejercicio 6.

TEST DE CONOCIMIENTOS

1 Clientes de mensajería instantánea son:
a) XMPP.
b) IRC.
c) Pidgin.
d) Todas son ciertas.

2 Para conectar con un servicio de mensajería desde Pidgin hay que especificar estos parámetros:
a) Protocolo de comunicación utilizado.
b) Usuario.
c) Contraseña.
d) Todas son ciertas.

3 Google Talk funciona sobre el protocolo
a) XMPP.
b) OSCAR.
c) IRC.
d) Ninguna es cierta.

4 La orden */CHANNEL* de IRC se usa para:
a) Anunciar que vamos a estar un tiempo sin atender la conversación.
b) Cambiar el apodo del usuario.
c) Enviar un mensaje a otro usuario.
d) Ninguna es cierta.

5 La orden IRC que se usa para introducir a un usuario en un canal es:
a) */CHANNEL*
b) */JOIN*
c) */QUERY*
d) a y b son ciertas.

6 El puerto por defecto de la herramienta de administración de Openfire es:
a) 7070.
b) 8080.
c) 9090.
d) Ninguna es cierta.

7 Los parámetros a especificar para configurar el servidor Openfire son:
a) Nombre de la base de datos de información de Openfire.
b) Dominio asociado.
c) Direcciones de correo electrónico de los usuarios.
d) Todas son ciertas.

8 Los usuarios que intercambian mensajes a través de Openfire se crean:
a) Manualmente en el servidor.
b) Automáticamente desde un servidor LDAP.
c) Automáticamente desde Clearspace.
d) Todas son ciertas.

9 Un registro O de un servidor IRC se usa para:
a) Establecer información administrativa.
b) Configurar conexiones con otros servidores.
c) Definir administradores del servicio.
d) Establecer los puertos de comunicación.

9 Servicios de audio

OBJETIVOS DEL CAPÍTULO

- ✓ Entender el funcionamiento general del servicio de audio.
- ✓ Conocer la terminología empleada en torno al servicio de audio.
- ✓ Distinguir las distintas formas de difusión del audio, especialmente el streaming.
- ✓ Describir las características de los principales formatos de audio.
- ✓ Introducir la tecnología streaming.
- ✓ Conocer la forma de suscribirse a reproducciones grabadas o podcast.
- ✓ Instalar y configurar los servicios de audio Windows Media Services e Icecast.
- ✓ Conocer distinto software de reproducción de audio y la forma de acceder a servidores de audio.

Todos somos conocedores de distintas formas en las que el audio se ha transmitido a lo largo del tiempo como por ejemplo la radio, cubriendo grandes distancias en su difusión, o mediante un reproductor de casete, en vías de extinción. El desarrollo tecnológico y sobre todo con la aparición de redes de ordenadores e Internet, ha provocado que se generen nuevas demandas por parte de los usuarios, como escuchar programas de radio vía Internet, los programas que fueron emitidos por radio o mantener conversaciones de voz. El servicio de audio ha surgido para proporcionar una alternativa a la transmisión tradicional, adaptándose a las nuevas necesidades de los usuarios, sobre todo para utilizarse sobre Internet.

Este capítulo aborda principalmente las transmisiones de ficheros de audio a través de un servidor y, de forma más trivial, las emisiones en directo, omitiéndose las conversaciones de voz a través de redes o VoIP, tratadas en el capítulo 12.

9.1 FUNCIONAMIENTO DEL SERVICIO

El objetivo básico del servicio de audio consiste en facilitar la transmisión de audio entre un emisor y un receptor. Para alcanzarlo podemos hacer una vez más referencia al modelo cliente-servidor, donde el servidor es el equipo que alberga el audio en forma de ficheros, o bien se encarga de obtenerlo de una fuente externa, como por ejemplo mediante un micrófono y una tarjeta de sonido (véase Figura 9.1). Cuando el audio se obtiene de una fuente externa que genera una señal que no es digital, suele realizarse un proceso de conversión o digitalización, además de su compresión para evitar que la difusión a través del software correspondiente consuma grandes recursos tanto en el servidor como de ancho de banda. Por su parte, el cliente se encargará de acceder al servidor mediante el software apropiado para escuchar la emisión en directo, o bien reproducir una grabada a través de los altavoces o auriculares conectados a una tarjeta de sonido.

Existen distintas maneras que el servidor es capaz de proporcionar el audio, así como la forma que tienen los clientes de obtenerla:

- **Descarga directa**: consiste en implementar este tipo de servicio alojando en un sitio web o ftp los archivos de audio que los potenciales clientes puedan requerir. Para proporcionarlo se necesitará implementar un servicio HTTP en el servidor (véase capítulo 3), de manera que atienda las demandas de los clientes para la descarga de los ficheros de audio mediante su navegador o el software adecuado. Esta forma de proporcionar dicho servicio requiere que el cliente descargue el archivo de audio para posteriormente reproducirlo de forma local. El conseguir que la reproducción sea más rápida dependerá del tamaño del archivo de audio descargado y del ancho de banda de la conexión utilizada en la descarga. A la hora de reproducir nuevamente los contenidos, no es necesario volver a descargarlos, sino simplemente abrir el archivo correspondiente para reproducirlo.
- **Descarga progresiva**: permite la reproducción del audio de forma simultánea a la descarga del archivo que lo contiene. Esta forma presenta inconvenientes debido a las diferencias en la velocidad de transmisión y de reproducción, ya que el reproductor se podría quedar sin sonido que reproducir.
- **Streaming**: se descarga tan solo la información necesaria a reproducir, permitiendo realizar ajustes en la calidad de la reproducción y ancho de banda utilizado para evitar cortes (véase apartado 9.3).

Para conseguir la transmisión de un flujo de sonido sobre redes conmutadas, debe existir un mecanismo previo de digitalización, convirtiendo el audio en paquetes antes de ser enviados al destinatario. Esta digitalización se realiza mediante técnicas de muestreo de la señal analógica generada por el dispositivo emisor del audio, dando lugar a una señal en formato digital. La **frecuencia** o **tasa de muestreo** nos indica el intervalo de tiempo transcurrido entre cada una de las muestras tomadas de la señal analógica. Es decir, cuanto mayor es dicha frecuencia, menor es el intervalo de tiempo de muestreo y, por tanto, la calidad de la señal digital resultante será mejor. Debido a las limitaciones del oído humano,

la frecuencia de muestreo tiene un umbral tras el cual su aumento no supondría una mejora en la calidad, ya que nos resultaría imperceptible.

Cada muestreo se cuantifica con un determinado número de bits, siendo más precisa a mayor número de bits utilizados. Debido al carácter de la señal analógica (continua o de infinitos valores), es imposible cuantificarla fielmente mediante la señal digital e inevitablemente presenta pérdidas tras la conversión.

Para reducir el espacio de almacenamiento del audio digitalizado y aumentar la velocidad de transmisión, se recurre a técnicas de compresión. Se ha de tener en cuenta que los mecanismos que implementa esta técnica también deben estar presentes en el receptor del audio, de forma que pueda interpretar el flujo de sonido en formato digital y comprimido que ha recibido en forma de paquetes. El software encargado de esta dititalización y compresión es efectuado por el **codificador/decodificador** o **códec**. Para conseguir un mayor grado de compresión, algunas técnicas aprovechan las características del oído humano para eliminar aquellos elementos de la señal que no son relevantes. Una de las técnicas más conocidas para la compresión es el estándar MPEG, utilizado también para vídeo.

La codificación debe tener un carácter escalable, es decir, debe poder adaptarse al ancho de banda utilizado y al número de usuarios conectados, de forma que la transmisión no se vea limitada por un incremento en el número de usuarios o por la reducción del ancho de banda.

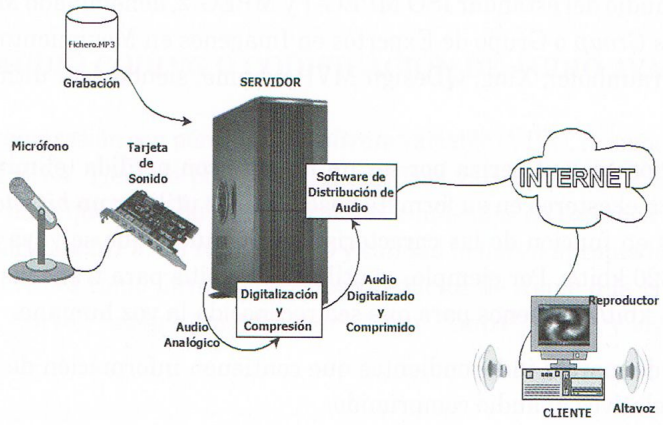


Figura 9.1. *Funcionamiento del servicio de audio. En esta figura se aprecian las posibles fuentes de audio, así como el proceso que sufre hasta que la información de audio llega al receptor para su reproducción*

A la secuencia de bits resultante de la digitalización y compresión del audio que se transmite por cada unidad de tiempo se denomina **bitrate** o tasa de bits. Si se utiliza una tasa alta, el flujo de audio se transmitirá a mayor velocidad, aunque por el contrario ocupará más ancho de banda y podrá entorpecer otras transmisiones. Para evitarlo se suele utilizar un *bitrate* variable o **VBR** (*Variable Bit Rate*), el cual cuantifica con un menor o mayor número de bits la señal de audio a transmitir, en función de si los fragmentos de audio corresponden a información no significativa, como es el caso de los silencios, o si son fragmentos donde se requiere mayor calidad. También existe la posibilidad de utilizar un *bitrate* constante o **CBR** (*Constant Bit Rate*), que cuantifica la señal de audio con un número determinado de bits independientemente de su aporte o no de información significativa.

Una o varias señales de audio pueden transportarse a la vez mediante un único flujo, las cuales se conocen como **canales**. De esta forma se denomina *mono* al flujo de un solo canal o que transporta una única señal, estéreo cuando transporta dos señales, o por ejemplo, *5.1* cuando transporta seis señales. En general al flujo que transporta más de una señal de audio se denomina *multicanal*.

9.2 FORMATOS DE AUDIO

De entre los formatos de audio más utilizados habitualmente, podemos encontrar algunos que no ofrecen compresión y otros que sí. Además, los formatos que utilizan compresión podemos catalogarlos en dos tipos:

- **Con pérdida**: comprimen el audio eliminando aquella información que no es perceptible por el oído humano.
- **Sin pérdida**: comprimen el audio eliminando redundancias en la señal de audio.

De entre los formatos de audio utilizados hoy en día podemos destacar los que se citan en los siguientes subapartados.

9.2.1 MP3

Es el formato de comprimido de audio por excelencia más conocido y tal vez utilizado por todos, logrando que aparezcan en el mercado gran cantidad de dispositivos para reproducción de audio en dicho formato. Forma parte del subsistema de compresión de audio del estándar ISO MPEG-1 y MPEG-2, denominado MPEG Layer III y desarrollado por el *Moving Pictures Experts Group* o Grupo de Expertos en Imágenes en Movimiento (MPEG). Podemos encontrar distintas versiones como la Fraunhofer, Xing, QDesign MVP o Lame, siendo ésta última una de las recomendadas debido a su rapidez y calidad.

Dicho formato de compresión se caracteriza por ser un formato con pérdida (elimina la información inservible), no es multicanal, ya que utiliza el estéreo en su formato base, y puede utilizar un *bitrate* CBR o VBR. Puede codificar el audio con distintos *bitrates* en función de las características del audio que se vaya a transmitir o de su calidad, obteniéndose un máximo de 320 kbit/s. Por ejemplo, se utilizan 96 kbit/s para transmisiones de radio FM, 192 kbit/s para sonido en calidad CD ó 4 kbit/s al menos para que sea reconocida la voz humana.

Cada archivo se compone de marcos independientes que contienen información de sincronización mediante una cabecera, así como los datos relativos al audio comprimido.

Este formato está patentado y por tanto requiere el pago de una licencia por su uso, utilizando como extensión de los ficheros ".mp3" y como tipos mime "audio/mpeg", "audio/MPA" o "audio/mpa-robust".

9.2.2 OGG VORBIS

Es un formato libre de código abierto desarrollado mayoritariamente con licencia GNU GPL, no siendo necesario el pago de licencias por su uso. Desarrollado por Xiph.Org, como alternativa a los formatos propietarios, ofrece un alto grado de compresión sin hacer que se pierda calidad en dicho proceso. Ogg hace referencia al contenedor de audio, vídeo y metadatos, y Vorbis al esquema específico de compresión de audio diseñado para estar contenido en Ogg. Este formato contempla un campo donde se puede almacenar información relativa al título, autor o albúm de la canción. Proporciona soporte para varios canales de sonido y admite el cambio del *bitrate* sin volver a codificar el archivo. La extensión utilizada por los ficheros de este formato es ".ogv", ".oga", "ogx" o ".ogg", y el tipo mime asociado "application/ogg".

9.2.3 MIDI (INSTRUMENTO MUSICAL DE INTERFAZ DIGITAL)

Es un estándar utilizado para trabajar con dispositivos de carácter electrónico asociados al terreno musical capaces de generar sonidos, como un sintetizador o tarjeta de sonido. Puesto que los sonidos pueden provenir de varios

dispositivos o instrumentos, se utiliza el método denominado canal para diferenciarlos, que asigna un número a cada uno de ellos.

Mediante este formato se transmiten mensajes al dispositivo receptor, de manera que los pueda interpretar como si de una partitura se tratara. Cada mensaje lleva consigo unas instrucciones referidas a las características que han de tener las notas, así como el momento de reproducirla.

Debido a las características de su compresión, puede combinarse con vídeo para ser utilizado en karaokes. Los archivos en este formato son de pequeño tamaño y su extensión es ".mid".

9.2.4 WAVE O WAV (*WAVEFORM AUDIO FILEFORMAT* O FORMATO DE FICHERO DE AUDIO EN FORMA DE ONDA)

Desarrollado por Microsoft, es utilizado para las grabaciones de discos compactos o CD utilizándose una frecuencia de muestreo de 44 Khz y una cuantificación de 16 bits. No utiliza compresión adquiriendo los archivos un gran tamaño, no siendo apropiados para utilizarlos a través de redes como Internet, quedando relegados para la reproducción de sonidos o voz de corta duración. Admite canales mono y estéreo y es la extensión ".wav" la utilizada en sus ficheros.

9.2.5 AAC (*ADVANCED AUDIO CODING* O CODIFICACIÓN DE AUDIO AVANZADA)

Es un formato que utiliza compresión con pérdida y un *bitrate* variable (VBR), reconocido como estándar y extensión de MPEG-2, e incluido en MPEG-4. Tiene la posibilidad de utilizar varios canales y la frecuencia de muestreo que puede llegar utilizar (96Khz) hace que sea uno de los formatos empleados en estudios de grabación, proporcionando un mejor rendimiento que el formato MP3. Su rendimiento y calidad lo hacen apropiado para la transmisión en redes y es utilizado por los IPod e ITunes como formato de estos productos de Apple o la Nintendo DSi. Las extensiones para este formato son ".m4a", ".m4b", ".m4p", ".m4v", ".m4r", ".3gp", ".mp4", ".aac", y los tipos mime asociados "audio/aac", "audio/aacp".

9.2.6 WMA (*WINDOWS MEDIA AUDIO*)

Desarrollado por Microsoft como formato de compresión de audio, que además de una reducción del archivo de audio consigue adaptarse a la velocidad de conexión, siendo aceptable para la reproducción en tiempo real a través de redes. La extensión de los archivos de este formato es ".wma".

9.2.7 REAL AUDIO

Desarrollado por Real Network para utilizarse en transmisiones de tiempo real como la radio, pudiendo utilizarse también para transmisiones bajo demanda. Para la reproducción de dicho formato se ha de utilizar su reproductor Real Player, permitiendo ajustar la recepción del sonido en función de determinados parámetros del cliente, como por ejemplo la velocidad en la conexión establecida. La principal extensión utilizada en los archivos en este formato es ".ra", aunque también encontramos ".ram", ".rm" o ".rmm".

9.3 STREAMING

Una forma ya mencionada de proporcionar el servicio de audio es el streaming o flujo, aplicable también al servicio de vídeo y, por tanto, conviene conocerlo de forma más detallada. Se caracteriza por permitir, entre otras cosas, ajustar la calidad de los contenidos a transmitir y por tanto del ancho de banda utilizado. Además no realiza descargas completas de los contenidos, sino descargas temporales del contenido que se está reproduciendo en un determinado momento, eliminándose tras su reproducción. Uno de los objetivos que persigue es conseguir que la reproducción se mantenga sin pausas ocasionadas por errores en la transmisión.

Dentro de la tecnología de streaming y atendiendo al momento en el que se proporciona, podemos distinguir dos formas de utilizarla:

- **Streaming en tiempo real o en directo**: el servidor asume el control del audio, digitalizándolo, comprimiéndolo y efectuando su transmisión de forma instantánea hacia el cliente. Suele utilizarse en transmisiones en directo o de difusión como la radio. Además del servidor encargado de proporcionar el flujo multimedia, es probable que se necesite un equipo independiente o **broadcaster** encargado de capturar y comprimir al vuelo la información multimedia que se pretende transmitir.

El término Webcast también es utilizado para la transmisión en vivo de audio o vídeo a través de Internet como si de la televisión o la radio se tratara. Dicha transmisión se realiza mediante difusión o broadcast a múltiples receptores a la vez.

Al tratarse de una transmisión en tiempo real, requiere de protocolos ligeros que no efectúen un control muy exhaustivo de la transmisión, evitando demoras al cliente. Aunque se produzcan pérdidas durante la transmisión del audio, durante su reproducción resulta apenas imperceptible para el cliente. Algunos de los protocolos utilizados en dicha tecnología son:

  - **RTSP** (*Real Time Streaming Protocol* o Protocolo de Flujo en Tiempo Real): se ocupa de controlar el flujo multimedia en ambas direcciones de manera que exista sincronización entre cliente y servidor, permitiendo al usuario el acceso aleatorio a partes del flujo (salto de capítulo, rebobinado, etc.).
  - **RTP** (*Real-time Transport Protocol* o Protocolo de Transporte en Tiempo real): es un protocolo especialmente diseñado para el transporte en tiempo real de información, y por tanto puede encargarse de la transmisión de contenido multimedia. Los reproductores utilizan su información para reproducción de contenidos en el orden y a la velocidad adecuada.
  - **RTCP** (*Real-time Control Protocol* o Protocolo de Control en Tiempo real): proporciona información que es utilizada por otros protocolos en capas superiores para adecuar la transmisión multimedia al estado en que se encuentra la red (congestionada, sin tráfico, etc.).
  - **UDP**: es un protocolo que no se encarga del control de errores como FTP, por tanto también puede ser utilizado en transmisiones de contenidos de naturaleza multimedia.

- **Streaming bajo demanda**: el contenido multimedia previamente se digitaliza y se comprime, almacenándose en forma de grabación en el servidor, de manera que los clientes puedan reproducirlo según sus necesidades, siendo este último quien asume el control de la recepción. En este caso no es tan relevante utilizar protocolos

que ejerzan mayor control de la transmisión como HTTP o FTP, ambos basados en TCP. Como desventaja, señalar que el servidor se tiene que encargar de proporcionar partes del flujo diferentes a los usuarios. Además, al haberse codificado el audio previamente, no se podrá adaptar al ancho de banda utilizado y a las características de los clientes.

El flujo multimedia puede tener uno o varios destinatarios a los que va dirigida dicha información, pudiendo distinguirse distintas formas de difundirla:

- **Unicast**: aunque los clientes acceden al mismo contenido multimedia, cada uno de ellos utiliza su propio flujo multimedia y por tanto una conexión con el servidor, haciéndose necesario un mayor ancho de banda ante el tráfico generado por los clientes en la red.
- **Broadcast**: el servidor envía el flujo multimedia a todos los equipos de la red, quieran o no recibir dicha información. Tiene el inconveniente de generar gran cantidad de información y por tanto puede llegar a saturar la red.
- **Multicast**: el mismo flujo multimedia es enviado por el servidor a todos los clientes que desean recibirlo a la vez, reduciendo el tráfico y la congestión de la red. Suele utilizarse en streaming en tiempo real y si se utilizan encaminadores como dispositivos de interconexión, deben utilizar los protocolos adecuados (por ejemplo DVMRP, MOSPF o PIM) para manejar el flujo de forma eficiente.
- **Relaying Media**: es una solución mixta que combina algunas de las anteriores formas de difusión, de forma que emplea *unicast* para la transmisión entre el servidor multimedia o un broadcaster y la red de destino donde se encuentran los clientes, y *multicast* para difundir el contenido multimedia a todos los clientes de la red de destino. Un equipo de la red local a la que pertenecen los clientes (relay), se encargará de la recepción del flujo unicast y de su conversión en multicast.

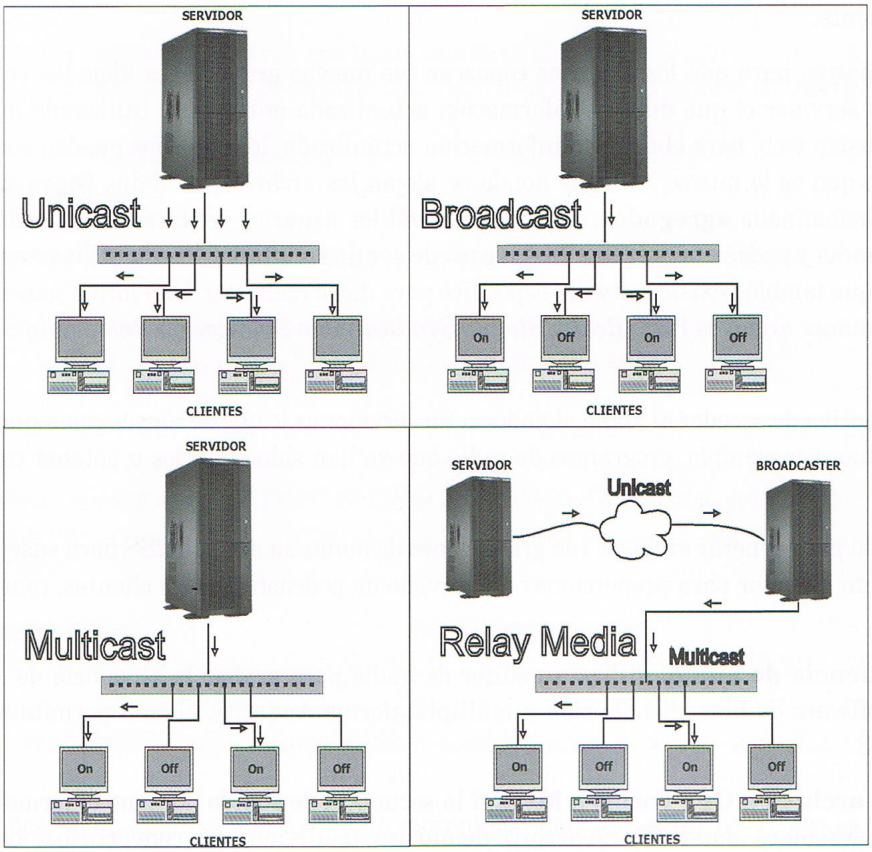


Figura 9.2. *Difusión de un flujo multimedia. En esta figura se aprecian mediante la dirección de las flechas las distintas formas de difundir un flujo multimedia, distinguiendo en algunos casos los clientes que no están disponibles*

Algunos de los problemas que nos podemos encontrar y que afectan a la utilización de dicha técnica son fácilmente deducibles, como un ancho de banda insuficiente, un retraso en los paquetes o latencia, un elevado número de usuarios demandando los contenidos multimedia o cortes en la reproducción o **lag**.

Para intentar evitar algunos de estos problemas y obtener una mejor sincronización entre el cliente y el servidor, el software de reproducción multimedia del cliente utiliza un buffer o zona temporal de memoria, donde se almacena el contenido multimedia que le llegan mediante un proceso denominado precarga o **buffering**. El empleo del buffer es lo que permite que, en caso de demoras, en la recepción de la información multimedia se pueda reproducir la que tiene almacenada.

Gracias a la precarga, se consigue continuidad en la reproducción multimedia, evitando pausas de cara al usuario en espera de más información. Otra forma empleada para mantener dicha continuidad consiste en degradar la calidad del vídeo, viéndose disminuido el número de fotogramas que se transmiten por unidad de tiempo, permitiendo conservar la calidad establecida para el audio.

9.4 SINDICACIÓN Y SUSCRIPCIÓN DE AUDIO. PODCAST

Las secuencias de audio pueden grabarse y ser almacenadas en un servidor para su posterior reproducción. Esto permite la descarga y reproducción diferida, no siendo necesario coincidir en el tiempo con su emisión. Para que el usuario pueda conocer los nuevos archivos alojados en el servidor tendría que acceder periódicamente y hacer la comprobación pertinente.

Una forma alternativa para que los usuarios conozcan las nuevas grabaciones alojadas en el servidor consiste en que sea el propio servidor el que difunda información actualizada entre ellos, utilizando lo que se conoce como **sindicación** o redifusión web. Para obtener la información actualizada, los usuarios pueden suscribirse a la **fuente de contenidos**, o lo que es lo mismo, el lugar donde se alojan los archivos de audio. Dicha suscripción se realiza mediante software denominado **agregador**, a través del cual los usuarios recibirán las novedades referentes a los nuevos archivos de audio y podrán acceder a ellos en caso de ser de su interés. Puede utilizarse un simple navegador como agregador, aunque también existe software específico para dicho menester. Una forma muy extendida de realizar la suscripción es mediante archivos RSS (*Really Simple Syndication* o Sindicación Realmente Simple), cuyo formato se basa en XML.

Esta forma alternativa de acceder al audio alojado en un servidor es lo que se conoce como **podcast** o **podcasting**, utilizado para escuchar, por ejemplo, programas de radio que ya han sido emitidos u obtener titulares de períodicos actualizados.

Una forma sencilla para generar archivos con grabaciones de audio, su archivo RSS para suscripción de los clientes y su alojamiento en un servidor para proporcionar un servicio de podcasting a los clientes, consiste en llevar a cabo los siguientes pasos:

1. **Obtener la secuencia de audio**: utiliza un editor de audio para grabar la secuencia de audio deseada, como por ejemplo el software de libre distribución y multiplataforma Audacity, el cual permite realizar la grabación directamente en MP3.

2. **Conversión del archivo a Ogg Vorbis o MP3**: si la secuencia de sonido no tiene el formato Ogg Vorbis o MP3 o si simplemente deseamos almacenar un archivo de música, tendremos que convertirlo a los formatos indicados, existiendo en el mercado un amplio abanico de este tipo de software como Audio Convert. Si se utiliza Audacity, a la

hora de guardar de forma automática con formato MP3 nos permite editar y añadir al archivo datos referentes al autor, álbum, género o el título de la grabación, entre otros (se pueden editar la etiqueta denominada ID3 Tag).

3 **Alojar el archivo en el servidor**: se pueden utilizar varios métodos para hacerlo, como por ejemplo mediante FTP (véase capítulo 4) o SSH (véase capítulo 5), existiendo numerosos clientes en el mercado como WinSCP o Filezilla.

4 **General el archivo RSS**: se puede utilizar un servicio de alojamiento que nos permite obtener la dirección del archivo a reproducir así como el RSS. Otra posibilidad es crear el RSS de forma manual, aunque existen plantillas que nos facilitan dicha tarea, como la que se muestra en el ejemplo 9.1, para un podcast en formato MP3. En nuestra página web, podremos crear un botón o enlace con la plantilla XML para que los clientes se puedan suscribir.

EJEMPLO 9.1

```
<rss version="2.0">

  <channel>

  <title>TITULO DE LA WEB</title>
  <itunes:explicit>Valor "si" para mayores de edad o "no" para todos los públicos
  </itunes:explicit>
  <link>Enlace a la web</link>
  <description>Descripción de la web</description>
  <itunes:subtitle>SUBTÍTULO DE LA WEB</itunes:subtitle>

  <!-- Línea opcional para incluir subtítulo -->
  <itunes:summary>Breve descripción de tu página</itunes:summary>

  <language>Idioma del podcast con el formato: "IDIOMA-PAIS" ("es-ES")
  </language>

<!-- Contenido para cada noticia o podcast al que suscribirse -->
    <item>
     <title>Título del podcast</title>
     <link>HTTP://Enlace al tema del podcast</link>
     <description>Descripción del podcast</description>
     <enclosure url="URL del MP3" length="tamaño en bytes del MP3"
     type="audio/mpeg"/>
     <guid isPermaLink="true">HTTP://Enlace al tema del podcast
     </guid>
    </item>

  </channel>

</rss>
```

Los usuarios que desean suscribirse a la fuente de contenidos suele encontrar un enlace en la página web, en la barra de direcciones o incluso puede utilizar un icono u opción de menú del navegador para llevarla a cabo (véase Figura 9.3).

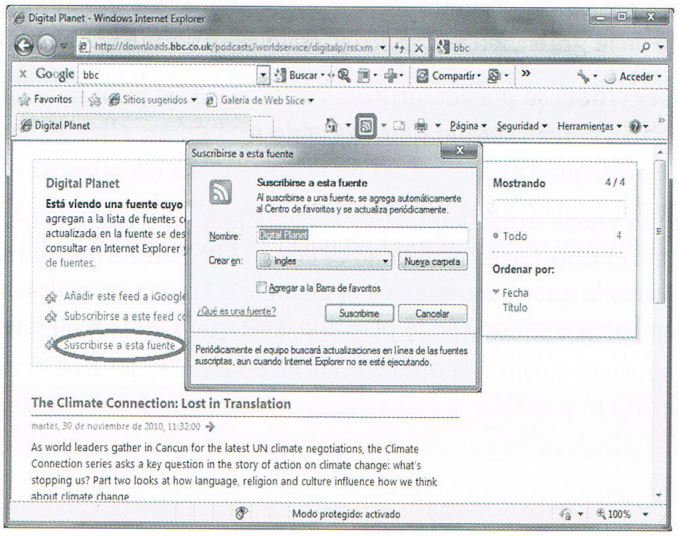


Figura 9.3. *Suscripción a un podcast con IExplorer. En esta figura se aprecia el botón que IExplorer pone a nuestra disposición para la suscripción a podcast RSS, pudiendo hacerlo mediante enlaces de la propia web, mostrándose la información requerida para la suscripción a la fuente de contenidos*

9.5 CONFIGURACIÓN DEL SERVIDOR

En este apartado se expone brevemente el software *Windows Media Services* desarrollado para algunas versiones del sistema operativo Windows de Microsoft, ejemplificándose mediante la puesta a disposición de los clientes un directorio con ficheros previamente grabados. También se aborda el software Icecast para sistemas operativos GNU/Linux, así como el codificador *Ices*, ejemplificándose sobre una distribución Debian 5 Lenny ofreciendo bajo demanda una lista de reproducción para los clientes.

La configuración de este servicio se asemeja en parte a la del servicio HTTP, ya que para la distribución de contenido previamente grabado es necesario un directorio donde ubicarlo a modo de sitio web. El streaming en tiempo real se trata y ejemplifica en el capítulo siguiente mediante la utilización de software de codificación.

9.5.1 CONFIGURACIÓN EN MICROSOFT WINDOWS

Las versiones 7 y 2008 Server de este sistema operativo disponen de software especializado en streaming denominado *Windows Media Services* (WMS), que permite generar en general flujos de carácter multimedia, soportando los formatos Windows Media, MP3 y MPEG. Su instalación puede ser completa o la denominada Core, que hace una instalación mínima. En un sistema operativo 2008 Server requiere seguir los siguientes pasos:

1 Descargar el software de la página de soporte de Microsoft (véase enlaces de interés), ya que dicha función no se incluye en el sistema operativo como la asignación automática de direcciones, transferencia de ficheros o servicio http entre otras. Descargaremos el archivo MSU acorde al procesador de nuestro equipo (32 ó 64 bits).

2 Ejecutaremos el fichero descargado en el paso anterior siguiendo los pasos del asistente para su instalación.

3 Ejecutamos el "Administrador de servidores" localizado dentro de las "Herramientas administrativas".

4 En el panel izquierdo pulsamos sobre "funciones", y en el panel derecho sobre el enlace "Agregar funciones", seleccionando la función "Servicios de multimedia de transmisión por secuencias", continuando con el asistente.

5 Si deseamos administrar de forma remota mediante web dicho servicio seleccionaremos, como servicio de función, "Administración basada en Web", el cual requiere también el servicio proporcionado por IIS (véase capítulo 3). Si además queremos un registro estadístico del uso del servicio seleccionaremos además el "Agente de registro".

6 El asistente nos indicará que se instalará software para el protocolo RTSP, continuando con el asistente hasta finalizar la instalación.

La configuración de este servicio se realiza mediante la herramienta administrativa "Servicios de Windows Media" o "Servicios de Windows Media (Web)" en el caso de administración mediante web, aunque también pude indicarse en un navegador como URL, la dirección IP del servidor junto con el puerto 8080. La configuración se realiza mediante **puntos de publicación** (véase Figura 9.4), estableciéndose uno por defecto. La creación de un punto de publicación conlleva realizar las siguientes acciones (véase ejemplo 9.2):

1 Iniciar la herramienta "Servicios de Windows Media".

2 Acceder al menú "Acción" y seleccionar la opción "Agregar punto de publicación (Asistente)".

3 Proporcionamos al asistente un nombre significativo para el punto de publicación.

4 Seleccionamos el tipo de contenido a transmitir:

- **Codificador**: se utiliza para transmisiones en directo.
- **Lista de reproducción**: se utiliza para transmisiones de varias secuencias de audio.
- **Un archivo**: se utiliza cuando se quiere difundir un archivo con una grabación de audio.
- **Archivos de un directorio**: se utiliza cuando se quiere publicar el contenido de un directorio a modo de lista de reproducción.

5 Se indica el tipo de punto de publicación, pudiendo seleccionar de difusión, en el que los clientes comparten la difusión de la secuencia de audio, y a petición, donde cada cliente selecciona la secuencia de audio a reproducir.

6 Seleccionamos la forma de entregar el contenido, si por unidifusión (unicast) o por multidifusión o multicast.

7 En este paso, si en el paso 4 seleccionamos "Codificador", indicaremos al asistente la URL que identifica al codificador, ya que se encargará de recoger la emisión en directo mediante el micrófono y codificarla. En caso de utilizar archivos o listas de reproducción, indicaremos el directorio donde se encuentran los ficheros de audio.

8 Activamos o no el registro de información de los clientes que se conecten.

9 Finalmente se nos muestra un resumen y se nos pregunta si queremos iniciar el punto de publicación al finalizar el asistente.

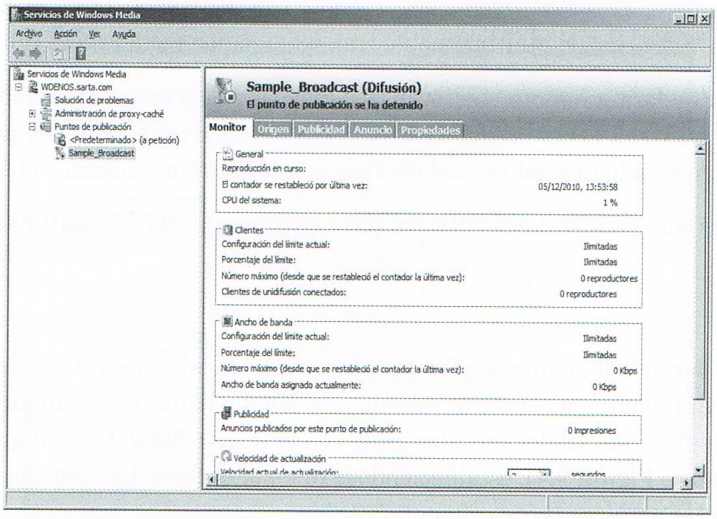


Figura 9.4. *Punto de publicación. Windows Media Services proporciona el servicio de audio mediante puntos de publicación, instalando uno por defecto (Sample_Broadcast) cuyas características y propiedades se muestran en el panel derecho*

Al seleccionar en el panel izquierdo de la herramienta "Servicios de Windows Media" el punto de publicación creado, en el panel central obtendremos varias fichas. La ficha "Origen" indica el directorio donde se encuentra el audio, o la URL donde se localiza el codificador del audio en directo. La ficha "Anuncio" nos indica las posibilidades que tenemos para acceder al punto de publicación, mientras que la ficha "Propiedades" permite establecer parámetros de configuración adicionales al punto de publicación.

EJEMPLO 9.2

Deseamos proporcionar un servicio de audio poniendo a disposición de los clientes un conjunto de archivos en formato MP3 para poner a disposición de los clientes el directorio *music* ubicado en la unidad *C*, al cual se le denominará PublicMusic. Se utilizará un sistema operativo Windows 2008 con el software Windows Media Services instalado.

Los pasos a seguir para la configuración del punto de publicación, son los siguientes:

1. Accedemos a "Inicio || Herramientas administrativas || Servicios de Windows Media".
2. En el panel izquierdo, pulsamos sobre el servidor.
3. Pulsamos sobre el menú "Acción" y elegimos la opción "Agregar un punto de publicación (Asistente)", tras el cual se iniciará el asistente.
4. Indicamos el nombre del punto de publicación: PublicMusic.
5. Seleccionamos como tipo de contenido la opción "Archivos".
6. Marcamos como punto de publicación a petición.
7. Accedemos *C:\music* mediante el botón "Examinar" para indicarlo como la ubicación del directorio.
8. Marcamos los dos tipos de reproducción de contenido.
9. No habilitamos el registro de unidifusión.
10. Tras mostrarse el resumen, finalizamos el asistente.

9.5.2 CONFIGURACIÓN EN GNU/LINUX

Existe una amplia variedad de software para la implementación de un servidor de audio, aunque podemos destacar *Shoutcast* o *Icecast*, siendo éste último sobre el que ejemplificaremos y explicaremos los aspectos más relevantes de su configuración utilizando una distribución Debian Lenny.

Icecast está desarrollado por *Xiph.org*, fundación que se encarga del proyecto que lleva su mismo nombre. Este software disponible para plataformas Microsoft y Linux, permite la difusión de audio en una red utilizando la tecnología de streaming, cuyas características principales son las siguientes:

- ✓ Soporta los formatos Ogg Vorbis y MP3.
- ✓ Gestiona la autenticación de clientes y proveedores de audio.
- ✓ Proporciona información al cliente acerca de su estado.
- ✓ Es capaz de proporcionar varios streamings de forma simultánea.
- ✓ Admite la posibilidad de que existan clientes que pueden proporcionar secuencias de audio o ficheros al servidor.
- ✓ Permite la emisión en directo a modo de radio.
- ✓ Permite variar la calidad del audio y limitar el número de clientes.
- ✓ Puede formar parte de una estructura arborescente junto con otros servidores para reparto de carga ante saturaciones.

El paquete necesario para su instalación es *icecast2*, tanto en Debian, como Fedora u OpenSuse, cuya configuración se realiza principalmente con el archivo *icecast.xml*, ubicado en el directorio */etc/icecast2*.

Puesto que el archivo de configuración tiene formato XML, las opciones de configuración se establecen entre etiquetas. La configuración se organiza en distintas secciones, atendiendo al aspecto de configuración a establecer. Algunas de las secciones más relevantes de la configuración son las que se exponen a continuación (véase ejemplo 9.3):

- **Establecimiento de límites**: mediante la etiqueta <clients> nos permite configurar entre otros parámetros el máximo número de clientes que se pueden conectar al servidor.
- **Autenticación**: mediante la etiqueta <authentication> nos permite configurar distintas contraseñas, cada una configurada con una etiqueta distinta:
  - Con la etiqueta <source-password> se configura la contraseña que se le solicitará y deberá conocer el codificador para la digitalización y compresión del audio.
  - La etiqueta <relay-password> permite configurar la contraseña que nuestro servidor utilizará para obtener audio de otro servidor.
  - Mediante la etiqueta <admin-user> se establece el nombre del administrador del servidor de audio.
  - La etiqueta <admin-password> establece la contraseña que utilizará el administrador para la administración del servidor a través de página web.
- **Otros parámetros del servidor**: permite configurar el nombre del equipo mediante la etiqueta <hostname>, el cual debe asociarse a una dirección IP pudiendo utilizarse localhost, ya que tiene asociada la dirección 127.0.0.1. También se puede configurar el puerto de escucha mediante la etiqueta <port>, y el puerto de escucha de una interfaz de red específica mediante la etiqueta <listen-socket>, indicando el puerto mediante <port> y la dirección IP que la interfaz tiene asociada mediante <bind-address>.

- **Rutas a ficheros**: mediante etiquetas permite configurar la localización de los diversos ficheros que intervienen en el servicio. La etiqueta <basedir> permite indicar el directorio base, con <logdir> la localización de los ficheros de bitácora, mediante <pidfile> la localización del fichero que contiene el PID del demonio de Icecast, con <webroot> se indica la ubicación de los ficheros que se pueden reproducir, <adminroot> indica la localización del directorio utilizado para labores de administración.

El demonio *icecast2* es el encargado de atender las solicitudes de los clientes, y al igual que otro servicio es necesario su puesta en marcha mediante el comando correspondiente, aunque previamente hay que editar el fichero */etc/default/icecast2* y establecer ENABLE con valor true. En Debian Lenny podemos utilizar la orden *sudo /etc/init.d/icecast2 start* para iniciar dicho servicio.

Puesto que Icecast utiliza archivos con formato Ogg Vorbis, necesitaremos el codificador correspondiente, como por ejemplo Ices, cuya instalación se puede realizar mediante Synaptic, la orden *apt-get* o descargarlo y compilarlo. Posteriormente crearemos el directorio */etc/ices2* y copiaremos el fichero *ices-playlist.xml* de */usr/share/doc/ices2/examples* al directorio que previamente se ha creado, ya que utilizaremos Icecast para permitir a los clientes la reproducción de una lista de reproducción. En caso de querer utilizarse para la transmisión en vivo a modo de radio, se configuraría el archivo *ices-live.xml*. La configuración de Ices al igual que Icecast, se realiza incluyendo los valores deseados entre las etiquetas correspondientes. Al menos estableceremos los siguientes parámetros en el fichero *ices-playlist.xml*:

- **Nombre de la radio**: lo establecemos mediante la etiqueta <name> localizada dentro de <stream>.
- **Género de nuestra radio**: se estable mediante la etiqueta <genre> también localizada en <stream>.
- **Descripción sobre nuestra radio**: utilizaremos otra etiqueta ubicada en <stream> denominada <description>.
- **Localización del fichero con la lista de reproducción**: mediante la etiqueta <param name="file"> localizada en <input>, indicamos su ubicación.
- **Nombre del servidor**: se establece mediante la etiqueta <hostname>, pudiendo utilizarse *localhost* para referirnos al propio equipo.
- **Puerto**: mediante la etiqueta <port> incluida dentro de <instance>, indicamos el puerto de escucha, por defecto el 8000.
- **Contraseña**: con la etiqueta <password> localizada dentro de <instance>, indicaremos la misma contraseña que utilizamos en <source-password> en la configuración de Icecast.
- **Bitrate**: por defecto utiliza un *bitrate* de 64kbps para la codificación, pudiéndose modificar mediante la etiqueta <nominal-bitrate> incluida en <encode>.

Una vez configurado dicho archivo debemos añadir al fichero que contendrá la lista de reproducción la ubicación de cada una de las canciones. Para ello ejecutaremos la orden *find RutaACanciones -iname "*.ogg" > RutaAFicheroDeListaDeReproduccion* (véase ejemplo 9.3). Finalmente la ejecución del codificador la realizaremos mediante la orden *ices2 /etc/ices2/ices-playlist.xml &*.



EJEMPLO 9.3

Deseamos configurar un servidor de audio Icecast mediante una distribución Debian Lenny 5, de forma que los archivos con formato ogg vorbis que tenemos almacenados en el directorio */tmp/music* estén a disposición de los clientes a través de nuestra emisora "radiostation", dedicada a música pop y rock, y cuya lista de reproducción generaremos en el mismo directorio donde reside el fichero de configuración de Icecast.

1. Instalamos el paquete *icecast2*:
```
$ sudo apt-get install icecast2
```
2. Editamos el fichero *icecast.xml* y modificamos las líneas que incluyen las siguientes etiquetas:
```
$ sudo nano /etc/icecast2/icecast.xml
      <source-password>tentenpie</source-password>
      <admin-user>icecast</admin-user>
      <admin-password>tentenpie</admin-password>
```
3. Editamos el fichero */etc/default/icecast2*:
```
$ sudo nano /etc/default/icecast2
      ENABLE=Yes
```
4. Iniciamos el servicio correspondiente a Icecast mediante la orden:
```
$ /etc/init.d/icecast2 start
```
5. Instalamos el codificador *ogg vorbis ices2*:
```
$ sudo apt-get install ices2
```
6. Creamos el directorio para el codificador y copiamos el fichero de configuración por defecto:
```
$ sudo mkdir /etc/ices2
$ sudo cp /usr/share/doc/ices2/examples/ices-playlist.xml /etc/ices2
```
7. Editamos el fichero de configuración del codificador y establecemos los parámetros de nuestra emisora mediante las siguientes etiquetas:
```
$ sudo nano /etc/ices2/ices-playlist.xml
      <name>My Radio Station</name>
      <genre>Pop_Rock</genre>
      <description>Radio dedicada al Pop y al Rock</description>
      ...
      <param name="file">/etc/icecast2/playlist.txt</param>
      ...
      <port>8000</port>
      <password>tentenpie</password>
      <mount>/radiostation</mount>
```
8. Generamos la lista de reproducción:
```
$ sudo find /tmp/música -iname "*.ogg" > /etc/icecast2/playlist.txt
```
9. Ejecutamos el codificador:
```
$ sudo ices2 /etc/ices2/ices-playlist.xml &
```

Mediante cualquier navegador web podremos administrar y tener acceso a información relativa a nuestro servidor de audio y, por tanto, a la emisora configurada (véase Figura 9.5). Para ello indicaremos la dirección IP y el puerto configurado previamente en */etc/icecast2/icecast2.xml*. La página de inicio nos solicitará el nombre de usuario y la contraseña que establecimos en el citado fichero de configuración.

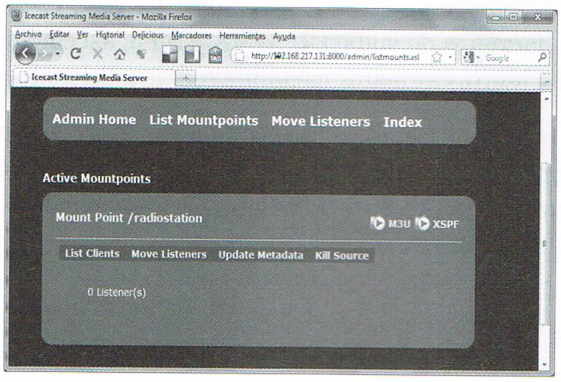


Figura 9.5. *En esta figura se muestra la página web de administración de Icecast, donde aparece la emisora radiostation, a la que de momento no se ha conectado ningún cliente*

9.6 CONFIGURACIÓN DE UN CLIENTE

Para escuchar secuencias de audio desde un cliente es necesario que éste posea el software necesario que haga audible la información transmitida proveniente del servidor. Dicho software deberá encargarse el proceso inverso al realizado previamente a la transmisión por el servidor (digitalización y compresión), decodificando las secuencias de audio.

El software utilizado para la reproducción de audio puede ser de dos tipos:

- **Navegador web**: algunos soportan la reproducción de distintos formatos de audio, aunque suelen admitir la instalación de *plugins* (véase capítulo 3) para poder reproducir el formato de audio deseado.
- **Software instalable**: también conocido como reproductor, se instala sobre el sistema operativo y existe una gran variedad de ellos. Dependiendo del software que se instale algunos a su vez instalan un conjunto de codecs por defecto, permitiendo reproducir un conjunto de formatos de audio de forma predeterminada. Algunos admiten la instalación de *plugins* para conseguirlo, mientras que otros requieren la instalación independiente de los denominados paquetes de codecs o **codecpacks**. Muchos de estos productos son de propósito general, permitiendo la reproducción de vídeo, e incluso algunos incorporan el software necesario para proporcionar también el servicio de audio. Algunos formatos de audio como Real Audio requieren la instalación de su propio reproductor Real Media Player.

Cuando se utiliza la tecnología de streaming, el software cliente utiliza un buffer para almacenar el contenido multimedia (audio o vídeo), de forma que cuando cuando tenga los suficientes contenidos almacenados comience su reproducción conjuntamente con la descarga. Además, cuando la transmisión no es continua y la velocidad decae, se utilizan también los contenidos almacenados del buffer para paliar temporalmente dicho problema.

En los siguientes apartados se tratan brevemente los reproductores Windows Media Player para sistemas operativos Microsoft Windows, y Banshee para GNU/Linux, indicándose cómo realizar el acceso a un servidor de audio.

9.6.1 CONFIGURACIÓN EN MICROSOFT WINDOWS

Microsoft Windows admite la instalación de distintos tipos de software de reproducción, como VLC media player, Media Player Cassic, Kantaris, Winamp o MPlayer, aunque el cliente más popular es el reproductor Windows Media Player, incluido en todas las versiones de este sistema operativo.

Windows Media Player es capaz de reproducir los formatos de audio CD, WMA y MP3, así como los formatos de vídeo DVD, MPG, AVI y WMV. También puede reproducir otros formatos mediante codecs adicionales de terceros.

Para la reproducción de audio difundido por un servidor de audio, basta con pulsar sobre el menú "Archivo" y seleccionar la opción "Abrir dirección URL ...", que nos conduce a un cuadro de diálogo para que indiquemos la URL a la que deseamos acceder (véase Figura 9.6). Si el archivo de audio reside en un servidor Windows Media Server, indicaremos *mms* como protocolo a utilizar en vez de http.

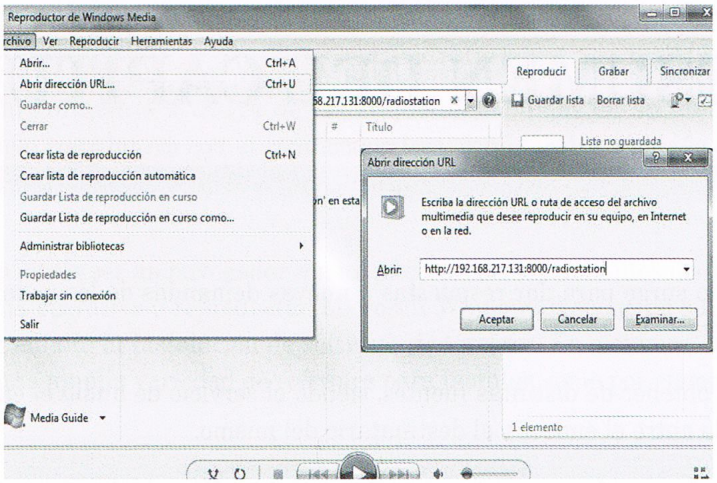


Figura 9.6. Acceso a un servidor de audio con Windows Media Player. El menú Archivo nos permite acceder a la URL del servidor de audio

9.6.2 CONFIGURACIÓN EN GNU/LINUX

En Linux también existe un aplio abanico de reproductores de audio como XMMS, Amarok, MPlayer, Kaffeine, Totem, Rhythmbox o Banshee, algunos de los cuales vienen instalados por defecto dependiendo de la distribución utilizada.

En nuestro caso abordaremos Banshee mediante una distribución OpenSuSE 11.1, caracterizado por permitir sintonizar radio vía Internet, organización de fonotecas locales y gestión de podcasts. Codifica, decodifica y por tanto reproduce distintos formatos de audio gracias a la plataforma o motor de reproducción GStreamer.

Para utilizarlo se requiere la instalación del paquete del mismo nombre, pudiendo realizarse por los procedimientos habituales que todos conocemos (apt-get, aptitude, Synaptic, YaST2, rpm, etc.).

Para acceder a un servidor de audio, tan solo necesitamos acceder al menú "Multimedia" y seleccionar la opción "Abrir ubicación...", apareciendo un cuadro de diálogo que nos permitirá indicar la URL de dicho servidor (véase Figura 9.7). En dicho menú se encuentra también ubicada la opción "Suscribirse a un podcast", que tras seleccionarla deberemos indicar la URL del podcast (véase Figura 9.7).

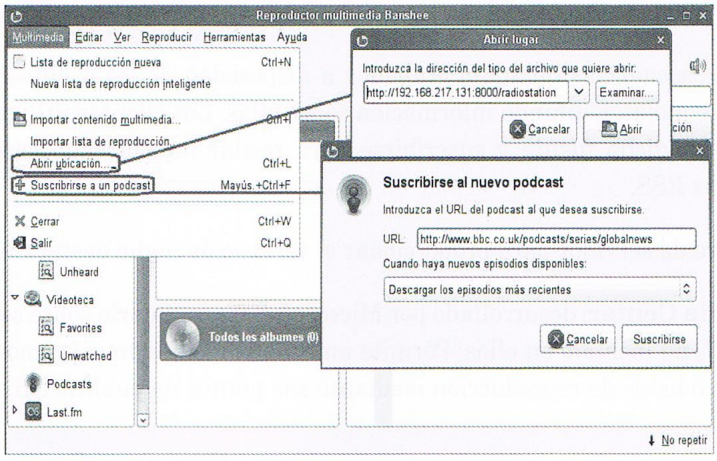


Figura 9.7. Mediante el menú Multimedia de Banshee podemos acceder a un servidor de audio así como suscribirnos a un podcast

RESUMEN DEL CAPÍTULO

El servicio de audio surge para dar respuestas a nuevas demandas de los usuarios originadas con el uso masivo de Internet.

El audio se puede obtener de distintas fuentes, siendo el servicio de audio el encargado de conseguir una transmisión fluida entre el emisor y el destinatario del mismo.

Distinguimos tres formas de proporcionar y obtener el audio, con descarga del servidor (directa), con descarga y reproducción simultánea (progresiva), o con descarga y reproducción de lo necesario (streaming).

Al obtener el audio de fuentes asíncronas, requiere su adaptación a la tecnologías de conmutación y por tanto su digitalización, empleándose una frecuencia o tasa de muestreo para cuantificar la señal. Dicha cuantificación puede generar gran cantidad de información, empleándose técnicas de compresión mediante un codificador/decodificador, pudiendo utilizarse distintas tasas de bits o *bitrate* para dicho proceso, distinguiendo aquellos que son variables (VBR) y constantes (CBR). Al codificarse el audio puede hacerse de varias señales y transmitirlas a la vez, obteniendo flujos monocanal o multicanal como el 5.1.

Al codificar el sonido podemos hacerlo utilizando formatos con y sin pérdida, siendo los más utilizados el formato MP3, Ogg Vorbis, MIDI, WAVE o WAV, AAC, WMA y Real Audio.

La técnica de streaming permite descargar solo aquella secuencia de audio o vídeo necesaria para su reproducción, permitiendo ajustar la calidad al ancho de banda, evitando interrupciones en la transmisión. Se puede utilizar para transmisiones en tiempo real siendo el broadcaster el encargado de su captura y codificación, empleándose protocolos ligeros para su transmisión, así como protocolos que permiten la sincronización y la adaptación al ancho de banda utilizado. También se puede utilizar realizando grabaciones previas almacenadas en un servidor. El flujo streaming puede difundirse a uno o varios destinatarios mediante unicast, broadcast, multicast y relaying media, empleando técnicas de precarga o buffering para conseguir la continuidad de la reproducción.

El podcasting pone secuencias de audio grabadas a disposición de los clientes mediante una fuente de contenidos, donde se alojan y difunde información sobre ellas. Los clientes utilizan un agregador como software para acceder a dicha fuente y suscribirse para recibir información actualizada, utilizándose habitualmente archivos RSS.

De entre el software de servidor para proporcionar el servicio de audio destacamos:

- **Windows Media Center**: desarrollado por Microsoft para instalarlo sobre sus sistemas operativos 2008 Server y 7, no incluido en ellos. Permite emisiones en directo así como proporcionar ficheros independientes o listas de reproducción mediante sus puntos de publicación.

- **Icecast**: soporta el formato Ogg Vorbis y MP3, siendo necesario el paquete icecast2 para su instalación, configurándose a través de las etiquetas incluidas en su archivo de configuración icecast.xml. Suele combinarse con el codificador Ices, configurable también mediante etiquetas y permitiendo ofrecer listas de reproducción que ofrecer a los clientes para su reproducción.

Un cliente de audio puede ser un navegador con los *plugins* correspondientes instalados, o un programa instalable en el sistema operativo o reproductor. Microsoft Windows dispone de su reproductor Windows Media Player, aunque admite la instalación de software de terceros. En sistemas operativos GNU/Linux disponemos también una amplia variedad de software para instalar, como por ejemplo Banshee.

EJERCICIOS PROPUESTOS

- **1.** Realiza la configuración del punto de publicación denominado UserRadio mediante un sistema operativo Windows 2008 Server, de forma que se utilice la carpeta "Musica" de uno de los usuarios para ponerla a disposición del resto.
- **2.** Indica cómo configurarías un cliente con Windows Media Player instalado para acceder al punto de publicación del ejercicio 1.
- **3.** Realiza la configuración de un equipo con sistema operativo GNU/Linux instalado para proporcionar una lista de reproducción de ficheros con formato ogg, ubicada en la carpeta personal de uno de los usuarios para proporcionársela al resto. La emisora creada se denominará SpeakerRadio.
- **4.** Indica cómo configurarías un cliente con el software Banshee instalado para acceder al a la emisora del ejercicio 3.
- **5.** Indica cómo configurarías el cliente de audio Banshee para acceder a un podcast de la BBC o de la Cadena Ser.

TEST DE CONOCIMIENTOS

1 La descarga progresiva:
- a) Realiza la descarga total del archivo a reproducir.
- b) Solo reproduce y descarga lo que se necesita en un determinado momento.
- c) La descarga y reproducción siempre está sincronizada.
- d) Ninguna de las anteriores.

2 El *bitrate* expresa:
- a) Los bits necesarios para digitalizar el audio en cada segundo.
- b) La velocidad a la que se digitaliza el audio.
- c) Los bits empleados en codificar el audio en cada segundo.
- d) La cantidad de bits necesarios para codificar el sonido.

3 El formato de audio Ogg Vorbis:
- a) Es un formato desarrollado por Microsoft para los discos compactos.
- b) Es un formato libre pero hay que pagar por él para utilizarlo.
- c) Es un contenedor de audio con pérdida de calidad.
- d) Al cambiar el *bitrate* del archivo no requiere volver a codificarlo.

4 En la técnica de streaming multicast:
- a) Se utiliza el mismo flujo y todos lo reciben aunque no lo quieran.
- b) Se aprovecha el mismo flujo para que lo reciban los clientes.
- c) Se utiliza un flujo para cada cliente que lo necesita.
- d) Ninguna de las anteriores.

5 En podcasting:
- a) El cliente utiliza la redifusión para suscribirse a la fuente de contenidos.
- b) El servidor difunde los contenidos mediante un agregador.
- c) El cliente utiliza el agregador para generar archivos RSS.
- d) La suscripción se puede realizar mediante RSS.

6 Ices2:
- a) Es el software necesario para proporcionar el servicio de audio.
- b) Es el software necesario para que codifique el audio de Icecast.
- c) Utiliza el fichero de configuración icecast.xml.
- d) b y c son ciertas.

7 La técnica de buffering:
- a) Es utilizada para evitar que se produzcan interrupciones.
- b) Es utilizada para sincronizar el cliente y el servidor.
- c) Permite utilizar audio almacenado ante cortes en la transmisión.
- d) Todas son ciertas.

8 En una transmisión de audio:
- a) Es importante ejercer fuerte control sobre ella para evitar fallos.
- b) Es importante adaptar su calidad al ancho de banda empleado.
- c) No es relevante utilizar información de tipo estadístico para su gestión.
- d) Todas son ciertas.

9 El formato MP3 de audio:
- a) Emplea información adicional para sincronización y compresión.
- b) Es un formato con pérdida que no se puede asemejar a la calidad CD.
- c) Siempre utiliza un *bitrate* fijo para conseguir una calidad sustancial.
- d) Siempre utiliza un *bitrate* variable para adaptarse al tipo de audio.

10 Servicios de vídeo

OBJETIVOS DEL CAPÍTULO

- ✓ Comprender el funcionamiento del servicio de vídeo así como la terminología empleada.
- ✓ Establecer puntos comunes con el servicio de audio.
- ✓ Describir las propiedades que caracterizan a una imagen.
- ✓ Conocer los principales formatos para imágenes y vídeos.
- ✓ Entender los fundamentos sobre videoconferencia y conocer distintas herramientas para su utilización.
- ✓ Instalar y configurar un servicio de vídeo streaming en directo.
- ✓ Conocer software de reproducción de vídeo para acceder a un servicio de vídeo.

Todos somos usuarios de la televisión, del cine, así como de otros medios de transmisión audiovisual. Si a este hecho añadimos que también lo somos de Internet, y por tanto de las redes, es fácil pensar en poder utilizar este elemento tan demandado hoy día para las transmisiones de multimedia, como por ejemplo la reproducción de vídeos musicales, comunicarnos con un amigo en la distancia o ver la televisión.

Aunque *a priori* las redes de datos no se pensaron para este tipo de transmisiones, estas nuevas exigencias y la convergencia de información de distinta naturaleza (datos, vídeo, audio, etc.), ha hecho posible que se desarrollen las tecnologías necesarias para hacerlo viable, como la utilización de protocolos orientados a las transmisiones en tiempo real.

Comprobaremos que el funcionamiento del servicio de vídeo guarda muchas similitudes con el servicio de audio, tratado en el capítulo anterior. Además, en la mayoría de los casos resulta inconcebible la transmisión de vídeo sin que se realice de forma conjunta con audio. Indicar que este capítulo no trata la suscripción o sindicación, ya que su tratamiento es similar al del audio (véase apartado 9.4).

10.1 FUNCIONAMIENTO DEL SERVICIO

El vídeo suele originarse tras su captura mediante una cámara, siendo habitual que también se realice del audio mediante el micrófono que llevan incorporado. Actualmente se utilizan cámaras de vídeo digitales, que permiten capturar aquellas secuencias de vídeo que deseamos y almacenarlas en un formato digital, bien en pequeños DVD regrabables o en discos duros, aunque a un nivel más profesional nos pueden servir para realizar emisiones en directo. Las grabaciones realizadas con este tipo de cámaras pueden pasarse fácilmente a un ordenador mediante una conexión USB o Firewire. Las antiguas cámaras aún utilizadas, guardan las capturas en cintas magnéticas, cuyo formato y tamaño ha evolucionado con el paso de los años. Para pasar las grabaciones con este tipo de cámaras a un ordenador y digitalizarlas se requiere de una capturadora, pudiendo instalarse en uno de los slots de expansión del ordenador, o incluso podemos encontrar capturadoras que se conectan a un puerto USB. La conexión de la cámara con la capturadora se realiza mediante conexiones de tipo RCA, S-Video, o a un nivel profesional mediante BNC. El paso de un dispositivo suele realizarse mediante software específico que suele acompañar a la capturadora. Hoy día también tenemos la posibilidad de realizar capturas de vídeo mediante una **webcam**, que pueden venir incorporada con el propio equipo como en portátiles o instalables como periféricos, siendo muy útiles sobre todo para establecer videoconferencias (véase apartado 10.5).

Una vez digitalizado el vídeo capturado y debido a la gran cantidad de información que genera, puede originar problemas en su transmisión necesitando grandes requerimientos de ancho de banda. De forma similar al audio será necesario utilizar codecs para su compresión (véase Figura 10.1), de forma que el ancho de banda no se vea tan afectado durante la transmisión. La codificación del vídeo se encargará de conseguir un compromiso adecuado entre la calidad obtenida por el cliente y el ancho de banda utilizado.

Tal y como se trató en el capitulo anterior, existen varias maneras de que el servidor pueda proporcionar el audio y que puede hacerse extensible al vídeo, como la descarga directa, progresiva y streaming (véase apartado 9.1), siendo ésta última la más apropiada para transferencias en tiempo real, no requiere espacio adicional ya que no realiza la descarga completa del flujo de vídeo en reproducción, permitiendo gestionar la calidad de transmisión dependiendo del ancho de banda y las posibilidades del cliente.

Además de la compresión del vídeo y una vez dividido en paquetes, se emplean protocolos como UDP y RTSP (véase apartado 9.3) consiguiendo que la transmisión sea continuada y que los errores sean inapreciables para el receptor. El control ante la pérdida de paquetes o variaciones en el ancho de banda se gestiona en la capa de aplicación de los

sistemas finales, es decir, en el software de vídeo, realizándose de forma independiente a las redes utilizadas y a los dispositivos de interconexión.

Cuando el equipo receptor recibe los paquetes y consigue ordenarlos, debe efectuar el proceso inverso al que se realizó en el emisor, descomprimiendo la información mediante los codecs. Finalmente, y para su reproducción, el cliente necesitará un reproductor que permita visualizar en el monitor el flujo de vídeo recibido, así como una tarjeta de sonido y unos altavoces o auriculares para escuchar el audio que lo acompaña. Este reproductor puede ser un navegador de web o software instalable o puede estar incluido en el sistema operativo.

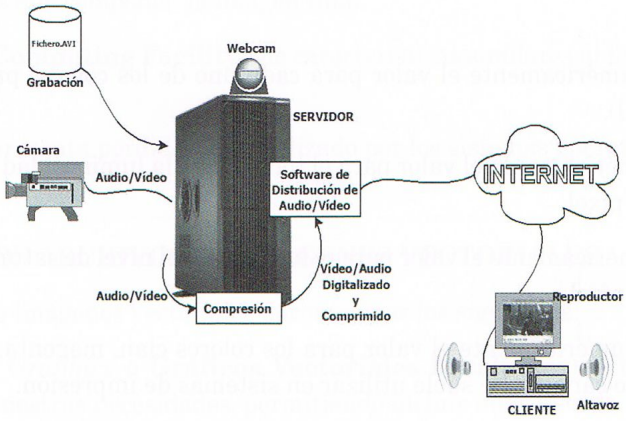


Figura 10.1. *Funcionamiento del servicio de vídeo. En esta figura se aprecian algunas fuentes posibles de obtener vídeo, así como el proceso que sufre hasta que la información de vídeo llega al receptor para su reproducción*

10.2 FORMATOS DE IMAGEN

Un vídeo está compuesto por una secuencia de imágenes, cuyas propiedades pueden condicionar la calidad del vídeo. Una imagen digital se puede obtener de distintas fuentes, como una cámara digital, una webcam, programas de retoque fotográfico o un escáner, entre otras, pudiendo distinguir dos grupos a la hora de diferenciarlas:

- **Imágenes de mapa de bits o bitmap**: están formadas por una matriz de cuadrículas o celdas, cada una de las cuales conocemos como **píxel** (*picture element*).
- **Imágenes vectoriales**: están formadas por formas geométricas controladas o definidas mediante cálculos matemáticos, presentando la ventaja de poder ampliarse o reducirse sin pérdida de calidad.

10.2.1 CARACTERÍSTICAS DE LAS IMÁGENES DE MAPA DE BITS

De entre los conceptos y características que podemos encontrar entorno a una imagen de mapa de bits destacamos los siguientes:

- **Profundidad del píxel o de bit**: indica el número de colores posibles que puede adquirir cada píxel y se cuantifica en bits. La profundidad más pequeña que puede tener un píxel es de un bit, dos colores o dos niveles de gris, ya que un bit solo puede tener valor de 0 ó 1. Al utilizar un número mayor de bits de profundidad, significará que se podrán hacer más combinaciones de ceros y unos, pudiendo representar más colores o niveles de gris. Por ejemplo, con 16 bits de profundidad podríamos obtener 2^{16} colores, o lo que es lo mismo 65536 colores.

- **Color real o RGB**: se considera como tal a la utilización de 24 bits de profundidad, ya que la cantidad de colores que se pueden obtener es lo que los humanos podemos percibir en el mundo real, asemejándose a la calidad fotográfica. Los 24 bits utilizados se organizan en tres canales que representan los colores primarios (Red o rojo, Green o verde y Blue o azul). Cada canal utiliza 8 de los 24 bits, pudiendo representar 2^8 ó 256 colores, de manera que las combinaciones posibles de colores entre los tres canales asciende a 16.777.216. Al utilizar 32 bits se usa un canal para representar, la transparencia denominado alfa, utilizado en la superposición de imágenes.
- **Modos de color**: es el modelo utilizado para cuantificar los colores de forma numérica. Los más utilizados son los siguientes.
  - RGB: representar numéricamente el valor para cada uno de los colores primarios que puede tener cada píxel (véase color real).
  - HLS: representa numéricamente el valor para el tono (*Hue*), la luminosidad (*Light*) y el nivel de saturación (*Saturation*) de cada píxel.
  - HSB: representa numéricamente el valor para el tono (*Hue*), el nivel de saturación (*Saturation*) y el de brillo (*Brightness*) de cada píxel.
  - CMYK: representa numéricamente el valor para los colores cian, magenta, amarillo y negro mediante 32 bits, utilizando cuatro canales. Se suele utilizar en sistemas de impresión.
- **Tamaño**: expresada la altura y anchura de la imagen en una unidad de longitud o en pixel.
- **Resolución**: expresada en puntos por pulgada (ppp), representa el número de píxeles utilizados por unidad de longitud, empleándose habitualmente la pulgada. Dicha resolución no se refiere a la del monitor donde visualizamos la imagen, aunque puede conducirnos a error. Sin embargo para visualizar las imágenes acordes a la resolución establecida para el monitor, se recomienda utilizar una resolución determinada, como por ejemplo utilizar 96 ppp en las imágenes cuando la resolución del monitor es de 1024 × 768. Al utilizar mayor resolución conseguimos mejorar la calidad de la imagen, ya que utilizará mayor número de píxeles y de menor tamaño, aunque el archivo donde se almacene la imagen verá incrementado su tamaño.

10.2.2 FORMATO DE LOS ARCHIVOS DE MAPA DE BITS

Debido a que una imagen de mapa de bits requiere el almacenamiento de información por cada uno de los bits que la componen, se requiere gran espacio de almacenamiento y, por tanto, se suelen utilizar técnicas de compresión para su almacenamiento, aunque algunas pueden presentar pérdidas de información. De entre los formatos más representativos para almacenar imágenes de mapa de bits podemos destacar los siguientes:

- **BMP (Bit Mapped Picture)**: no presenta pérdidas y es utilizado por sistemas operativos Microsoft Windows para almacenar imágenes de hasta 24 bits de profundidad.
- **GIF (Graphic Interchange Format)**: no presenta pérdidas utilizando hasta 8 bits de profundidad, permitiendo animaciones y cuya utilización se ha enfocado principalmente a la web.
- **JPG o JPEG (Joint Photographic Experts Group)**: presenta pérdidas utilizando hasta 16 bits de profundidad y siendo uno de los formatos más utilizados por su alto nivel de compresión. Es recomendable no utilizar imágenes con este formato si se van a editar o retocar, ya que se volvería a comprimir con la consiguiente pérdidad de calidad.
- **TIF o TIFF (Tagged Image File Format)**: no presenta pérdidas y, por tanto, las imágenes almacenadas son de alta calidad aunque ocupan gran espacio en disco. Es un formato reconocido por casi todos los sistemas

operativos, así que puede utilizarse a la hora de escanear o si se quiere obtener una buena resolución en la impresión.

- **PNG** (**Portable Network Graphics**): presenta pérdidas y se creó como reemplazo del formato GIF por su mejora en la calidad (hasta 24 bits de profundidad) y la reducción del espacio en disco, aunque no permite animaciones.
- **PSD** (**PhotoShop Document**): presenta pérdidas y es utilizado por el software Photoshop para la edición de imágenes o retoque fotográfico, almacenando, entre otras, información relativa a los canales o las capas de imágenes superpuestas que componen la imagen final.
- **XCF** (**eXperimental Computing Facility**): de características similares al formato PSD aunque utilizado por el software libre GIMP.
- **PICT** (**PICTure**): no presenta pérdidas y es utilizado por los sistemas operativos de los equipos MAC.

10.2.3 FORMATO DE LOS ARCHIVOS DE IMÁGENES VECTORIALES

De entre los formatos para imágenes vectoriales encontramos los siguientes:

- **SVG** (*Scalable Vector Graphics* o **Gráficos Vectoriales Escalables**): está basado en XML y, por tanto, podemos adaptarlo a nuestras necesidades, permitiendo incluir imágenes de mapa de bits.
- **WMF** (*Windows MetaFile* o *MetaFichero Windows*): puede incluir también imágenes con formato de mapa de bits y se adaptándose muy bien a los programas de dibujo.
- **SWF** (*ShockWave Flash*): también conocido como tecnología flash desarrollada por Macromedia, es utilizado para representar imágenes utilizadas sobre todo en animaciones para la web.
- **EPS** (*Encapsulated PostScript Language* o **Lenguaje Encapsulado PostScript**): formato antiguo que puede contener tanto mapa de bits como gráficos vectoriales, constando de una parte imprimible y otra de previsualización, que de forma similar a un borrador nos permite visualizar a rasgos generales su contenido.
- **PDF** (*Portable Document Format* o **Formato de Documento Portable**): es un formato conocido por todos y utilizado sobre todo en la lectura e impresión de documentos sin pérdida de calidad que solemos descargar de Internet.

10.3 FORMATOS DE VÍDEO

Un vídeo no es ni más ni menos que la sucesión de imágenes denominados fotogramas o **frames**, que al pasar de una a otra a una determinada velocidad, nos da la impresión de que la imagen inicial ha cobrado vida percibiendo su movimiento. En una secuencia de vídeo podemos diferenciar una serie de parámetros que lo caracterizan y que afectan a la calidad que pueda tener el mismo, distinguimos los siguientes:

- **Fotogramas por segundo** (*framerate*): indica la frecuencia con la que los fotogramas se muestran por unidad de tiempo (segundo). A mayor número de fotogramas, significa que se percibe menos el tránsito de un fotograma a otro y, por tanto, se apreciará mejor calidad. Su abreviatura es **fps**, aunque también se puede expresar en hertzios (Hz). Por ejemplo, las normas europeas de transmisión televisiva PAL y SECAM establecen una frecuencia de 25 Hz, mientras que la norma estadounidense NTSC lo hace a 29,97 Hz.

- **Resolución**: expresada en píxeles, se indican los que se han utilizado para el ancho y el alto de las imágenes. Por ejemplo, un DVD con formato NTSC tiene una resolución de 720 × 480, mientras que un Super VCD tiene una resolución de 480 × 480.
- **Bitrate**: de significado similar al utilizado en la codificación del audio, expresa la información que se almacena (expresada en bits o múltiplos) por unidad de tiempo (segundo) a la hora de codificar las secuencias de imágenes.

En los siguientes apartados y pese a la existencia de una amplia variedad de formatos de vídeo, se abordan algunos de los más utilizados. Los formatos de vídeo indican la manera en que se almacenan los vídeos en nuestro ordenador, y tienen unas propiedades que los caracterizan atendiendo a los parámetros anteriores. Muchos de ellos son catalogados como **contenedores multimedia**, ya que almacenan audio, vídeo, subtítulos y otro tipo de información variada bajo un formato definido. Estos formatos contenedores codifican el audio y el vídeo por separado, uniéndose posteriormente en un archivo acorde al formato escogido para su transmisión. Es el reproductor cliente el que se tienen que encargar de separar el audio y vídeo, necesitando de los códecs necesarios para poder reproducir cada uno de ellos.

10.3.1 MPEG (*MOVING PICTURES EXPERTS GROUP* O GRUPO DE EXPERTOS EN IMÁGENES EN MOVIMIENTO)

En realidad no es un formato, sino un estándar ISO que define los métodos y normas a seguir para la codificación y la compresión tanto de imágenes en movimiento como del audio asociado. Ateniéndonos a sus directrices, podremos utilizar distintos codecs.

10.3.2 AVI (*AUDIO VIDEO INTERLEAVE* O AUDIO Y VÍDEO INTERCALADO)

Desarrollado por Microsoft, es un formato contenedor de audio y vídeo, los cuales pueden codificarse prácticamente en el formato que se desee. El almacenamiento del audio y del vídeo se realiza mediante capas intercaladas, es decir, utilizando una capa de vídeo seguida de una de audio y así sucesivamente. Puede contener audio en distintos idiomas, cada uno en secuencias independientes, de manera que el usuario pueda seleccionar el idioma mediante su reproductor. Proporciona una excelente calidad y pueden utilizarse sin compresión (*raw* o crudo) o con compresión mediante el empleo de codecs. La extensión de los archivos suele ser ".avi".

10.3.3 ASF (*ADVANCED STREAMING FORMAT* O FORMATO AVANZADO DE SECUENCIAS)

Desarrollado por Microsoft, está enfocado específicamente al streaming y se utiliza en la tecnología *Windows Media* (véase apartado 10.6.1), adecuándose al ancho de banda utilizado. Es un formato contenedor de audio y vídeo, pudiendo utilizarse la mayoría de codificaciones para cada uno de ellos, empleando la extensión ".asf" para sus ficheros.

10.3.4 WMV (*WINDOWS MEDIA VIDEO*)

Desarrollado por Microsoft, junto con Windows Media Audio o WMA (véase apartado 9.2.6), fueron introducidos para diferenciar el vídeo del audio mediante formatos separados, aunque se pueden utilizar de forma combinada. Este formato puede incluirse en otros formatos contenedores como ASF o AVI. La extensión de los ficheros es ".wmv", pudiendo renombrarse con extensión ".asf" para utilizarse con tecnología Windows Media. Indicar que su versión 9 también recibe el nombre de VC-1.

10.3.5 MKV (*MATROSKA VIDEO*)

Este novedoso formato contenedor debe su nombre a las famosas muñecas rusas (Matroska o Matrioska), ya que su filosofía se asemeja a ellas. Este formato de código abierto es capaz de contener en un único archivo, vídeo, sonido y subtítulos. Además, permite entre otras cosas la creación de menús, selección del idioma de audio o la elección de un subtítulo. La extensión utilizada por los ficheros de este formato es ".mkv".

10.3.6 QUICKTIME

A pesar de haber sido desarrolado por Apple para sus computadoras, se ha hecho extensible a otras plataformas. En sí es una tecnología que entre otras cosas permite la reproducción y edición de vídeo digital, ampliando la funcionalidad del sistema operativo en el manejo de archivos dinámicos. La extensión utilizada por los ficheros es ".mov".

10.3.7 REAL VIDEO

Al igual que Real Audio está desarrollado por Real Networks y solo puede reproducirse con el reproductor Real Media Player. Se caracteriza por requerir poco espacio en disco haciéndolo apropiado para utilizarlo en videostreaming. La extensión de sus archivos son: ".rv", ".ram", ".rm" y ".rmvb", utilizándose como tipo MIME *audio/x-pn-realvideo*.

10.3.8 FLASH VIDEO

Utilizado por conocidos sitios como Youtube o Google Video para la transmisión de vídeo a través de Internet gracias a la tecnología *Adobe Flash*. El contenido de este formato contenedor puede incluirse en ficheros ".swf". Los archivos con este formato pueden reproducirse mediante aplicaciones instaladas en el sistema operativo como "VLC", o bien ser reproducidos a través de un navegador gracias al *plugin* "Adobe Flash Player" (véase apartado 10.7).

10.3.9 OGG U OGV

Desarrollado por Xiph.org como formato contenedor de código abierto, que permite una alta compresión de vídeo con pérdida, siendo muy enficiente en las transmisiones multimedia mediante streaming. Admite la compresión de sonido y de vídeo empleando un único formato y los ficheros pueden utilizar la extensión ".ogg", aunque si son exclusivamente de vídeo pueden utilizar extensión ".ogv". Los tipo mime asociados a este formato son *application/ogg* y *video/ogg*.

10.3.10 DV (*DIGITAL VIDEO* O VÍDEO DIGITAL)

Es un formato ditital utilizado por videocámaras para almacenar las grabaciones de vídeo y para su transferencia a otro dispositivo como puede ser un ordenador. El sonido lo almacena en formato similar al de un disco compacto, comprimiéndose el vídeo de forma que ocupe poco espacio y con una calidad aceptable.

10.4 COMPRESIÓN DE VÍDEO

Al igual que sucede con el audio y debido a la gran cantidad de información que requiere el almacenamiento y transmisión de las secuencias de vídeo, se utilizan algoritmos matemáticos que la reduzcan o compriman, empleándose entre otras las siguientes técnicas:

- **Intra-frame** o **compresión espacial**: comprime los fotogramas por separado y, por tanto, obtiene una alta calidad, requiriendo gran espacio de almacenamiento. Un ejemplo de utilización de este método de compresión lo tenemos en la obtención de ficheros con formato AVI.
- **Inter-frame** o **redundancia temporal**: comprime el vídeo ateniéndose a las diferencias existentes entre los fotogramas, debido a que en determinadas secuencias de vídeo no es necesario cambiar la escena o simplemente requiere realizar una pequeña modificación, ya que la imagen no varía o lo hace sensiblemente. Obtiene una menor calidad que el anterior y es utilizado en la obtención de ficheros con formato MPEG.

De entre los codecs más utilizados para este menester, podemos citar los siguientes:

- **WMV**: desarrollado y utilizado por sistemas operativos Microsoft Windows para su reproductor.
- **MPEG**: segmenta las muestras obtenidas de imagen y sonido, basando su compresión en la técnica inter-frame. Atendiendo a la calidad que ofrecen y el ancho de banda que utilizan, existen diversos variantes:
  - MPEG-1: utiliza hasta dos canales para sonido (estereo) y una velocidad de 1,5 Mbps para almacenar vídeo. Creado para incluir vídeo en un CD de calidad similar al VHS con una resolución de 352 × 240 píxel.
  - MPEG-2: utiliza hasta cinco canales de sonido, utilizando una velocidad de hasta 40 Mbps y una resolución de 720 × 486 píxel. Es utilizado en vídeos en soporte DVD.
  - MPEG-4 o H.264: diseñado específicamente para la codificación de información multimedia utilizada en páginas web y dispositivos móviles. Los archivos tienen extensiones ".mp4", ".m4a", ".m4v" o ".mp4v", y suele utilizar el audio en formato AAC (véase apartado 9.2.5), pudiendo hacerlo también con formato MP3. Consume muy poco ancho de banda y ofrece una resolución de 176 × 144 píxel, convirtiéndolo en un formato propicio para establecer videoconferencias a través de Internet.
- **DivX**: basado en MPEG-4 y de calidad similar al DVD, es muy popular para la reproducción de vídeo a través de Internet como en reproductores de películas de uso doméstico, ya que consigue un alto grado de compresión consiguiento almacenar películas de DVD en un solo CD.
- **Xvid**: aunque también se basa en MPEG-4 y sus características son similares a DivX, es un codec libre.
- **DV**: utilizado por las videocámaras digitales almacenando el sonido en formato similar al de un disco compacto, comprimiéndose únicamente el vídeo de forma que ocupa poco espacio y manteniendo una calidad aceptable.

10.5 VIDEOCONFERENCIA

La difusión de vídeo presenta un gran inconveniente cuando dos o más personas desean comunicarse, y es su poco grado de interacción. El software de videoconferencia suple esta carencia permitiendo establecer una comunicación interactiva, bidireccional y en tiempo real entre dos o más personas mediante la transmisión de vídeo, audio y datos

como si estuvieran presentes en el mismo despacho. Este software se apoya en elementos hardware como cámaras de vídeo, micrófonos, monitores y redes de transporte para establecer contacto audiovisual entre los interlocutores.

Este tipo de transmisiones hace que el vídeo consuma un ancho de banda considerable, y por tanto su calidad va a depender de la misma así como el grado de compresión que se le aplique, recomendándose utilizar formatos más ligeros así como la utilización de ventanas cuyo tamaño en píxeles sea más reducido, como por ejemplo de 300 × 200.

Este tipo de software se aplica, entre otras cosas, para mantener reuniones ejecutivas, en congresos, cursos, seminarios, educación a distancia, o simplemente para contactar con alguien al que no hemos visto o no hemos tenido contacto recientemente. Las ventajas de este tipo de tecnología se hacen patentes, ya que evita gastos en desplazamientos, se ahorra tiempo ya que no hace falta viajar o buscar aparcamiento, permitiendo que la comunicación sea visual entre los interlocutores, favoreciendo la toma rápida de dicisiones.

Dependiendo de los dispositivos que intervengan en la videoconferencia, podemos establecer la siguiente clasificación:

- ✓ **Punto a punto**: se utilizan dos equipos en la conversación, a su vez distinguimos los siguientes tipos.
  - **Uno a uno o Desktop**: en una solución económica que se utiliza principalmente de ámbito doméstico, interviniendo dos personas en la conversación, realizándose la compresión del vídeo y del audio mediante software.
  - **Uno con un grupo**: utilizado principalmente en entornos empresariales, una persona mantiene una conversación con un grupo de ellas. El grupo puede utilizar una ubicación acondicionada expresamente con hardware específico y de cierta calidad o Room System, resultando una opción costosa. Otra opción es utilizar una plataforma o carrito que incluye todo el hardware necesario y que se puede desplazar fácilmente, denominada Roollabout, siendo una opción más económica que la anterior.
  - **Grupo con un grupo**: cada uno de los equipos permite intervenir a un grupo de personas en la videoconferencia y se encuentran ubicadas en un espacio convenientemente acondicionado con el hardware necesario.
- ✓ **Multipunto o multiconferencia**: se utilizan más de dos equipos en la conversación. Antes de iniciar la conversación se ha de determinar los interlocutores a visualizar en el monitor (todos, a unos pocos, solo al que habla...), así como la forma de hacer llegar la voz (uno habla y el resto escucha o todos pueden hablar). A su vez distinguimos los siguientes tipos.
  - **Centralizada**: todos los equipos participantes en la conversación contactan con un MCU (*Multipoint Control Unit* o Unidad de Multipunto de Control), el cual recibe los flujos multimedia y de control y se encarga de gestionar las conferencias.
  - **Descentralizada**: los equipos participantes se envían los flujos multimedia mediante paquetes multicast, optimizando el ancho de banda, aunque el flujo de control es gestionado a través de las MCU.

La tecnología utilizada en videoconferencia cumple estándares internacionales, como el conocido H.323, desarrollado por la ITU, que sustenta los pilares para transmisiones multimedia sobre redes de conmutación de paquetes. Se caracteriza por permitir establecer videoconferencias punto a punto o multipunto permitiendo, entre otras cosas gestionar el ancho de banda o las llamadas.

Existe diversidad de software utilizado para este tipo de transmisiones, pudiendo encontrar software instalable sobre el sistema operativo, y gracias a la tecnología Web 2.0 podemos llevar a cabo conversaciones utilizando un simple navegador web. También se han desarrollado herramientas de código abierto basadas en protocolos de mensajería, permitiendo utilizar cuentas de correo electrónico de MSN o Yahoo para establecer conversaciones y videconferencias, tal es el caso de AMSN o Pidgin, aunque sus posibilidades se limitan a ciertas redes de mensajería.

En este capítulo no se expone la instalación y configuración de software para videoconferencia instalable sobre un sistema operativo, ya que en el capítulo 12 se hace lo propio con el software Ekiga, disponible para varias plataformas y, aunque se ha orientado a la tecnología VoIP, puede también utilizarse para videoconferencia. Indicar que soporta el estándar H.323, permitiendo la conexión a través de un MCU. También podemos crearnos una cuenta SIP gratuita en la página principal de este software mediante el enlace "Get a Free-SIP Address", la cual podremos utilizar para establecer una videoconferencia con otro usuario que también haya obtenido su cuenta.

10.5.1 VIDEOCONFERENCIA MEDIANTE NAVEGADOR WEB CON DIMDIM

Podemos encontrar software propietario de videoconferencia para establecer conversaciones a través de nuestro navegador web, como *GTalk* de Google o *Messenger* de Microsoft. Su utilización está vinculada a una cuenta de correo, requiriendo autenticarnos en GMail o Windows Live, respectivamente, ofreciéndose como alternativa al uso del correo electrónico.

También encontramos sofware de videoconferencia ajeno a nuestras cuentas de correo y de código abierto como *Dimdim* (adquirido recientemente por *Salesforce*), que permite en tiempo real llevar a cabo reuniones o conversaciones colaborativas, cuyas características son las siguientes:

- ✓ Dispone de tres versiones: la versión *Free* o gratuita, que permite conversar a diez personas de forma simultánea; la *Pro* a cincuenta, utilizando cuatro cámaras proporcionando herramientas de colaboración y la *Webinar*, permite lo que la versión Pro, además de la gestión de grupos mediante análisis e informes.
- ✓ No necesita instalación, tan solo requiere utilizar un navegador web.
- ✓ Permite compartir nuestro escritorio, una región del mismo o una aplicación con el resto de interlocutores mediante la instalación del plugin *myScreen*, descargable en forma de ejecutable.
- ✓ Permite la utilización de cámaras, micrófonos así como un área para conversar.
- ✓ Mediante un widget se puede alojar en un sitio web para que otras personas puedan registrarse en una videoconferencia que hayamos planificado, para posteriormente compartir con ellos las conversaciones que se estén llevando a cabo.
- ✓ Sin necesidad de instalar software adicional, podemos grabar las conversaciones.
- ✓ Permite utilizar una pizarra multipágina, que crea un entorno de colaboración para que entre otras cosas los interlocutores editen contenidos, utilicen un puntero láser o un zoom sobre una imagen entre otras herramientas.
- ✓ Facilita la incorporación de la conversación que se está llevando a cabo a redes sociales mediante la utilización de URL cortas.
- ✓ Se puede integrar con otros servicios orientados a la web como YouTube, Flikr o Moodle.

La utilización de dicho software se realiza accediendo a la página principal de Dimdim (véase referencia bibliográfica), requiriendo un registro previo indicando un nombre de usuario a utilizar, una dirección de correo y una contraseña. Como se aprecia en la Figura 10.2, podemos observar las distintas partes que conforman dicha herramienta:

- *Opciones situadas en la parte superior*: muestra información acerca de la duración de la conversación y permite acabarla con el enlace "End Meeting". Mediante la lista Tools permite configurar la sesión, seleccionar el elemento a compartir mediante un asistente u obtener información sobre la conversación.
- *Show Items*: mediante este elemento podemos elegir entre compartir el escritorio, un área del mismo o una aplicación (Share Screen), utilizar una pizarra compartida como en la figura (Share Whiteboard), o bien compartir un documento (Share Document).
- *Participantes*: indica los nombres de los participantes de la conversación, permitiendo invitar con un *email* a otro participante mediante el botón "Invite", o gestionar los permisos sobre otros participantes mediante el botón "Manage".
- *Video Chat* (*Live*): permite activar nuestra cámara, así como nuestro micrófono. El icono con forma de rueda dentada permite seleccionar el dispositivo de vídeo y el de audio, con el icono de micrófono se activa o desactiva, el de full-screen para activar o desactivar la visualización a pantalla completa y, finalmente, el icono para aumentar o disminuir el volumen.

- *Now Sharing*: mostrada en la parte central de la herramienta, muestra lo que en dicho momento estemos compartiendo, permitiendo interactuar mediante iconos con el elemento compartido. Incluye también el botón "Record" para guardar la conversación.
- *Public Chat*: muestra un historial con los mensajes emitidos por los usuarios, proporcionando un área de texto para escribir nuestro mensaje e incluso incluir un emoticono. Puede ocultarse o mostrarse mediante la doble flecha situada en la parte superior derecha.

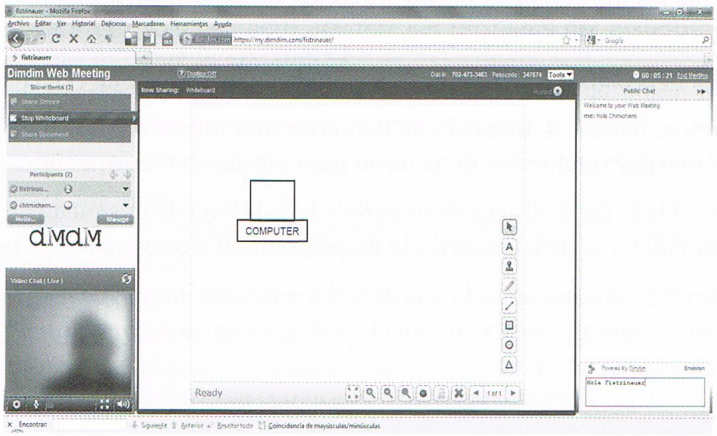


Figura 10.2. *Videoconferencia web con Dimdim. En esta figura se aprecian cada uno de los elementos que integran dicha herramienta web, utilizándose en este caso una pizarra compartida para ilustrar al receptor*

Como alternativas podemos utilizar software de carácter más sencillo como Ubiqq, que permite comunicarnos compartiendo una URL, o Tokbox que permite en tiempo real llevar a cabo reuniones o conversaciones colaborativas, y cuyas características son las siguientes:

- ✓ Dispone de tres versiones: la versión gratuita *Vídeo Chat* creada para conversaciones casuales, y las versiones de pago *Vídeo Meeting*, orientada a conversaciones establecidas bajo agenda y de carácter más formal, y *Vídeo Conference*, enfocada para una audiencia multitudinaria.
- ✓ No necesita instalación, tan solo requiere utilizar un navegador web.
- ✓ Se pueden establecer conversaciones con hasta un máximo de 20 personas.
- ✓ Permite la utilización de cámaras, micrófonos así como un área para conversar (chat box).
- ✓ Es posible invitar a otras personas mediante un mensaje que será enviado a aquellas cuentas de email que indiquemos. También se puede utilizar la URL que dicha herramienta proporciona para incluirla en Twitter o Facebook para que otras personas se unan a la conversación.
- ✓ Nos da la posibilidad de compartir vídeos de YouTube con otras personas sin abandonar la aplicación.
- ✓ Los contactos de otras aplicaciones como GTalk, Yahoo o Facebook y otros clientes de mensajería instantánea podemos importarlos a dicha aplicación web.
- ✓ Podemos grabar mensajes en formato de vídeo con una duración máxima de diez minutos, de forma que en ausencia de una persona, dicha aplicación se lo envíe mediante email.
- ✓ Mediante el API (*Application Programming Interface* o *Interfaz de Programación de Aplicaciones*) Opentok nos permite incluir un videochat en nuestro sitio web.

El acceso al software de Tokbox se se realiza accediendo a su página principal (véase referencia bibliográfica), donde encontraremos un enlace en la parte superior que nos remitirá a una página de registro, solicitándonos sobre todo una dirección de correo y una contraseña de acceso. Las distintas partes que conforman dicha herramienta son las siguientes:

- **Botón "Call Now"**: permite invitar a una o varias personas indicando su email y un mensaje, así como compartir vídeos de YouTube. Antes de realizar la invitación pertinente, nos da la posibilidad de activar la cámara y el micrófono mostrando nuestra imagen en la parte inferior.

- **Menú situado en la parte superior derecha**: nos permite modificar los datos referentes a nuestro perfil (opción *Me*), acceder a los vídeo mensajes que hayamos recibido (opción *Messages*), ajustar diversos aspectos referentes a nuestra cuenta como la selección y configuración de los dispositivos de captura de vídeo y sonido o editar los datos de acceso (usuario y contraseña), y mediante la opción "Help", obtener ayuda de la utilización de la herramienta organizada en categorías.
- **Llamadas recientes** (*Recent Calls*): muestra a modo de historial una relación de llamadas o conversaciones realizadas a otros usuarios indicando su hora y dirección de correo, permitiéndonos reanudarla mediante los enlaces "call again".
- **Llamadas entrantes** (*Upcoming Calls*): muestra a modo de histórico una relación de llamadas recibidas.
- **Búsqueda de usuarios**: mediante una caja de texto con una lupa a su derecha situada en la parte superior derecha, nos permite escribir un nombre de usuario para efectuar su búsqueda.
- **Estado del usuario**: al lado de la silueta de usuario y bajo la caja de búsqueda de usuarios, encontramos una lista desplegable para indicar a otros usuarios la disponibilidad a conversar que tenemos.
- **Contactos**: Mediante esta ventana situada a la derecha podemos llamar, buscar, editar, y añadir contactos, así como importarlos de otras aplicaciones web como *GTalk* o invitar a conversar a otra persona.

10.6 CONFIGURACIÓN DEL SERVIDOR

En este apartado se aborda la configuración de un servidor con sistema operativo Windows 2008 Server mediante *Windows Media Encoder* para codificar el audio y el vídeo, y *Windows Media Services* para su distribución. También se configura mediante una distribución Debian 5 Lenny el software de servicio de streaming *Darwin Streaming Server*, junto con su herramienta de codificación *mp4live*. En ambos casos la configuración se ejemplifica para una transmisión en directo.

10.6.1 CONFIGURACIÓN EN MICROSOFT WINDOWS

Tal y como se expuso en capítulo anterior, el software de servidor utilizado para las transmisiones de flujo multimedia correspondía a *Windows Media Services*. Para las transmisiones en vivo es necesario combinarlo con software que permita la codificación del audio y del vídeo, de forma que lo que se está capturando mediante una cámara y un micrófono, inmediatamente pueda ser difundido a través de *Windows Media Services*. Para poder codificar el audio y vídeo Microsoft desarrolló el software *Netshow Encoder*, que posteriormente evolucionó a *Windows Media Encoder* y que recientemente ha sido reemplazado por *Windows Expression Encoder*, cuya versión 4 puede obtenerse de forma gratuita pero no incluye soporte para H.264, siendo necesaria la instalación del correspondiente *Microsoft Framework .NET*.

Este apartado aborda la utilización del software de codificiación *Windows Media Encoder* mediante el ejemplo 10.1, no profundizándose en su configuración. Indicar que *Windows Media Encoder* pone a disposición de *Windows Media Services* un servicio para que pueda acceder al audio y vídeo codificado, no siendo necesaria la instalación explícita de servicio alguno en el equipo donde se vaya a instalar este software de codificación.

Puesto que la instalación y configuración del software *Windows Media Services* quedó expuesta en el apartado 9.5.1 del capítulo anterior, tan solo se ejemplificá su utilización (véase ejemplo 10.2) junto con *Windows Media Encoder* para proporcionar un servicio de streaming en tiempo real. Al no ser necesario que el software de difusión y el de codificación multimedia residan en el mismo equipo, la configuración del software en los ejemplos, se ha realizado sobre servidores independientes.

EJEMPLO 10.1

Se desea utilizar el software de codificación Windows Media Encoder sobre un equipo cuya dirección IP es la 192.168.1.15, el cual tiene conectado una cámara de vídeo y un micrófono para permitir una transmisión en directo.

Los pasos para poner en funcionamiento este software de codificación son los siguientes:

1. La instalación del software tan solo requiere aceptar los términos del acuerdo de licencia e indicar la carpeta de instalación para que pueda efectuarse.
2. Para iniciar dicha herramienta tan solo es necesario acceder desde el botón de "Inicio" a "Todos los programas" y localizar el programa denominado "Windows Media Encoder".
3. Seleccionaremos el icono "Broadcast a live event" y pulsaremos sobre el botón "Aceptar".
4. Un asistente no indicará los dispositivos de audio y vídeo utilizados por defecto, pudiendo ajustar parámetros como el brillo, saturación o la mezcla de entrada maestra mediante los correspondientes botones de "Configuración", aunque por defecto dejaremos la configuración tal cual.
5. Posteriormente debemos seleccionar el método de difusión, marcando "Pull from the encoder".
6. Seguidamente el asistente nos permite seleccionar el puerto a utilizar, así como la URL correspondiente para que el servicio HTTP nos permita acceder al audio y vídeo codificado. Podemos dejar los valores por defecto y acceder posteriormente al flujo multimedia codificado indicando como URL la dirección IP del equipo.
7. Mediante "Encoding Options" indicamos el tipo de codificación que deseamos. Por defecto utiliza el método CDR, dándonos la posibilidad de utilizar múltiples codificaciones con *bitrates*, *framerates* y tamaño de la ventana distintos. Si disponemos de ancho de banda suficiente podemos dejar las opciones por defecto.
8. Con "Archive File" nos permite guardar una copia del contenido multimedia codificado, no siendo necesario en este caso.
9. "Include Video Files" nos da la posibilidad de utilizar ficheros de vídeo como por ejemplo de bienvenida o despedida, no siendo tampo necesarios.
10. Opcionalmente podemos rellenar un formulario con datos referentes al vídeo difundido, como por ejemplo el título y el autor.
11. Finalmente se muestra un resumen de la configuración realizada, donde marcaremos la casilla de verificación "Begin broadcasting when I click Finish" para iniciar la codificación tras finalizar el asistente.
12. Tras pulsar el botón "Finalizar", la codificación se iniciará mostrándonos lo que actualmente se está codificando, un informe estadístico, un botón de "Stop" para detener la codificación, etc. (véase Figura 10.3).

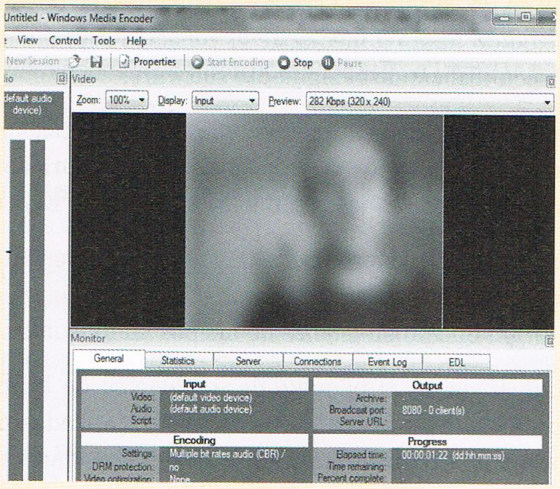


Figura 10.3. *Windows Media Encoder. En esta figura se aprecia el resultado de la codificación en vivo utilizándose 282 Kbps para la transmisión con una ventana de 320 x 240 píxeles. Nos da el acceso a información de tipo estadístico y la posibilidad de detener la emisión*

EJEMPLO 10.2

Se desea realizar una transmisión en directo desde un servidor con Windows 2008 Server que tiene instalado el software Windows Media Services, y cuya dirección IP es la 192.168.1.15. El punto de publicación se denominará "EnVivo" y se utilizará "Unidifusión".

Los pasos a realizar para crear y configurar el punto de publicación son los siguientes:

1. Iniciamos la herramienta "Servicios de Windows Media" desde "Herramientas administrativas".
2. Desplegaremos el árbol del panel izquierdo y sobre "Puntos de publicación" seleccionamos la opción "Agregar punto de publicación (Asistente)" del menú contextual.
3. Indicamos "EnVivo" como "Nombre del punto de publicación".
4. Seleccionaremos "Codificador" como "Tipo de contenido".
5. Marcaremos "Punto de publicación de difusión" como el "Tipo de punto de publicación".
6. Seleccionaremos "Unidifusión" como la forma de entrega del punto de publicación.
7. Indicaremos *http://192.168.1.39:8080* como URL del codificador, ya que es en dicho equipo donde en el ejemplo anterior se configuró el software Windows Media Encoder.
8. No utilizaremos registro de unidifusión.
9. Tras mostrarnos un resumen del punto de publicación configurado, marcaremos "Iniciar punto de publicación cuando finalice el asistente".
10. Antes de finalizar desmarcaremos "Una vez haya finalizado el asistente", observando la información referente a la forma de acceder al punto de publicación (*mms://192.168.1.15/EnVivo*).

10.6.2 CONFIGURACIÓN EN GNU/LINUX

La instalación en GNU/Linux de un servidor de streaming de vídeo se puede realizar mediante software diverso, como *Icecast* tratado en el capítulo de audio o mediante el conocido reproductor *VLC* o *VideoLAN*. Este apartado ilustra la instalación y configuración utilizando el siguiente software:

- **Darwin Streaming Server**: será el encargado de atender las peticiones cliente, facilitándoles mediante el protocolo RTSP, el flujo de vídeo en tiempo real resultante de la captura de la cámara y su posterior codificación, o archivos bajo demanda en diversos formatos como MP4, MOV, MPEG2 o MP3.
- **MPEG4IP**: desarrollado por Cisco Systems para implementar el estándar MPEG4 para una asociación de varias empresas denominada ISMA (*Internet Streaming Media Alliance*), cuyo objeto es el de establecerlo como un estándar de cara a Internet en transmisiones de medios audivisuales.
- **Herramienta mp4live**: incluida en el paquete de instalación de MPEG4IP, permite difusión multicast y soporta IPv6, se utiliza para codificar las capturas de vídeo realizadas por la cámara para transmisiones en directo, así como grabarlas en un archivo para transmisiones bajo demanda. También puede codificar el audio en formato MP3 o AAC, entre otros, permitiendo establecer distintos *bitrates* así como distintos *framerates* y resoluciones de ventana para el vídeo. El flujo de audio y vídeo codificado es entregado a *Darwin Streaming Server* para su difusión.

La instalación y configuración del software mencionado se realiza mediante el ejemplo 10.3 sobre una distribución Debian Lenny 5, aunque hay que indicar que previamente debemos asegurarnos de que nuestra cámara o webcam así como el micrófono, sean reconocidos por dicho sistema operativo (consulte los enlaces de interés al final del capítulo).

EJEMPLO 10.3

Se desea realizar una transmisión en directo desde un equipo con una distribución Debian Lenny instalada, cuya dirección IP es la 192.168.1.15 y el cual reconoce perfectamente la webcam integrada en su monitor, así como el micrófono. Utilizaremos la configuración por defecto y nos aseguraremos que el audio se codifica en formato AAC, utilizando en principio un tiempo de 15 minutos para la transmisión.

La instalación y configuración del software necesario se basa prácticamente en la ejecución de órdenes con los privilegios necesarios, así como la configuración de la herramienta *mp4live*. Los pasos a realizar son los siguientes:

1. Descargamos el software Darwin Streaming Server mediante la orden:
   ```
   wget -c http://static.macosforge.org/dss/downloads/DarwinStreamingSrvr5.5.5-Linux.tar.gz
   ```
2. Descomprimimos el software descargado anteriormente:
   ```
   tar -xvzf DarwinStreamingSrvr5.5.5-Linux.tar.gz
   ```
3. Creamos el grupo y usuario *gtss*:
   ```
   addgroup --system qtss
   adduser --system --no-create-home --group qtss
   ```
4. Instalamos el software Darwin Streaming Server para que se copien los archivos a sus directorios correspondientes, preguntándonos un usuario y contraseña para su posterior configuración mediante una interfaz web:
   ```
   cd DarwinStreamingSrvrlinux-Linux
   ./Install
   ```
5. Instalamos el paquete *mpeg4ip-server* mediante la herramienta *Synaptic*, la órden *apt-get* o la herramienta *aptitude*, siendo recomendable ésta última, ya que es posible que haya que desinstalar algunos paquetes como *libavcodec52* y *libdirac-encoder0*, e instalar otras versiones anteriores:
   ```
   aptitude install mpeg4ip-server
   mp4live
   ```
6. Comprobamos que realmente se está ejecutando:
   ```
   ps -ef | grep DarwinStreamingServer
   ```
7. Si no está ejecución lo haremos con la orden:
   ```
   /usr/local/sbin/DarwinStreamingServer
   ```
8. Configuramos el servicio Darwin Streaming Server iniciando un navegador web e indicando como URL:
   ```
   http://192.168.1.15:1220
   ```
9. El asistente nos solicitará la siguiente información:
   - A pesar de haber indicado una contraseña en la instalación del software, es posible que nos solice cambiarla.

- El directorio donde ubicaremos el contenido multimedia (General Settings), por defecto */usr/local/media*:
- El puerto de escucha (*Port Settings*). No marcaremos la casilla para ofrecer streaming a través del puerto 80, ya que es posible que en un futuro podamos instalar el servicio http. Por defecto se utilizarán los puertos 554 para los protocolos TCP y UDP.
- Si quisiéramos ofrecer una lista de reproducción (*Playlist*) podríamos crear una con los archivos multimedia que tuviésemos grabados. Puesto que la transmisión es en directo, no se creará.

10. Iniciamos la herramienta *mp4live* ejecutando la orden de su mismo nombre.
```
mp4live
```

11. La configuración de la herramienta *mp4live* requiere que (véase Figura 10.4):
    - Tanto el vídeo como el audio tenga la casilla "Enable" marcada.
    - "Duration" lo estableceremos a 15.
    - En la sección "Audio" desplegaremos la lista desplegable "Profile:" y seleccionaremos "Change Profile Settings", asegurándonos que "Encoding" tiene el valor "AAC".
    - "SDP File" lo dejaremos tal cual (default.sdp), que contendrá la información necesaria para acceder a la transmisión en directo, aunque nos aseguraremos que dicho fichero se ubica en */usr/local/movies*.
    - Marcamos "Preview Video Source" para ver una previsualización de lo que vamos a transmitir.
    - Guardaremos los parámetros de codificación seleccionados mediante "File || Guardar".
    - Pulsamos el botón "Start" para iniciar la transmisión.

12. Finalmente, y para acceder a la transmisión en directo, abriremos la URL *rtsp://192.168.1.15:554/default.sdp* desde un reproductor con soporte para el protocolo RTSP.

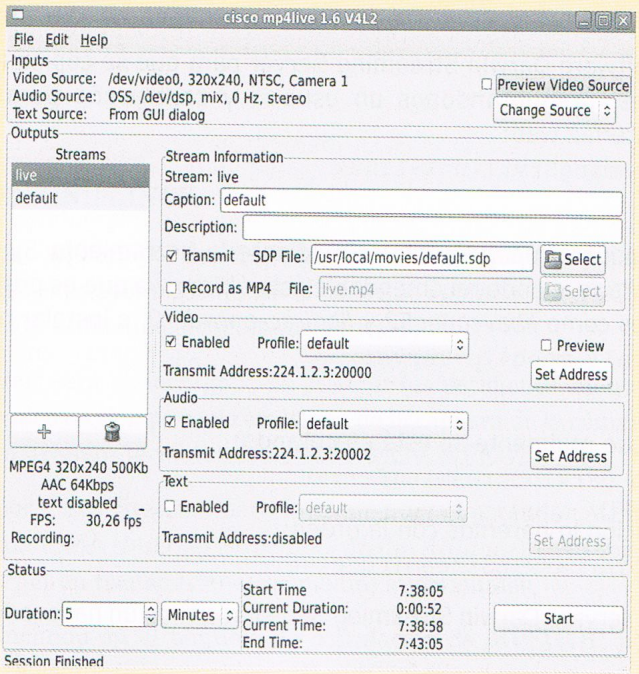


Figura 10.4. *Herramienta mp4live. La figura muestra las posibilidades de configuración de dicha herramienta, el directorio donde se almacenará el fichero ".sdp", el formato elegido para la transmisión de vídeo (MPEG4) y audio (AAC), así como los fotogramas por segundo y el tiempo de transmisión. El botón "Start" dará inicio a la transmisión*

10.7 CONFIGURACIÓN DE UN CLIENTE

En el capítulo anterior relativo al servicio de audio, se trató la posibilidad de reproducir sonido a través de un navegador web gracias a la instalación de *plugins*. Para la reproducción de vídeo de forma independiente o conjunta con el audio, es también necesaria la instalación de *plugins*, los cuales pueden estar desarrollados con distinta tecnología:

- **Adobe Flash**: esta tecnología permite crear archivos multimedia basados en fotogramas y está soportada por varios navegadores. La reproducción de dichos contenidos se lleva a cablo mediante el reproductor Adobe Flash Player, instalable mediante un *plugin* en el navegador.
- **Adobe Shockwave**: desarrollada en un principio por Macromedia y adquirida posteriormente por Adobe. Aunque no es tan famoso y utilizado como el anterior, también permite la reproducción de contendios interactivos como juegos o vídeos. Se instala de igual manera mediante un *plugin* en el navegador, es capaz de reproducir archivos flash y contiene un excelente motor 3D.
- **Microsoft Silverlight**: desarrollado por Microsoft, es una versión mini del marco de trabajo .NET, permitiendo que nuestro navegador, y mediante la instalación de un *plugin*, pueda manejar contenido multimedia de forma óptima. Su parte visual se basa en un lenguaje derivado de XML denominado XAML (*eXtensible Application Markup Language* o Lenguaje Extensible de Marcas para Aplicaciones). De su parte operativa, se encarga un lenguaje de programación como JavaScript o Java, pudiendo utilizarse otros. Soporta vídeo de alta definición, anunciándose también soporte para H.264.

En un entorno doméstico para la reproducción de contenido multimedia también es posible utilizar lo que se conoce como **Media Center** o Centro Multimedia. Un Centro Multimedia puede ser un equipo construido especificamente para tal fin, o un ordenador de propósito general al que se le añade el hardware y el software necesario. La reproducción de los contenidos multimedia pueden realizarla desde distintos medios o fuentes, como por ejemplo desde una unidad de DVD, un disco duro externo, una carpeta compartida en otro equipo, o incluso a tráves de Internet. Existe software especializado para dicho propósito, como Elisa (actualmente Moovida), instalable en sistemas operativos GNU/Linux y Windows, aunque sistemas operativos como Windows 7 ya incluyen el software necesario para poder utilizar nuestro ordenador como Media Center, pudiendo utilizarse un mando a distancia para su manejo.

En los siguientes apartados se abordan dos reproductores instalables muy conocidos, como *VLC* para plataformas Microsoft Windows y *Kaffeine* para plataformas GNU/Linux.

10.7.1 CONFIGURACIÓN EN WINDOWS

Aparte del propio reproductor de Microsoft (Windows Media Player), existe una gran variedad desarrollados para este sistema operativo, desde el clásico y sencillo Media Player Classic, el conocido BS Player que permite la descarga de los codecs necesarios, o los propietarios Quicktime de Apple (véase Figura 10.5) y Real Player de Real Networks. No podíamos pasar por alto un reproductor muy utilizado actualmente por todos y con un gran auge, VLC Media Player.



Figura 10.5. *Reproductor Quictime de Apple. En esta figura se aprecian los elementos de dicho reproductor: barra de menú, botonera e información de estado, indicándonos que se ha llevado una reproducción de una emisión en vivo cuya duración ha sido de 4:08 minutos*

VLC es un reproductor disponible para varios sistemas operativos, entre ellos Microsoft Windows y GNU/Linux. Además de servirnos como reproductor, también puede ejercer como servidor de streaming (consulte su wiki), soportando distintos protocolos como MMS, UDP/RTP, TCP/UDP o HTTP/FTP, así como una amplia variedad de formatos de audio y vídeo.

La interfaz está compuesta de distintas partes: la barra de menús, el control deslizante de tiempo, la botonera habitual de reproducción junto con otros con funciones especiales y el control del volumen, y en la parte inferior se muestra información de estado, como la velocidad de reproducción, el tiempo transcurrido de la reproducción, así como el restante. En la barra de menús se encuentran las siguientes opciones principales:

- **Medio**: permite elegir el medio de reproducción a utilizar (archivo almacenado localmente o en red, dvd, cd, etc.), e incluso seleccionar los dispositivos de captura (cámara y micrófono) para un emisión en directo. La opción "Abrir volcado de red" nos permite indicar una URL para acceder al archivo remoto o emisión en directo a reproducir (véase Figura 10.6).
- **Reproducción**: nos da prácticamente las mismas posibilidades que la botonera de reproducción, además de la gestión de favoritos, así como distintas operaciones a la hora de reproducción de DVD, como seleccionar un capítulo determinado.
- **Audio**: elegimos la pista de audio a reproducir, en mono o estéreo, podemos utilizar un efecto de visualización al reproducir el audio así como manipular su volumen.
- **Vídeo**: podemos establecer diversos aspectos relacionados con el vídeo que estamos reproduciendo, como elegir la pista de vídeo o de subtítulos, si queremos visualizar la reproducción a pantalla completa, realizar una captura de pantalla o establecer diversos tamaños y proporciones para la reproducción en curso.
- **Herramientas**: permite entre otras cosas utilizar distintos filtros y efectos durante la reproducción multimedia, permite establecer la velocidad de los subtítulos en referencia al vídeo, así como establecer las preferencias de distintos aspectos configuración como del audio o vídeo.
- **Ver**: permite establecer diversas opciones de visualización relativas a la interfaz, como por ejemplo poder mostrar una lista de reproducción, ver la reproducción a pantalla completa o personalizar la interfaz con los botones que deseamos.
- **Ayuda**: nos proporciona ayuda proporcionándonos distintos enlaces, buscar actualizaciones del software, así como mostrarnos la versión que tenemos instalada.

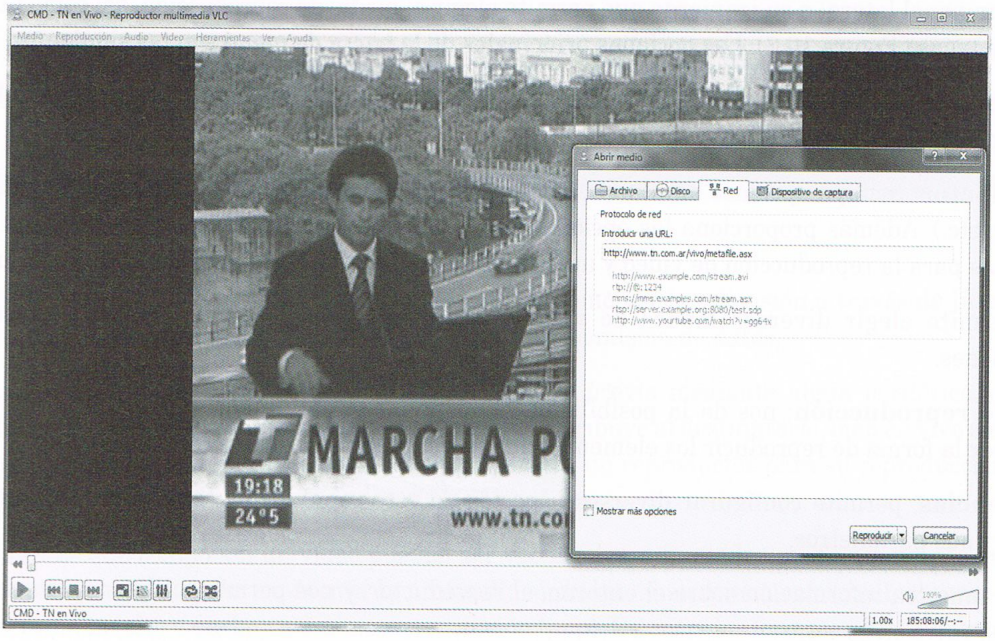


Figura 10.6. *Apertura de URL con el reproductor VLC. La opción "Volcado de red" permite el acceso a una URL como la indicada en esta figura, correspondiente al canal argentino Todo Noticias o TN*

10.7.2 CONFIGURACIÓN EN GNU/LINUX

En GNU/Linux disponemos de lo que se conoce como motor de reproducción de contenido multimedia, tal es el caso de Xine o GStreamer. Estos proporcionan sobre todo una biblioteca para que pueda ser utilizada por distintos reproductores. En GNU/Linux encontramos diversos reproductores de vídeo, cada uno con unas características que lo hacen más adecuado y recomendable para cierto tipo de reproducciones. Los reproductores también pueden ser de carácter ligero como Totem, necesitando pocos recursos para su ejecución, aunque no por eso dejan de cumplir su función correctamente. Otros disponen de unas opciones de configuración y complementos que los hacen más completos como Banshee, tratado en el capítulo anterior. Aunque tal vez el más conocido y utilizado sea MPlayer, en este apartado trataremos el reproductor Kaffeine para entornos KDE, cuyas características principales son las siguientes:

- ✓ Utiliza la biblioteca del motor de reproducción Xine, aunque puede utilizar la de GStreamer.
- ✓ Reproduce distintos formatos de soporte físico como CD, DVD y Vídeo CD.
- ✓ También soporta los formatos más comunes de vídeo como AVI, MPEG, MOV o WMV, así como de audio, como por ejemplo AAC o MP3.
- ✓ Tiene la posibilidad de utilizar streaming mediante los protocolos HTTP, TCP, UTP, MMS, RTSP o RTP.
- ✓ Permite la reproducción de películas con subtítulos en formato ".srt".
- ✓ Puede utilizarse mediante el navegador web Konqueror y mediante un *plugin* con Mozilla Firefox.

Dispone de una interfaz muy sencilla de utilizar y cuyos elementos básicos son: la barra de menús, la botonera de reproducción, un control para el volumen, información sobre el tiempo de reproducción junto con un elemento

desplazador y un panel lateral a su izquierda que permite elegir el medio de reproducción, así como utilizar una lista de reproducción (véase Figura 10.7). Las opciones principales de la barra de menú son las siguientes:

- **Archivo**: permite elegir el medio de reproducción a utilizar, pudiendo utilizarse una URL para la reproducción desde un servidor de streaming.
- **Reproductor**: incluye opciones similares a la botonera de reproducción (iniciar, parar, pausar, siguiente, anterior, etc.). Además proporciona las opciones necesarias para la reproducción de DVD, así como opciones exclusivas para la reproducción de vídeo y audio y aquellas relativas a la utilización de subtítulos.
- **Ver**: permite elegir diversos modos de visualizar la reproducción en curso así como establecer sus proporciones.
- **Lista de reproducción**: nos da la posibilidad de gestionar (crear, importar, etc.) listas de reproducción y establecer la forma de reproducir los elementos que la integran (aleatoria o repetitiva).
- **Preferencias**: permite configurar diversos aspectos de este reproductor como el motor de reproducción a utilizar y sus parámetros.
- **Ayuda**: muestra información sobre el entorno, el reproductor, y nos permite utilizar un manual sobre dicho software, entre otras cosas.

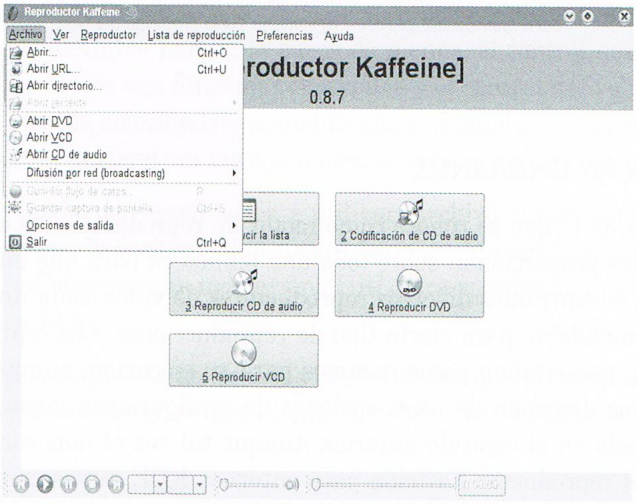


Figura 10.7. *Reproductor KDE Kaffeine. Apreciamos los distintos elementos de dicho reproductor (menú, botonera, tiempos de reproducción, barra de desplazamiento), como el menú "Archivo" que nos permite abrir distintos medios de reproducción, entre ellos una URL*

RESUMEN DEL CAPÍTULO

El servicio de vídeo hace posible demandas de usuario como ver la televisión a través de Internet, y a pesar de ser una red que en principio solo se pensó para transmisión de datos.

Para la transmisión de vídeo es necesaria una captura previa mediante algún periférico, como por ejemplo una webcam. El vídeo digitalizado se codifica y se distribuye al destinatario, bien en vivo o mediante grabaciones para posterior reproducción. El cliente utilizará un reproductor para su reproducción, siendo necesario tener el mismo codec instalado con el que se codificó.

Las imágenes que componen un vídeo pueden ser vectoriales, o formadas mediante mapas de bits, en las cuales tendremos que tener en cuenta la profundidad de bit, si se utiliza color real, el modo de color utilizado, el tamaño (alto y ancho), así como su resolución (ppp). De entre los formatos de archivos relativos a mapa de bits, destacar BMP, GIF, JPG o JPEG, TIF o TIFF, PNG, PSD, XCF y PICT.

El vídeo se compone de fotogramas, cuyos parámetros más representativos son los fotogramas por segundo, la resolución y el *bitrate*.

Los formatos de vídeo representan la forma de almacenarlos, destacando los formatos contendores, que permiten codificar el audio y el vídeo en formatos independientes además de almacenar otro tipo de información, y todo bajo un formato definido. De entre los formatos más utilizados destacar MPEG, AVI, ASF, WMV, MKV, Quicktime, RealV Video, Flash Video, Ogg u Ogv y DV.

Para la codificación del vídeo se pueden utilizar técnicas de compresión espacial o temporal, siendo los codecs más utilizados el WMV, MPEG, DivX, Xvid o DV.

Una forma de interactuar con el vídeo y el audio es mediante la videoconferencia, que necesita los periféricos necesarios para la captura de audio y vídeo para una comunicación bidireccional. Es importante utilizar el codec y la resolución apropiada para poder mantener reuniones a distancia, impartir cursos, etc. Se puede utilizar entre dos equipos distantes en formato uno a uno, uno con un grupo o grupo con grupo, siendo diferente la calidad de los periféricos y recursos necesarios para cada uno de ellos. También se puede utilizar entre varios equipos distantes, donde la gestión de la conversación puede realizarse a través de una MCU (centralizada), o gestionando solo la información de control mediante la MCU (descentralizada).

El estándar H.323 es el más conocido para esta tecnología, que puede utilizarse mediante herramientas instalables como Ekiga, así como aplicaciones orientadas a la tecnología Web 2.0 para conversar a través de nuestro navegador, como por ejemplo *Dimdim*, que además de conversar mediante webcam y micrófono, permite mantener conversaciones escritas, compartir nuestro escritorio, una parte de él o una aplicación, así como utilizar una pizarra virtual.

Microsoft dispone de las herramientas *Media Encoder* y *Expression Encoder* para la codificación multimedia, además del servicio *Media Services* para su distribución. En GNU/Linux podemos utilizar el software desarrollado por Cisco *Darwin Streaming Server* para la difusión multimedia, utilizando la herramienta que incluye *mp4live* para la codificación del audio y vídeo.

Uno de los reproductores de vídeo y audio multiplataforma más utilizado actualmente es VLC, que incluso puede ejercer de servidor de streaming. A pesar de ser tal vez MPlayer el reproductor más conocido en el mundo Linux, Kaffeine es una de las alternativas interesantes que puede utilizar un motor de reproducción Xine o GStreamer.

También podemos utilizar equipos especializados o adaptados para la reproducción de contenido multimedia desde fuentes distintas, conocidos como Media Center. Para adaptar un equipo podemos instalar software sobre el sistema operativo como Moovida, aunque otros como Windows 7 ya disponen del software necesario.

EJERCICIOS PROPUESTOS

- **1.** Indica el *bitrate* que deberíamos utilizar para codificar una secuencia multimedia de una hora de duración en un CD de 800 Mb.
- **2.** Indica los pasos a realizar para llevar a cabo la configuración de los ejemplos 10.1 y 10.2 sobre el mismo servidor.
- **3.** Descarga e instala el reproductor VLC para acceder al servidor de streaming del ejercicio anterior.
- **4.** Descarga e instala la aplicación de Apple Real Player y accede al servidor de streaming del ejemplo 10.3 para reproducir la emisión en directo.
- **5.** ¿Es posible la instalación del reproductor GNU/Linux Kaffeine y el software de streaming Darwin Streaming Server en un mismo equipo? Razona tu respuesta.
- **6.** Lleva a cabo la instalación y posterior configuración para implementar el ejemplo 10.3.
- **7.** Crea una cuenta con Dimdim para poder compartir tu escritorio con un compañero o amigo que también disponga de cuenta.

TEST DE CONOCIMIENTOS

1 La profundidad de una imagen indica:
- a) El número de píxeles que la componen.
- b) Los bits utilizados para codificar el color de los píxeles.
- c) La resolución que se le ha dado.
- d) Los bits de fondo que tiene.

2 El *framerate* utilizado:
- a) Indica los bits necesarios para codificar una imagen en movimiento.
- b) Cuanto mayor sea menor será la calidad de la secuencia multimedia.
- c) Indica los fotogramas que se muestran cada segundo.
- d) Es el número de bits utilizados para el tránsito de una imagen a otra.

3 Un formato contenedor:
- a) Indica la manera de almacenar información diversa además de vídeo y audio.
- b) Define un único formato donde se codifica simultáneamente audio y vídeo.
- c) Codifica de forma independiente el audio y el vídeo.
- d) a y c son correctas.

4 MPEG:
- a) Codifica el contenido multimedia mediante compresión espacial.
- b) Ninguna de sus variantes puede utilizarse para videoconferencia.
- c) Define como codificar y comprimir el audio y el vídeo.
- d) Solo emplea codecs definidos en dicho estándar como MPEG-4.

5 La compresión de redundancia temporal:
- a) Comprime cada fotograma por separado en cada unidad de tiempo.
- b) Comprime las diferencias entre fotogramas.
- c) Tiene muy buena calidad y requiere gran espacio para almacenarse.
- d) Es utilizado por MPEG y AVI para obtener ficheros de alta calidad.

6 En una conferencia multipunto centralizada:
- a) Los interlocutores se envían la información mediante multicast.
- b) Los equipos conversan a través de un MCU.
- c) La información de control es centralizada mientras que el flujo multimedia no.
- d) Ninguna de las anteriores.

7 La herramienta web Dimdim:
- a) Permite tres formas de compartir el escritorio o una parte de él.
- b) Permite establecer videoconferencias pero no compartir el escritorio.
- c) Además de videoconferencia solo permite utilizar una pizarra virtual.
- d) Ninguna de las anteriores.

8 El software de Microsoft Windows Media Encoder:
- a) No se pueden ejecutar simultáneamente en la misma máquina junto con Windows Media Server.
- b) Requiere que además instalemos un servicio específico para su funcionamiento.
- c) Tan solo distribuye el flujo de vídeo entre los clientes que lo solicitan.
- d) Ninguna de las anteriores.

9 Darwin Streaming Server:
- a) Incluye la herramienta *mp4live* para la codificación del vídeo.
- b) Es software de codificación de vídeo capturado con una cámara.
- c) Pretende ser un estándar de Internet para transmisiones audiovisuales.
- d) Utiliza el vídeo codificado para proporcionarlo a los clientes.

11 Otros servicios

OBJETIVOS DEL CAPÍTULO

- ✓ Describir los servicios de noticias y listas de distribución.
- ✓ Instalar y configurar los servicios de noticias y listas de distribución.
- ✓ Determinar el tipo de lista y los modos de acceso permitidos.
- ✓ Crear cuentas de usuario y verificar el acceso a los servicios de noticias y listas de distribución.
- ✓ Describir el funcionamiento de los servicios horarios.
- ✓ Instalar y configurar los servicios horarios.
- ✓ Elaborar documentación relativa a la instalación, configuración y recomendaciones de uso de los servicios horarios, de noticias y listas de distribución.

En los capítulos 6 y 7 de este libro se explica con detalle el funcionamiento del sistema de correo electrónico, en el que los usuarios pueden enviar mensajes con datos adjuntos utilizando las direcciones con el formato *usuario@dominio*. En este capítulo se explica con detalle el funcionamiento de las **listas de distribución de correo electrónico** que, funcionando conjuntamente con el correo electrónico, permiten aumentar las características de este sistema de mensajería y ofrecer servicios de difusión de información y noticias.

En muchas ocasiones puede ser necesario disponer de un mecanismo que sincronice todos los equipos de la red con la misma hora. Este mecanismo de sincronización, si funciona de una manera automática, permite a los administradores de la red darse un pequeño respiro ya que no tienen que andar de un lado para otro actualizando fechas y horas en todos los equipos de la red. En este capítulo también se explica el funcionamiento del servicio horario NTP.

11.1 LISTAS DE DISTRIBUCIÓN DE CORREO

Las **listas de correo** o **listas de distribución** están diseñadas para el envío masivo de mensajes a una gran cantidad de usuarios. Esta función ya está disponible en el sistema de correo electrónico convencional, ya que un usuario puede especificar varias direcciones de destino. Sin embargo, en una lista de correo electrónico se pueden especificar millones de usuarios destinatarios. Además, para que no se produzcan prácticas abusivas, son los mismos usuarios los que se registran en esas listas si desean recibir los mensajes y pueden darse de baja en cualquier momento.

11.1.1 INTRODUCCIÓN

Una lista de correo se define a través de una dirección de correo electrónico con el formato convencional *usuario@dominio*. Las personas que desean recibir correo de esa lista se inscriben en ella especificando su dirección de correo electrónico particular. A partir de ese momento, cualquier usuario que envíe un mensaje a la dirección de la lista, será redirigido a todas las direcciones de los usuarios que se han registrado en ella. El registro de los usuarios en la lista de distribución puede ser libre o también puede estar controlado por un administrador, encargado de aprobar o rechazar las solicitudes que llegan.

Para que el mecanismo de listas de distribución funcione correctamente, es necesario disponer de un servidor de correo electrónico (véase el capítulo 7 de este libro), además de un programa de gestión de listas de correo. Además, las listas de distribución también deben reconocer una serie de comandos para que los usuarios puedan cambiar sus opciones de suscripción o darse de baja. Estos comandos son enviados directamente a la dirección de la lista, a otra dirección habilitada al efecto o pueden ser accesibles a través de una página web.

Hay que tener en cuenta que, si bien la instalación y configuración de un servicio de listas de distribución de correo en sí mismo no resulta excesivamente compleja, sí que puede ser problemática por la gran cantidad de servicios de los que depende. Para que un servidor de listas de distribución funcione correctamente, es necesario que los servicios de red, DNS, agente de transporte de correo (SMTP) y agente de usuario de correo funcionen en perfecta coordinación.

Actualmente existen muchos programas de gestión de listas que se distribuyen libremente o con licencia. Ejemplos de estos programas son LISTSERV, Mailman, phpList, Microsoft Exchange Server, etc. En Internet también están disponibles muchos servicios de listas de distribución, como Google Groups, Yahoo! Groups o eListas.

En los apartados 11.1.2 y 11.1.3 se explica cómo instalar y configurar un servidor de listas de distribución en los sistemas operativos Microsoft Windows y GNU/Linux.

11.1.1.1 Tipos de listas de distribución

El servicio de listas de correo puede se de varios tipos, dependiendo de la forma en la que funcione:

- **Boletín de noticias** (*newsletter*): solamente un grupo de usuarios privilegiados puede escribir mensajes en esa lista, que después son distribuidos al resto. Se trata de un sistema que permite la difusión de noticias o cualquier otro tipo de información, ya sea de carácter general o de índole comercial.
- **Lista de discusión**: también llamada lista de debate, se trata de un mecanismo empleado para realizar discusiones sobre determinados temas o simplemente intercambiar información. Para ello, cualquier usuario registrado en la lista puede enviar mensajes a ella, que son recibidos por el resto de usuarios que forman parte de ella. A su vez, estos usuarios pueden enviar sus propios mensajes o contestar a aquellos que han recibido y estos vuelven a ser enviados a todos los miembros. Este mecanismo de intercambio de mensajes es muy parecido al utilizado en los foros, donde cada ususario puede dejar un mensaje que luego puede ser consultado o contestado por el resto.

A su vez, los miembros de una lista de correo pueden recibir los mensajes de varias formas, lo que permite llevar a cabo un mayor control para evitar que se saturen los buzones de correo de los usuarios:

- **Modo normal**: cada usuario recibe todos los mensajes que llegan a la lista de distribución.
- **Modo resumen**: cada usuario recibe un único mensaje que contiene, a su vez, todos los mensajes que llegan a la lista en el día.
- **Modo de correo web**: los usuarios no reciben los mensajes que llegan a la lista, pero pueden consultarlos a través de una página web.

11.1.1.2 Reglas de participación

En cualquier debate televisivo o radiofónico se establecen una serie de **normas** que los interlocutores deben respetar para que la comunicación se desarrolle con fluidez y sin contratiempos. Estas normas tienen que ver con el respeto al turno de palabra, centrarse en el tema tratado, respetar la opinión de los demás, no insultar, etc. Normas de este tipo también deben ser aplicadas en las listas de distribución de correo o, de lo contrario, nos podemos encontrar con situaciones no deseadas. A estas normas también se las conoce como **reglas de etiqueta**.

En general, en un sistema de gestión de listas de distribución de correo se suelen establecer las siguientes normas, que deben respetar todos los participantes:

- Tratar a todos los participantes con respeto, sin despreciar sus opiniones.
- No utilizar la lista de distribución con fines publicitarios o lucrativos.
- Seguir la temática de la lista, evitando tratar asuntos irrelevantes o que no tienen nada que ver. Algunas listas permiten esto, pero obligan a que los usuarios identifiquen este tipo de mensajes como "fuera de contexto", "off-topic" u "OT".
- No enviar archivos adjuntos que superen un tamaño máximo, para evitar que se pueda saturar el servidor o hacer más lentas las comunicaciones.
- Evitar que las direcciones de correo de los participantes sean visibles en los mensajes. Esto impide que estas direcciones puedan ser utilizadas por otras personas para el envío de correo basura.

Habitualmente, los sistemas de gestión de listas de distribución de correo utilizan procesos automáticos que se encargan de verificar que todos los mensajes cumplen con las normas de participación. Si se detecta que alguno de

estos mensajes no cumple alguna norma, entonces éste es automáticamente eliminado para evitar que sea difundido a los miembros de la lista. En algunos casos, esta tarea es perfectamente automatizable cuando el sistema es capaz de detectar determinados patrones en los mensajes enviados (por ejemplo, insultos, palabras malsonantes, símbolos o caracteres especiales, como "@", etc.).

En otras situaciones, puede no ser posible que el sistema compruebe automáticamente si los mensajes cumplen con las normas de participación, por ejemplo, cuando se quiere determinar si contienen información relacionada con el tema a tratar. En esos casos, puede ser necesaria la intervención de una persona que se encargue de comprobar el contenido de cada uno de los mensajes enviados a la lista, antes de que sean reenviados a los miembros. A esta persona se la conoce como **moderador**, que es un usuario privilegiado que puede eliminar aquellos mensajes que no cumplen con las normas de participación.

11.1.2 INSTALACIÓN Y CONFIGURACIÓN EN MICROSOFT WINDOWS

Como se explica en el capítulo 7, en los sistemas Microsoft Windows se puede utilizar Microsoft Exchange Server, un paquete que convierte a un equipo en un potente servidor de correo electrónico. Microsoft Exchange Server se distribuye de forma independiente de cualquier otro producto de Microsoft por lo que, para poder utilizarlo, es necesario adquirir las correspondientes licencias de uso.

Microsoft Exchange Server ofrece mecanismos para manejar listas de distribución de correo, que en el contexto de este programa se denominan **grupos de distribución**. En Exchange Server 2007 se pueden crear dos tipos de grupos:

- **Grupos de distribución**: se utilizan única y exclusivamente para la distribución de mensajes de correo electrónico. Estos grupos son las listas de distribución de las que se habla en este capítulo.
- **Grupos de seguridad**: se trata de grupos definidos en el Directorio Activo de la red Microsoft. Se utilizan fundamentalmente para establecer o denegar permisos de acceso a los recursos disponibles en la red. Si estos grupos tienen el correo habilitado, entonces también pueden distribuir los mensajes de correo a todos sus miembros (usuarios).

A su vez, los grupos de distribución que se pueden definir en Exchange Server 2007 son los siguientes:

- **Grupos de distribución estáticos**: las direcciones de correo de los usuarios que pertenecen a ellos se establecen de antemano, es decir, se define una lista de direcciones a la que se le puede agregar o eliminar miembros.
- **Grupos de distribución dinámicos**: las direcciones de correo de los usuarios que pertenecen a ellos no se especifican, sino que se indican en base a determinadas reglas. Si un usuario cumple con estas reglas, entonces será considerado miembro del grupo. En caso contrario no será considerado miembro del grupo y, por lo tanto, no recibirá los mensajes de ese grupo de distribución. A estos grupos se les denominan **grupos de distribución basados en consultas** en Exchange Server 2003.

Para poder utilizar los grupos de seguridad y grupos de distribución en Microsoft Exchange Server es necesario que esta herramienta se encuentre pertectamente instalada y configurada en el equipo. En el apartado 7.1.2 del capítulo 7 se explica con detalle cómo instalar y configurar Exchange Server 2007.

La gestión de las listas o grupos de distribución en Exchange Server 2007 se realiza a través de la Consola de administración de Exchange, que está disponible en el menú de inicio. Una vez en ella, seleccionados "Microsoft Exchange | | Configuración de destinatarios | | Grupo de distribución" en el árbol de objetos de la parte izquierda de la ventana. Esto nos mostrará una lista con los grupos de distribución o grupos de seguridad con correo habilitado que ya existen en el sistema (véase la Figura 11.1).

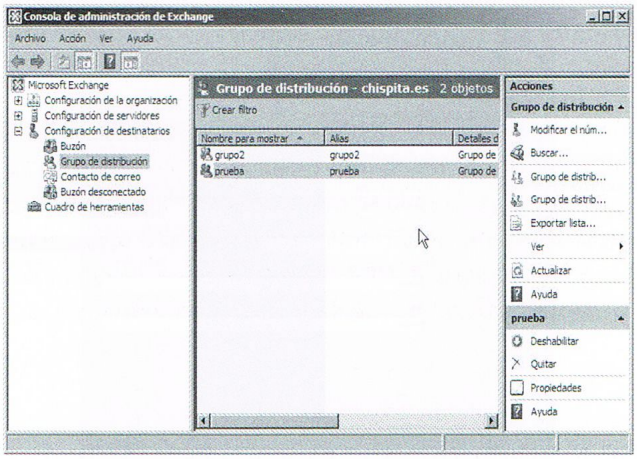


Figura 11.1. *Ventana principal de gestión de grupos de distribución y seguridad en Exchange Server 2007. Desde esta ventana se pueden realizar todas las operaciones necesarias, como creación o eliminación de grupos, cambios en sus propiedades, etc.*

11.1.2.1 Gestión de grupos de distribución

Para crear un nuevo grupo de distribución en Exchange Server 2007 hay que seguir estos pasos:

1 Acceder a la consola de administración de Exchange seleccionando "Inicio || Todos los programas || Microsoft Exchange Server 2007 || Consola de administración de Exchange" (véase el apartado 7.1.2.3).

2 En el árbol de objetos de la parte izquierda de la ventana que aparece, desplegar los elementos "Microsoft Exchange || Configuración de destinatarios" y selecciona "Grupo de distribución". Esto mostrará una ventana como la de la Figura 11.1.

3 Seleccionar "Acción || Grupo de distribución nuevo..." del menú principal o la opción "Grupo de distribución nuevo..." si se pulsa con el botón derecho del ratón sobre el elemento "Grupo de distribución". Esto mostrará una ventana como la de la Figura 11.2.

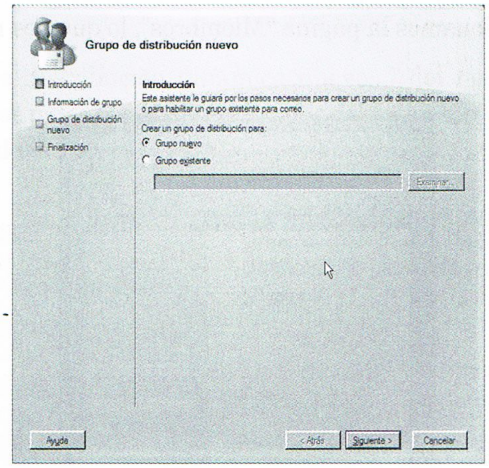


Figura 11.2. *Asistente para la creación de un nuevo grupo de distribución en Exchange Server 2007. Aquí se especifica si se va a crear un nuevo grupo o se va a habilitar un grupo existente*

4 En la ventana que aparece (Figura 11.2) seleccionaremos la opción "Grupo nuevo" y pulsaremos el botón "Siguiente". Esto mostrará una ventana como la de la Figura 11.3.

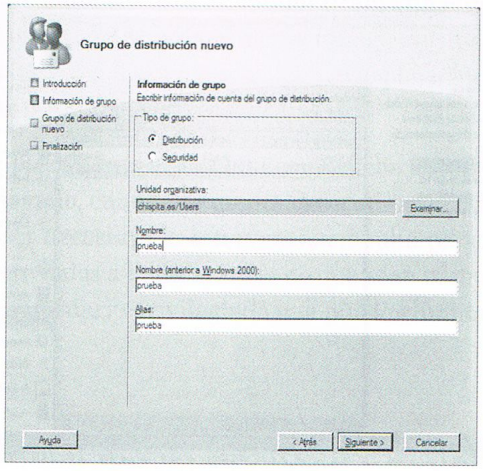


Figura 11.3. *Segunda ventana del asistente para la creación de un nuevo grupo de distribución en Exchange Server 2007. En ella se indica el tipo de grupo que se va a crear y el nombre que lo va a identificar*

5 En la ventana de la Figura 11.3 marcamos el botón de opción "Distribución" y especificamos el nombre del grupo en el cuadro de texto correspondiente. A continuación, pulsamos en el botón "Siguiente".

6 En la nueva ventana que aparece, se muestra un resumen con las opciones que hemos especificado para crear el grupo. Si pulsamos en el botón "Nuevo", nos creará el grupo (aparecerá una nueva ventana indicándonoslo). A partir de ese momento, ya podremos utilizar el grupo creado para distribuir mensajes de correo electrónico.

Para añadir direcciones de correo a un grupo de distribución hay que seguir estos pasos:

1 En la ventana principal de la Consola de administración de Exchange, desplegamos los elementos "Microsoft Exchange | | Configuración de destinatarios" y seleccionamos "Grupo de distribución". Esto mostrará una ventana central con los grupos definidos (véase la Figura 11.1).

2 Seleccionamos el grupo de distribución al que queremos añadir direcciones de correo, pulsamos con el botón derecho del ratón sobre él y seleccionamos la opción "Propiedades".

3 En la ventana que aparece, seleccionamos la página "Miembros", lo que nos mostrará la información de la Figura 11.4.

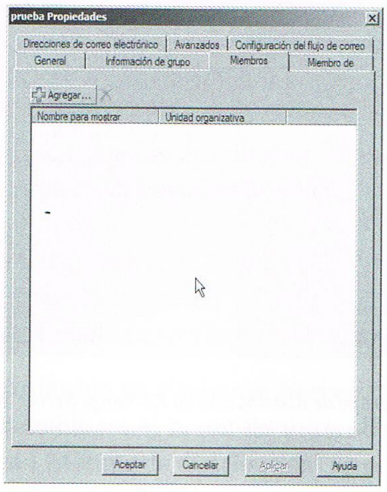


Figura 11.4. *Miembros de un grupo de distribución en Exchange Server 2007. Aquí se muestran los usuarios que recibirán los mensajes de esta lista de distribución*

4 Ahora, pulsamos el botón "Agregar...", lo que nos mostrará una ventana para seleccionar el usuario que deseamos añadir (Figura 11.5). Una vez seleccionado el usuario o usuarios que nos interesen, pulsamos el botón "Aceptar" para añadirlos al grupo.

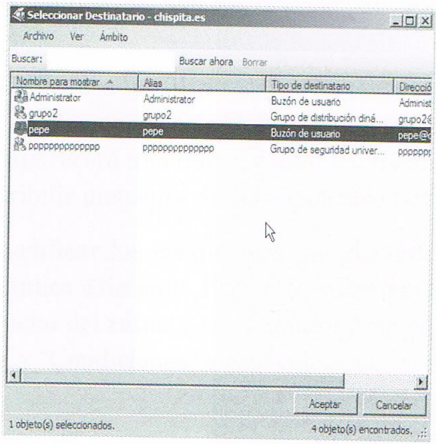


Figura 11.5. *Añadir un usuario a una lista de distribución en Exchange Server 2007. Aquí se muestra una lista de los usuarios definidos en el dominio de la red Microsoft, cuyas direcciones de correo pueden ser añadidas al grupo*

Los pasos indicados anteriormente se utilizan para añadir la cuenta de correo de un usuario definido en el dominio de la red Microsoft. También es posible añadir directamente una dirección de correo electrónico al grupo de distribución, aunque esta dirección pertenezca a un usuario que no esta registrado en el dominio. Para ello, hay que seguir los mismos pasos, pero en este caso a través de la pestaña "Direcciones de correo electrónico" de la ventana de propiedades del grupo (Figura 11.4).

11.1.2.2 Gestión de grupos de distribución dinámicos

Para crear un nuevo grupo de distribución dinámico en Exchange Server 2007 hay que seguir estos pasos:

1 Acceder a la consola de administración de Exchange seleccionando "Inicio || Todos los programas || Microsoft Exchange Server 2007 || Consola de administración de Exchange" (véase el apartado 7.1.2.3).

2 En el árbol de objetos de la parte izquierda de la ventana que aparece, desplegar los elementos "Microsoft Exchange || Configuración de destinatarios" y selecciona "Grupo de distribución". Esto mostrará una ventana como la de la Figura 11.1.

3 Seleccionar "Acción || Grupo de distribución dinámica nuevo..." del menú principal o la opción "Grupo de distribución dinámica nuevo..." si se pulsa con el botón derecho del ratón sobre el elemento "Grupo de distribución". Esto mostrará una ventana como la de la Figura 11.6.

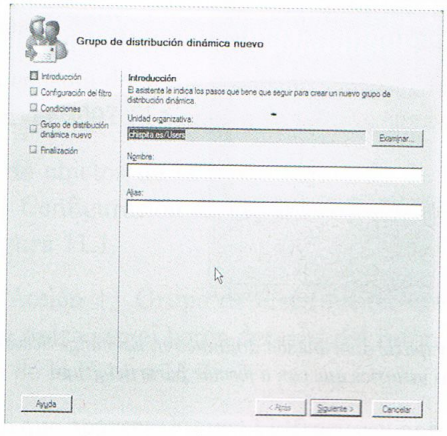


Figura 11.6. *Asistente para la creación de un nuevo grupo de distribución dinámico en Exchange Server 2007. Aquí se indica el nombre que va a identificar al grupo*

4 En la ventana de la Figura 11.6 especificamos el nombre del grupo en el cuadro de texto correspondiente. A continuación, pulsamos en el botón "Siguiente", lo que nos mostrará una ventana como la de la Figura 11.7.

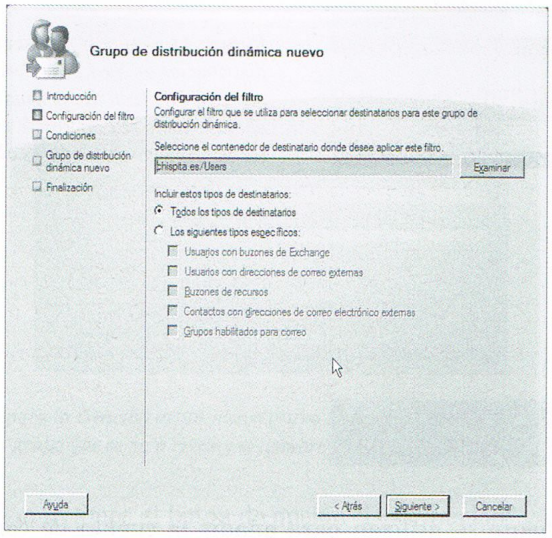


Figura 11.7. *Segunda ventana del asistente para la creación de un nuevo grupo de distribución dinámico en Exchange Server 2007. En ella se especifican los miembros que van a formar parte de él*

5 En la ventana que aparece (Figura 11.7) se especifican los miembros que van a pertenecer a este grupo. Si se marca el botón de opción "Todos los tipos de destinatarios" se entenderá que a este grupo pertenecerán todos los usuarios del sistema. Sin embargo, si se marca el botón de opción "Los siguientes tipos específicos" solo pertenecerán a este grupo aquellos usuarios que cumplan las reglas de las casillas de verificación que se marquen.

6 Una vez seleccionados los tipos de usuarios, pulsamos en el botón "Siguiente", lo que nos mostrará una ventana como la de la Figura 11.8.

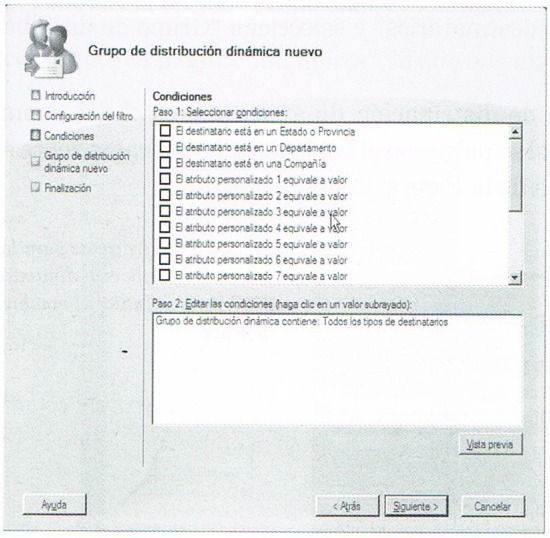


Figura 11.8. *Tercera ventana del asistente para la creación de un nuevo grupo de distribución dinámico en Exchange Server 2007. En ella se especifican filtros más restrictivos que especifican los usuarios que van a formar parte del grupo*

7 En la ventana de la Figura 11.8 se especifican filtros más restrictivos para los usuarios que van a formar parte de este grupo. Estos filtros pueden seleccionar usuarios deacuerdo con algunos de sus atributos, como su nombre, departamento al que pertenece, etc. Si se pulsa en el botón "Vista previa" se mostrará una lista con los usuarios que cumplen las condiciones que hemos especificado, es decir, los que van a formar parte del grupo de distribución dinámico.

8 Una vez especificados los filtros, se pulsa en el botón "Siguiente". En la nueva ventana que aparece, se muestra un resumen con las opciones que hemos especificado para crear el grupo. Si pulsamos en el botón "Nuevo", nos creará el grupo (aparecerá una nueva ventana indicándonoslo). A partir de ese momento, ya podremos utilizar el grupo creado para distribuir mensajes de correo electrónico.

Es posible modificar las condiciones que deben cumplirse para que los usuarios formen parte de un grupo de distribución dinámico existente. Para ello, solamente tenemos que seleccionar el grupo en cuestión, pulsar sobre él con el botón derecho del ratón y seleccionar "Propiedades". En la ventana que aparece, tenemos que seleccionar las pestañas "Filtro" y "Condiciones" y especificar las condiciones que nos interesen.

11.1.2.3 Gestión de grupos de seguridad

Los grupos de seguridad se utilizan ampliamente en los sistemas Microsoft Windows para definir una serie de usuarios a los que se les van a conceder un conjunto de privilegios sobre operaciones que se realizan en el mismo equipo o en otros que están accesibles a través de la red. Además, si estos tienen habilitada una cuenta de correo electrónico, pueden ser utilizados para distribuir mensajes entre los usuarios que forman parte de él, como si se tratase de una lista de distribución.

Para crear un grupo de seguridad con correo habilitado podemos hacerlo de dos formas distintas:

- Creando el grupo a través de las herramientas disponibles en el Directorio Activo y después habilitar la transferencia de correo en Microsoft Exchange Server. En primer lugar, es necesario crear la cuenta de grupo usando la herramienta "Usuarios y equipos de Active Directory" que está disponible en la opción "Herramientas administrativas" del menú de inicio. Después, hay que abrir la Consola de administración de Exchange para habiliar el correo de esa cuenta de grupo. Esta forma de trabajar será más utilizada por aquellos administradores que estén más acostumbrados a trabajar con el Directorio Activo de la red de Microsoft.
- Creando el grupo y habilitando el transporte de correo, todo ello desde Microsoft Exchange Server. Esta opción permite realizar todos los pasos directamente desde la Consola de administración de Exchange, sin necesidad de utilizar otras herramientas.

Para crear un grupo de seguridad con correo habiliado desde la Consola de administración de Exchange hay que seguir estos pasos:

1 Acceder a la consola de administración de Exchange seleccionando "Inicio || Todos los programas || Microsoft Exchange Server 2007 || Consola de administración de Exchange" (véase el apartado 7.1.2.3).

2 En el árbol de objetos de la parte izquierda de la ventana que aparece, desplegar los elementos "Microsoft Exchange || Configuración de destinatarios" y selecciona "Grupo de distribución". Esto mostrará una ventana como la de la Figura 11.1.

3 Seleccionar "Acción || Grupo de distribución nuevo..." del menú principal o la opción "Grupo de distribución nuevo..." si se pulsa con el botón derecho del ratón sobre el elemento "Grupo de distribución". Esto mostrará una ventana como la de la Figura 11.2.

4 En la ventana que aparece (Figura 11.2) seleccionaremos la opción "Grupo nuevo" y pulsaremos el botón "Siguiente". Esto mostrará una ventana como la de la Figura 11.3.

5 En la ventana de la Figura 11.3 marcamos el botón de opción "Seguridad" y especificamos el nombre del grupo en el cuadro de texto correspondiente. A continuación, pulsamos en el botón "Siguiente".

6 En la nueva ventana que aparece, se muestra un resumen con las opciones que hemos especificado para crear el grupo. Si pulsamos en el botón "Nuevo", nos creará el grupo (aparecerá una nueva ventana indicándonoslo). A partir de ese momento ya podremos utilizar el grupo creado para distribuir mensajes de correo electrónico.

Para añadir direcciones de correo a un grupo de distribución hay que seguir los mismos pasos indicados en el apartado 11.1.2.1, pero esta vez tenemos que seleccionar el grupo de seguridad que nos interese. Al igual que ocurre con los grupos de distribución, en los grupos de seguridad se pueden añadir cuentas de usuario definidas en el Directorio Activo. También es posible añadir directamente una dirección de correo electrónico al grupo de seguridad, aunque esta dirección pertenezca a un usuario que no esta registrado en el dominio. Para ello, hay que utilizar la pestaña "Direcciones de correo electrónico" de la ventana de propiedades del grupo (Figura 11.4).

11.1.3 INSTALACIÓN Y CONFIGURACIÓN EN GNU/LINUX

Si utilizamos sistemas GNU/Linux existen muchas posibilidades a la hora de elegir el gestor de listas de distribución a utilizar. Por simplicidad de uso, funcionalidad y compatibilidad con los sistemas de correo más utilizados, nos decantaremos por **Mailman**, que se distribuye bajo licencia GPL.

Las características más importantes de Mailman son las siguientes:

- ✓ Incluye una herramienta de administración web para realizar la mayoría de las tareas.
- ✓ Moderación, suscripción a listas abiertas y cerradas, listas cerradas de miembros, filtros aplicados a los mensajes, etc.
- ✓ Almacenamiento de los archivos enviados y gestión a través de una herramienta web.
- ✓ Detección de correo basura.
- ✓ Soporte para *hosts* virtuales (véase el capítulo 3).

11.1.3.1 Instalación y configuración del servidor

Los pasos genéricos para instalar Mailman en la mayoría de distribuciones GNU/Linux son los siguientes:

1 Comprobar que el servidor web Apache se encuentra instalado y funciona correctamente (véase el capítulo 3). Si no está instalado, se instalará con el paquete Mailman, ya que existe una dependencia entre ambos.

2 Comprobar que el servidor de correo *Sendmail* se encuentra instalado y funciona correctamente (véase el apartado 7.2).

3 Instalar el paquete con la herramienta correspondiente. Por ejemplo, en Debian 5 habrá que usar la siguiente orden:

```
# apt-get install mailman
```

4 Dependiendo de la versión de Mailman a instalar, es posible que aparezca una ventana donde se especifica el idioma que deseamos utilizar. También puede aparecer otra ventana advirtiendo que Mailman necesita generar una lista del sitio que permite el envío de recordatorios de contraseñas. Para crear esta lista hay que ejecutar esta orden:

```
# newlist mailman
```

5 Una vez hecho esto, procederemos a comprobar si los permisos establecidos sobre determinados archivos y carpetas del sistema son correctos. Para ello, ejecutamos la siguiente orden:

```
# ./check_perms
```

6 Si la orden anterior no muestra ningún mensaje de error, entonces significa que todo está correcto. En caso contrario, hay que ejecutar la siguiente orden para corregir los permisos:

```
# ./check_perms -f
```

7 Si la orden *check_perms* no funciona como se espera (se muestran errores y un mensaje que comienza con "Traceback"), consulte el apartado 11.1.3.3 donde se explica cómo solucionar este problema.

8 A continuación, es necesario configurar el servidor Apache para que los usuarios puedan consultar los mensajes. Es posible encontrar un ejemplo de archivo de configuración para Apache en la carpeta de instalación de Mailman (por ejemplo, en Debian 5 es */etc/mailman/apache.conf*). Lo que tenemos que añadir al archivo de configuración de Apache (en Debian 5 es */etc/apache2/sites-enabled/000-default*) es lo siguiente (hay que sustituir *<ruta1>*, *<ruta2>* y *<ruta3>* por las rutas correctas donde se haya instalado Mailman):

```
ScriptAlias /cgi-bin/mailman/  <ruta1>/cgi-bin/mailman/
Alias       /pipermail/        <ruta2>/archives/public/
Alias       /images/mailman/   <ruta3>/images/mailman/
<Directory <ruta1>/cgi-bin/mailman/>
    AllowOverride None
    Options ExecCGI
    AddHandler cgi-script .cgi
    Order allow,deny
    Allow from all
</Directory>
<Directory <ruta2>/archives/public/>
    Options Indexes FollowSymLinks
    AllowOverride None
    Order allow, deny
    Allow from all
</Directory>
<Directory <ruta3>/images/mailman/>
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
```

9 Si estamos utilizando Debian 5, tendremos que sustituir *<ruta1>* por */usr/lib*, *<ruta2>* por */var/lib/mailman* y *<ruta3>* por */usr/share*. Consulte el capítulo 3 de este libro y los archivos de configuración de ejemplo de Mailman para obtener más información sobre estas directivas del servidor Apache. Hay que tener en cuenta que el archivo de configuración de Mailman, llamado **mm_cfg.py** (en Debian 5 está ubicado en */etc/mailman*), debe estar en consonancia con los parámetros indicados en la configuración de Apache. Habitualmente, habrá que cambiar la dirección de correo para suscripciones y el nombre del servidor, por ejemplo:

```
DEFAULT_EMAIL_HOST='servidor.chispita.es'
DEFAULT_URL_HOST='servidor.chispita.es'
```

10 Una vez que se ha añadido esta información al archivo de configuración de Apache y Mailman, hay que reiniciar el proceso demonio del servidor Apache para que los cambios tengan efecto. En Debian 5 hay que ejecutar esta orden:

```
# apache2ctl restart
```

11 Se puede comprobar que las páginas web de administración de Mailman están disponibles si se accede a la dirección de suscripción (a las listas):

```
http://localhost/cgi-bin/mailman/listinfo/mailman
```

12 Seguidamente, es necesario configurar correctamente *Sendmail* para que sea capaz de interactuar con las listas de distribución definidas en Mailman. Para ello, seguiremos estos pasos:

1 Crear el archivo *mailman.aliases* con permisos de ejecución, dentro de la carpeta */usr/local/sbin*. Este archivo debe contener lo siguiente (las rutas a los archivos *aliases* y *newaliases* pueden ser diferentes):

```
/bin/cp /var/lib/mailman/data/aliases /etc/mailman.aliases
/usr/sbin/newaliases
```

2 Establecer los siguientes parámetros en el archivo de configuración *mm_cfg.py* de Mailman (le estamos indicando que use Postfix pero en realidad es para *Sendmail*):

```
MTA='Postfix'
POSTFIX_ALIAS_CMD='/usr/bin/sudo /usr/local/sbin/mailman.
aliases'
POSTFIX_STYLE_VIRTUAL_DOMAINS=[]
```

3 Ahora hay que indicar a *Sendmail* sobre el archivo que hemos creado. Para ello, accedemos al archivo de configuración de *Sendmail*, llamado *sendmail.mc* (véase el apartado 7.2.1), desde un editor o Webmin y buscamos esta línea:

```
define(`ALIAS_FILE',`/etc/aliases')dnl
```

4 La línea anterior la temenos que cambiar por esta otra:

```
define(`ALIAS_FILE',`/etc/aliases,/etc/mailman.aliases')
dnl
```

5 Ahora hay que compilar el archivo de configuración y reiniciar el proceso demonio de *Sendmail* para que los cambios tengan efecto (véase el apartado 7.2.1).

6 Seguidamente, necesitamos conceder permisos al usuario que ejecuta los procesos demonio Apache y Mailman para que puedan ejecutar el archivo que hemos creado en el paso 1. Supondremos que estos usuarios son *www-data* y *list*, que son los utilizados en Debian 5, aunque pueden cambiar en otras distribuciones o versiones. Para saber con qué cuentas de usuario se están ejecutando los procesos Apache y Mailman hay que consultar la información que aparece más a la izquierda cuando se ejecutan estas órdenes:

```
# ps -ef | grep apache2
# ps -ef | grep mailman
```

7 Para ello, editamos el archivo */etc/sudoers* y le añadimos estas líneas:

```
www-data ALL=NOPASSWD: /usr/local/sbin/mailman.aliases
list ALL=NOPASSWD: /usr/local/sbin/mailman.aliases
```

8 Ahona, ejecutamos lo siguiente (si el usuario con el que se ejecuta Mailman no es *list*, hay que sustituirlo por el que corresponda):

```
# su list
$ /usr/lib/mailman/bin/genaliases
```

9 Lo anterior debe haber creado dos archivos: *aliases* y *mailman.aliases*, ambos dentro de la carpeta */etc*.

10 Finalmente, reiniciamos el proceso demonio de Mailman para que todos los cambios tengan efecto.

13 Una vez que se ha completado la integración de Mailman con *Sendmail*, es necesario crear una lista especial, habitualmente denominada *mailman*, a través de la cual se envían los recordatorios de las contraseñas (en caso de que éstas hayan sido olvidadas por los usuarios). Además, esta lista de distribución también se utiliza para que Mailman funcione correctamente. Para crear esta lista, hay que especificar la siguiente URL, como se explica en el apartado 11.1.3.2 (si es que estamos utilizando el navegador en el equipo local):

```
http://localhost/cgi-bin/mailman/create
```

14 Seguidamente, tenemos que configurar el proceso demonio *cron* para que ciertas operaciones rutinarias que realiza Mailman se ejecuten en el equipo de forma periódica. Para ello, tenemos que ejecutar estas órdenes (el usuario *list* puede ser diferente y también la ubicación del archivo *crontab.in*):

```
# crontab -u list /usr/libmailman/cron/crontab.in
```

15 Finalmente, inciamos el proceso demonio Mailman. Si queremos que las listas de distribución estén disponibles cada vez que se arranque el equipo, deberemos configurar convenientemente los niveles de ejecución. En Debian 5 tendremos que ejecutar esta orden:

```
# /etc/init.d/mailman start
```

16 Ahora solo nos queda comporbar que todo funciona. En primer lugar, tenemos que verificar que podemos crear una lista de distribución. Esto lo podemos hacer ejecutando lo siguiente (nos pedirá el nombre de la lista de distribución, el correo electrónico del administrador de la lista y la contraseña):

```
# /usr/lib/mailman/bin/newlist
```

17 También podemos crear una nueva lista de distribución accediendo a esta página (véase la Figura 11.9):

```
http://localhost/cgi-bin/mailman/create
```

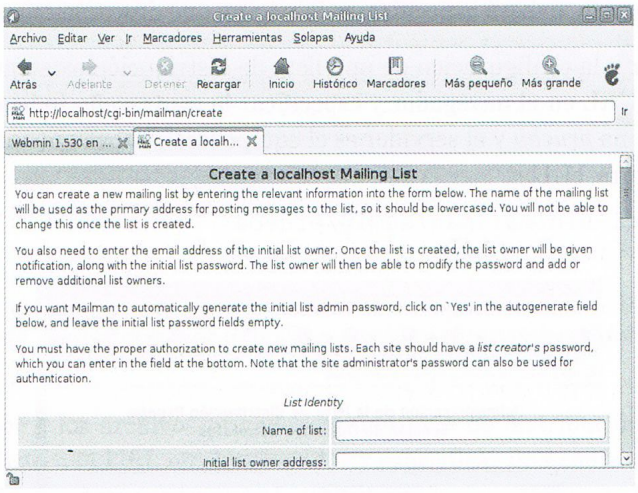


***Figura 11.9**. Ventana de creación de listas de distribución en Mailman. Desde esta ventana se pueden crear las listas a las que posteriormente se registrarán los usuarios con sus direcciones de correo*

18 Ahora comprobamos si podemos añadir direcciones de usuarios de correo a esa lista, para lo que accederemos a esta página, donde *<lista>* debe sustituirse por el nombre de la lista de distribución que hemos creado en los pasos anteriores (véase la Figura 11.10):

```
http://localhost/cgi-bin/mailman/listinfo/<lista>
```

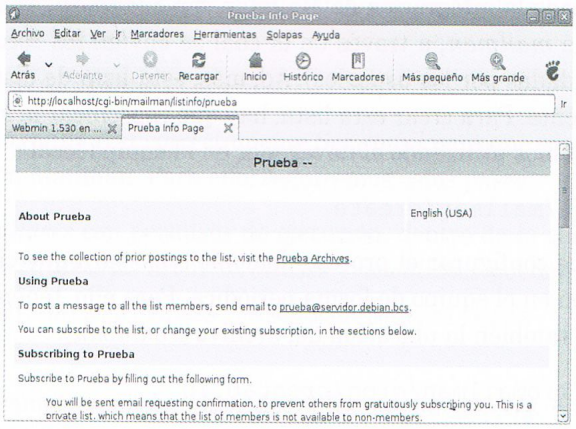


Figura 11.10. *Ventana de registro de usuarios en una lista de distribución Mailman. Aquí los usuarios especifican su dirección de correo electrónico, de forma que recibirán todos los mensajes que lleguen a esta lista*

19 A continuación, podemos comprobar si los mensajes enviados a esa lista de distribución son distribuidos a las direcciones de los usuarios registrados en ella.

11.1.3.2 Administración de Mailman

Como se explica en apartados anteriores, Mailman se gestiona a través de una interfaz web que permite realizar todas las operaciones relacionadas con la administración de las listas de distribución de correo. A estas páginas web se accede especificando la siguiente dirección en el navegador, donde *<servidor>* debe sustituirse por el nombre o dirección IP del equipo que funciona como servidor Mailman (o *localhost* si se refiere al equipo local):

```
http://localhost/cgi-bin/mailman/
```

A continuación de esta dirección, deberá especificarse la página que deseamos consultar, que puede ser:

- **admin**: permite acceder a la configuración de una lista de distribución existente. Para ello, hay que añadir el nombre de la lista a la URL en el navegador y especificar la contraseña indicada cuando se creó la lista. Por ejemplo, si la lista se llama *prueba* y el servidor es el equipo local, habrá que introducir la siguiente URL en el navegador (véase la Figura 11.11):

  ```
  http://localhost/cgi-bin/mailman/admin/prueba
  ```

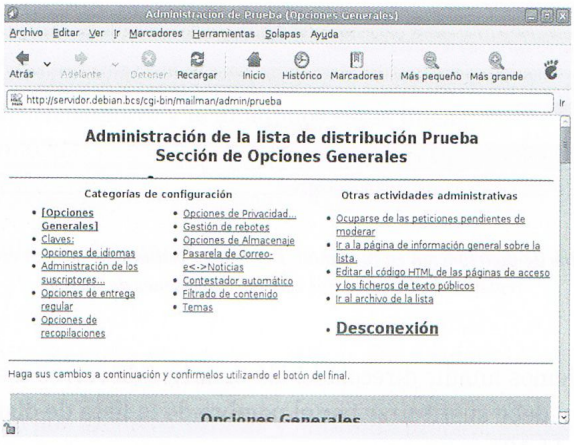


Figura 11.11. *Ventana principal de administración de una lista de distribución en Mailman. En esta ventana se muestran todas las opciones para la correcta gestión de una lista llamada "Prueba"*

- **admindb**: permite acceder a la lista de peticiones de suscripción pendientes de valorar en una lista de distribución existente. Para ello, hay que añadir el nombre de la lista a la URL en el navegador y especificar la contraseña indicada cuando se creó la lista. Por ejemplo, si la lista se llama *prueba* y el servidor es el equipo local, habrá que introducir la siguiente URL en el navegador:

```
http://localhost/cgi-bin/mailman/admindb/prueba
```

- **create**: permite crear una nueva lista de distribución de correo en el servidor. Esta operación también se puede realizar usando la orden *newlist* y, para mayor comodidad, se puede especificar una plantilla genérica que permite establecer una serie de parámetros que suelen ser comunes para la mayoría de las listas (esta plantilla es *sitelist.cfg* y suele ubicarse en */var/lib/mailman/data*). Para crear una lista con la orden *newlist* y la plantilla por defecto hay que ejecutar esto:

```
# newlist <nombre_lista>
# config_list -i /var/lib/mailman/data/sitelist.cfg
<nombre_lista>
```

- **edithtml**: se utiliza para modificar las páginas de gestión de las listas de distribución, de forma que éstas se muestren a nuestro gusto o con texto en nuestro idioma.

- **listinfo**: muestra un listado con todas las listas de distribución existentes. Si pulsamos sobre alguna de ellas, nos mostrará una página para suscribirnos a ella (véase la Figura 11.12).

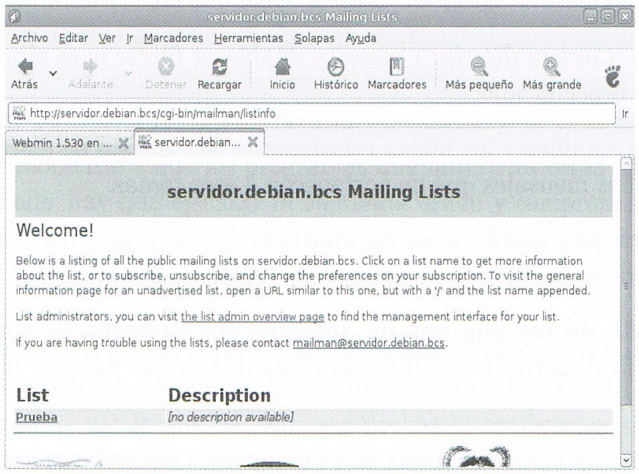


Figura 11.12. Ventana que muestra las listas disponibles en el servidor Mailman. Según se muestra en este listado, solamente aparece una lista llamada "Prueba". Si se pulsa sobre ella, se accederá a su página de configuración

- **private**: permite acceder a los archivos privados de una lista de distribución existente. Para ello, hay que añadir el nombre de la lista a la URL en el navegador y especificar una contraseña. Por ejemplo, si la lista se llama *prueba* y el servidor es el equipo local, habrá que introducir la siguiente URL en el navegador:

```
http://localhost/cgi-bin/mailman/private/prueba
```

Inicialmente, las páginas de gestión de las listas de distribución en Mailman aparecerán en el idioma por defecto (inglés), pero éste puede ser cambiado. Para ello, hay que seleccionar el idioma deseado en el enlace "Language options", dentro de la página configuración de la lista de distribución. Las opciones más importantes que están disponibles a la hora de administrar una lista de distribución son las siguientes (véase la Figura 11.11):

- **Opciones generales** (*General options*): especifica las características generales de la lista, como su nombre, dirección de correo del administrador, dirección de correo del moderador, descripción, información que se muestra en los mensajes, etc.
- **Claves** (*Passwords*): aquí se establecen las contraseñas del administrador y del moderador de la lista.
- **Opciones de idiomas** (*Language options*): especifica los idiomas utilizados en la lista.
- **Administración de los suscriptores** (*Membership management*): muestra la lista de usuarios que pertenecen a la lista y opciones para añadir o eliminar usuarios, ya sea individualmente o de forma masiva.
- **Opciones de entrega regular** (*Non-digest options*): establece las políticas relacionadas con el envío de los mensajes.
- **Opciones de privacidad** (*Privacy options*): establece las políticas de suscripción a las listas, como si es necesaria la aprobación de los usuarios registrados.
- **Opciones de almacenaje** (*Archiving options*): especifica cómo se guardan los archivos enviados con los mensajes.
- **Pasarela de correo-e<->Noticas** (*Mail<->News gateways*): incluye opciones para enlazar la lista de distribución con grupos de noticias.
- **Contestador automático** (*Auto-responder*): especifica opciones de respuesta automática a mensajes enviados.
- **Filtrado de contenido** (*Content filtering*): permite establecer filtros para eliminar aquéllos mensajes que no cumplen las condiciones especificadas.
- **Temas** (*Topics*): permite establecer los temas relacionados con la lista de distribución, además de filtros que permitan eliminar aquéllos mensajes que no pertenecen a esos temas.
- **Ocuparse de las peticiones pendientes de moderar** (*Tend to pending moderator requests*): se usa para gestionar las peticiones de suscripción a la lista (véase la página *admindb*).
- **Editar el código HTML de las páginas de acceso y los ficheros de texto públicos** (*Edit the public HTML pages and text files*): permite modificar el contenido de las páginas que gestionan la lista (véase la página *edithtml*).
- **Ir al archivo de la lista** (*Go to list archives*): permite accede a los archivos enviados en los mensajes que han sido guardados en el servidor.
- **Desconexión** (*Logout*): se usa para abandonar la página de administración de la lista.

En la instalación que se realiza siguiendo los pasos especificados en el apartado 11.1.3.1, no se especifica ninguna contraseña para el acceso a las páginas web de administración de Mailman (exceptuando las contraseñas que se especifican para cada una de las listas de distribución que se crean). Esto significa que cualquier usuario que acceda a determinadas páginas de administración de Mailman, habitualmente desde otro equipo a través de la red (especificando el nombre o dirección IP del servidor), tendrá privilegios para realizar ciertas operaciones, como crear nuevas listas. Para evitar esto, hay que establecer las contraseñas correspondientes, que son dos:

- Una contraseña de administrador global de Mailman, que se establece con esta orden:

```
# mmsitepass <contraseña_administrador>
```

- Una contraseña para crear nuevas listas de distribución en Mailman, que se establece con esta orden:

```
# mmsitepass -c <contraseña_crear>
```

11.1.3.3 Problemas y soluciones

Cuando el servicio de listas de distribución Mailman no funciona correctamente, es necesario planificar el proceso de detección y solución de problemas porque existen muchos servicios complejos que también están involucrados. Antes de pasar a comprobar directamente si la configuración de Mailman es correcta, es necesario revisar si otros servicios están funcionando correctamente:

- El acceso a la red.
- El servicio DNS (véase el capítulo 2 de este libro).
- El servidor de correo electrónico *Sendmail* y *Cyrus* (véase el capítulo 7).

Una vez que hemos comprobado que estos servicios funcionan correctamente, podemos pasar a comprobar la configuración de Mailman. Para ello, es recomendable seguir los pasos sobre su instalación y configuración que se explican en el apartado 11.1.3.1.

Algunos posibles problemas de funcionamiento de Mailman son los siguientes:

- **La distribución de GNU/Linux que utilizo no incluye ningún paquete *mailman* para instalar**: en ese caso, hay que instalar el paquete fuente, que está disponible para cualquier versión de GNU/Linux.
- **En las páginas web de administración de Mailman aparece el mensaje "404 File not found"**: esto es debido a que el servidor Apache no se ha configurado correctamente. Hay que comprobar que hay acceso a la carpeta *<ruta1>/cgi-bin/mailman* y que se pueden ejecutar los programas que contiene (directiva *ScriptAlias*). Es posible que en el archivo de configuración de Apache aparezca alguna otra directiva *ScriptAlias* y, si es así, hay que eliminarla o comentarla (poniéndole el símbolo # delante).
- **En las páginas web de administración de Mailman aparece el mensaje "Internal server error"**: esto suele ser debido normalmente a que los programas que muestran estas páginas no tienen asociados los permisos correctos. Para ello, hay que ejecutar la siguiente orden y comprobar que ésta no muestra ningún error:

```
# ./check_perms -f
```

- **Cuando se envía un mensaje a una lista de distribución, éste es devuelto indicando que la lista no existe**: este problema suele ser debido a dos posibles causas. Es posible que Mailman y Sendmail no se comuniquen correctamente, por lo que hay que comprobar la configuración (véase el apartado 11.1.3.1). También es posible que la base de datos de alias no esté correctamente actualizada, porque no se ejecuta el contenido del archivo *mailman.aliases* o porque hay que ejecutar de forma explícita la orden *newaliases* (véase el apartado 11.1.3.1).
- **Cuando se envía un mensaje a la lista, éste es devuelto con el error "sh: mailman not available for sendmail programs"**: la versión de Sendmail que se está utilizando ejecuta un intérprete restringido denominado *smrsh*, para que el sistema de correo sea más seguro.
- **Aparece el mensaje de error "Traceback (most recent call last)..."**: esto es debido a que no se encuentra instalado el paquete de desarrollo del lenguaje Python, que es el utilizado por Mailman. Para solucionar este problema, hay que instalar el paquete *python-XXX-dev*, donde *XXX* especifica la versión de Python que tenemos instalada en el equipo. Para saber qué versión utiliza nuestro equipo debemos consultar los paquetes Python que ya están instalados en él. Este error también puede ser debido a una incorrecta configuración de las variables de entorno del idioma. Para solucionar esto, hay que ejecutar las siguientes órdenes:

```
# LC_ALL=C
# LANG=C
# export LC_ALL
# export LANG
```

11.2 SERVICIOS DE REDIFUSIÓN

Los servicios de **redifusión** o **sindicación** se han convertido actualmente en un método muy común de intercambio de información en Internet. Muchos de estos servicios funcionan en base al protocolo **RSS** (*Really Simple Syndication* o Sindicación Realmente Simple), que actualmente se encuentra en la versión 2.0, aunque también pueden funcionar en base al protocolo **Atom**, que está definido formalmente en RFC 4287 y RFC 5023.

El funcionamiento de RSS es muy simple y se basa en que existe una fuente de información actualizada a la que los usuarios se suscriben para recibirla en sus equipos. Estos usuarios pueden leer la información, que llega en formato XML, utilizando algún programa cliente específico, denominado **agregador** o también a través de un navegador, ya que las versiones modernas de estos también soportan la visualización de la información en formato RSS.

Algunos de los programas cliente o agregadores más utilizados actualmente son:

- **Google Reader**: es compatible con RSS y Atom y también permite el envío de información actualizada que ha sido publicada en blogs.
- **Bloglines**: permite la visualización de la información en forma de mosaico o lista y es compatible con la red social Twitter.
- **FeedDemon**: funciona sobre Fuentes RSS y en plataformas Microsoft Windows. Se distribuye libremente (véase la Figura 11.13).
- **RSS Bandit**: también funciona para fuentes RSS y en plataformas Microsoft Windows.

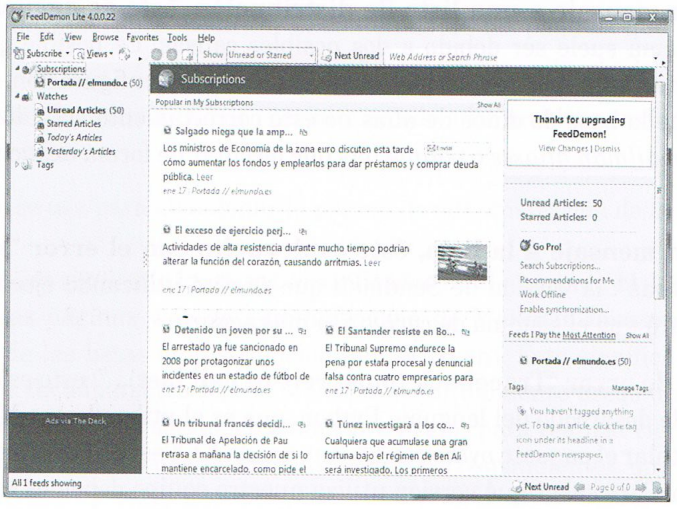


Figura 11.13. Ventana principal de FeedDemon. Aquí se puede observar cómo se muestra la información recibida por el usuario en formato de lista

Para poder acceder a la información facilitada por un servicio RSS, lo primero que tenemos que hacer es instalar el programa cliente o agregador. A continuación, tenemos que buscar la URL de la fuente RSS que, habitualmente nos aparecerá en la página web corresponciente como un enlace con el logotipo RSS. Simplemente tenemos que copiar ese enlace y pegarlo en el agregador y, a partir de ese momento, el programa descargará automáticamente la información para que esté disponible en nuestro equipo.

11.3 EL SERVICIO HORARIO NTP

El protocolo **NTP** (*Network Time Protocol* o Protocolo de Tiempo de Red) se utiliza para sincronizar las fechas y horas de los equipos informáticos de una red. La primera versión del protocolo NTP se puso en marcha en 1985 por Dave Mills, lo que le convierte en uno de los protocolos más antiguos que todavía hoy funcionan en TCP/IP.

El protocolo NTP está organizado en una jerarquía de equipos en la red. Los equipos de la jerarquía superior sincronizan sus relojes a través de sistemas de precisión como relojes atómicos o relojes GPS. Los equipos de segundo nivel se sincronizan con los equipos de primer nivel a través del envío de mensajes UDP que pueden tener una latencia variable. Esta jerarquía puede continuar, dependiendo de la versión del protocolo NTP que se utilice, hasta 256 niveles (la futura versión 5 de NTP se espera que solo soporte 8 niveles). Por **latencia variable** se entiende que el sistema de sincronización debe tener en cuenta que los mensajes UDP se envían a intervalos de tiempo distintos con un tiempo de llegada a su destino también distinto.

El protocolo NTP permite que los equipos se sincronicen con un margen de hasta 10 milisegundos si están conectados en una red de área extensa como Internet. En redes locales más pequeñas donde la velocidad de transmisión es mayor se pueden conseguir sincronizaciones de hasta 200 microsegundos.

El protocolo NTP está definido formalmente en los documentos RFC 778, RFC 891, RFC 956, RFC 958 y RFC 1305. Existen otros protocolos para la sincronización horaria que funcionan con mecanismos más simplificados como **Daytime** (RFC 867), que funciona sobre el demonio *inetd* en el puerto por defecto 13 y **SNTP** (*Simple Network Time Protocol* o Protocolo Simple de Tiempo de Red), que se define formalmente en RFC 1361, RFC 1769, RFC 2030 y RFC 4330. También hay otros protocolos como ICMP y HTTP que permiten la sincronización horaria (véase el capítulo 3).

11.3.1 CONFIGURACIÓN DE UN SERVIDOR NTP

El protocolo NTP está implementado por diferentes organismos y desarrolladores, como el **ISC** (*Internet Systems Consortium*), OpenBSD y DragonFly BSD. También existen versiones para otros sistemas operativos como Microsoft Windows. Todas estas versiones deben seguir lo indicado en los RFC para evitar problemas de compatibilidad en una red con diferentes equipos.

En los apartados siguientes se explica cómo instalar y configurar un servidor NTP en Microsoft Windows y GNU/Linux.

11.3.1.1 Configuración en Windows

Los sistemas Microsoft Windows incluyen mecanismos automáticos que permiten sincronizar la hora entre los equipos que están conectados al dominio. De esta forma, el equipo que funciona como controlador primario de dominio

sincroniza su reloj con el resto de equipos de ese dominio. Este mecanismo, llamado **WTS** (*Windows Time Service* o Servicio de Tiempo de Windows) o *W32Time*, funciona gracias a un programa en ejecución llamado *w32time.exe*. Aunque este servicio resulta muy efectivo para que todos los equipos mantengan la misma hora, tiene el inconveniente de que no es compatible con NTP. Esto significa que no permite sincronizar la hora en equipos que no están conectados al dominio o aquellos que no ejecutan un sistema operativo de Microsoft.

Sin embargo, el servicio de tiempo de Windows que se incluye en los servidores Windows 2000/2003/2008 también se puede ejecutar en modo de compatibilidad con NTP, de forma que cualquier cliente NTP pueda sincronizarse con él (equipos GNU/Linux, conmutadores, encaminadores, etc.). En los sistemas Windows Server 2003/2008 y Windows Vista/7 se puede hacer de esta forma:

- En el menú de inicio, ejecutar la orden *regedt32*, que es el programa que se utiliza para modificar el registro de Windows.
- En la ventana que aparece, seleccionar la opción del menú principal "Archivo || Exportar". En el cuadro de diálogo que se muestra, especificar la ubicación y el nombre del archivo, que contendrá una copia del registro de Windows. De esta forma, mantendremos una copia de seguridad por si hay problemas.
- Ahora, hay que modificar las siguientes claves del registro, que contendrán los valores que se indican:
  - **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\AnnounceFlags**: indica la fiabilidad que tiene el servidor de tiempo. El valor recomendado es 5 (decimal).
  - **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NTPClient\SpecialPollInterval**: especifica el tiempo en segundos que el equipo sincronizará su hora con otros servidores NTP (véase la entrada de registro siguiente). El valor recomendado es 900 (decimal) que se corresponde con 15 minutos.
  - **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\NtpServer**: contiene una lista de nombres de servidores NTP, separados por espacios, con los que este servidor se sincronizará. Habitualmente, esta entrada ya contiene los nombres de algunos servidores NTP de Internet con los que se puede sincronizar.
  - **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NTPServer\Enabled**: indica si el servidor NTP está active en este equipo. El valor 1 indicará que el servidor NTP estará activo.
  - **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\Type**: especifica el protocolo que utilizará este servidor de tiempo. Si se indica el valor "NTP", entonces el equipo funcionará como un servidor NTP nativo.

11.3.1.2 Configuración en GNU/Linux

Para que un equipo Linux funcione como servidor NTP, es necesario que mantenga en ejecución un proceso demonio llamado comúnmente *ntpd*. Este proceso utiliza el puerto 123 por defecto para enviar mensajes UDP con la fecha y hora sincronizada.

Para obtener un buen rendimiento en el funcionamiento del protocolo NTP, es recomendable tener un reloj NTP estándar con *lazo de seguimiento de fase* implementado en el núcleo del sistema operativo (*kernel*), en vez de solo usar la intervención de un demonio NTP externo. Esta característica permite compensar las desviaciones de tiempo que producen los imprecisos relojes de los ordenadores sin necesidad de que un servidor NTP lo realice constantemente. Todas las versiones de GNU/Linux modernas soportan esta característica.

11.3.2 CONFIGURACIÓN DE UN CLIENTE NTP

Cuando un equipo funciona como servidor de tiempo en base al protocolo NTP, se asegura que éste podrá sincronizar su hora con equipos cliente de características muy diversas (GNU/Linux, Mac OS X, Cisco IOS, etc.). En los apartados siguientes se explica cómo se configura un equipo Microsoft Windows y GNU/Linux para que funcione como cliente NTP.

11.3.2.1 Configuración en Windows

Para acceder a la configuración del cliente horario NTP en Microsoft Windows 7 hay que seguir estos pasos:

1 Acceder al Panel de Control desde el menú de inicio del escritorio.

2 Seleccionar y hacer doble clic sobre el icono "Fecha y hora".

3 En la ventana que aparece, seleccionar la página "Hora de Internet". En ella, hay que pulsar en el botón "Cambiar la configuración...".

4 En la ventana que aparece (véase la Figura 11.14), marcar la opción "Sincronizar con un servidor horario de Internet", especificar la dirección o nombre del servidor NTP en el cuadro de texto titulado "Servidor" y pulsar en el botón "Actualizar ahora".

5 Finalmente, pulsar en el botón "Aceptar" para que los cambios realizados se guarden.

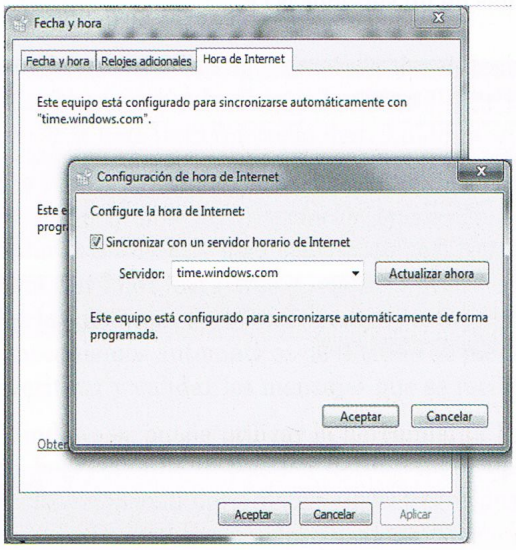


Figura 11.14. *Configuración del cliente NTP en Microsoft Windows 7*

11.3.2.2 Configuración en GNU/Linux

Para configurar un cliente NTP en OpenSUSE hay que seguir estos pasos:

1 Seleccionar "Servicios de red || Configuración de NTP" en la ventana principal de la herramienta YaST. Esto mostrará una ventana como la de la Figura 11.15.

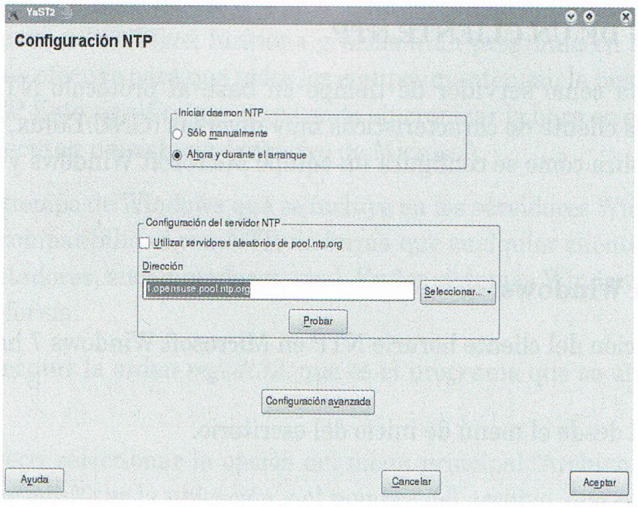


Figura 11.15. *Configuración del cliente NTP en YaST. En esta ventana se puede indicar si el proceso demonio del cliente NTP se inicia automáticamente en el arranque y la dirección o nombre del servidor NTP*

2 Tenemos dos opciones de inicio del proceso demonio que se encarga de enviar las peticiones de actualización: "Solo manualmente" (el proceso lo tenemos que iniciar manualmente) o "Ahora y durante el arranque" (el proceso se inicia ahora y cada vez que se inicia el equipo). Por su parte, en el campo "Direccción" se especifica el nombre o dirección IP del servidor NTP.

3 A continuación, pulsamos en el botón "Configuración avanzada", lo que mostrará una ventana como la de la Figura 11.16. En ella, se puede indicar más de un servidor NTP.

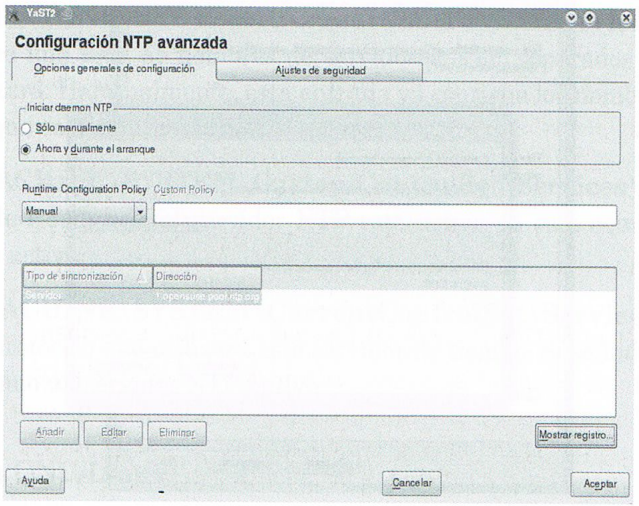


Figura 11.16. *Configuración avanzada del cliente NTP en YaST. Aquí se pueden configurar opciones adicionales de funcionamiento del proceso cliente*

4 En la página "Ajustes de seguridad" hay que marcar la opción "Puerto abierto en el cortafuegos" en caso de que tengamos activo algún cortafuegos. De lo contrario, éste filtrará todos los mensajes NTP.

En los sistemas Fedora y Debian se pueden utilizar las siguientes órdenes del intérprete para gestionar la hora del sistema y sincronizarla con un servidor NTP:

- **date**: establece la fecha y hora del equipo, con el formato *MMDDhhmmCCYY*.
- **hwclock**: especifica la distribución de fecha y hora a utilizar. Por ejemplo, el argumento *--utc* especifica que la hora del sistema está en formato UTC.
- **ntpdate**: establece la hora actual del sistema en base a la información facilitada por un servidor NTP, que se ha especificado como argumento (su nombre o dirección IP). Esta orden se incluye con el paquete que lleva el mismo nombre. Es recomendable ejecutar esta orden periódicamente usando, por ejemplo, el planificador de tareas *cron*, para que la sincronización se realice a intervalos de tiempo regulares.

RESUMEN DEL CAPÍTULO

Las **listas de distribución** permiten el envío de mensajes de correo a un conjunto de usuarios que previamente se han registrado en esas listas. Esta característica ya está disponible en un sistema de correo electrónico convencional, pero gracias a las listas de distribución se puede enviar un mismo mensaje a millones de usuarios de forma automática, especificando únicamente la dirección asignada a la lista.

Para que el mecanismo de listas de distribución funcione perfectamente en un servidor de Internet, es necesario que otros servicios también funcionen bien: el servicio de red, el servicio DNS para resolver las direcciones del servidor y de los destinatarios y el servicio de correo electrónico. Estos servicios pueden estar integrados en el mismo equipo donde se ejecuta el servicio de listas de distribución o pueden estar instalados en otros equipos, para reducir la carga de trabajo.

Las listas de distribución pueden ser de dos tipos: los **boletines de noticias**, en los que solamente algunos miembros pueden enviar mensajes a la lista y las **listas de discusión**, en las que todos los usuarios pueden enviar mensajes a la lista para que sean distribuidos a sus miembros.

Las reglas de participación o reglas de etiqueta son una serie de normas que hay que establecer en cualquier sistema que permita el intercambio de información entre usuarios. Gracias a estas normas, la comunicación se puede desarrollar con fluidez y soin contratiempos. Normas como tratar a las personas con respeto, no utilizar el sistema con fines lucrativos o seguir la temática de la lista son fundamentales para que el sistema resulte útil a los usuarios. Para hacer cumplir estas normas, los sistemas de gestión de listas de distribución incluyen mecanismos automáticos de filtrado de mensajes y la posibilidad de definir un **moderador**, encargado de verificar y validar los mensajes que se reciben.

En los sistemas Microsoft Windows se puede utilizar la herramienta Exchange Server para gestionar listas de distribución. En esta herramienta se pueden definir los grupos de distribución, grupos de distribución dinámicos y grupos de seguridad para distribuir los mensajes a sus miembros. En un grupo de distribución dinámico, los usuarios miembros se especifican en base a determinaodos criterios, por lo que esta relación no tiene que definirse manualmente. Por su parte, los grupos de seguridad permiten también la distribución de mensajes de correo entre sus miembros, además de gestionar los permisos sobre los recursos del equipo o del dominio.

En los sistemas GNU/Linux se puede utilizar el paquete Mailman, que permite la gestión de las listas de distribución y es compatible con los paquetes de servicios más utilizados en la actualidad (Apache, Sendmail, Postfix, etc.). Mailman incluye una herramienta web de administración y permite la moderación, suscripción, listas cerradas y abiertas, filtros, etc. Para que Mailman funcione en un servidor local o de

Internet, es necesario que éste tenga perfectamente configurado el servicio DNS, páginas web (como Apache) y correo (como Sendmail y *Cyrus*).

La gestión de Mailman se realiza a través de una página web que incluye los siguientes enlaces: *admin* (para administrar las listas definidas), *admindb* (acceso a las peticiones de suscripción), *create* (creación de nuevas listas), *edithtml* (modificación de las propias páginas de configuración), *listinfo* (relación de listas de distribución disponibles) y *private* (archivos adjuntos a los mensajes).

EJERCICIOS PROPUESTOS

1. ¿Es posible que una misma dirección de correo electrónico esté asociada a diferentes listas de distribución? ¿Cómo?

2. Indica los pasos que debes seguir para definir las siguientes listas de distribución de correo en Exchange Server:

- Lista1: ines, moli, elena y ana.
- Lista2: moli, ana y clara.
- Lista3: ines y clara.

3. ¿Es posible establecer restricciones en cuanto al tamaño de los mensajes enviados a un grupo de distribución de Exchange Server? ¿Se pueden limitar los usuarios que pueden enviar mensajes al grupo de distribución?

4. Suponemos que tenemos una red local definida por un dominio de la red Microsoft llamado "empresa.es" donde se han creado una serie de cuentas de usuario. Algunas de esas cuentas, pertenecen a personas que trabajan en el departamento de ventas, por lo que a sus cuentas de usuario se les ha establecido la pertenencia al grupo "Ventas". ¿Cómo se puede configurar el servidor de forma que enviando un mensaje a la dirección *ventas@empresa.es* éste llegue a todos los trabajadores de ese departamento?

5. ¿Es posible desactivar de forma temporal un grupo de distribución en Exchange Server sin necesidad de eliminarlo del sistema? ¿Cómo se puede activar posteriormente para que los mensajes vuelvan a ser enviados a los destinatarios?

6. ¿Es mejor utilizar un grupo de distribución o un grupo de seguridad para enviar mensajes de correo a grupos de usuarios en Exchange Server?

7. Crea una lista de distribución en Mailman y explica los pasos a realizar para que un usuario registre su dirección de correo en ella y el administrador autorice ese alta.

8. Sobre la lista de distribución creada en el ejercicio anterior, indica qué configuraciones debes realizar para que los archivos enviados con los mensajes sean automáticamente almacenados en el servidor. Indica también cómo pueden acceder los miembros de la lista a esos archivos.

9. Indica los pasos que debes seguir para configurar el filtrado en una lista de distribución con Mailman de forma que se eliminen automáticamente aquellos mensajes que contengan algunas palabras malsonantes o groseras.

10. Especifica los pasos a seguir para configurar tu sistema GNU/Linux de forma que se sincronice con algún servidor NTP de Internet.

11. Repite el ejercicio anterior pero esta vez sobre Microsoft Windows 7.

12. Si un cliente NTP solicita sincronizarse con un servidor, envía un mensaje de solicitud y espera una respuesta con la hora actual. Si no conocemos el tiempo que tardan estos dos mensajes en llegar a su destino, ¿cómo crees que sea posible que el cliente pueda sincronizar su hora con la del servidor sin sufrir ninguna variación significativa?

13. Indica los pasos a seguir para configurar en tu equipo un cliente RSS que muestre noticias publicadas por algún servidor de Internet.

TEST DE CONOCIMIENTOS

1 Un boletín de noticias es:
- a) Un sistema de lista de distribución.
- b) Un sistema en el que solo unos pocos usuarios privilegiados pueden enviar mensajes.
- c) Un sistema en el que los usuarios se pueden dar de alta para recibir información.
- d) Todas son ciertas.

2 Un grupo de distribución en Windows permite:
- a) Enviar mensajes a los usuarios que pertenecen a él.
- b) Establecer permisos para el acceso a recursos compartidos.
- c) Definir los usuarios que pertenecen a él en base a diferentes reglas.
- d) a y c son correctas.

3 En un grupo de distribución dinámico los usuarios miembros se pueden definir en base a:
- a) Aquellos que no estén definidos en el Directorio Activo.
- b) Los que su nombre comience por "p".
- c) Aquellos que pertenezcan al grupo "Desarrollo".
- d) Todas las anteriores.

4 Para poder distribuir correo a los usuarios que pertenezcan a un grupo de seguridad es necesario:
- a) Registrar direcciones de correo para los usuarios del grupo.
- b) Activar el reenvío del correo al grupo.
- c) Nada, simplemente enviar mensajes al grupo.
- d) a y b son ciertas.

5 Mailman necesita los siguientes servicios para funcionar correctamente:
- a) DHCP.
- b) Correo.
- c) Openfire.
- d) Ninguna es cierta.

6 Para autorizar o desautorizar una petición de suscripción en Mailman hay que accede a la página:
- a) Administración de los suscriptores.
- b) Ocuparse de las peticiones pendientes de moderar.
- c) Filtrado de contenido.
- d) Opciones de privacidad.

7 El servicio RSS se usa para:
- a) Distribuir información a varios usuarios.
- b) Enviar mensajes de correo a varios usuarios a la vez.
- c) Publicar periódicos.
- d) Todas son ciertas.

8 El protocolo NTP permite:
- a) Dar la hora exacta a los usuarios que consultan los servidores.
- b) Obtener el equipo que tiene la hora más exacta.
- c) Sincronizar nuestro ordenador con la hora de otro.
- d) b y c son ciertas.

9 La orden *ntpdate* se usa para:
- a) Consultar la fecha y hora en nuestro equipo.
- b) Establecer la distribución horaria que se va a utilizar.
- c) Establecer manualmente la fecha y hora actuales.
- d) Ninguna es cierta.

12 VoIP

OBJETIVOS DEL CAPÍTULO

- ✓ Comprender el funcionamiento de la telefonía tradicional.
- ✓ Entender en general el funcionamiento de la tecnología VoIP así como los protocolos utilizados para hacerla efectiva.
- ✓ Distinguir los factores que influyen para obtener conversaciones de calidad e identificar algunas de las acciones para mejorarla.
- ✓ Conocer los elementos principales en un sistema de telefonía VoIP y la función que desempeña cada uno.
- ✓ Aprender a configurar clientes de telefonía VoIP para comunicarse mediante PBX.
- ✓ Entender las características y posibilidades del PBX software 3CX y Asterisk.
- ✓ Utilizar un PBX software para crear extensiones para los clientes.

En este capítulo se aborda una tecnología cada vez es más utilizada por proveedores de servicios para proporcionarnos telefonía a bajo coste y que también está teniendo repercusión en el mundo empresarial, sustituyendo los antiguos sistemas telefónicos que permitían las comunicaciones de voz entre el personal de sus distintas áreas, secciones o departamentos.

VoIP aprovecha las infraestructuras creadas de sistemas de redes de datos para cubrir cortas distancias, así como las creadas por los sistemas de telefonía para cubrir mayores distancias. Esto es posible ya que VoIP utiliza la arquitectura TCP/IP, haciéndonos suponer la existencia de una serie de protocolos que materializan la transmisión de voz.

Para utilizar esta tecnología se requieren de una serie de dispositivos que se describen a lo largo del capítulo, así como otros para poder seguir utilizando los dispositivos tradicionales. El dispositivo por excelencia es el PBX, que a modo de centralita, gestiona las comunicaciones internas y externas de la empresa. Existen soluciones propietarias como Microsoft Office Communication Server o Cisco Call Center para su implementación. En este capítulo se ejemplifica mediante la instalación de software libre Asterisk, que goza de gran popularidad y prácticamente se ha convertido en un estándar.

12.1 TELEFONÍA TRADICIONAL

12.1.1 PÚBLICA

En sus orígenes la transmisión de voz se ha realizado mediante el envío de señales analógicas sobre la red de telefonía básica conocida como RTB o POTS (*Plain Old Telephone Service*). Los usuarios necesitan de un terminal o teléfono analógico para convertir la voz en señales analógicas mediante su transductor, gracias a técnicas de modulación. El terminal dispone de un puerto FXO (*Foreign eXchange Office* o Interfaz de Central Externa), que se conecta al puerto FXS (*Foreign eXchange Subscriber* o Interfaz de Abonado Externo) que pone a nuestra disposición la compañía telefónica, más conocido como PTR (Punto de Terminación de Red) o roseta telefónica. Ambos puertos se conectan mediante un latiguillo de cable paralelo de telefonía, en cuyos extremos tiene engastados conectores RJ11. El puerto FXS está conectado a un par de hilos de cobre o línea tendidos por la compañía telefónica desde la central de telefonía, estableciéndose lo que se denomina un **bucle local** o de abonado, el cual proporciona corriente eléctrica, permite el envío de señales acústicas y gestiona el marcado de números en el terminal.

Las centrales telefónicas realizan una función similar a la de los conmutadores en una red de ordenadores, estableciendo las conexiones entre las líneas de los abonados a la compañía telefónica. La transmisión de las señales analógicas utiliza la técnica de conmutación de circuitos, que establece un camino único dedicado entre el emisor y receptor, y se utiliza durante todo el proceso de transmisión. Finalizada la comunicación, dicho camino se libera para poder utilizarse por otros usuarios. Las centrales telefónicas identifican a cada usuario mediante una dirección, conocida vulgarmente como número de teléfono. Las centrales cubren áreas geográficas concretas, uniéndose entre sí mediante **líneas troncales** o **trunk lines** (véase Figura 12.1) para proporcionar una cobertura a nivel nacional e internacional. Para transportar las conversaciones de varios usuarios sobre las líneas troncales, se utilizan técnicas de multiplexación, como FDM (*Frecuency Division Multiplexing* o Multiplexación por División de Frecuencia), que utiliza distintos rangos de frecuencias que el canal de transmisión es capaz de soportar, para trasmitir cada una de las conversaciones.

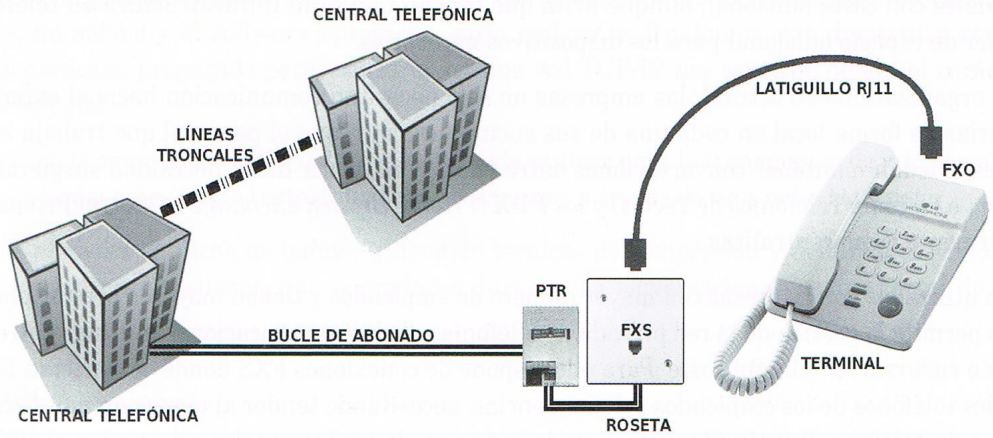


Figura 12.1. Elementos que intervienen en telefonía tradicional. El terminal se conecta mediante su puerto FXO al puerto FXS de la roseta, la cual está conectada al PTR y forma un bucle de abonado con la central telefónica. Las centrales entre sí se unen mediante líneas troncales

En 1940 el teorema de Nyquist fue demostrado matemáticamente por Claude Shannon, probando que se podían convertir las señales analógicas de la RTB a formato digital. Se patentó el dispositivo que realizaba dicha trasnformación, denominado **codificador-decodificador**, quedando abierto el camino para la transmisión de información manejada por computadores o información digital a través de la RTB. Hacia 1960 se empezaron a desarrollar diversos tipos de redes digitales de ordenadores, y posteriormente hacia 1984, se creó una red para la transmisión de voz mediante el envío de señales digitales, la **Red Digital de Servicios Integrados** o **RDSI**. Esta red al igual que la RTB, también se basa en la técnica de conmutación de circuitos. Al hacerse patente la eficiencia de las transmisiones en formato digital, más rápidas que las analógicas, las conexiones entre centrales se convirtieron a formato digital, dejándose los bucles de abonado con el formato analógico. Gracias a los codificadores-decodificadores, en las centrales de telefonía es donde se realiza la conversión analógico-digital y viceversa. Las conversaciones de varios usuarios se transmiten por las líneas troncales gracias a la técnica de multiplexación por división de tiempo o TDM (*Time Division Multiplexing* o Multiplexación por División de Tiempo), que asigna el canal de transmisión a cada conversación, durante un intervalo de tiempo.

El término RTC o Red Telefónica Conmutada o PSTN (*Public Switched Telephone Network*) hace referencia a cualquier red que utiliza técnicas de conmutación, independientemente del tipo de señal que transporta (analógicas o digitales). La RTC utiliza en Estados Unidos y Canadá el sistema SS7 (*Signaling System 7* o Sistema de Señalización 7) o C7 en Europa, para coordinar las centrales telefónicas, permitiendo obtener diversos datos referidos a las llamadas como su duración, posibilitando la facturación de las llamadas.

12.1.2 PRIVADA

Las redes públicas han servido a empresas la comunicación entre sus diversas sucursales, repartidas por la geografía comarcal, nacional e incluso mundial. Por lo general el coste de las llamadas depende de la distancia donde estén localizadas dichas sucursales, pudiéndose incrementar en función de los servicios contratados. Algunas empresas han optado por adquirir sus propias líneas de telefonía para comunicar sus suscursales o utilizar otros modelos de comunicación como **Centrex** (*Central Office Exchange Service* u Oficina Central de Servicio de Intercambio).

El modelo Centrex permite a las empresas la utilización de la RTC para sus comunicaciones, aunque con algunas diferencias respecto al modelo tradicional. En el modelo Centrex, el bucle local entre la empresa y la compañía telefónica no se realiza directamente con la central, sino en un dispositivo más sofisticado cuya propiedad y gestión es de la compañía telefónica y se ubica en sus instalaciones. La utilización de este modelo proporciona a las empresas

servicios adicionales con coste adicional, aunque evita que tengan una gran infraestructura en telecomunicaciones, así como disponer de espacio adicional para los dispositivos necesarios.

Debido a su organización estructural, las empresas no solo necesitan comunicación hacia el exterior, haciéndose también necesarias de forma local en cada una de sus sucursales, para que el personal que trabaja en sus distintas áreas o secciones, puedan mantener conversaciones entre ellos. Para cubrir dicha necesidad surgieron los **KTS** (*Key Telephone System* o Sistema Telefónico de Teclas) y los **PBX** (*Private Branch eXchange* o Central Privada Secundaria), conocidos vulgarmente como centralitas.

Los PBX son utilizados por empresas con mayor número de empleados y tienen mayores prestaciones que los KTS. Este dispositivo permite la gestión de la red privada de telefonía o de las comunicaciones internas entre los empleados de una empresa o sucursal sin ningún coste. Para ello dispone de conexiones FXS donde se conectan los puertos FXO de cada uno de los teléfonos de los empleados o dependencias, necesitando tender al menos un par de cables paralelos entre el PBX y cada teléfono. Para la identificación de cada uno de los terminales conectados al PBX se utiliza un número, el cual recibe el nombre de **extensión**. Los PBX también permiten las comunicaciones con el exterior, ya que se disponen de puertos FXO para conectarse a la RTC. Estos puertos se conectan a las rosetas telefónicas o PTR, que instala la compañía telefónica a la que se contratan las líneas. Si se contratan varias, se puede por ejemplo, realizar llamadas hacia el exterior y enviar o rececibir faxes de forma simultánea. La conexión hacia el exterior se puede realizar mediante líneas públicas, o mediante el alquiler de líneas para crear redes privadas entre distintas sucursales de una empresa. Los PBX también ofrecen características utilizadas en la telefonía tradicional, como buzón de voz, devolución o transferencia de llamadas y conferencias. Las últimas generaciones de PBX permiten también la conexión con dispositivos **track móvil**, que permiten utilizar las redes de telefonía móvil si las llamadas van dirigidas a un usuario de dichas redes, abaratándose las llamadas que efectuándolas sobre la RTC. La utilización de un track móvil requiere la contratación de una línea móvil y la inserción de la tarjeta SIM, en dicho dispositivo. Actualmente los PBX suelen ser modulares, permitiendo mediante la instalación de distintos módulos con puertos FXO o FXS, cubrir las necesidades internas y de cara hacia el exterior.

12.2 FUNCIONAMIENTO DE VOIP

Las siglas VoIP significan *Voice over Internet Protocol*, o en castellano: "Voz sobre el Protocolo de Interred". De forma general podemos decir que VoIP, es la transmisión de voz utilizando los mismos protocolos que emplean las redes de computadoras TCP/IP para la transmisión e intercambio de datos. Si extrapolamos esta idea a Internet, podemos decir que VoIP utiliza los mismos protocolos que se utilizan en Internet en la transmisión de información, para la transmisión de voz. *A priori* esta idea nos permite obtener conclusiones inmediatas y, de la misma forma apreciar las ventajas de esta tecnología, entre otras:

- Puede utilizarse aprovechando la infraestructura creada para una red local o de Internet, con independencia de los medios de transmisión utilizados, permitiendo mantener varias conversaciones simultáneas.
- En empresas no requiere de una instalación simultánea de cableado telefónico para conectar los teléfonos a la centralita o PBX.
- Permite comunicarnos con otra persona sin importarnos la distancia ni el lugar en el que nos encontramos, no siendo necesario utilizar el sistema de telefonía tradicional para efectuar llamadas Internacionales, con el consiguiente ahorro económico.

- No requiere de grandes inversiones para su puesta en funcionamiento. Con un ordenador con tarjeta de sonido, altavoces, micrófono y el software apropiado, sería suficiente. Cualquier otro dispositivo como un móvil de última generación, preparado para utilizarse en una red TCP/IP nos serviría, de ahí el carácter portable de dicha tecnología.
- Al basarse en la arquitectura TCP/IP, no solo se puede utilizar para la transmisión de voz, permitiendo también el envío de imágenes, vídeo o texto, tal y como lo hacemos a través de una red o Internet.
- Hace más eficiente el ancho de banda, utilizando técnicas de compresión y evitando el envío de información durante los espacios de silencio que se producen durante las conversaciones, ya que carece de sentido.

12.2.1 CODECS

Puesto que VoIP se sustenta sobre una arquitectura basada en la técnica de conmutación de paquetes, deben existir unos mecanismos que permitan al emisor convertir la voz en paquetes para enviarlos a su destinatario. Para conseguirlo, se realiza un muestreo de la señal en formato analógico generada al emitir la voz sobre un dispositivo de audio, obteniéndose una señal en formato digital. Si el muestreo de la señal es alto, la señal digital tendrá mayor longitud y se necesitará más tiempo para su transmisión, pero redunda en una mejor calidad del servicio (QoS). Por el contrario, si el muestreo de la señal es bajo, la señal digital será de menor longitud y la velocidad de transmisión será mayor, aunque la calidad del servicio se verá afectada. Para reducir la longitud de la señal digital a transmitir y aumentar la velocidad de transmisión, se suele recurrir a técnicas de compresión. También deben existir unos mecanismos que permitan al destinatario realizar el proceso inverso, es decir, extraer la voz de los paquetes de forma ordenada para que el mensaje sea audible (véase Figura 12.2). El responsable de realizar este proceso de digitalización se denominan **codificador/decodificador de voz** o **codec**, algunos de los más representativos y utilizados en VoIP se muestran en la tabla 12.1.

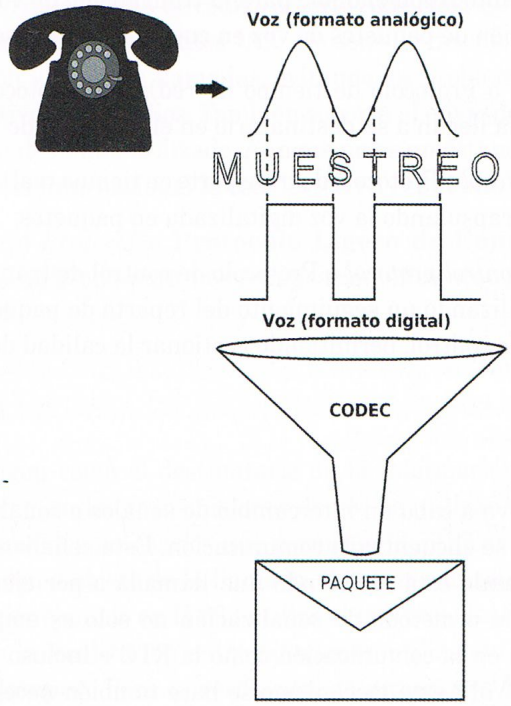


Figura 12.2. *Conversión a paquetes de la voz. La voz emitida a través del terminal se convierte en señales analógicas, que mediante un proceso de muestreo se convierten a formato digital. El codec empaqueta la voz digitalizada, la comprime y empaqueta*

Tabla 12.1. Codecs definidos por la ITU

Codec	Ancho de banda	Codificación
G.711	64 Kbps	Mediante técnica PCM (*Pulse Code Modulation* o Modulación por Impulsos Codificados).
G.722	48, 56 y 64 Kbps	A 7 KHz de frecuencia.
G.723.1	5'3, 6'3 Kpbs	Mediante una variante de PCM.
G.726	16, 24, 32, 40 Kpbs	Mediante la variante de PCM, ADPCM (*Adaptive Differential Pulse Code Modulation*).
G.728	16 Kpbs	Mediante código de retardo bajo.
G.729	8 Kpbs	Mediante código algebraico.

12.2.2 TRANSPORTE Y CONTROL DE LA TRANSMISIÓN

Una vez digitalizada la voz en un mensaje, este se divide en fragmentos más pequeños o paquetes para enviarlos al destinatario de la conversación. VoIP debe establecer unos mecanismos que al menos aseguren que la voz codificada y comprimida, se entregue a su destinatario en un intervalo de tiempo determinado y con la calidad suficiente. En caso contrario la conversación tendría cortes y por tanto se degradaría la calidad del servicio. Para garantizar la transmisión, VoIP se integra en la arquitectura TCP/IP utilizando una serie de protocolos en la capa de aplicación, que recurren al protocolo de la capa de transporte UDP. El protocolo UDP no ejerce control sobre la transmisión como TCP, haciendo que sea más rápido y por tanto recomendable para la transmisión de voz en tiempo real. La combinación de protocolos que permiten la transmisión de paquetes de voz en cuestión de nanosegundos, son los siguientes:

- **NTP** (*Network time protocol* o Protocolo de tiempo de red): este protocolo se encarga de controlar que los fragmentos de voz digitalizada llegan a su destinatario en el intervalo de tiempo requerido.
- **RTP** (*Real-time transport protocol* o Protocolo de transporte en tiempo real): proporciona funciones de transporte de red extremo a extremo, encapsulando la voz digitalizada en paquetes.
- **RTCP** (*Real-time transport control protocol* o Protocolo de control de tranporte en tiempo real): este protocolo se complementa con RTP, realizando un seguimiento del reparto de paquetes de voz digitalizada mediante el envío periódico de paquetes de control, permitiendo gestionar la calidad del servicio (QoS).

12.2.3 SEÑALIZACIÓN

En la telefonía tradicional, se lleva a cabo un intercambio de señales o señalización para que el usuario obtenga información sobre del estado en que se encuentra la comunicación. Esta señalización, permite al usuario determinar cuando la línea está disponible, cuando está recibiendo una llamada o por ejemplo cuando está comunicando. La manera de conseguir la señalización o método de señalización no solo es empleado por los terminales, sino por todos los elementos que intervienen en la comunicación como la RTC e incluso los PBX, de forma que se garantiza la comunicación entre usuarios. En VoIP este mecanismo se hace también necesario, y donde se consigue gracias a una serie de protocolos que utilizan la capa UDP para el transporte de la información de señalización que requieren utilizar. Los protocolos desarrollados por organismos de estandarización más utilizados son los siguientes:

- **H.323**: es un protocolo diseñado por la ITU, cuyo propósito original fue la transmisión de videoconferencias a través de redes locales. Su diseño se basa en la RTC apostándo por la simplicidad en la señalización y una alta disponibilidad para la transmisión de audio y vídeo. De hecho, se caracteriza por su rapidez si lo comparamos con otros protocolos como SIP. Para conseguir su objetivo engloba varios protocolos, como Q.931 utilizado para la señalización inicial de llamadas, H.225 utilizado para el control de la llamada y H.245 utilizado para el control para comunicaciones multimedia.

Como curiosidad indicar que el famoso programa Netmeeting de Microsoft disponible para las versiones Windos Me, 2000 y XP, utiliza el protocolo H.323 para sus transmisiones de vídeo y audio.

- **SIP** (*Session Initiation Protocol* o **Protocolo de Inicio de Sesión**): es un protocolo diseñado por la IETF para la transmisión de telefonía, vídeo y mensajes instantáneos, utilizando conexiones distintas para voz y señalización. De diseño sencillo, modular y flexible, los mensajes se envían en formato texto similar a HTTP y soporta gran variedad de esquemas de direccionamiento, permitiendo referenciar a los usuarios de forma similar a SMTP. Este protocolo se encarga de la autenticación de usuarios, de negociar la calidad de la comunicación (QoS) y del intercambio de direcciones IP y los puertos utilizados para la señalización y la transmisión de voz.

Existen otros protocolos de carácter privado, que se desarrollaron para aportar características de las que adolecen los protocolos anteriormente mencionados:

- **IAX2** (*Inter-Asterisk eXchange revision 2* o **Intercambio entre dispositivos Asterisk versión 2**): creado por Digium, la compañía que desarrolló el PBX de código abierto **Asterisk**. Es utilizado para la comunicación entre servidores Asterisk y entre servidores y clientes IAX. De sencillo diseño, utiliza el mismo puerto (4569) para la información de señalización y para las llamadas, evitando los problemas ocasionados por la traducción de direcciones o NAT en dispositivos intemedios. También soporta el envio de llamadas simultáneas o **trunking**, consiguiendo reducir el ancho de banda utilizado. Aunque no es un estándar como SIP su reconocimiento y su alto grado de utilización a nivel internacional lo convierten en candidato a sustituirlo.
- **SCCP** (*Skinny Client Control Protocol* o **Protocolo Ligero de Control de Clientes**): es un protocolo propietario de Cisco Systems utilizado para la comunicación eficiente entre los terminales IP de Cisco y su PBX software o Call Manager.

12.2.4 DIRECCIONAMIENTO

En una red TCP/IP tanto el origen como el destinatario de la información es un equipo, el cual se identifica mediante su dirección IP, sin embargo, en las transmisiones de voz se utilizan números de teléfono o bien nombres de usuario. VoIP establece los mecanismos necesarios que permiten identificar el equipo y servicio correspondiente al número de teléfono o usuario, origen u objeto de la llamada. Estos mecanismos de direccionamiento dependen del protocolo de señalización utilizado, por ejemplo en H.323 utiliza el protocolo RAS (*Registration, Admision and Status* o Registro, Admisión y Estado) para la localización entre estaciones, utilizando un dispositivo o equipo que gestiona la comunicación denominado **gatekeeper**. Para la resolución de direcciones IP, H.323 también puede valerse de servicios DNS. El protocolo SIP denomina **URI** (*Uniform Resource Identifier* o Identificador Uniforme de Recurso) a las direcciones que identifican a un usuario, cuyo formato es:

sip:Usuario@Equipo:Puerto

donde *:Puerto* de escucha es opcional, y como *Equipo* se puede indicar un nombre de dominio o dirección IP. La traducción o resolución de URIs utilizadas por SIP, puede realizarse mediante servicios DNS.

12.2.5 QOS (*QUALITY OF SERVICE* O CALIDAD DEL SERVICIO)

El éxito de VoIP se consigue cuando la conversación entre las partes que intervienen, es satisfactoria. Los medios de transmisión y los dispositivos intermedios utilizados, influyen a la hora de mejorar o empobrecer la calidad en las conversaciones. Por ejemplo, la velocidad de transmisión y la inmunidad frente al ruido en redes Giga Ethernet, es superior frente a una red inalámbrica y *a priori*, la QoS será mejor. Para garantizar la calidad de las conversaciones, han de tenerse en cuenta los siguientes factores:

- **Ancho de banda**: se debe optimizar y conseguir que sea constante con independencia del estado de otras conexiones. Para conseguirlo puede reservarse un ancho de banda para los paquetes de voz. Su reducción influirá en el número de paquetes de voz transmitidos y, por tanto, en la conversación.
- **Latencia o retardo**: es el retraso sufrido por los paquetes de voz en el tránsito desde su origen al destinatario, pudiendo verse influidos por los dispositivos intermedios por los que atraviesan el flujo de paquetes. Algunas recomendaciones para reducir su efecto y que su valor no supere los 150 ms son:

Establecer políticas QoS adecuadas en dispositivos intermedios.

  - Dar prioridad a los paquetes de voz frente a los de datos, sobre todo en redes inalámbricas.
  - Ubicar en el segmento de red de menor congestión el PBX.

- **Jitter**: técnicamente es la variación en el tiempo en la llegada de los paquetes de voz y se debe a causas distintas como la congestión en la red de datos o la al enviarse los paquetes por distintas rutas. Para reducir su efecto se aconseja la utilización de buffers, también denominados jitter-buffers, donde se almacenarán de forma temporal los paquetes hasta la llegada del más lento, momento en el que se enviarán o reproducirán a intervalos constantes. La unidad de medida empleada para el buffer es el milisegundo, indicando el tiempo de espera o almacenamiento hasta la reproducción o envío de la voz empaquetada. El valor utilizado comúnmente para el buffer es de 100 ms, cuyo incremento repercutirá en el aumento de la latencia total.
- **Eco o reverberación**: se produce por ejemplo cuando se escuchar al emisor mediante unos altavoces y la voz se cuelan nuevamente por el micrófono. Cuando el retardo del eco respecto a la señal original es igual o superior a 10ms, el oído humano es capaz de detectarlo. Para solucionarlo se pueden utilizar dispositivos canceladores de eco que aumentan el tiempo de procesamiento de las señales o utilizar supresores de eco convirtiendo la comunicación de *full-duplex* a *half-duplex* de forma que eviten la comunicación en dos sentidos.
- **Pérdida de paquetes**: puesto que en VoIP suele utilizarse UDP como protocolo de transporte el cual no está orientado a conexión, hay que paquetes que no llegan a su destino, siendo más problemático cuando las pérdidas se producen a ráfagas. Este problema puede agravarse si el nivel de compresión de la voz es alto, ya que puede suponer la pérdida de más paquetes, por tanto habrá que tener en cuenta el codec a utilizar. No se recomienda que su valor supere el 1%, y suele reducirse evitando la transmisión de los silencios que aparecen en las conversaciones.

12.3 ELEMENTOS VOIP

En este apartado se abordan aquellos elementos hardware y software más comunes que podemos encontrar en la implantación de un sistema de telefonía VoIP sobre redes Ethernet. Se han omitido todos aquellos aspectos relativos a las redes de datos, ya que no son objeto de este libro.

12.3.1 REDES DE TELEFONÍA CABLEADAS

Uno de los elementos necesarios y comúnmente utilizados por compañías y organizaciones para las comunicaciones con el exterior, son las redes de telefonía cableadas. En este apartado se exponen la mayoría de ellas, tratando sus aspectos más relevantes.

12.3.1.1 DSL

Las tecnologías DSL (*Digital Subscriber Line* o Línea Digital de Suscriptor) están basadas en la idea de utilizar la RTB para la transmisión de información a alta velocidad. Una variante de estas redes es ADSL (*Asymetric Digital Subscriber Line* o Línea Digital Asimétrica de Abonado) y se llama asimétrica porque, por cuestiones técnicas, la velocidad de transmisión en un sentido es menor que en otro. Como contrapartida, también existen las líneas SDSL (*Symetric Digital Subscriber Line* o Línea Digital Simétrica de Abonado), donde la comunicación se realiza a la misma velocidad en ambos sentidos. Puesto que hoy en día la mayoría de la población dispone en sus casas de una toma telefónica de dos hilos, se plantea toda esa red sin necesidad de instalar otra nueva.

El problema que se plantea consiste en utilizar una red telefónica de baja calidad para transmitir datos a alta velocidad. La solución de ADSL consiste en utilizar circuitos integrados ASP (*Advanced Signal Processor* o Procesador de Señales Avanzado) para eliminar electrónicamente todas las interferencias producidas en la comunicación.

ADSL debe verse como una solución de compromiso, que se instala en los hogares de forma rápida, más que una solución a largo plazo. Hoy en día ya se ha implantado por muchas compañías de comunicaciones y la mayoría de usuarios la utilizan como acceso rápido a Internet.

Las redes ADSL pueden utilizar diferentes protocolos de transporte de datos, como TCP/IP o ATM (*Asynchronous Transfer Mode* o Modo de Transferencia Asíncrono). La arquitectura ATM define un conjunto de protocolos de comunicación que permite la implementación de servicios que requieren una gran velocidad de transmisión. ATM permite la difusión de películas, la videoconferencia de alta calidad, además de todos los tipos de transferencias de información que se utilizan hoy en día.

12.3.1.2 RDSI

La red RDSI dispone de su propio cableado, permitiendo no solo la transmisión de voz, sino de datos, de imagen y sonido en tiempo real, etc. Para permitir diferentes tipos de transmisión, se utiliza la técnica de multiplexación creando canales independientes para ser transmitidos por un único medio. Algunos de estos canales son utilizados para transportar información de control de las comunicaciones. La utilización de canales también permite la contratación de distintas velocidades y capacidades.

Para la instalación de un acceso a RDSI, la compañía telefónica instala un dispositivo denominado NT1 o TR1, el cual se conecta mediante cable de par trenzado a la central de la compañía. Las conexiones del NT1 con las tomas de

pared se realizan con dos pares trenzados, mientras que las conexiones entre las rosetas de pared y los terminales RDSI se realizan con latiguillos de ocho hilos. La Figura 12.3 muestra esta estructura de conexión.

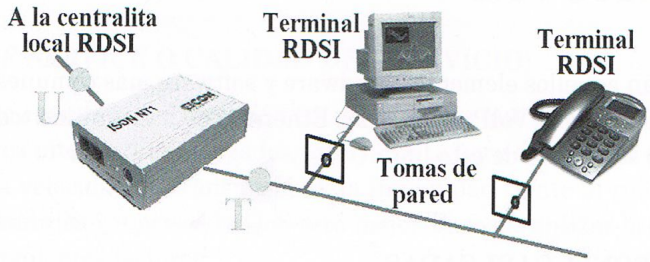


Figura 12.3. *Conexión física RDSI entre el cliente y centralita local. Este ejemplo de conexión se realiza para usuarios que no van a utilizar más de ocho dispositivos para la transmisión*

Ante demandas de más capacidad, la compañía telefónica puede instalar un dispositivo adicional denominado NT2 o TR2 conectado al NT1.

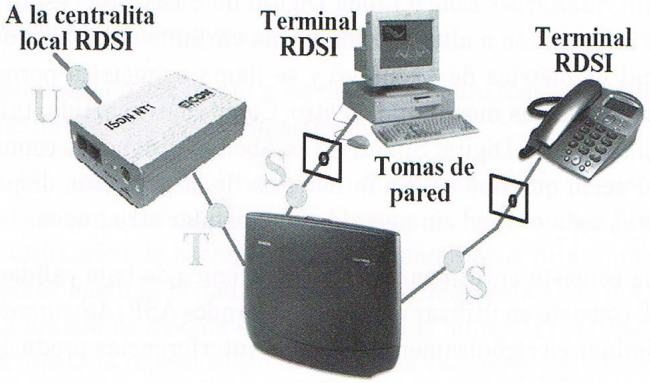


Figura 12.4. *Conexión física RDSI para empresa. Aquí se permite una mayor cantidad de conexiones simultáneas (a través del punto S)*

Cuando se contrata una conexión RDSI, los terminales a utilizar deben ser digitales, aunque también se puede utilizar un dispositivo denominado TA (*Terminal Adapter* o Adaptador de Terminal) para conectar terminales analógicos, realizando la conversión analógico-digital de las señales. La conexión de ordenadores a la RDSI requiere la instalación de un adaptador o módem, además de software complementario, como el driver, protocolos V110, HDLC y X.75, y la librería CAPI (*Common IDSN API* o API Común de RDSI) para que las aplicaciones puedan acceder a la red.

En una conexión de cliente RDSI existen cuatro puntos de referencia básicos a tener en cuenta:

- **U**: es la conexión entre la central RDSI de la compañía telefónica y el NT1. Puede ser un par trenzado de cobre de dos hilos o fibra óptica.
- **T**: es la conexión básica de RDSI que soporta la conexión simultánea de hasta ocho dispositivos digitales.
- **S**: es el punto donde se conectan los terminales digitales específicos de RDSI, con capacidad para más de ocho.
- **R**: es el punto deonde se conectan los terminales que nos son RDSI (analógicos convencionales).

En RDSI se han estandarizado varios tipos de canales lógicos, cada uno de los cuales transmite un determinado tipo de información:

- **A**: canal analógico para transmisión de voz a 4 kHz.
- **B**: canal digital modulado mediante técnica PCM de 64 kbps para voz o datos.
- **C**: canal digital de 8 ó 16 kbps.
- **D**: canal digital de 64 kpbs para señalización interna de RDSI.
- **H**: canal digital de 384, 1536 ó 1.920 kpbs.

El abonado puede disponer de estos canales para su conexión pero, según el estándar, no se permite que éste decida una combinación arbitraria de canales y solo se permiten las siguientes:

- **Acceso básico**: dos canales B más un canal D. También se llama BRI (*Basic Rate Interface* o Interfaz de Tasa Básica).
- **Acceso primario**: este tipo se ha conocido como *líneas alquiladas*, ya que tradicionalmente se han utilizado para la construcción de redes privadas entre sucursales de una misma organización o empresa, aunque también se han utilizado para la interconexión de centrales telefónicas. Ofrecen las siguientes posibilidades:
  - **23 canales B y un canal D**: también denominado T1 y se utiliza en Norteamérica, Japón (también denominado J1) y Corea del Sur. Como técnica de señalización utiliza la *Señalización por Robo de Bit* o *Robbed Bit Signaling*.
  - **30 canales B, uno D y uno de alarma y sincronización**: también denominado E1 y se utiliza en el resto del mundo y por tanto en Europa. Utiliza técnicas de multiplexación para la señalización.
- **Acceso híbrido**: un canal A y un canal C.

Otros sistemas de acceso digital se muestran en la siguiente tabla, donde se aprecian algunas comparativas como el ancho de banda o los canales utilizados.

Tabla 12.2. Otros sistemas de acceso digital

Acceso	Medio de transmisión	Canales	Equivalencia	Ancho de banda (Mbps)	Área Geográfica
T1		24		1,544 Mbps	Norteamérica, Corea del Sur y Japón.
E1		32		2,048 Mpbs	Resto del mundo.
T3	Cable coaxial Enlace de microondas	672	28 T1	44,736 Mbps	Norteamérica, Corea del Sur y Japón.
E3	Cable coaxial	512	16 E1	34,368 Mbps	Resto del mundo.
T4	Cable coaxial Enlace de microondas	4032	168 T1	274,176 Mbps	Norteamérica, Corea del Sur y Japón.
SONET	Fibra óptica			51,840 Mbps-39,813 Gbps	Norteamérica.
SDH	Fibra óptica			51,840 Mbps-39,813 Gbps	Resto del mundo.

12.3.2 REDES DE TELEFONÍA INALÁMBRICAS

12.3.2.1 LMDS

LMDS (*Local Multipoint Distribution System* o Sistema Local de Distribución Multipunto) es un sistema que utiliza el aire como medio de transmisión para la comunicación desde una estación base a los abonados del servicio. Permite la transmisión de voz, datos, Internet y vídeo mediante la emisión de ondas radioléctricas de alta frecuencia (28-40 Ghz), y se suele utilizar para cubrir zonas geográficas donde es difícil el acceso mediante cable. A mayor frecuencia las velocidades son más altas (hasta 8 Mbps), pero la zona de cobertura es menor. Los usuarios necesitan instalar una antena receptora bidireccional y orientada hacia la estación base.

12.3.2.2 GSM

GSM (*Global System for Mobile communications* o Sistema Global para las Comunicaciones Móviles) es un estándar bien definido que utiliza la conmutación de circuitos para la comunicación entre teléfonos móviles y que realiza la transmisión de voz y señalización en formato digital. Para su funcionamiento se utiliza una red compleja de **estaciones base** o **BS** (*Base Station*) que dan cobertura a un área geográfica determinada, denominada **celda** o **célula**. Los terminales de usuario buscan siempre una estación base a la que conectarse utilizando un rango o banda de frecuencia determinado, siendo el más común el comprendido entre 900 MHz y 1800 MHz. La trasmisión de voz se realiza gracias a codificadores-decodificadores de audio o codecs, que digitalizan y comprimen la voz.

La utilización de GSM requiere la inserción de una tarjeta **SIM** (*Subscriber Identity Module* o Módulo de Identidad del Suscriptor) en el terminal, la cual es proporcionada por el proveedor del servicio de telefonía móvil. Esta tarjeta tiene una capacidad determinada y almacena información relativa a la suscripción del servicio y los parámetros necesarios para conectarse a la red, pudiendo también almacenar la agenda de teléfonos.

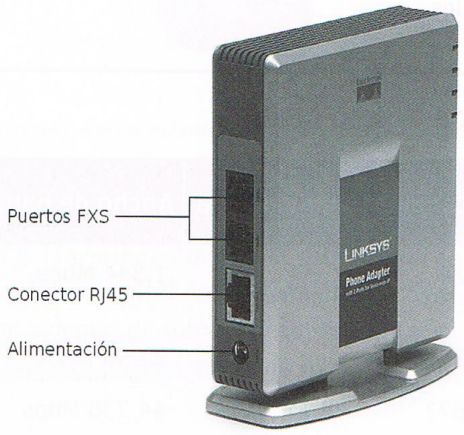


Figura 12.5. *Enlace GSM para VoIP 2N Voiceblue modelo Enterprise. Dispositivo que permite a una red de datos mediante el puerto Ethernet, o los puertos USB el acceso a una red de telefonía móvil GSM permitiendo con este modelo hasta cuatro conversaciones simultáneas*

La información de señalización se realiza mediante ráfagas, como al encenderse, apagarse, recibir o emitir llamadas, de forma que se optimize la utilización de la red. Esta forma de señalización también se utiliza para el envío de **SMS** (*Short Message Service* o Servicio de Mensajes Cortos).

La evolución de este estándar catalogado como 2G (*Second Generation* o de Segunda Generación), ha posibilitado la transmisión de datos mediante conmutación de paquetes gracias al servicio **GPRS** (*General Packet Radio Service*

o Servicio General de Paquetes vía Radio), también conocido como 2,5G. Algunas de las mejoras de GPRS respecto a GSM, es la posibilidad de enviar mensajes multimedia o MMS (*Multimedia Messaging Service* o Servicio de Mensajería Multimedia), o la utilización del estándar abierto WAP (*Wireless Application Protocol* o Protocolo para Aplicaciones Inalámbricas), para que los terminales puedan acceder a aplicaciones y servicios disponibles en Internet, como por ejemplo el correo electrónico.

Avances tecnológicos posteriores han dado lugar a la telefonía móvil 3G (*Third Generation* o de Tercera Generación), donde surgió la tecnología **UMTS** (*Universal Mobile Telecommunications System* o Sistema Universal de Comunicaciones Móviles). UMTS mejora los servicios ofrecidos por generaciones previas, consiguiendo mayores velocidades de transmisión gracias a las altas frecuancias con las que trabaja, mayor calidad de voz con menos interferencias, mecanismos de seguridad más seguros, o mayor facilidad para la utilización de aplicaciones multimedia. Al igual que GPRS, utiliza la conmutación de paquetes para la transmisión de información, y permite la conexión permanente a la red. A pesar de las expectativas creadas para esta tecnología como la televisión móvil o videoconferencia, el principal uso de UMTS es el acceso a Internet desde el propio terminal o desde un ordenador. De su evolución ha surgido el sistema **HSDPA** (*High-Speed Downlink Packet Access* o Acceso para Transmisión de Paquetes en Telefonía Móvil de Alta Velocidad) que alcanza mayores velocidades de transmisión y se considera como el telonero de la cuarta generación de la telefonía móvil.

Tabla 12.3. Tabla comparativa de velocidades en tecnologías móvil

Tecnología	Velocidad
GSM	9800 bps
GPRS	115 Kbps
UMTS	2 Mbps
HSDPA	Hasta 14 Mbps

12.3.3 ATA (*ANALOG TELEPHONE ADAPTOR* O ADAPTADOR TELEFÓNICO ANALÓGICO)

Un adaptador ATA es un dispositivo que permite utilizar teléfonos tradicionales o analógicos sobre una red de datos. Su función es la de convertir las señales analógicas procedentes del terminal a señales digitales utilizada en la red de ordenadores. Su comportamiento es la de un equipo terminal, ya que interpreta y obedece la señalización que le llega (identificador de llamadas, nombre en el display, led de mensajes, etc.). Suele constar de una toma de alimentación, uno o varios puertos FXS para conectar teléfonos analógicos y un puerto RJ45 para conectarse a la red de ordenadores (véase Figura 12.6).

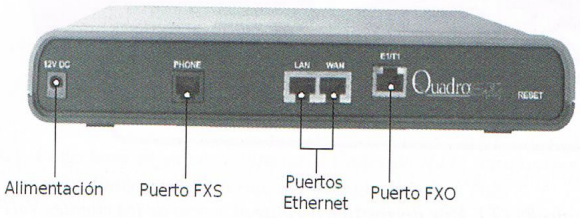


Figura 12.6. *Adaptador ATA Linksys. Las partes más significativas son sus puertos FXS, la toma para alimentación eléctrica y el conector RJ45 hembra para la conexión a la red Ethernet*

12.3.4 GATEWAYS O PASARELAS VOIP

Ya hemos visto que la característica principal de VoIP es poder transmitir voz a través de una red de datos, aunque a veces el destinatario no se encuentra en ella y es necesario el acceso a otro tipo de redes, como la RTC o una red de telefonía móvil. La función de un gateway será precisamente el posibilitarnos el acceso a otras redes, generalmente de carácter público, reduciéndo en ocasiones el coste de las facturas. En una organización o empresa estos dispositivos pueden conectarse al PBX de forma qu todos los usuarios dispongan de acceso otras redes. Podemos distinguir los siguientes tipos de gateways:

- **VoIP-RTC**: realiza el transporte de voz de una red de datos a la RTC. Su funcionamiento es parecido a un ATA aunque no se comporta como tal, ya que no interpreta ni obedece la señalización que le llega, sino que la transporta hasta el terminal para que sea éste último quien la interprete y obedezca. Suele constar de una toma de alimentación, uno o varios puertos FXO para conectarse a los puertos FXS que dan acceso a la RTC (roseta o PTR), al menos un puerto RJ45 para conectarse a la red de datos y, opcionalmente, uno o varios puertos FXS para conectar teléfonos analógicos (véase Figura 12.6).
- **VoIP-GSM**: las llamadas realizadas desde terminales VoIP desde una red de datos a terminales de una red de telefonía móvil, son más costosas que las realizadas entre terminales de telefonía móvil. Estos dispositivos permitirán un ahorro considerable, ya que realiza el transporte de voz de una red de datos a una red de telefonía móvil GSM. Constan de una toma de alimentación, alojamiento para una o varias SIM dependiendo de los canales GSM contratados, al menos un conector RJ45 para su conexión a la red de datos, una o varias antenas GSM y, opcionalmente, pueden disponer de otro tipo de puertos para su gestión. La Figura 12.7 le muestra un escenario de su utilización.

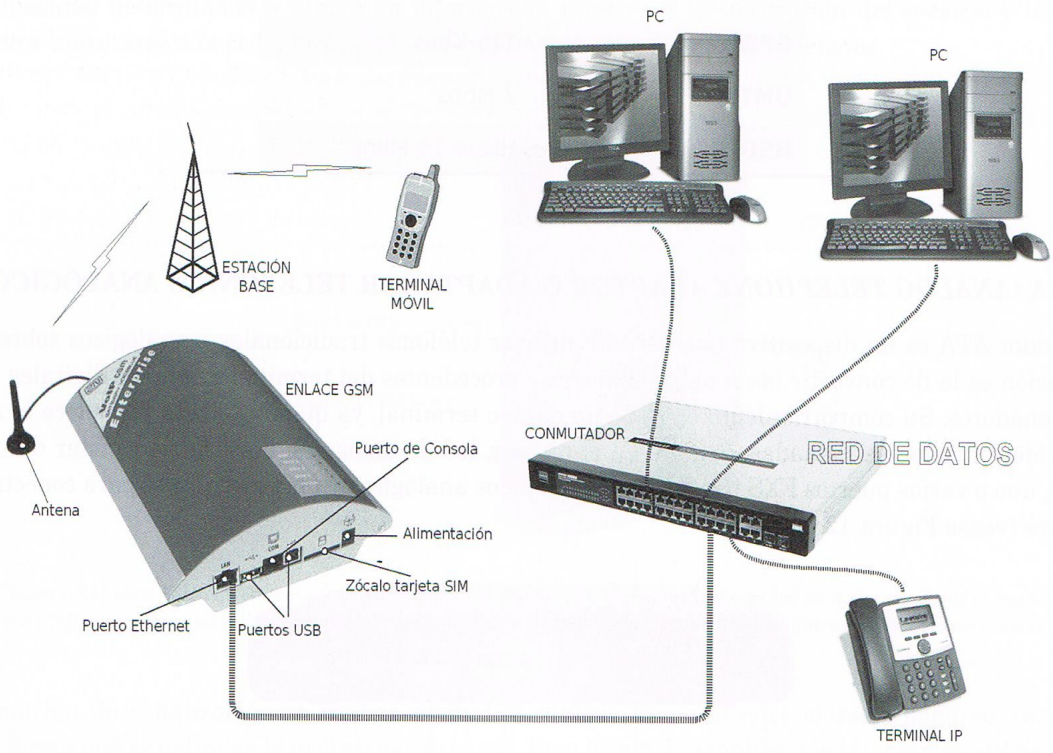


Figura 12.7. *Gateway Epygi modelo QuadroE1/T1. Este dispositivo permite el acceso de los clientes VoIP de una red de datos (puerto Ethernet) o con terminal analógico (puerto FXS), para conectarse a la red de telefonía soportado 30 ó 24 llamadas de forma simultánea dependiendo del tipo de conexión utilizada (E1 o T1)*

12.3.5 TERMINALES

En el mercado podemos encontrar diversos tipos de terminales VoIP, de entre los cuales podemos destacar dos tipos:

- **Terminales USB**: tienen la apariencia de uno terminal tradicional pero no funcionan por sí sólos, y requieren la conexión a un puerto USB de un ordenador conectado a una red de datos. En el ordenador habría que instalar el controlador de dicho dispositivo para su correcto funcionamiento, y conectar el ordenador a la red de datos.
- **Terminales IP**: permiten conectarse directamente a la red de datos, ya que poseen al menos un puerto para establecer la conexión. Los más habituales disponen de un conector hembra RJ45, el cual se conectará mediante un latiguillo a una toma de red de pared. Los modelos que disponen de varios puertos, suelen además desempeñar funciones de conmutador o encaminador, pudiendo tener conectado un ordenador sin necesidad de conectarlo a una toma de red de pared. Los terminales IP necesitan de alimentación eléctrica suministrada mediante la red eléctrica, aunque también puede obtener la energía eléctrica mediante la red Ethernet utilizando tecnología PoE (*Power over Ethernet* o Alimentación sobre Ethernet) o mediante un adaptador de corriente (véase Figura 12.8). Los terminales IP se pueden clasificar en tres categorías (baja, media y avanzada) en función de las características (pantalla, teclas programables, etc.) y prestaciones del mismo. Por tanto podemos encontrarnos terminales de gama baja con funciones tradicionales como la de los terminales analógicos, hasta permitir acceso a un servicio LDAP o HTTP de los terminales de gama avanzada. Estos dispositivos necesitan ser configurados asignándole una dirección IP o utilizando un servicio DHCP. Su configuración dependerá del procedimiento establecido por el fabricante e indicado en su manual de instrucciones.
- **Terminales software**: Los terminales software son programas desarrollados para su ejecución en ordenador u otro dispositivo como una PDA o un terminal de telefonía móvil que tenga acceso a una red TCP/IP. Podemos encontrar diferentes tipos como los **sofphone**, desarrollado para instalarse y ejecutarse mediante el sistema operativo o **webphone**, desarrollado para ejecutarse mediante navegador web. Su ventaja respecto a teléfonos USB o IP estriba en su coste, ya que podemos encontrar software de libre distribución como Ekiga (véase apartado 12.5.2) o freeware como X-Lite de CounterPath (véase apartado 12.5.1), sin necesidad de comprar un terminal hardware o mediante el pago de una o varias licencias. Como inconveniente, señalar la dependencia del dispositivo donde esté instalado, ya que un mal funcionamiento o reinicio influirá a la hora de reanudar la conversación en curso.

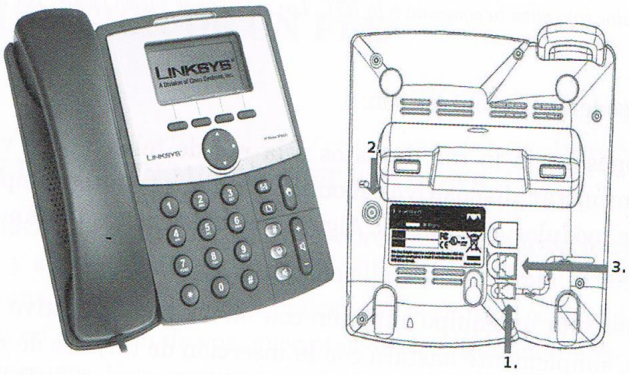


Figura 12.8. *Telefono VoIP Linksys SPA 922. Conectores en su parte inferior: 1.Conexión RJ11 para auricular y micrófono. 2. Conexión para fuente de alimentación externa. 3. Conexión Ethernet PoE*

12.3.6 PBX

La función de un PBX en el ámbito de la tecnología VoIP es similar al de la telefonía tradicional, permitiendo que varios usuarios de una organización o empresa se comuniquen entre sí y compartan conexiones telefónicas para efectuar llamadas hacia el exterior. Suelen incorporar servicios de valor añadido de forma que los usuarios puedan efectuar transferencias de llamadas o por ejemplo la utilización de un servicio de respuestas de voz interactiva o IVR (*Interactive Voice Response* o Servicio de Respuestas de Voz). Podemos decir que un PBX VoIP puede actuar de intermediario entre la red de datos de la organización o empresa y las líneas de telefonía, requiriendo la conexión a ambas. Para conectarse a la red de datos, es necesario que disponga de al menos un interfaz de red acorde a la red utilizada (por ejemplo Ethernet), el cual se podría conectarse a un conmutador o switch. Sin embargo, para conectarse a las redes de telefonía, necesitará de puertos FXO acordes al tipo de líneas contratadas (RTB, RDSI, E1, etc.) para actuar de pasarela. De forma alternativa en vez de actuar de pasarela, podría conectarse a una de ellas, siendo la pasarela la que se conectaría a las líneas contratadas. Si además se desea que el PBX admita la conexión de teléfonos tradicionales o analógicos ejerciendo de ATA, tendrá que disponer de puertos FXS.

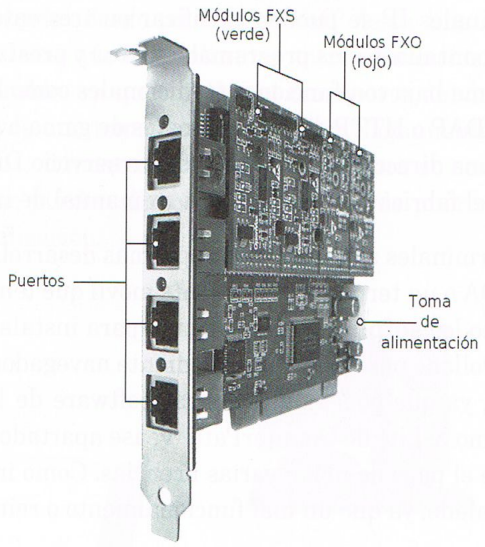


Figura 12.9. *Tarjeta OpenVox A400P. Permite la instalación de módulos FXS en color verde para la conexión de terminales analógicos y módulos FXO en color rojo para la conexión a la RTC. Los módulos se suelen vender por separado*

Los tipos de PBX VoIP que podemos encontrar son:

- **Hardware**: las conexiónes hacia la red de datos y la red de telefonía ya vienen integradas en el propio dispositivo. Podemos encontrar dispositivos modulares, que permiten ampliar el número de conexiones mediante la inserción de módulos adicionales. Algunos modelos incluso están disponibles con un chasis para su instalación en un armario o rack.
- **Software o IP PBX**: necesita un equipo anfitrión con un sistema operativo instalado. Para la conexión del equipo a la red de datos, simplemente bastará con la inserción de tarjetas de red. Para la conexión del equipo a la red telefónica existen en el mercado tarjetas (por ejemplo para bus PCI) con puertos FXO, y también encontramos tarjetas para la conexión de teléfonos analógicos con puertos FXS. Estas tarjetas se insertarán en los slots de expansión situados en la placa base del equipo utilizado como PBX. Algunas de estas tarjetas son modulares como la OpenVox A400P (véase Figura 12.9), permitiendo la inserción de módulos de cada tipo, identificándose en color verde los FXS y en rojo los FXO. La utilización de tarjetas con puertos FXO no son necesarias, ya que el equipo podría estar conectado a un gateway formando una pequeña red. Un ejemplo

de PBX software lo tenemos con 3CX (véase apartado 12.4.1). utilizado en plataformas Microsoft Windows y Asterisk para plataformas GNU/Linux (véase apartado 12.4.2). Un posible escenario podría ser el mostrado por la Figura 12.10.

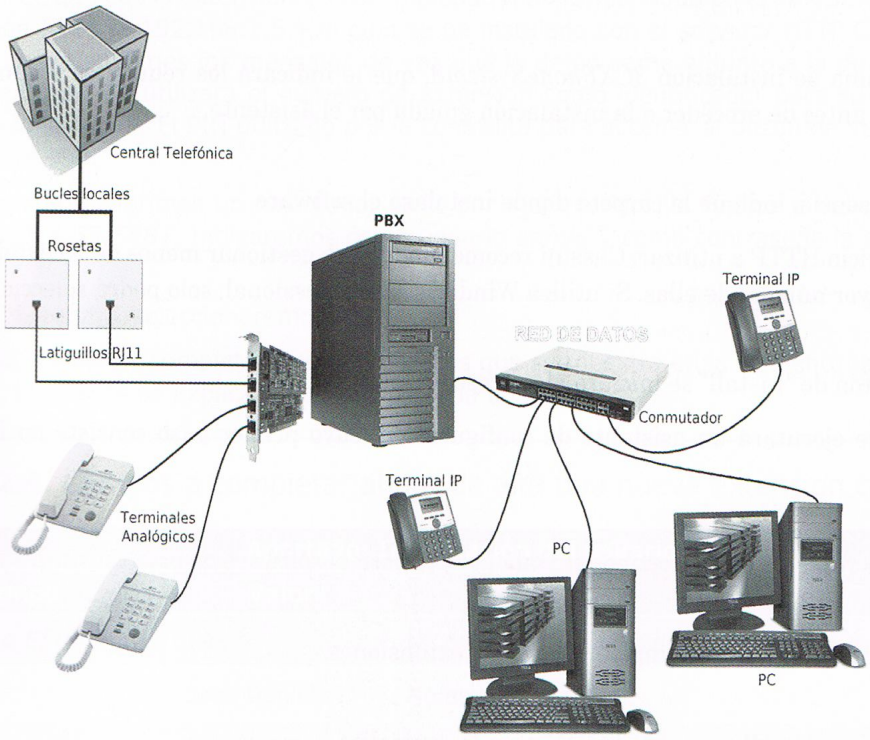


Figura 12.10. *Escenario de telefonía VoIP con PBX. La red de datos es utilizada indistintamente por terminales IP o PCs, los cuales también pueden utilizar la tecnología VoIP mediante softphones. El PBX gestiona las comunicaciones internas y externas mediante tarjetas insertadas en los slots de expansión, algunos de los cuales admiten terminales analógicos además de la conexión a una red de telefonía*

12.4 CONFIGURACIÓN DE UN PBX

12.4.1 CONFIGURACIÓN DE 3CX EN MICROSOFT WINDOWS

Este software permite una fácil instalación de un PBX sobre una plataforma Microsoft Windows y que utiliza el estándar SIP. Su configuración y administración resulta sencilla gracias a una intuitiva interfaz web. De entre sus características comunes a todas sus versiones podemos indicar que permite el control de llamadas, desvío de llamadas, retomar llamadas que aparecen en el buzon de voz, encriptación de voz la cual debe soportarse por los teléfonos, o reinicio remoto de uno o varios equipos. Este producto puede adquirirlo de forma gratuita (véase enlaces de interés) recibiendo por correo electrónico una clave de activación, aunque también dispone de versiones comerciales como la *Small Business*, *Pro* o *Enterprise*. Estas versiones de pago tienen funciones adicionales como por ejemplo, chat de texto, libreta de teléfonos, lista negra de teléfonos no deseados o la integración del correo de voz con Microsoft Outlook (CRM).

Para realizar su instalación se requiere como sistema operativo XP Professional, Vista Business, 2003 Server ó 2008 Server. Además requiere del .NET Framework 2.0 o superior, al menos un puerto si se utiliza IIS (véase capítulo 3) como servidor web, el puerto 5060 disponible para SIP, opcionalmente el puerto 5090 para un túnel seguro, y los puertos 5480, 5482, 5483, 5485, 5486 y 5487 disponibles. La instalación de la versión 8, conlleva seguir los siguientes pasos:

1. Ejecute el programa de instalación *3CXPhoneSystem8*, que le indicará los requisitos a cumplir y una serie de recomendaciones antes de proceder a la instalación guiada por el asistente.
2. Tras aceptar la licencia, indique la carpeta donde instalará el software.
3. Seleccione el servicio HTTP a utilizar: Cassini recomendado para gestionar menos de 25 extensiones o IIS para la gestión de un mayor número de ellas. Si utiliza Windows XP Professional, solo podrá seleccionar Cassini.
4. Tras pulsar el botón de "Install" se iniciará el proceso de instalación.
5. Posteriormente se ejecutará un asistente de configuración, cuyo primer paso consiste en indicar el idioma de configuración.
6. Seleccione "Crear Nueva Central" cuando instala por primera el software de esta centralita.
7. Indique el número de dígitos que empleará para las extensiones.
8. Establezca una dirección IP o nombre FQDN para la centralita.
9. Configure los datos correspondientes al servidor SMTP y la dirección de correo utilizada como remitente para el envío de mensajes de voz.
10. Indique un nombre y una contraseña para el administrador de la centralita.
11. Posteriormente debe crear al menos una extensión, indicando además de los datos personales de la persona a la que asignará la extensión, su e-mail, un identificador y contraseña de autenticación y un PIN para los mensajes de voz. Opcionalmente puede introducir la dirección MAC del teléfono asociado a la extensión así como el modelo utilizado. Finalmente indique la interfaz de red de la centralita a la que el teléfono está conectado y pulse sobre el botón "Agregar".
12. Asigne una extensión a la figura del operador, el cual recibirá las llamadas entrantes. Indique también la extensión a marcar por los usuarios cuando quieran recibir los mensajes de voz.
13. Opcionalmente puede indicar los datos de su proveedor VoIP, o puede omitir este paso (Skip).
14. Para finalizar el proceso de instalación, 3CX crea una base de datos con toda la configuración y, opcionalmente, le permite el registro para obtener información de soporte y sobre dispositivos VoIP.

Para administrar la centralita, si instaló el servidor HTTP de 3CX Cassini, debemos utilizar un navegador web e indicar como URL *http://Servidor_PBX:5481*. En el caso de utilizar IIS como servidor HTTP, indicaremos *http://Servidor_PBX/Management*. En ambos casos como *Servidor_PBX* indicaremos el nombre (FQDN) o dirección IP del equipo que tiene el equipo con el software PBX 3CX. El ejemplo 12.1 le expone un ejemplo de utilización de esta centralita para realizar una operación habitual, la creación de una extensión.

EJEMPLO 12.1

Se desea dar de alta con la extensión 195 al empleado *Juan Daniel Roda* en el PBX 3CX de la compañía, cuya dirección IP es la 192.168.1.5 y el cual se ha instalado con el servidor HTTP Cassini del propio de 3CX. Se desea enviarles los mensajes de voz que le dejen como adjunto a la dirección de correo *jdroda@gmail.com*. Se utilizará el número de extensión como identificador para su autenticación, y como contraseña *fritilla*. El PIN utilizado por la centralita para acceder al buzón de voz y escuchar los mensajes es el 999.

Para gestionar 3CX, abrimos un navegador web, por ejemplo Mozilla Firefox e indicamos como URL *http://192.168.1.63:5481*. Indicaremos como usuario *admin* y como contraseña la establecida en la instalación de 3CX.

En el menú "Agregar", seleccionaremos "Extensión".

En la pestaña "General" completaremos los campos que se muestra en la siguiente tabla y que ilustra la Figura 12.11, donde se explica la función de cada uno.

Tabla 12.4. Campos a completar al dar de alta una nueva extensión con 3CX

Apartado: Información del usuario		
Campo	**Valor**	**Función**
Número de Extensión	193	Nº de extensión asignada al usuario.
Nombre	Juan Daniel	Nombre de usuario.
Apellido	Roda	Apellido del usuario.
Dirección de E-mail	jdroda@gmail.com	Dirección de *e-mail* para entrega de correos de voz y faxes.
Apartado: Autenticación		
Campo	**Valor**	**Función**
ID	195	Identificador de usuario para autenticarse en la centralita.
Contraseña	fritilla	Contraseña del usuario para autenticarse en la centralita.
Apartado: Configuración de correo de voz		
Campo	**Valor**	**Función**
Habilitar correo de voz	Enabled	Habilita las opciones relativas a la utilización de un buzón de voz para escuchar los mensajes que nos dejen.
Reproducir ID de persona que llamó	-	Permite reproducir el identificador del emisor del mensaje de voz, antes que el propio mensaje.
Mencionar fecha/ hora del mensaje		Permite reproducir la fecha y hora antes de escuchar el mensaje de voz.
Número de PIN		Se indica el PIN para acceder al buzón de voz.
Opciones de E-mail		Permite escoger la forma en la que se enviarán los mensajes de voz.

Pulsamos el botón "Aplicar" y "Aceptar" para hacer efectiva el alta de la extensión.

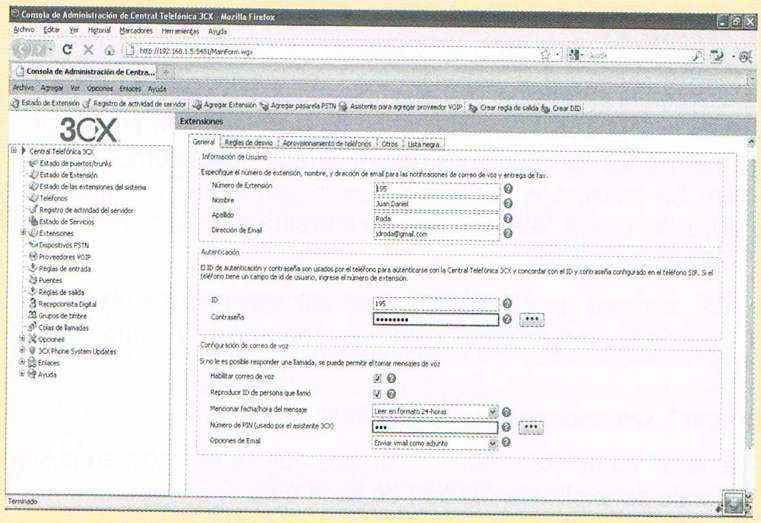


Figura 12.11. Ejemplo de creación de una extensión con el PBX software 3CX

12.4.2 CONFIGURACIÓN DE ASTERISK CON FREEPBX EN GNU/LINUX

Asterisk es software Open Source bajo licencia GPL desarrollado por Mark Spencer, fundador de la empresa Digium. Este software permite la creación de un PBX de estructura modular, siendo posible activar o desactivar aquellos módulos que nos interesen utilizar así como la instalación de nuevos módulos (véase tabla 12.5). Asterisk además de soportar las funcionalidades de una centralita tradicional, posibilita entre otras cosas la realización de transferencias, reproducción d música ante esperas, gestión de extensiones, gestión de buzones de voz, realización de desvíos de llamadas, redirección desde sistemas de mensajería a teléfonos o usuarios VoIP (servicio *follow-me*), interacción automática con usuarios mediante respuestas grabadas (IVR), realización de conferencias donde sea el usuario el que quiera participar (*meet-me*) o gestión de colas de llamadas.

Tabla 12.5. Módulos que componen Asterisk y su funcionalidad

Módulo	Funcionalidad
Core	Es el núcleo del sistema, como si de un sistema operativo se tratara, cuya función principal es la de realizar las operaciones básicas, permitiendo también la instalación, activación y desactivación de módulos.
Recursos	Son módulos que añaden funcionalidades complementarias al núcleo.
Canales	Son módulos que permiten utilizar diferentes protocolos de señalización como IAX, SIP o H.323.
Aplicaciónes y funciones	Son módulos que permiten la configuración de Asterisk.
CDR	Es software que permite generar información que se almacena en un registro telefónico para su posterior gestión.
Codecs	Son módulos que permiten la codificación/decodificación de la voz, así como su compresión.
Formatos	Es software que permite a Asterisk la gestión de diversos formatos de vídeo y audio.

Para su funcionamiento, Asterisk utiliza los denominados **canales** para gestión de las llamadas entrantes o salientes, provenientes o con destino a telefonía de naturaleza analógica, digital o VoIP. Los canales más importantes que soporta son SIP e IAX2 para VoIP, Zap para líneas ananlógicas y digitales, y mISND para RDSI. Su comportamiento lógico ante una llamada que entra o sale a través de sus canales se define mediante lo que se denomina **dialplan**. Un dialplan se compone de varios **contextos**, que permiten diferenciar la ubicación de las llamadas, de forma que por ejemplo se puedan aplicar políticas distintas de seguridad según su procedencia. Cada contexto está formado por un conjunto de **extensiones**, las cuales podemos definir como una serie de órdenes o aplicaciones que se ejecutarán para controlar el comportamiento de las llamadas y del propio sistema. Un ejemplo de orden sería *dial* que permite realizar una llamada saliente.

Actualmente Asterisk dispone de dos versiones la 1.4 y la 1.6, ésta última con capacidad para la transmisión también de vídeo. La instalación de cualquiera de sus versiones se puede realizar mediante dos procedimientos:

- **Sobre una distribución previamente instalada**: consiste en utilizar un equipo con una distribución GNU/Linux ya instalada antes de proceder a su instalación, la cual para usuarios usuarios poco expertos puede resultar compleja y cuyos pasos se resumen a continuación:
  - Descarga de paquetes: al menos se requiere la descarga del paquete *asterisk*, si se utilizan tarjetas analógicas el paquete *zaptel* actualmente denominado *dadhi*, *asterisk-addons* para disponer de aplicaciones extra de asterisk, *asterisk-sound* para disponer de los sonidos estandar, y finalmente si se utilizan tarjetas digitales *libpri*. Con el paquete *zaptel* es recomendable utilizar los ficheros cabecera del núcleo y las librerías *newt* y *zttool*.
  - Es necesario tener instaladas las herramientas *gcc*, *make*, *openssl* y la librería *libncurses5-dev*.
  - Compilar cada uno de los paquetes.
  - Configuración de los canales (SIP, IAX y/o H.323).
  - Configuración de las conexiones analógicas y/o digitales.
- **Mediante la instalación de una distribución precompilada**: consiste en descargar software a modo de sistema operativo (generalmente una ISO) que incorpora a su vez el software de Asterisk, no siendo necesarios grandes conocimientos para su instalación, quedando el PBX listo para utilizarse y con una configuración por defecto. La mayoría de los disponibles son de código abierto como DebPBX o AsteriskNow y se gestionan a través de una interfaz gráfica.

Gracias al código abierto, se han desarrollado aplicaciones independientes a Asterisk, que se intengran con él y permiten ampliar su funcionalidad, como la plataforma de tarificación **A2Billing**, gestionada mediante interfaz web y utilizada por ejemplo en la facturación de locutorios y cibercafés. Otra aplicación muy conocida y ampliamente utilizada es **Avantfax**, que gracias al paquete *hylafax* permite la gestión de faxes mediante web, su descarga en formato PDF o la utilización del correo electrónico para su reenvío.

Asterisk permite una gestión en modo orden mediante su intérprete de órdenes CLI (*Command Line Interpreter*) y la edición de ficheros de configuración. Puesto que no todos los usuarios tienen la misma desenvoltura en este tipo de entorno, se desarrollaron una serie de aplicaciones web para su administración, siendo la más conocida y utilizada la aplicación GNU/GPL **FreePBX**.

Puesto que para el desarrollo de FreePBX se utilizó Perl y PHP, se requiere la instalación del intérprete PHP para su funcionamiento, un servidor web como Apache para proporcionar las páginas demandadas por los administradores de Asterisk y el sistema gestor de bases de datos MySQL. FreePBX almacena la información de las configuraciones realizadas en bases de datos MySQL, reescribiendo desde estas los ficheros de configuración de Asterisk. Puesto que Asterisk permite la gestión de buzones de voz, se requiere un servidor de correo (véase capítulo 6 y 7) como Sendmail para asociar los mensajes de voz a cuentas de correo. Para su óptimo funcionamiento, se requiere una correcta configuración de Apache (véase capítulo 3), PHP, Sendmail y MySQL.

La instalación de Asterisk no es objeto de este libro y se expone un ejemplo de la utilización de su interfaz web FreePBX para crear una extensión SIP sobre una distribución precompilada DebPBX.

FreePBX viene acompañado de un conjunto de módulos (véase tabla 12.6) para establecer una configuración básica de Asterisk, los cuales también son descargables desde Internet. Existen otros módulos que permiten administrar otros aspectos de Asterisk que los módulos básicos no cubren.

Tabla 12.6. Módulos básicos de la aplicación de administración web de Asterisk, FreePBX

Módulo	Función
Adminstrators	Gestiona los permisos para usuarios de FreePBX.
Extensions	Gestiona las extensiones.
Feature Codes	Gestiona características y/o aplicaciones que vienen configuradas por defecto.
General Settings	Gestiona los parámetros globales o generales del PBX.
Outbound Routes	Gestiona las llamadas salientes, indicando la ruta a seguir según el patrón al que se ajusten.
Trunks	Gestiona la conexión con el exterior, como por ejemplo la de canales RDSI.
Inbound Routes	Gesitiona según los parámetros indicados, las llamadas entrantes al PBX.
Zap Channel DIDs (Direct Inward Dialing)	Gestiona la asignación de números de teléfono (DID) a los puertos de la tarjeta analógica para identificar la línea analógica de la llamada entrante.
Music On Hold	Gestiona la música en espera.
System Recordings	Gestiona las grabaciones realizadas o descargadas de forma personalizada.

Una operación básica como la creación de una extensión mediante FreePBX no requiere la instalación de módulos adicionales, ya que el módulo *Extensions* viene instalado por defecto. Para conocer los pasos a realizar, consulte el ejemplo que a continuación se expone.

EJEMPLO 12.2

Se desea dar de alta a la empleada Francisca Curri en el PBX Asterisk de la compañía, cuya dirección IP es la 192.168.1.5, instalado mediante una distribución precompilada denominada DebPBX. La extensión que se le ha asignado es la 193 y, por tanto, su cuenta SIP es la 193@192.168.1.5, a la que se ha establecido la contraseña *currita*. Los mensajes de voz se enviarán al correo electrónico *fcurri@gmail.com* para su posterior escucha y cuya contraseña coincide con el de la extensión. El servidor dispone de la interfaz web FreePBX para la administración de Asterisk.

Para acceder a la interfaz gráfica de administración de Asterisk, FreePBX, necesitamos abrir un navegador e indicamos como URL la siguiente:

```
http://192.168.1.5/admin
```

Ingresamos el usuario y contraseña de administrador, que por defecto en DebPBX son:

```
root
debpbx
```

De entre los menús de la izquierda, seleccionamos la opción "Extensions" del menú "Basic" en la pestaña "Setup".

Seleccionamos de la lista desplegable "Device" el tipo de dispositivo a utilizar según el protocolo de señalización a utilizar, en este caso escogeremos "Generic SIP Device" y pulsaremos el botón "Submit".

A continuación hay que completar los campos del formulario para dar de alta la extensión del usuario (véase Figura 12.12).

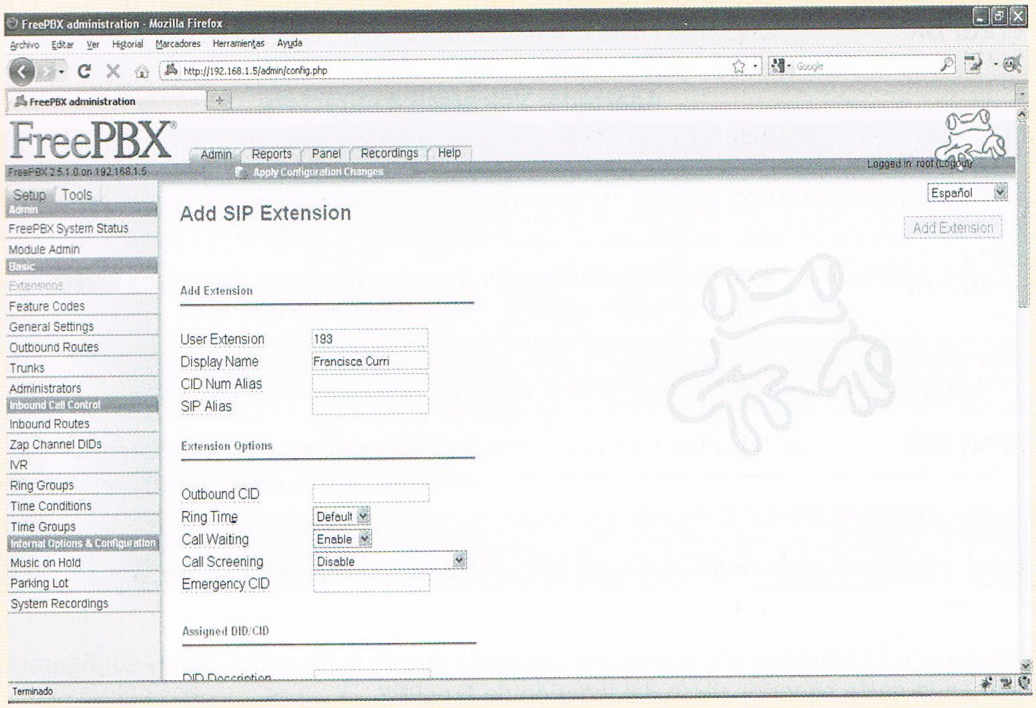


Figura 12.12. *Ejemplo de creación de una extensión con la interfaz web FreePBX para el PBX software Asterisk*

Rellenaremos los campos que se muestra en la siguiente tabla, donde se explica la función de cada uno.

Tabla 12.7. Campos a completar al dar de alta una nueva extensión con FreePBX

Apartado: Add Extensions		
Campo	**Valor**	**Función**
User Extension	193	Nº de extensión asignada al usuario.
Display Name	Francisca Curri	Nombre de usuario a mostrar.
Apartado: Device Options		
Campo	**Valor**	**Función**
Secret	currita	Contraseña de acceso a la cuenta SIP.

Pulsamos el botón "Submit" de la parte inferior del formulario.

Para editar la extensión y añadir los parámetros relativos al buzón de voz, pulsamos en la parte derecha sobre la extensión recientemente creada "Francisca Curri <193>". Completaremos los campos indicados en la tabla 12.8 y finalmente pulsaremos el botón "Submit".

Tabla 12.8. Campos a completar en una extensión con buzón de voz con FreePBX

Apartado: Voicemail & Directory		
Campo	**Valor**	**Función**
Voicemail Password	currita	Contraseña de acceso al buzón de voz para escuchar los mensajes.
Email Address	fcurri@gmail.com	Dirección de correo electrónico donde se enviarán los mensajes de voz.
Email Attachment	Yes	Permite adjuntar al correo electrónico el mensaje de voz.
Play CID	Yes	Permite reproducir el identificador del emisor del mensaje de voz, antes que el propio mensaje.
Play Envelope	Yes	Permite reproducir la fecha y hora antes de escuchar el mensaje de voz.

Las operaciones realizadas no tendrán validez hasta que se pulse sobre "Apply configuration changes", situado en la parte superior cerca del logotipo de FreePBX.

12.5 CONFIGURACIÓN DE UN CLIENTE VOIP

12.5.1 CONFIGURACIÓN EN MICROSOFT WINDOWS

X-Lite es un softphone que, además de efectuar llamadas mediante el protocolo SIP, permite realizar videoconferencias. Dispone de un libro de contactos personales y registra en un historial las llamadas recibidas y efectuadas. La conexión de teléfonos USB o de auriculares, no suele requerir configuración adicional. Su instalación no presenta dificultad alguna, ya que su asistente le guiará durante dicho proceso. Su interfaz es muy intuitiva y se distinguen las siguientes partes (véase Figura 12.13):

- **Display and Dialpad**: situado en la parte central, contiene en la parte superior botones de menú, minimizar y ocultar en la barra de tareas. Más abajo encontramos una pantalla donde se muestra información de la llamada efectuada o recibida. En la parte inferior dispone de un teclado de marcación, controles de volumen para el micrófono y altavoz o auricular, teclas de tono y finalización de llamada, y teclas adicionales para autorespuesta, autoconferencia, no molestar o conferencia.
- **Video Drawer**: permite establecer conversaciones de vídeo, pudiéndose realizar ajustes previos así como detener o iniciar el envío de vídeo. Se despliega en la parte izquierda de esta aplicación al pulsar sobre la flecha situada y que apunta también hacia la izquierda.
- **Calls & Contacts Drawer**: permite configurar la disponibilidad del usuario, gestionar los contactos mediante la pestaña "Contacts" y consultar un histórico de llamadas mediante la pestaña "Calls". Se despliega en la parte derecha al pulsar sobre la flecha situada y que apunta hacia dicha dirección.



Figura 12.13. *Softphone para Microsoft Windows X-Lite. Se pueden apreciar las distintas partes de esta herramienta, especialmente el "Call & Contacts" donde se distingue el contacto Curri, a la que aún no se le ha asignado un grupo. En el display se puede observar que el usuario 195 se ha conectado satisfactoriamente al PBX*

Antes de configurar un cliente debe establecer los dispositivos de audio y vídeo que utilizará. Seleccione "Options..." del menú y acceda al apartado "Devices", donde puede escoger mediante listas desplegables la cámara, los auriculares con micrófono, un teléfono manos libres e incluso el volumen del "ring" de llamada que quiere utilizar y del que dispone su equipo. Para configurar un cliente VoIP después de ejecutar X-Lite, siga los siguientes pasos:

1 Pulse sobre el botón de menú o el botón derecho del ratón sobre la pantalla y seleccione "SIP Account Settings...".

2 En el cuadro de diálogo se muestran las cuentas creadas, su estado, el dominio, así como el usuario y nombre mostrado. Pulse sobre el botón "Add" para añadir una cuenta nueva.

3 En la pestaña "Account", deberá proporcionar los siguientes datos (véase Figura 12.14):

- **Display name**: es el nombre que se mostrará en la pantalla de X-Lite.
- **User name**: es la cuenta de usuario SIP.
- **Password**: contraseña del usuario cuya cuenta se ha indicado en "User name".
- **Authorization name**: aunque puede no ser requerida, se suele indicar la misma que en "User name".
- **Domain**: se indica el dominio o dirección IP del servidor VoIP.
- **Register with domain and receive incoming calls**: se suele marcar, desmarcándose en caso de que el servidor VoIP no acepte llamadas entrantes.
- **Set outbound via**: se selecciona si el tráfico va a ir dirigido a un proxy o si se va a realizar a través de un dispositivo del dominio, indicándose en cada caso su dirección IP o el nombre correspondiente.

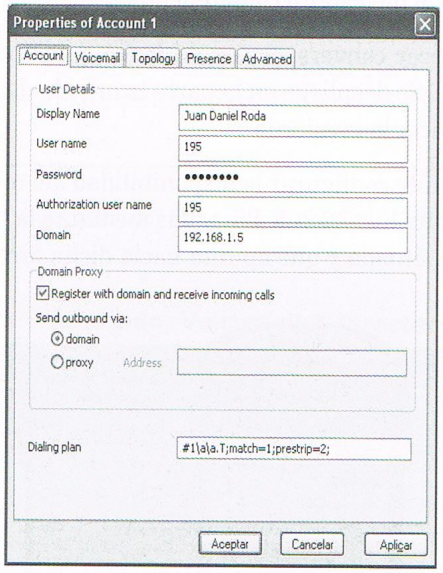


Figura 12.14. *Ejemplo de configuración de una cuenta con el softphone Ekiga*

Para efectuar una llamada, despliegue el "Calls & Contacts Drawer" (véase Figura 12.13). En la pestaña "Contacts" puede desplegar la lista también denominada "Contacts" y seleccionar "Add Contact...", que le mostrará un cuadro de diálogo para introducir los datos del nuevo contacto, siendo los más básicos los siguientes:

- **Name**: se indica el nombre y apellidos del usuario.
- **Display as**: se indica el nombre a mostrar en la pantalla de X-Lite.
- **Group**: permite incluir al nuevo contacto dentro de un grupo facilitando la organización de los contactos.
- **Contact methods**: se selecciona el medio que utilizaremos para contactar con dicho contacto y se indica el teléfono o dirección.

EJEMPLO 12.3

El empleado Juan Daniel Roda ha sido dado de alta en el PBX 3CX de la compañía en la que trabaja y cuya dirección IP es la 192.168.1.5. La extensión que se le ha asignado es la 195 y la contraseña *fritilla*. Se desea configurar su softphone X-Lite instalado en su ordenador para que pueda efectuar llamadas a nivel interno.

Una vez abierto el programa, se despliega el menú (flecha hacia abajo) y seleccionamos "SIP Account Settings...".

Pulsamos sobre el botón "Add" y en la pestaña "Account" indicamos sus datos:

- Display Name: Juan Daniel Roda
- User name: 195
- Password: fritilla
- Authorization user name: 195
- Domain: 192.168.1.63
- Register with domain and receive incoming calls: marcado
- Send outbound via: domain

Pulsamos el botón "Aceptar" y cerramos con "Close" la ventana de cuentas. Si el registro en el PBX es correcto mostrará en la pantalla los siguientes mensajes (véase Figura 12.13):

```
Ready
Your username is: 195
```

12.5.2 CONFIGURACIÓN DE UN CLIENTE EN GNU/LINUX

Ekiga es un softphone de software libre, disponible para GNU/Linux y con versión beta para sistemas Microsoft Windows. Permite videoconferencias y envío de mensajes instantáneos, soportando vídeo y sonido de alta calidad. Puede trabajar con dispositivos hardware y software propietario siempre y cuando utilicen los estándares H.323 y SIP. También puede gestionar una agenda de contactos local y remota, proporcionando soporte para autenticación mediante LDAP. Su instalación es guiada por un asistente y apenas requiere la intervención del usuario.

Su interfaz gráfica consta de los siguientes elementos (véase Figura 12.15):

- **Barra de menú**: situado en la parte superior, mediante "Chat" nos permite acceder a diversas opciones relacionadas con las llamadas (llamar, añadir contacto, suspender sonido, etc.), con "Editar" nos permite gestionar las cuentas y preferencias de la aplicación, con "Ver" muestra u oculta los diferentes elementos, así como modificar la ventana de la aplicación y con "Ayuda" muestra información relevante de Ekiga y da acceso a las páginas de ayuda.
- **Barra de dirección**: situado bajo el menú, permite indicar la URI del destinatario para efectuar la llamada o videoconferencia. En su parte derecha se situan los botones de llamar y colgar.
- **Panel de contactos, teclado e histórico**: mediante tres pestañas nos permite la gestión de contactos que se pueden organizar en grupos, utilizar un teclado numérico para marcar el número de teléfono del destinatario y visualizar el histórico de llamadas entrantes y salientes.
- **Panel de llamada**: es opcional y permite configurar las opciones de audio y vídeo durante la llamada.
- **Barra de disponibilidad**: permite hacer público a otros usuarios nuestra disponibilidad.

- **Barra de estado**: muestra al usuario diversos mensajes en función del estado en que se encuentra la llamada, como el ancho de banda utilizado o la disponibilidad del destinatario.

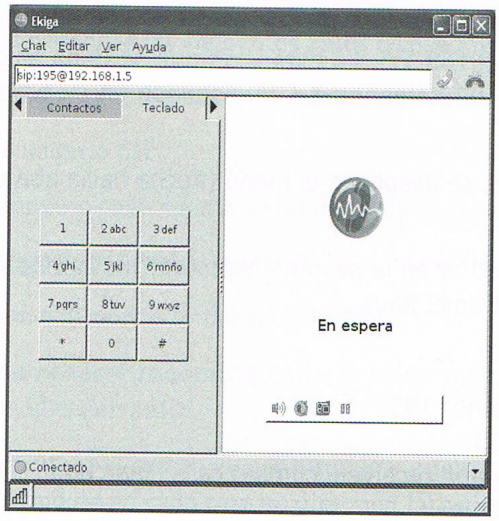


Figura 12.15. *Softphone multiplataforma Ekiga. Se pueden apreciar los distintos paneles que lo conforman, así como el resto de sus elementos. En la barra de dirección se ha indicado una URI para contactar con el usuario 195@192.168.1.5*

Previo a su configuración, se deben establecer los dispositivos a utilizar para las llamadas, como los de audio (altavoces o auriculares y micrófono) y vídeo (webcam). Seleccione la opción "Preferencias" del menú "Editar" y acceda al subapartado "Dispositivos" del apartado "Sonido" y posteriormente "Vídeo", para establezcer los dispositivos que tiene instalados en su equipo.

La configuración de un cliente VoIP mediante SIP con esta aplicación requiere seguir los siguientes pasos (véase ejemplo 12.4):

1 Seleccione la opción "Cuentas" del menú "Editar".

2 Se mostrará una ventana con las cuentas disponibles, el estado en el que se encuentran y si tienen correo de voz. Mediante la casilla de verificación situada a la izquierda de cada cuenta, se podrán marcar aquellas que se deseen tener activas. Para crear una nueva cuenta, acceda al menú "Cuentas" y seleccione la opción "Añadir una cuenta SIP", en la que deberá completar los siguientes parámetros (véase Figura 12.16):

- **Nombre**: se indica el nombre de la cuenta para distinguirla de las demás.
- **Servidor de registro**: se indica la dirección IP o el enombre del servidor VoIP.
- **Usuario**: indique el nombre del usuario registrado en el servidor VoIP.
- **Usuario para autenticación**: si es diferente del parámetro anterior, el parámetro "Usuario" se utilizará para controlar la identidad de salida para la cuenta que estamos añadiendo.
- **Contraseña**: teclee la contraseña del usuario que se autenticará en el servidor de registro.
- **Tiempo de expiración**: se establece el tiempo tras el cual la autenticación debe realizarse nuevamente.
- **Activar cuenta**: esta casilla de verificación permite tener disponible la cuenta o no.

3 Acepte y cierre las ventanas.

Para efectuar una llamada a otro usuario, indique en la ventana la URI de la persona con la que quiere contactar, siguiendo el formato *sip:usuario@servidor*. Para llamar a un teléfono utilice el formato *sip:NúmeroDeTeléfono* o *+CPNúmeroDeTeléfono*, donde CP es el código del país al que pertenece el *NúmeroDeTeléfono*. Posteriormente pulse sobre el botón de llamada.

EJEMPLO 12.4

La empleada Francisca Curri más conocida como Curri, ha sido dado de alta en el PBX Asterisk de la compañía en la que trabaja, y cuya dirección IP es la 192.168.1.5. La extensión que se le ha asignado es la 193 y, por tanto, su cuenta es la 193@192.168.1.5 a la que se ha establecido la contraseña *currita*. Se desea configurar el software Ekiga instalado en su ordenador para que pueda efectuar llamadas, cuya prueba la realizará con Juan Daniel Roda del ejemplo 12.3, el cual se añadirá a la libreta de contactos perteneciente al grupo *local*.

Una vez en ejecución el programa, se despliega el menú "Editar" y seleccionamos "Cuentas". Seleccionamos "Añadir una cuenta SIP" del menú cuentas y establecemos los parámetros de los siguientes campos (véase Figura 12.16):

- Nombre: Francisca Curri
- Servidor de registro: 192.168.1.5
- Usuario: Curri
- Usuario para autenticación: 193
- Contraseña: currita
- Tiempo de expiración: 3600 (establecido por defecto)
- Activar cuenta: marcado

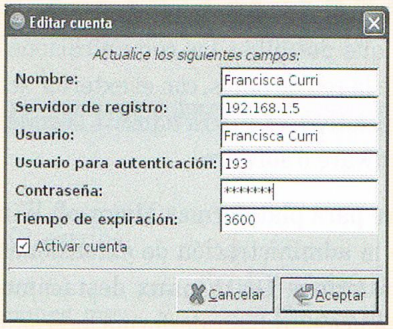


Figura 12.16. *Softphone multiplataforma Ekiga*

Pulsamos sobre el botón "Aceptar" y posteriormente "Cerrar" para finalizar la configuración de la cuenta.

Para añadir a la libreta de contactos a *Juan Daniel Roda*, accedemos al menú "Chat" y seleccionamos "Añadir contacto" e indicamos:

- Nombre: Juan Daniel Roda.
- Direccion: sip:195@192.168.1.5.
- Poner los contactos en grupos: tecleamos *Interno* en el cuadro de texto situado a la izquierda del botón "Añadir", el cual pulsaremos posteriormente.

Finalmente pulsaríamos el botón de "Aceptar", y en el panel de contactos desplegaríamos el grupo *Interno* de la *Lista local*, seleccionando a *Juan Daniel Roda* y pulsando sobre el botón de llamada.

RESUMEN DEL CAPÍTULO

En la telefonía tradicional la transmisión de la voz se realiza mediante señales en formato analógico. Los usuarios se conectan a las centralitas de sus proveedores gracias a un bucle local. A su vez las centralitas se unen entre sí mediante líneas troncales para cubrir determinadas áreas geográficas. La aparición de la red RDSI, permitió la transmisión de voz y datos mediante señales en formato digital.

A nivel empresarial, se han utilizado centralitas o PBX para la gestión de comunicaciones internas entre extensiones, y además con el exterior, incluidas las redes de telefonía móvil.

VoIP utiliza las infraestructuras y protocolos de una red TCP/IP, para la transmisión de voz en forma de paquetes. Para su funcionamiento requiere la codificación y compresión de la voz, utilizar protocolos de control y transporte (NTP, RTP y RTCP), establecer sistemas de señalización como H.323 y SIP, y emplear un sistema de direccionamiento para la localización del destinatario y el origen en una conversación. Para garantizar su éxito se necesitan controlar ciertos factores, como el ancho de banda, latencia, jitter, eco y pérdida de paquetes.

Los elementos hardware más comunes que pueden intervenir en un escenario VoIP son: redes de telefonía cableada com DSL o RDSI, redes de telefonía inalámbrica como LMDS o GSM, adaptadores para teléfonos analógicos (ATA), gateways para el acceso a redes de carácter público (RTC o GSM), terminales (USB, IP o software) y el PBX.

El PBX VoIP es el dispositivo que posibilita las comunicaciones internas entre los empleados de una empresa u organización a través de la red de datos, con el exterior actuando de pasarela o bien conectándose a una y pudiendo actuar como dispositivo ATA para admitir la conexión de terminales analógicos. Un PBX VoIP puede ser de naturaleza hardware o sofware.

De entre los PBX VoIP software para plataformas Microsoft Windows distinguimos 3CX, con ediciones gratuita y comercial que permite la administración de extensiones y teléfonos SIP mediante un servicio HTTP (IIS o Cassini). Para plataformas GNU/Linux destacamos Asterisk es de carácter modular y puede instalarse sobre una distribución, o bien de forma precompilada como por ejemplo con DebPBX o AsteriskNow. Asterisk se puede administrar mediante interfaz web con FreePBX (requiere Apache, MySQL y PHP), utilizar un sistema de tarificación con A2Billing o la gestión de faxes con Avantfax.

Como terminales VoIP software o softphones, destacar X-Lite para plataformas Microsoft Windows, que utiliza el protocolo SIP. Consta de un Display y un Dialpad donde se ve el estado de la llamada y se puede marcan un número, un Video Drawer utilizado para las conversaciones de vídeo, y un Calls & Contacts Drawer para la gestión de contactos e histórico de llamadas. Para plataformas GNU/Linux, entre otros, encontramos Ekiga, que soporta H.323 y SIP. Dispone de barra de menú para llevar a cabo las operaciones posibles, una barra de dirección para indicar las URI, un panel que integra en tres pestañas para la gestión de contactos, la marcación de números y la gestión del histórico de llamadas, un panel para realizar videoconferencias, una barra de disponibilidad y una barra de estado.

EJERCICIOS PROPUESTOS

- **1.** Instale y configure 3CX con la extensión del ejemplo 12.1.
- **2.** Añada una nueva extensión a 3CX para el usuario del ejemplo 12.2.
- **3.** Utilice FreePBX para crear la extensión del ejemplo 12.2.
- **4.** Utilice FreePBX para crear la extensión del ejemplo 12.1.
- **5.** Configure el softphone X-Lite para el empleado del ejemplo 12.3.
- **6.** Configure el softphone X-Lite para el empleado del ejemplo 12.4.
- **7.** Configure el softphone Ekiga para el empleado del ejemplo 12.4.
- **8.** Configure el softphone Ekiga para el empleado del ejemplo 12.3.
- **9.** Compruebe el funcionamiento de los clientes de los ejercicios anteriores, efectuando una llamada entre ellos.

TEST DE CONOCIMIENTOS

1 La principal diferencia entre SIP e IAX2 estriba en:
- a) Cómo realizan la traducción de direcciones mediante NAT.
- b) El número de puertos o conexiones utilizadas.
- c) El número de puertos utilizados para las señales.
- d) El número de puertos utilizados para las llamadas.

2 Cuando los paquetes se retrasan al llegar al destinatario, se puede:
- a) Ampliar el ancho de banda.
- b) Utilizar buffers para su almacenamiento.
- c) Evitar la transmisión de silencios.
- d) Priorizar los paquetes de voz frente a los de datos.

3 Un acceso E1
- a) Consta de 23 canales B más uno D.
- b) Consta de 30 canales B y uno D.
- c) Consta de 23 canales B, uno D y un canal de alarma y sincronización.
- d) Consta de 32 canales.

4 En una red GSM:
- e) Los terminales de usuario dependen de una celda.
- f) GPRS es el servicio que permite la transmisión de mensajes MMS.
- g) La información de señalización es constante con la estación base.
- h) La a y b son ciertas.

5 La diferencia entre un ATA y un Gateway radica en:
- a) El tipo de tratamiento dado a la información de señalización.
- b) La conversión que realizan de las señales.
- c) El número de puertos utilizados para conectar teléfonos analógicos.
- d) Ninguna de las anteriores.

6 Un terminal IP para la conexión a una red de datos:
- a) Necesita al menos dos conectores.
- b) Necesita un conector, además de uno para la red telefónica.
- c) Necesita un conector y actúa de conmutador.
- d) Al menos debe disponer de un conector.

7 El transporte para la transmisión de paquetes de voz se realiza sobre UDP porque:
- a) Evita el control sobre los paquetes.
- b) Permite las conexiones orientadas a conexión.
- c) Permite encaminar los paquetes por rutas distintas.
- d) Del control se encarga TCP.

8 El software codificador/decodificador o codec:
- a) Solamente se encarga de la digitalización de la voz.
- b) Digitaliza y encripta la voz.
- c) Digitaliza y reproduce la voz.
- d) Digitaliza y comprime la voz.

9 El término FXO se define como:
- a) Un interfaz que permite la conexión de teléfonos analógicos.
- b) Un puerto que permite la conexión de líneas digitales.
- c) Una interfaz que permite la conexión a una línea de telefonía.
- d) Un puerto conectado directamente a la central de telefonía.

Material adicional

El material adicional de este libro puede descargarlo en nuestro portal Web: *http://www.ra-ma.es*.

Debe dirigirse a la ficha correspondiente a esta obra, dentro de la ficha encontrará el enlace para poder realizar la descarga. Dicha descarga consiste en un fichero ZIP con una contraseña de este tipo: XXX-XX-XXXX-XXX-X la cual se corresponde con el ISBN de este libro.

Podrá localizar el número de ISBN en la página 2 (página de créditos). Para su correcta descompresión deberá introducir los dígitos y los guiones.

Cuando descomprima el fichero obtendrá los archivos que complementan al libro para que pueda continuar con su aprendizaje.

INFORMACIÓN ADICIONAL Y GARANTÍA

- RA-MA EDITORIAL garantiza que estos contenidos han sido sometidos a un riguroso control de calidad.
- Los archivos están libres de virus, para comprobarlo se han utilizado las últimas versiones de los antivirus líderes en el mercado.
- RA-MA EDITORIAL no se hace responsable de cualquier pérdida, daño o costes provocados por el uso incorrecto del contenido descargable.
- Este material es gratuito y se distribuye como contenido complementario al libro que ha adquirido, por lo que queda terminantemente prohibida su venta o distribución.

API Común de RDSI, 328
APIPA. *Véase* Direccionamiento IP privado automático
Apodo, 243
Applet, 88
apt-get, orden, 21, 22, 64, 65, 132, 138, 302
aquota.group, archivo, 135
aquota.user, archivo, 135
Archivo
  adjunto de correo, 180
  de registro, 69, 103
Arquitectura TCP/IP, 93, 112, 114, 125, 140
ASF. *Véase* Formato Avanzado de Secuencias
Asignación dinámica de direcciones, 12, 43, 124, 333
  configuración en Linux, 15
Asistente de componentes de Windows, 159
ASP. *Véase* Procesador de Señales Avanzado
Asterisk
  A2Billing, 339
  AsteriskNow, 339
  Avantfax, 339
  canales, 339
  contextos, 339
  DebPBX, 339
  dialplan, 339
  extensiones, 339
  FreePBX, 339
asterisk-addons, paquete, 339
asterisk, paquete, 339
asterisk-sound, paquete, 339
ATA. *Véase* Adaptador telefónico analógico
Audacity, programa, 256
Audio y vídeo intercalado, 274
Autenticación simple y capa de seguridad, 211
AVI. *Véase* Audio y vídeo intercalado

B

Banshee, reproductor, 264, 265
Banshee, reproductor, 287
Bastante buena confidencialidad, 186
BIND. *Véase* dominio de nombres de Internet de Berkeley
bind9-doc, paquete, 64, 65
bind9, paquete, 64, 65
bind, carpeta, 64, 65
bind-chrootenv, paquete, 65, 67
bind, paquete, 65, 67
Bit Mapped Picture, 272
Bitrate, 251
Bitrate constante, 251
Bitrate variable, 251
BMP. *Véase* Bit Mapped Picture
BNC, conexión, 270
Boletín de noticias, 295
Broadcaster, 254
BS Player, reproductor, 285
Bucle local o de abonado, 320
Buffering, 256
Buzón de correo, 180

C

CA. *Véase* Entidad certificadora
Caché
  de nombres, 52
Calidad del servicio, 323, 324, 326
  ancho de banda, 326
  eco, 326
  jitter, 326
  latencia, 326
  pérdida de paquetes, 326
  retardo, 326
  reverberación, 326
Canales de audio, 251
Capa de conexión segura, 92, 96, 100, 103, 114, 124, 155
Central privada secundaria, 322, 324
Centrex. *Véase* Oficina Central de Servicio de Intercambio
Centro de redes y recursos compartidos, 30, 33, 42, 78, 80
Centro multimedia, 285
CGI. *Véase* Interfaz de pasarela común
check_perms, orden, 303, 309
chmod, orden, 134, 135
Cifrado, 153
  de clave pública, 153, 165
  de clave privada, 153
  DSA, algoritmo, 153

Índice Alfabético

Símbolos

.3gp, extensión, 253
.asf, extensión, 274
.avi, extensión, 274
.H.323, estándar, 277, 278
.m4a, extensión, 253, 276
.m4b, extensión, 253
.m4p, extensión, 253
.m4r, extensión, 253
.m4v, extensión, 253, 276
.mid, extensión, 253
.mkv, extensión, 275
.mov, extensión, 275
.mp3, extensión, 252
.mp4, extensión, 253, 276
.mp4v, extensión, 276
.NET Framework 2.0, 336
.ogg, extensión, 252
.ogv, extensión, 275
.ra, extensión, 253
.ram, extensión, 253, 275
.rm, extensión, 253, 275
.rmm, extensión, 253
.rmvb, extensión, 275
.rv, extensión, 275
.srt, extensión, 287
.swf, extensión, 275
.wav, extensión, 253
.wma, extensión, 253
.wmv, extensión, 274

A

a2enmod, orden, 106
A6, registro DNS, 64
AAAA, registro DNS, 64
Acceso para transmisión de paquetes en telefonía
    móvil de alta velocidad, 331
Acceso web de Outlook, 206
ACL. *Véase* Lista de control de acceso
ActiveX, control, 168, 155
Actualización
    dinámica DNS, 55
Adaptador
    telefónico analógico, 331
AdBlock, herramienta, 117
Administración remota, 161, 152
Administrador de servicios de Internet, 95, 98, 99, 126,
    127, 130, 131, 132
Adobe Flash Player, plugin, 275
Adobe Flash Player, reproductor, 285
Adobe Flash, tecnología, 275, 285
Adobe Shockwave, tecnología, 285
AES, algoritmo de encriptación, 92
Agente de transferencia de correo, 181
Agente de usuario de correo, 181, 198
Ajax. *Véase* JavaScript y XML asíncrono
Allow, directiva, 106
AllowOverride, directiva, 106
Amarok, reproductor, 265
AMSN, software, 277
Apache, 94, 101, 302, 309
    contenedor, 105
    directiva, 106, 105
    entorno global, 105
    máquina virtual, 101
    módulos, 101, 106
    servidor principal, 105
    servidor virtual, 101, 105, 106
apache2ctl, orden, 303
apache2, paquete, 102
apache2-prefork, paquete, 102
API Común de RDSI, 328
APIPA. *Véase* Direccionamiento IP privado
    automático

Apodo, 243
Applet, 88
apt-get, orden, 21, 22, 64, 65, 132, 138, 302
aquota.group, archivo, 135
aquota.user, archivo, 135
Archivo
  adjunto de correo, 180
  de registro, 69, 103
Arquitectura TCP/IP, 93, 112, 114, 125, 140
ASF. *Véase* Formato Avanzado de Secuencias
Asignación dinámica de direcciones, 12, 43, 124, 333
  configuración en Linux, 15
Asistente de componentes de Windows, 159
ASP. *Véase* Procesador de Señales Avanzado
Asterisk
  A2Billing, 339
  AsteriskNow, 339
  Avantfax, 339
  canales, 339
  contextos, 339
  DebPBX, 339
  dialplan, 339
  extensiones, 339
  FreePBX, 339
asterisk-addons, paquete, 339
asterisk, paquete, 339
asterisk-sound, paquete, 339
ATA. *Véase* Adaptador telefónico analógico
Audacity, programa, 256
Audio y vídeo intercalado, 274
Autenticación simple y capa de seguridad, 211
AVI. *Véase* Audio y vídeo intercalado

B

Banshee, reproductor, 264, 265, 287
Bastante buena confidencialidad, 186
BIND. *Véase* Dominio de nombres de Internet de Berkeley
bind9-doc, paquete, 64, 65
bind9, paquete, 64, 65
bind, carpeta, 64, 65
bind-chrootenv, paquete, 65, 67
bind, paquete, 65, 67
Bit Mapped Picture, 272
Bitrate, 251
Bitrate constante, 251
Bitrate variable, 251
BMP. *Véase* Bit Mapped Picture
BNC, conexión, 270
Boletín de noticias, 295
Broadcaster, 254
BS Player, reproductor, 285
Bucle local o de abonado, 320
Buffering, 256
Buzón de correo, 180

C

CA. *Véase* Entidad certificadora
Caché
  de nombres, 52
Calidad del servicio, 323, 324, 326
  ancho de banda, 326
  eco, 326
  jitter, 326
  latencia, 326
  pérdida de paquetes, 326
  retardo, 326
  reverberación, 326
Canales de audio, 251
Capa de conexión segura, 92, 96, 100, 103, 114, 124, 155
Central privada secundaria, 322, 324
Centrex. *Véase* Oficina Central de Servicio de Intercambio
Centro de redes y recursos compartidos, 30, 33, 42, 78, 80
Centro multimedia, 285
CGI. *Véase* Interfaz de pasarela común
check_perms, orden, 303, 309
chmod, orden, 134, 135
Cifrado, 153
  de clave pública, 153, 165
  de clave privada, 153
  DSA, algoritmo, 153
  RSA, algoritmo, 153
Cliente, 12
  de mensajería instantánea, 226
Cliente-servidor, 12, 223

Cliente VoIP
Ekiga, 345
X-Lite, 343
cmd.exe, orden, 140
Codecpack, 264
codificador-decodificador, 321
Comité de Actividades de Internet, 12
Compresión
espacial, 276
redundancia temporal, 276
Computación en red virtual, 154, 161, 162
Conector, 211
Conexión
FTP, 164
TCP, 122, 152
config, archivo, 34
config_list, orden, 307
Configuración
automática, 12
predeterminada, 12
Consorcio de Sistemas de Internet, 21, 52, 311
Consulta DNS recursiva, 54
Contenedor multimedia, 274
Conversación retransmitida por Internet, 223
Cookie, 114
Corporación de Internet para la Asignación de nombres y números, 55
Correo basura, 189
Correo electrónico, 180
Correspondencia
directa, 54
inversa, 55
cron, demonio, 315
crontab, orden, 305
CSS. *Véase* Hojas de estilo en cascada
Codec, 251, 270, 271, 323
Cuotas de disco, 213
CVS. *Véase* Sistema de versiones concurrentes
cyradm, orden, 212
Cyrus, 210, 217
cyrus2.2, demonio, 211
cyrus.conf, archivo, 210, 217
cyrus, paquete, 206
cyrus, usuario, 211, 213, 217

D

dadhi, paquete, 339
Darwin Streaming Server, 279, 282
date, orden, 315
Daytime. *Véase* Resolvedor RFC 867
DCPROMO, orden, 203
defaultdomain, archivo, 82, 83
Demonio de caché del servicio de mobres, 84
Demonio FTP muy seguro, 132, 136
modo standalone, 132, 136
Deny, directiva, 106
Descarga directa, 250, 270
Descarga progresiva, 250, 270
dev, carpeta, 34
dhclient.leases, archivo, 35
dhclient, paquete, 35
dhclient, proceso demonio, 35
DHCP. *Véase* Asignación dinámica de direcciones
dhcp3-server, paquete, 21, 22
dhcp, carpeta, 21, 22, 25, 27
dhcp-client, paquete, 35
dhcpd3, orden, 21, 23
dhcpd.conf, archivo, 21, 22, 25, 27, 28
dhcpd, demonio, 21
dhcpd.leases, archivo, 27
dhcpd, orden, 21, 23, 25
DHCPNACK, mensaje, 21, 22, 27
dhcp, paquete, 35
dhcp-server, demonio, 21
dhcp-server, paquete, 23, 25
dhcpv6-client, paquete, 35
dhcpv6, paquete, 35
dial, orden, 339
dig, orden, 76, 84
Dimdim, 278
Direccionamiento IP privado automático, 14, 43, 44
Directorio activo, 202
Directorio personal, 132, 134, 170, 171
Directory, contenedor, 106
DirectoryIndex, directiva, 105
DivX, codec, 276
DNS. *Véase* Sistema de nombres de dominio
DocumentRoot, directiva, 105, 106

Dominio, 51, 52
de país, 50
genérico, 50
Dominio de nombres de Internet de Berkeley, 55, 63
dpkg, orden, 132, 138, 140
Dual DHCP DNS Server, 19, 21, 62, 63
DualServer.EXE, archivo, 19, 21, 62, 63
DualServer.INI, archivo, 19, 21, 62, 63
DV. *Véase* Vídeo digital
DV, codec, 276

E

Eco, 153
Eco ICMP, 14
Edición y versionado distribuidos sobre la Web, 91
Elisa. *Véase* Moovida
E-mail. *Véase* Correo electrónico
Emulador de terminal, 153, 154
Encabezado HTTP, 96
Encaminador, 93
Entidad certificadora, 92, 93, 99
Entorno de ejecución de prearranque, 124
Entorno de escritorio GNOME, 136, 140, 162, 173
Entorno de escritorio K, 115, 136, 140, 161, 172
EPS. *Véase* Lenguaje Encapsulado PostScript
equota, orden, 135
Escritorio remoto para administración, 155
Escritorios remotos, herramienta, 167
etc, carpeta, 25, 67
Exim, 207
eXperimental Computing Facility, 273
export, orden, 310
Extensiones multipropósito de correo de Internet, 183
Extensión, 322

F

Fábrica Nacional de Moneda y Timbre, entidad certificadora, 92
FDM. *Véase* Multiplexación por division de frecuencia
Fichero de intercambio de información personal, 99
Filezilla, programa, 146, 257
find, orden, 171, 170
Firewire, conexión, 270
Flash Video, 275
Formato avanzado de secuencias, 274
Formato de documento portable, 273
Formato de fichero de audio en forma de onda, 253
Foro, 295
Fotograma, 273
Fotogramas por segundo, 273
fps. *Véase* Fotogramas por segundo
frame. *Véase* Fotograma
framerate. *Véase* Fotogramas por segundo
fstab, archivo, 134
FTP. *Véase* Protocolo de transferencia de archivos
FTPES. *Véase* Protocolo de transferencia de archivos explícito
FTPS. *Véase* Protocolo de transferencia de ficheros implícito
ftpusers, archivo, 134
FXO. *Véase* Interfaz de central externa
FXS. *Véase* Interfaz de abonado externo

G

GAIM, 227
Gatekeeper, 325
Gateway. *Véase* Pasarela
Gateway VoIP. *Véase* Pasarela
gbindadmin, paquete, 65
gcc, herramienta, 339
gdhcpd, paquete, 21, 22, 25
gdm.conf, archivo, 160, 171
genaliases, orden, 304
Gestor de pantalla GDM, 160, 161
GIF. *Véase* Graphic Interchange Format
GIMP, software, 273
glibc, 80
GNOME, entorno de escritorio, 132
gnome-network-admin, paquete, 39, 82
gnome-rdp, herramienta, 173
GNU GPL
licencia, 165
GNU GPL, licencia, 154, 157
GNU, licencia, 164
GnuPG. *Véase* Guardián de privacidad de GNU, 188
gnupg, paquete, 187, 188
Google, 115
Google Talk, 228

GPG. *Véase* Guardián de privacidad de GNU, 187, 188
GPRS. *Véase* Servicio General de Paquetes vía Radio
Graphic Interchange Format, 272
grep, orden, 138, 140
Gráficos Vectoriales Escalables, 273
Grupo de Expertos en Imágenes en Movimiento, 274
Grupos de distribución, 296
  basados en consultas, 296
  dinámicos, 296
  estáticos, 296
Grupos de seguridad, 296
GSM. *Véase* Sistema global para las comunicaciones móviles
GStreamer, motor de reproducción, 265
GStreamer, motor de reproducción de contenido multimedia, 287
Guardián de privacidad de GNU, 186

H

Hiperenlace, 88, 93, 113
Hipertexto, 88
Hojas de Estilo en Cascada, 93
home, carpeta, 188
host, orden, 84
hosts, archivo, 54, 82, 83, 84
hotssh, herramienta, 170
HSDPA. *Véase* Acceso para transmisión de paquetes en telefonía móvil de alta velocidad
HTML, 88. *Véase* Lenguaje de marcas de hipertexto
htpasswd, orden, 107
httpd, paquete, 102
http, protocolo, 264
HTTP, protocolo, 287
HTTPS. *Véase* Protocolo seguro de transferencia de hipertexto
hwclock, orden, 315

I

IAX2. *Véase* Intercambio entre dispositivos Asterisk
Icecast, 261, 258
  etiqueta <admin-password>, 261
  etiqueta <adminroot>, 262
  etiqueta <admin-user>, 261
  etiqueta <authentication>, 261
  etiqueta <basedir>, 262
  etiqueta <bind-address>, 261
  etiqueta <clients>, 261
  etiqueta <hostname>, 261
  etiqueta <listen-socket>, 261
  etiqueta <logdir>, 262
  etiqueta <pidfile>, 262
  etiqueta <port>, 261
  etiqueta <relay-password>, 261
  etiqueta <source-password>, 261
  etiqueta <webroot>, 262
icecast2, paquete, 261
icecast.xml, archivo, 261, 263
Ices
  etiqueta <description>, 262
  etiqueta <encode>, 262
  etiqueta <genre>, 262
  etiqueta <hostname>, 262
  etiqueta <input>, 262
  etiqueta <instance>, 262
  etiqueta <name>, 262
  etiqueta <nominal-bitrate>, 262
  etiqueta <param>, 262
  etiqueta <password>, 262
  etiqueta <port>, 262
  etiqueta <stream>, 262
Ices, codificador, 258
Identificador del proceso, 104
Identificador uniforme de recursos, 50, 325
ifcfg-eth0, archivo, 39, 40
ifconfig, orden, 21, 33, 34, 40, 41, 42
ifdown, orden, 34, 39, 40
ifup, orden, 34, 39, 40
Imagen
  de mapa de bits, 271
  vectorial, 271
Imagen de mapa de bits
  color real, 272
  modos de color, 272
  profundidad, 271
  resolución, 272
  tamaño, 272
IMAP. *Véase* Protocolo interactivo de acceso a correo
imapd.conf, archivo, 210, 217

imtest, orden, 211, 213
in-addr.arpa, dominio, 55
index.htm, archivo, 89, 91
index.html, archivo, 89, 91, 98, 99, 103
Indicación por Nombre de Servidor, 109
inetd, demonio, 311
Instrumento Musical de Interfaz Digital, 252
Intercambio entre dispositivos Asterisk, 325
Interfaces, archivo, 34, 39, 40
Interfaz de Abonado Externo, 320, 334
Interfaz de Central Externa, 320, 334
Interfaz de pasarela común, 89, 96, 103
Interfaz de red, 98, 99, 104, 105, 125, 140
Internet Explorer
  Aceleradores, 112
  Crash Recovery, 112
  Cross Site Scripting, 112
  Filtrado InPrivate, 112
  Filtro SmartScreen, 112
  WebSlices, 112
IP. *Véase* Protocolo de interred
ip6.arpa, dominio, 55
ip6.int, dominio, 55
iptables, orden, 45
IRC. *Véase* Conversación retransmitida por Internet
  configuración, 242
  órdenes, 231, 232
ircd.conf, archivo, 242
ircd, paquete, 242
ircd, proceso demonio, 242
IVR. *Véase* Servicio de respuestas de voz interactiva

J

Jabber. *Véase* Protocolo extensible de mensajería y presencia
Java Runtime Environment, 168, 174
JavaScript y XML asíncrono, 89
Joint Photographic Experts Group, 272
JPG. *Véase* Joint Photographic Experts Group
JRE. *Véase* Java Runtime Environment
JSP. *Véase* Páginas de servidor java

K

Kaffeine, reproductor, 265, 285, 287
Kantaris, reproductor, 264
KDE. *Véase* Entorno de escritorio K
KDE, Entorno de escritorio, 132
kde4-krdc, paquete, 172
kde4-krfb, paquete, 161
kde4-kssh, paquete, 170
kdeaddons, paquete, 116
kdenetwork, paquete, 161, 172
KIO slave, programas, 115
Konqueror, navegador, 287
KPackageKit, gestor de paquetes, 132
KPackageKit, herramienta, 102
krdc, herramienta, 172
krfb, herramienta, 161
KSSH, herramienta, 170
KTS. *Véase* Sistema telefónico de teclas

L

Lag, 256
Latencia variable, 311
Lazo de seguimiento de fase, 312
Lenguaje de marcas de hipertexto, 88, 89, 183
Lenguaje encapsulado postscript, 273
Lenguaje extensible de marcas, 285, 273
Lenguaje extensible de marcas para aplicaciones, 285
Lenguajes de programación
  ASP, 88
  C++, 88
  Java, 88
  Javascript, 89
  PHP, 101, 88
libapache2-mod-gnutls, paquete, 109
libc, 80
libncurses5-dev, librería, 339
libpri, paquete, 339
Librerías GNU de C, 80
libsasl2-2, paquete, 211
Línea digital asimétrica de abonado, 327
Línea digital de abonado, 327
Línea digital simétrica de abonado, 327
Líneas troncales, 320
Lista de control de acceso, 69, 213
Lista de correo, 180
Lista de discusión, 295

Listas de correo, 294
Listas de distribución, 294
LMDS. *Véase* Sistema local de distribución multipunto
lmtp, conector, 217, 211
LoadModule, directiva, 106
localhost, 108, 98
Localizador universal de recursos, 50, 89, 93, 98, 99, 101, 104, 105, 108, 111, 113, 144, 145, 170, 259, 260, 264, 265, 286
log, carpeta, 216
log, registro, 217

M

mail, carpeta, 216
mail.err, archivo, 216
mail.log, archivo, 216
Mailman, 302
mailman.aliases, archivo, 304, 309
mailman, orden, 305
mailman, paquete, 302
mail, orden, 193
mail.warn, archivo, 216
make, herramienta, 339
Malware, 112
Matroska Video, 275
Media center. *Véase* Centro multimedia
Media Player Classic, reproductor, 264, 285
Mensajería instantánea, 222
Metafichero Windows, 273
MHS. *Véase* Servicio de gestión de mensajes
Microsoft Framework .NET, 280
MicrosoftSilverlight, tecnología, 285
MIDI. *Véase* Instrumento musical de interfaz digital
MIME. *Véase* Extensiones multipropósito de correo de Internet
mkgroup, orden, 156
mkpasswd, orden, 156
MKV. *Véase* Matroska Video
mm_cfg.py, archivo, 303, 304
mmsitepass, orden, 308
mms, protocolo, 264
MMS, protocolo, 286, 287
mod-auth, módulo, 107
Moderador, 296
mod-gnutls, módulo, 109
Modo de transferencia asíncrono, 327
mod-ssl, módulo, 109
Moovida, media center, 285
MOTIS, 181
mount, orden, 135
Mozilla Firefox, navegador, 287
MP3, 252, 253, 258, 261, 264
mp4live, herramienta de codificación, 279, 282
MPEG. *Véase* Grupo de expertos en imágenes en movimiento
MPEG-1, 252
MPEG-2, 252, 253
MPEG-4, 253
MPEG4IP, 282
MPEG, codec, 276
MPlayer, reproductor, 264, 265, 287
Máquina virtual, 103
MSDOS, 96
MTA. *Véase* Agente de transferencia de correo
MUA. *Véase* Agente de usuario de correo
Módulo de identidad del suscriptor, 330
Multiplexación por división de frecuencia, 320
MX, registro, 198
myScreen, plugin, 278
MySQL, 339

N

named, carpeta, 67
named.conf, archivo, 64, 65, 67, 68, 75, 76
named, demonio, 63, 64
NameVirtualHost, directiva, 106
Navegador, 89, 93, 113, 114, 115, 123, 144, 169
  Chrome, 111, 144
  Complementos, 112
  Epiphany, 111
  Galeon, 111
  Internet Explorer, 111, 112, 114, 144, 168
  Konqueror, 104, 105, 111, 115, 116, 170
  Marcador, 117
  Mozilla Firefox, 144, 145
  Opera, 111, 144
  Pestaña, 117

Seamonkey, 111
netsh, orden, 42
Netshow Encoder, software de codificación, 280
NetworkManager, 37, 39, 81, 82
newaliases, orden, 309
newlist, orden, 302, 305, 307
Newsletter. *Véase* Boletín de noticias
newt, librería, 339
Nick, 223
Niveles de ejecución, 242
nmap, orden, 211
Nombre de dominio totalmente cualificado, 51, 93, 95, 336
nscd.conf, archivo, 84
nslookup, orden, 76, 84
NSLOOKUP, orden, 79, 80
nsswitch.conf, archivo, 82, 83, 84
NTP. *Véase* Protocolo de tiempo de red
ntpdate, orden, 315
ntpdate, paquete, 315
ntpd, demonio, 312

O

Oficina Central de Servicio de Intercambio, 321
Ogg Vorbis, 252, 261, 262
OpenPGP, 186
OpenSSH, 153
openssh-client, paquete, 170
openssh, paquete, 160, 170
OpenSSH, paquete, 137
openssh-server, paquete, 160
OpenSSH Server, servicio, 157
OpenSSH, software, 156
openssl, herramienta, 339
OpenSSL, paquete, 109
OpenSSL, software, 92
options, archivo, 188
Options, directiva, 106
Order, directiva, 106
OSCAR. *Véase* Sistema abierto para la comunicación en tiempo real
OWA. *Véase* Acceso web de Outlook

P

PAM, 134
Pasarela VoIP, 332
Pasarela VoIP-GSM, 332
Pasarela VoIP-RTC, 332
PBX VoIP, 334
  3CX, 335
  Asterisk, 338
  hardware, 334
  software, 334
PDF. *Véase* Formato de documento portable
Petición de comentarios, 12
Petición FTP, 136
Petición HTTP, 102
PFX. *Véase* Fichero de intercambio de información personal
Página, 88, 91, 98, 99, 102, 104, 105, 108, 113
  de inicio, 113
  dinámica, 88
  estática, 88
  favoritos, 113, 114
  historial, 113, 114
  índice, 91, 93, 96, 98, 99, 103, 104, 105
Páginas de servidor Java, 88
PGP. *Véase* Bastante buena confidencialidad
PhotoShop Document, 273
PHP, 339
PICT. *Véase* PICTure
PICTure, 273
PID. *Véase* Identificador del proceso
Pidgin, 227
Pidgin, software, 277
ping, orden, 43, 42
Píxel, 271
Plain Old Telephone Service, 320
PNG. *Véase* Portable Network Graphics
Podcast, 256
  agregador, 256
  fuente de contenidos, 256
  sindicación, 256
POP3. *Véase* Protocolo de oficina postal
Portable Network Graphics, 273
ports.conf, archivo, 107

Postfix, 207
POTS. *Véase* Plain Old Telephone Service
ppp. *Véase* Puntos por pulgada
Procesador de señales avanzado, 327
Protocolo
  TCP, 255, 324
  UDP, 124, 154, 254, 347, 326, 324, 350
Protocolo de Capa de Conexión Segura, 137
Protocolo de computación en red virtual, 154, 157, 165, 172
Protocolo de control de administrador de la pantalla X, 154
Protocolo de control de transporte en tiempo real, 254, 324
Protocolo de datagramas de usuario, 124, 254
Protocolo de escritorio remoto, 154, 174, 172, 157
Protocolo de flujo en tiempo real, 254
Protocolo de inicio de sesión, 278, 325
Protocolo de interred, 124
Protocolo de mensajes de control de internet, 14, 42, 43
Protocolo de oficina postal, 185, 198, 210
Protocolo de registro, admisión y estado, 325
Protocolo de tiempo de red, 311, 324
Protocolo de transferencia de archivos, 88, 89, 122, 124, 127, 255, 257
  órdenes, 142
Protocolo de transferencia de archivos explícito, 124
Protocolo de transferencia de archivos implícito, 124
Protocolo de transferencia de hipertexto, 88, 89, 198, 255
Protocolo de transferencia de hipertexto seguro, 92
Protocolo de transporte en tiempo real, 254, 324
Protocolo extensible de mensajería y presencia, 224
Protocolo H.323, 325
Protocolo interactivo de acceso a correo, 185, 198
Protocolo ligero de acceso al directorio, 200
Protocolo ligero de control de clientes, 325
Protocolo seguro de transferencia de hipertexto, 89, 92, 93, 100
Protocolo simple de tiempo de red, 311
Protocolo simple de transferencia de correo, 184, 199, 336
Protocolo trivial de transferencia de archivos, 124
PSD. *Véase* PhotoShop Document
ps, orden, 304
PTR. *Véase* Puntero de registro de recursos; *Véase* Punto de terminación de red
Puerto
  bien conocido, 12
  FTP, 132, 127, 164
  HTTP, 93, 95, 96, 99, 103, 104, 105
  HTTPS, 96
  IRC, 242, 243
  RDP, 155
  rlogin, 153
  SSH, 164, 153
  Telnet, 153
  VNC, 154, 157
Puntero de registro de recursos, 55
Punto de terminación de red, 320
Puntos por pulgada, 272
PuTTY, programa, 163, 165
PXE. *Véase* Entorno de ejecución de prearranque

Q

QMail, 207
Quicktime, 275
Quictime, reproductor, 285
quotaoff, orden, 135
quotaon, orden, 135
quota, paquete, 134

R

RAS. *Véase* Protocolo de registro, admisión y estado
RCA, conexión, 270
rcapache2, orden, 108
rdesktop, paquete, 174
RDP. *Véase* Protocolo de escritorio remoto
Real Audio, 253
Real Media Player, reproductor, 264
Real Player, reproductor, 285
Real Video, 275
RealVNC, programa, 157, 165
Red de Telefonía Básica, 320
Red Digital de Servicios Integrados, 321
  Acceso básico, 329
  Acceso híbrido, 329
  Acceso primario, 329

Adaptador de Terminal, 328
NT1, 327
NT2, 328
TR1, 327
TR2, 328
Red telefónica conmutada, 320
regedt32, orden, 312
Registrador de dominios, 55
Registro de recursos, 53
Registros de IRC, 242
Registros de zona, tipos, 53
Reglas de etiqueta, 295
resolv.conf, archivo, 41, 82, 83
Resolvedor, 54
RFC 778, 311
RFC 821, 184
RFC 822, 182
RFC 867, 311
RFC 891, 311
RFC 956, 311
RFC 958, 311
RFC 1032, 56
RFC 1033, 55
RFC 1034, 54
RFC 1035, 54
RFC 1305, 311
RFC 1341, 183
RFC 1361, 311
RFC 1421, 188
RFC 1422, 188
RFC 1423, 188
RFC 1424, 188
RFC 1464, 53
RFC 1521, 183
RFC 1769, 311
RFC 2030, 311
RFC 2045, 183
RFC 2046, 183
RFC 2535, 56
RFC 3152, 55
RFC 3363, 53
RFC 3364, 53
RFC 3920, 224
RFC 3921, 224
RFC 3922, 224
RFC 3923, 224
RFC 4330, 311
Rhythmbox, reproductor, 265
rlogin, orden, 164
root, usuario, 35, 80
rpm, orden, 132
RR. *Véase* Registro de recursos
RSA, algoritmo de encriptación, 92
rsh-client, paquete, 170
rsh, paquete, 170
rsh-server, paquete, 160
RSS. *Véase* Sindicación realmente simple
RTB. *Véase* Red de telefonía básica
RTCP. *Véase* Protocolo de control de transporte en tiempo real
RTP. *Véase* Protocolo de transporte en tiempo real
RTP, protocolo, 287
RTSP. *Véase* Protocolo de flujo en tiempo real
RTSP, protocolo, 287

S

SASL. *Véase* Autenticación simple y capa de seguridad
sasl2-bin, paquete, 211
saslauth, archivo, 211
saslauth, proceso demonio, 211
saslpassdw2, orden, 211
SCCP. *Véase* Protocolo ligero de control de clientes
scp, orden, 153, 164, 165, 170, 171
ScriptAlias, directiva, 309
SDSL. *Véase* Línea digital simétrica de abonado;
Seguridad de la capa de transporte, 92, 124
Seguridad en capa de transmisión, 200
Sendmail, 206, 207, 302
sendmail-bin, paquete, 207
sendmail.cf, archivo, 207, 216, 217
sendmail.cf.errors, archivo, 216
sendmail.cf, orden, 211
sendmail.mc, archivo, 207, 211, 216, 304
sendmail, paquete, 207
sendmail, proceso demonio, 209
sensible-mda, paquete, 216, 217
ServerAdmin, directiva, 105

ServerName, directiva, 105
service, orden, 108
Servicio de acceso remoto mediante interfaz web
  cliente, 174
  cliente Windows, 169
  configuración, 159, 162
Servicio de computación en red virtual, 153
  cliente, 172
Servicio de escritorio remoto
  cliente, 166, 172
  cliente VNC, 165
  configuración, 157
Servicio de escritorio remoto VNC
  configuración, 161
Servicio de gestión de mensajes, 181
Servicio de información de Internet, 95
  credenciales, 96
Servicio de mensajes cortos, 330
Servicio de respuestas de voz interactiva, 334
Servicio de terminal server
  cliente, 165, 174
  configuración, 157
Servicio de tiempo de Windows, 312
Servicio FTP, 88, 123, 153, 257
  acceso público, 123, 131, 132, 137, 138, 140
  acceso privado, 123
  cliente, 125, 140, 145, 146
  cliente, línea de órdenes, 140
  cliente, navegador, 144
  cliente, programas específicos, 145
  conexión de control, 122
  conexión de datos, 122
  configuración, 124
  raíz del sitio, 124, 134
  servidor Windows, 125
  sitio con aislamiento de usuarios, 127, 132
  sitio FTP, 123, 125, 127, 129, 131, 132
  órdenes, 140, 141, 142
  usuario anónimo, 131, 132
Servicio general de paquetes vía radio, 330
Servicio HTTP, 88, 98, 99, 104, 105, 250
  cliente HTTP, 112
  configuración, 94
  módulos, 102
  parámetros de configuración, 93
  raíz del sitio, 93, 98, 99, 103, 104, 105, 106, 108
  sitio web, 89, 91, 95, 96, 108
Servicio IRC
  cliente, 231
  servidor, 242
Servicio rlogin
  cliente, 170, 163
  conexión, 164
  configuración, 160
Servicios de información de Internet, 198, 202
Servicios de Windows Media, herramienta, 259
Servicios de Windows Media (Web), herramienta, 259
Servicio shell seguro
  cliente, 163, 170
  conexión, 164, 170
  configuración, 160
  copia, 164
  transferencia, 164
Servicios, herramienta, 157
Servicio SSH
  configuración, 156
Servicio telnet
  cliente, 163, 170
  conexión, 164
  configuración, 156, 160
Servicio terminal remoto, 152
  acceso remoto mediante interfaz web, 155
  escritorio remoto, 154
  rlogin, 153
  Shell seguro, 153
  telnet, 152
  Terminal server, 154
  X-terminal, 154
Servicio x-terminal
  configuración, 160
Servidor, 12
  de aplicaciones, 202
  de correo, 198
  DNS, 57
  FTP, 123
  HTTP, 91, 94, 101, 102, 103
  Proxy, 93, 112, 114, 125, 140
  VNC, 157, 165

Web, 106, 115
Servidor de información de Internet, 94, 95, 99, 125, 126, 131, 132, 155, 159
configuración, 127
directorio virtual, 98, 129
iniciar, 130
módulo administrado, 97
módulo nativo, 97
reglas de caché, 97
Servidor DNS, 51
primario, 54
secundario, 54
Servidor IRC, 242
Servidor virtual, 101, 103, 104
Servlet, 88
Sesión remota
gráfica, 152
mediante órdenes, 152
setupssh, programa, 156
sftp, orden, 153, 164, 165
shadow, archivo, 210
Shell seguro, 115, 123, 137, 153, 160, 257
ShockWave Flash, 273
Shoutcast, 261
S-HTTP. *Véase* Protocolo de transferencia de hipertexto seguro
shttp, extensión, 92
SIM. *Véase* Módulo de Identidad del Suscriptor
Sindicación realmente simple, 111, 256, 257
SIP. *Véase* Protocolo de Inicio de Sesión
Sistema abierto para la comunicación en tiempo real, 224
Sistema de archivos, 88
Sistema de archivos virtual, 122
Sistema de nombres de dominio, 50, 91, 93, 101, 183, 198, 203, 214, 325
Sistema de señalización, 321
Sistema de versiones concurrentes, 91
Sistema global para las comunicaciones móviles, 330
celda, 330
célula, 330
estaciones base, 330
Sistema local de distribución multipunto, 330
Sistema telefónico de teclas, 322
sitelist.cfg, archivo, 307
sites-enabled, carpeta, 303
Sitio, 93, 95, 98, 99, 104, 105, 106, 123, 127, 155
Skype, 225
smrsh, orden, 309
SMS. *Véase* Servicio de Mensajes Cortos
SMTP. *Véase* Protocolo simple de transferencia de correo
SNI. *Véase* Indicación por nombre de servidor
SNMP. *Véase* Protocolo simple de administración de red
SNTP. *Véase* Protocolo simple de tiempo de red
Software de libre distribución, 146, 157, 165, 163
Software espía, 114
Spam. *Véase* Correo basura
Spyware. *Véase* Software espía
SS7. *Véase* Sistema de Señalización 7
SSH. *Véase* Shell seguro
ssh, orden, 153, 164, 165, 170, 171, 172
SSL. *Véase* Capa de conexión segura
SSLCertificateFile, directiva, 109
SSLEngine, directiva, 109
SSLRequireSSL, directiva, 109
Streaming, 254, 250, 270
bajo demanda, 254
difusión broadcast, 255
difusión multicast, 255
difusión streaming media, 255
difusión unicast, 255
en tiempo real, 254
sudoers, archivo, 304
SVG. *Véase* Gráficos vectoriales escalables
S-Video, conexión, 270
SWF. *Véase* ShockWave Flash
Synaptic, gestor de paquetes, 132
Synaptic, herramienta, 102
syslog, archivo, 21, 22
system-config-httpd, paquete, 103
system-config-network-gui, orden, 38, 39
system-config-network, herramienta, 37, 39
system-config-network, paquete, 38, 39
system-config-vsftpd, paquete, 136, 137, 140

T

Tagged Image File Format, 272
Tasa de muestreo, 250
TCP/IP, arquitectura, 12
TCP, protocolo, 287
TDES, algoritmo de encriptación, 92
TDM. *Véase* Multiplexación por división de frecuencia
telnetd, paquete, 160
telnet, orden, 164
telnet, paquete, 170
Telnet, protocolo, 152
telnet-server, paquete, 160
Teredo, 33
Terminales VoIP, 333
  Ekiga, 278, 333
  IP, 333
  softphone, 333
  software, 333
  USB, 333
  webphone, 333
  X-Lite, 333
Terminal Server
  modo administración remota, 154
  modo servidor de aplicaciones, 155
Terminal virtual, 140
Tiempo de expiración, 72, 76
Tiempo de reintento de transferencia, 72, 76
Tiempo de vida, 72, 76
TIF. *Véase* Tagged Image File Format
TIFF. *Véase* Tagged Image File Format
tigervnc, paquete, 173
tigervnc-server, paquete, 162
tightvnc, paquete, 162, 173
TightVNC, programa, 165
tightvncserver, paquete, 162
TighVNC, programa, 157
Timeout, 132
TLS. *Véase* Seguridad en capa de transmisión
Totem, reproductor, 265 287
touch, orden, 135
Track móvil, 322
Traducción de direcciones de red, 325
Transferenca segura de, información, 165
Transferencia de archivos
  binario, 123
  texto, 123
Transferencia de zona, 54
  incremental, 54
Trunking, 325
Trunk lines. *Véase* Líneas troncales
tsclient, paquete, 174
tsclient, utilidad, 173
TSL. *Véase* Seguridad de la capa de transporte

U

UDP. *Véase* Protocolo de datagramas de usuario
UDP, protocolo, 270
UltraVNC, programa, 157, 165
UNC, 96
UNIX, 96
URI. *Véase* Identificador uniforme de recursos
URL. *Véase* Localizador universal de recursos
URTSP, protocolo, 270
USB, conexión, 270
USB, puerto, 270
UTP, protocolo, 287

V

VBR. *Véase* Bitrate variable
Ventanas emergentes, 111
Verisign, entidad certificadora, 92
Vídeo
  bitrate, 274
  fotogramas por segundo, 273
  resolución, 274
Videoconferencia, 276
  centralizada, 277
  descentralizada, 277
  grupo con un grupo, 277
  multipunto o multiconferencia, 277
  punto a punto, 277
  uno a uno, 277
  uno con un grupo, 277
Vídeo digital, 275
Vinagre, herramienta, 173
vino, herramienta, 162
VirtualHost, contenedor, 106

Virtual Hosts. *Véase* Servidor Virtual
Visor, 89
VLC, reproductor, 264, 275, 282, 285
VNC. *Véase* Protocolo de computación en red virtual
vnc, archivo, 162
vncpasswd, orden, 162
vncserver, orden, 162
vncviewer, orden, 173, 174
vsftpd. *Véase* Demonio FTP muy seguro
vsftpd, archivo, 136
vsftpd.chroot_list, archivo, 134
vsftpd.conf, archivo, 132, 133
vsftpd, demonio, 137, 138, 139, 140
vsftpd, orden, 136
vsftpd, paquete, 132, 138, 140

W

WAV. *Véase* Formato de Fichero de audio en forma de onda
WAVE. *Véase* Formato de fichero de audio en forma de onda
Webalizer, herramienta, 108
webalizer, orden, 108
webalizer, paquete, 108
Webcam, 270
WebDAV. *Véase* Edición y versionado distribuidos sobre la web
Webmaster, 93, 103
Webmin, herramienta, 67
widget, 278
Winamp, reproductor, 264
Windows Expression Encoder, software de codificación, 280
Windows Media Encoder, software de codificación, 280, 279
Windows Media Player, reproductor, 264
Windows Media Services, 258, 279, 280
  punto de publicación, 259
Windows Media, tecnología, 274
Windows Media Video, 274
WinSCP, programa, 164, 165, 257
WMF. *Véase* Metafichero Windows
WMV. *Véase* Windows Media Video
WMV, códec, 276
World Wide Web, 88
WTS. *Véase* Servicio de tiempo de Windows
WWW. *Véase* World Wide Web
www-data, usuario, 304

X

X.400, protocolo, 181
X.500, protocolo, 181
X.509, estandar de certificados, 92
XAML. *Véase* Lenguaje extensible de marcas para aplicaciones
XCF. *Véase* eXperimental Computing Facility
XDMCP. *Véase* Protocolo de control de administrador de la pantalla X
Xine, motor de reproducción de contenido multimedia, 287
xinetd, demonio, 136, 160
XML. *Véase* Lenguaje de marcas extensible
XMMS, reproductor, 265
XMPP. *Véase* Protocolo extensible de mensajería y presencia
xstartup, archivo, 162
X-Terminal
  aplicaciones X Window remotas, 154, 161, 171
  sesión X Window remota, 154, 160, 171
xtightvncviewer, paquete, 173
Xvid, codec, 276
X-window, 163, 153

Y

yast2-dhcp-server, paquete, 23, 25
yast2-dns-server, paquete, 23, 25, 65, 67
yast2-ftp-server, paquete, 136
yast2-http-server, paquete, 102
yum, orden, 132

Z

zaptel, paquete, 339
Zona, 51, 53
  de delegación, 55
  maestra, 70
  predefinida, 64
  solo caché, 70
  subordinada, 70
zttool, librería, 339

La presente obra está dirigida a los estudiantes del Ciclo Formativo de Grado Superior de **Administración de Sistemas Informáticos en Red**, en concreto al Módulo Profesional **Servicios de Red e Internet**, aunque también puede utilizarse por los alumnos de estudios universitarios de Informática con el propósito de ampliar contenidos.

Los contenidos incluidos en este libro abarcan desde los servicios básicos que ofrece una red de comunicación (DHCP o DNS) hasta otros servicios más avanzados, como las listas de distribución de correo, la mensajería instantánea o VoIP, pasando por servicios de amplio uso en la actualidad, como la transferencia de páginas web o el correo electrónico.

Servicios de Red e Internet contiene también descripciones detalladas sobre cómo instalar este tipo de servicios en los sistemas operativos de red Microsoft Windows y GNU/Linux.

Los capítulos incluyen ejercicios con el propósito de facilitar la asimilación de los conocimientos tratados. Así mismo, se incorporan test de conocimientos y ejercicios propuestos con la finalidad de comprobar que los objetivos de cada capítulo se han asimilado correctamente.



En la página web de **Ra-Ma** (**www.ra-ma.es**) se encuentra disponible el material de apoyo y complementario.

9 788499 640907

ra-ma.es

Ra-Ma®