Redes locales

Instalación y configuración básicas

José Luis Raya, Laura Raya,
Miguel Á. Martínez

Alfaomega Ra-Ma®

REDES LOCALES.
INSTALACIÓN
Y
CONFIGURACIÓN
BÁSICAS

REDES LOCALES. INSTALACIÓN Y CONFIGURACIÓN BÁSICAS

José Luis Raya Cabrera
Laura Raya González
Miguel Á. Martínez Ruiz

Alfaomega Ra-Ma

Datos catalográficos

Raya, José; Raya, Laura y Martínez, Miguel
Redes locales. Instalación y configuración básicas

Primera Edición

Alfaomega Grupo Editor, S.A. de C.V., México

ISBN: 978-970-15-1433-7

Formato: 17 x 23 cm Páginas: 412

Redes locales. Instalación y configuración básicas
José Luis Raya Cabrera, Laura Raya González, Miguel Á. Martínez Ruiz
ISBN: 978-84-7897-886-1, edición original publicada por RA-MA Editorial, Madrid, España

Primera edición: Alfaomega Grupo Editor, México, octubre 2008

Pitágoras 1139, Col. Del Valle, 03100, México D.F.

Miembro de la Cámara Nacional de la Industria Editorial Mexicana
Registro No. 2317

Pág. Web: **http://www.alfaomega.com.mx**
E-mail: **libreriapitagoras@alfaomega.com.mx**

ISBN: 978-970-15-1433-7

Nota importante:
La información contenida en esta obra tiene un fin exclusivamente didáctico y, por lo tanto, no está previsto su aprovechamiento a nivel profesional o industrial. Las indicaciones técnicas y programas incluidos, han sido elaborados con gran cuidado por el autor y reproducidos bajo estrictas normas de control. ALFAOMEGA GRUPO EDITOR, S.A. de C.V. no será jurídicamente responsable por: errores u omisiones; daños y perjuicios que se pudieran atribuir al uso de la información comprendida en este libro, ni por la utilización indebida que pudiera dársele.

Edición autorizada para venta en México y todo el continente americano.

Impreso en México. Printed in Mexico.

Empresas del grupo:

México: Alfaomega Grupo Editor, S.A. de C.V. – Pitágoras 1139, Col. Del Valle, México, D.F. – C.P. 03100.
Tel.: (52-55) 5089-7740 – Fax: (52-55) 5575-2420 / 2490. Sin costo: 01-800-020-4396
E-mail: libreriapitagoras@alfaomega.com.mx

Colombia: Alfaomega Colombiana S.A. – Carrera 15 No. 64 A 29 – PBX (57-1) 2100122
Fax: (57-1) 6068648 – E-mail: scliente@alfaomega.com.co

Chile: Alfaomega Grupo Editor, S.A. – General del Canto 370-Providencia, Santiago, Chile
Tel.: (56-2) 235-4248 – Fax: (56-2) 235-5786 – E-mail: agechile@alfaomega.cl

Argentina: Alfaomega Grupo Editor Argentino, S.A. – Paraguay 1307 P.B. “11”, Capital Federal,
Buenos Aires, C.P. 1057 – Tel.: (54-11) 4811-7183 / 8352, E-mail: ventas@alfaomegaeditor.com.ar

CONTENIDO

CAPÍTULO 7. ADMINISTRACIÓN Y GESTIÓN DE REDES 263

Capítulo 1

INTRODUCCIÓN A LAS REDES

CONCEPTO DE RED

Una red de ordenadores es un sistema de interconexión entre equipos que permite compartir recursos e información. Para ello, es necesario contar, además de con los ordenadores correspondientes, con las tarjetas de red, los cables de conexión, los dispositivos de interconexión y el *software* conveniente.

ORIGEN DE LAS REDES DE ORDENADORES

El origen y desarrollo de las redes de computadoras está basado en la colaboración de científicos de numerosos campos.

Aunque los primeros avances en el estudio de redes de computadoras se dieron en los Estados Unidos, el hecho que motivó su avance rápido se produjo en la URSS. Tras el primer lanzamiento del satélite artificial Sputnik, por parte de la URSS, en los Estados Unidos se abrió un periodo de crisis, se sentían derrotados en la Guerra Fría y necesitaban una revisión de las políticas de desarrollo científico y tecnológico que se habían realizado hasta entonces.

Por ello, surge en 1957 la agencia **ARPA** (*Advanced Research Projects Agency*, *Agencia de proyectos avanzados de investigación*) dependiente del Departamento de Defensa. Evidentemente, sus objetivos estaban vinculados con el desarrollo tecnológico aplicado a la defensa, pues se consideraba altamente peligroso que la URSS fuese por delante en las distintas carreras emprendidas en la Guerra Fría.

A pesar de habernos remontado a finales de los años 50, no se producen verdaderos avances hasta comienzos de la década de los años 60 y se centraron más en aspectos conceptuales que tecnológicos. Así, en 1962 en la agencia ARPA se propuso la interconexión de ordenadores para el desarrollo de trabajo colaborativo entre sus investigadores. Simultáneamente, en el **MIT** (*Instituto Tecnológico de Massachussets*) se escribió un artículo sobre tecnología de comunicación por cable mediante conmutación de paquetes, sentando así las bases para la comunicación entre computadores.

Con el patrocinio de ARPA, un año después, dos máquinas situadas en el *MIT* y en *System Development Corporation* de Santa Mónica se unieron mediante una línea dedicada cuya velocidad de transmisión era de 1200 bits por segundo.

COMPONENTES DE UNA RED

Una red está formada, principalmente, por los ordenadores con sus respectivos periféricos, por los elementos de conexión de los mismos y por el software necesario.

1. Los ordenadores, que pueden desarrollar dos funciones distintas: de servidores o de estaciones de trabajo (para obtener más información, vea el apartado *Arquitectura cliente/servidor*).

2. Se entiende por elementos de conexión a las tarjetas de red que se encuentran en los ordenadores y a los cables que las unen.

   Además de los elementos indicados anteriormente, si se van a conectar más de dos equipos, es necesario disponer de elementos de interconexión para conectarlos entre sí.

3. Dentro del software se puede distinguir entre los sistemas operativos y los protocolos de comunicaciones.

Todo lo anterior se irá desarrollando en capítulos sucesivos.

TIPOS DE REDES

Hay varios criterios por los que se pueden clasificar las redes de ordenadores, según su tecnología, su tamaño, su topología... En este apartado vamos a centrarnos en dos aspectos considerados como fundamentales y que permiten determinar exactamente la situación actual de las redes de ordenadores.

Por su tamaño

Según su tamaño, se pueden distinguir varios tipos de redes en función de su extensión:

- Si se conectan todos los ordenadores dentro de un mismo edificio, se denomina *LAN* (*Local Area Network*).
- Si se encuentran en edificios diferentes distribuidos dentro de la misma universidad, se denomina *CAN* (*Campus Area Network*).
- Si se encuentran en edificios diferentes distribuidos en distancias no superiores al ámbito urbano, *MAN* (*Metropolitan Area Network*).
- Si están instalados en edificios diferentes de la misma o distinta localidad, provincia o país, *WAN* (*Wide Area Network*).

Por la forma de conexión

Según la forma en que estén conectados los ordenadores, se pueden establecer varias categorías:

- **Redes sin tarjetas**. Utilizan enlaces a través de los puertos serie o paralelo para transferir archivos o compartir periféricos.
- **Redes punto a punto**. Un circuito punto a punto es un conjunto de medios que hace posible la comunicación entre dos ordenadores determinados de forma permanente.
- **Redes entre iguales**. Todos los ordenadores conectados pueden compartir información con los demás.
- **Redes basadas en servidores** centrales utilizando el modelo básico cliente-servidor.

VENTAJAS DE LAS REDES

Entre las ventajas de utilizar una red se encuentran:

- Posibilidad de compartir periféricos costosos como son: impresoras láser, scanner, fax, etc.
- Posibilidad de compartir grandes cantidades de información a través de distintos programas, bases de datos, etc., de manera que sea más fácil su uso y actualización.
- Reduce e, incluso, elimina la duplicidad de trabajos.
- Permite utilizar el correo electrónico para enviar o recibir mensajes de diferentes usuarios de la misma red e incluso de redes diferentes.
- Reemplaza o complementa miniordenadores de forma eficiente y con un coste bastante más reducido.
- Establece enlaces con *mainframes*. De esta forma, un ordenador de gran potencia actúa como servidor haciendo que los recursos disponibles estén accesibles para cada uno de los ordenadores personales conectados.
- Permite mejorar la seguridad y control de la información que se utiliza, permitiendo la entrada de determinados usuarios, accediendo únicamente a cierta información o impidiendo la modificación de diversos datos.

Inicialmente, la instalación de una red se realiza para compartir los dispositivos periféricos u otros dispositivos de salida caros, por ejemplo, las impresoras láser, los fax, etc.

Pero a medida que va creciendo la red, el compartir dichos dispositivos pierde relevancia en comparación con el resto de las ventajas. Las redes enlazan también a las personas proporcionando una herramienta efectiva para la comunicación a través del correo electrónico. Los mensajes se envían instantáneamente a través de la red, los planes de trabajo pueden actualizarse tan pronto como ocurran cambios y se pueden planificar las reuniones sin necesidad de llamadas telefónicas.

ARQUITECTURA CLIENTE/SERVIDOR

Al principio de la utilización de las redes, se conectaban los ordenadores entre sí para compartir los recursos de todos los ordenadores que estaban conectados.

Con el paso del tiempo, los usuarios fueron necesitando acceder a mayor cantidad de información y de forma más rápida, por lo que fue surgiendo la necesidad de un nuevo tipo de ordenador: el servidor.

Un servidor es un ordenador que permite compartir sus recursos con otros ordenadores que están conectados a él. Los servidores pueden ser de varios tipos y entre ellos se encuentran los siguientes:

- **Servidor de archivos**. Mantiene los archivos en subdirectorios privados y compartidos para los usuarios de la red.

- **Servidor de impresión**. Tiene conectadas una o más impresoras que comparte con los demás usuarios.

- **Servidor de comunicaciones**. Permite enlazar diferentes redes locales o una red local con grandes ordenadores o miniordenadores.

- **Servidor de correo electrónico**. Proporciona servicios de correo electrónico para la red.

- **Servidor Web**. Proporciona un lugar para guardar y administrar los documentos *HTML* que pueden ser accesibles por los usuarios de la red a través de los navegadores.

- **Servidor FTP**. Se utiliza para guardar los archivos que pueden ser descargados por los usuarios de la red.

- **Servidor proxy**. Se utiliza para monitorizar y controlar el acceso entre las redes. Cambia la dirección *IP* de los paquetes de los usuarios para ocultar los datos de la red interna a *Internet* y cuando recibe contestación externa, la devuelve al usuario que la ha solicitado. Su uso reduce la amenaza de piratas que visualicen el tráfico de la red para conseguir información sobre los ordenadores de la red interna.

Según el sistema operativo de red que se utilice y las necesidades de la empresa, puede ocurrir que los distintos tipos de servidores residan en el mismo ordenador o se encuentren distribuidos entre aquellos que forman parte de la red.

Así mismo, los servidores de archivos pueden establecerse como dedicados o no dedicados, según se dediquen sólo a la gestión de la red o, además, se puedan utilizar como estación de trabajo. La conveniencia de utilizar uno u otro va estar indicada por la cantidad de estaciones de trabajo de que se vaya a disponer; cuanto mayor sea el número de ellas, más conveniente será disponer de un servidor dedicado.

No es recomendable utilizar un servidor no dedicado como estación de trabajo, ya que, en caso de que ese ordenador tenga algún problema, la totalidad del sistema puede dejar de funcionar, con los consiguientes inconvenientes y pérdidas irreparables que se pueden producir.

El resto de los ordenadores de la red se denominan estaciones de trabajo o clientes, y desde ellos se facilita a los usuarios el acceso a los servidores y periféricos de la red.

Cada estación de trabajo es, por lo general, un ordenador que funciona con su propio sistema operativo. A diferencia de un ordenador aislado, la estación de trabajo tiene una tarjeta de red y está físicamente conectada por medio de cables con el servidor.

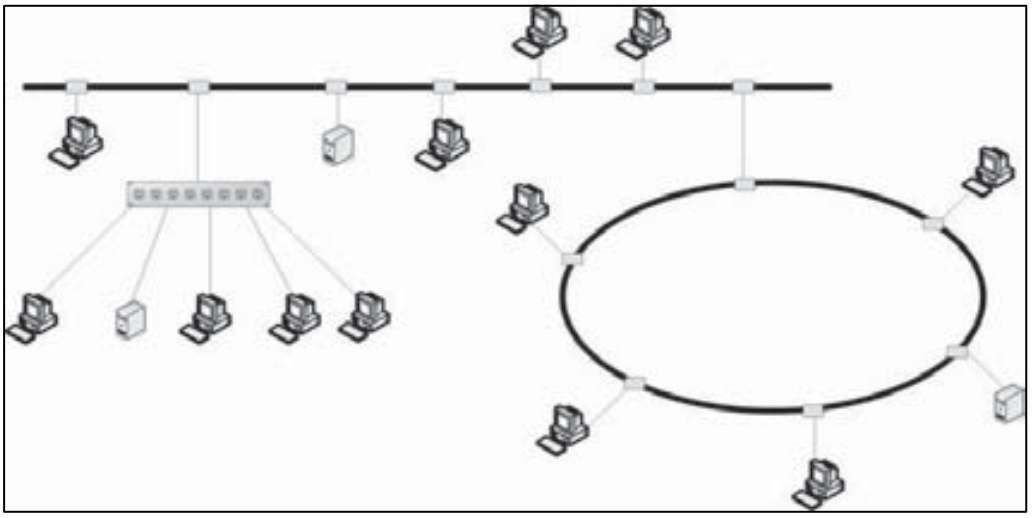


Figura 1.1. Esquema de una red con topología de bus, estrella y anillo

DISTRIBUCIÓN DE ESPACIO EN LOS DISCOS DUROS

En una red el disco o los discos duros pueden ser utilizados de tres maneras distintas: de forma privada, compartida o pública (que pueden coexistir sin ningún tipo de problema).

- En una utilización privada, los archivos que se encuentran en ellos son personales y únicamente tiene acceso su propietario para operaciones de lectura, escritura, borrado y creación de nuevos archivos.

- En una utilización compartida, los archivos que se encuentran en ellos tienen niveles de acceso distintos en función de las autorizaciones dadas por el administrador de la red. Por tanto, puede haber archivos que pueden ser utilizados totalmente por todos los usuarios, archivos que pueden ser utilizados parcialmente por todos los usuarios y archivos que sólo pueden ser utilizados por un usuario o un grupo de usuarios.

- En una utilización pública, los archivos pueden ser leídos, modificados o borrados por todos los usuarios (aunque sería recomendable que las dos últimas opciones las realizaran personas específicas que tuvieran un nivel de acceso superior).

COMPARTICIÓN DE PERIFÉRICOS

Dentro de las ventajas de una red se encuentra la posibilidad de compartir los periféricos que se encuentran en ella y, en especial, las impresoras.

Para poder compartir una impresora, ésta ha de estar conectada al servidor de archivos de la red o a un servidor específico denominado **servidor de impresión**.

El servidor de impresión y/o el servidor de archivos disponen de un programa que controla los trabajos de impresión mandados por los usuarios. Este programa crea una zona de almacenamiento temporal de datos en el disco donde se guardan todos los trabajos pendientes de imprimir (**cola de impresión**) hasta que la impresora queda libre y son dirigidos a ella para ser impresos.

Se puede especificar el orden en que se van a imprimir, el número de copias, la impresora a usar, el formato de impresión que se va a utilizar, si se coloca una primera página identificativa del trabajo (**banner**), etc.

DOMINIOS Y SERVICIOS DE DIRECTORIO

Servidor independiente

La gran mayoría de las primeras redes incorporaban un único servidor (**servidor independiente**) por lo que los usuarios no tenían excesivas dificultades para localizar sus archivos, impresoras y otros recursos para ser compartidos. Los archivos podían encontrarse con comandos de *MS-DOS*, las impresoras se podían seleccionar fácilmente de una lista, los usuarios eran dados de alta por el administrador de la red y no necesitaban disponer de grandes conocimientos de redes.

Añadir un segundo servidor significaba, necesariamente, alguna complicación. Cada servidor mantenía su propia lista de usuarios y recursos por lo que debían crearse y mantenerse de forma separada (si era necesario cambiar a un usuario o una impresora de servidor, había que borrarlo de uno y crearlo en el otro).

Los usuarios debían conectarse e introducir su contraseña para cada servidor (aunque podía ser automatizado) y los administradores de redes tenían que estar haciendo llamadas para sincronizar los servidores.

También surgía el problema de que los usuarios debían conocer qué servidor era el que administraba a la impresora que quería utilizar y en qué lugar se encontraban los archivos que necesitaba.

Y el problema podía ir creciendo si se añadían más servidores a la red.

Servicios de Directorio

Los **servicios de directorio** es un paso más en la mejora de la organización de la red. Permiten que un usuario se conecte a la red garantizándose el acceso a los recursos compartidos sin preocuparse por el servidor donde están disponibles, en lugar de tener que conectarse a varios servidores.

Los usuarios no necesitan indicar a qué servidor se conectan (ellos se conectan a la red) ni en qué servidor se encuentra la impresora que quieren utilizar.

Sin embargo, es importante tener cuidado con la planificación de la red (por lo que será necesario que todos los departamentos se involucren en su organización) y los administradores de servicios de directorio necesitarán ser más cualificados que los administradores de servidores independientes.

Grupos de trabajo

Los **grupos de trabajo** son conceptualmente contrarios a los servicios de directorio.

Los servicios de directorio se administran de forma centralizada y los grupos de trabajo son dirigidos por los usuarios cuando reúnen los recursos de sus ordenadores.

Con una conexión punto a punto, los usuarios comparten los recursos de sus ordenadores con otros usuarios (así, éstos pueden utilizar los archivos, las

impresoras, compartir un módem o un *CD-ROM* de todos y cada uno de los ordenadores del grupo de trabajo).

Los usuarios individuales administran los recursos de sus ordenadores, indicando qué recursos pueden ser compartidos y cuáles van a tener un uso restringido.

Este tipo de redes puede tener dos problemas en grandes organizaciones:

- Algunos recursos compartidos son difíciles de localizar para los usuarios.
- Los recursos se comparten con un grupo limitado de colaboradores.

Microsoft introdujo el concepto de trabajo en grupo con *Windows 3.11 para Trabajo en Grupo* y permitía establecer grupos que podían fácilmente ver y compartir sus recursos (la única seguridad de la que estaba provisto era el uso de contraseñas para restringir el uso de determinados recursos a usuarios específicos). Para localizar recursos en la red se utilizaban servicios de exploración.

Posteriormente, con *Windows NT* y *Windows 95*/*98* se suministraban dos utilidades (*Entorno de Red* y *Explorador*) que permitían explorar la red e identificar recursos a los que conectarse.

Dominios

El **dominio** fue introducido por *Microsoft* para *Windows NT* y toma prestados conceptos de los grupos de trabajo y de los servicios de directorio.

Los dominios son un sistema que posibilita dividir redes extensas en redes parciales reducidas que simplifican el trabajo de administración. Comprenden un grupo de ordenadores, usuarios y recursos de la red que cuentan con una base de datos de seguridad común.

De la misma manera que los grupos de trabajo, los dominios pueden ser administrados usando una mezcla de controles locales y centrales. Los dominios pueden ser desarrollados fácilmente y con menos planificación que un servicio de directorio.

Igual que los servicios de directorio, coloca los recursos de varios servidores en una única estructura organizativa. Así, a los usuarios se les conceden privilegios de conectarse a un dominio en lugar de conectarse a servidores independientes.

Los servidores que forman parte de un dominio muestran sus servicios a los usuarios y éstos pueden conectarse a aquellos a los que se les ha concedido permiso.

Se pueden ver los recursos de un dominio mucho mejor que se verían en un grupo de trabajo y con un nivel de seguridad mayor.

Cuando sea necesario configurar varios dominios, los administradores pueden establecer relaciones de confianza entre los dominios. Dichas relaciones de confianza simplifican la administración de la red ya que un usuario necesitará tener únicamente una cuenta (los otros dominios confían en que el dominio al que pertenece el usuario autentifique su conexión).

El acceso de un usuario a los recursos de un dominio es supervisado por un controlador de dominio (en el que dispone de una cuenta y una contraseña que es usada para un control de acceso a los recursos).

Un servidor puede actuar de tres maneras dentro de un dominio:

- **Controlador principal de dominio**. Es un servidor en el que almacena la copia maestra de la base de datos de grupos y usuarios del dominio.

- **Controlador de reserva de dominio**. Es otro servidor en el que se almacena una copia de seguridad de la base de datos de grupos y usuarios del dominio.

- **Servidor independiente**. Es otro u otros servidores que participan en un dominio únicamente para compartir sus recursos.

Directorio Activo

El **Directorio Activo** es la implementación de los **Servicios de Directorio** para *Windows 2000/2003*. Su objetivo fundamental es ampliar las funciones del sistema de dominios para facilitar la gestión y administración de las redes.

Su estructura se basa en los siguientes conceptos:

- **Dominio**. Es la estructura fundamental. Permite agrupar todos los objetos que se administrarán de forma estructurada y jerárquica.

- **Unidad organizativa**. Es una unidad jerárquica inferior del dominio que puede estar compuesta por una serie de objetos y/o por otras unidades organizativas.

- **Grupos**. Son conjuntos de objetos del mismo tipo y se utilizan fundamentalmente para la asignación de derechos de acceso a los recursos.
- **Objetos**. En una representación de un recurso de red (usuarios, ordenadores, impresoras, etc.).

PAQUETES DE DATOS

La transmisión de datos de gran extensión en formato de un único bloque no es conveniente y, por tanto, los datos a enviar se dividirán en segmentos más pequeños llamados **paquetes**.

Éstos se dividen en cuatro partes:

- **Cabecera**, que está formada por el identificativo del bloque de comienzo, el identificativo del lugar del destino del paquete, el identificativo del origen del paquete y la información referente al protocolo que se está utilizando.
- **Información**, que contiene el texto o la parte del texto que se va a transmitir.
- **Control de errores**, que contiene la información necesaria para que el sistema pueda verificar si los datos del paquete se han recibido correctamente.
- **Bloque final**, que contiene la información que indica que el paquete ha finalizado.

<table>
<tr><td colspan="4">CABECERA</td><td rowspan="2">INFORMACIÓN</td><td rowspan="2">CONTROL DE ERRORES</td><td rowspan="2">BLOQUE FINAL</td></tr>
<tr><td>BLOQUE DE COMIENZO</td><td>DIRECCIÓN DE DESTINO</td><td>DIRECCIÓN DE ORIGEN</td><td>PROTO COLO</td></tr>
</table>

Figura 1.2. Representación esquemática de un paquete de datos

Además de estas cuatro partes, también se incluye, en cada paquete de datos, un número de secuencia que sirve para que todos los paquetes recompongan el mensaje completo en el orden correcto, y otra información de control que permite evitar el envío de paquetes duplicados y/o la pérdida de uno de ellos.

CODIFICACIÓN DE LOS DATOS

En informática, la unidad más pequeña de información es el **bit** (dígito binario). La información que contiene son: unos o ceros que se utilizan para indicar si hay presencia o no de carga eléctrica.

La unión de ocho **bits** forma un **byte** u **octeto** y es la agrupación básica de información binaria equivalente a un carácter.

Para el intercambio de información entre ordenadores se han desarrollado distintos sistemas de codificación, siendo el más común el código **ASCII** (**American Standard Code for Information Interchange**). Es un código que emplea siete **bits** más un octavo como control de paridad (*bit* que se añade en situación 1 ó 0 para que el número total de *bits* en situación 1 sea par).

Al principio sólo existían 128 códigos (del 0 al 127) que representaban las letras minúsculas, mayúsculas, los números, los signos de puntuación y los caracteres de control que se usan para dar instrucciones de impresión.

Posteriormente, se añadieron los códigos ampliados que contenían caracteres griegos, caracteres gráficos, las vocales acentuadas y la Ñ.

Actualmente los códigos **ASCII** son 256 que van desde el 0 al 255 (ver figura 1.3).

0		1	(	2	)	3	⊂	4	⊄
5	⊇	6	⊆	7		8	3	9	
10	4	11	%	12	&	13	*	14	+
15	ə	16	<	17	=	18	⎤	19	.
20	&	21	ə	22	,	23	0	24	8
25	9	26	⎢	27	″	28	2	29	⎠
30		31		32		33	!	34	"
35	#	36	$	37	%	38	&	39	'
40	(	41	)	42	*	43	+	44	,
45	-	46	.	47	/	48	0	49	1
50	2	51	3	52	4	53	5	54	6
55	7	56	8	57	9	58	:	59	;
60	<	61	=	62	>	63	?	64	@
65	A	66	B	67	C	68	D	69	E
70	F	71	G	72	H	73	I	74	J
75	K	76	L	77	M	78	N	79	O
80	P	81	Q	82	R	83	S	84	T
85	U	86	V	87	W	88	X	89	Y
90	Z	91	[	92	\	93	]	94	^
95	_	96	`	97	a	98	b	99	c
100	d	101	e	102	f	103	g	104	h
105	i	106	j	107	k	108	l	109	m
110	n	111	o	112	p	113	q	114	r
115	s	116	t	117	u	118	v	119	w
120	x	121	y	122	z	123	{	124	|
125	}	126	~	127	–	128	Ç	129	ü
130	é	131	â	132	ä	133	à	134	å
135	ç	136	ê	137	ë	138	è	139	ï
140	î	141	ì	142	Ä	143	Å	144	É
145	æ	146	Æ	147	ô	148	ö	149	ò
150	û	151	ù	152	ÿ	153	Ö	154	Ü
155	ø	156	,	157	Ø	158	H	159	/
160	á	161	í	162	ó	163	ú	164	ñ
165	Ñ	166	0	167	1	168	)	169	7
170	5	171	2	172	3	173	(	174	*
175	+	176	?	177	?	178	?	179	?
180	?	181	Á	182	Â	183	À	184	8
185	?	186	?	187	?	188	?	189	4
190	–	191	?	192	?	193	?	194	?
195	?	196	?	197	?	198	ã	199	Ã
200	?	201	?	202	?	203	?	204	?
205	?	206	?	207	9	208	ð	209	Ð
210	Ê	211	Ë	212	È	213	2	214	Í
215	Î	216	Ï	217	?	218	?	219	?
220	?	221	|	222	Ì	223	?	224	Ó
225	ß	226	Ô	227	Ò	228	õ	229	Õ
230	µ	231	þ	232	Þ	233	Ú	234	Û
235	Ù	236	ý	237	Ý	238	-	239	´
240	–	241	∀	242	=	243	:	244	&
245	ə	246	)	247	,	248	E	249	¨
250	A	251	o	252	;	253	5	254	#

Figura 1.3. Códigos ASCII

NIVELES OSI

Al principio del desarrollo de la informática, cada fabricante establecía los procedimientos de comunicación entre sus ordenadores de forma independiente, por lo que resultaba muy difícil, por no decir imposible, la comunicación entre ordenadores de fabricantes distintos.

Poco a poco se fue haciendo necesario disponer de unas normas comunes que permitiesen la intercomunicación entre todos los ordenadores.

De todos los protocolos propuestos destaca el modelo *OSI* (*Open Systems Interconnection*), cuya traducción al castellano es *Interconexión de Sistemas Abiertos,* que fue propuesto por la *Organización Internacional de Normalización (ISO)*.

ISO, que es una organización no gubernamental fundada en 1947, tiene por misión la coordinación del desarrollo y aprobación de estándares a nivel internacional. Su ámbito de trabajo cubre todas las áreas, incluyendo las redes locales, a excepción de las áreas electrotécnicas que son coordinadas por *IEC* (*International Electrotechnical Commission*).

El modelo *OSI*, cuya actividad se empezó a desarrollar en 1977 y llegó a constituirse como estándar internacional en 1983, trata de establecer las bases para la definición de protocolos de comunicación entre sistemas informáticos.

Propone dividir en niveles todas las tareas que se llevan a cabo en una comunicación entre ordenadores. Todos los niveles estarían bien definidos y no interferirían con los demás. De ese modo, si fuera necesario una corrección o modificación en un nivel, no afectaría al resto.

En total se formarían siete niveles (los cuatro primeros tendrían funciones de comunicación y los tres restantes de proceso). Cada uno de los siete niveles dispondría de los protocolos específicos para el control de dicho nivel.

NIVEL 1	FÍSICO
NIVEL 2	ENLACE DE DATOS
NIVEL 3	RED
NIVEL 4	TRANSPORTE
NIVEL 5	SESIÓN
NIVEL 6	PRESENTACIÓN
NIVEL 7	APLICACIÓN

Figura 1.4. Niveles OSI

Nivel físico

En este nivel se definen las características eléctricas y mecánicas de la red necesarias para establecer y mantener la conexión física (se incluyen las dimensiones físicas de los conectores, los cables y los tipos de señales que van a circular por ellos). Los sistemas de redes locales más habituales definidos en este nivel son: *Ethernet*, red en anillo con paso de testigo (*Token Ring*) e interfaz de datos distribuidos por fibra (*FDDI*, *Fiber Distributed Data Interface*).

Nivel de enlace de datos

Se encarga de establecer y mantener el flujo de datos que discurre entre los usuarios. Controla si se van a producir errores y los corrige (se incluye el formato de los bloques de datos, los códigos de dirección, el orden de los datos transmitidos, la detección y la recuperación de errores). Las normas *Ethernet* y *Token Ring* también están definidas en este nivel.

Nivel de red

Se encarga de decidir por dónde se han de transmitir los datos dentro de la red (se incluye la administración y gestión de los datos, la emisión de mensajes y la regulación del tráfico de la red). Entre los protocolos más utilizados definidos en este nivel se encuentran: *Protocolo Internet* (*IP, Internet Protocol*) y el *Intercambio de paquetes entre redes* (*IPX*, *Internetwork Packet Exchange*) de *Novell*.

Nivel de transporte

Asegura la transferencia de la información a pesar de los fallos que pudieran ocurrir en los niveles anteriores (se incluye la detección de bloqueos, caídas del sistema, asegurar la igualdad entre la velocidad de transmisión y la velocidad de recepción y la búsqueda de rutas alternativas). Entre los protocolos de este nivel más utilizados se encuentran el *Protocolo de Control de la Transmisión* (*TCP*, *Transmission Control Protocol*) de *Internet*, el *Intercambio Secuencial de paquetes* (*SPX*, *Sequenced Packet Exchange*) de *Novell* y *NetBIOS/NetBEUI* de *Microsoft*.

Nivel de sesión

Organiza las funciones que permiten que dos usuarios se comuniquen a través de la red (se incluyen las tareas de seguridad, contraseñas de usuarios y la administración del sistema).

Nivel de presentación

Traduce la información del formato de la máquina a un formato comprensible por los usuarios (se incluye el control de las impresoras, emulación de terminal y los sistemas de codificación).

Nivel de aplicación

Se encarga del intercambio de información entre los usuarios y el sistema operativo (se incluye la transferencia de archivos y los programas de aplicación).

Proceso de la comunicación

El proceso que se produce desde que un usuario envía un mensaje hasta que llega a su destino consiste en una bajada a través de todos los niveles (con sus correspondientes protocolos) desde el nivel séptimo hasta llegar al primero. Allí se encontrará en el canal de datos que le dirigirá al usuario destino y volverá a subir por todos los niveles hasta llegar al último de ellos.

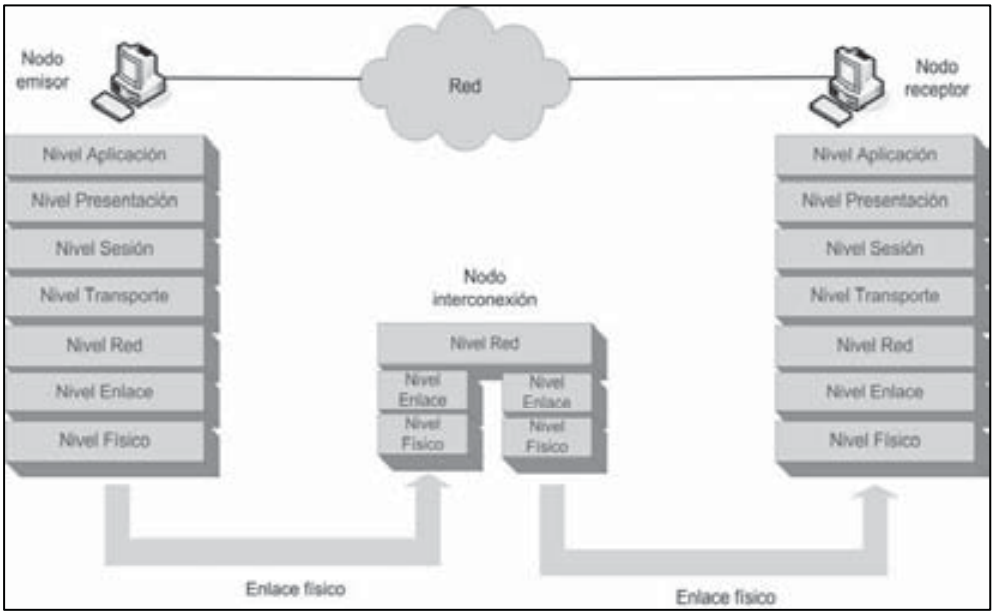


Figura 1.5. Proceso de comunicación del modelo OSI

En el gráfico anterior se puede observar lo siguiente:

- Los niveles inferiores proporcionan servicios a los niveles superiores.
- Cada nivel dispone de un conjunto de servicios.
- Los servicios están definidos mediante protocolos.
- Los programadores y diseñadores de productos sólo deben preocuparse por los protocolos del nivel en el que trabajan, los servicios proporcionados a los niveles superiores y los servicios proporcionados por los niveles inferiores.

Capítulo 2

CONCEPTOS BÁSICOS Y HARDWARE DE RED

ADAPTADORES DE RED

Los adaptadores o tarjetas de red actúan como la interfaz física o conexión entre el ordenador y el cable de red.

Se colocan en una ranura de expansión de cada ordenador de la red. Después de que la tarjeta ha sido instalada, se conecta el cable de red al conector de la misma para establecer la conexión física entre el ordenador y el resto de la red.

Una tarjeta de red realiza las siguientes acciones:

- **Prepara los datos del ordenador para su envío a la red**. Los datos se mueven en el ordenador, a través del *bus de datos*, en forma de *bits* en paralelo (los viejos buses, como los usados en el original *IBM-PC*, se conocían como buses de 8 *bits* ya que sólo podían mover 8 *bits* simultáneamente. El *IBM-PC-AT* usaba un bus de 16 *bits*. Actualmente los ordenadores usan buses de 32 *bits*) y, cuando llegan a la tarjeta, los transmite en forma de *bits* en serie.

- **Envía dichos datos a la red** indicando su dirección para distinguirlos de las otras tarjetas de la red (la dirección *MAC* son 12 dígitos hexadecimales y está determinadas por el *IEEE*. El comité asigna bloques de direcciones a cada fabricante de tarjetas. Los fabricantes introducen esas direcciones en *chips* en las tarjetas con un proceso conocido como *burning*, nacimiento de la dirección en la tarjeta. Con este proceso, cada tarjeta y, por lo tanto, cada ordenador, tiene una dirección física única en la red).

- Controla el flujo de datos entre el ordenador y el sistema de cableado.

- Recibe los datos entrantes en serie del cable y los traduce en *bytes* en paralelo que el ordenador pueda comprender.

Antes de que la tarjeta emisora envíe los datos a la red, se establece un diálogo electrónico con la tarjeta receptora para que ambas se pongan de acuerdo en lo siguiente:

- El tamaño máximo de los paquetes de datos que se quieren enviar.

- El total de datos a ser enviados antes de la confirmación.

- El intervalo de tiempo entre cada envío de paquetes de datos.

- El tiempo a esperar antes de que sea enviada la confirmación.

- Cuántos datos se pueden almacenar en la memoria de cada tarjeta.

- La velocidad de transmisión de los datos.

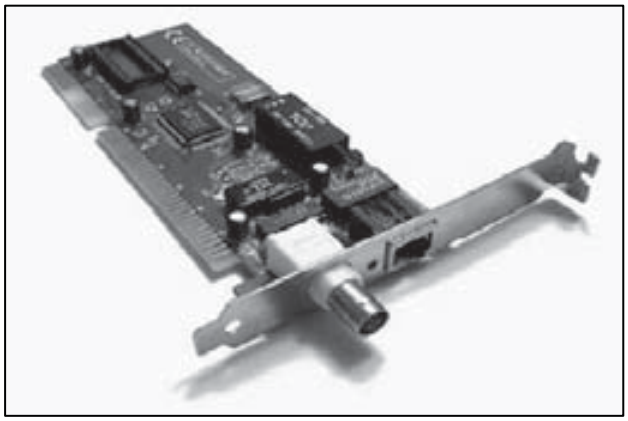


Figura 2.1. Tarjeta de red con un conector BNC y otro RJ45

Cada tarjeta indica a la otra sus parámetros y acepta (o se adapta) los parámetros de la otra. Cuando todos los detalles de la comunicación han sido determinados, las dos tarjetas empiezan a enviar o recibir datos.

Cada tarjeta de red puede tener dos conectores integrados (*BNC* o *RJ45*) y, normalmente, determina automáticamente en el que está conectado el cable de red.

TRANSMISIÓN DE LOS DATOS

Se entiende por **transmisión de los datos** al proceso de transporte de la información codificada de un punto a otro.

En toda transmisión de datos se ha de aceptar la información, convertirla a un formato que se pueda enviar rápidamente y de forma fiable, transmitir los datos a un determinado lugar y, una vez recibidos de forma correcta, volverlos a convertir al formato que el receptor pueda reconocer y comprender.

Todas esas acciones forman el proceso de transmisión, que puede dividir el proceso de transmisión de datos en tres funciones: edición, conversión y control.

- Las funciones de edición dan el formato adecuado a los datos y se encargan de controlar los errores.
- Las funciones de conversión se encargan de convertir los datos al formato adecuado.
- Las funciones de control se ocupan del control de la red y del envío y recepción de los mensajes.

Todas estas funciones se implementan por medio de protocolos.

MEDIOS DE TRANSMISIÓN

Los medios que se utilizan para la transmisión de datos se clasifican en guiados y no guiados. Los **medios guiados** son aquellos que utilizan un medio sólido (un cable) para la transmisión de datos y los no guiados utilizan el aire para ello: son los medios inalámbricos.

Los cables (medios guiados) transmiten impulsos eléctricos o lumínicos. Los bits se transforman en la tarjeta de red y se convierten en señales eléctricas o lumínicas específicas que están determinadas por el protocolo que implemente esa red.

La velocidad de transmisión, el alcance y la calidad (ausencia de ruidos e interferencias) son los elementos que caracterizan este tipo de medio. La evolución de esta tecnología ha estado orientada por la optimización de estas tres variables.

Podemos considerar tres tipos de medios guiados distintos:

- Par trenzado.
- Cable coaxial.
- Fibra óptica.

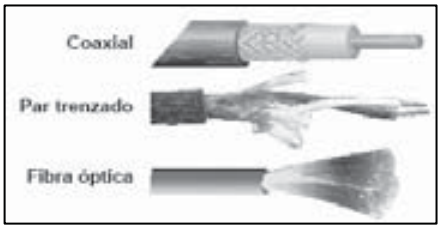


Figura 2.2. Los tres tipos de cables

En el siguiente esquema (aun con riesgo de realizar una excesiva simplificación) se muestran las características comparadas de los tres tipos de cables utilizados para transmisión de voz y datos:

	Par trenzado	Coaxial	Fibra óptica
Ancho de banda	Bajo	Moderado	Muy alto
Instalación	Sencilla	Fácil	Difícil
Longitud	Baja	Moderada	Muy alta
Costo	Barato	Moderado	Muy caro
Fiabilidad de la transmisión	Baja	Alta	Muy Alta
Interferencias	Alta	Moderada	Ninguna
Seguridad	Baja	Baja	Alta
Topología	Bus Estrella Anillo	Bus - -	- Estrella Anillo

Cable de par trenzado

Este cable consiste en pares de hilos trenzados y recubiertos de una capa aislante externa. Es de fácil instalación y ofrece cierta protección contra las interferencias externas. Puede estar apantallado (**STP**) con una impedancia de 120-150 ohmios o sin apantallar (**UTP**) con una impedancia de 100 ohmios. Los conectores que se utilizan son los denominados **RJ45**.

En función de sus características se pueden clasificar en cuatro categorías:

- **Categoría 3**. Se utiliza para transmitir datos con una velocidad de transmisión de hasta 10 *Mbps* con longitudes de segmento inferiores a 100 metros y una longitud máxima de red de 500 metros.

- **Categoría 4**. Se utiliza para transmitir datos con una velocidad de transmisión de hasta 16 *Mbps* (actualmente está en desuso).

- **Categoría 5**. Se utiliza para transmitir datos con una velocidad de transmisión de hasta 100 *Mbps*.

- **Categoría 6**. Se utiliza para transmitir datos con una velocidad de transmisión de hasta 1000 *Mbps*. Es el más utilizado actualmente.

Figura 2.3. Cables de par trenzado apantallado y sin apantallar

Cable coaxial

Es un cable formado por un hilo conductor central rodeado de un material aislante que, a su vez, está rodeado por una malla fina de hilos de cobre o aluminio o una malla fina cilíndrica. Todo el cable está rodeado por un aislamiento que le sirve de protección para reducir las emisiones eléctricas.

Se usa normalmente para datos y para los sistemas de antenas colectivas de televisión.

Trasmite una sola señal a una velocidad de transmisión alta.

En función de sus características se clasifica en dos categorías:

- **Cable coaxial grueso** (**10BASE5**). Tiene un grosor de 0,5 pulgadas, lleva un conector tipo **N**, alcanza una velocidad de transmisión de 10 *Mbps* y una longitud máxima de 500 metros de segmento de red. También se denomina **Thick Ethernet**.

- **Cable coaxial delgado** (**10BASE2**). Tiene un grosor de 0,25 pulgadas, lleva un conector tipo **BNC**, alcanza una velocidad de transmisión de 10 *Mbps* y una longitud máxima de 200 metros de segmento de red. También se denomina **Thin Ethernet**.

Figura 2.4. Cable coaxial con conector BNC

Cable de fibra óptica

Está formado por un cable compuesto por fibras de vidrio (o plástico). Cada filamento tiene un núcleo central de fibra de vidrio con un alto índice de refracción que está rodeado de una capa de material similar pero con un índice de refracción menor. De esa manera aísla las fibras y evita que se produzcan interferencias entre filamentos contiguos a la vez que protege al núcleo. Todo el conjunto está protegido por otras capas aislantes y absorbentes de luz.

Está formado por tres componentes:

- **Transmisor de energía óptica**. Lleva un modulador para transformar la señal electrónica entrante a la frecuencia aceptada por la fuente luminosa, la cual convierte la señal electrónica (electrones) en una señal óptica (fotones) que se emite a través de la fibra óptica.

- **Fibra óptica**. Su componente es el silicio y se conecta a la fuente luminosa y al detector de energía óptica. Dichas conexiones requieren una tecnología compleja.

- **Detector de energía óptica**. Normalmente es un fotodiodo que convierte la señal óptica recibida en electrones (es necesario también un amplificador para regenerar la señal).

Puede alcanzar velocidades muy altas a grandes distancias sin necesidad de usar repetidores (el producto de la distancia en kilómetros por la velocidad en *Mbps* no puede ser superior a 30. Por ejemplo, puede alcanzar una velocidad de 50 *Mbps* en una distancia de 600 metros o una velocidad 10 *Mbps* a 3.000 metros. Experimentalmente, se han llegado a conseguir velocidades de 200.000 *Mbps*).

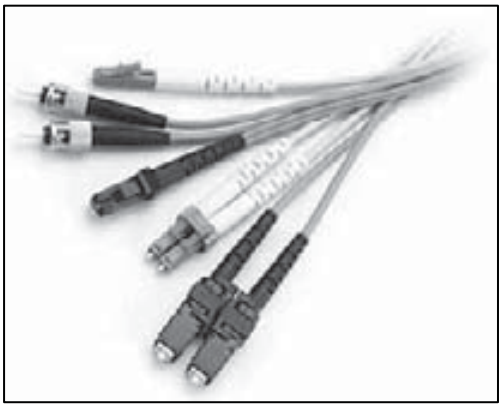


Figura 2.5. Cable de fibra óptica con sus conectores

Medios no guiados

Los medios no guiados se basan en la propagación de ondas electromagnéticas por el espacio. Una radiación electromagnética tiene una naturaleza dual, como onda y como corpúsculo, y su comportamiento dependerá de las características ondulatorias de la radiación, especialmente de la longitud de onda.

Se pueden dar los siguientes:

- **Ondas de radio**. Son ondas electromagnéticas cuya longitud de onda es superior a los 30 cm. Son capaces de recorrer grandes distancias, y pueden atravesar materiales sólidos, como paredes o edificios. Son ondas multi-direccionales, es decir, se propagan en todas las direcciones. Su mayor problema son las interferencias entre usuarios. Estas ondas son las que emplean las redes Wi-Fi, Home RF o Bluetooth.

- **Microondas**. Se basan en la transmisión de ondas electromagnéticas cuya longitud de onda varía entre 30 cm y un milímetro. Estas ondas viajan en línea recta, por lo que emisor y receptor deben estar alineados cuidadosamente. Tienen dificultades para atravesar edificios. Debido a la propia curvatura de la tierra, la distancia entre dos repetidores no debe exceder de unos 80 Kms. de distancia. Es una forma económica para comunicar dos zonas geográficas mediante dos torres suficientemente altas para que sus extremos sean visibles.

- **Infrarrojos**. Son ondas electromagnéticas (longitud de onda entre 1 milímetro y 750 nanómetros) direccionales incapaces de atravesar

objetos sólidos (paredes, por ejemplo) que están indicadas para transmisiones de corta distancia. Las tarjetas de red inalámbricas utilizadas en algunas redes locales emplean esta tecnología: resultan muy cómodas para ordenadores portátiles. Sin embargo, no se consiguen altas velocidades de transmisión.

- **Ondas de luz**. Las ondas láser son unidireccionales. Se pueden utilizar para comunicar dos edificios próximos instalando en cada uno de ellos un emisor láser y un fotodetector. A mayor longitud de onda de la radiación, el comportamiento se asemeja más al ondulatorio, mientras que si se disminuye la longitud de onda de la radiación, se produce una aproximación al comportamiento de la materia.

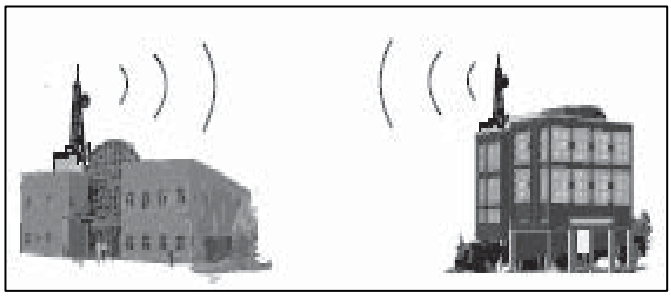


Figura 2.6. Transmisión por microondas entre dos edificios

DISPOSITIVOS DE INTERCONEXIÓN

Entre los equipos que se utilizan para llevar a cabo una transmisión de datos entre distintos equipos (tanto para LAN como para WAN), se encuentran los siguientes:

Módem

Es un equipo que convierte las señales digitales del ordenador a las analógicas de la línea telefónica (modulación), las envía a otro ordenador y, cuando las recibe éste, las vuelve a convertir de analógicas a digitales (demodulación). Permite conectar equipos que están muy separados físicamente o para acceder a Internet, a través de la red telefónica conmutada. Actualmente están en desuso.

Figura 2.7. Módem externo

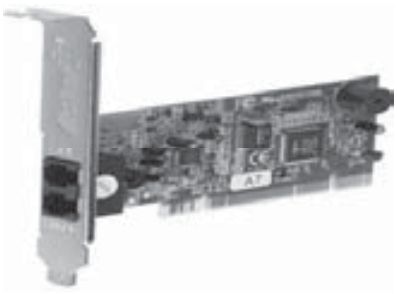


Figura 2.8. Módem interno

Módem de cable

El módem de cable es un dispositivo que permite la provisión de servicios de datos de banda ancha a través de las redes de los operadores de televisión por cable.

Los operadores de cable han ofrecido tradicionalmente servicios de televisión por cable utilizando una infraestructura basada en el cable coaxial. Sin embargo, la modernización de estas infraestructuras ha permitido a dichos operadores proporcionar servicios de datos bidireccionales, especialmente el servicio de conexión a Internet.

Figura 2.9. Módem de cable

La red de cable utiliza un medio compartido en el que los usuarios no tienen un ancho de banda fijo en recepción que permite reducir los costes de mantenimiento y operación frente a tecnologías como la RDSI o la ADSL en las

que por cada usuario conectado simultáneamente al sistema debe existir una "línea física" entre el usuario y la central local. Esto no sólo supone el desperdicio en costes por mantener la línea ocupada, cuando no existe transmisión de datos, sino también por el gran número de dispositivos y complejidad del equipamiento de la central cuando el número de usuarios es elevado.

El inconveniente de la red de cable es que el ancho de banda se divide entre el número de usuarios conectados por lo que, a mayor número de usuarios, más lenta será la conexión y viceversa.

Módem ADSL

En las décadas de los años 80 y 90, los módems fueron los dispositivos de transmisión de datos más extendidos. Antes de que las operadoras de telecomunicaciones construyeran las grandes redes digitales, la única forma de transmitir datos a larga distancia era utilizando la red telefónica conmutada y en este escenario los módems eran fundamentales.

Actualmente, el desarrollo de las redes digitales así como el uso de nuevas tecnologías como ADSL y cable han propiciado que en muchos casos los módems tradicionales hayan dejado de utilizarse. Además, la velocidad de transmisión de datos utilizando dichos módems había alcanzado su límite.

La tecnología ADSL se utiliza para aprovechar todo el ancho de banda que ofrece el bucle local de abonado y multiplexar las señales de voz y datos (se verá más en profundidad en un capítulo posterior). Ofrece lo que se conoce comúnmente como acceso de banda ancha a las redes de datos, especialmente Internet. Su inconveniente es que requiere la adaptación de las infraestructuras de comunicaciones de los operadores, además su uso depende de un factor importante que es la longitud del bucle de abonado, siendo imposible su uso para distancias mayores a 5 Km.

La velocidad de transmisión depende de la distancia a la central y, aunque actualmente, el límite teórico en sentido bajada es de 13 Mbps, en la práctica las velocidades máximas típicas son de 8 Mbps. La velocidad máxima teórica de subida está en 1'5 Mbps aunque en la práctica se puede alcanzar hasta 1 Mbps. Las versiones ADSL2 y ADSL2+ ofrecen tasas de transferencia superiores de hasta 24 Mbps teóricos aunque eso sí, con una menor cobertura.

Figura 2.10. Módem ADSL

Lógicamente, para hacer uso de la tecnología ADSL es necesario utilizar un módem o un router diseñado a tal efecto. Los módems ADSL, al igual que los módems de banda vocal, pueden ser internos o externos aunque la mayor parte de los que se han comercializado son externos. A diferencia de los módems de banda vocal, los módems ADSL externos utilizan el interfaz USB para su conexión con el ordenador debido sobre todo a las velocidades más altas que se alcanzan con este interfaz.

Repetidor

Es un dispositivo encargado de regenerar la señal (no de amplificarla) en un segmento de una red homogénea ampliando su cobertura. Su forma de actuar es la siguiente: recoge la señal que circula por la red y la reenvía sin efectuar ningún tipo de interpretación de dicha señal.

Son capaces de conectar diferentes medios físicos de transmisión. Sin embargo, no suelen utilizarse para conectar redes de banda base con redes de banda ancha ya que los métodos de decodificación de la información son muy diferentes.

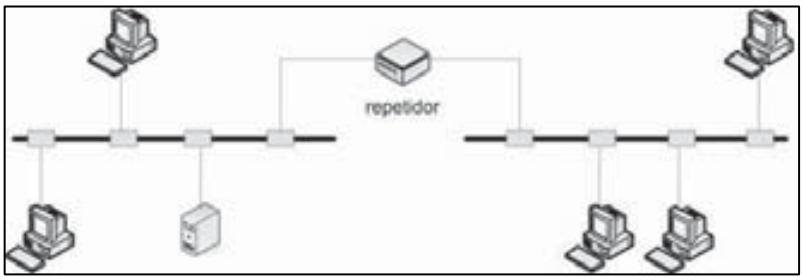


Figura 2.11. Conexión de un repetidor

Concentrador (*Hub*)

Es un equipo que permite compartir el uso de una línea entre varios ordenadores. Todos los ordenadores conectados a un concentrador pueden usar la línea, aunque no de forma simultánea, ni utilizando distintos protocolos, ni distintas velocidades de transmisión.

El concentrador simplemente regenera y transmite la señal que recibe, pero no es capaz de identificar hacia dónde va la trama de datos y en función de ello filtrar el tráfico; igualmente, tampoco pueden ser empleados para seleccionar la mejor ruta para dirigir las tramas.

Su funcionamiento es muy sencillo, todos los equipos de la red se conectan al concentrador, mediante un cable. Cuando un equipo envía un mensaje, los datos llegan al concentrador y este los regenera (mejora su calidad eléctrica) y los retransmite a todos los puestos que están conectados a cada uno de sus puertos.

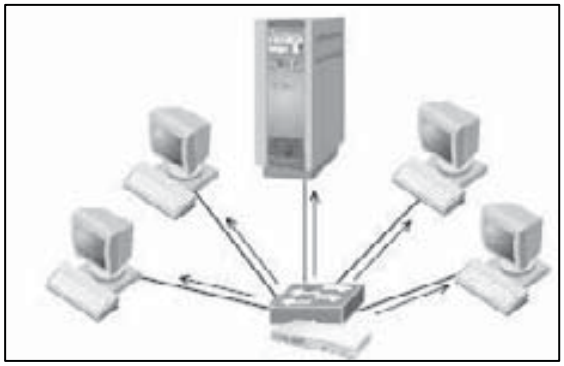


Figura 2.12. Un concentrador retransmite por todos sus puertos los mensajes que recibe

Al no filtrar el tráfico y reenviar los datos a todos los puestos puede suceder que, cuando un equipo quiera enviar una trama de datos, encuentre su zona de la red ocupada por datos que no se le han enviado, o que se produzca una colisión entre los datos enviados por otro equipo y los que acaba de enviar él. Si un concentrador tiene conectados doce equipos a sus puertos, cuando llega un mensaje, se multiplica por doce, ya que los envía por todos sus puertos, lo que aumenta enormemente el tráfico.

Conmutador (*Switch*)

Un conmutador se utiliza igual que un concentrador pero se caracteriza por no enviar los paquetes a todos los puertos, sino únicamente por el puerto correspondiente al destinatario de los datos.

Su función consiste en tomar la dirección MAC destino de una trama de datos (es la dirección que identifica a la tarjeta de red) y, en función de ella, enviar la información por el puerto correspondiente. En comparación con el concentrador, actúa más inteligentemente ya que filtra el tráfico y tiene capacidad de reconocimiento. Los datos pueden conducirse por rutas separadas, mientras que en el concentrador, las tramas son conducidas por todos los puertos.

Los conmutadores son capaces de realizar esto utilizando una mejor electrónica que la empleada por los concentradores, troceando el ancho de banda en franjas, llamadas canales, lo suficientemente grandes como para dar servicio a cada puerto de conmutación.

La diferencia entre un conmutador y un puente (*bridge*) es que el puente debe recibir todo el paquete antes de dirigirlo al puerto correspondiente y un conmutador dirige el paquete a su destino una vez recibido el encabezado del paquete (en ella se encuentra la dirección *IP* del destinatario). Gracias a ello, los conmutadores producen un retraso mínimo en la conmutación (del orden de 40 microsegundos, mientras que el puente supera los 1.000 microsegundos).

De esta manera, utilizando un conmutador se puede dividir una red en varios segmentos y limitar el tráfico al segmento o segmentos a los que pertenece el paquete. Su utilización permite que cada usuario o grupo de usuario tenga su propio segmento dedicado con ancho de banda dedicado, con una mucha menor tasa de colisiones y un mejor tiempo de respuesta en lugar de lo que ocurre en una red Ethernet tradicional en la que muchos usuarios comparten el mismo ancho de banda.

Figura 2.13. Conmutador de 24 puertos

Se pueden utilizar los conmutadores y los concentradores conjuntamente, tal y como se puede ver en la figura siguiente:

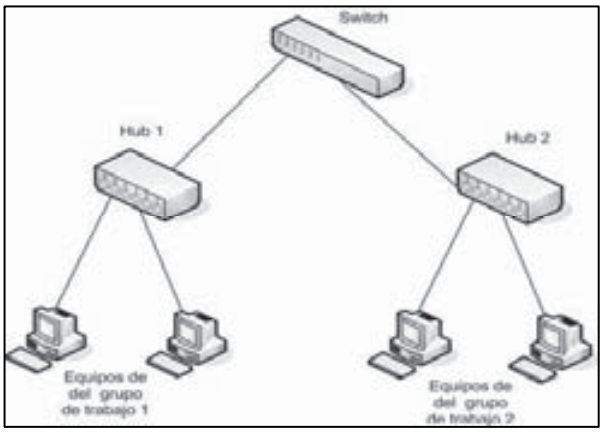


Figura 2.14. Esquema de conexionado uniendo dos hubs mediante un switch

Las diferencias principales entre un hub y un switch son las siguientes:

- Un hub es un dispositivo *pasivo* de interconexión, el switch es activo.
- Un hub realiza funciones de la capa 1 (Física) del modelo OSI y el switch en la capa 2 (Enlace de datos).
- El hub repite la señal que recibe a través de un puerto al resto de los puertos mientras que el switch toma la dirección MAC destino de una trama de datos y, en función de ella, envía la información por el puerto correspondiente.
- En un hub se produce un número más elevado de colisiones que en un switch.
- La velocidad de transmisión del hub siempre es la correspondiente al dispositivo más lento conectado mientras que el switch negocia con cada uno de los dispositivos que se conectan a él la velocidad de funcionamiento (10 ó 100 Mbps) así como si van a funcionar en modo *full-duplex* o *half-duplex*.
- El hub no es configurable mientras que el switch sí y, además, permite la creación de VLAN.
- El hub es más barato.

Puente (Bridge)

Es un sistema formado por *hardware* y *software* que permite conectar dos redes locales entre sí. Se pueden colocar en el servidor de archivos o, mejor, en el servidor de comunicaciones.

Cuando dos redes locales necesitan comunicarse entre sí, necesitan contar con un puente en cada una de ellas para poder conectarse.

Ambas redes han de usar el mismo protocolo de comunicaciones.

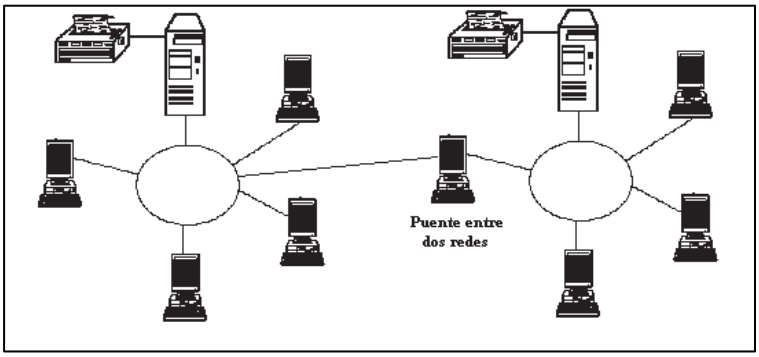


Figura 2.15. Representación esquemática de dos redes unidas por un puente

Sus funciones básicas son las de autoaprendizaje, filtrado y reenvío. Es decir, si necesita reenviar un paquete de datos a una dirección de red que no está incluida en su tabla de destinos, examina los campos de dirección del paquete (filtrado) y las dirige a la dirección que ha localizado (reenvío). A continuación, la añade a su tabla de destinos (autoaprendizaje).

La utilización de puentes para unir dos redes es una idea mejor que la configuración de una red grande que englobe a ambas. La razón está en que las redes van perdiendo rendimiento al aumentar el tráfico y se va perdiendo tiempo de respuesta, de este modo, al estar dividida la red se reduce el tráfico y el tiempo de respuesta.

Otra razón es el límite de expansión de la red grande. Todas las redes cuentan con un número máximo de estaciones que pueden soportar, si se desea sobrepasar ese número la única alternativa es crear otra red conectada por un puente.

Encaminador (Router)

Un encaminador no sólo incorpora la función de filtrado característica de los puentes, sino que, además, determina la ruta hacia su destino. Se utiliza tanto en redes de área local como en redes de área extensa. Permite la comunicación entre un equipo individual e Internet, entre una red e Internet o entre dos redes.

Las funciones de un router son:

- Interconectar redes (físicas y lógicas).
- Recibir los paquetes de datos y almacenarlos para distribuirlos progresivamente en función de la situación de la red.
- Averiguar las direcciones IP de las redes y equipos que están conectados a sus puertos para realizar un envío óptimo de los paquetes.
- Evitar la congestión de las redes.

Un router posee dos direcciones IP, una pública para acceder a Internet y otra privada para la red interna.

Se basan en la utilización de un esquema de direccionamiento jerárquico (tablas de rutas) que distinguen entre la dirección del dispositivo dentro de la red y la dirección de la red. Para ello incorporan protocolos de nivel de red.

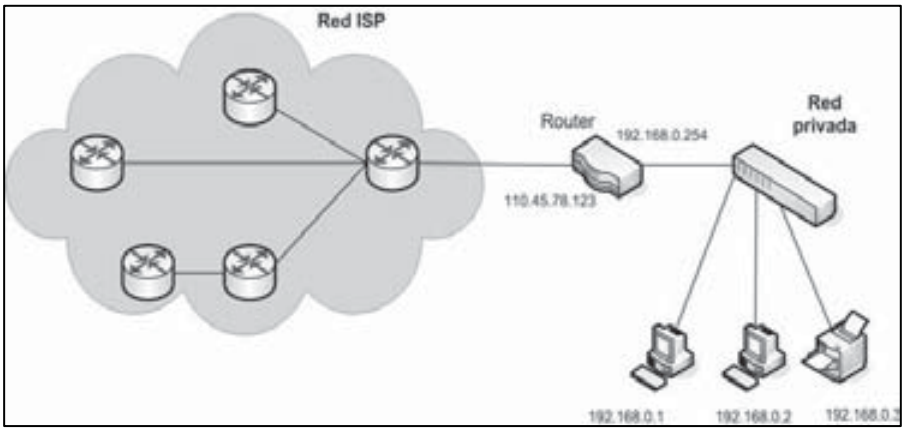


Figura 2.16. Representación esquemática de dos redes unidas por un router

Para realizar su función incorporan algún tipo de algoritmo, siendo uno de los más básicos el *Protocolo de Información de Encaminamiento* (*RIP*) que calcula la distancia entre el encaminador y la estación receptora de un paquete como el número de saltos requeridos, ignorando otros tipos de atributos como el tiempo de transferencia entre dos saltos, etc.

Los protocolos de encaminamiento varían en función de las diferentes arquitecturas de comunicaciones de red existentes, por lo que se diseñan para una arquitectura específica.

Los encaminadores se diferencian de los puentes en dos aspectos:

- Actúa sobre los paquetes transferidos entre los niveles de red de las estaciones, a diferencia de los puentes que lo hacen sobre el nivel de enlace de datos.

- Ambos equipos son, teóricamente, transparentes a las estaciones finales que comunican. Sin embargo, normalmente las estaciones tienen definido el encaminador al que deben dirigirse.

Pasarela (Gateway)

Es un sistema formado por *hardware* y *software* que permite las comunicaciones entre una red local y un gran ordenador (*mainframe*) o un miniordenador (porque utilizan protocolos de nivel de transporte, sesión, presentación y aplicación distintos). Se suelen colocar en el servidor de comunicaciones.

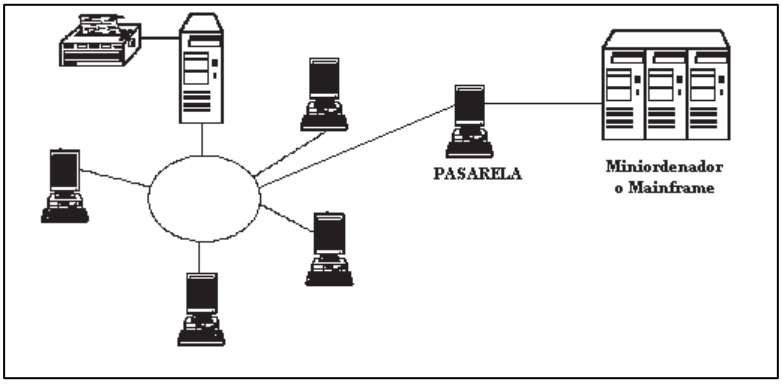


Figura 2.17. Representación esquemática de una red unida a un miniordenador utilizando una pasarela

De este modo podrá obtener datos del mini o del *mainframe* o bien enviarles datos para su almacenamiento.

La pasarela realiza la traducción completa entre las familias de protocolos, proporcionando una conectividad completa entre redes de distinta naturaleza.

El enlace entre ambos protocolos necesitará algún tipo de emulación que haga que la estación de trabajo imite el funcionamiento de un terminal y ceda el control al mini o al *mainframe*. Esta emulación se puede conseguir por medio de *software* (con un programa), de *hardware* (con una tarjeta) o de ambos.

Al igual que los encaminadores, están definidos para un determinado escenario de comunicaciones.

Pero a cambio de sus ventajas, el retraso de propagación de un paquete que atraviesa una pasarela es mucho mayor que el experimentado en los otros dispositivos.

Cortafuegos (Firewalls)

La función de un cortafuegos (*firewall*) es filtrar los intentos de establecimiento de conexión de forma que se pueda detectar e impedir el acceso al sistema a posibles intrusos sin que ni siquiera se haya llegado a establecer un enlace directo entre ellos.

El cortafuegos puede ser configurado para permitir que sólo determinadas direcciones, origen y destino, puedan acceder a su red (o desde ella).

Las funciones de cortafuegos se pueden realizar por:

- Ordenadores dedicados exclusivamente al filtrado de paquetes (servidor *proxy*).
- Encaminadores de red (*routers)* configurados para esta tarea.
- Programas de *software* para distintos sistemas operativos.
- Cualquier otro dispositivo intercalado entre la red y el exterior que soporte el filtrado de paquetes según unos parámetros previamente definidos.

Entre los posibles beneficios de utilizar cortafuegos se encuentran:

- Acceso controlado a la red.
- Protección para servicios de *Internet* que sean vulnerables.
- Administración de seguridad centralizada.
- Estadísticas de las conexiones a la red.
- Filtrado sofisticado de paquetes. Los filtros de paquetes controlan qué tipos de paquetes *IP* pueden acceder a los servicios de la red interna. Así, puede denegar paquetes, bloquear paquetes de un ordenador determinado de *Internet*, rechazar direcciones fantasmas, evitar ataques *FRAG* (un ataque *FRAG* se produce cuando se provoca un fallo en el algoritmo de reensamblado de los paquetes *IP* que se reciben debido al envío de fragmentos de paquetes trucados) o evitar ataques *SYN* (un ataque *SYN* se produce cuando se inunda un servidor con requerimientos de conexiones falsas que evitan el procesamiento de requerimientos verdaderos).
- Configuración desde un sistema de *hardware* independiente que no dependa de ningún otro sistema de *hardware* y *software*.

Entre las posibles razones para no utilizar un cortafuegos se encuentran:

- El acceso a los servicios deseados puede llegar a ser más complejo de lo normal.
- El peligro de acceso por una puerta trasera a la red se incrementa si no se tiene prevista su inutilización.
- Es necesaria una administración suplementaria de la red.
- El coste económico es mayor.
- La configuración se hace demasiado compleja para realizarla de forma adecuada.

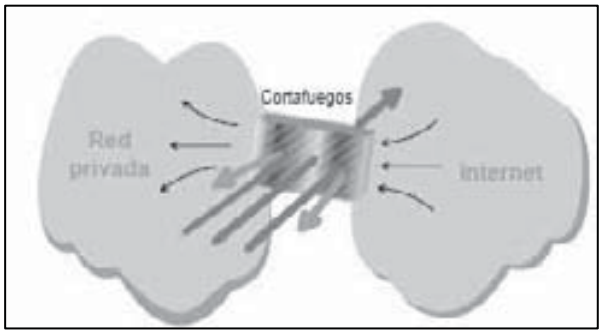


Figura 2.18. El cortafuegos controla el tráfico entre la red privada e Internet

TCP/IP

El nombre *TCP/IP* proviene de dos de los protocolos más importantes de la familia de protocolos *Internet*, el *Transmission Control Protocol* (*TCP*) y el *Internet Protocol* (*IP*).

La principal virtud de *TCP/IP* estriba en que está diseñado para enlazar ordenadores de diferentes tipos, incluyendo *PCs*, minis y *mainframes*, que ejecuten sistemas operativos distintos, sobre redes de área local y redes de área extensa y, por tanto, permite la conexión de equipos distantes geográficamente.

Otro gran factor que ha permitido su expansión es la utilización de *TCP/IP* como estándar de *Internet*.

El mayor problema de *TCP/IP* estriba en la dificultad de su configuración, por lo que no es recomendable su uso para utilizarlo en una red pequeña.

TCP/IP fue desarrollado en 1972 por el Departamento de Defensa de los Estados Unidos, ejecutándose en *ARPANET* (una red de área extensa del Departamento de Defensa). Posteriormente, una red dedicada exclusivamente a aspectos militares denominada *MILNET* se separó de *ARPANET*. Fue el germen de lo que después constituiría *Internet*.

La arquitectura *TCP/IP* transfiere datos mediante el ensamblaje de datos en paquetes. Cada paquete comienza con una cabecera que contiene información de control seguida de los datos.

El *Internet Protocol* (*IP*), un protocolo del nivel de red de *OSI*, permite a las aplicaciones ejecutarse de forma transparente sobre las redes interconectadas. De esta forma, las aplicaciones no necesitan conocer qué *hardware* está siendo

utilizado en la red y, por tanto, la misma aplicación puede ejecutarse en cualquier arquitectura de red.

El *Transmission Control Protocol* (*TCP*), un protocolo del nivel de transporte de *OSI*, asegura que los datos sean entregados, que lo que se recibe corresponde con lo que se envió y que los paquetes sean reensamblados en el orden en que fueron enviados.

UNIX se empezó a comercializar como el principal sistema operativo que utilizaba *TCP/IP* y llegaron a ser sinónimos.

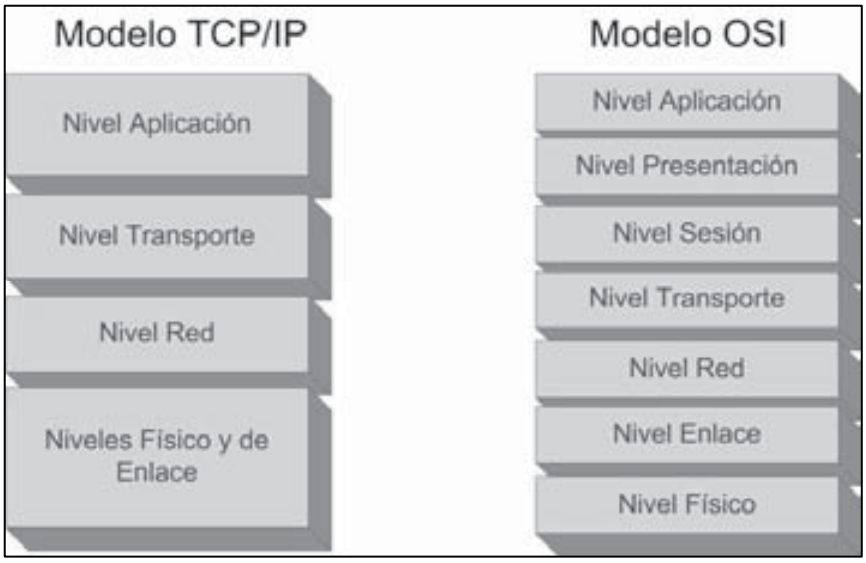


Figura 2.19. Comparación del modelo TCP/IP y el modelo OSI

Cómo denominar a un ordenador en TCP/IP

Es importante que se establezca la identificación de la estación de trabajo de una forma que evite su duplicidad dentro de todos los ordenadores que puedan conectarse.

Para ello, en *TCP/IP*, se utiliza el nombre del usuario y el nombre del dominio de la red.

Para identificar al usuario es necesario nombrarlo evitando que pueda haber dos con el mismo nombre y produzca confusiones al servidor de la red.

Para identificar a la red se utiliza el concepto de dominio. La estructura del dominio se asemeja a un árbol invertido (es decir, el tronco se encuentra en la parte superior y las ramas en la parte inferior) y cada hoja corresponde a un dominio.

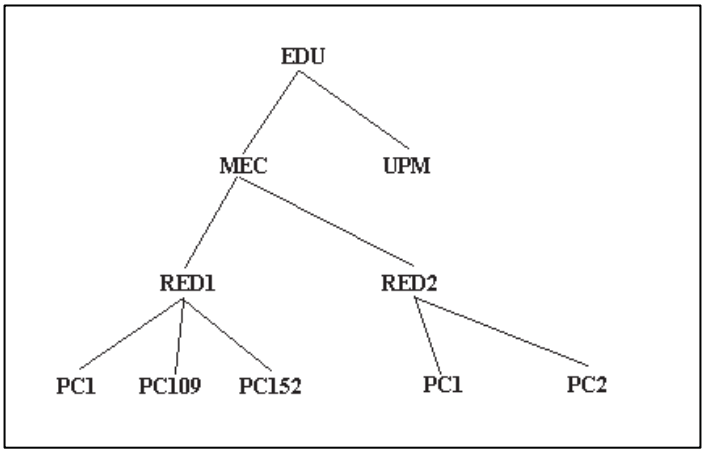


Figura 2.20. Estructura en árbol para identificar a un equipo

La identificación de un dominio está formada por varios apartados separados por un punto (por ejemplo, *RED1.MEC.EDU*). Cada uno de ellos recibe el nombre de subdominio. El subdominio situado más a la derecha es el de carácter más general y recibe el nombre de dominio de nivel alto.

El nombre de un dominio completamente calificado (*FQDN*, *Full Qualified Domain Name*) ha de empezar por el nombre de la estación de trabajo (*HOST*), un punto y el nombre de la red (*DOMINIO*). Por ejemplo, si se denomina al *PC* como *PC109* y a la red principal como *RED1*, la identificación completa de la estación de trabajo sería *PC109.RED1*.

Si, a su vez, esta red formara parte de otra red superior, se volvería a poner otro punto y el nombre de dicha red (por ejemplo, *PC109.RED1.MEC*). En este caso, después del *HOST* vendría el *SUBDOMINIO* (es posible tener varios niveles de subdominios) y, para finalizar, el *DOMINIO*.

También es interesante identificar a la institución de la que forma parte la red, así como la organización o el país a la que pertenece. Para ello, se le habrán de añadir estos dos nuevos conceptos separados, también, por puntos.

Si se toma como ejemplo la identificación *RODRIGUEZJL@PC109.RED1.MEC.EDU* se ve que el usuario (*RODRIGUEZJL*) se separa con una arroba

del dominio, que está formado por el nombre de la estación (*PC109*), de la red (*RED1*), de la institución (*MEC*) y de la organización (*EDU*).

Existe una institución que se encarga del registro de todas las direcciones *IP* y sus correspondientes dominios que se denomina *INTERNIC* y que ha delegado para España sus funciones en *REDIRIS*.

DOMINIO DE ALTO NIVEL DE ORGANIZACIÓN	
DOMINIO	SIGNIFICADO
com	Organización comercial
edu	Institución educativa
gov	Institución gubernamental
int	Organización internacional
mil	Organización militar
net	Organización de red
org	Organización sin ánimo de lucro
es	Organización española
fr	Organización francesa
uk	Organización inglesa
de	Organización alemana

Figura 2.21. Dominios de alto nivel

Direcciones IPv4

Las direcciones *IP* consiguen que el envío de datos entre ordenadores se realice de forma eficaz, de forma parecida a como se utilizan los números de teléfono en las llamadas telefónicas.

Actualmente, las direcciones *IP* de la versión actual (*Ipv4*) tienen 32 *bits*, formados por cuatro campos de 8 *bits* (octeto), cada uno, separados por puntos.

Por tanto, las direcciones *IP* están en representación binaria (por ejemplo, 01111111.00000000.00000000.00000001). Cada uno de los campos de 8 *bits* puede tener un valor que esté comprendido entre 00000000 (cero en decimal) y 11111111 (255 en decimal).

Normalmente y debido a la dificultad del sistema binario, la dirección *IP* se representa en decimal. Por ejemplo, la dirección *IP* indicada anteriormente 01111111.00000000.00000000.00000001 (en representación binaria) tiene su correspondencia con 127.0.0.1 (en representación decimal).

La forma de pasar de un sistema binario a un sistema decimal se hace por potencias de dos en función de la posición de cada uno dentro del octeto, correspondiendo cero a la primera posición a la derecha y siete a la primera posición de la izquierda (por ejemplo, 00000001 corresponde a 1 ya que $2^0=1$, 00000010 corresponde a 2 ya que $2^1=2$ y 00001000 corresponde a 8 ya que $2^3=8$).

Si hay varios unos en el octeto, se deberán sumar los resultados de las potencias de dos correspondientes a su posición (por ejemplo, 00001001 corresponde a 9 ya que $2^3+2^0=8+1=9$ y 01001001 corresponde a 73 ya que $2^6+2^3+2^0=64+8+1=73$).

Los cuatro octetos de la dirección *IP* componen una dirección de red y una dirección de equipo que están en función de la clase de red correspondiente.

Existen cinco clases de redes: *A*, *B*, *C*, *D* o *E* (esta diferenciación viene dada en función del número de ordenadores que va a tener la red).

- La **clase A** contiene 7 *bits* para direcciones de red (el primer *bit* del octeto siempre es un cero) y los 24 *bits* restantes representan a direcciones de equipo. De esta manera, permite tener un máximo de 128 redes (aunque en realidad tienen 126, ya que están reservadas las redes cuya dirección de red empieza por cero y por 127), cada una de las cuales puede tener 16.777.216 ordenadores (aunque en realidad tienen 16.777.214 ordenadores cada una, ya que se reservan aquellas direcciones de equipo, en binario, cuyos valores sean todos ceros o todos unos). Las direcciones, en representación decimal, estarán comprendidas entre 0.0.0.0. y 127.255.255.255 y la máscara de subred será de 255.0.0.0.

- La **clase B** contiene 14 *bits* para direcciones de red (ya que el valor de los dos primeros *bits* del primer octeto ha de ser siempre 10) y 16 *bits* para direcciones de equipo, lo que permite tener un máximo de 16.384 redes, cada una de las cuales puede tener 65.536 ordenadores (aunque en realidad tienen 65.534 ordenadores cada una, ya que se reservan aquellas direcciones de equipo, en binario, cuyos valores sean todos ceros o todos unos). Las direcciones, en representación decimal, estarán comprendidas entre 128.0.0.0 y 191.255.255.255 y su máscara de subred será de 255.255.0.0.

- La **clase C** contiene 21 *bits* para direcciones de red (ya que el valor de los tres primeros *bits* del primer octeto ha de ser siempre 110) y 8 *bits* para direcciones de equipo, lo que permite tener un máximo de 2.097.152 redes, cada una de las cuales puede tener 256 ordenadores (aunque en realidad tienen 254 ordenadores cada una, ya que se reservan aquellas direcciones de equipo, en binario, cuyos valores sean todos ceros o todos unos). Las direcciones, en representación decimal, estarán comprendidas entre 192.0.0.0 y 223.255.255.255 y su máscara de subred será de 255.255.255.0.

- La **clase D** se reserva todas las direcciones para multidestino (*multicasting*), es decir, un ordenador transmite un mensaje a un grupo específico de ordenadores de esta clase. El valor de los cuatro primeros *bits* del primer octeto ha de ser siempre 1110 y los últimos 28 *bits* representan los grupos multidestino. Las direcciones, en representación decimal, estarán comprendidas entre 224.0.0.0 y 239.255.255.255.

- La **clase E** se utiliza con fines experimentales únicamente y no está disponible para el público. El valor de los cuatro primeros *bits* del primer octeto ha de ser siempre 1111 y las direcciones, en representación decimal, estarán comprendidas entre 240.0.0.0 y 255.255.255.255.

La dirección de equipo indica el número que corresponde al ordenador dentro de la red (por ejemplo, al primer ordenador de una dirección de red de clase *C* 192.11.91 se le otorgará la dirección *IP* 192.11.91.1, al segundo 192.11.91.2, al cuarto 192.11.91.4 y así sucesivamente).

Segmentación de la red

Actualmente debido al uso masivo de aplicaciones cliente-servidor y multimedias que requieren la transmisión de grandes volúmenes de información, la tecnología de redes de área local, que en algunos casos data desde hace unos 20 años, se ha visto en la necesidad de transmitir un gran volumen de datos y con mayor rapidez. Esta necesidad ha obligado a buscar tecnologías que permitan aumentar el ancho de banda y mejorar, e incluso intentar asegurar, los tiempos de respuestas.

Como se ha visto anteriormente, la red *Ethernet* funciona a una velocidad de 10 *Mbps*, implementada en una topología física de configuración en bus o en una topología física de configuración en *estrella* dentro de una topología lógica de *bus* mediante el uso de concentradores, y que, como método de control de acceso, utiliza *CSMA/CD*.

Como la duración de la transmisión es limitada (ya que el tamaño máximo del paquete es de 1.526 *bytes*) y entre una transmisión y otra se debe esperar un lapso mínimo de tiempo, nadie puede adueñarse del canal de comunicación ya que en el momento de terminar de transmitir un paquete, otra estación puede iniciar una nueva.

En ese momento, puede suceder que dos nodos intenten transmitir simultáneamente. Cuando esto se produce, ambas transmisiones chocan, se mezclan y se pierde su contenido. A este proceso se le denomina **colisión**. Para superar este inconveniente, cada nodo sigue escuchando para detectar estas colisiones. Cuando detecta una colisión deja de transmitir inmediatamente, espera que no haya actividad e intenta transmitir de nuevo. Si vuelve a haber una colisión cada estación calcula un tiempo de espera aleatorio antes de volver a transmitir y así disminuir la probabilidad de una nueva colisión.

Este tipo de red tiene un excelente rendimiento en redes de carga baja o media, pero pasado este punto su rendimiento se degrada notablemente. Esto es debido a que hay una mayor cantidad de paquetes para enviar y, por tanto, mayor número de intentos de transmisiones, lo que hace que la probabilidad de que ocurran colisiones aumente drásticamente. Este aumento se traduce, además de en una disminución del ancho de banda efectivo, en un aumento del retardo de las transmisiones o deterioro del tiempo de respuesta.

Cuando se comienzan a presentar estos problemas de rendimiento, una posible solución es dividir la red en segmentos separados que se conectarán mediante puentes (*bridges*), procurando reducir el tráfico entre dichos segmentos al mínimo, pues el puente sólo dejará pasar desde un segmento a otro aquellos paquetes que vayan dirigidos específicamente a algún nodo en el segmento destino. Cuanto más segmentada esté la red, mejor será su rendimiento pues cada uno de los segmentos tendrá menos estaciones y una probabilidad mucho menor de producirse colisiones (es conveniente colocar los servidores en segmentos independientes).

La solución anterior tiene un defecto. Para que sea óptima se debe evitar el flujo de tráfico innecesario al cruzar segmentos intermedios, es decir, se debería evitar que para llegar a un segmento dado se deba pasar por otro. Bajo esta perspectiva, cada segmento en la red debería conectarse con todos los demás a través de un puente distinto. Por ello, el número de puentes necesarios es igual al número de segmentos de la red al cuadrado, pues se deben conectar cada uno de los segmentos con todos los restantes (topología *malla completa*). Esto significa que para redes medianas y grandes esta solución es impracticable, tanto por su costo como por la complejidad de su administración.

Otra posibilidad más factible es la utilización de conmutadores en lugar de puentes o de concentradores que permiten aumentar el ancho de banda, reducir el tráfico de la red y aumentar la velocidad de transmisión.

LAS DIRECCIONES IP EN UNA SEGMENTACIÓN DE RED

Cuando se explicó anteriormente la dirección *IP*, se indicó que tanto ésta como la máscara de subred estaban en función de la clase a la que pertenecía la red. Por ejemplo, la dirección *IP* (en representación binaria) correspondiente para la dirección *IP* 18.0.0.1 (en representación decimal) correspondiente a la clase *A* es la siguiente:

Dirección red	Dirección equipo		
00010010	00000000	00000000	00000001

Y su máscara de red es 255.0.0.0 que corresponde a:

Dirección red	Dirección equipo		
11111111	00000000	00000000	00000000

que indica que hay 8 *bits* para marcar la dirección de red y 24 *bits* para la dirección de equipo (11111111 corresponde a 255 en decimal).

Si la dirección *IP* (en representación binaria) correspondiente para la dirección *IP* 164.56.0.10 (en representación decimal) correspondiente a la clase B es la siguiente:

Dirección red		Dirección equipo	
10100100	00111000	00000000	00001010

Y su máscara de red es 255.255.0.0 que corresponde a:

Dirección red		Dirección equipo	
11111111	11111111	00000000	00000000

que indica que hay 16 *bits* para marcar la dirección de red y 16 *bits* para la dirección de equipo.

Si de la dirección de equipo se toman unos *bits* para indicar también la dirección de red, se estará estableciendo una **subred**. La combinación de las partes correspondientes a las direcciones de red y de subred se conoce con el nombre de **prefijo de red extendida**.

De esta manera, el ejemplo anterior quedaría así:

Dirección red		Dirección subred	Dirección equipo
10100100	00111000	11111111	00001010

DETERMINAR EL NÚMERO DE SUBREDES NECESARIAS

El primer paso a seguir cuando se desea segmentar una red es decidir el número de subredes que se necesitan y, así, establecer las direcciones *IP* de cada subred y su máscara correspondiente.

Si se toma, como ejemplo, que la red que se va a segmentar es una clase *B* (con máscara de red 255.255.0.0) y con dirección 164.56.0.0 (en representación decimal), resulta que su dirección (en representación binaria) es:

Dirección red		Dirección equipo	
10100100	00111000	00000000	00000000

Una vez realizadas las evaluaciones pertinentes, se considera que con diez subredes es suficiente para cubrir las necesidades actuales. El primer paso a seguir es convertir el número decimal 10 a su representación binaria (1010).

El número binario 1010 necesita cuatro *bits* para representarse y, por tanto, se han de tomar cuatro *bits* de la dirección de equipo para indicar la dirección de subred.

La dirección en representación binaria del ejemplo que se está indicando será:

Dirección red		Dirección subred	Dirección equipo	
10100100	00111000	1010	0000	00000000

Y su máscara de red es 255.255.240.0 que corresponde a:

Dirección red		Dirección subred	Dirección equipo	
11111111	11111111	1111	0000	00000000

que indica que hay 20 *bits* para marcar la dirección de red y 12 *bits* para la dirección de equipo (el tercer octeto será 11110000 que corresponde a 240 en decimal).

Otra manera de representar la máscara de subred es indicarla en notación alternativa indicando la dirección *IP* en decimal de la red y el número de *bits* que se toman para indicar la dirección de red (en el ejemplo, sería 164.56.0.0/20).

Otro aspecto a considerar es el número de subredes posibles que se pueden tener con la máscara 255.255.240.0.

Binario	Decimal
00000000	0
00010000	16
00100000	32
00110000	48
01000000	64
01010000	80
01100000	96
01110000	112
10000000	128
10010000	144
10100000	160
10110000	176
11000000	192
11010000	208
11100000	224
11110000	240

Como se puede observar, hay 16 posibles combinaciones que se pueden obtener utilizando los primeros cuatro *bits* del octeto.

Se puede usar la ecuación 2^n para determinar el número de subredes que se pueden obtener (*n* indica el número de *bits* que se va a utilizar*)*.

De esta manera, se obtienen las subredes que se indican en la tabla siguiente:

Nº bits	Nº de subredes
1	2
2	4
3	8
4	16
5	32
6	64
7	128
8	256

Ahora se deberá considerar si las subredes que se necesitan actualmente (10) y las posibles combinaciones que se pueden obtener con los cuatro *bits* (16) son suficientes para las necesidades futuras o se debe ampliar el número de *bits* que se pasan a dirección de subred.

DETERMINAR EL NÚMERO DE EQUIPOS DISPONIBLES

El siguiente paso es determinar el número de equipos disponibles en cada segmento de la red que está en función del número de *bits* que se han dejado para determinar la dirección de equipo (en el ejemplo anterior es 12).

Para ello, se utiliza la misma fórmula anterior ya que no se puede utilizar las direcciones de equipos con todos ceros o todos unos. De esta manera, se obtiene que con 12 *bits* se puede disponer de 4.094 equipos en cada segmento.

ESTABLECIENDO EL DEPÓSITO DE DIRECCIONES IP

El último paso es identificar las direcciones *IP* que se pueden usar en los segmentos de red y que estará determinado por la primera dirección *IP* de la red (en el ejemplo, 164.56.0.0) y su máscara de subred (255.255.240.0 ó 164.56.0.0/20).

De esta manera, se obtiene la tabla siguiente con las 16 posibles combinaciones de direcciones de red (para esta máscara):

Dirección de red binaria	Dirección de red decimal
10100100 00111000 00000000 00000000	164.56.0.0
10100100 00111000 00010000 00000000	164.56.16.0
10100100 00111000 00100000 00000000	164.56.32.0
10100100 00111000 00110000 00000000	164.56.48.0
10100100 00111000 01000000 00000000	164.56.64.0
10100100 00111000 01010000 00000000	164.56.80.0
10100100 00111000 01100000 00000000	164.56.96.0
10100100 00111000 01110000 00000000	164.56.112.0
10100100 00111000 10000000 00000000	164.56.128.0
10100100 00111000 10010000 00000000	164.56.144.0
10100100 00111000 10100000 00000000	164.56.160.0
10100100 00111000 10110000 00000000	164.56.176.0
10100100 00111000 11000000 00000000	164.56.192.0
10100100 00111000 11010000 00000000	164.56.208.0
10100100 00111000 11100000 00000000	164.56.224.0
10100100 00111000 11110000 00000000	164.56.240.0

La segunda dirección a determinar será la dirección de difusión para cada una de las posibles redes (esta dirección corresponde a poner todos unos en los *bits* de equipo).

De esta manera, se obtiene la tabla siguiente con las 14 posibles combinaciones de direcciones de difusión (para esta máscara):

Dirección de red binaria	Dirección de red decimal
10100100 00111000 00001111 11111111	164.56.15.255
10100100 00111000 00011111 11111111	164.56.31.255
10100100 00111000 00101111 11111111	164.56.47.255
10100100 00111000 00111111 11111111	164.56.63.255
10100100 00111000 01001111 11111111	164.56.79.255
10100100 00111000 01011111 11111111	164.56.95.255
10100100 00111000 01101111 11111111	164.56.111.255
10100100 00111000 01111111 11111111	164.56.127.255
10100100 00111000 10001111 11111111	164.56.143.255
10100100 00111000 10011111 11111111	164.56.159.255
10100100 00111000 10101111 11111111	164.56.175.255
10100100 00111000 10111111 11111111	164.56.191.255
10100100 00111000 11001111 11111111	164.56.207.255
10100100 00111000 11011111 11111111	164.56.223.255
10100100 00111000 11101111 11111111	164.56.229.255
10100100 00111000 11111111 11111111	164.56.255.255

Utilizando las dos tablas se obtiene el depósito de direcciones *IP* que se puede utilizar en cada una de las 16 combinaciones posibles (para esta máscara):

Dirección de red	Dirección de inicio	Dirección final	Dirección de difusión
164.56.0.0	164.56.0.1	164.56.15.254	164.56.15.255
164.56.16.0	164.56.16.1	164.56.31.254	164.56.31.255
164.56.32.0	164.56.32.1	164.56.47.254	164.56.47.255
164.56.48.0	164.56.48.1	164.56.63.254	164.56.63.255
164.56.64.0	164.56.64.1	164.56.79.254	164.56.79.255
164.56.80.0	164.56.80.1	164.56.95.254	164.56.95.255
164.56.96.0	164.56.96.1	164.56.111.254	164.56.111.255
164.56.112.0	164.56.112.1	164.56.127.254	164.56.127.255
164.56.128.0	164.56.128.1	164.56.143.254	164.56.143.255
164.56.144.0	164.56.144.1	164.56.159.254	164.56.159.255
164.56.160.0	164.56.160.1	164.56.175.254	164.56.175.255
164.56.176.0	164.56.176.1	164.56.191.254	164.56.191.255
164.56.192.0	164.56.192.1	164.56.207.254	164.56.207.255

Dirección de red	Dirección de inicio	Dirección final	Dirección de difusión
164.56.208.0	164.56.208.1	164.56.223.254	164.56.223.255
164.56.224.0	164.56.224.1	164.56.239.254	164.56.239.255
164.56.240.0	164.56.240.1	164.56.255.254	164.56.255.255

CONSTRUIR UNA TABLA DE SUBREDES

Todo el proceso que se ha estado siguiendo para realizar los cálculos anteriores para una determinada máscara ha sido complejo. Se puede construir una tabla rápida que simplifique los cálculos a seguir.

Esta tabla de doble entrada tendrá en la fila superior el número de *bits* de la dirección de equipo tomados para la dirección de subred y las tres columnas de información siguientes:

Nº de bits	1	2	3	4	5	6	7	8
Incremento								
Máscara de subred								
Nº de redes								

En la fila *Incremento* se indicará el valor decimal correspondiente al *bit* dentro del octeto (recuerde que este número se calcula con 2^n donde *n* toma los valores de cero a siete de derecha a izquierda). De esta manera, los valores serán los siguientes:

Nº de bits	1	2	3	4	5	6	7	8
Incremento	128	64	32	16	8	4	2	1
Máscara de subred								
Nº de redes								

Este valor va a determinar el valor de incremento de las direcciones de inicio del depósito de direcciones de cada subred.

La segunda fila determina el valor de la máscara de subred y está basado en el número de *bits* de la dirección de equipo tomados para la dirección de subred. Este valor se calcula sumando los valores de incremento de los *bits* que se toman y que se muestran en la tabla siguiente:

Nº de bits	1	2	3	4	5	6	7	8
Incremento	128	64	32	16	8	4	2	1
Máscara de subred	128	192	224	240	248	252	254	255
Nº de redes								

La última fila es el número de redes que se pueden obtener en cada caso (se calcula con la fórmula 2^n donde *n* toma los valores de los *bits* tomados):

Nº de bits	1	2	3	4	5	6	7	8
Incremento	128	64	32	16	8	4	2	1
Máscara de subred	128	192	224	240	248	252	254	255
Nº de redes	2	4	8	16	32	64	128	256

Direccionamiento IPv6

En el futuro, el tamaño de la dirección *IPv6* aumentará de 32 a 128 *bits* para poder soportar un número mayor de nodos direccionables, más niveles de direcciones jerárquicas y una autoconfiguración más sencilla de las direcciones (actualmente Windows Vista y Windows Server 2008 ya pueden ser configurados con direccionamiento IPv6 e IPv4).

Habrá tres formas de representar dichas direcciones:

- La primera forma, que es la más aceptada, consiste en representarla de la manera *x:x:x:x:x:x:x:x*, donde las *x* representan los valores hexadecimales de los ocho bloques de 16 bits cada uno.

  Ejemplos:

  FADB:CA58:96A4:B215:FABC:BA61:7994:1782
  A090:1:0:8:A800:290C:1:817B

  Como puede observarse, no es necesario escribir todos los ceros que hay por delante de un valor hexadecimal en un campo individual, pero se ha de tener por lo menos una cifra en cada campo.

- La segunda forma consiste en suprimir los ceros que se encuentran en medio de las direcciones. La expresión de dos "::" indicaría uno o varios grupos de 16 *bits* iguales a 0. Por ejemplo, la dirección siguiente:

  A123:FF01:0:0:0:0:0:92

  se representaría de la manera siguiente:

  A123:FF01::92

  los "::" sólo pueden aparecer una vez en la dirección.

- Otra forma, más cómoda cuando haya un entorno mixto de nodos con direcciones nuevas y antiguas, es representarla de la manera *x:x:x:x:x:x:d.d.d.d*, donde las *x* son valores hexadecimales (6 grupos de 16 *bits* en la representación futura) y las *d* son valores decimales (4 grupos de 8 *bits* en la representación estándar actual).

  Ejemplos:

  0:0:0:0:0:A234:23.1.67.4
  0:0:0:0:0:1:129.154.52.1

  o con el formato comprimido

  ::A234:23.1.67.4
  ::1:129.154.52.31

El **prefijo** es la parte de la dirección que indica los bits que tienen valores fijos o que son los bits del identificador de red. Los prefijos de los sitios y los identificadores de subred en IPv6 se expresan de la misma forma que la notación *Enrutamiento entre dominios sin clase* (*CIDR*) de IPv4. Un prefijo IPv6 se escribe con la notación *dirección/longitudDePrefijo*.

El **prefijo de sitio** de una dirección IPv6 ocupa como máximo los 48 bits de la parte más a la izquierda de la dirección IPv6. Por ejemplo, el prefijo de sitio de la dirección IPv6 2001:db8:3c4d:0015:0000:0000:1a2f:1a2b/48 se ubica en los 48 bits que hay más a la izquierda (2001:db8:3c4d, ya que cada bloque son 16 bits). Se puede utilizar la representación siguiente (con ceros comprimidos) para representar este prefijo: 2001:db8:3c4d::/48.

También se puede especificar un **prefijo de subred**, que define la topología interna de la red respecto a un encaminador. La dirección IPv6 de ejemplo tiene el siguiente prefijo de subred: 2001:db8:3c4d:15::/64. El prefijo de subred siempre contiene 64 bits. Estos bits incluyen 48 del prefijo de sitio, además de 16 bits para el ID de subred.

IPv6 es una nueva versión de *IP* y representa una fuerte evolución con respecto a *IPv4* (aunque sus principales funciones se conservan en **IPv6**, excepto ciertas funciones poco o nada utilizadas que fueron suprimidas o convertidas en otras opciones) ya que se añadieron ocho grandes características:

- Cuenta con posibilidades extendidas de direccionamiento y encaminamiento. El tamaño de la dirección *IP* aumenta de 32 a 128 *bits* para poder soportar un número más grande de nodos direccionables, más

niveles de direcciones jerárquicas y una autoconfiguración más sencilla de las direcciones.

- Queda definido un mecanismo adaptable de difusión y un nuevo tipo de direcciones en *cluster*.
- Incorpora un formato de cabecera simplificado. Algunos campos de formato de la cabecera han sido suprimidos o convertidos en opciones, y la cabecera está simplificada y reducida a un tratamiento común en todos los *routers*, lo que disminuye la dificultad de su mantenimiento.
- Cuenta con posibilidades de extensión de las cabeceras y de opciones. Las opciones están contenidas en cabeceras suplementarias colocadas entre la cabecera *IPv6* y la cabecera del paquete de transporte (*T-PDU*, *Transport Protocol Data Unit*). La mayoría de las opciones de las cabeceras de *IPv6* no son examinadas ni tratadas por los *routers* intermedios. Contrariamente a la versión actual, las opciones pueden ser de longitud variable y no existe tamaño límite.
- Define extensiones que permiten la autenticación de los usuarios y la integridad de los datos mediante herramientas de criptografía.
- Contiene varias formas de autoconfiguración como la configuración *Plug and Play* de direcciones de nodos sobre una red aislada gracias a las características ofrecidas por *DHCP*.
- Tiene una función extendida de *Source Routing* gracias a *SRDP* (*Source Demand Routing Protocol*) para difundir el encaminamiento a rutas interdominio e intradominio.
- Una transición de *IPv4* a *IPv6* sencilla y flexible.

Asignación dinámica de direcciones IP

En una red normal cada equipo debe tener asignada una dirección *IP* de forma estática si utiliza el protocolo *TCP/IP*, pero en una red con un servidor *DHCP*, éstas se asignarán cuando sea necesario (asignación dinámica).

DHCP (*Dynamic Host Configuration Protocol*) es un sistema desarrollado para asignar direcciones *IP* a los clientes que lo soliciten.

El proceso a seguir por un equipo que quiera conseguir una dirección *IP* es el siguiente:

1. Envía un mensaje al servidor *DHCP* solicitando una dirección *IP*.

2. El servidor *DHCP* responde ofreciendo varias direcciones *IP* que tiene disponibles de las indicadas en la instalación (entre las que están eliminadas aquellas consideradas convenientes).
3. El cliente selecciona una y envía una solicitud de uso de la dirección al servidor *DHCP*.
4. El servidor *DHCP* admite la solicitud y garantiza al cliente la concesión del uso de la dirección.
5. El cliente utiliza la dirección para conectarse a la red.

Las direcciones se conceden por un período de tiempo determinado. Cuando dicho período ha finalizado, el cliente deberá solicitar la renovación de la concesión o la dirección pasará al estado de disponible. Si solicita la renovación y no puede renovársela, se le reasignará otra.

Resolver nombres de ordenadores

Todo ordenador lleva una dirección *IP* y un nombre de equipo. Normalmente se necesitará indicar la dirección *IP* para conectarse a uno de ellos y poder realizar procesos con *TCP/IP*.

Pero también es posible realizar una conexión indicando únicamente el nombre del equipo (que es más sencillo de recordar que su dirección *IP*). Para ello, se utiliza un servidor DNS.

SERVIDOR DNS

DNS (*Domain Name System*) es un sistema que usa servidores distribuidos a lo largo de la red para resolver el nombre de un ordenador (con la estructura de nombre de ordenador, nombre de subdominio y nombre de dominio) en una dirección *IP* (de esta manera, no es necesario tener que recordar y usar su dirección *IP*).

Por tanto, se necesita un archivo que realice dicha conversión (que es lo necesario para establecer la conexión).

En una primera fase se utilizaba un archivo para realizar esta función que recibía el nombre de *HOSTS*. He aquí un ejemplo básico de archivo *HOSTS*:

```
172.16.132.1        principal
172.16.132.30       jlr
171.16.132.31       personal
165.16.132.41       secretaría
```

También era posible utilizarlo indicando el nombre completo del equipo. He aquí un ejemplo de este tipo de archivo *HOSTS*:

172.16.132.1	principal
172.16.132.1	principal.contabilidad.es
172.16.132.30	jlr
172.16.132.30	jlr.contabilidad.es
172.16.132.31	personal
172.16.132.31	personal.contabilidad.es
165.16.132.41	secretaría
165.16.132.41	secretaría.contabilidad.es

Este archivo tiene que estar situado en el mismo lugar donde se encuentra *TCP/IP* en el equipo y está determinado por el sistema operativo (normalmente se encuentra en un directorio *ETC*).

Otra posibilidad es que el servidor *DNS* cuente con una base de datos para poder resolver el nombre del ordenador.

La información que se encuentra en dicha base de datos se incluye en *registros de recursos* (*RR)*.

Entre dichos *registros de recurso* se encuentran:

- **Dirección** *(A).* Asigna un nombre de un ordenador a una dirección *IP* concreta.

- **Dirección IPv6**. *(AAAA)*. Asigna un nombre de un ordenador a una dirección *IPv6* concreta.

- **Inicio de autoridad** *(SOA)*. Indica el inicio de autoridad para la zona (los servidores de nombres tienen información completa acerca de una parte del dominio llamada *zona*, entonces se dice que tiene autoridad para esa zona).

- **Intercambiador de correo** *(MX)*. Identifica el equipo a que se va a entregar correo en el dominio.

- **Nombre canónico** *(CNAME)*. Se utiliza para asignar un alias al equipo.

- **Puntero de dominio** *(PTR)*. Asigna direcciones *IP* a nombres de equipo.

- **Servidor de nombre** *(NS)*. Asocia un nombre de dominio con un nombre de equipo para un servidor de nombre concreto.

- **Ubicación de servicios** *(SRV)*. Asigna un nombre de dominio *DNS* a una lista especificada de equipos que ofrecen un tipo específico de servicio.

Los servidores *DNS* pueden realizar los siguientes papeles:

- **Servidor de nombre primario**. Este tipo de servidor *DNS* mantiene la base de datos de nombres y direcciones para una zona, guardando información sobre la forma de contactar con servidores de nombre de zonas inferiores y superiores.

- **Servidor de nombre secundario**. Este tipo de servidor *DNS* obtiene información de la zona de un servidor maestro (puede ser de un servidor primario o de otro secundario que tiene una copia del archivo de zona). Esta información se guarda en un archivo de sólo lectura para aumentar la fiabilidad y descargar trabajo al servidor *DNS* primario. Para mantener actualizada dicha base de datos se realizan *transferencias de zonas*. Estas transferencias de zonas se hacen al arrancar el servidor secundario y cada vez que se detecta una modificación en la base de datos principal.

- **Servidor de nombre maestro**. Este tipo de servidor *DNS* transfiere el archivo de zona a un servidor secundario (puede actuar como servidor maestro tanto un servidor primario como un secundario).

- **Servidor de nombre sólo de caché**. Este tipo de servidor *DNS* no almacena ningún archivo de información de zona. Cuando un equipo solicita a un servidor *DNS*, primario o secundario, la resolución de un nombre de equipo, el servidor de sólo caché guarda la dirección *IP* que devuelve el servidor *DNS* antes de enviarla al equipo que realizó la consulta. En caso de necesitarse resolver otra vez el nombre del equipo anterior, en vez de consultarse al servidor *DNS* primario o secundario, se consultará al servidor de sólo caché.

Protocolos TCP/IP

TCP/IP es una familia de protocolos desarrollados para permitir la comunicación entre ordenadores de cualquier tipo de red o fabricante, respetando los protocolos de cada red individual.

Los protocolos *TCP/IP* se estructuran en cuatro niveles funcionales:

APLICACIÓN
TRANSPORTE
RED
FÍSICO

Figura 2.22. Niveles TCP/IP

- El **nivel físico** corresponde al *hardware*. Puede ser un cable coaxial, un cable par trenzado, cable de fibra óptica o una línea telefónica. *TCP/IP* no considera oficialmente el nivel físico como componente específico de su modelo y tiende a agrupar el nivel físico con el nivel de red.

- El **nivel de red**. Independientemente del medio físico que se utilice, necesitará una tarjeta de red específica que, a su vez, dependerá de un *software* llamado controlador de dispositivo proporcionado por el sistema operativo o por el fabricante. Proporciona fiabilidad (aunque no necesariamente) en la distribución de datos que pueden adoptar diferentes formatos. El protocolo específico de este nivel es *IP*, aunque también se encuentran: *ARP*, *RARP* e *ICMP*.

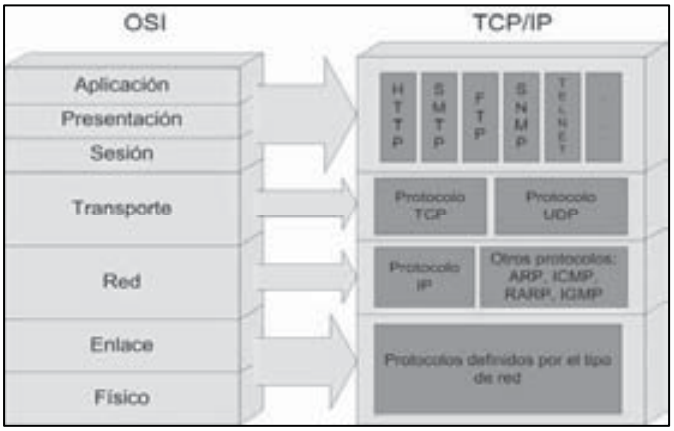


Figura 2.23. Comparativa OSI- TCP/IP de cuatro capas

- El **nivel de transporte** suministra a las aplicaciones servicios de comunicaciones desde la estación emisora a la receptora. Utiliza dos tipos de protocolos: *TCP* que es fiable y orientado a conexión y *UDP* que es no fiable y no orientado a conexión.

- El **nivel de aplicación** corresponde a las aplicaciones disponibles para los usuarios como pueden ser: *FTP*, *SNMP*, *TELNET*, etc.

PROTOCOLOS DEL NIVEL DE RED

IP

IP (*Internet Protocol*) se encarga de seleccionar la trayectoria a seguir por los datagramas, es decir, por dónde se deben encaminar los datagramas salientes pudiendo llevar a cabo tareas de fragmentación y reensamblado.

Este protocolo, que no es fiable ni está orientado a conexión, no garantiza el control de flujo, la recuperación de errores ni que los datos lleguen a su destino.

IP no se encarga de controlar que sus datagramas, que envía a través de la red, puedan perderse, llegar desordenados o duplicados. Para ello, tendrán que ser contempladas por protocolos del nivel de transporte.

Los datagramas *IP* contienen una cabecera con información para el nivel *IP* y datos. Estos datagramas se encapsulan en tramas que, dependiendo de la red física utilizada, tienen una longitud determinada.

Cuando los datagramas viajan de unos equipos a otros pueden atravesar diferentes tipos de redes. El tamaño máximo de estos paquetes puede variar de una red a otra dependiendo del medio físico que se emplee para su transmisión. A este tamaño máximo se le denomina *MTU* (*Unidad Máxima de Transmisión*) y ninguna red puede transmitir ningún paquete cuya longitud exceda del *MTU* de dicha red.

Debido a este problema, es necesario reconvertir los datagramas *IP* en el formato requerido por cada una de las redes que va atravesando. Esto es lo que se denomina *fragmentación y reensamblado*.

La *fragmentación* divide los paquetes en fragmentos de menor longitud (se realiza en el nivel más inferior posible y de forma transparente al resto de los niveles) y el *reensamblado* realiza la operación contraria.

ARP

ARP (*Address Resolution Protocol*) es un protocolo que se utiliza para convertir las direcciones *IP* en direcciones físicas que puedan ser utilizadas por los manejadores.

Para poder realizar esta conversión, existe en cada ordenador un módulo *ARP* que utiliza una **tabla de direcciones ARP**, que en la mayoría de los

ordenadores trata como si fuera una memoria intermedia (*caché*), de forma que la información que lleva mucho tiempo sin utilizarse se borra.

Si encuentra la correspondencia entre la dirección *IP* y la dirección física se procede a la transmisión.

Si no la encuentra en la tabla, se genera una petición *ARP* que se difunde por toda la red. Si alguno de los ordenadores de la red reconoce su propia dirección *IP* en la petición *ARP*, envía un mensaje de respuesta indicando su dirección física y se graba en la **tabla de Direcciones ARP**.

RARP

RARP (*Reverse Address Resolution Protocol*) se utiliza cuando, al producirse el arranque inicial, los ordenadores no conocen su dirección *IP*.

Requiere que exista en la red, al menos, un servidor *RARP*. Cuando un ordenador desea conocer su dirección *IP*, envía un paquete que contiene su propia dirección física.

El servidor *RARP*, al recibir el paquete, busca en su tabla *RARP* la dirección *IP* correspondiente a la dirección física inicial indicada en el paquete y envía un paquete al ordenador origen con esta información.

A diferencia del protocolo *ARP* que se incorpora normalmente en todos los productos *TCP/IP*, el protocolo *RARP* sólo se incorpora en unos pocos productos.

ICMP

ICMP (*Internet Control Message Protocol*) es un protocolo de mantenimiento/gestión de red que ayuda a supervisar la red.

Se utiliza para poder encontrar una ruta a través de la cual los datagramas viajen por la red y alcancen su destino.

El objetivo principal de *ICMP* es proporcionar la información de error o control entre nodos. La implementación de *ICMP* es obligatoria como un subconjunto lógico del protocolo *IP*.

Los mensajes de error de este protocolo normalmente los genera y los procesa *TCP/IP* y no el usuario.

Existen cuatro tipos de mensajes *ICMP*:

- Mensajes de destino no alcanzable.
- Mensajes de control de congestión.
- Mensajes de redireccionamiento.
- Mensajes de tiempo excedido.

Una de las utilidades de diagnóstico que utiliza este protocolo es la utilidad *PING* (se utiliza para comprobar si un equipo está conectado a la red).

PROTOCOLOS DEL NIVEL DE TRANSPORTE

En este nivel se encuentran los protocolos *TCP* y *UDP*.

TCP

TCP (*Transmission Control Protocol*) es un protocolo orientado a conexión que utiliza los servicios del nivel de red.

Al igual que cualquier protocolo orientado a conexión consta de tres fases:

1. **Establecimiento de la conexión**. Se inicia con el intercambio de tres mensajes, garantiza que los dos extremos de la transmisión estén preparados para la transferencia de datos y permite que ambos acuerden los números iniciales de secuencia (cada extremo elige un número de forma aleatoria).

2. **Transferencia de los datos**. La unidad de datos que utiliza es el segmento y su longitud se mide en *octetos*. La transmisión es fiable ya que permite la recuperación ante datos perdidos, erróneos o duplicados, así como garantiza la secuencia de entrega, para lo que se añade a la cabecera del segmento de datos un número de secuencia y un código de control. La fiabilidad de la recepción se consigue mediante la confirmación de la recepción, los temporizadores de espera de confirmación y la retransmisión de segmentos.

3. **Liberación de la conexión**. Cuando una aplicación comunica que no tiene más datos que transmitir, *TCP* finaliza la conexión en una dirección. Desde ese momento, *TCP* no vuelve a enviar datos en ese sentido, permitiendo que los datos circulen en el sentido contrario hasta que el emisor cierra también esa conexión.

TCP permite *multiplexación*, es decir, una conexión *TCP* puede ser utilizada simultáneamente por varios usuarios.

Como normalmente existe más de un proceso de usuario o aplicación utilizando *TCP* de forma simultánea, es necesario identificar los datos asociados a cada proceso. Para ello, se utilizan los *puertos*. Un *puerto* es una palabra de 16 *bits* que identifica hacia qué aplicación o proceso han de dirigirse los datos.

Hay aplicaciones que tienen asignado el mismo número de puerto, ya que realizan funciones de servidores normalizados que utilizan los servicios *TCP/IP*. Estos puertos reservados se encuentran en el archivo *SERVICES* que se encuentra en el directorio *ETC* y corresponden a números superiores a 1, indicando también si corresponden al protocolo *TCP* o *UDP*. Algunos ejemplos de puertos son:

Nº de puerto	Servicio
21	FTP
23	Telnet
25	SMTP
69	TFTP
80	HTTP
161	SNMP

Un *socket* está compuesto por un par de números que identifican de manera única a cada aplicación. Cada *socket* se compone de dos campos:

1. La **dirección IP** del ordenador en el que se está ejecutando la aplicación.
2. El **puerto** a través del cual la aplicación se comunica con *TCP/IP*.

UDP

UDP (*User Datagram Protocol*) es un protocolo que se basa en el intercambio de datagramas. *UDP* permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

El inconveniente de esta forma de actuación es que no hay confirmación de recepción ni de haber recibido los datagramas en el orden adecuado, debiendo ser la aplicación la que se encargue de controlarlo.

Al igual que el protocolo *TCP*, utiliza puertos y *sockets* y, también, permite la *multiplexación*.

PROTOCOLOS DEL NIVEL DE APLICACIÓN

Todas las aplicaciones *TCP/IP* utilizan el modelo cliente/servidor.

En este nivel se encuentran un buen número de protocolos de los cuales se van a describir los siguientes: *FTP*, *HTTP*, *SMTP*, *SNMP* y *TELNET*.

FTP

FTP (*File Transfer Protocol*) es el más utilizado de todos los protocolos de aplicación y uno de los más antiguos.

Se utiliza para la transferencia de archivos proporcionando acceso interactivo, especificaciones de formato y control de autentificación (aunque es posible conectarse como el usuario *anonymous* que no necesita contraseña).

HTTP

HTTP (*HyperText Transfer Protocol*) es uno de los protocolos más recientes. Se utiliza para manejar la consulta de hipertexto y el acceso de datos con *World Wide Web* (*WWW*). El tráfico generado por este protocolo ha pasado, debido a la influencia de *Internet*, a ser muy grande.

SMTP

SMTP (*Simple Mail Transfer Protocol*) es un protocolo de correo electrónico. Especifica el formato exacto de los mensajes que un cliente debe enviar desde un ordenador al servidor de otro, pero no especifica cómo debe almacenarse el correo ni con qué frecuencia se debe intentar el envío de los mensajes.

SNMP

SNMP (*Simple Network Management Protocol*) sirve para administrar los sistemas de forma remota. También se puede utilizar para supervisar el tráfico de la red desde una o varias estaciones de trabajo llamadas administradores *SNMP*.

Los elementos de la red que puede administrar y monitorizar son dispositivos como ordenadores, puertas de enlace (encaminadotes o routers), *mainframes*, miniordenadores, conmutador, concentrador, etc.

TELNET

TELNET permite que un usuario, desde un terminal, acceda a los recursos y aplicaciones de otros ordenadores.

Una vez que la conexión queda establecida, actúa de intermediario entre ambos ordenadores.

Enviando paquetes en la subred local

Una de las responsabilidades de *IP* es determinar si un paquete debe ser enviado a la subred local o bien debe ser encaminado a otra subred.

Se siguen los pasos siguientes:

- *IP* recibe una trama de *TCP* que está dirigida a una dirección *IP* determinada.
- *IP* compara el identificativo de la subred de la dirección recibida con el identificativo de la subred local. Si ambos coinciden, la trama se envía localmente.
- Antes de proceder al envío local, *IP* debe determinar la dirección de la red física que corresponde a la dirección *IP* destino. Para ello, utiliza *ARP*.
- *IP* añade la siguiente información a la trama:
  - La dirección *IP* origen.
  - La dirección física de la red origen.
  - La dirección *IP* destino.
  - La dirección física de la red destino.
- *IP* pasa el paquete con las direcciones añadidas al protocolo de nivel inferior que lo lleva a su destino.

Enviando paquetes a la subred remota

Si en el punto 2 del apartado anterior se determina que las dos subredes (origen y destino) son distintas, es una indicación clara de que el paquete se tiene que encaminar hacia una subred remota.

Cuando un ordenador está conectado con el exterior, debe estar configurado con una dirección *IP* de una puerta de enlace (*router o encaminador*) por defecto.

Como el paquete tiene que dirigirse hacia el exterior, *IP* dirige el paquete a la puerta de enlace por defecto.

Allí se realizan distintos algoritmos de encaminamiento (que pueden ser simples o complejos) hasta que se identifica al router de la subred a la que tiene que enviar el paquete. Entonces, lo envía para que lo haga llegar al ordenador destino.

Para identificar al router de la subred remota, es necesario consultar la tabla de encaminamiento que está disponible por defecto.

Esta tabla puede ser:

- **Estática**. Este tipo de tabla lo tiene que crear manualmente el administrador de la red y no se actualiza automáticamente cuando se producen cambios en la red. Debe contener, por lo menos, los datos siguientes:
  - **Direcciones de red**. Indica las direcciones *IP* remotas a las que va tener acceso.
  - **Máscara de subred**. Indica la máscara correspondiente a la subred de la dirección *IP* remota.
  - **Dirección de la puerta de enlace**. Indica la dirección del *router* que se usará para enviar un paquete a una dirección *IP* remota.
  - **Dirección física de la red**. Indica la dirección física de la red remota.
- **Dinámicas**. Este tipo de tablas se actualizan automáticamente cuando se produce algún tipo de cambio en la red. Para ello, se utilizan varios algoritmos de encaminamiento. Entre ellos, se encuentran:
  - **OSPF** (*Open Shortest Path First*). Este algoritmo está basado en el estado de enlaces. Cada encaminador envía, de forma periódica, paquetes de estado de enlaces que describen sus conexiones a sus vecinos. Usando estas comunicaciones, los encaminadores vecinos elaboran una base de datos de estado de enlaces que utilizan para identificar encaminamientos.

Este algoritmo detecta bucles en la transmisión de ruta que evitan el problema de que dos rutas se llamen entre ellas y puede estar emitiendo los mensajes de estado de enlaces indefinidamente.

También obligan a la autentificación de los intercambios que evitan que una persona ajena pueda recibir la información de ruta.

- **RIP** (*Routing Information Protocol*). Este algoritmo está basado en el vector/distancia y está disponible en dos versiones: *RIP I* y *RIP II* (soporta el uso de máscaras de subred).

  Si un encaminador conoce varias rutas para llegar a un destino, asigna un coste a la ruta en función de los saltos que deba realizar (cuanto más encaminadores tenga que cruzar más saltos tendrá que realizar).

  Cada 30 segundos envía un mensaje con su tabla de encaminamiento a los demás, que actualizan sus propias tablas con los datos recibidos (esto origina un aumento considerable del tráfico de la red).

  Este algoritmo no detecta bucles en la transmisión de ruta, por lo que se daría el problema de que dos rutas que se llamen entre ellas estarían emitiendo sus tablas de encaminamiento indefinidamente.

  Tampoco obligan a la autentificación de los intercambios, por lo que una persona ajena podría recibir la información de rutas enviadas por los encaminadores.

MECÁNICA DE RED (PARTE PRÁCTICA)

Estándares de cableado estructurado

Un estándar de cableado estructurado especifica cómo debe organizarse la instalación del cableado de comunicaciones en edificios. Engloba todas las aplicaciones de comunicaciones, como voz, megafonía, conexiones de ordenadores, etc. El estándar especifica de forma concisa el tipo de cable a utilizar, conectores, longitudes máximas de los tramos, organización de los elementos de interconexión, etc.

Aplicar un estándar de cableado estructurado ofrece muchas ventajas, entre las que destacamos:

- ☑ Facilita las tareas de mantenimiento y supervisión, ya que resulta más sencillo identificar las estructuras de cableado.
- ☑ Asegura un funcionamiento óptimo si se cumplen todos los requisitos del estándar.
- ☑ Posibilita la inclusión de una alta densidad de cableado.
- ☑ Permite la integración de diferentes tecnologías de redes.
- ☑ Resulta fácilmente ampliable.

Existen tres estándares internacionales de cableado estructurado, que en la práctica tienen diferencias muy poco significativas:

- **ISO/IEC 11801**. Estándar a nivel internacional.
- **EN-50173**. Norma europea basada en la anterior.
- **ANSI/EIA/TIA-568**. Norma utilizada en Estados Unidos.

Como se trata de un conjunto de especificaciones muy amplio, nos remitiremos al montaje y organización del cableado, sin tener en cuenta aspectos de carácter eléctrico y electrónico.

Todos los estándares mencionados incluyen compatibilidad para cableado telefónico convencional, redes *Ethernet* (exceptuando 10Base-2, 10Base-5 y 10Broad-36), ATM, *Frame Relay* y RDSI.

SUBSISTEMAS DE CABLEADO ESTRUCTURADO

El conjunto de todo el cableado estructurado de un edificio es su *sistema de comunicaciones*. Puesto que está organizado en varias partes, existen diferentes *subsistemas*, cada uno de los cuales engloba un subconjunto de especificaciones.

La figura 2.24 muestra de forma esquemática todos los elementos que intervienen en el cableado estructurado de un edificio. Más adelante se especificará con detalle la organización de los armarios de comunicaciones.

Esos subsistemas son los siguientes:

- **Cableado de campus**. Se utiliza para interconectar los diferentes edificios de la organización. Puesto que por éste circula gran cantidad de tráfico, se recomienda el uso de fibra óptica.

- **Entrada del edificio**. Es el punto en el que se conectan los cables exteriores con los cables interiores del edificio. Se puede decir que es la frontera que separa la instalación que es responsabilidad de la compañía de comunicaciones con la instalación privada.

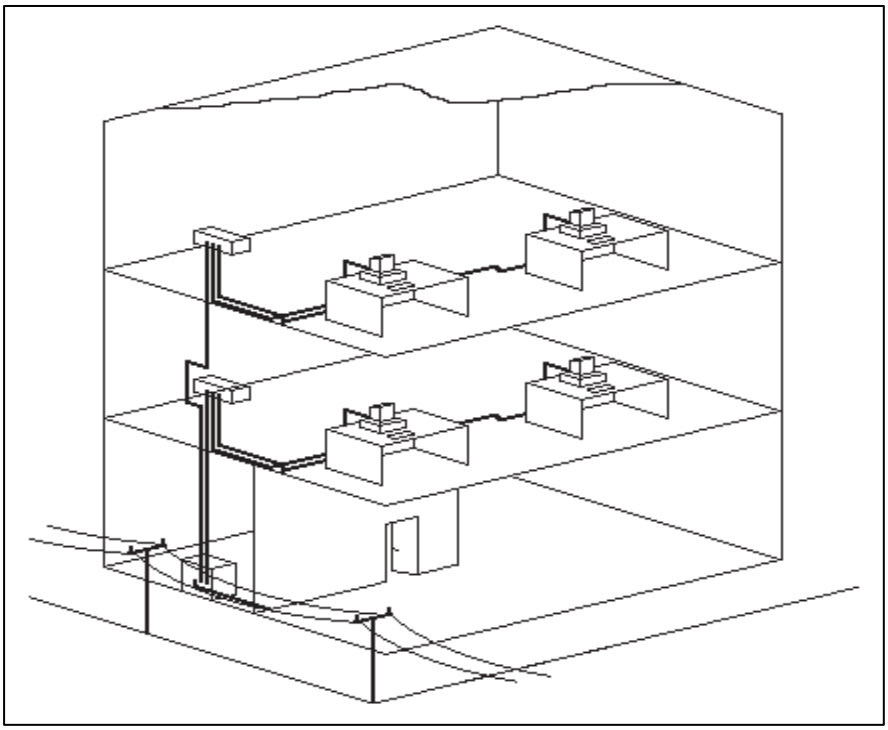


Figura 2.24. Elementos del cableado estructurado. Diagrama simplificado

- **Sala de equipamiento**. Es el punto en el que confluyen todas las conexiones del edificio, por lo que su complejidad de montaje es mayor que la de cualquier otra sala. Se podría considerar que es la "sala de máquinas" de todo el bloque.

- **Cableado troncal**. Es el encargado de llevar a cabo la comunicación de todos los elementos del edificio, a través del cableado vertical (entre plantas), las conexiones con el exterior y los cables que comunican

otros edificios colindantes. Se utilizará cableado UTP de hasta 800 m de longitud para transmisión de voz y FTP de hasta 90 m para transmisión de datos. En el caso de que se use fibra óptica, se permiten hasta 2.000 m en fibra multimodo y 3.000 m en fibra monomodo.

- **Armarios de distribución**. Es el lugar en el que confluyen los cables de comunicaciones. Contienen todos los concentradores de cableado, conmutadores, puentes, etc., montados en los armarios en *rack* y conectados mediante paneles de distribución. Existen varios tipos de armarios de distribución, dependiendo del lugar que ocupan dentro de la organización: *distribuidor de campus* (que conecta los diferentes edificios), *distribuidor de edificio* (montado en la sala de equipamiento) y *distribuidor de planta* (donde confluyen las conexiones de toda la planta).

- **Cableado horizontal**. Se extiende desde las conexiones de pared (también llamadas *rosetas*) de las oficinas y despachos hasta los armarios de comunicaciones. En el estándar se reconocen los siguientes medios: cable UTP 100 Ω de 4 pares, cable FTP 150 Ω de 2 pares y cable de 2 fibras de 62.5/125 μm (para enlaces de elevado tráfico). Así mismo, existen unos límites máximos en lo que se refiere a las longitudes de los cables: 5 m para los *latiguillos* que van de la estación a la roseta, 90 m de cableado interno y 6 m para los latiguillos de los armarios de comunicaciones.

- **Área de trabajo**. Es el punto de conexión entre los dispositivos (ordenadores, etc.) y las rosetas. En cada roseta se deberán instalar, al menos, dos conexiones, una para voz (RJ-11) y otra para datos (RJ-45).

ESPECIFICACIONES DE CONEXIONES

El estándar ANSI/EIA/TIA-568 está dividido en varios boletines técnicos que establecen los elementos de transmisión. Éstos son:

- **TSB36**. Especifica la utilización de cableado de par trenzado.

- **TSB40**. Establece el uso del conector RJ-45 y los métodos para realizar empalmes de cableado.

- **TSB53**. Especifica la utilización de cableado de par trenzado apantallado.

La figura 2.25 muestra la estructura de un par trenzado, junto con los conectores RJ-45 que se utilizan y el orden de numeración de los *pines*. Para enlazar el cable al conector, se utiliza una herramienta llamada *engastadora*.

Los cables UTP y FTP suelen ir engastados de fábrica (a estos cables se les llaman *latiguillos*), aunque, si se desea montar el cableado interno de la red, será necesario engastarlos manualmente. En esas condiciones, es necesario cumplir una serie de normas, que aparecen resumidas esquemáticamente en la figura 2.26.

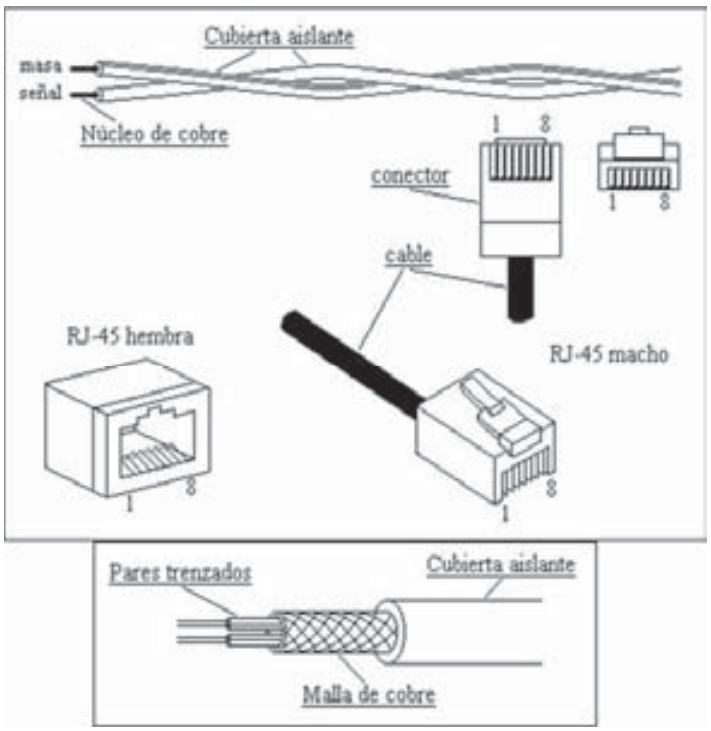


Figura 2.25. Cableado UTP/FTP y conectores RJ-45

Los estándares de cableado estructurado definen varios tipos de conexiones que se pueden utilizar a la hora de ensamblar el cableado de par trenzado con el conector RJ-45 (véase la figura 2.25), tanto machos como hembras. De todas ellas, las que más se utilizan son la ANSI/EIA/TIA-568A ANSI/EIA/TIA-568B y será el instalador el que decida cuál resulta más recomendable usar, sobre todo si ya existe cableado anterior que se desea reutilizar. Hay que tener en cuenta que no es aconsejable utilizar las dos normas a la vez al realizar el cableado de un edificio, ya que puede dar lugar a problemas de instalación y mantenimiento.

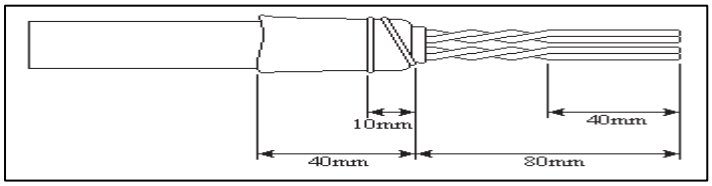


Figura 2.26. Enlace de un cable FTP a un conector RJ-45. Aquí aparecen las longitudes máximas de los tramos en el extremo del cable para asegurar que la transmisión se realizará con un margen de interferencias máximo aceptable. Los cables no se deben destrenzar más de 40 mm ni deben separarse de la malla más de 80 mm

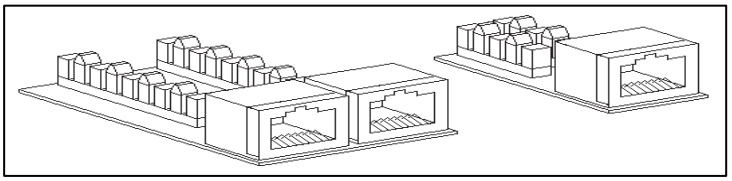


Figura 2.27. Conectores RJ-45 hembra. A la izquierda aparecen los conectores utilizados en los paneles de conexiones, mientras que a la derecha aparece el conector RJ-45 hembra utilizado en las rosetas de pared. Para engastar estos conectores, se utiliza una herramienta diferente a las engastadoras de RJ-45 macho

Figura 2.28. Herramienta de impacto para engastar los cables en una roseta

Figura 2.29. Crimpadora para engastar los cables en un conector RJ-45

Para el montaje de *cables cruzados*, se engasta cada extremo utilizando un estándar diferente (uno será 568A y el otro 568B). Este tipo de conexiones se utiliza para comunicar dos estaciones sin necesidad de utilizar un concentrador de cableado intermedio o en el cableado troncal cuando se conectan concentradores o conmutadores entre sí (y no existe ningún puerto que realice ese cruce de forma automática).

En este anexo no se incluye la especificación para el montaje de los conectores RJ-45 hembra de roseta y panel. Normalmente, cada fabricante utiliza un orden de colores diferente que suele ir convenientemente documentado en sus productos.

ANSI/EIA/TIA-568A

Según este estándar, la forma de engastar un cable UTP o FTP con un conector RJ-45 macho sigue el orden especificado en la tabla siguiente (véase la figura 2.25 en donde aparece el orden de numeración de las patillas del conector).

Tabla 2.1. ANSI/EIA/TIA-568A

Pin n.º	*Par n.º*	*Color*	*Uso*
1	3	Blanco verde	Transmisión
2	3	Verde	Masa
3	2	Blanco naranja	Recepción
4	1	Azul	Masa
5	1	Blanco azul	Transmisión
6	2	Naranja	Masa
7	4	Blanco marrón	Recepción
8	4	Marrón	Masa

ANSI/EIA/TIA-568B

Según este otro estándar, los cables UTP o FTP se engastan al conector RJ-45 macho siguiendo el orden establecido en la tabla 2.2. Hay que tener en cuenta que, como se ha indicado anteriormente, para el montaje de latiguillos cruzados que unan elementos de interconexión de redes, un extremo será 568A y el otro 568B. El orden de este montaje es indiferente.

Tabla 2.2. ANSI/EIA/TIA-568B

Pin n.º	*Par n.º*	*Color*	*Uso*
1	2	Blanco naranja	Recepción
2	2	Naranja	Masa
3	3	Blanco verde	Transmisión

Pin n.º	*Par n.º*	*Color*	*Uso*
4	1	Azul	Masa
5	1	Blanco azul	Transmisión
6	3	Verde	Masa
7	4	Blanco marrón	Recepción
8	4	Marrón	Masa

Cableado UTP de 100 Ω

Puesto que las necesidades de transmisión han ido en aumento, ha sido necesaria una mejora en la calidad del cableado UTP. Las capacidades de transmisión han sido divididas por categorías y se exponen en la tabla 2.3.

Tabla 2.3. Categorías de cableado

Categoría	Frecuencia de funcionamiento	Aplicaciones
3	16 Mhz	*Ethernet* (10 Mbps), *Token Ring* (4 Mbps), *Localtalk* y telefonía.
4	20 Mhz	*Ethernet* (10 Mbps), *Token Ring* (4 Mbps), *Localtalk* y telefonía.
5	100 Mhz	*Ethernet* (10-100 Mbps), *Token Ring* (4-16 Mbps) y ATM (155 Mbps).
5e	100 Mhz	*Ethernet* (10-100 Mbps), *Gigabit Ethernet* (1 Gbps) y ATM (155 Mbps).
6	250 Mhz	Todavía en fase de desarrollo.
7	600 Mhz	Todavía en fase de desarrollo.

Para asegurar la integridad completa del sistema, los cables horizontales deben terminar en cableado de la misma categoría (o superior). Así mismo, los cables utilizados para conectar los concentradores y los latiguillos también deben ser de la misma categoría (o superior).

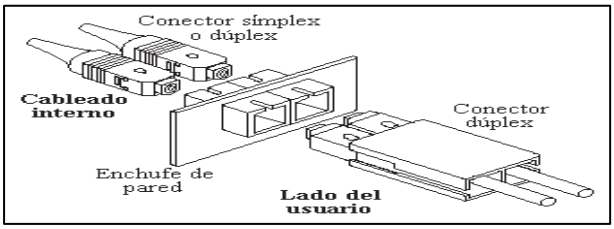


Figura 2.30. Conectores 568SC para fibra óptica. La parte interior de cada roseta puede albergar conectores simplex o dúplex, pero en la parte externa estas conexiones deberán ser siempre dúplex

Finalmente, se debe mencionar que el cableado UTP de la red no cumplirá con la categoría 3, 4, 5, 6 ó 7, a menos que todos los componentes del sistema satisfagan los requerimientos de sus respectivas categorías.

Cableado de fibra óptica

Según el estándar ANSI/EIA/TIA-568, los conectores utilizados para los cables de fibra son los 568SC símplex/dúplex que aparecen en la figura 2.30.

El cableado horizontal se realizará utilizando cableado de fibra multimodo, con un mínimo de dos fibras (una para cada sentido de la transmisión). Por su parte, el cable troncal y el de campus se podrán realizar con fibra multimodo o monomodo (en caso de que las distancias excedan los 2 km). Se utiliza el color azul para identificar los conectores y adaptadores monomodo y el color beige, para los multimodo.

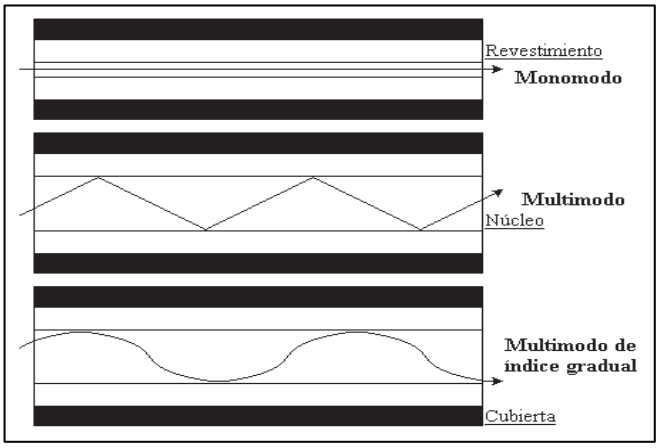


Figura 2.31. Tipos de transmisión en cables de fibra óptica. La fibra monomodo es tan delgada como un pelo humano

Norma ISO/IEC 11801

La norma ISO/IEC 11801 es mucho más amplia que la ANSI/EIA/TIA-568, ya que determina también la distribución del cableado en edificios, además de las normas de cableado y conexiones que también incluye el estándar americano. La tabla 2.4 muestra las diferencias entre estas dos normas en cuanto a cableado y conectores definidos.

Tabla 2.4. Algunas diferencias entre ISO/IEC 11801 y ANSI/EIA/TIA-568

Norma	Impedancia del cableado de cobre	Conectores para cobre	Cableado de fibra óptica	Conectores para fibra óptica
ANSI/EIA/ TIA-568	100 Ω	RJ-45	50/125 µm	568SC
ISO/IEC 11801	120 Ω y 150 Ω	RJ-45 y empalmes	62,5/ 125 µm	ST

INSTALACIÓN DEL CABLEADO

Para conectar todas las estaciones de la red, se utilizan los armarios de comunicaciones. Éstos contienen los concentradores de cableado, conmutadores, puentes y encaminadores, aunque no se conectan directamente al cable de cada estación, sino que se sigue un conjunto de normas:

- ☑ Cada estación se conecta a un enchufe de pared (roseta) a través de un cable llamado **latiguillo**.
- ☑ Las rosetas se conectan internamente mediante cableado contenido en canalizaciones y canaletas de pared (con un máximo de 90 m de longitud).
- ☑ El cableado de las canalizaciones no se conecta directamente a los concentradores de cableado, sino que se utilizan unos dispositivos intermedios llamados **paneles de parcheo** (*patch panels*). Cada panel puede conectar uno o varios dispositivos de interconexión (dependiendo del número de puertos), aunque es conveniente por simplicidad que el dispositivo esté conectado a un solo panel.
- ☑ Los paneles de parcheo se conectan a los dispositivos de interconexión de la red a través de latiguillos de pequeña longitud (máximo 6 m). Se pueden utilizar latiguillos de colores para identificar las diferentes secciones o departamentos que conectan.
- ☑ Los paneles de parcheo y los dispositivos de interconexión, además de los armarios de comunicaciones, deben estar conectados a tierra.
- ☑ No es conveniente conectar en cascada más de dos concentradores de cableado si se desea cumplir con las especificaciones de categoría 5, 6 y 7. En caso necesario, estas conexiones deberán realizarse en estrella (utilizando un concentrador central).

La figura 2.32 muestra la organización interna de un armario de comunicaciones. La instalación de todos los elementos de interconexión se llama **en *rack***, que consiste en atornillar todos los elementos a unas barras verticales convenientemente perforadas. Este método permite organizar más fácilmente el cableado en el interior del armario de comunicaciones.

Toda esta organización de cableado tiene como objetivo permitir una mejor administración de la red, aislando más rápidamente problemas en las conexiones y permitiendo una mayor facilidad a la hora de realizar cambios y ampliaciones.

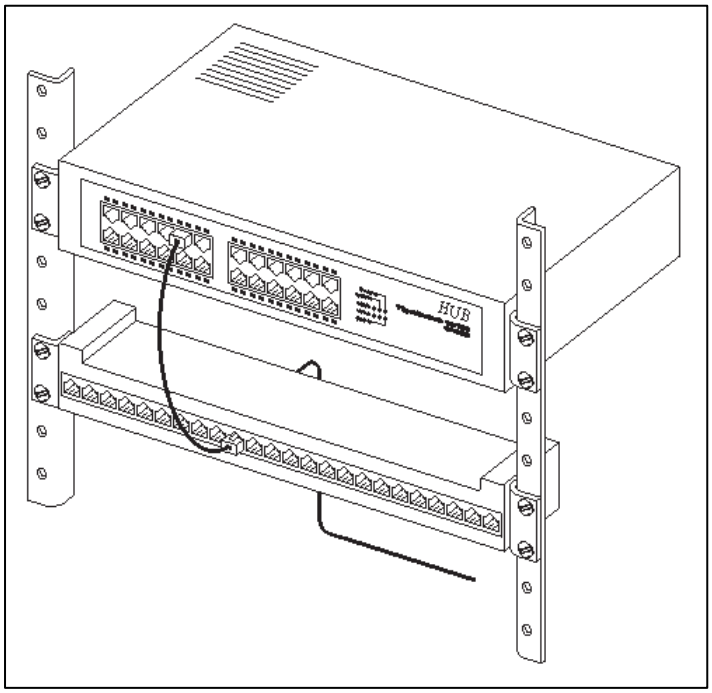


Figura 2.32. Organización de un armario de comunicaciones. Cada dispositivo de interconexión necesita un panel de conexiones para conectarse al cableado de la instalación

Certificación de la instalación

La certificación de una instalación de cableado se utiliza para comprobar que ésta es adecuada para las necesidades de comunicación de la organización. Esta certificación permite comprobar también que todas las conexiones se han realizado correctamente (pares sueltos, niveles de ruido, etc.) y que no existen cables mal instalados en los conductos (torsiones mínimas, radios de curvatura,

etc.). Todos los estándares de cableado estructurado establecen una serie de normas a seguir a la hora de certificar una instalación de cableado.

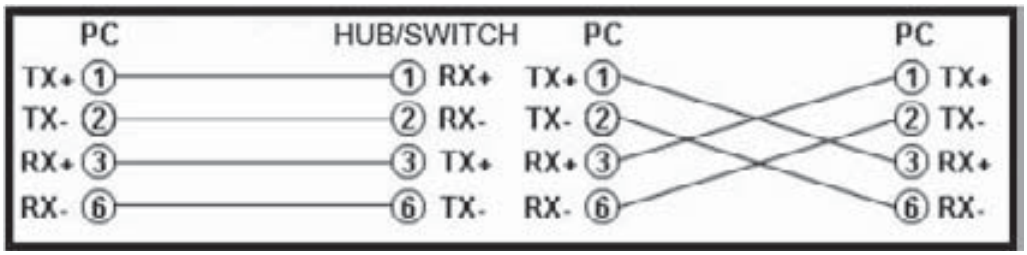
La certificación del cableado se realiza utilizando aparatos portátiles que miden los parámetros más importantes del cableado: diafonía, atenuación y longitud. Estos aparatos se denominan genéricamente ***testers* de red** (ver figura 2.33). Los más sencillos permiten solamente comprobar si los conectores se han engastado convenientemente (todos los pines están unidos), mientras que los más sofisticados son capaces de medir radios de curvatura de los cables, longitudes, etc.

Dependiendo del tipo de aplicación, categoría y velocidad máxima de transmisión de la instalación del cableado, los certificados que se realizan tienen en cuenta diferentes valores de diafonía, atenuación y longitud. Evidentemente, cuanto mayor sea la velocidad de transmisión y categoría a certificar, mayores serán también las exigencias de los valores indicados anteriormente.

Figura 2.33. Tester de red para RJ-11 y RJ-45

Construir un cable de red RJ-45

Para construir un cable de red RJ-45 para unir un equipo a un hub/switch o a otro PC (cable cruzado), se utiliza el diagrama de conexionado siguiente:



El conexionado de la izquierda es para un cable de red que vaya desde un PC a un hub o un switch y el de la derecha para un cable cruzado que una dos PCs.

Como se vio anteriormente, existen dos únicas terminaciones de cables que corresponden a los conectores EIA/TIA 568A y EIA/TIA 568B.

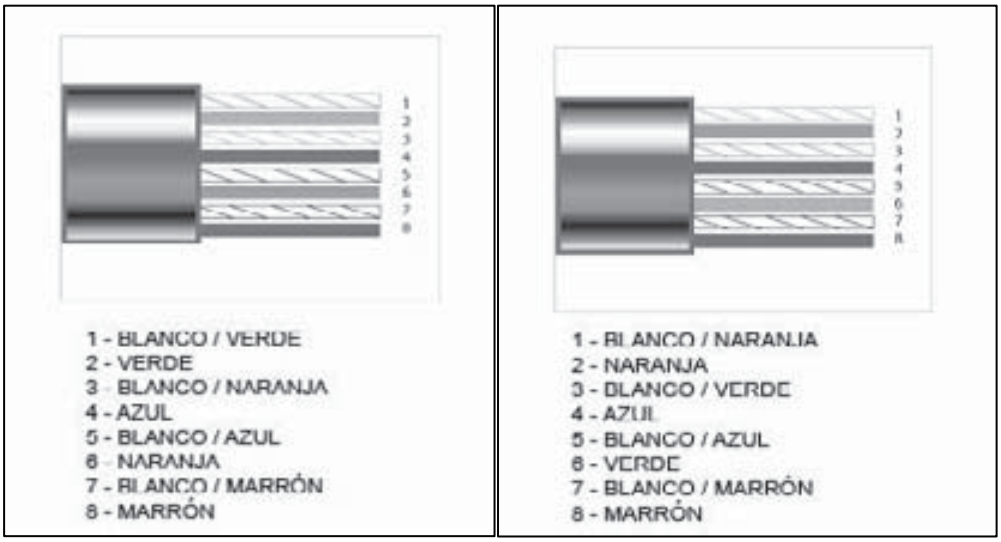


Figura 2.34. EIA/TIA 568A *Figura 2.35. EIA/TIA 568B*

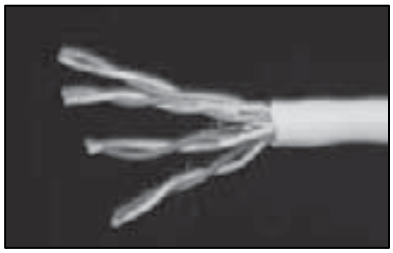
La norma 568-B, es la más habitual pero se van a indicar las dos formas de colocación de los cables.

Se van a necesitar tres cosas:

- Cable UTP de categoría 5 ó 6 .
- Conectores RJ-45 .
- Una crimpadora o tenazas especiales para crimpar.

El proceso que se ha de seguir es muy sencillo:

1. Medir bien la longitud del cable y cortarlo a la medida deseada. Luego, hay que retirar unos 2 centímetros del recubrimiento del cable en los extremos. El cable es en realidad un conjunto de cables de colores trenzados entre sí por pares.

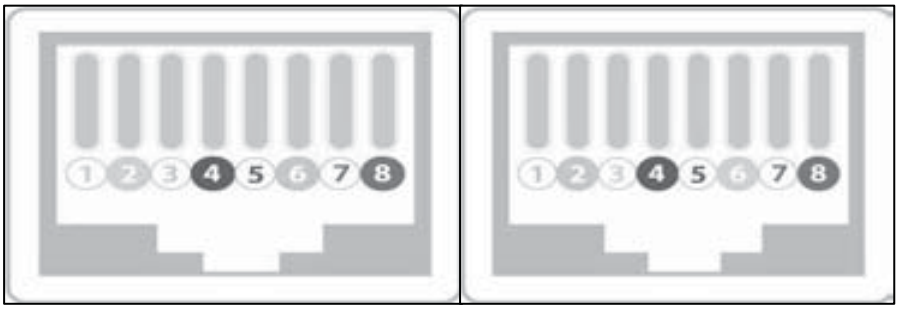


2. El siguiente paso es destrenzar los cables pequeños y ponerlos en paralelo.

3. Después, hay que realizar un corte limpio con la parte correspondiente de la crimpadora, de modo que todos los cables queden bien emparejados.

4. Una vez igualados los cables, hay que introducirlos con cuidado en el conector RJ-45, cada cable por su carril hasta que haga tope con el fondo.

5. De izquierda a derecha, los cables han de seguir el orden de color siguiente, según sea el formato 568A o 568B.



1 - BLANCO / VERDE
2 - VERDE
3 - BLANCO / NARANJA
4 - AZUL
5 - BLANCO / AZUL
6 - NARANJA
7 - BLANCO / MARRÓN
8 - MARRÓN

Figura 2.36 EIA/TIA 568A

1 - BLANCO / NARANJA
2 - NARANJA
3 - BLANCO / VERDE
4 - AZUL
5 - BLANCO / AZUL
6 - VERDE
7 - BLANCO / MARRÓN
8 - MARRÓN

Figura 2.37 EIA/TIA 568B

6. Si nos equivocamos o los cables no se colocan en este orden sea uno u otro, el cable no servirá. Por supuesto se ha de usar el mismo orden en los dos extremos del cable.

7. Por último, hay que presionar con las tenazas crimpadoras el conector RJ-45 con los cables dentro y apretar fuerte.

   Las chapas metálicas del cabezal perforarán cada cable y harán contacto con el hilo conductor interior. Si hay algún cable que no llegue a hacer contacto el cable no funcionará.

8. Después, hay que proceder exactamente igual con el otro extremo del cable y el cable RJ 45 estará listo para usarse.

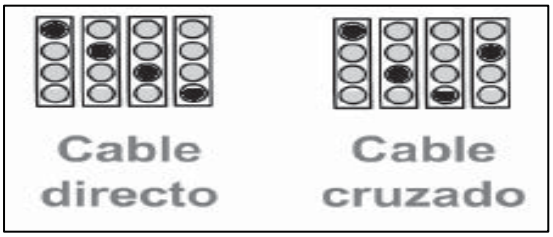
NOTA. Si lo que se desea hacer es conectar 2 PCs sin necesidad de concentradores o conmutadores, se deberá preparar un **cable cruzado**. Para ello, una punta del cable se preparará según el formato 568A y la otra con el 568B.

Prueba de los cables

Una vez que se ha preparado el cable, hay que probar su funcionamiento antes de utilizarlo. Para ello, se necesita un tester y seguir los pasos siguientes:

1. Se conecta cada extremo del cable a un conector RJ-45 (en caso de estar separados por bastante distancia, se pueden separar las dos partes del tester).

2. Se pulsa el botón correspondiente y se observa el color de los leds (los colores oscuros se corresponden con el verde):



3. Si sigue la pauta indicada en la figura anterior, el cable está correcto. En caso de que algún led sea de color rojo o no esté iluminado, el cable es incorrecto y habría que volverlo a preparar.

Montar una roseta

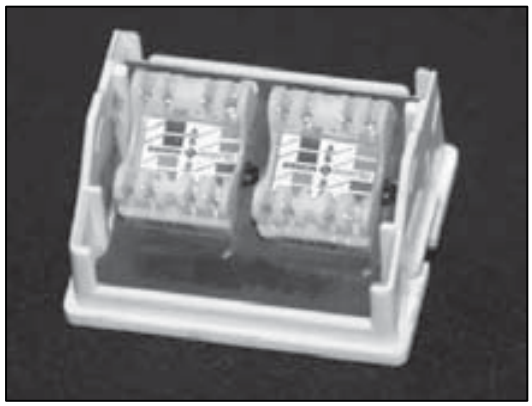
La roseta es un elemento de conectividad de red que pertenece al subsistema de cableado horizontal. Se emplea para permitir la conexión de un PC mediante un cable de red a una conexión fija de pared. Al final del cable al que se ha conectado la roseta se encontrará un elemento similar que permitirá la conexión de ese terminal de cable a un dispositivo de electrónica de red. El proceso de conexión debe seguir los estándares de color de las redes Ethernet.

Para montar el cableado de una roseta, siga los pasos siguientes:

1. Hay que retirar unos 2 centímetros del recubrimiento del cable en los extremos y destrenzar los cables pequeños y ponerlos en paralelo.

2. Después, hay que realizar un corte limpio con la parte correspondiente de la crimpadora, de modo que todos los cables queden bien emparejados.

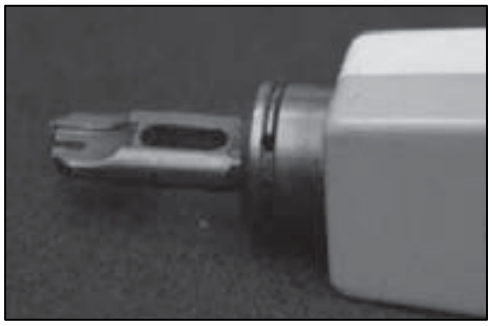
3. Una vez realizado lo anterior, hay que fijarse en el detalle de los colores que se indican en la roseta, los triángulos de color significan hilo blanco pareja de color, los cuadrados completos son el hilo de color correspondiente (si se fija bien, hay dos parejas de colores: una con el formato A y otro con el B). En la figura inferior, los colores de izquierda a derecha de la parte superior para el formato A son: Blanco/Azul, Azul, Blanco/Naranja; Naranja y los de la parte inferior: Blanco/Verde; Verde, Blanco/Marrón y Marrón.



NOTA. Rosetas de otros fabricantes pueden indicar los códigos de los pares blanco-color con otros símbolos como, por ejemplo, un cuadrado dividido en dos triángulos uno de los cuales es de color y, el otro, blanco.

4. Se posicionan los hilos en las ranuras correspondientes como se puede ver en la foto y se aprieta un poco con la uña para que queden encajados.

5. Una vez introducidos, se coge la herramienta de impacto. Esta tiene doble finalidad: por un lado, introduce el cable en los contactos de la roseta garantizando la conexión eléctrica y, por otro, corta el aislante sobrante.

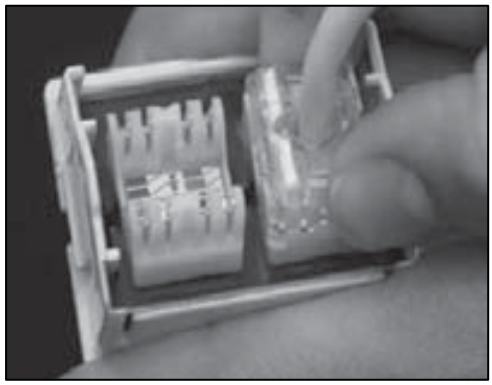


6. En la herramienta de impacto, la cuchilla que tiene en uno de sus lados es más larga y angulada. Este extremo tendrá que situarse en la parte exterior de cada uno de los contactos de la roseta, porque si se pone en el interior, lo que hará será cortar el hilo por la parte de la conexión y ésta dejará de funcionar.

7. Se presionan los hilos con la herramienta de impacto hasta que haga tope y suene un “clac”.

8. Se comprueba que los cables estén bien sujetos tirando suavemente de ellos. Si se salieran, indicaría que estaba mal colocada. La roseta no es como los conectores de los latiguillos y, si no se han dañado mucho, los conectores se podrán reutilizar nuevamente.

9. Para finalizar, se tapa la zona de trabajo con el fin de proteger las conexiones y se coloca en la caja de la pared.



Instalación de un adaptador de red

Normalmente, en los ordenadores modernos los adaptadores de red vienen en la placa base por lo que no es necesario instalarlos.

Pero en el caso de haberse estropeado dicho adaptador o querer instalarlo en un ordenador que no lo tenga en la placa base, se va a indicar cómo realizarlo a continuación.

Dicho proceso tiene dos partes diferenciadas:

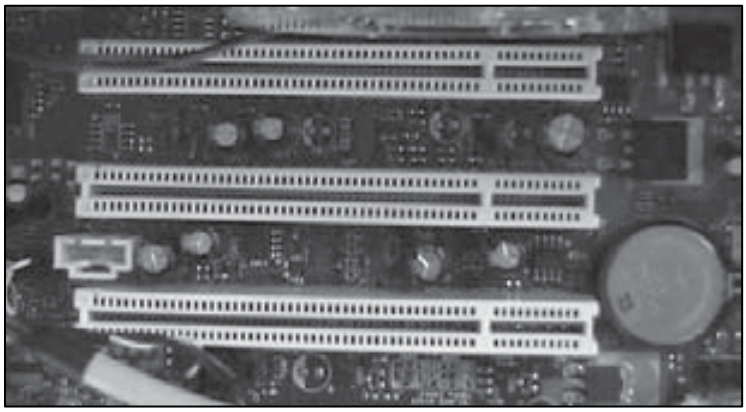
- La instalación física de un adaptador de red (pasos 1 al 4) es un simple proceso de manipulación del hardware.

- La instalación lógica del adaptador (pasos 5 al 10) supone la instalación de los drivers o controladores que son los elementos que crean una interfaz entre el sistema operativo del equipo y dicho adaptador de red (cualquier dispositivo de un equipo dispone de los drivers necesarios que permiten que el sistema operativo se entienda con él).

El proceso a seguir es el siguiente:

1. Hay que desatornillar la caja del ordenador para tener acceso a su interior (es necesario que antes de quitar dicha tapa se haya desenchufado cualquier conexión eléctrica externa).

2. Observe los slots PCI libres que haya en la placa base.



3. Inserte el adaptador en el bus hasta que haya encajado perfectamente y coloque el tornillo para sujetarlo a la caja.

4. Conecte la alimentación eléctrica y encienda el equipo (cuando haya comprobado que todo funciona correctamente, cierre la caja del ordenador).

5. Al arrancar el sistema operativo, detectará que se ha instalado nuevo hardware y solicitará los drivers, ya que se trata de un dispositivo *Plug and Play*.

6. Introduzca el disquete o el CD- ROM con los drivers de la tarjeta (los drivers suelen ser encontrados automáticamente por el sistema operativo. En caso de no ser así, deberá seguir el proceso de instalación indicado por el fabricante).

7. Complete la instalación de los drivers siguiendo las instrucciones que se vayan ofreciendo (dependiendo del sistema operativo, puede solicitar el disco de instalación de dicho sistema o reiniciar el equipo).

8. Una vez reiniciado el equipo, en **Adaptadores de red**, **Administrador de dispositivos**, **Hardware**, **Propiedades** de **Mi PC**, compruebe que se ha instalado la tarjeta y que no se ha producido ningún conflicto (es decir, que no haya ninguna marca amarilla ni roja).

9. Compruebe que aparece el icono **Entorno de red** o **Mis sitios de red** en el escritorio.

10. El último paso lo constituiría la configuración de protocolos, clientes y servicios de un equipo en red (se indicará en la parte práctica del próximo capítulo y dependerá de la opción deseada).

Instalación de un adaptador inalámbrico

Normalmente, en los portátiles actuales y en algunos de los ordenadores de sobremesa, los adaptadores inalámbricos vienen en la placa base por lo que no es necesario instalarlos.

Pero en el caso de haberse estropeado dicho adaptador o querer instalarlo en un equipo que no lo tenga en la placa base, se va a indicar cómo realizarlo a continuación.

Dicho proceso tiene dos partes diferenciadas:

- La instalación física de un adaptador inalámbrico (paso 1) es un simple proceso de manipulación del hardware.

- La instalación lógica del adaptador (pasos 2 al 9) supone la instalación de los drivers o controladores que son los elementos que crean una interfaz entre el sistema operativo del equipo y dicho adaptador inalámbrico (cualquier dispositivo de un equipo dispone de los drivers necesarios que permiten que el sistema operativo se entienda con él).

El proceso a seguir es el siguiente:

1. El adaptador inalámbrico se conectará en el lugar adecuado para ello del equipo (USB, PCMCIA…).

2. Una vez instalado físicamente, aparecerá en la pantalla del equipo una ventana de nuevo dispositivo hardware encontrado.

3. En la siguiente pantalla, hay que decirle que busque el controlador recomendado para dicho adaptador inalámbrico y que busque el driver en la unidad de disquete o del CD-ROM (previamente se habrá que poner en dicho lugar).

4. Una vez encontrado el controlador, mostrará una ventana en donde habrá que indicar que se inicie la instalación.

5. Empezará a cargar los archivos y deberá aparecer una pantalla para que se le diga el identificador SSID que se desea poner (es un código incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID).

6. Cuando haya finalizado la instalación, dirá si ha terminado correctamente y si es preciso reiniciar el equipo.

7. Una vez reiniciado el equipo (en su caso), en **Adaptadores de red**, **Administrador de dispositivos**, **Hardware**, **Propiedades** de **Mi PC** (Windows XP o Server 2003) o **Adaptadores de red**, **Administrador de dispositivos**, **Propiedades** de **Equipo** (Windows Vista), compruebe que se ha instalado la tarjeta y que no se ha producido ningún conflicto (es decir, que no haya ninguna marca amarilla ni roja).

8. Compruebe que aparece el icono **Red** (Windows Vista) o **Mis sitios de red** (Windows XP o Server 2003) en el escritorio.

9. El último paso lo constituiría la configuración de protocolos, encriptación y seguridad (se indicará en la parte práctica del próximo capítulo y dependerá de la opción deseada).

Capítulo 3

REDES LAN

INTRODUCCIÓN

Hasta ahora, se ha visto lo que son las redes desde un punto de vista conceptual, su definición, arquitectura lógica y se ha hablado sobre los distintos tipos de redes.

Las redes locales son las estructuras de comunicación entre ordenadores que abarcan un área limitada: un centro escolar, un edificio, una empresa, etc. Son las redes que se encuentran más próximas a nosotros, si bien, hasta ahora, y a través de la conexión a Internet, hemos tenido un mejor conocimiento de otras tecnologías y otros tipos de redes.

Las características de una red LAN son:

- **Zona geográfica limitada**. Son redes que no se extienden en ámbitos geográficos amplios, lo que permite emplear medios de comunicación privados para la interconexión de ordenadores.

- **Los ordenadores comparten un mismo medio de comunicación**. Todos los ordenadores están conectados a un medio común, por lo que para su utilización deben competir por él pudiéndose provocar colisiones entre los paquetes de datos.

- **Son redes de difusión**. Al disponer de un medio compartido pueden enviar mensajes al resto de los equipos de forma simultánea.

- **Redes optimizadas**. Permiten una gran rapidez y fiabilidad a la hora de transmitir datos.

El desarrollo de las LAN ha buscado siempre una mayor fiabilidad, rapidez y costes más asequibles a la vez que se intentaba solucionar los problemas que el medio de comunicación empleado presentaba.

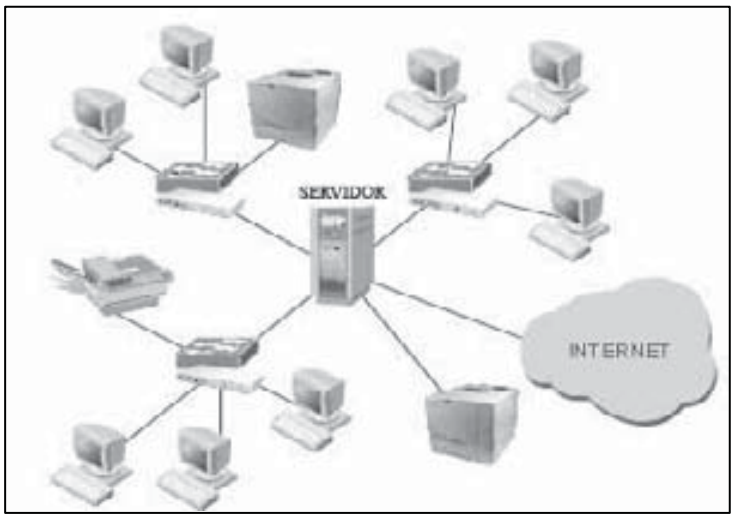


Figura 3.1. Representación esquemática de una red local de una empresa

TOPOLOGÍAS DE LAS REDES LOCALES

Se denomina topología a la forma geométrica en que están distribuidas las estaciones de trabajo y los cables que las conectan.

Las estaciones de trabajo de una red se comunican entre sí mediante una conexión física, y el objeto de la topología es buscar la forma más económica y eficaz de conectarlas para, al mismo tiempo, facilitar la fiabilidad del sistema, evitar los tiempos de espera en la transmisión de los datos, permitir un mejor control de la red y permitir de forma eficiente el aumento de las estaciones de trabajo.

La forma más utilizada actualmente es la configuración en estrella.

Topología en malla

En esta topología cada dispositivo tiene un enlace dedicado y exclusivo por cada otro dispositivo que forme parte de la red.

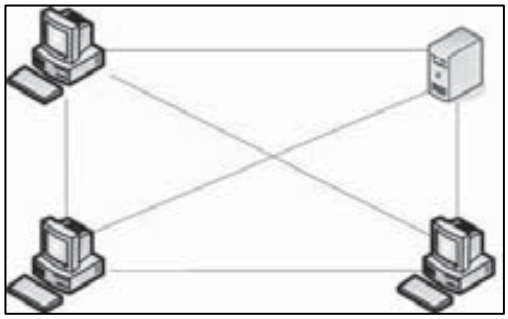


Figura 3.2. Topología en malla

Aunque esta topología es la más eficiente en cuando a rendimiento, es prácticamente inviable en la mayor parte de los casos ya que es muy cara de implementar y muy compleja de mantener o ampliar.

Topología en bus

Es una topología multipunto donde un mismo enlace físico actúa como red troncal que une todos los dispositivos a la red.

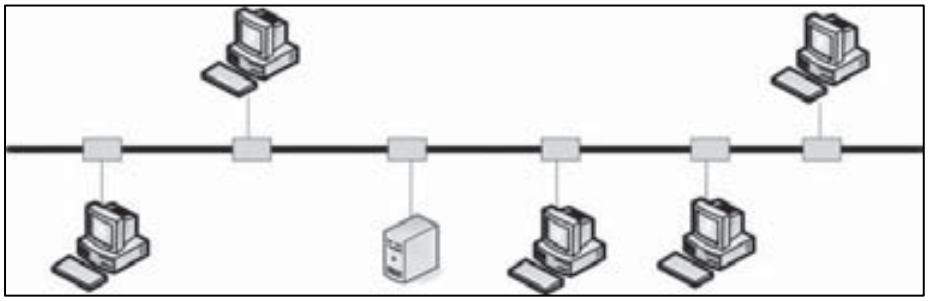


Figura 3.3. Topología en bus

Esta configuración es fácil de instalar, la cantidad de cable a utilizar es mínima, tiene una gran flexibilidad a la hora de aumentar o disminuir el número de estaciones y el fallo de una estación no repercute en la red, aunque la ruptura de un cable la dejará totalmente inutilizada.

Topología en anillo

En esta topología cada dispositivo tiene una línea de conexión dedicada y exclusiva solamente con los dos dispositivos más cercanos.

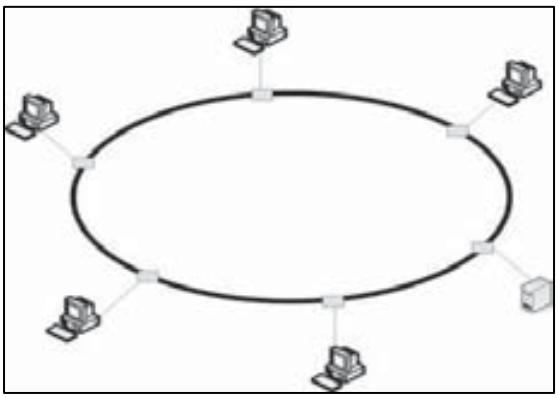


Figura 3.4. Topología en anillo

En las primeras redes de este tipo los datos se movían en una única dirección, de manera que toda la información tenía que pasar por todas las estaciones hasta llegar a la de destino donde se quedaba. Actualmente, disponen de dos canales y transmiten en direcciones diferentes por cada uno de ellos.

Este tipo de redes permite aumentar o disminuir el número de estaciones sin dificultad; pero, a medida que aumenta el flujo de información, será menor la velocidad de respuesta de la red.

Topología en estrella

En esta configuración todos los equipos están conectados directamente al conmutador y las comunicaciones se han de hacer necesariamente a través de él.

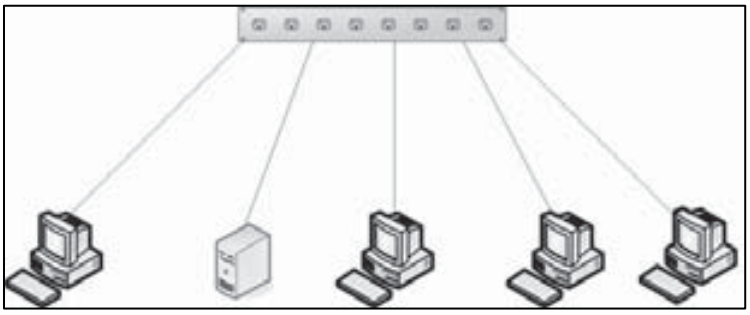


Figura 3.5. Topología en estrella

Permite incrementar y disminuir fácilmente el número de estaciones.

Si se produce un fallo en una de ellas no repercutirá en el funcionamiento general de la red; pero, si se produce un fallo en el conmutador, la red completa se vendrá abajo.

Topología en árbol

Esta topología es una variante de la topología en estrella.

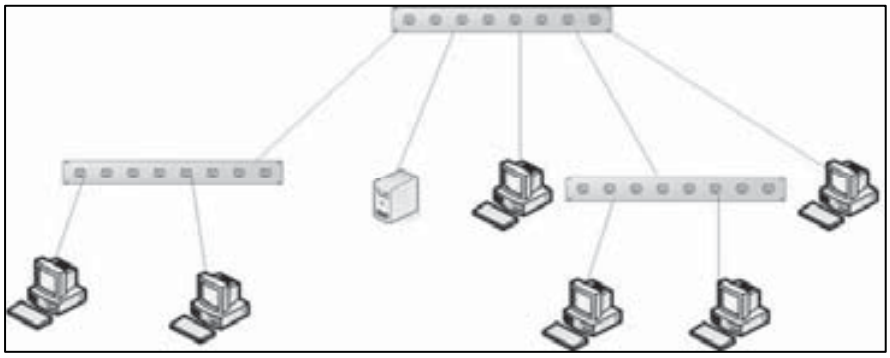


Figura 3.6. Topología en árbol

Topología híbrida

Se utiliza este término para referirse a la combinación de varias de las topologías anteriores.

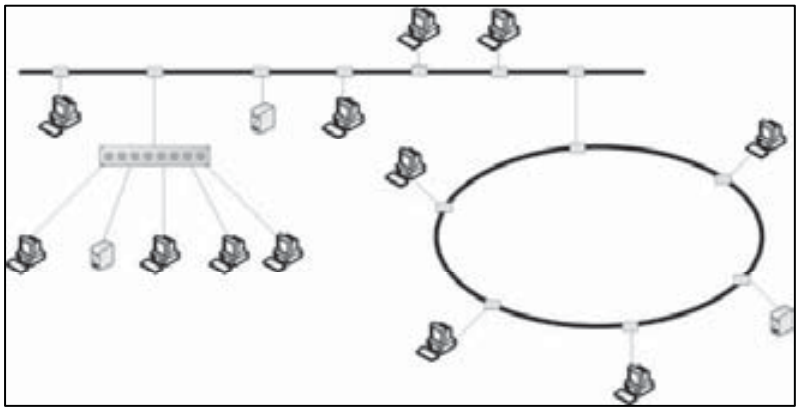


Figura 3.7. Topología híbrida

Topología física y lógica

Todas las configuraciones que se han estado viendo hasta ahora son llamadas topologías físicas porque describen cómo está extendido el cableado.

Además, cada red designa una topología lógica que describe la red desde la perspectiva de las señales que viajan a través de ella.

Un diseño de red puede tener distinta topología física y lógica (es decir, la forma en que esté cableada una red no tiene por qué reflejar necesariamente la forma en que viajan las señales a través de ella).

Por ejemplo, observe la figura siguiente:

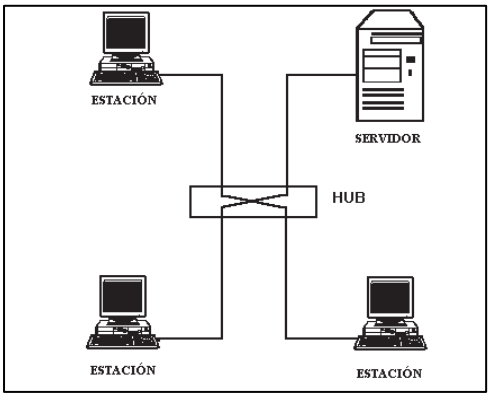


Figura 3.8. Topología física y lógica

En ella se muestra una disposición física de configuración en *estrella*.

Cada estación envía y recibe señales por el mismo cable. En el concentrador (*hub*) se mezclan las señales de todas las estaciones y son transmitidas a todas ellas (es decir, actúa igual que si estuviera en una configuración en *bus*).

Por tanto, es una topología física de *estrella* que funciona como una topología lógica de *bus*.

Muchas redes nuevas utilizan este modelo ya que es fácil de modificar la situación de cada estación (sólo hay que desconectar un cable) sin perjuicio para la red entera y, además, incrementa las posibilidades de detección de problemas de red.

CONFIGURACIÓN DE LA LÍNEA

Se conoce como configuración de la línea a la forma en la que dos o más dispositivos que se comunican se conectan a un enlace. El enlace es el medio físico por el que se transfieren los datos. En función de esta definición existen dos configuraciones de línea posibles:

- **Punto a punto**: cuando existe un enlace dedicado entre dos dispositivos. Toda la capacidad del canal se reserva para la transmisión entre ambos dispositivos.

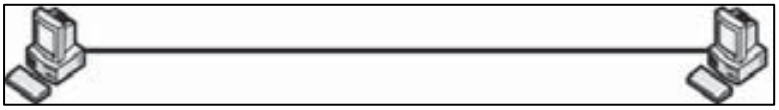


Figura 3.9. Configuración punto a punto

- **Multipunto**: cuando varios dispositivos comparten el mismo enlace. En esta configuración, la capacidad del canal es compartida en el espacio o en el tiempo.

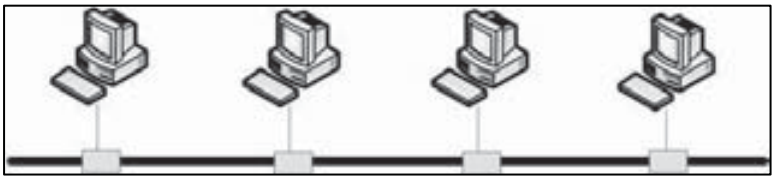


Figura 3.10. Configuración multipunto

TIPOS DE REDES LOCALES

Hay muchos tipos distintos de redes locales, por lo que se pueden realizar múltiples combinaciones distintas al seleccionar el tipo de cableado, la topología, el tipo de transmisión e incluso los protocolos utilizados. Estos factores van a determinar la *arquitectura de la red local*.

Sin embargo, de todas las posibles soluciones hay dos que ya están establecidas y que, al mismo tiempo, cuentan con una gran difusión dentro del mundo de las redes locales:

- Ethernet.
- Token Ring.

Ethernet

Esta arquitectura de red fue desarrollada por *Xerox Corporation* para enlazar un grupo de microordenadores, que estaban distribuidos por los laboratorios de investigación de *Palo Alto* en California, para poder intercambiar programas y datos, así como compartir los periféricos.

En un principio se creó para ser utilizada con cable coaxial de banda base, aunque actualmente se pueden utilizar otros tipos de cable y es la que está más extendida.

Si se utiliza cable coaxial grueso, se pueden tener hasta cuatro tramos de cable (unidos con repetidores) y los ordenadores se conectan al cable por medio de transceptores (la distancia máxima entre el ordenador y el transceptor ha de ser de 15 metros). Se pueden conectar ordenadores en tres tramos únicamente, con un máximo de 100 estaciones en cada tramo.

Si se utiliza cable coaxial fino, no es necesario utilizar transceptores, pudiéndose conectar el cable al ordenador por medio de una conexión *BNC* en forma de *T*. El número máximo de tramos es de cinco y la longitud máxima de cada tramo es, aproximadamente, de un tercio de la longitud máxima conseguida con el cable coaxial grueso (550 metros). Así mismo, el número máximo de estaciones es de 30 por cada uno de los tres tramos en los que se pueden conectar ordenadores.

Las implementaciones Ethernet anteriores tenían varios inconvenientes. Además de que su implantación requería una alta inversión inicial, el mantenimiento posterior también suponía una fuente de problemas. En este tipo de redes, las rupturas de cables o malas derivaciones eran difíciles de detectar y afectaban al rendimiento de la red entera.

En este escenario, el IEEE publicó en 1990 la implementación 10BASE-T (la letra T es de Twisted, trenzado), basada en un elemento central donde se implementa un bus lógico pero utilizando una topología física en estrella. Las uniones entre cada estación y el elemento central se realizan utilizando cable de par trenzado de categoría 3. Muchos edificios disponían de una infraestructura con este tipo de cable para dar servicio telefónico por lo que se podía aprovechar para implementar las redes 10BASE-T. La topología en estrella favoreció su mantenimiento ya que los problemas en una sección de cable sólo afectarían a la estación a la que daba servicio. En definitiva, esta implementación Ethernet era la más barata y la más fácil de mantener por lo que se convirtió rápidamente en la más popular.

Paralelamente al desarrollo de los estándares para redes locales se desarrollaron normativas de cableado de telecomunicaciones para edificios comerciales que permiten constituir lo que se conoce como cableado estructurado. Las primeras normas de cableado estructurado fueron publicadas como EIA/TIA.

Los datos se transmiten a una velocidad de 10 *Mbps* a una distancia máxima de dos kilómetros.

Utiliza un protocolo de contienda *CSMA/CD* (*Acceso múltiple por detección de portadora con detección de colisiones*) en donde cualquier estación puede intentar transmitir en cualquier momento, pero, como todas utilizan un canal único, sólo una estación puede transmitir datos simultáneamente.

El tamaño del bloque de datos puede oscilar desde 72 hasta 1.526 *bytes* (con un tamaño normal de 256 *bytes*).

Todas las estaciones tienen asignada una dirección para la tarjeta de red que permite que, cuando se cambia de lugar una estación, no haya posibilidad de conflictos y, por tanto, se puede reconfigurar completamente la red local con unos mínimos cambios en el sistema operativo.

Fast Ethernet

Esta moderna arquitectura de red está basada en la tecnología *Ethernet* descrita anteriormente, pero cuenta con las siguientes variaciones que le permiten transmitir a una velocidad de 100 *Mbps*:

- Está construida con *hubs/switchs* distribuidos que utilizan líneas dedicadas para cada ordenador.

- Los cables utilizados son: *100BaseTX*, *100BaseFX* y *100BaseT4*. La diferencia entre estos tres tipos de cables está en que el cable *100BaseTX* usa dos de los cuatro pares de hilos (igual que un cable *UTP* normal), que deben ser de categoría 5 (por su mayor calidad), el cable *100BaseFX* es el equivalente en fibra óptica del cable *100BaseTX* y el cable *100BaseT4* utiliza los cuatro pares de hilos, que pueden ser de categoría 3 ó 5.

- Necesita tarjetas de red específicas para la velocidad de transmisión de 100 *Mbps*.

Al igual que la arquitectura de red *Ethernet*, utiliza el protocolo de contienda *CSMA/CD* (*Acceso múltiple por detección de portadora con detección de colisiones*) y su coste de instalación es similar.

Gigabit Ethernet

Entre los años 1998 y 1999 el IEEE amplió el estándar para incluir un nuevo tipo de redes, llamado de forma genérica **Gigabit Ethernet**. Este estándar se desarrolló bajo dos especificaciones: la primera desarrollada en 1998 llamada **1000BASE-X** que utiliza fibra óptica y la segunda desarrollada en 1999 llamada **1000BASE-T** que utiliza cable de cobre de par trenzado UTP de categorías 5, 5e o 6 con una longitud máxima de 100 metros, con transmisión half-dúplex o full-dúplex y en su diseño se intentó mantener la compatibilidad con las versiones anteriores.

La principal característica de Gigabit Ethernet es que la velocidad de transmisión es de 1.000 Mbps o 1 Gbps.

10-Gigabit Ethernet

En el año 2002 se publicó un nuevo estándar llamado **10-Gigabit Ethernet**, que funciona a velocidades de 10 Gbps sobre fibra óptica. Esta primera especificación de 10-Gigabit Ethernet incluye varias implementaciones de la misma, entre las que se encuentran 10GBASE-SR para distancias cortas hasta 300 metros, 10GBASE-LR que utiliza fibra óptica monomodo y admite distancias de hasta 20 Km, 10GBASE-LX4 que utiliza multiplexación por división de onda (WDM).

La última implementación de 10-Gigabit Ethernet sobre fibra óptica es 10GBASE-LRM publicada en 2006 (IEEE 802.3aq) y que utiliza fibra óptica multimodo compatible con FDDI.

La especificación de la tecnología 10-Gigabit Ethernet sobre cable UTP se ha publicado en 2006 (IEEE 802.3an). Utiliza cable de categoría 6 con una distancia máxima de 100 metros. Sin embargo, los primeros productos que se han lanzado bajo este estándar en cable de cobre utilizan cable InfiniBand con una limitación de 15 metros como distancia máxima.

TOKEN RING

Esta arquitectura de red fue creada por *IBM* en octubre de 1985 aunque anteriormente había comercializado dos tipos de redes locales: una red de banda base a 375 *Kbps* y para un máximo de 64 ordenadores, y una red de banda ancha a 2 *Mbps* para un máximo de 72 ordenadores.

Emplea una topología de anillo con protocolo de paso de testigo y se puede utilizar cable de par trenzado, cable coaxial y fibra óptica.

Los datos se transmiten a una velocidad de 4 *Mbps*, pudiéndose conectar hasta un máximo de 8 ordenadores y a una distancia máxima de 350 metros en cada unidad de acceso multiestación (**MAU**) si se utiliza con cable coaxial (si se utiliza con fibra óptica puede llegar hasta una velocidad de 16 *Mbps*).

No obstante, como se pueden conectar hasta 12 unidades de acceso multiestación (*MAU*), el número de ordenadores conectados y la distancia máxima pueden aumentar considerablemente.

REDES LOCALES INALÁMBRICAS

Cuando se precisa movilidad en las comunicaciones el cable se convierte en un inconveniente más que en una ayuda. Depender de un enlace físico supone una seria limitación para conseguir una absoluta libertad de movimientos. Para salvar estos obstáculos las redes inalámbricas son la alternativa perfecta. Esta tecnología comenzó hace unos 5 años, pero ahora es cuando se está empezando a usar, debido al abaratamiento de los costes y a su estandarización.

Las comunicaciones de radio han estado a nuestra disposición desde hace ya bastante tiempo, teniendo como principal aplicación la comunicación mediante el uso de la voz. Hoy en día, los sistemas de radio de dos vías para comunicaciones de voz punto a punto o multipunto son ampliamente usados. Sin embargo, aunque los ingenieros ya conocían las técnicas para modular una señal de radio con la cual conseguir el envío de datos binarios, sólo recientemente han podido desarrollar y desplegar servicios de datos inalámbricos a gran escala.

Como muestra del complejo campo de las redes sin cables, el mundo de los denominados datos inalámbricos incluyen enlaces fijos de microondas, redes LAN inalámbricas, datos sobre redes celulares, redes WAN inalámbricas, enlaces mediante satélites, redes de transmisión digital, redes con paginación de una y dos vías, rayos infrarrojos difusos, comunicaciones basadas en láser, sistema de Posicionamiento Global (GPS) y muchos más. Múltiples tecnologías, muchas de las cuales son utilizadas por millones de usuarios día a día sin conocer cómo la información ha llegado hasta ellos.

Se conoce con el término genérico de **WLAN** (Wireless LAN, redes LAN inalámbrica) a las redes de área local que utilizan ondas electromagnéticas (radio e infrarrojo) para la transmisión de datos entre los equipos conectados a dichas redes. Al igual que en las redes LAN cableadas, los dispositivos que se interconectan por medio de las redes WLAN están situados en un área de extensión limitada.

Los dispositivos Wi-Fi se pueden conectar a través de dos modos de operación:

- Ad hoc
- Infraestructura

El **modo Ad hoc** se utiliza para conectar mediante Wi-Fi dos dispositivos de forma sencilla. La configuración Ad hoc no requiere muchas opciones de configuración. Se pueden conectar en una red *Ad hoc* hasta 10 dispositivos aunque esto no suele ser habitual.

El **modo infraestructura** permite más posibilidades a las redes inalámbricas. En este modo existe un elemento centralizador de la transferencia de información llamado **punto de acceso**. El uso del modo infraestructura utilizando puntos de acceso permite un mayor alcance a las redes así como comunicaciones más seguras y con más posibilidades de configuración. Además, los puntos de acceso permiten la conexión entre la red inalámbrica y una red cableada para lo cual incluyen un puerto de conexión a la red cableada, normalmente de tipo RJ-45.

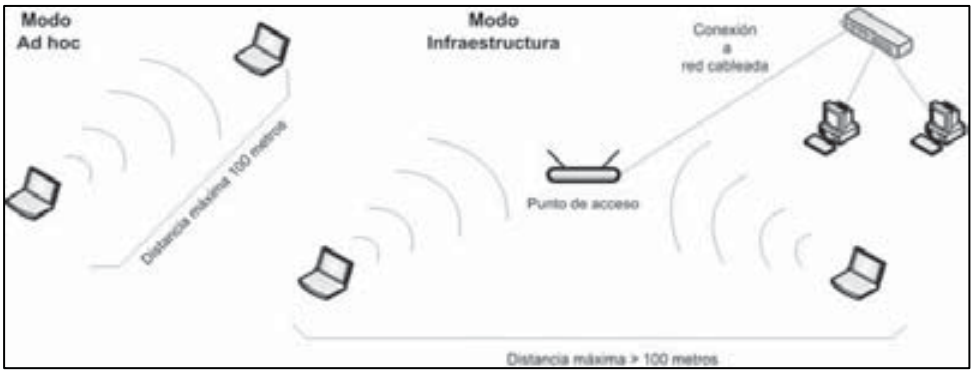


Figura 3.11. Modos Ad hoc e infraestructura

Las principales ventajas de una red inalámbrica son:

- La movilidad y libertad de movimientos de los equipos.

- La facilidad de implementar la red en un tiempo mucho menor que el que llevaría una red convencional y sin afectar la infraestructura del edificio existente. Se consiguen conexiones que serían inviables con otro tipo de medio por limitantes arquitectónicos o de distancias, o por estar prohibido tender cableado.

- La flexibilidad, porque con la misma facilidad con que se instala, se desinstala. Esto elimina la necesidad de levantar el cableado existente en el caso de un traslado.

Actualmente, las técnicas más extendidas para su utilización en redes inalámbricas son: infrarrojos y radio.

Infrarrojos

Los infrarrojos son ondas electromagnéticas que se propagan en línea recta y que pueden ser interrumpidas por cuerpos opacos.

Todas las redes sin hilos por infrarrojos operan usando un rayo de luz infrarroja para transportar los datos entre dispositivos. Estos sistemas necesitan generar señales muy fuertes, debido a que las señales de transmisión dispersas son susceptibles a la luz desde fuentes como ventanas.

Puede transmitir señales con alta velocidad debido al alto ancho de banda de la luz infrarroja (puede emitir a 10 *Mbps*).

Hay cuatro tipos de redes de infrarrojos:

- **Redes en línea de vista (Line-of-sight)**. Como su propio nombre indica, este tipo sólo transmite si el transmisor y el receptor se ven limpiamente.

- **Redes por dispersión de infrarrojos (Scatter)**. Este tipo emite transmisiones para que reboten en las paredes y techos, y eventualmente contacten con el receptor.

- **Redes por reflexión (Reflective)**. En este tipo, los transceptores ópticos situados cerca de los ordenadores transmiten hacia un punto común que redirige las transmisiones al ordenador apropiado.

- **Telepunto óptico de banda ancha**. Este tipo proporciona servicios de banda ancha. Es capaz de manejar requerimientos de alta calidad multimedia que pueden coincidir con los proporcionados por una red de cable.

No se ven afectados por interferencias externas (con la excepción de la fuerte luz ambiental) y puede alcanzar hasta 200 metros entre el emisor y el receptor. No es necesaria la obtención de una licencia administrativa para su uso.

Radio

Se pueden distinguir principalmente los siguientes estándares relacionados con las redes inalámbricas (realmente, únicamente se puede considerar como estándar los dos primeros y los otros dos como tecnologías especializadas):

- **IEEE 802.11** es el estándar para redes WLAN y cubre las funciones del nivel físico y del subnivel MAC del nivel de enlace.

  La primera versión de este estándar se desarrolló en 1997. En esta primera especificación se incluía como medios de transmisión tanto infrarrojos como las ondas radioeléctricas a una frecuencia de 2'4 GHz. La velocidad de transmisión máxima alcanzada era de 1 ó 2 Mbps. El uso de infrarrojos como medio de transmisión, aunque se llegó a especificar en el estándar, nunca se llegó a utilizar debido a las limitaciones de este tipo de comunicaciones.

  La especificación de la frecuencia de trabajo de 2'4 GHz realmente se refiere a una banda de frecuencias que va desde 2'4 GHz hasta 2'4835 GHz (es decir, ocupa un ancho de banda de 83'5 MHz). Lo interesante de esta banda de frecuencias es que no requiere licencia de uso. Por el contrario, como esta banda de frecuencias es de uso libre, es utilizada por otros dispositivos, como hornos microondas, teléfonos inalámbricos o dispositivos Bluetooth con los que podría tener interferencias.

  En el año 1999 el IEEE publica dos nuevas especificaciones del estándar 802.11. Una de ellas es la especificación **IEEE 802.11a** e incluye las siguientes características:

  - Utiliza la banda de frecuencias de 5 GHz (5'725 a 5'850 GHz).
  - Velocidad de transmisión máxima: 54 Mbps.

  La especificación 802.11a ha tenido mayor repercusión en Estados Unidos y Japón que en Europa ya que aquí, la banda de los 5 GHz estaba reservada para las redes HiperLAN/2.

  La otra especificación publicada en 1999 es la **IEEE 802.11b** con las siguientes características:

  - Utiliza la banda de frecuencias de 2'4 GHz.
  - Velocidad de transmisión máxima: 11 Mbps.

En 2003, se publica el estándar **IEEE 802.11g** que es el que más penetración ha tenido en el mercado. Sus características son las siguientes:

- Opera en la banda de 2'4 GHz.
- Alcanza una velocidad de hasta 54 Mbps.
- Los dispositivos fabricados para 802.11g son compatibles con 802.11b.

Se está desarrollando una nueva implementación que permitirá velocidades máximas de hasta 540 Mbps, llamado **IEEE 802.11n** y que puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a). Gracias a ello, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada y en 802.11n permite alcanzar un mayor rendimiento.

- **HiperLAN**. El **ETSI** (**European Telecommunications Standards Institute**) llevó a cabo durante los años 1991 y 1996 este proyecto con el que pretendía conseguir una tasa de transferencia mayor que la ofrecida por la especificación *IEEE 802.11*. Incluía cuatro estándares diferentes, de los cuales el denominado Tipo 1 es el que verdaderamente se ajusta a las necesidades futuras de las *WLAN*, estimándose una velocidad de transmisión de 23,5 *Mbps* (54 *Mbps* con *HiperLAN/2*), muy superior a los 11 *Mbps* de la actual normativa *IEEE 802.11b*.

- **Bluetooth** que es una tecnología de corto alcance y de bajo consumo diseñada para conexión de periféricos a ordenador o para dispositivos portátiles (por ejemplo, los auriculares inalámbricos de *Ericsson*. Como en Europa no está permitido conducir con un teléfono móvil, utilizando dichos auriculares y un teléfono *Bluetooth*, sólo es necesario decir *responder* o *llamar al número determinado* para realizar la conexión, aunque el teléfono se encuentre en un maletín o en una cartera). Está optimizada para los transceptores de radio de bajo consumo ideales para los dispositivos personales. Su alcance reducido es bueno para detecciones de proximidad pero como las señales no son suficientemente fuertes para penetrar paredes, suelos o cubrir toda una casa, no es adecuado para redes inalámbricas.

- **HOMERF** que es una tecnología diseñada para la conectividad sin hilos dentro de un hogar e, incluso, interoperar con las redes públicas de telefonía e *Internet*. Opera en la banda de 2,4 GHz, pero

combinando elementos de los estándares **DECT** (**Digitally Enhanced Cordless Telephone**) e ***IEEE 802.11***.

Componentes de las redes inalámbricas

En una red inalámbrica se pueden distinguir:

- Un encaminador para el acceso a Internet.
- Un punto de acceso como mínimo.
- Clientes inalámbricos.

Las dos primeras opciones pueden sustituirse por un **encaminador inalámbrico** que es simplemente un router con una interfaz inalámbrica (se distingue de un router normal porque lleva una o dos antenas).

PUNTO DE ACCESO

Un punto de acceso es un concentrador inalámbrico. El transmisor/receptor conecta entre sí los nodos de la red inalámbrica y, normalmente, también sirve de puente entre ellos y la red cableada. Un conjunto de puntos de acceso (coordinados) se pueden conectar los unos con otros para crear una gran red inalámbrica.

Desde el punto de vista de los clientes inalámbricos (como los ordenadores portátiles o las estaciones móviles), un punto de acceso proporciona un *cable virtual* entre los clientes asociados. Este *cable inalámbrico* conecta tanto a los clientes entre sí, como los clientes con la red cableada.

Figura 3.12. Punto de acceso

Un punto de acceso debe distinguirse de un encaminador inalámbrico (muy común en el mercado actual) que es una combinación entre un punto de acceso y

un encaminador o router y que puede ejecutar tareas más complejas que las de un punto de acceso.

Figura 3.13. Router inalámbrico

Un punto de acceso también se puede utilizar como **repetidor** para ampliar la distancia entre los distintos nodos de una red Wi-Fi.

Los clientes se han de conectar al punto de acceso mediante su nombre. Este mecanismo de identificación se conoce como **SSID** (*Service Set Identifier*, *Identificador del Conjunto de Servicio*) y debe ser el mismo para todos los miembros de una red inalámbrica específica. Todos los puntos de acceso y los clientes que pertenecen a un mismo **ESS** (*Extended Service Set*, *Conjunto de Servicio extendido*) se deben configurar con el mismo *ID* (**ESSID**).

CLIENTES INALÁMBRICOS

Un cliente inalámbrico es cualquier estación inalámbrica que se conecta a una LAN inalámbrica para compartir sus recursos. Una estación inalámbrica se define como cualquier ordenador con una tarjeta adaptadora de red inalámbrica instalada que transmite y recibe señales de Radio Frecuencia (RF).

Figura 3.14. Tarjeta de red Wi-Fi interna

Algunos de los clientes inalámbricos más comunes son los ordenadores portátiles, PDAs, equipos de vigilancia y teléfonos inalámbricos de VoIP (Voz IP).

Figura 3.15. Tarjeta de red Wi-Fi USB

Seguridad de una red inalámbrica

Es evidente que uno de los factores que más importancia tiene cuando se decide utilizar o implementar una red inalámbrica es la seguridad. Esto es así por que, a diferencia de lo que ocurre en las redes cableadas, los datos transferidos a través de redes inalámbricas utilizan un medio de comunicación que no está restringido, como es el aire. Nuestros datos viajan por un medio de comunicación accesible a cualquier dispositivo, externo a la red pero con la capacidad de captación de la señal radioeléctrica. Esta característica hace necesario algún método de cifrado de la información que se transmite en una red inalámbrica.

El mecanismo de seguridad inicialmente especificado en el estándar 802.11 es **WEP (Wired Equivalent Privacy, Privacidad equivalente al cable)**. Este mecanismo está considerado actualmente como poco robusto y relativamente fácil de romper. Se basa en la utilización de claves simétricas, por lo que tanto las estaciones como el punto de acceso deben conocer la clave. La encriptación de los datos se basa en un algoritmo llamado **RC4**.

Debido a las debilidades de WEP, el IEEE comenzó a desarrollar un nuevo estándar de seguridad con la asignación **IEEE 802.11i**. Esta especificación incluye un esquema de encriptación alternativo llamado **TKIP (Temporal Key Integrity Protocol)**.

Mientras la IEEE finalizaba el estándar IEEE 802.11i y para corregir las debilidades del sistema *WEP*, la *Wi-Fi Alliance* desarrolló un estándar temporal para sustituir a WEP conocido como **WPA (Wi-Fi Protected Access, Acceso protegido Wi-Fi)**. Esta especificación utiliza *TKIP* como mecanismo de encriptación, al igual que IEEE 802.11i. Sin embargo se puede utilizar el mismo hardware que *WEP*, es decir, no es necesario cambiar las tarjetas de red a los puntos de acceso, siendo necesario cambiar únicamente el *firmware* de dichos dispositivos. Este sistema también utiliza claves simétricas con el algoritmo *RC4*, pero para añadir protección adicional, *TKIP* genera claves temporales que son cambiadas de forma dinámica. Añade algunas mejoras más respecto a *WEP*, por ejemplo, usa un vector de iniciación de 48 bits en lugar de los 24 utilizados en *WEP*.

WPA utiliza, además, un proceso de autentificación desarrollado bajo el estándar **IEEE 802.1x** y que define un procedimiento de control de acceso al nivel de acceso al medio (MAC). El componente más importante de este estándar es el llamado **EAP (Extensible Authentication Protocol)** que surgió como mejora del método de autenticación utilizado en *PPP*. En *WPA* se admiten dos procesos de autentificación. El primero, conocido como **WPA Entrerprise**, se lleva a cabo a través de un servidor de autentificación (normalmente un servidor RADIUS) y se utiliza habitualmente en entornos profesionales. El segundo, que se conoce como **WPA Personal** o **WPA-PSK**, se lleva a cabo través de una clave pre-compartida **(PSK, Pre-shared Key)** y se utiliza en entornos menos restrictivos y entornos domésticos.

En 2004 se publica el estándar IEEE 802.11i al que también se le conoce como **WPA2**. Uno de los principales cambios es la utilización de **AES (Advanced Encryption Standard, Estándar de encriptación avanzado)** en lugar de usar *RC4*, aunque el uso de este estándar implica un cambio del hardware utilizado. Incluye además el uso de IEEE 802.1x con todas las características de *WPA*.

Además de los mecanismos de seguridad anteriores existen algunas estrategias más que pueden llevarse a cabo. Una de las posibilidades que muchos puntos de acceso proporcionan es el llamado **filtrado por dirección MAC**, en el cual es necesario almacenar en el punto de acceso las direcciones MAC de los dispositivos que forman parte de la red Wi-Fi, de forma que el punto de acceso no permitirá el acceso a la red a ningún dispositivo cuya dirección MAC no esté en la lista. Este método no es factible en sistemas Wi-Fi donde los usuarios conectados al sistema no son fijos, como en hoteles, puntos de acceso públicos, etc.

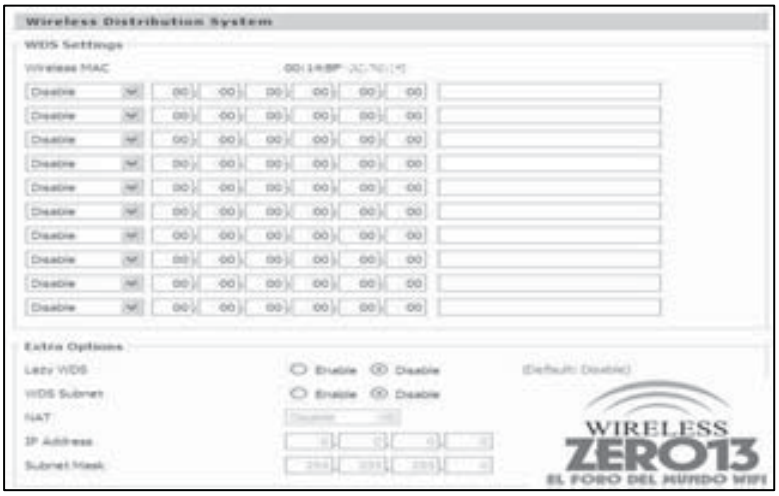


Figura 3.16. Tabla del filtrado por direcciones MAC

SEGMENTACIÓN DE LA RED (PARTE PRÁCTICA)

Planteamos una situación que se puede dar actualmente en cualquier empresa y es la siguiente:

- La empresa dispone de doce ordenadores repartidos por igual en cuatro departamentos: Gerencia, Contabilidad, Producción y Ventas.
- Todos los ordenadores han de estar unidos al mismo conmutador.
- Habrá que crear cuatro subredes independientes, una por departamento y no deberá haber interconexión entre los ordenadores de un departamento con los del resto.
- Los ordenadores han de tener una configuración IP estática.

Se va a utilizar la última tabla que se explica en el apartado *Construir una tabla de subredes* dentro de *Segmentación de la red* del capítulo 2:

Nº de bits	1	2	3	4	5	6	7	8
Incremento	128	64	32	16	8	4	2	1
Máscara de subred	128	192	224	240	248	252	254	255
Nº de redes	2	4	8	16	32	64	128	256

Hay que fijarse en la celda correspondiente a 4 en la fila *Nº de redes*:

Nº de bits	1	2	3	4	5	6	7	8
Incremento		64						
Máscara de subred		192						
Nº de redes		4						

Observe la columna correspondiente a dicha celda que indica:

- Incremento: 64 (es decir, cada subred podría tener un máximo de 64 direcciones de los que se podría utilizar 62 direcciones IP para equipos).
- Máscara de subred: 192 (que se podría corresponder con 255.255.255.192 si es de clase C).

Con todo ello, una posible solución de la segmentación es la siguiente:

Dirección de red	Dirección de inicio	Dirección final	Dirección de broadcast
192.168.0.0	192.168.0.1	192.168.0.62	192.168.0.63
192.168.0.64	192.168.0.65	192.168.0.126	192.168.0.127
192.168.0.128	192.168.0.129	192.168.0.190	192.168.0.191
192.168.0.192	192.168.0.193	192.168.0.254	192.168.0.255

Y una posible asignación de las direcciones IP de los equipos podría ser la siguiente:

Nombre equipo	Dirección IP	Máscara de subred
G-PC1	192.168.0.2	255.255.255.192
G-PC2	192.168.0.3	255.255.255.192
G-PC3	192.168.0.4	255.255.255.192
G-PC4	192.168.0.5	255.255.255.192
C-PC1	192.168.0.66	255.255.255.192
C-PC2	192.168.0.67	255.255.255.192
C-PC3	192.168.0.68	255.255.255.192
C-PC4	192.168.0.69	255.255.255.192
V-PC1	192.168.0.130	255.255.255.192
V-PC2	192.168.0.131	255.255.255.192
V-PC3	192.168.0.132	255.255.255.192
V-PC4	192.168.0.133	255.255.255.192
P-PC1	192.168.0.194	255.255.255.192
P-PC2	192.168.0.195	255.255.255.192
P-PC3	192.168.0.196	255.255.255.192
P-PC4	192.168.0.197	255.255.255.192

Fíjese que las primeras direcciones de cada rango de las subredes se han dejado sin asignar para reservarlas en caso de utilizarse un router en el futuro para salir a Internet (se explicará en el capítulo siguiente).

COMUNICACIONES ENTRE DOS EQUIPOS (PARTE PRÁCTICA)

A través de un cable RJ45 cruzado

Este procedimiento va a permitir la interconexión de dos equipos a través de los adaptadores de red empleando un cable UTP cruzado.

Se da por supuesto que los ordenadores tienen instalados los adaptadores de red y que está preparado el latiguillo del cable UTP categoría 5 cruzado (para ver cómo hacerlo, consulte la parte práctica del capítulo 2).

Una vez conectados ambos equipos mediante el cable cruzado a través de los adaptadores de red, siga los pasos siguientes:

En **Windows XP**:

1. Pulse con el botón derecho del ratón sobre **Mis sitios de red** (si no aparece en el Escritorio, se encuentra en el **menú Inicio**) y seleccione **Propiedades**.

2. En la ventana que se ha abierto (**Conexiones de red**), pulse con el botón derecho del ratón sobre **Conexión de área local** y seleccione **Propiedades**.

3. Verá que hay varios elementos instalados, entre ellos Cliente para redes Microsoft, Compartir impresoras y archivos para redes Microsoft y Protocolo Internet (TCP/IP). Fíjese que el cuadrado que hay a su izquierda está activado, ya que en caso contrario, dichos elementos estarían desactivados.

4. Para conectar dos equipos a través de un cable cruzado, no es necesario modificar las configuraciones que vienen por defecto a excepción de la dirección IP asignada de forma dinámica. Para poner una dirección IP estática, vea el apartado *Configuración TCP/IP estática para un equipo*.

5. Ahora se va a identificar cada uno de los equipos. Para ello, pulse **Mi PC** con el botón derecho del ratón, elija **Propiedades**, seleccione la pestaña **Nombre de equipo** y pulse en **Cambiar**.

6. Indique un nombre distinto para cada uno de los dos equipos y hágalos formar parte a los dos del mismo grupo de trabajo. Cuando haya

finalizado, pulse en **Aceptar** dos veces y reinicie los equipos si así se le indica.

7. Cuando se hayan reiniciado, seleccione el icono **Mis sitios de red** y, después, **Ver equipos del grupo de trabajo** (se encuentra a la izquierda en **Tareas de red)**.

8. Verá que se muestran los dos equipos (en caso de no ver un equipo que tiene Windows Vista, vea el apartado *Activar el uso compartido de archivos en Windows Vista*). Pulse sobre el otro equipo (recuerde que únicamente accederá directamente a dicho equipo si el usuario se encuentra dado de alta en ambos equipos y tiene la misma contraseña. En caso contrario, le mostrará una ventana para que indique el usuario y la contraseña con la que desea conectarse) y verá los directorios que tiene compartidos (para ver cómo compartir un directorio, vea el apartado *Cómo compartir directorios* del capítulo 7).

9. Pulse sobre el directorio compartido que desee y verá los archivos que se encuentra en él y podrá actuar con ellos en función de los permisos que tiene adjudicados.

NOTA. Si tiene problemas al compartir archivos o una impresora de una red, asegúrese de que *Firewall de Windows* no está bloqueando **Compartir archivos e impresoras**. Para ello, vea el apartado *Activar el compartir archivos en el Firewall de Windows*.

En **Windows Vista**:

1. Pulse con el botón derecho del ratón sobre **Red** (si no aparece en el Escritorio, se encuentra en el **menú Inicio**) y seleccione **Propiedades**.

2. En la ventana que se ha abierto (**Centro de redes y recursos compartidos**), pulse sobre **Administrar conexiones de red** (se encuentra en el panel izquierdo), pulse con el botón derecho del ratón sobre **Conexión de área local** y seleccione **Propiedades**.

3. Si se lo indica, pulse **Continuar** para indicar que desea dar permiso para seguir con la operación. Verá que hay varios elementos instalados, entre ellos Cliente para redes Microsoft, Compartir impresoras y archivos para redes Microsoft, Protocolo Internet versión 4 (TCP/IPv4) y Protocolo Internet versión 6 (TCP/IPv6). Fíjese que el cuadrado que hay a su izquierda está marcado, ya que en caso contrario, dichos elementos estarían desactivados.

4. Para conectar dos equipos a través de un cable cruzado, no es necesario modificar las configuraciones que vienen por defecto a excepción de la dirección IP asignada de forma dinámica. Para poner una dirección IP estática, vea el apartado *Configuración TCP/IP estática para un equipo*.

5. Ahora se va a identificar cada uno de los equipos. Para ello, pulse **Equipo** con el botón derecho del ratón, elija **Propiedades**, pulse en **Cambiar la configuración** y pulse en **Continuar** para poder continuar con el proceso (si se lo pide).

6. Pulse en **Cambiar** e indique un nombre distinto para cada uno de los dos equipos y hágalos formar parte a los dos del mismo grupo de trabajo. Cuando haya finalizado, pulse en **Aceptar** dos veces y reinicie los equipos si así se le indica.

7. Cuando se hayan reiniciado, seleccione la opción **Red** del menú **Inicio** y verá que se muestran los dos equipos (en caso de no ver los equipos, vea el apartado *Activar la detección de redes en Windows Vista*). Pulse sobre el otro equipo (recuerde que únicamente accederá directamente a dicho equipo si el usuario se encuentra dado de alta en ambos equipos y tiene la misma contraseña. En caso contrario, le mostrará una ventana para que indique el usuario y la contraseña con la que desea conectarse) y verá los directorios que tiene compartidos (para ver cómo compartir un directorio, vea el apartado *Cómo compartir directorios* del capítulo 7).

8. Pulse sobre el directorio compartido que desee y verá los archivos que se encuentra en él y podrá actuar con ellos en función de los permisos que tiene adjudicados.

NOTA. Si tiene problemas al compartir archivos o una impresora de una red, asegúrese de que *Firewall de Windows* no está bloqueando **Compartir archivos e impresoras**. Para ello, vea el apartado *Activar el compartir archivos en el Firewall de Windows*.

A través de un cable USB

Este procedimiento va a permitir la interconexión de dos equipos a través de un cable USB.

Una vez instalado en ambos equipos el software correspondiente que viene con el cable USB y, después, conectados los dos equipos con dicho cable, siga los

pasos siguientes (únicamente se va a describir cómo hacerlo en Windows XP, ya que es el software que había disponible):

1. Pulse con el botón derecho del ratón sobre **Mis sitios de red** (si no aparece en el Escritorio, se encuentra en el **menú Inicio**) y seleccione **Propiedades**.

2. En la ventana que se ha abierto (**Conexiones de red**), pulse con el botón derecho del ratón sobre **Conexión de área local** y seleccione **Propiedades**.

3. Verá que hay varios elementos instalados, entre ellos Cliente para redes Microsoft, Compartir impresoras y archivos para redes Microsoft y Protocolo Internet (TCP/IP). Fíjese que el cuadrado que hay a su izquierda está activado, ya que en caso contrario, dichos elementos estarían desactivados.

4. Para conectar dos equipos a través de un cable cruzado, no es necesario modificar las configuraciones que vienen por defecto a excepción de la dirección IP asignada de forma dinámica. Para poner una dirección IP estática, vea el apartado *Configuración TCP/IP estática para un equipo*.

5. Ahora se va a identificar cada uno de los equipos. Para ello, pulse **Mi PC** con el botón derecho del ratón, elija **Propiedades**, seleccione la pestaña **Nombre de equipo** y pulse en **Cambiar**.

6. Indique un nombre distinto para cada uno de los dos equipos y hágalos formar parte a los dos del mismo grupo de trabajo. Cuando haya finalizado, pulse en **Aceptar** dos veces y reinicie los equipos si así se le indica.

7. Cuando se hayan reiniciado, seleccione el icono **Mis sitios de red y**, después, **Ver equipos del grupo de trabajo** (se encuentra a la izquierda en **Tareas de red)**.

8. Verá que se muestran los dos equipos (en caso de no ver un equipo que tiene Windows Vista, vea el apartado *Activar el uso compartido de archivos en Windows Vista*). Pulse sobre el otro equipo (recuerde que únicamente accederá directamente a dicho equipo si el usuario se encuentra dado de alta en ambos equipos y tiene la misma contraseña. En caso contrario, le mostrará una ventana para que indique el usuario y la contraseña con la que desea conectarse) y verá los directorios que

tiene compartidos (para ver cómo compartir un directorio, vea el apartado *Cómo compartir directorios* del capítulo 7).

9. Pulse sobre el directorio compartido que desee y verá los archivos que se encuentra en él y podrá actuar con ellos en función de los permisos que tiene adjudicados.

NOTA. Si tiene problemas al compartir archivos o una impresora de una red, asegúrese de que *Firewall de Windows* no está bloqueando **Compartir archivos e impresoras**. Para ello, vea el apartado *Activar el compartir archivos en el Firewall de Windows*.

A través de un adaptador inalámbrico ad hoc

Este procedimiento va a permitir la interconexión de dos equipos a través de dos adaptadores inalámbricos.

Se da por supuesto que los ordenadores tienen instalados los adaptadores inalámbricos, ya que su instalación va a depender del fabricante o de si vienen instalados en la placa base del equipo.

Una vez instalados ambos adaptadores inalámbricos, lo primero que hay que hacer es crear una red inalámbrica ad hoc en un equipo para poderse conectar a ella desde el otro equipo. Para ello, siga los pasos siguientes:

En **Windows XP**:

1. Pulse con el botón derecho del ratón sobre **Mis sitios de red** (si no aparece en el Escritorio, se encuentra en el **menú Inicio**) y seleccione **Propiedades**.

2. En la ventana que se ha abierto (**Conexiones de red**), pulse con el botón derecho del ratón sobre **Conexiones de red inalámbricas** y seleccione **Propiedades**.

3. Pulse en la ficha **Redes inalámbricas** y le mostrará una pantalla parecida a la siguiente:

4. Pulse en **Agregar**, escriba el SSID que desee, mantenga **WEP** como **Cifrado de datos** (ya que es una red temporal), desactive la casilla **La clave la proporciono yo automáticamente**, indique la clave de red que desee poner (la deberá confirmar), active la casilla **Ésta es una red de equipo a equipo (ad hoc)**…, pulse en **Aceptar** dos veces y ya estará creada la nueva red inalámbrica ad hoc.

En **Windows Vista**:

1. Pulse con el botón derecho del ratón sobre **Red** (si no aparece en el Escritorio, se encuentra en el **menú Inicio**) y seleccione **Propiedades**.

2. En la ventana que se ha abierto (**Centro de redes y recursos compartidos**), pulse sobre **Conectarse a una red** y le mostrará las redes inalámbricas que hay creadas.

3. Para crear una red ad hoc, pulse en **Configurar una conexión o red** y le mostrará las opciones de conexión.

4. Seleccione **Configurar una red ad hoc inalámbrica (de equipo a equipo)** y pulse **Siguiente**.

5. Le mostrará una pantalla con información. Cuando la haya leído, pulse en **Siguiente**.

6. Indique el **Nombre de red** (**SSID**) que desee, deje **WEP** como **Tipo de seguridad** (ya que es una red temporal) y la clave de seguridad que desee. Cuando haya acabado, pulse en **Siguiente**.

7. Cuando haya terminado de crearla, le mostrará una nueva pantalla con información. Cuando la haya leído, pulse en **Cerrar** y ya estará creada la nueva red inalámbrica ad hoc.

Ahora queda preparar los dos ordenadores para la conexión. Para ello, siga los pasos siguientes:

En **Windows XP**:

1. Pulse con el botón derecho del ratón sobre **Mis sitios de red** (si no aparece en el Escritorio, se encuentra en el **menú Inicio**) y seleccione **Propiedades**.

2. En la ventana que se ha abierto (**Conexiones de red**), pulse con el botón derecho del ratón sobre **Conexiones de red inalámbricas** y seleccione **Propiedades**.

3. Está en la ficha **General** y verá que hay varios elementos instalados, entre ellos Cliente para redes Microsoft, Compartir impresoras y archivos para redes Microsoft y Protocolo Internet (TCP/IP). Fíjese que el cuadrado que hay a su izquierda está activado, ya que en caso contrario, dichos elementos estarían desactivados.

4. Para conectar dos equipos a través de un cable cruzado, no es necesario modificar las configuraciones que vienen por defecto a excepción de la dirección IP asignada de forma dinámica. Para poner una dirección IP estática, vea el apartado *Configuración TCP/IP estática para un equipo*.

5. Ahora se va a identificar cada uno de los equipos. Para ello, pulse **Mi PC** con el botón derecho del ratón, elija **Propiedades**, seleccione la pestaña **Nombre de equipo** y pulse en **Cambiar**.

6. Indique un nombre distinto para cada uno de los dos equipos y hágalos formar parte a los dos del mismo grupo de trabajo. Cuando haya finalizado, pulse en **Aceptar** dos veces y reinicie los equipos si así se le indica.

En **Windows Vista**:

1. Pulse con el botón derecho del ratón sobre **Red** (si no aparece en el Escritorio, se encuentra en el **menú Inicio**) y seleccione **Propiedades**.

2. En la ventana que se ha abierto (**Centro de redes y recursos compartidos**), pulse sobre **Administrar conexiones de red** (se encuentra en el panel izquierdo), pulse con el botón derecho del ratón sobre **Conexión de red inalámbrica** y seleccione **Propiedades**.

3. Si se lo indica, pulse **Continuar** para indicar que desea dar permiso para seguir con la operación. Verá que hay varios elementos instalados, entre ellos Cliente para redes Microsoft, Compartir impresoras y archivos para redes Microsoft, Protocolo Internet versión 4 (TCP/IPv4) y Protocolo Internet versión 6 (TCP/IPv6). Fíjese que el cuadrado que hay a su izquierda está marcado, ya que en caso contrario, dichos elementos estarían desactivados.

4. Para conectar dos equipos a través de un cable cruzado, no es necesario modificar las configuraciones que vienen por defecto a excepción de la dirección IP asignada de forma dinámica. Para poner una dirección IP estática, vea el apartado *Configuración TCP/IP estática para un equipo*.

5. Ahora se va a identificar cada uno de los equipos. Para ello, pulse **Equipo** con el botón derecho del ratón, elija **Propiedades**, pulse en **Cambiar la configuración** y pulse en **Continuar** para poder continuar con el proceso (si se lo pide).

6. Pulse en **Cambiar** e indique un nombre distinto para cada uno de los dos equipos y hágalos formar parte a los dos del mismo grupo de trabajo. Cuando haya finalizado, pulse en **Aceptar** dos veces y reinicie los equipos si así se le indica.

Ya queda únicamente, conectarse a la red inalámbrica que acabamos de crear y compartir los archivos. Para ello, siga los pasos siguientes:

En **Windows XP**:

1. Cuando se hayan reiniciado los equipos, desde el equipo en el que no se creó la red inalámbrica ad hoc, seleccione el icono **Mis sitios de red** y, después, **Ver redes inalámbricas disponibles** (se encuentra en el panel izquierdo).

2. Seleccione dicha red inalámbrica y pulse en **Conectar**.

3. Indique la clave de red que indicó anteriormente dos veces y pulse en **Aceptar**. Al cabo de un momento se habrá conectado a la red. Compruebe desde **Ver redes inalámbricas disponibles** de ambos equipos que están conectados por si no se hubiera realizado la conexión automática en el que creó la red inalámbrica.

4. Seleccione el icono **Mis sitios de red** y, después, **Ver equipos del grupo de trabajo** (se encuentra a la izquierda en **Tareas de red**).

5. Verá que se muestran los dos equipos (en caso de no ver un equipo que tiene Windows Vista, vea el apartado *Activar el uso compartido de archivos en Windows Vista*). Pulse sobre el otro equipo (recuerde que únicamente accederá directamente a dicho equipo si el usuario se encuentra dado de alta en ambos equipos y tiene la misma contraseña. En caso contrario, le mostrará una ventana para que indique el usuario y la contraseña con la que desea conectarse) y verá los directorios que

tiene compartidos (para ver cómo compartir un directorio, vea el apartado *Cómo compartir directorios* del capítulo 7).

6. Pulse sobre el directorio compartido que desee y verá los archivos que se encuentra en él y podrá actuar con ellos en función de los permisos que tiene adjudicados.

NOTA. Si tiene problemas al compartir archivos o una impresora de una red, asegúrese de que *Firewall de Windows* no está bloqueando **Compartir archivos e impresoras**. Para ello, vea el apartado *Activar el compartir archivos en el Firewall de Windows*.

En **Windows Vista**:

1. Pulse con el botón derecho del ratón sobre **Red** (si no aparece en el Escritorio, se encuentra en el **menú Inicio**) y seleccione **Propiedades**.

2. En la ventana que se ha abierto (**Centro de redes y recursos compartidos**), pulse sobre **Conectarse a una red** y le mostrará las redes inalámbricas que hay creadas.

3. Seleccione dicha red inalámbrica y pulse en **Conectar**.

4. Indique la clave de red que indicó anteriormente y pulse en **Aceptar**. Al cabo de un momento se habrá conectado a la red. Compruebe en la ventana **Centro de redes y recursos compartidos** de ambos equipos que están conectados por si no se hubiera realizado la conexión automática en el que creó la red inalámbrica.

5. Seleccione la opción **Red** del menú **Inicio** y verá que se muestran los dos equipos (en caso de no ver un equipo que tiene Windows Vista, vea el apartado *Activar el uso compartido de archivos en Windows Vista*). Pulse sobre el otro equipo (recuerde que únicamente accederá directamente a dicho equipo si el usuario se encuentra dado de alta en ambos equipos y tiene la misma contraseña. En caso contrario, le mostrará una ventana para que indique el usuario y la contraseña con la que desea conectarse) y verá los directorios que tiene compartidos (para ver cómo compartir un directorio, vea el apartado *Cómo compartir directorios* del capítulo 7).

6. Pulse sobre el directorio compartido que desee y verá los archivos que se encuentra en él y podrá actuar con ellos en función de los permisos que tiene adjudicados.

NOTA. Si tiene problemas al compartir archivos o una impresora de una red, asegúrese de que *Firewall de Windows* no está bloqueando **Compartir archivos e impresoras**. Para ello, vea el apartado *Activar el compartir archivos en el Firewall de Windows*.

COMUNICACIONES A TRAVÉS DE UNA RED (PARTE PRÁCTICA)

Activar la detección de redes en Windows Vista

La **detección de redes** es una configuración de red que:

- Determina si otros equipos y dispositivos de la red son *visibles* desde su equipo y si otros equipos de la red pueden *ver* su equipo.
- Determina si puede tener acceso a dispositivos y archivos compartidos de otros equipos de la red y si las personas que usan otros equipos de la red pueden tener acceso a los dispositivos y archivos compartidos de su equipo.
- Ayuda a proporcionar el nivel adecuado de seguridad y acceso a un equipo, basándose en la ubicación de las redes a las que se conecta.

Existen dos estados de detección de redes:

- **Activado**.
- **Desactivado**.

Cuando se conecta a una red, en función de la ubicación de red que elija, Windows asigna un estado de detección de redes a la red y abre los puertos de *Firewall de Windows* apropiados. Por tanto, se pueden dar varios problemas:

- No se ve ningún equipo ni dispositivo en la carpeta **Red**. Esto puede producirse por dos motivos:
    - **El equipo no está conectado a la red**. En este caso, pulse en **Conectarse a una red** y seleccione la red que desee.
    - **La detección de redes le impide ver otros equipos y dispositivos**. Compruebe si la opción de detección de redes del equipo está desactivada desde el **Centro de redes y recursos compartidos**.

      Si está desactivada la detección de redes, pulse en el botón de flecha para expandir la sección, pulse en **Activar la detección de redes** y, después, pulse en **Aplicar** (si le solicita una contraseña de administrador o una confirmación, escriba la contraseña o proporcione la confirmación).
- No se ve un equipo o dispositivo que debería verse en la carpeta **Red**. Esto se puede producir por dos motivos:
    - **El equipo o dispositivo no está en la red**. Para resolver este problema, agregue el equipo a la red conectándolo al concentrador o conmutador, o mediante el asistente para conectarse a una red (si la red es inalámbrica).
    - **La configuración de detección de redes del equipo que no se ve está desactivada**. Para cambiar la configuración de detección de redes en otro equipo, inicie sesión en él y pulse en el menú **Inicio**, en **Panel de control** y en **Centro de redes y de recursos compartidos**. Pulse en el botón de flecha para expandir la sección **Detección de redes**, pulse en **Activar la detección de redes** y, después, pulse en **Aplicar**.

NOTA. Puede tardar varios minutos hasta que los equipos con versiones anteriores de Windows se detecten y puedan verse en la carpeta **Red**.

Normalmente, tarda en verse un equipo que ejecuta Windows Vista desde un equipo que ejecuta Windows XP.

Cuando se accede a la carpeta **Red** y está desactivada la detección de redes, se indica en la parte superior de la pantalla, pudiéndose activar desde ese lugar.

Activar el uso compartido de archivos en Windows Vista

Se pueden compartir archivos en Windows Vista de dos maneras:

- **Desde cualquier carpeta del equipo**. Con este método de compartir archivos, puede decidir quién podrá realizar cambios en los archivos que comparte y qué tipo de cambios (de haber alguno) pueden realizarse en los mismos. Puede hacerlo estableciendo permisos de uso compartido que se pueden conceder a un individuo o a un grupo de usuarios de la misma red.

- **Desde la carpeta pública del equipo**. Con este método de compartir archivos, puede copiar o mover archivos a la carpeta pública y se comparten desde dicha ubicación. Si activa el uso compartido de archivos para la carpeta pública, cualquiera con una cuenta de usuario y una contraseña en el equipo, así como *Todos* en la red, podrán ver todos los archivos de la carpeta pública y sus subcarpetas. No se puede limitar a las personas para que sólo vean algunos archivos de la carpeta pública. Sin embargo, pueden establecerse permisos que limiten a las personas el acceso a la carpeta pública o que les limiten el cambio de archivos o la creación de nuevos.

  También se puede activar el uso compartido protegiéndole con contraseña. De esta manera, limitará el acceso a la carpeta pública a las personas con una cuenta de usuario y contraseña en el equipo. De manera predeterminada, el acceso de red a la carpeta pública está desactivado a menos que lo habilite.

Para habilitar el uso compartido de archivos e impresoras en un equipo con Windows Vista, asegúrese de que la detección de redes y el uso compartido de impresoras están activados siguiendo estos pasos:

1. Abra el **Centro de redes y recursos compartidos** desde el **Panel de control.**

2. Si la detección de redes está desactivada, pulse en el botón de flecha para expandir la sección, pulse en **Activar la detección de redes** y, a continuación, pulse en **Aplicar** (si le solicita una contraseña de administrador o una confirmación, escriba la contraseña o proporcione la confirmación).

3. Si el uso compartido de archivos está desactivado, pulse en el botón de flecha para expandir la sección, pulse en **Activar el uso compartido de archivos** y, a continuación, pulse en **Aplicar** (si le solicita una contraseña de administrador o una confirmación, escriba la contraseña o proporcione la confirmación).

4. Si el uso compartido de impresoras está desactivado, pulse en el botón de flecha para expandir la sección, pulse en **Activar compartir impresora** y, a continuación, pulse en **Aplicar** (si le solicita una contraseña de administrador o una confirmación, escriba la contraseña o proporcione la confirmación).

5. Si todavía tiene problemas al compartir archivos o una impresora de una red, asegúrese de que *Firewall de Windows* no está bloqueando **Compartir archivos e impresoras**. Para ello, vea el apartado *Activar el compartir archivos en el Firewall de Windows*.

Activar el compartir archivos en el Firewall de Windows

Si tiene problemas al compartir archivos o una impresora de una red, compruebe que el *Firewall de Windows* no está bloqueando **Compartir archivos e impresoras**. Para ello, siga los pasos siguientes:

1. Abra el **Firewall de Windows** desde el **Panel de control**.

2. Pulse en **Permitir un programa a través de Firewall de Windows** (se encuentra en el panel izquierdo) y, si le solicita una contraseña de administrador o una confirmación, escriba la contraseña o proporcione la confirmación.

3. En la lista **Programa o puerto**, asegúrese de que la casilla **Compartir archivos e impresoras** está activada y, a continuación, pulse en **Aceptar**.

Montaje y configuración de una red con un switch

Para montar una red con varios ordenadores utilizando un conmutador, únicamente es necesario disponer de:

- Los ordenadores que se deseen utilizar teniendo cada uno de ellos una tarjeta de red correctamente instalada y configurada (para ver cómo hacerlo, vaya al apartado *Instalación de un adaptador de red* del capítulo 2).

- Un conmutador o switch que tenga suficientes puertas para los ordenadores que se deseen conectar. En caso de querer conectar más ordenadores que puertas tenga el switch, se podrán poner varios en cascada, uniéndolos con un cable normal (si los conmutadores son modernos) o con un cable cruzado si son antiguos y poseen un puerto UPLINK.

- Un cable RJ45 por ordenador (en caso de haber más de un switch, hará falta un cable más por switch que exceda de uno).

Una vez se disponga de todo el material, únicamente será necesario conectar cada ordenador con el switch mediante un cable RJ45 y ya estará preparada la red local.

Ahora habrá que configurar cada ordenador para que funcionen en red (para ver cómo hacerlo, vaya al apartado *Conexión de un equipo a un conmutador/concentrador*). Normalmente, los conmutadores no precisan ser configurados. No obstante, hay conmutadores avanzados que pueden ser configurador para montar una VLAN o llevar a cabo tareas estadísticas (en este libro no se mostrará cómo configurar un conmutador, ya que no son tareas básicas para montar una red).

Para tener acceso a Internet, habrá que instalar un router ADSL al switch, para ver cómo configurarlo vea el apartado *Configuración de un router ADSL* del capítulo 4).

Conexión de un equipo a un conmutador/concentrador

Para configurar un equipo conectado a un conmutador/concentrador para que funcione en red, siga los pasos siguientes:

En **Windows XP** o **Server 2003**:

1. Pulse con el botón derecho del ratón sobre **Mis sitios de red** (si no aparece en el Escritorio, se encuentra en el **menú Inicio**) y seleccione **Propiedades**.

2. En la ventana que se ha abierto (**Conexiones de red**), pulse con el botón derecho del ratón sobre **Conexión de área local** y seleccione **Propiedades**.

3. Verá que hay varios elementos instalados, entre ellos Cliente para redes Microsoft, Compartir impresoras y archivos para redes Microsoft y Protocolo Internet (TCP/IP). Fíjese que el cuadrado que hay a su izquierda está activado, ya que en caso contrario, dichos elementos estarían desactivados.

4. Para conectar un equipo a un conmutador/concentrador, no es necesario modificar las configuraciones que vienen por defecto a excepción de la dirección IP asignada de forma dinámica (si no se cuenta con un servidor DHCP que la proporcione). Para poner una dirección IP estática, vea el apartado *Conexión de un equipo a través de un cable RJ45*. Para configurar un servidor DHCP, vaya al apartado correspondiente del capítulo 6.

5. Ahora se va a identificar cada uno de los equipos. Para ello, pulse **Mi PC** con el botón derecho del ratón, elija **Propiedades**, seleccione la pestaña **Nombre de equipo** y pulse en **Cambiar**.

6. Indique un nombre distinto para cada uno de los equipos conectados a la red y hágalos formar parte del mismo grupo de trabajo (si desea unir un ordenador a un dominio, vea el apartado *Cómo unir un ordenador a un dominio* del capítulo 6). Cuando haya finalizado, pulse en **Aceptar** dos veces y reinicie los equipos si así se le indica.

7. Cuando se hayan reiniciado, seleccione el icono **Mis sitios de red** y, después, **Ver equipos del grupo de trabajo** (se encuentra a la izquierda en **Tareas de red)**.

8. Verá que se muestran los equipos (en caso de no ver un equipo que tiene Windows Vista, vea el apartado *Activar el uso compartido de archivos en Windows Vista*). Pulse sobre otro equipo (recuerde que únicamente accederá directamente a dicho equipo si el usuario se encuentra dado de alta en ambos equipos y tiene la misma contraseña. En caso contrario, le mostrará una ventana para que indique el usuario y la contraseña con la que desea conectarse) y verá los directorios que tiene compartidos (para ver cómo compartir un directorio, vea el apartado *Cómo compartir directorios* del capítulo 7).

9. Pulse sobre el directorio compartido que desee y verá los archivos que se encuentra en él y podrá actuar con ellos en función de los permisos que tiene adjudicados.

NOTA. Si tiene problemas al compartir archivos o una impresora de una red, asegúrese de que *Firewall de Windows* no está bloqueando **Compartir archivos e impresoras**. Para ello, vea el apartado *Activar el compartir archivos en el Firewall de Windows*.

En **Windows Vista**:

1. Pulse con el botón derecho del ratón sobre **Red** (si no aparece en el Escritorio, se encuentra en el **menú Inicio**) y seleccione **Propiedades**.

2. En la ventana que se ha abierto (**Centro de redes y recursos compartidos**), pulse sobre **Administrar conexiones de red** (se encuentra en el panel izquierdo), pulse con el botón derecho del ratón sobre **Conexión de área local** y seleccione **Propiedades**.

3. Si se lo indica, pulse **Continuar** para indicar que desea dar permiso para seguir con la operación. Verá que hay varios elementos instalados, entre ellos Cliente para redes Microsoft, Compartir impresoras y archivos para redes Microsoft, Protocolo Internet versión 4 (TCP/IPv4) y Protocolo Internet versión 6 (TCP/IPv6). Fíjese que el cuadrado que hay a su izquierda está marcado, ya que en caso contrario, dichos elementos estarían desactivados.

4. Para conectar un equipo a un conmutador/concentrador, no es necesario modificar las configuraciones que vienen por defecto a excepción de la dirección IP asignada de forma dinámica (si no se cuenta con un servidor DHCP que la proporcione). Para poner una dirección IP estática, vea el apartado *Conexión de un equipo a través de un cable RJ45*. Para configurar un servidor DHCP, vaya al apartado correspondiente del capítulo 6.

5. Ahora se va a identificar cada uno de los equipos. Para ello, pulse **Equipo** con el botón derecho del ratón, elija **Propiedades**, pulse en **Cambiar la configuración** y pulse en **Continuar** para poder continuar con el proceso (si se lo pide).

6. Pulse en **Cambiar** e indique un nombre distinto para cada uno de los equipos conectados a la red y hágalos formar parte del mismo grupo de trabajo (si desea unir un ordenador a un dominio, vea el apartado *Cómo unir un ordenador a un dominio* del capítulo 6). Cuando haya finalizado, pulse en **Aceptar** dos veces y reinicie los equipos si así se le indica.

7. Cuando se hayan reiniciado, seleccione la opción **Red** del menú **Inicio** y verá que se muestran los equipos (en caso de no ver los equipos, vea el apartado *Activar la detección de redes en Windows Vista*). Pulse sobre otro equipo (recuerde que únicamente accederá directamente a dicho equipo si el usuario se encuentra dado de alta en ambos equipos y tiene la misma contraseña. En caso contrario, le mostrará una ventana para que indique el usuario y la contraseña con la que desea conectarse) y verá los directorios que tiene compartidos (para ver cómo compartir un directorio, vea el apartado *Cómo compartir directorios* del capítulo 7).

8. Pulse sobre el directorio compartido que desee y verá los archivos que se encuentra en él y podrá actuar con ellos en función de los permisos que tiene adjudicados.

NOTA. Si tiene problemas al compartir archivos o una impresora de una red, asegúrese de que *Firewall de Windows* no está bloqueando **Compartir archivos e impresoras**. Para ello, vea el apartado *Activar el compartir archivos en el Firewall de Windows*.

Configuración TCP/IP estática para un equipo

Para configurar el protocolo **TCP/IP** de forma estática (es decir, para asignar al equipo una dirección IP fija), siga los pasos siguientes:

En **Windows XP** o **Server 2003**:

1. Pulse con el botón derecho del ratón sobre **Mis sitios de red** (si no aparece en el Escritorio, se encuentra en el **menú Inicio**) y seleccione **Propiedades**.

2. En la ventana que se ha abierto (**Conexiones de red**), pulse con el botón derecho del ratón sobre **Conexión de área local** (si es para un adaptador de red) o **Conexiones de red inalámbricas** (si es para un adaptador inalámbrico) y seleccione **Propiedades**.

3. En la pantalla que le muestra, seleccione **Protocolo Internet (TCP/IP)** y pulse en **Propiedades**.

4. Le mostrará una pantalla parecida a la siguiente:

En ella se encuentran las opciones siguientes:

- **Obtener una dirección IP automáticamente**. Si activa esta casilla es porque dispone de un servidor DHCP que le va a dar una dirección IP para trabajar en la red.

- **Usar la siguiente dirección IP**. Si activa esta casilla es porque desea indicar una dirección IP fija para el equipo. Tendrá que indicar los datos siguientes:

  - **Dirección IP**. En ella se ha de indicar la **dirección IP** asignada al equipo (no deberá estar utilizada en ningún otro equipo ya que daría errores al no poder estar duplicada). En el ejemplo, se trata de una red de tipo **C**, la dirección del ordenador es 192.168.0.7.

  - **Máscara de subred**. Automáticamente el sistema le dirá la máscara de subred que le corresponde (en el ejemplo, es 255.255.255.0). Este valor no deberá cambiarlo a no ser que haya realizado una segmentación de la red.

- **Puerta de enlace predeterminada**. Cuando la red se comunica con el exterior con otras redes o con Internet, es necesario utilizar encaminador o un **router** (se explicará lo que es en el capítulo siguiente). En este apartado se ha de indicar la dirección IP privada del router. En caso de no poner ninguna dirección o de no disponer de router, el equipo no tendría salida a Internet.

- **Obtener la dirección del servidor DNS automáticamente**. Si activa esta casilla es porque dispone de un servidor DHCP que le va a indicar las direcciones IP de los servidores DNS que realizan la traducción de direcciones.

- **Usar las siguientes direcciones de servidor DNS**. Si activa esta casilla es porque desea indicar una o dos direcciones IP fijas para los servidores DNS que realizan la traducción de direcciones. En este caso, tendrá que indicar las direcciones IP de dichos servidores.

- **Opciones avanzadas**. Permite realizar modificaciones en los datos que acaba de indicar. Normalmente, no es necesario utilizar estas opciones, a no ser que desee indicar más de una dirección IP para el equipo o más de dos servidores DNS.

5. Para terminar la configuración del protocolo **TCP/IP**, pulse **Aceptar** varias veces hasta que se cierren las ventanas que ha abierto.

En **Windows Vista**:

1. Pulse con el botón derecho del ratón sobre **Red** (si no aparece en el Escritorio, se encuentra en el **menú Inicio**) y seleccione **Propiedades**.

2. En la ventana que se ha abierto (**Centro de redes y recursos compartidos**), pulse sobre **Administrar conexiones de red** (se encuentra en el panel izquierdo), pulse con el botón derecho del ratón sobre **Conexión de área local** y seleccione **Propiedades**.

3. Si se lo indica, pulse **Continuar** para indicar que desea dar permiso para seguir con la operación. Verá que hay varios elementos instalados, entre ellos Cliente para redes Microsoft, Compartir impresoras y archivos para redes Microsoft, Protocolo Internet versión 4 (TCP/IPv4) y Protocolo Internet versión 6 (TCP/IPv6). Fíjese que el cuadrado que hay a su izquierda está marcado, ya que en caso contrario, dichos elementos estarían desactivados.

6. En la pantalla que le muestra, seleccione **Protocolo Internet versión 4 (TCP/IPv4)** y pulse en **Propiedades**.

7. Le mostrará una pantalla parecida a la siguiente:

En ella se encuentran las opciones siguientes:

- **Obtener una dirección IP automáticamente**. Si activa esta casilla es porque dispone de un servidor DHCP que le va a dar una dirección IP para trabajar en la red.

- **Usar la siguiente dirección IP**. Si activa esta casilla es porque desea indicar una dirección IP fija para el equipo. Tendrá que indicar los datos siguientes:

  - **Dirección IP**. En ella se ha de indicar la **dirección IP** asignada al equipo (no deberá estar utilizada en ningún otro equipo ya que daría errores al no poder estar duplicada). En el ejemplo, se trata de una red de tipo **C**, la dirección del ordenador es 192.168.0.111.

  - **Máscara de subred**. Automáticamente el sistema le dirá la máscara de subred que le corresponde (en el ejemplo, es 255.255.255.0). Este valor no deberá cambiarlo a no ser que haya realizado una segmentación de la red.

  - **Puerta de enlace predeterminada**. Cuando la red se comunica con el exterior con otras redes o con Internet, es necesario utilizar encaminador o un **router** (se explicará lo

que es en el capítulo siguiente). En este apartado se ha de indicar la dirección IP privada del router. En caso de no poner ninguna dirección o de no disponer de router, el equipo no tendría salida a Internet.

- **Obtener la dirección del servidor DNS automáticamente**. Si activa esta casilla es porque dispone de un servidor DHCP que le va a indicar las direcciones IP de los servidores DNS que realizan la traducción de direcciones.

- **Usar las siguientes direcciones de servidor DNS**. Si activa esta casilla es porque desea indicar una o dos direcciones IP fijas para los servidores DNS que realizan la traducción de direcciones. En este caso, tendrá que indicar las direcciones IP de dichos servidores.

- **Opciones avanzadas**. Permite realizar modificaciones en los datos que acaba de indicar. Normalmente, no es necesario utilizar estas opciones, a no ser que desee indicar más de una dirección IP para el equipo o más de dos servidores DNS.

8. Para terminar la configuración del protocolo **TCP/IPv4**, pulse **Aceptar** varias veces hasta que se cierren las ventanas que ha abierto.

En principio no es necesario configurar el protocolo TCP/IP versión 6 a no ser que vaya a instalar un controlador de dominio. Por si fuera necesario, siga los pasos siguientes para instalarlo:

1. Desde la pantalla **Propiedades de Conexión de área local**, seleccione **Protocolo Internet versión 6 (TCP/IPv6)** y pulse en **Propiedades**.

2. Le mostrará una pantalla parecida a la siguiente:

En ella se encuentran las opciones siguientes:

- **Obtener una dirección IPv6 automáticamente**. Si activa esta casilla es porque dispone de un servidor DHCP que le va a dar una dirección IP para trabajar en la red.

- **Usar la siguiente dirección IP**. Si activa esta casilla es porque desea indicar una dirección IP fija para el equipo. Tendrá que indicar los datos siguientes (para ver como se indica una dirección IP para este protocolo, vea el apartado *Direccionamiento IPv6* del capítulo dos):

    - **Dirección IPv6**. En ella se ha de indicar la **dirección IPv6** asignada al equipo (no deberá estar utilizada en ningún otro equipo ya que daría errores al no poder estar duplicada).

    - **Longitud del prefijo de subred**. Es el valor que indica cuántos bits contiguos de la parte izquierda de la dirección componen el prefijo de subred.

    - **Puerta de enlace predeterminada**. Cuando la red se comunica con el exterior con otras redes o con Internet, es necesario utilizar encaminador o un **router** (se explicará lo que es en el capítulo siguiente). En este apartado se ha de indicar la dirección IP privada del router. En caso de no poner ninguna dirección o de no disponer de router, el equipo no tendría salida a Internet.

- **Obtener la dirección del servidor DNS automáticamente**. Si activa esta casilla es porque dispone de un servidor DHCP que le va a indicar las direcciones IP de los servidores DNS que realizan la traducción de direcciones.

- **Usar las siguientes direcciones de servidor DNS**. Si activa esta casilla es porque desea indicar una o dos direcciones IP fijas para los servidores DNS que realizan la traducción de direcciones. En este caso, tendrá que indicar las direcciones IP de dichos servidores.

- **Opciones avanzadas**. Permite realizar modificaciones en los datos que acaba de indicar. Normalmente, no es necesario utilizar estas opciones, a no ser que desee indicar más de una dirección IP para el equipo o más de dos servidores DNS.

9. Para terminar la configuración del protocolo **TCP/IPv6**, pulse **Aceptar** varias veces hasta que se cierren las ventanas que ha abierto.

Configuración de un punto de acceso

Si se quiere instalar una red inalámbrica básica se necesitan generalmente dos dispositivos: un punto de acceso (AP) y un equipo con un adaptador de red inalámbrico. En este punto, nos vamos a centrar solamente en lo referente al punto de acceso (en el capítulo 2 se indicó cómo instalar un adaptador inalámbrico).

Se han de realizar las siguientes operaciones:

a. Instalación del punto de acceso.

b. Conexión física del punto de acceso a la red local existente.

c. Configuración del punto de acceso.

DESCRIPCIÓN DEL PUNTO DE ACCESO

La figura siguiente muestra los indicadores LED del punto de acceso.

Dichos indicadores son los siguientes:

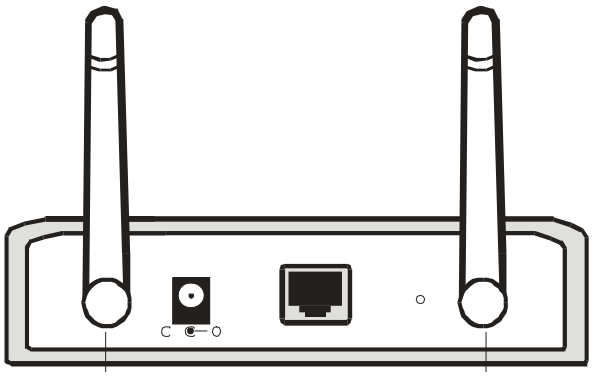
- **Power**. Este indicador se pone verde cuando el punto de acceso se conecta al enchufe, de lo contrario, se apaga.

- **LAN**. Este indicador se pone verde cuando el puerto LAN está conectado a una Ethernet de 100 Mbps y amarillo si es de 10 Mbps. El indicador parpadea mientras se transmite o recibe datos de la red Ethernet.

- **WLAN**. El indicador se pone verde cuando está activa la WLAN y parpadea mientras está recibiendo o enviando paquetes inalámbricos.

Panel posterior

La siguiente figura muestra el panel posterior del punto de acceso:



- **Ethernet**. Es el puerto de enlace Ethernet 10/100 Mbps a través de un conector RJ45. Se ha de conectar al switch/hub.

- **Reset**. Es el lugar en donde se restablece la configuración predeterminada de fábrica, una vez que se pulsa este botón durante 10 segundos, el LED de la WLAN se apagará y, cuando el punto de acceso esté listo, dicho LED comenzará a parpadear.

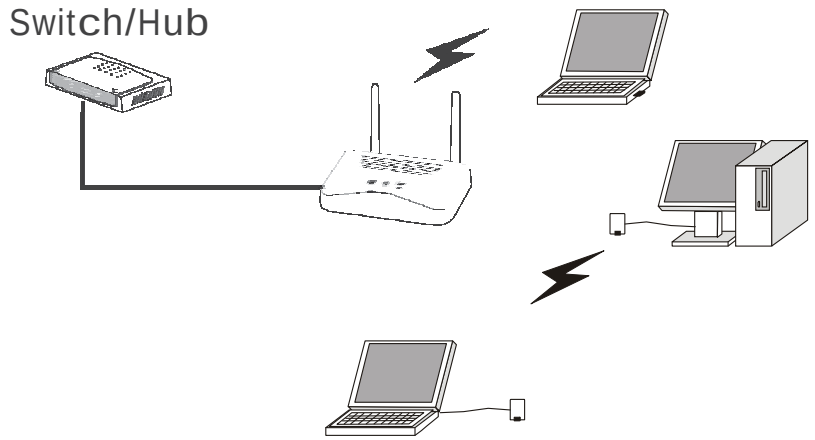
  Si el punto de acceso se ha bloqueado en su configuración, pulse y suelte este botón para liberarlo.

- **DC Power**. Permite conectar el adaptador de energía DC al enchufe de corriente.

- **Antenas**. Son las que permiten la conexión con los equipos inalámbricos. Las que vienen de fábrica se pueden sustituir por otras con más sensibilidad y que permiten transmitir a mayor distancia. En caso de desear conectarlo a una antena exterior, hágalo en la antena indicada en el manual.

CONEXIÓN DEL PUNTO DE ACCESO

El esquema de la conexión del punto de acceso es el que se muestra en la figura siguiente:



Proceda de la manera siguiente:

1. Enchufe un extremo de un cable de red RJ45 normal a un puerto del switch/hub.

2. Conecte el otro extremo de dicho cable de red RJ45 a la conexión trasera correspondiente del punto de acceso.

3. Conecte a la corriente eléctrica el punto de acceso y compruebe los LED para comprobar su situación:

    - Al cabo de un momento, los LED LAN y WLAN se iluminarán indicando que el estado del punto de acceso es normal.

    - Si el indicador LAN no se enciende compruebe que el cable RJ-45 está bien conectado tanto en el punto de acceso como en el switch/hub. Si está bien conectado, puede haber un problema con el cable, pruebe a sustituirlo. Si sigue sin funcionar, pulse y suelte el botón de reset para desbloquearlo. Si sigue sin funcionar, puede ser que el punto de acceso esté mal o el puerto del switch7hub en donde está conectado el cable.

CONFIGURACIÓN DEL PUNTO DE ACCESO

El punto de acceso dispone de una interfaz Web que permite su configuración antes de proceder a conectarlo a la red inalámbrica.

Para proceder a su configuración, siga los pasos siguientes:

1. A través de un explorador Web, escriba como URL la dirección IP del punto de acceso que viene configurada por defecto (deberá consultar el manual para averiguarlo. En el ejemplo, viene con la 192.168.0.100). Tenga en cuenta que el equipo desde el que se vaya a realizar la configuración deberá tener una dirección IP en el mismo rango, ya que, en caso contrario, no se podrá conectar (para poner una dirección IP estática, vea el apartado *Conexión de un equipo a través de un cable RJ45*).

2. Le mostrará una pantalla en la que deberá indicar el usuario y la contraseña que tiene por defecto (para averiguarlo, consulte el manual).

3. Le mostrará una pantalla con un resumen de la configuración actual del punto de acceso:

En la parte izquierda, se muestran seis grupos con las funciones de configuración:

Network

En este grupo se encuentran los apartados siguientes:

¬

- **LAN setup**. Permite configurar el direccionamiento IP del punto de acceso:

    - **DHCP**. Si activa esta casilla, estará indicando que el punto de acceso tendrá una dirección IP dinámica (no es recomendable).
    - **Static IP**. Si activa esta casilla, deberá indicar la dirección IP, la máscara de subred y la puerta de enlace predeterminada (es la dirección del router).

  Si realiza algún cambio, recuerde pulsar en **Apply** (Aplicar) para que se guarde.

- **Wireless settings**. En este apartado le mostrará la pantalla siguiente:

  En ella se encuentra los apartados:

  - **Regulatory Domain (Radio settings)**. Pulse en **change región** y aparecerá una ventana para que seleccione el país en el que está utilizando este dispositivo inalámbrico (los usuarios son responsables de garantizar que el canal conjunto de configuración cumpla las normas reguladoras de estos países).

  - **SSID (Wireless LAN)**. Permite indicar el nombre de la red inalámbrica que es una cadena ASCII de hasta 32 caracteres. Este nombre deberá ser el mismo en todas las estaciones y se utiliza para impedir la unión involuntaria de personas.

- **Band**. Permite seleccionar la banda de radio que se va a utilizar. En el ejemplo, se puede seleccionar entre modo mixto, sólo 802.11g o sólo 802.11b.

- **Radio Channel**. Permite seleccionar el canal que se va a utilizar para comunicarse (difieren del país que se seleccionó anteriormente).

- **Broadcast SSID**. Al activar esta casilla, está indicando que el punto de acceso emita el SSID a las estaciones (si está desactivada, las estaciones deberán saber el SSID con antelación).

Si realiza algún cambio, recuerde pulsar en **Apply** (Aplicar) para que se guarde.

- **WDS Links**. **WDS** (**Wireless Distribution System**) utiliza los medios de comunicación inalámbrica para comunicarse con otros puntos de acceso. Al entrar en la pantalla de WDS, verá una lista de puntos de acceso. Pulse en la casilla **Enable** para habilitar dicha comunicación y poder utilizar un punto de acceso repetidor.

  Si realiza algún cambio, recuerde pulsar en **Apply** (Aplicar) para que se guarde.

Security

Este grupo se utiliza para proteger las comunicaciones inalámbricas de escuchas ilegales y, de forma secundaria, prevenir el acceso no autorizado a una red inalámbrica.

Al entrar en **Wireless security** verá la pantalla siguiente:

En ella se encuentran los apartados:

- **Access Control List (ACL)**. Si pulsa esta opción, verá la pantalla siguiente:

Si se activa la casilla **Enable access control list**, permitirá a los clientes cuyas direcciones MAC se encuentren en lista inferior realizar la función contraria a la establecida por defecto.

En **Defaul Access** se puede indicar lo que se hará por defecto con los clientes que no se encuentren en la lista inferior: **Accept** (Aceptar) o **Reject** (Rechazar).

Si pulsa en **Add**, podrá añadir direcciones MAC a la lista inferior y , si pulsa en **Delete**, podrá quitar la dirección MAC que seleccione.

Si realiza algún cambio, recuerde pulsar en **Apply** (Aplicar) para que se guarde.

- **RADIUS Servers**. Un servidor *RADIUS* (*Remote Dial-autenticación de usuario de servicios*) se utiliza para autenticar la conexión de los clientes a la red inalámbrica utilizando TKIP, AES o WEP.

En **Reauthentication Time** se puede indicar los segundos en los que desea que se reautentifique el cliente.

Si pulsa en **Add**, le mostrará una pantalla para que indique la dirección IP del servidor Radius, el puerto UDP y el secreto (es la clave que se utilizará entre el punto de acceso y el servidor Radius).

Si realiza algún cambio, recuerde pulsar en **Apply** (Aplicar) para que se guarde.

- **Wired Equivalent Privacy (WEP)**. La encriptación WEP no fue puesta en práctica con la norma 802.11. Además, WEP no es completamente seguro, ya que en un paquete de datos la dirección MAC no está cifrada y los hackers pueden utilizarla para penetrar en una red falsificando la dirección MAC.

  Para elegir el cifrado WEP, active la casilla **Use WEP security** e indique si desea utilizar:

  - **64 bits**. Si selecciona esta opción, tendrá que escribir 10 valores en el rango (0-F, hexadecimal) que será la clave a utilizar por los clientes para conectarse al punto de acceso.
  - **128-bits**. Si selecciona esta opción, tendrá que escribir 26 valores en el rango (0-F, hexadecimal) que será la clave a utilizar por los clientes para conectarse al punto de acceso.

  Si realiza algún cambio, recuerde pulsar en **Apply** (Aplicar) para que se guarde.

- **802.1x Security**. Para hacer frente a las deficiencias de WEP, la industria está trabajando en soluciones basadas en la especificación 802.1x, que se basa en el **protocolo de autenticación extensible** (**EAP**). Esta opción requiere disponer de un servidor RADIUS.

  Para elegir esta opción, active la casilla **Use 802.1x security** e indique si desea utilizar 64 ó 128 bits para el tamaño de la clave de la seguridad 802.1x.

  También deberá indicar:

  - **No Rekeying**. Si activa esta casilla, los clientes no tendrán que volver a indicar la clave para autenticarse con el servidor Radius.
  - El tiempo que ha de pasar para que los clientes se vuelvan a autentificar.
  - El número de paquetes que han de transmitirse para que los clientes se vuelvan a autentificar.

  Si realiza algún cambio, recuerde pulsar en **Apply** (Aplicar) para que se guarde.

- **Wi-Fi Protected Access (WPA). WPA** es el más moderno y mejor sistema de seguridad Wi-Fi. Hay dos modos disponibles:

    - **Pre-Shared Key**. Le da la opción de dos métodos de encriptación: **TKIP** (**Temporal Key Integrity Protocol**) que utiliza un método de encriptación más fuerte e incorpora **Mensaje Integridad Código** (**MIC**) para proporcionar protección contra hackers.
    - **AES** (**Advanced Encryption System**), que utiliza un bloque simétrico de 128 bits de cifrado de datos.

    - Si activa la casilla **Disable WPA security**, estará indicando que no quiere utilizar esta encriptación.

    - Si activa la casilla **Use WPA with pre-shared key**, tendrá que escribir entre 8 y 63 caracteres que serán la clave a utilizar por los clientes para conectarse al punto de acceso.

    - Si activa la casilla **Use WPA with Radius server**, estará indicando que la autenticación entre el servidor Radius, el punto de acceso y los clientes se hará utilizando una **Group Key Rekey**. Esta opción requiere disponer de un servidor RADIUS

      También deberá indicar:

        - **No Rekeying**. Si activa esta casilla, los clientes no tendrán que volver a indicar la clave para autenticarse con el servidor Radius.
        - El tiempo que ha de pasar para que los clientes se vuelvan a autentificar.
        - El número de paquetes que han de transmitirse para que los clientes se vuelvan a autentificar.
        - **Update Group Key…** Si activa esta casilla, estará indicando que se debe actualizar la clave cuando la estación o el cliente dejen el *Grupo de Redes* (*BSS*, *Basic Service Set*).

    Si realiza algún cambio, recuerde pulsar en **Apply** (Aplicar) para que se guarde.

- **Status**. En este grupo se mostrará un resumen de la configuración de la estación (es el informe que muestra al conectarse estadísticas de las conexiones inalámbricas e informes de los sucesos ocurridos en el punto de acceso).

- **Clients**. Este grupo muestra la lista de los clientes que se han conectado al punto de acceso y la lista de los puntos de acceso que se pueden conectar con este punto de acceso (es la lista que se puede utilizar para enlaces *WDS* explicados anteriormente).

- **Tools**. Esta opción le ayudará a actualizar el firmware del punto de acceso.

- **Configuration**. Esta opción le ayudará a modificar la contraseña del punto de acceso y, también, a bloquear el punto de acceso para evitar cambios en su configuración (para desbloquearlo, deberá pulsar el botón **Reset** del panel posterior del punto de acceso).

Una vez realizados todos los cambios necesarios en la configuración del punto de acceso, ya estará preparado para que los clientes lo utilicen. Para ello, continúe con el apartado *Montaje y configuración de una red inalámbrica*.

Montaje y configuración de una red inalámbrica

Una vez que el punto de acceso inalámbrico está instalado y configurado se puede proceder a conectarle los equipos para montar la red inalámbrica.

Para ello, todos los equipos que se deseen conectar a dicha red inalámbrica deberán disponer de adaptadores de red inalámbricos perfectamente instalados (para ver cómo hacerlo, vea el apartado *Instalación de un adaptador inalámbrico* del capítulo 2).

También deberá estar preparado el direccionamiento IP que podrá ser dinámico (si se dispone de un servidor DHCP. Para configurar un servidor DHCP, vaya al apartado correspondiente del capítulo 6) o estático (si no se dispone de servidor DHCP. En este caso, vea el apartado *Configuración TCP/IP estática para un equipo*).

Ahora, se va a proceder a configurar uno de los equipos para conectarlo a la red inalámbrica. Para ello, siga los pasos siguientes (se supone que el punto de acceso está totalmente operativo y el equipo tiene el direccionamiento IP correcto y en el mismo rango que el punto de acceso):

En **Windows XP**:

1. Desde el equipo que desea unir a la red inalámbrica, pulse en el icono

   Conexiones de red inalámbricas que se encuentra a la derecha de la Barra de tareas.

2. Le mostrará todos los puntos de acceso con los que ha contactado. Seleccione el SSID correspondiente a su punto de acceso y pulse en **Conectar**.

3. Indique la clave de red que puso en la configuración del punto de acceso (que deberá repetir), pulse en **Conectar** y, al cabo de un momento, le indicará que está conectado al punto de acceso.

4. Cierre la ventana **Conexiones de red inalámbricas** y verá que en su icono ha desaparecido el aspa roja.

5. Ya puede ver los equipos de su grupo de trabajo y compartir archivos e impresoras con ellos tal y como se explicó anteriormente (para obtener más información, vea el apartado *Conexión de un equipo a un conmutador/concentrador*).

6. A partir de este momento, cada vez que reinicie el equipo, se establecerá una conexión automática con el punto de acceso (si no desea que sea así, pulse en **Desconectar** de la lista de redes inalámbricas antes de apagar el equipo).

Para ver la configuración que ha tomado el adaptador inalámbrico (que será la que tenía el punto de acceso), siga los pasos siguientes:

1. Pulse con el botón derecho del ratón sobre **Mis sitios de red** (si no aparece en el Escritorio, se encuentra en el **menú Inicio**) y seleccione **Propiedades**.

2. En la ventana que se ha abierto (**Conexiones de red**), pulse con el botón derecho del ratón sobre **Conexiones de red inalámbricas** y seleccione **Propiedades**.

3. Pulse sobre la ficha **Redes inalámbricas** y, en **Redes preferidas**, seleccione el SSID correspondiente a su punto de acceso.

4. Después, pulse en **Propiedades** y verá una pantalla parecida a la siguiente:

En ella verá los siguientes apartados:

- **Nombre de red (SSID)**. Es el SSID que indicó en la configuración del punto de acceso.
- **Autenticación de red**. Indica el tipo de autenticación que configuró en el punto de acceso.
- **Cifrado de datos**. Indica el tipo de encriptación que indicó en la configuración del punto de acceso.
- **Clave de red**. Indica la clave que indicó en la configuración del punto de acceso que es la que ha escrito cuando se conectó desde el equipo.
- **Confirme la clave de red**. Es la misma clave anterior repetida.

Cuando haya finalizado, pulse **Aceptar** o **Cancelar** (dependiendo de si desea guardar los cambios que haya realizado y que deberán coincidir con los del punto de acceso, ya que, en caso contrario, no se podrá volver a conectar).

Ya puede proceder igual con todos los equipos que desee unir al punto de acceso y establecer una red con todos ellos.

Para tener acceso a Internet, habrá que instalar un router ADSL al switch, para ver cómo configurarlo vea el apartado *Configuración de un router ADSL* del capítulo 4).

En **Windows Vista**:

1. Desde el equipo que desea unir a la red inalámbrica, pulse en el icono

    que se encuentra a la derecha de la Barra de tareas y **seleccione Conectarse a una red**.

2. Le mostrará todos los puntos de acceso con los que ha contactado. Seleccione el SSID correspondiente a su punto de acceso y pulse en **Conectar**.

3. Indique la clave de red que puso en la configuración del punto de acceso (que deberá repetir), pulse en **Conectar** y, al cabo de un momento, le indicará que está conectado al punto de acceso.

4. Cierre la ventana **Conectarse a una red** y verá que en su icono ha desaparecido el aspa roja.

5. Ya puede ver los equipos de su grupo de trabajo y compartir archivos e impresoras con ellos tal y como se explicó anteriormente (para obtener más información, vea el apartado *Conexión de un equipo a un conmutador/concentrador*).

6. A partir de este momento, cada vez que reinicie el equipo, se establecerá una conexión automática con el punto de acceso (si no desea que sea así, pulse con el botón izquierdo del ratón en el icono **Conectarse a una red**, después, **Conectar o Desconectar** y, por último, en **Desconectar**, antes de apagar el equipo).

Para ver la configuración que ha tomado el adaptador inalámbrico (que será la que tenía el punto de acceso), siga los pasos siguientes:

1. Pulse con el botón derecho del ratón sobre **Red** (si no aparece en el Escritorio, se encuentra en el **menú Inicio**) y seleccione **Propiedades**.

2. En la ventana que se ha abierto (**Centro de redes y recursos compartidos**), verá que está conectado al punto de acceso. Pulse sobre **Ver estado** de la conexión de red inalámbrica que está establecida.

3. Le mostrará una pantalla con un resumen sobre dicha conexión. Pulse sobre **Propiedades inalámbricas** y verá el SSID del punto de acceso. También podrá indicar si desea que se conecte automáticamente a esta red si está a su alcance y si desea que se conecte a una red preferida si está disponible.

4. Si pulsa sobre **Seguridad**, verá la pantalla siguiente:

En ella verá los siguientes apartados:

- **Tipo de seguridad**. Indica el tipo de seguridad que configuró en el punto de acceso.
- **Tipo de cifrado**. Indica el tipo de encriptación que indicó en la configuración del punto de acceso.
- **Clave de seguridad de red**. Indica la clave que indicó en la configuración del punto de acceso que es la que ha escrito cuando se conectó desde el equipo.
- **Mostrar caracteres**. Indica que muestre la clave de red anterior en lugar de asteriscos.

Cuando haya finalizado, pulse **Aceptar** o **Cancelar** (dependiendo de si desea guardar los cambios que haya realizado y que deberán coincidir con los del punto de acceso, ya que, en caso contrario, no se podrá volver a conectar).

Ya puede proceder igual con todos los equipos que desee unir al punto de acceso y establecer una red con todos ellos.

Para tener acceso a Internet, habrá que instalar un router ADSL al switch, para ver cómo configurarlo vea el apartado *Configuración de un router ADSL* del capítulo 4).

Capítulo 4

REDES WAN

INTRODUCCIÓN

Cuando se ha hablado de las redes de área local (*LAN*), se ha considerado un sistema cerrado de comunicación entre ordenadores (se podría haber tratado la posibilidad de un acceso al exterior a través del correo electrónico o Internet que se tratará en profundidad en el capítulo 5).

Toda la infraestructura de la red: ordenadores, cableado, adaptadores, concentradores, pertenecía a la propia red. Sin embargo, llega un momento en el que, por la longitud de la conexión entre máquinas o conjuntos de máquinas, es imposible mantener una red LAN y se debe recurrir a otros sistemas de comunicación. Es, en este momento, en el que nos estamos refiriendo a las redes WAN.

Una **red WAN** (**Wide Area Network**) es aquella que se encuentra formada por la interconexión de otras redes en un área geográfica amplia empleando, para ello, sistemas de telecomunicaciones. Normalmente, estos enlaces no son administrados por los gestores de la red ya que son aportados por compañías externas, operadoras telefónicas. Generalmente, deberíamos hablar de conexiones WAN, más que de redes WAN, pues son los sistemas de conexión los que van a poder definir con más claridad este tipo de red. El sistema más sencillo de conectar dos redes LAN sería mediante un enlace dedicado contratado a una operadora.

Al ser las distancias entre máquinas considerablemente mayores en las redes tipo WAN, es necesaria una tecnología diferente que garantice adecuadamente la transmisión de datos. Es en este punto donde mencionamos la tecnología ATM o la Red Digital de Servicios Integrados (RDSI).

En el caso de redes de tipo inalámbricas nacen nuevos conceptos como **WWAN** (**Wireless Wide Area Network**) que se tratarán posteriormente.

TIPOS DE REDES WAN

El criterio más eficiente para la clasificación de las conexiones WAN es la utilización o no de circuitos dedicados.

Los **circuitos dedicados** son aquellos en los que el medio de transmisión entre los puntos permanece permanentemente abierto.

Cuando no existe un circuito abierto permanentemente, sino que deben estar conectados los distintos canales físicos para establecer la conexión entre los puntos, se habla de **circuitos conmutados**.

En función de todo ello, se pueden dar dos tipos de redes WAN:

- **WAN dedicada**. Comprende un conjunto de medios que hacen posible la comunicación entre dos puntos determinados, de forma permanente y sin posibilidad de acceder a la red pública telefónica ni a ningún otro circuito, durante las 24 horas del día, sin necesidad de realizar ningún tipo de marcado para establecer la comunicación. Este tipo de circuitos está indicado siempre que se deseen transmitir grandes volúmenes de datos entre dos puntos o una velocidad de transmisión alta. También se le denomina **circuitos punto a punto**.

- **WAN conmutada**. Para este tipo, se crea, mantiene y finaliza un circuito físico de conexión dedicado, proporcionado por una compañía de telecomunicaciones. Esta tecnología sería similar a la que se emplea en las llamadas telefónicas y mantiene un ancho de banda estable.

La selección de una u otra tecnología WAN depende, en gran medida, de las prestaciones que se ofrecen y su coste. Por regla general, el ancho de banda en este tipo de conexión es caro y se debe analizar si se desea una conexión permanente o las necesidades de comunicación no han de ser constantes y se puede emplear un sistema que emplee pago mediante tarifa.

TECNOLOGÍAS DE ACCESO REMOTO

Hasta este momento, se han estado analizando los elementos que permiten la conexión en red. Algunos de los dispositivos de interconexión vistos en el capítulo 2 tenían como objeto permitir la comunicación entre dos redes distintas. Sin embargo, la mayoría de las redes locales que existen en este momento no se conectan a través de líneas privadas dedicadas creadas para ello; lo hacen a través de redes de comunicación públicas empleando para ello distintas tecnologías.

En general, esta intercomunicación tiene por objeto:

- Mantener comunicadas distintas LAN de una misma empresa.
- Acceder a Internet.
- Acceder desde un equipo a una LAN remota empleando para ello una **red privada virtual** (**VPN**).

Al tratarse de redes de comunicación públicas, las tecnologías empleadas deben ser las que ya están implementadas por las grandes compañías.

ADSL

La tecnología **ADSL** (**Asymmetric Digital Subscriber Line**) es parte de una familia denominada genéricamente **xDSL** (**X-type Digital Subscriber Line**). Está diseñada para ofrecer servicios de banda ancha y permitir, por sus características, una instalación rápida y con un coste inferior a otras tecnologías.

Tradicionalmente, la línea telefónica se ha utilizado para la transmisión de señales dentro de la llamada *banda vocal* (caso de los módems convencionales). Cualquier señal fuera de esta banda es filtrada (eliminada), tanto por los teléfonos como por los equipos de las centrales telefónicas.

Sin embargo, la propia línea telefónica en sí misma admite señales de frecuencias mucho más altas, aunque limitadas según las características de cada línea en particular. El desarrollo de nuevas tecnologías (como ADSL) aprovecha esta circunstancia posibilitando un importante incremento de las velocidades utilizables sobre dicha línea.

Todo esto es posible debido a que la tecnología ADSL utiliza el ancho de banda disponible por encima del requerido por el servicio telefónico hasta el límite permitido por la propia línea.

Se puede observar que la banda de frecuencias que utiliza ADSL se divide en dos sub-bandas, una para las señales enviadas desde el usuario hacia la red (ascendente) y otra mayor, para las señales recibidas por el usuario desde la red (descendente). Esta asimetría, característica de ADSL, permite alcanzar mayores velocidades en sentido red – usuario, lo cual se adapta perfectamente a los servicios de acceso a la información (por ejemplo, Internet) en los que, normalmente, el volumen de información recibido es mucho mayor que el enviado.

Esto permite alcanzar elevadas velocidades de transmisión en el bucle de abonado, que dependerán de diversos factores tales como longitud del bucle, calibre de los pares, existencia de ramas múltiples, paso por zonas ruidosas, etc. (vea la tabla 4.1 para ver una comparativa de las velocidades).

Actualmente, en diversos países las empresas de telefonía están implantando versiones mejoradas de esta tecnología como ADSL2 y ADSL2+ con capacidad de suministro de televisión y video de alta calidad por el par telefónico, lo cual supone una dura competencia entre los operadores telefónicos y los de cable, y la aparición de ofertas integradas de voz, datos y televisión.

El *hardware* necesario para su implementación es relativamente sencillo y barato. En cuanto al usuario, sólo necesita un router *ADSL* o un módem *ADSL* (suele ser una tarjeta *PCI* si es interno mientras que, si es externo, se conecta al equipo mediante una tarjeta de red). Adicionalmente, es necesario incorporar filtros separadores (**splitters** o **microfiltros**) que permitan discriminar la señal de las frecuencias de banda vocal y ADSL, posibilitando la coexistencia junto con el servicio telefónico básico.

Tabla 4.1. Comparativa de velocidades en ADSL

	ADSL	ADSL2	ADSL2+
Ancho de banda de descarga	0,5 MHz	1,1 MHz	2,2 MHz
Velocidad máxima de subida	1 Mbps	2 Mbps	2 Mbps
Velocidad máxima de descarga	8 Mbps	12 Mbps	24 Mbps
Distancia	2,0 km	2,5 km	2,5 km
Tiempo de sincronización	10 a 1000 s	3 s	3 s

Entre sus ventajas se encuentran:

- Ofrece la posibilidad de hablar por teléfono mientras se navega por Internet, ya que, como se ha indicado anteriormente, voz y datos trabajan en bandas separadas, lo cual implica canales separados.

- Usa una infraestructura existente (la de la red telefónica básica). Esto es ventajoso, tanto para los operadores que no tienen que afrontar grandes gastos para la implantación de esta tecnología, como para los usuarios, ya que el costo y el tiempo que tardan en tener disponible el servicio es menor que si el operador tuviese que emprender obras para generar nueva infraestructura.

- Los usuarios de ADSL disponen de conexión permanente a Internet, al no tener que establecer esta conexión mediante marcación o señalización hacia la red. Esto es posible porque se dispone de conexión punto a punto, por lo que la línea existente entre la central y el usuario no es compartida, lo que además garantiza un ancho de banda dedicado a cada usuario, y aumenta la calidad del servicio. Esto es comparable con una arquitectura de red conmutada.

- Ofrece una velocidad de conexión mucho mayor que la obtenida mediante marcación telefónica a Internet (módem). Éste es el aspecto más interesante para los usuarios.

Entre sus inconvenientes se encuentran:

- En España, a diferencia de otros países y de lo que sucede con el cable en su ámbito, no existe la posibilidad de dar de alta el ADSL independientemente de la línea de teléfono fijo.

- No todas las líneas telefónicas pueden ofrecer este servicio, debido a que las exigencias de calidad del par, tanto de ruido como de atenuación, por distancia a la central, son más estrictas que para el servicio telefónico básico. De hecho, el límite teórico para un servicio aceptable equivale a 10 km y a partir de 1 km pierde bastante velocidad.

- Debido al cuidado que requieren estas líneas, el servicio no es económico en países con pocas o malas infraestructuras, sobre todo si lo comparamos con los precios en otros países con infraestructuras más avanzadas.

- El router ADSL necesario para disponer de conexión, o en su defecto, el módem ADSL, es caro (en menor medida en el caso del módem). No obstante, en España es frecuente que los proveedores de servicios a Internet subvencionen estos aparatos.

Para ADSL se dispone de tarifa plana. Dicha tarifa es independiente del tráfico cursado, es decir, pagando una cantidad fija se tiene la posibilidad de navegar todo lo que se desee.

Hay que añadir, además, el precio del módem/router y su instalación que va en función del tipo de aparato y de la compañía que lo proporciona e instala.

Gracias a la competencia entre las distintas compañías salen ofertas promocionales que abaratan los costes a los usuarios.

Para la puesta en marcha del servicio ADSL, el operador dominante debe actuar directamente sobre la línea de acceso de cada abonado y crear la infraestructura necesaria en cada central y en cada demarcación. Por ello, la implantación del ADSL se ha ido haciendo de forma progresiva.

Si el servicio telefónico de una localidad no pertenece a una central adaptada entonces un usuario no se podrá contratar ADSL con ningún proveedor de servicios de Internet.

ADSL2 y ADSL2+

La migración de ADSL a **ADSL2** sólo requiere establecer entre la central telefónica y el usuario un terminal especial que permita el nuevo ancho de banda, lo que no supone un enorme gasto por parte de los proveedores de servicio. Ya existen proveedores europeos que lo ofertan, por lo que puede decirse que ADSL2 está totalmente preparado para reemplazar al ADSL convencional a corto plazo.

El sistema ADSL2 contempla una mejora en los aparatos encargados de proveer el servicio, destinados a añadir una serie de facilidades que permiten realizar diagnósticos durante la fase de instalación, uso o mejora del servicio.

Incluso el tiempo empleado para realizar la conexión inicial desde el terminal al proveedor es de 3 segundos, siendo de 10 segundos en el ADSL convencional.

Otra ventaja es que es capaz de dar cobertura a bucles más largos que los posibles con ADSL. Ello también implica que ADSL2 proporcione mayores velocidades a puntos alejados con respecto a ADSL.

ADSL2+ es una evolución del sistema ADSL y ADSL2. La principal diferencia con respecto a un sistema ADSL es que la cantidad de espectro que se puede usar sobre el cable de cobre del bucle de abonado es el doble. Este espectro de más se usa normalmente para alojar en canal de bajada de información desde la central al abonado, proporcionando un mayor caudal de información.

Teóricamente, la velocidad que un sistema ADSL2+ puede alcanzar supera los 16 Mbps para distancias cercanas a la central. A medida que la distancia a la central aumenta, esta ventaja se hace más pequeña. A partir de unos 3000 metros, la diferencia con ADSL es marginal.

La parte superior del espectro que ADSL2+ utiliza también es la más vulnerable a la diafonía y a la atenuación, por tanto al aumentar la distancia, el ruido por diafonía y la atenuación son mayores.

ADSL rural

Hace tiempo que Telefónica lanzó al mercado el **ADSL rural** para zonas donde no llegaba la banda ancha, al menos a través del par de cobre. El proyecto cofinanciado por los Fondos FEDER (en el caso de las comunidades autónomas de Andalucía, Asturias, Canarias, Castilla y León, Castilla-La Mancha, Comunidad Valenciana, Galicia o la Región de Murcia) pretende disminuir la brecha digital del campo con respecto a las ciudades y, sobre todo, facilitar un acceso a Internet de calidad.

Sus características son:

- Línea de conexión permanente a Internet.
- Alta velocidad: desde 512 Kbps hasta 4 Mbps.
- No ocupa la línea telefónica.
- Cuota fija mensual para navegar las 24 horas del día.
- Conexión inalámbrica, mediante Módem-Router Wi-Fi opcional.
- Velocidades de contratación diferentes.

Un estudio ha comprobado que la gente que se conecta desde el campo con un ADSL rural navega mucho más lento que la gente que se conecta desde la ciudad con el ADSL convencional, pero no es sólo que es más lento sino que además es más caro.

VDSL

VDSL (**Very high bit-rate Digital Subscriber Line**, **DSL de muy alta tasa de transferencia**) es una tecnología de acceso a Internet de banda ancha, perteneciente a la familia de tecnologías xDSL que transmiten los impulsos sobre pares de cobre.

Se trata de una evolución del ADSL, que puede suministrarse de manera asimétrica (52 Mbit/s de descarga y 12 Mbit/s de subida) o de manera simétrica (26 Mbit/s tanto en subida como en bajada), en condiciones ideales sin resistencia de los pares de cobre y con una distancia nula a la central.

Esta tecnología sustituirá al ADSL y ADSL2+ permitiendo mayores velocidades y la emisión de contenidos en alta definición.

La tecnología VDSL utiliza 4 canales para la transmisión de datos, dos para descarga y 2 para subida, con lo cual se aumenta la potencia de transmisión de manera sustancial.

Las aplicaciones para las que más está siendo usada la tecnología VSDL son para la transmisión de televisión de alta definición por red. VDSL es capaz de transmitir vídeo comprimido, una señal en tiempo real poco apta para los esquemas de retransmisión de error utilizados en las comunicaciones de datos.

FTTH

Todo apunta a que Telefónica reutilizará en los próximos años la infraestructura de fibra óptica desplegada en el pasado. Detrás de ello se esconde la tecnología **FTTH** (**Fiber To The Home**, **Fibra hasta el hogar**). Esta tecnología se basa en la utilización de cables de fibra óptica y sistemas de distribución ópticos para la distribución de servicios avanzados a los hogares y negocios de los abonados.

Esta infraestructura permite crear redes simétricas de 100 Mbps, lo que significa que tan prodigioso ancho de banda es el mismo para la recepción y la emisión. Ya se han hecho pruebas de campo llegando a 50 Mbps en distancias de hasta 20 Km.

FTTN

FTTN (**Fiber to the Node**, **Fibra hasta el nodo**) constituye una eficaz combinación de fibra óptica y cable de cobre, donde el elemento diferencial con respecto a FTTH es el tramo de fibra óptica utilizado.

Esta tecnología consiste en llevar fibra hasta un punto del vecindario y completar la instalación con VSDL sobre hilos de cobre hasta el teléfono.

Redes de cable

Las redes de cable, que tienen una topología ramificada, contienen cuatro partes:

- **Equipo de cabecera**. Su labor es multiplexar el ancho de banda disponible entre las conexiones existentes, controlar el buen funcionamiento de todas ellas y monitorizar continuamente el estado de la red. Suele constar de varios elementos para captar los distintos tipos de señal que le pueden llegar.

- **Red troncal**. La red troncal está formada por anillos de fibra óptica que recorren cierto número de nodos primarios. Dichos nodos ópticos permiten que la información en forma de señales ópticas se transmita entre ellos y, a su vez, están conectados con los secundarios que formarán la siguiente parte de la red. A través de ella, se transportarán las señales generadas por las cabeceras a todos los puntos que alcanza la distribución de la red de cable.

- **Red de distribución**. La red de distribución está constituida por un bus de cable coaxial de banda ancha al que se conectan los diferentes usuarios mediante la correspondiente acometida. En los nodos secundarios, desde los que parte este tipo de cable y que conectan con los primarios, la señal óptica se convierte en eléctrica. Las conexiones entre ambos tipos de nodo son de tipo punto a punto esencialmente, aunque se pueden utilizar otro tipo de estructuras de interconexión. Debido a que la capacidad de la fibra óptica es mucho mayor que la del cable coaxial de banda ancha, un único nodo óptico soportará varias conexiones de coaxial (actualmente, se considera que ha de haber cuatro conexiones de coaxial por cada nodo óptico).

- **Acometida a la casa del abonado**. Es la parte que podría compararse con el bucle de abonado que actualmente se utiliza en las comunicaciones telefónicas de la red telefónica básica. Su función se limita a la instalación en los edificios y hogares de abonados de todo lo referente al módem de cable. A éste además se añade un separador (*splitter*), que divide la señal que proviene del coaxial.

Las redes de cable necesitan tener habilitado, además del canal descendente, el canal ascendente o de retorno para enviar información desde el usuario hasta la cabecera.

Una vez habilitada la comunicación en ambos sentidos, el equipo de cabecera puede actuar de dos maneras distintas:

- Transmitiendo todo lo recibido por un canal ascendente hacia uno descendente. De esta forma, el par de canales se comporta como un bus y el equipo de cabecera actúa como un repetidor. Junto a este repetidor se coloca un módem de cabecera que recoge del canal descendente los datos que van a otras subredes e inserta en el canal ascendente (antes de que llegue al repetidor) datos procedentes de otras subredes. Cuando se ponga en funcionamiento un sistema, todos los usuarios estarán conectados a una misma subred y, a medida que el tráfico aumente, habrá que ir habilitando subredes adicionales.

- Examinando cada paquete de datos y transmitiendo únicamente por el canal descendente en el que se encuentre el destinatario. Es decir, realiza funciones de encaminamiento (no es un simple repetidor) entre varios canales ascendentes y varios descendentes, además del tráfico proveniente de otras redes.

Evidentemente, cuanto menor sea el número de usuarios por nodo, mayor ancho de banda habrá disponible de forma individual para cada usuario y menor número de dispositivos electrónicos entre abonado y cabecera por lo que aumentará la calidad.

Para montar una red de cable se necesita un módem de cable. Para que funcione el sistema se ha de colocar un separador (*splitter*) en el domicilio del abonado, para separar (desde el cable coaxial que llega del exterior) la línea de datos que van al ordenador de la línea que transporta los canales de televisión.

Los módem de cable, generalmente, se conectan a los ordenadores a través de un cable de categoría 5 con un conector *RJ45* (también pueden soportar conectores *USB*).

En cuanto al protocolo de transmisión de datos, todo está basado en *Ethernet* e *IP*, por lo que el control de flujo, control de errores y cualquier otro elemento de comunicación cumple con lo estipulado por estos protocolos.

Un dispositivo denominado **Cable Modem Termination System** (**CMTS**) se coloca en el equipo de cabecera local, con el fin de controlar el acceso de cada módem de cable a la red. El tráfico se enruta desde el *CMTS* hasta las instalaciones de un proveedor de cable que realizará la conexión a *Internet*.

Algunos proveedores utilizan servidores *proxy* y servidores de *caché* para almacenar copias de las páginas *Web* más visitadas por sus subscriptores. De esta

manera, su cliente tendrá un acceso más rápido para ver las páginas *Web* más visitadas.

La velocidad anunciada en la publicidad es equivalente a la anunciada por las compañías telefónicas con ADSL.

La forma de tarificación es mediante tarifa plana pero algunas compañías establecen un límite máximo de descarga. Según la tarifa que se contrate se tendrá derecho a una mayor o menor cantidad de información. Y si se supera el límite, se pagarán aparte los datos descargados en exceso.

El servicio de las redes de cable comprende Internet, teléfono y televisión por lo que existen ofertas en forma de paquetes para que los usuarios se abonen a varios de estos servicios simultáneamente.

Debido a que las redes de cable ofrecen servicio telefónico, también pueden ofrecer el servicio de Internet a través de la línea de teléfono, esto es, usando el módem de siempre, y además algunas compañías, con tarifa plana de 24 horas.

Sistemas de acceso vía radio

Se entiende por **sistemas de acceso vía radio** aquellos sistemas que utilizan el espectro radioeléctrico en el aire, en lugar del par de cobre, cable coaxial o fibra óptica para llevar la red de telecomunicaciones a casa del cliente.

Se les conoce también con el nombre de **bucle local inalámbrico** (**WLL**) o **sistemas de acceso inalámbrico punto–multipunto**.

LMDS

Entre los sistemas de acceso vía radio se encuentra **LMDS** que es un sistema de comunicación punto–multipunto inalámbrico que surge para facilitar el despliegue de las redes de los operadores de cable permitiendo servicios digitales bidireccionales de vídeo y datos en las bandas de 27,5 a 29,5 *GHz* o 40,5 a 42,5 *GHz* (en España, las licencias concedidas recientemente por el Ministerio de Fomento se encuentran en las bandas de 3,4 a 3,6 *GHz*, orientadas a usuarios de gama baja, por ejemplo residenciales, y 24,5 a 26,5 *GHz*).

En ambos casos, la arquitectura del sistema consiste en una serie de estaciones base interconectadas entre sí y con el centro de control de red por medio de cable o radioenlaces, dando servicio a una serie de abonados fijos distribuidos por el interior de celdas de radio variable.

Su funcionamiento consiste en convertir la señal que viaja por cable en ondas de radio, captarlas mediante antenas instaladas en cada edificio y distribuirla a los abonados por cable.

Dada la anchura de banda disponible, *LMDS* puede ser el soporte de una gran variedad de servicios simultáneos: televisión multicanal (difusión, pago por visión, vídeo por demanda), telefonía, datos, servicios interactivos multimedia (tele-educación, telemedicina, acceso a *Internet* en banda ancha, etc.) con una inversión inferior a la que implica la solución equivalente cableada y con un despliegue más rápido, ya que no requiere abrir zanjas por toda la ciudad.

El acrónimo *LMDS* proviene de:

- **Local**. Indica las características de propagación de las señales en este rango de frecuencias. Las ondas milimétricas de baja potencia pierden energía rápidamente, alcanzando una distancia limitada, entre 2 y 8 km aproximadamente.

- **Multipunto**. Indica que las señales son transmitidas según la filosofía punto-multipunto. Una estación radiobase gestiona las comunicaciones bidireccionales de más de 4000 usuarios. Como se verá más adelante, el enlace inalámbrico entre el suscriptor y la estación es una transmisión punto a punto.

- **Distribución**. Se refiere a la distribución de las señales, las cuales pueden ser tráfico bidireccional de voz, datos, Internet y video. *LMDS* proporciona banda ancha con velocidades de usuario de hasta 8 *Mbps*.

- **Servicio**. Servicios múltiples de voz y datos combinados con diferentes calidades de servicio y ancho de banda dinámico; los servicios ofrecidos en una red *LMDS* dependen completamente del tipo de negocio del operador.

La tecnología *LMDS* se está introduciendo lentamente en Europa y ya existen distintas compañías que fabrican equipos con distintas características de modulación, transmisión y frecuencias de trabajo, como Alcatel, Ericsson y Lucent Technologies.

VIMAX

WiMax (**Worldwide Interoperability for Microwave Access**) es una tecnología de transmisión inalámbrica que permite crear zonas de acceso concurrente de hasta 48 Km de radio y velocidades de hasta 70 Mbps sin necesidad de visibilidad directa.

La tecnología WiMax será la base de las Redes Metropolitanas de acceso a Internet, servirá de apoyo para facilitar las conexiones en zonas rurales y se utilizará en el mundo empresarial para implementar las comunicaciones internas. Además, su popularización supondrá el despegue definitivo de otras tecnologías, como **VoIP** (llamadas de voz sobre el protocolo IP).

WiMax está pensado principalmente como tecnología de "última milla" y se puede usar para enlaces de acceso, MAN o incluso WAN. WiMax destaca por su capacidad como tecnología portadora, sobre la que se puede transportar IP, ATM, Frame Relay y voz, lo que la hace perfectamente adecuada para entornos de grandes redes corporativas de voz y datos así como para operadores de telecomunicaciones.

WiMax funciona de forma similar a Wi-Fi pero a velocidades más altas, mayores distancias y para un mayor número de usuarios. Un sistema WiMax está formado por dos partes:

- Las torres WiMax que dan cobertura de hasta 8.000 kilómetros cuadrados (según el tipo de señal transmitida).

- Los receptores, es decir, las tarjetas que se conectan al PC, portátil, PDA y demás, para tener acceso al sistema.

Hay dos formas de ofrecer señal:

- **Cuando hay objetos que se interpongan entre la antena y el receptor**. En este caso, se opera con bajas frecuencias (entre los 2 y los 11 Ghz) para así no sufrir interferencias por la presencia de objetos. Naturalmente, esto hace que el ancho de banda disponible sea menor. Las antenas que ofrezcan este servicio tendrán una cobertura de 65 Km^2 (más o menos como las de los teléfonos móviles).

- **Cuando no hay nada que se interponga entre la antena y el receptor**. En este caso, se opera a muy altas frecuencias, del orden de 66 Ghz, disponiendo de un gran ancho de banda. Además, las antenas que ofrezcan este servicio tendrán una cobertura de hasta 9.300 Km^2.

Los usuarios normales (que son los que operan a bajas frecuencias) van a notar mucha diferencia con el Wi-Fi actual en dos aspectos fundamentales: la velocidad que sube hasta los 70 Mbps y la señal que llega a ser válida hasta los 50 Km (con condiciones atmosféricas favorables).

Esta tecnología está basada en el estándar IEEE 802.16 y cuenta con dos especificaciones: 802.16.a (para sistemas fijos) y 802.16e (para sistemas móviles). En la tabla siguiente se muestran algunas de las características de cada una de ellas:

	802.16	802.16a	802.16e
Espectro	10 - 66 GHz	< 11 GHz	< 6 GHz
Funcionamiento	Sólo con visión directa	Sin visión directa (NLOS)	Sin visión directa (NLOS)
Tasa de bit	32 - 134 Mbit/s con canales de 28 MHz	Hasta 75 Mbit/s con canales de 20 MHz	Hasta 15 Mbit/s con canales de 5 MHz
Movilidad	Sistema fijo	Sistema fijo	Movilidad pedestre
Anchos de banda	20, 25 y 28 MHz	Seleccionables entre 1,25 y 20 MHz	Igual que 802.16a con los canales de subida para ahorrar potencia
Radio de celda típico	2 - 5 km aprox.	5 - 10 km aprox. (alcance máximo de unos 50 km)	2 - 5 km aprox.

En cuanto a seguridad, por el momento WiMax incorpora *3DES* (*Triple Data Encription Standard*) pero se prevé que incorpore *AES* (*Advanced Encryption Standard*) cuando comience su comercialización a gran escala.

Todo esto convierte a WiMax en una tecnología de banda ancha alternativa a *xDSL* o el cable. De hecho, también se la conoce como **WDSL** (**Wireless DSL**).

Sistemas de acceso vía telefónica

Se puede decir que los sistemas de acceso por vía telefónica son sistemas inalámbricos de acceso global.

La **telefonía móvil** (también llamada **telefonía celular**) básicamente está formada por dos grandes partes: una red de comunicaciones (o red de telefonía móvil) y los terminales (o teléfonos móviles) que permiten el acceso a dicha red.

La telefonía móvil consiste en la combinación de una red de estaciones transmisoras-receptoras de radio (repetidores, estaciones base o *BTS*) y una serie de centrales telefónicas de conmutación de primer y segundo nivel (*MSC* y *BSC*, respectivamente), que posibilita la comunicación entre los terminales telefónicos

portátiles (teléfonos móviles) o entre terminales portátiles y teléfonos de la red fija tradicional.

Ha habido un avance muy rápido de esta tecnología que ha ido avanzando cada vez más rápidamente en sus posibilidades. A continuación, se va a realizar una breve descripción de las más recientes que son las que están actualmente en funcionamiento.

2G

Aunque los sistemas **2G** (segunda generación) tenían ciertas capacidades de transmisión de datos, fundamentalmente se trataban de un sistema que daba soporte a servicios de voz. Mientras se desarrollaba la tercera generación (3G), se creó una ampliación de la tecnología 2G que añadía nuevas capacidades de transmisión de datos (se denominó 2,5G). Entre las tecnologías existentes 2,5G se encuentra GPRS.

GPRS (**General Packet Radio Service**) es un sistema de transmisión de datos por paquetes dentro del estándar **GSM** (**Global System for Mobile Telecommunication**).

Como las tradicionales redes *GSM* no se adaptaban adecuadamente a las necesidades de transmisión de datos con terminales móviles, surgió *GPRS* con el objetivo de integrar el mundo *IP* con el mundo de la telefonía móvil, creándose toda una red paralela a la red *GSM* y orientada exclusivamente a la transmisión de datos.

En *GSM*, cuando se realiza una llamada se asigna un canal de comunicación al usuario, que permanecerá asignado aunque no se envíen datos, mientras que en *GPRS* los canales de comunicación se comparten entre los distintos usuarios dinámicamente, de modo que un usuario sólo tiene asignado un canal cuando se está realmente transmitiendo datos. Para utilizar *GPRS* se precisa un terminal móvil que soporte esta tecnología. Como la mayoría de dichos terminales soportan también *GSM*, se podrán realizar llamadas de voz utilizando la red *GSM* de modo habitual y las llamadas de datos (conexión a *Internet*, *WAP*...) con *GPRS*.

Las aplicaciones que se pueden utilizar con *GPRS* son las siguientes:

- Correo electrónico. Dichos mensajes son recibidos en el momento en el móvil, no siendo necesario conectarse con el servidor para verificar si hay nuevos mensajes.

- Navegar por *Internet*. Es posible acceder directamente a páginas *web* escritas en *HTML* y tener acceso a todos los contenidos, incluyendo imágenes.

- Transmisión de ficheros audio.

- Transferencia de documentos, etc.

Además, *GPRS* cuenta con las siguientes ventajas:

- Conexión de alta velocidad. Teóricamente la velocidad máxima de transmisión de datos que se puede alcanzar es de 171.2 *Kbps* (esta velocidad es tres veces superior a la que se consigue con módem en las redes de telefonía fija actuales y diez veces más rápida que con *GSM*). En *GSM* sólo se puede tener asignado un canal, sin embargo, con *GPRS*, se pueden tener asignados varios canales (con un máximo de ocho), tanto en el sentido de transmisión del móvil a la estación base como de la estación base al móvil, permitiendo que la velocidad de transmisión aumente con el número de canales asignados. Además, *GPRS* permite el uso de esquemas de codificación de datos que permiten una velocidad de transferencia de datos mayor que en *GSM*.

- Conexión permanente. Un usuario *GPRS* puede estar conectado todo el tiempo que desee, puesto que no hace uso de recursos de red (y, por tanto, no paga) mientras no esté recibiendo ni transmitiendo datos.

- Facturación basada en la cantidad de tráfico transmitido, calidades de servicio, etc.

3G

3G es la abreviatura de tercera-generación de telefonía móvil. Los servicios asociados con la tercera generación proporcionan la posibilidad de transferir tanto voz (una llamada telefónica) como datos (como la descarga de programas, intercambio de correo electrónico y mensajería instantánea).

Inicialmente la instalación de redes 3G fue lenta. Esto se debió a que los operadores necesitaban adquirir una licencia adicional para un espectro de frecuencias diferente al que era utilizado por la tecnología 2G.

Dispone de una base única conocida como **WCDMA** (**Wideband CDMA**) sobre la que se desarrollaron tres modos opcionales. Entre ellos, se encuentra UMTS.

En la tecnología **UMTS** (**Universal Mobile Telecommunications System**), las llamadas de voz y datos recorren el mismo camino en la Red de Acceso, pero se bifurcan en la Red de Conmutación, donde hay una red para atender a las llamadas de voz y otra para las llamadas de datos. Los elementos que gestionan estas llamadas son diferentes, y los lenguajes o protocolos que utilizan también lo son. El reto tecnológico consiste en que el usuario no necesite saber por dónde se está cursando su llamada y reciba los servicios de voz y datos de una forma transparente.

Las características de los sistemas de tercera generación son las siguientes:

- Transmisión simétrica/asimétrica de alta fiabilidad.
- Alta velocidad de transmisión: 144 *kbps* en entornos rurales (movilidad total), 384 *kbps* entornos urbanos (movilidad limitada) y 2 *Mbps* de pico (500 *kbps* de forma continua) en interiores (terminales estáticos).
- Utilización dinámica del ancho de banda disponible según la aplicación.
- Soporte de comunicación de paquetes y circuitos.
- Acceso a *Internet*, comercio electrónico, video y sonido en tiempo real.
- Cobertura mundial, con servicios terrestres y vía satélite.

3,5G

Es la evolución de la tercera generación (3G) de tecnología móvil y se considera el paso previo antes de la cuarta generación (4G).

La tecnología **HSDPA** (**High Speed Downlink Packet Access**) es la optimización de la tecnología UMTS y consiste en un nuevo canal compartido en el enlace descendente que mejora significativamente la capacidad máxima de transferencia de información hasta alcanzar tasas de 14 Mbps.

HSDPA lleva a las redes WCDMA a su máximo potencial en la prestación de servicios de banda ancha, mediante un aumento en la capacidad de datos celulares. De la misma manera en que UMTS incrementa la eficiencia espectral en comparación con GPRS, HSDPA incrementa la eficiencia espectral en comparación con WCDMA.

La mayoría de los operadores de 3G ofrecen esta tecnología en su red. La principal utilidad del servicio es acceso a Internet con mayor ancho de banda y menor latencia. Esto permite navegar, hacer descargas de correo electrónico, música y vídeo a mayor velocidad. Los operadores han enfocado el servicio como un acceso móvil a Internet de banda ancha para ordenadores portátiles.

4G

La tercera generación no está todavía bien introducida en el mercado y, sin embargo, los desarrolladores ya están trabajando en una nueva tecnología.

4G son las siglas de la cuarta generación de tecnologías de telefonía móvil. A día de hoy no hay ninguna definición de la 4G, pero se puede resumir que sus características principales que se están considerando son las siguientes:

- Abandona el acceso tipo CDMA característico de UMTS.
- Utiliza *SDR* (*Software Defined Radios*) para optimizar el acceso radio.
- La red completa prevista será todo IP.
- Las tasas de pico máximas previstas son de 100 Mbps en enlace descendente y 50 Mbps en enlace ascendente (con espectros en ambos sentidos de 20 Mhz).
- Al menos habrá 200 usuarios activos por cada célula de 5MHz.
- Tamaño óptimo de células de 5 km, pudiendo alcanzar los 100 km con una respuesta aceptable.
- Coexistencia y transparencia con los estándares anteriores.

CONECTAR UN EQUIPO VÍA MÓVIL (PARTE PRÁCTICA)

Es posible conectar un portátil o equipo de sobremesa a Internet desde cualquier lugar, utilizando un módem 3G o 3,5G que se conecte al equipo por un puerto USB.

También se puede utilizar un móvil como módem conectándolo al equipo por Bluetooth o USB.

Para ello, hay que disponer de un contrato con una compañía telefónica y utilizar un módulo de datos para que salga más económico.

De la misma manera, es posible conectarse a la red local de la empresa desde cualquier lugar sin necesidad de desplazarse hasta la sede de la empresa (este servicio requiere una contratación específica).

En el ejemplo, se va a utilizar el módem USB 3,5G Plus Novatel Ovation MC950D de Movistar. Este módem utiliza tecnología HSDPA que permite hasta 7,2 Mbps de bajada y hasta 2 Mbps de subida. Además, funciona con Windows XP y Vista, utilizando un puerto USB 1.1 ó 2.0.

Una vez que se ha colocado la tarjeta SIM en el módem, instalado los drivers y cargado el Escritorio Movistar (los ficheros necesarios vienen almacenados dentro del dispositivo), siga los pasos siguientes (en XP y Vista):

1. Ejecute el icono **Escritorio Movistar** que se ha creado en el escritorio del equipo y verá la pantalla que se encuentra a la derecha:

2. Indique el PIN de la tarjeta SIM, pulse en **Aceptar** y comenzará a realizar varios procesos (podrá verlos en la última línea de la pantalla). Cuando haya finalizado, le indicará que la tarjeta está preparada y verá la pantalla principal del Escritorio Movistar.

3. Pulse en el triángulo que hay a la derecha de **Conectar** y verá que se encuentra habilitada la opción **Conectar a GPRS/3G.**

4. Seleccione dicha opción y le mostrará una nueva pantalla para que seleccione **Internet GPRS/3G** y pulse en **Conectar**.

5. Comenzará a validar el nombre del usuario y la contraseña (se encuentran en la tarjeta SIM) y, al cabo de un momento, le mostrará en la parte derecha de la barra de tareas que se encuentra conectado y la velocidad a la que lo está haciendo.

6. Desde este momento, puede abrir el **Movistar Internet** del **Escritorio Movistar** o el explorador que desee de su equipo para acceder a las páginas Web de Internet que quiera o abrir su programa de correo electrónico para recibir o enviar mensajes.

7. Otra opción que está disponible es **Mensajes** que le permite enviar mensajes SMS tecleando el texto y el destinatario desde el equipo. También podrá recibir mensajes destinados al número de teléfono correspondiente a la tarjeta SIM y almacenarlos en el equipo.

8. Tenga en cuenta que paga por cantidad de datos movidos (dependerá del módulo de datos que haya contratado) y no por el tiempo que esté conectado.

9. Cuando desee finalizar la sesión, pulse en **Desconectar** y habrá acabado la conexión.

CONFIGURACIÓN DE UN ROUTER ADSL (PARTE PRÁCTICA)

Una de las diferencias entre un router tradicional y un router ADSL es que éstos últimos son equipos que trabajan de forma independiente de los ordenadores a los que está conectado. Por tanto, para que funcione correctamente necesita disponer de determinada información (direcciones IP, máscaras de red, tipo de conexión, etc.) que se han de indicar en el proceso de configuración.

Conceptos previos

MODO MONOPUESTO O MULTIPUESTO

Un router en **modo multipuesto** (o **routed**, es decir, que pueda ser utilizado por varios ordenadores simultáneamente) necesita siempre estar

configurado con determinada información, mientras que si que está en **modo monopuesto** (o **bridged**, es decir, que sólo puede ser utilizado por un ordenador) no requiere de tanta configuración, ya que únicamente se limita a pasar la información que les llega del ordenador al proveedor ADSL.

No hay que confundir el modo multipuesto con compartir la conexión de Internet, que significa que un equipo tiene conexión en modo monopuesto pero su conexión se comparte con el resto de equipos de la red a través del software que se encuentra en dicho equipo.

DIRECCIÓN IP ESTÁTICA O DINÁMICA

Cuando se contrata la conexión ADSL con un proveedor, éste puede proporcionar una IP pública estática para la conexión o le asignará una dirección IP de forma dinámica cada vez que el router se inicie (que luego se irá renovando cada cierto tiempo en función de la configuración que le haya dado al router).

EL PROTOCOLO DE CONEXIÓN

El protocolo de conexión del router con el proveedor ADSL depende de varios factores:

- Si se ha contratado una dirección IP estática o dinámica.
- Si el router está configurado en modo monopuesto o multipuesto.
- Si utiliza el protocolo Ethernet o ATM.
- Del protocolo adoptado (PPP o IP).

En función de todos los factores anteriores, se pueden dar los siguientes protocolos de conexión:

- **RFC 2516 PPPoE**. Este protocolo se utiliza cuando se tiene una dirección IP pública dinámica asignada por el proveedor y utiliza el protocolo PPP sobre Ethernet. Es para un modo multipuesto. Se necesita indicar un nombre de usuario y una contraseña para que realice la conexión con el equipo del proveedor. En la figura siguiente se muestra la pantalla **Basic Setup** del router Linksys WAG54GS.

- **RFC 2364 PPPoA**. Este protocolo se utiliza cuando se tiene una dirección IP pública dinámica asignada por el proveedor y utiliza el protocolo PPP sobre ATM. Es para un modo multipuesto. Se necesita indicar un nombre de usuario y una contraseña para que realice la conexión con el equipo del proveedor. La pantalla de configuración de este protocolo es similar a la del RFC 2516 PPPoE.

- **IPoA**. Este protocolo se utiliza cuando se tiene una dirección IP pública estática y utiliza el protocolo IP sobre ATM. Es para un modo multipuesto. En la figura siguiente se muestra la pantalla **Basic Setup** del router Linksys WAG54GS.

- **RFC 1483 Routed**. Este protocolo se utiliza cuando se tiene una dirección IP pública estática y utiliza el protocolo IP sobre ATM. Es para un modo multipuesto. En la figura siguiente se muestra la pantalla **Remote Site IP** del router OfficeConnect Remote 812 de 3Com.

- **RFC 1483 Bridged**. Este protocolo se utiliza cuando se tiene una dirección IP pública estática y utiliza el protocolo IP sobre ATM. Es para un modo monopuesto. En la figura siguiente se muestra la pantalla **Edit connection** del router Sabih x7768r.

- **Bridge Mode Only**, es decir, haciendo la función de un módem. Es para un modo monopuesto. En la figura siguiente se muestra la pantalla **Basic Setup** del router Linksys WAG54GS.

En la tabla siguiente se muestran los protocolos que utilizan algunos proveedores de servicio ADSL:

Proveedor	Protocolo	Tipo de IP
Arrakis	PPPoA	IP Dinámica
Auna	PPPoA	IP Dinámica
Comunitel	PPPoA	IP Dinámica
Eresmas	PPPoA	IP Dinámica
EuskalTel	PPPoA	IP Dinámica
Jazztel	PPPoA	IP Dinámica
Jazztel 20Mb	PPPoE	IP Dinámica
Orange	PPPoE	IP Dinámica
Telefónica-España	PPPoE	IP Dinámica
Tele 2	PPPoA	IP Dinámica
Terra	PPPoE	IP Dinámica
Ya.com	PPPoA / PPPoE	IP Dinámica
Telefónica	IPOA / RFC1483	IP Fija
Terra	IPOA / RFC1483	IP Fija
Wanadoo	IPOA / RFC1483	IP Fija
Ya.com	IPOA / RFC1483	IP Fija

LAS DISTINTAS DIRECCIONES IP

Cuando se va a configurar un router, es necesario saber distinguir los distintos tipos de direcciones IP que hay que proporcionar:

- **IP externa del router** o **dirección IP WAN.** Es la dirección IP visible desde Internet (**IP pública**). La proporciona el proveedor de acceso a Internet.

- **IP interna del router** o **dirección IP LAN**. Es la dirección IP que pertenece a la red interna (**IP privada**). Hay unos rangos de IP reservados para este tipo de dirección IP:

    - De 10.0.0.0 a 10.255.255.255
    - De 172.16.0.0 a 172.31.255.255
    - De 192.168.0.0 a 192.168.255.255

- **IP del router remoto**. Es la dirección IP del router de la red del proveedor de acceso a Internet. En algunos routers se denomina también **Default Gateway**.

- **IP gestión del módem**. Esta dirección IP la proporciona el proveedor de acceso para el modo monopuesto para no tener que emplear dos direcciones públicas (en Telefónica se denomina así, pero otros proveedores pueden darle otra denominación).

Dependiendo del modo en el que esté configurado el router, estas direcciones tienen los valores siguientes:

	Ordenador	Router (LAN)	Router (WAN)	Router Remoto
Monopuesto	IP pública	(IP pública AND máscara) + 1	IP gestión del módem	IP del router remoto (IP pública AND máscara)
Multipuesto (NAT)	IP privada (por ejemplo, 192.168.0.2)	IP privada (por ejemplo, 192.168.0.1)	IP pública	IP del router remoto (IP pública AND máscara) + 2

LA OPERACIÓN AND

La **operación AND** no es una operación aritmética como la suma o la resta, sino que se trata de una operación lógica que está pensada para llevarse a cabo con números binarios.

Los números binarios solo pueden tener dos valores: 0 y 1.

La operación AND consiste en que el resultado de la operación sea 1 sólo cuando el primer y segundo número son 1. En caso contrario, el resultado será 0.

1 AND 1 = 1
0 AND 1 = 0
1 AND 0 = 0
0 AND 0 = 0

Por ejemplo:

IP: 80.20.10.50
Máscara de subred: 255.255.255.0

Se pasan los valores a formato binario:

IP: 01010000 . 00010100 . 00001010 . 00110010
Máscara: 11111111 . 11111111 . 11111111 . 00000000

Se efectúa la operación AND:

Resultado: 01010000 . 00010100 . 00001010 . 00000000

Resultado en decimal: 80.20.10.0

¿QUÉ ES NAT?

NAT (**Network Address Translation**) es una opción que incorporan los routers (que están en modo multipuesto) para realizar una traducción de direcciones entre la red privada e Internet.

Sirve principalmente para permitir que varios equipos con direcciones IP privadas accedan a Internet a través de una única IP pública (la del router).

NAT hace que a los paquetes de información que viajan desde una red a la otra se les cambie el *origen* para que parezca que proceden del router y a sus respuestas se les cambia el *destino* para que lleguen al router a la vuelta.

Para poder identificar el tráfico de cada ordenador de la red se utiliza el número de puerto. El router se encarga de realizar la conversión del número de puerto para poder identificar a cada equipo Esto se hace mediante **NAPT** (**Network Address Port Translation**) o **PAT** (**Port Address Translation**). De esta manera, el router hará llegar cada respuesta al equipo que envió el paquete original.

DHCP

Podemos hacer que el router asigne automáticamente las IP privadas a los equipos de la red interna. Para ello, se ha de habilitar el servidor DHCP interno que incorpora el router.

Una vez que está habilitado el servidor DHCP, habrá que indicar en qué dirección IP va a comenzar a realizar asignaciones y las direcciones IP de los servidores DNS.

Con esta información, cuando un equipo se encienda, lo primero que hará será conectarse al servidor DHCP y recoger la dirección IP privada que le ha asignado y las direcciones IP de los servidores DNS para poder acceder a Internet.

EL MAPEO DE LOS PUERTOS

El hecho de que sea necesario mapear uno o más puertos para hacer funcionar ciertas aplicaciones en un determinado sistema depende principalmente de dos factores:

- Del **hardware y modo de conexión a Internet** que se utiliza.
- Del **software** o aplicación que se quiere ejecutar.

Hardware

El hecho de que sea necesario mapear puertos para hacer funcionar una aplicación en un determinado sistema se produce cuando la conexión a Internet de dicho sistema atraviesa un router con capacidades de NAT o PAT, es decir, **cuando la conexión pasa por un router en multipuesto**.

A pesar de que una aplicación lo requiera, **NO** es necesario mapear puertos cuando la conexión a Internet se establezca a través de un router en monopuesto, un módem ADSL o un cable-módem, ya que todos estos dispositivos no realizan funciones de NAT, es decir, todos los puertos están ya abiertos.

Software

Desde el punto de vista que se va a analizar, se van a clasificar las aplicaciones en tres tipos:

- **Aplicaciones cliente**. Son aplicaciones cuya función es recibir datos y para ello los solicitan a un servidor que se los envía. Estas aplicaciones **no precisan de mapeo de puertos**. Como ejemplos de estas aplicaciones podemos citar: Internet Explorer (o cualquier otro navegador web), clientes FTP (como CuteFTP) o clientes de correo electrónico (como Outlook Express).

- **Aplicaciones servidor**. Son aplicaciones diseñadas para enviar datos hacia aquellos usuarios que se los solicitan. Por tanto, es necesario poder conectarse a los puertos de los servidores para que éstos puedan enviar los datos solicitados. Estas aplicaciones **sí precisan realizar el mapeo de uno o más puertos en caso de tener que pasar por routers que se encuentren en modo multipuesto** (por ejemplo, servidores Web).

- **Aplicaciones cliente-servidor**. Estas aplicaciones realizan las dos funciones anteriores y, por tanto, **también requieren realizar el mapeo de uno o más puertos en caso de tener que pasar por routers que se encuentren en modo multipuesto** (por ejemplo, eMule, eDonkey, Bittorrent, etc.).

¿Qué puertos hay que mapear?

Los puertos TCP o UDP se numeran desde el 1 al 65535. Los puertos que van desde el 1 al 1023 se denominan **puertos bien conocidos** (**Well known ports**) y están reservados para determinados estándares de comunicación (Web, FTP, Telnet...).

El resto de puertos desde el 1024 al 65535 se denominan **puertos azarosos**, y son utilizados por diversas aplicaciones.

Los puertos azarosos se pueden dividir en **puertos registrados** (**Registered Ports**) que van desde el 1024 al 49151 y en **puertos privados o dinámicos** (**Dynamic and/or Private Ports**) que van del 49152 al 65535.

Lo puertos utilizados por cada aplicación son propios y dependen de la aplicación de que se trate.

En la pantalla siguiente se muestran los puertos que están habilitados en el router Linksys WAG54GS.

En la pantalla siguiente se muestran los puertos que están deshabilitados en el router Linksys WAG54GS.

WIRELESS

Hay routers que además de su función de encaminamiento y de actuar como conmutadores realizan tareas de punto de acceso para tener una red inalámbrica. Por ello, si se desea, es necesario configurarla igual que un punto de acceso y hay que conocer los apartados siguientes (para obtener más información, vaya al apartado *Configuración de un punto de acceso* del capítulo 3):

- **SSID (Wireless Network Name)**. Permite indicar el nombre de la red inalámbrica que es una cadena ASCII de hasta 32 caracteres. Este nombre deberá ser el mismo en todas las estaciones y se utiliza para impedir la unión involuntaria de personas.

- **Wireless Network Mode**. Esta opción permite seleccionar la banda de radio que se va a utilizar. Si se selecciona *B-Only*, se bloquearán los accesos que utilizan 802.11g; del mismo modo, si se selecciona *G-Only*, se denegarán los accesos a través de 802.11b. Si se desea permitir todos los accesos, hay que seleccionar *Mixed*.

- **Wireless Channel**. Permite seleccionar el canal que se va a utilizar para comunicarse.

- **Wireless SSID Broadcast**. Al activar esta casilla, está indicando que el punto de acceso emita el SSID a las estaciones (si está desactivada, las estaciones deberán saber el SSID con antelación).

  A continuación, se muestran la pantalla **Basic Wireless settings** del router Linksys WAG54GS.

- **Wireless security**. Con este apartado se puede indicar el método de cifrado que se desea establecer entre los equipos y el punto de acceso inalámbrico. Se podrá seleccionar entre:

  - **Wired Equivalent Privacy (WEP)**. La encriptación WEP no fue puesta en práctica con la norma 802.11. Además, WEP no

es completamente seguro, ya que en un paquete de datos la dirección MAC no está cifrada y los hackers pueden utilizarla para penetrar en una red falsificando la dirección MAC. Se puede utilizar con dos tipos de encriptación: 64 y 128 bits.

A continuación, se muestra el modo WEP de la pantalla **Wireless security** del router Linksys WAG54GS:

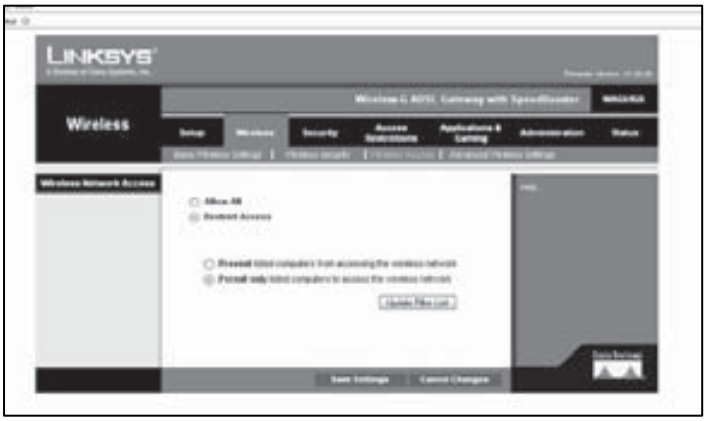
- **Wi-Fi Protected Access (WPA). WPA** es el más moderno y mejor sistema de seguridad Wi-Fi. A través de sus distintas opciones, permite utilizar dos métodos de encriptación:

  - **TKIP** (**Temporal Key Integrity Protocol**) que utiliza un método de encriptación más fuerte e incorpora **Mensaje Integridad Código** (**MIC**) para proporcionar protección contra hackers.

  - **AES** (**Advanced Encryption System**), que utiliza un bloque simétrico de 128 bits de cifrado de datos.

A continuación, se muestra el modo WPA de la pantalla **Wireless security** del router Linksys WAG54GS:

- **Wireless Access**. Si activa **Restrict access**, permitirá a los clientes cuyas direcciones MAC se encuentren en la lista de control (*ACL*) realizar la función contraria a la establecida por defecto: **Prevent** (denegar el acceso) o **Permit only** (permitir el acceso). A continuación, se muestra la pantalla **Wireless access** del router Linksys WAG54GS.



Al pulsar en **Update Filter List**, le mostrará la pantalla siguiente para que indique las direcciones MAC que desee.

OTRAS POSIBILIDADES

Además de las posibilidades indicadas anteriormente, los routers pueden tener otras como, por ejemplo:

- Restringir el acceso a Internet durante los días y horas indicados a los equipos que se desee.
- Realizar una copia de seguridad de la configuración del router y restaurarla cuando sea necesario.
- Actualizar su firmware.
- Devolver el router a la configuración de fábrica.
- Ver información resumida sobre su configuración.
- Permitir o bloquear el paso de VPN.

Configuración del router

Generalmente, los routers ADSL se configuran mediante un programa específico proporcionado por la empresa que ha suministrado el router.

No obstante, en caso de no disponer de dicho programa o para ver la configuración que se ha realizado, se puede hacer de tres maneras (aunque no todas ellas pueden ser utilizadas en todos los modelos):

- **Acceso remoto Web.** Es necesario conectar el equipo al router mediante un cable RJ45 y acceder a través de un navegador de Internet. Es necesario que el router disponga de dirección IP y que el equipo se encuentre en el mismo rango de direccionamiento que el router.

En la pantalla siguiente, se accede a un router con la dirección 192.168.1.1 utilizando Internet Explorer:

- **Acceso remoto Telnet.** Es necesario conectar el equipo al router mediante un cable RJ45 y acceder a través de una aplicación Telnet. Es necesario que el router disponga de dirección IP y que el equipo se encuentre en el mismo rango de direccionamiento que el router.

  En la pantalla siguiente, se accede a un router con la dirección 192.168.1.1 utilizando el comando **Telnet** desde el **Símbolo del sistema**:

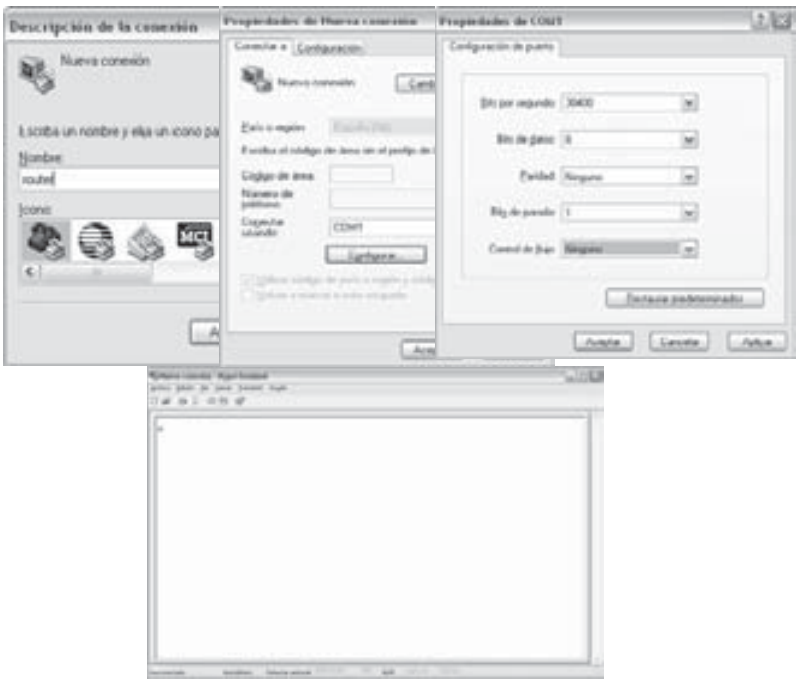
  En Windows Vista, hay que instalar previamente el cliente Telnet desde **Inicio**, **Panel de control**, **Programas y características** y **Activar o desactivar características de Windows**.

- **Acceso local (consola).** Es necesario conectar el equipo al router mediante un cable serie y acceder a través de una aplicación como Hyperterminal de Windows. No se necesita disponer de

direccionamiento IP previo, pero habrá que configurar dicho puerto serie con los parámetros:

- **Velocidad**: 38.400 bps (en caso de no funcionar bien, pruebe con 9.600 bps).
- **Bits de datos**: 8
- **Paridad**: ninguna
- **Bit de parada**: 1.
- **Control de flujo**: ninguno

Una vez seleccionado **Hyperterminal** que se encuentra en **Inicio, Todos los programas, Accesorios, Comunicaciones**, verá la serie de pantallas siguientes (deberá ir pulsando en **Aceptar** con los valores indicados):



En Windows Vista no existe Hyperterminal, por lo que habrá que utilizar una de las otras dos opciones (otra posibilidad es copiar los ficheros *C:\Archivos de programa\Windows NT\hypertrm.exe y C:\WINDOWS\system32\hypertrm.dll* de Windows XP en los mismos directorios de Windows Vista y poner un acceso directo en el Escritorio).

Debido a que existen infinidad de routers ADSL entre los que proporcionan los proveedores de acceso y los que se pueden comprar libremente por los usuarios, no se van a indicar configuraciones específicas para ninguno.

No obstante, existen páginas Web específicas orientadas al tema del ADSL, que ofrecen esas informaciones. Entre ellas se encuentran las siguientes:

www.adsl4ever.com
www.internautas.org
www.bandaancha.st
www.adslayuda.com
www.adslnet.es

Bloquear el acceso remoto

Es posible bloquear el acceso remoto a la configuración del router y así evitar modificaciones indeseadas, ya que, aunque se necesita un nombre de usuario y una contraseña, siempre es posible que alguien pueda acceder a él.

Por todo ello, es posible en la mayoría de los routers bloquear el acceso desde la red remota (Internet) y permitir el acceso desde la red local o desde Hyperterminal. Este bloqueo se puede acceder evitando el acceso por Web y por Telnet.

Para ello y dependiendo de los routers, hay dos alternativas distintas:

- Bloqueando el acceso desde la red remota por los puertos TCP-80 (acceso Web) y TCP-23 (acceso Telnet).

  En la pantalla siguiente se pueden ver los dos filtros que se han puesto en el router OfficeConnect Remote 812 de 3Com:

Para poner estos filtros, desde la pantalla inicial de configuración del router por Web y después de haber indicado el nombre de usuario y su contraseña, proceda de la manera siguiente:

1. Pulse **Configuration** y **Setup Filtres**.

2. Active la casilla **From all Remote Sites** y pulse **Next**.

3. Pulse **Create Filter** y verá la pantalla siguiente:

4. En **Filter Name**, indique el nombre que desee poner a este filtro, active la casilla **Advanced IP**, pulse **Next** y verá la pantalla siguiente:

5. Active la casilla **TCP Destination Port is Equal to**, indique 80 y pulse **Next.**

6. Pasará a una nueva pantalla en donde se encuentra el filtro que acaba de crear con la condición que ha puesto. En esta pantalla podría añadir más condiciones para el filtro (si pulsa en **Add)** o eliminar una condición (si pulsa **Delete**).

7. En el ejemplo, pulse **Save filter** y le mostrará una pantalla con la lista de filtros del router en donde se encuentra el filtro que acaba de crear para restringir el acceso por Web.

8. Repita todo el proceso pero ahora ponga 23 en **TCP Destination Port is Equal to** para que el filtro bloquee el acceso por Telnet.

9. Cuando haya finalizado, pulse en **Save Configuration** (se encuentra en la parte izquierda) para guardar los cambios realizados en la configuración del router.

- Abriendo un puerto para el acceso remoto de administración.

  En la pantalla siguiente se puede ver la pantalla de administración del router **Linksys WAG54GS**.

  Para poner este puerto para la administración remota, desde la pantalla inicial de configuración del router por Web y después de haber indicado el nombre de usuario y su contraseña, proceda de la manera siguiente:

  1. Pulse en la pantalla **Administration**.

2. En el apartado de la izquierda **Remote Gateway Access**, active la casilla **Enable** para permitir la administración remota y ponga el puerto que desee en **Management Port** (en el ejemplo, 8080).

3. Pulse en **Save Settings** para guardar los cambios que se han realizado en la configuración.

Capítulo 5

INTERNET, INTRANET Y EXTRANET

INTERNET

Internet se podría definir como una red que engloba una serie de redes de ordenadores con la finalidad de permitir el libre intercambio de información entre sus usuarios. Es posible tener acceso a cualquier información: desde las fotografías enviadas por el satélite *Meteosat* hasta información conseguida en una universidad americana o bien conseguir un programa de utilidad pública que se encuentre en un ordenador australiano.

Sin embargo, conectarse a Internet es como entrar en una inmensa biblioteca. Hay una gran cantidad de libros en interminables estanterías que contienen una cantidad enorme de información que si no se sabe cómo buscarla será totalmente inservible.

Además, Internet no es un servicio centralizado. No existe ninguna empresa a la que se pueda solicitar un catálogo de todos los servicios, de todas las bases de datos o un índice donde aparezcan todos los temas. Internet sólo se limita a establecer los procedimientos de interconexión, pero cada red o cada ordenador tienen su propio dueño.

El precio de conexión a Internet varía de acuerdo con el coste de mantenimiento de cada red, que es la que fija las tarifas a los usuarios que se conectan a ella. También es posible encontrar redes subvencionadas por los respectivos gobiernos, por lo que los centros que se conecten a ellas sólo pagan por la conexión al punto de acceso más cercano.

La forma más sencilla para acceder a Internet es a través de un router/módem ADSL. Con este método se dispone de un acceso completo a Internet a la velocidad contratada con la compañía que presta el servicio.

INTRANET

Intranet es un término relativamente nuevo y puede utilizarse para definir una red privada que utiliza el conjunto de protocolos *TCP/IP* y no está conectada a Internet.

Durante muchos años las redes con protocolos *TCP/IP* accedían a Internet para tener acceso a las múltiples utilidades que estaban disponibles.

A partir de 1994, empezó a ganar adeptos una opción que consistía en utilizar dichos protocolos y las posibilidades que brindaban los servicios disponibles en Internet, pero sin permitir el acceso a Internet. De esta manera surgió el concepto de Intranet.

Gracias a la sencillez de su construcción, de su uso y de su economía, su expansión ha sido muy rápida.

Entre sus múltiples ventajas se encuentran:

- **Interoperabilidad**. Se tiene acceso a todos los servicios de Internet pero restringidos al uso interno de la empresa y a todos los productos de la red.
- **Escalabilidad**. Se puede dar acceso fácilmente a nuevos usuarios de la empresa a dichos servicios sin molestias para los que ya la están utilizando.
- **Seguridad**. Se produce una gran mejora en la seguridad de la red local al evitar el acceso de usuarios no autorizados a nuestros servicios Internet.
- **Disminución de los costes**. Permite una disminución drástica de los costes de correo, papel y de la factura telefónica al simplificar las comunicaciones internas y el intercambio de información.

- **Aumento de la efectividad**. Si está bien diseñada, permite una mejora de la efectividad al tener acceso de forma sencilla a una serie de servicios que simplifican el trabajo y mejoran el tiempo de acceso a la información.

La forma más sencilla para montar una Intranet es a través de una LAN, MAN o WAN.

EXTRANET

El concepto **Extranet** es una mezcla de Internet e Intranet y sirve para definir a una red privada virtual que utiliza a Internet como medio de transporte de la información entre sus propios nodos. También recibe el nombre de **VPN** (**Virtual Private Networks**).

Gracias a una Extranet se pueden unir dos Intranets que se encuentran situadas en distintas ubicaciones utilizando *ADSL*. Una vez en Internet, los datos serán transmitidos por distintas rutas alternativas hasta llegar a la sede destino.

Para evitar la conexión de personas no autorizadas a las Intranets, será necesario contar con cortafuegos (*firewalls*) y *proxies* que autentifiquen los accesos, así como proceder a una encriptación de los paquetes que van a viajar desde una sede a la otra.

De esta manera, se tendrá una gran reducción de costes para la empresa y una alta fiabilidad.

SERVICIOS QUE PUEDEN UTILIZARSE

Basan su utilidad básicamente en cuatro servicios: *groupware*, acceso remoto, transferencia de archivos y páginas *Web*.

Groupware

Se entiende por **groupware** a distintas herramientas que ayudan a las personas a trabajar juntas de forma fácil y eficaz de forma que puedan comunicarse entre ellas, colaborar y coordinarse.

Normalmente, se clasifica el *groupware* en función de la forma en que se va a utilizar cada una de sus herramientas, por lo que se puede dividir de la siguiente manera:

- Herramientas de trabajo conjunto.
- Herramientas de trabajo individual.

Las herramientas de trabajo conjunto comprenden: los programas de calendario y planificación, las teleconferencias, las videoconferencias, los sistemas de reunión electrónica (*EMS*), las pizarras y los programas de conversación (*chat*).

Las herramientas de trabajo individual comprenden: el correo electrónico, los servicios de noticias, las herramientas de escritura en grupo y los programas de flujo de trabajo.

PROGRAMAS DE CALENDARIO Y PLANIFICACIÓN

Los programas de calendario y planificación facilitan el trabajo de planificar las reuniones, avisar a los participantes y solicitar su confirmación de asistencia.

Entre dichos programas se encuentran: *Lotus Notes* y *Microsoft Outlook*.

TELECONFERENCIAS

Las teleconferencias consisten en la utilización de micrófonos y altavoces para que la gente que se encuentre en lugares distintos pueda discutir los temas que considere oportunos.

Entre los programas que permiten su utilización se encuentran: *Microsoft NetMeeting* y *Messenger* (lo hay de distintos proveedores).

VIDEOCONFERENCIAS

Las videoconferencias consisten en la utilización de micrófonos, altavoces y videocámaras para que los participantes en una conversación, además de oír sus voces, puedan ver sus imágenes y las de su entorno.

Entre los programas que permiten su utilización se encuentran: *Microsoft NetMeeting* y *Messenger* (lo hay de distintos proveedores).

SISTEMAS DE REUNIÓN ELECTRÓNICA (EMS)

Estos programas hacen que todos los participantes en una reunión puedan utilizar los ordenadores para exponer sus ideas simultáneamente y llegar, si es necesario, a una votación de forma anónima.

Entre los programas que permiten su utilización se encuentra *Microsoft Office One Note*.

PIZARRAS DE DATOS

Las pizarras de datos permiten que dos o más personas que se encuentran en lugares distintos puedan ver y señalar el mismo documento a la vez. También posibilitan que se puedan guardar los cambios realizados, así como su impresión para cada uno de los participantes.

Entre los programas que permiten su utilización se encuentran: *Microsoft NetMeeting* y *Messenger* (lo hay de distintos proveedores).

PROGRAMAS DE CONVERSACIÓN

Los programas de conversación permiten charlar con otro participante que se encuentre en otro lugar distinto, escribiendo en el teclado y visualizando sus contestaciones en la pantalla del ordenador.

Entre los programas que permiten su utilización se encuentran: *Microsoft NetMeeting* y *Messenger* (lo hay de distintos proveedores).

CORREO ELECTRÓNICO

Con el correo electrónico cada usuario puede contactar con cualquier otro usuario en cualquier lugar del mundo e intercambiar con él información, mensajes, imágenes y archivos.

Es posible enviar correo a una sola persona de una forma sencilla, pero si lo que desea es enviar el mismo mensaje a un grupo de personas, el tener que repetir el mismo mensaje varias veces o el tener que escribir todas las direcciones de las personas que van a recibir el mismo mensaje, resultaría una tarea larga y tediosa.

Para evitarlo existen las listas de distribución que se encargan de redirigir todos los mensajes a todos y cada uno de los miembros de la lista de distribución.

Para acceder a este servicio se pueden utilizar: *Lotus Notes*, *Microsoft Outlook* y *Outlook Express*.

También se puede acceder a servidores de correo Web como, por ejemplo, *Gmail*, *Yahoo* y *Hotmail*.

SERVICIO DE NOTICIAS

Con el servicio de noticias cada usuario puede suscribirse a los temas que le interesen, así como tener acceso, diariamente, a toda la información generada sobre ellos.

Un *servidor de noticias* permite compartir información y crear debates sobre un tema concreto. Actúa igual que un tablón de anuncios en el que los usuarios colocan sus mensajes y contestan a los que están publicados creando varios hilos de comunicación en función de los temas que van saliendo.

Existen dos tipos de grupos de noticias:

- Sin moderador, es decir, todas las noticias se añaden directamente al tablón de anuncios.

- Con moderador. Esto quiere decir que los artículos que envían los usuarios no se añaden automáticamente al grupo de noticias sino que previamente son revisados por un moderador que determina si el artículo tiene interés para publicarse o no. Los grupos de noticias con moderador son más leídos porque el nivel de noticias de baja calidad es mínimo.

Existen muchos servidores de noticias que están replicados en todos los nodos de Internet. De esta forma, sólo es necesario conectarse al servidor de noticias más cercano para poder participar en cualquier debate.

Para acceder a este servicio se pueden utilizar: *Lotus Notes*, *Microsoft Outlook* y *Outlook Express*.

HERRAMIENTAS DE ESCRITURA EN GRUPO

Estos programas permiten a dos o más personas colaborar en la redacción de un mismo documento de forma separada y simultáneamente. Todas las modificaciones realizadas son aceptadas exceptuándose aquellas que han sido hechas por dos o más personas. En estos casos, será el propietario del documento el que determinará los cambios que se guardarán.

Entre los programas que permiten su utilización se encuentran: *Lotus Notes*, *Microsoft NetMeeting* y *Microsoft Office One Note*.

PROGRAMAS DE FLUJO DE TRABAJO

Estos programas permiten estructurar actividades basadas en un conjunto de reglas que controlan el flujo del trabajo. Para ello, se dispone de formularios que, una vez cumplimentado por una persona, se envían a la siguiente persona que debe trabajar con él por medio del correo electrónico que utiliza bases de datos documentales para encaminar la información al lugar a donde debe ir y así sucesivamente hasta la finalización del formulario.

Entre los programas que permiten su utilización se encuentran: *Lotus Notes* y *Microsoft Office One Note*.

Acceso remoto

A través del acceso remoto se puede conectar a otro ordenador o a otra red situada en cualquier parte del mundo, de la misma forma que si se tratara de una estación de trabajo de ella.

Entre los programas que permiten su utilización se encuentran: *Putty* y *WinSCP*.

Transferencia de archivos

Mediante la transferencia de archivos se pueden enviar archivos a otro usuario directamente.

Entre los programas que permiten su utilización se encuentran: *Microsoft NetMeeting* y *Messenger* (lo hay de distintos proveedores).

También se puede utilizar un cliente FTP como *CuteFTP* o *FileZilla* para acceder a un servidor FTP en donde están guardados los archivos.

Páginas Web

Las páginas *Web* básicamente están formadas por texto e imágenes pero pueden añadirse sonidos y vídeos para aumentar su atractivo.

Así mismo, utilizan enlaces que es un método de presentación de información mediante el cual al seleccionar cualquier palabra presente en el texto se puede ampliar la información sobre ella, es decir, cualquier palabra marcada se encuentra enlazada con otros documentos que pueden ser tanto textos como gráficos o sonido.

Mediante este sistema se puede ampliar información sobre cualquier palabra o concepto, avanzando de documento en documento hasta encontrar la información deseada.

El programa cliente que se utiliza recibe el nombre de navegador o explorador y permite al usuario realizar una transferencia de archivos o acceder a documentos que se encuentran en otro servidor *Web*.

Existen varios programas que actúan como clientes del sistema *WWW* y que es preciso tener instalados en el ordenador. La mayor parte son de dominio público y se pueden obtener de forma gratuita a través de Internet. Los más conocidos son *Mozilla* y *Microsoft Internet Explorer*.

Para la creación de páginas *Web* se pueden utilizar, entre otros, los lenguajes de programación *HTML*, *JAVA* y *JAVASCRIPT*, aunque también existen programas que permiten generar las páginas *Web* con cierta facilidad y sin tener grandes conocimientos de programación como son *Microsoft FrontPage y Adobe Dreamweaver*.

INTERNET COMO RED P2P

Últimamente, las siglas **P2P** (**Peer to Peer**, **Punto a Punto**) están incorporadas a la jerga de Internet, en los medios de comunicación y en todos los despachos que tengan relación con ordenadores.

Esta tecnología, por tanto, se basa en intercambios directos de información sin pasar por un servidor. Por tanto, no hay ningún elemento que pudiera hacer algún tipo de control centralizado.

Según esto, se puede decir que se vuelve a los inicios de Internet cuando las grandes universidades se intercambiaban datos de igual a igual. Internet se diseñó inicialmente, con el propósito de intercambiar información entre ordenadores, a través de sus direcciones IP.

Las grandes bases de datos, motores de búsqueda, portales, servidores, etc. han ido apareciendo después, según han ido surgiendo nuevas necesidades y también intereses comerciales o de otro tipo.

P2P representa el triunfo de la descentralización frente al control central. El PC de cualquier usuario, que hasta ahora era un elemento pasivo, únicamente recibiendo información, puede convertirse en un elemento activo, que también puede dar información a otros o participar en algún proceso común, aportando su capacidad de procesamiento. La gente tiene información que quiere compartir con

los demás. Con esta tecnología se está dando más importancia al PC. Esta forma de trabajar se llama "proceso distribuido". Puede ser especialmente útil para la colaboración en tareas muy complejas, que a un ordenador único le costaría demasiado. Más controvertido resulta el intercambio libre de ficheros, obras de arte, música, etc., que están sujetas a leyes de propiedad.

Actualmente, para mandar un archivo por correo electrónico hay que pegarlo en un mensaje, porque aunque los ordenadores estén unidos por una red, no se puede grabar el archivo directamente en el otro ordenador. Con la tecnología P2P se puede mandar información directamente de un ordenador a otro sin tener que pasar por máquinas centrales (servidores) que están en Internet.

Estamos aún en los comienzos de esta tecnología y habrá que resolver problemas como el ancho de banda, que es muy pequeña todavía en muchos usuarios y, sobre todo, la falta de seguridad, etc.

Tecnologías P2P

FREENET

Freenet es una red de comunicaciones entre pares, descentralizada y diseñada para resistir la censura. Utiliza el ancho de banda y espacio de almacenamiento de los equipos de sus miembros para permitir publicar u obtener información de todo tipo en completo anonimato.

Su creador, Ian Clarke, es un apóstol de las fórmulas de intercambio entre iguales y cree que Freenet supone una revolución en la distribución de contenidos. Su idea todavía no se ha traducido en beneficios, a pesar de que cobra por ciertos servicios de almacenamiento y ancho de banda.

Pero la polémica más fuerte gira en torno al carácter ilegal o inmoral de sus contenidos, el 59% de los textos que se intercambian tratan sobre drogas y el 89% de las imágenes son pornográficas.

AIMSTER

Aimster permite el intercambio de archivos uniéndolos a mensajes instantáneos. Para ello, cifra la información y es imposible reconocer qué tipo de archivos están siendo enviados (música, datos, vídeos, etc.).

Actualmente está demandada por las compañías discográficas americanas.

GNUTELLA

Gnutella es, básicamente, una red de ordenadores descentralizada, carente de servidor central.

No se trata de un programa, es más bien una tecnología, un protocolo que permite interconectar ordenadores que estén "escuchando" señales enviadas desde otros equipos. Va de usuario en usuario buscando la información que necesita, esto hace que la búsqueda sea muy laboriosa y si las comunicaciones entre ellos son muy lentas el proceso se puede colapsar. A pesar de sus siglas iniciales GNU, no está claro que sea un programa de código libre y abierto.

JABBER

Jabber es un protocolo libre para mensajería instantánea, basado en el estándar XML.

La red de Jabber está formada por miles de grandes y pequeños servidores en todo el mundo, interconectados por Internet. Habitualmente la red es utilizada por alrededor de un millón de personas.

Es el proyecto más aceptado como la alternativa libre al sistema **Messenger**. Aunque es un protocolo bastante minoritario, está creciendo más cada día, gracias a los usuarios y a Google, que ha creado un cliente de mensajería instantánea que utiliza Jabber, **Google Talk**.

NAPSTER

Napster, aún no siendo estrictamente un programa P2P (hay algún servidor central entre los usuarios), es el programa que ha revolucionado el panorama de Internet.

El intercambio de música libremente, sin tener en cuenta los derechos de autor, ha hecho poner el grito en el cielo a las industrias discográficas que han demandado a esta compañía.

Napster guarda una relación de la música que ofrecen todos sus usuarios, él directamente no la ofrece, solamente hace de intermediario.

La juez encargada del caso ha obligado a Napster a parar este intercambio gratuito. Ha habido varias sentencias que han afectado a otras compañías que también pueden quedar al margen de la ley. En este caso se encuentra el programa *Aimster,* combina mensajería con intercambio de ficheros, o *IMesh*, de origen israelí y muy extendido. Estos programas, para no ser demandados como en el caso

de Napster, permiten sólo un intercambio entre amigos, cosa que legalmente no está tan clara que sea ilegal como en el caso anterior.

EMULE

eMule es un programa para intercambio de archivos con sistema P2P utilizando el protocolo eDonkey 2000 y la red Kad, publicado como software libre para sistemas Microsoft Windows.

Creado en un principio como alternativa al programa eDonkey, en poco tiempo lo superó en funciones, y sumando el hecho de que era libre y gratuito, entre otros motivos, lograron que en poco tiempo lo superase en popularidad para convertirse en uno de los programas más usados por los usuarios de P2P. Existen también múltiples programas derivados con el objetivo de portarlo a otros sistemas operativos, como lMule, xMule o aMule.

Sus principales características son:

- Intercambio directo de archivos entre sus clientes.
- Recuperación rápida de partes corruptas.
- Usa un sistema de créditos por el cual quien más sube a la red más descarga, si bien puede funcionar también con este sistema desactivado.

BITTORRENT

BitTorrent es un protocolo diseñado para el intercambio de archivos entre iguales.

A diferencia de los sistemas de compartición de ficheros tradicionales, su principal objetivo es el proporcionar una forma eficiente de distribuir un mismo fichero a un gran grupo de personas, forzando a todos los que descargan un fichero a compartirlo también con otros.

Para ello, primero se distribuye por medios convencionales un pequeño fichero con extensión *.torrent*. Este fichero es estático, por lo que se suele encontrar en páginas web, y contiene la dirección de un servidor de búsqueda, que se encarga de localizar posibles fuentes con el fichero o parte de él.

Este servidor realmente se encuentra centralizado y provee estadísticas acerca del número de transferencias, el número de nodos con una copia completa del fichero y el número de nodos que posee sólo una porción del mismo.

El fichero deseado es descargado de las fuentes encontradas por el servidor de búsqueda y, al mismo tiempo que se realiza la descarga, se comienza a subir las partes disponibles del fichero a otras fuentes, utilizando el ancho de banda asignado a ello. De esta manera, cada nodo inevitablemente contribuye a la distribución de dicho fichero. El sistema se encarga de favorecer a quienes compartan más, por lo que, a mayor ancho de banda, mayor será el número de conexiones a nodos de descarga que se establecerán.

Cuando un usuario comienza la descarga de un fichero, BitTorrent no comienza necesariamente por el principio del fichero, sino que se baja por partes al azar. Luego los usuarios se conectan entre sí para bajar el fichero. Si entre los usuarios conectados se dispone de cada parte del fichero completo (aun estando dividido), finalmente todos obtendrán una copia completa de él. Por supuesto, inicialmente alguien debe poseer el fichero completo para comenzar el proceso. Este método produce importantes mejoras en la velocidad de transferencia cuando muchos usuarios se conectan para bajar un mismo fichero. Cuando no existan ya más nodos con el fichero completo (semillas o *seeds*) conectados al servidor de búsqueda, existe la posibilidad de que el fichero no pueda ser completado.

POSIBILIDADES DE FUTURO

Durante los últimos años se ha experimentando la entrada de un fenómeno llamado Internet.

De forma similar a la evolución de la telefonía móvil (que ha originado una nueva forma de comunicación entre las personas), mediante el uso de Internet se han conseguido nuevas formas de comunicación y de colaboración tanto en el terreno personal como laboral.

Hasta la irrupción de Internet, básicamente se utilizaban tres formas de comunicación: la oral, la telefónica y la epistolar. Si se analizan cada una de estas, se observa lo siguiente:

- Mediante la comunicación oral, se consigue un medio *interactivo* y de *realimentación* inmediata entre los interlocutores. Muchas veces es necesario establecer un espacio tanto temporal como físico para poder llevar a cabo el encuentro, lo que no siempre es posible si los interlocutores se encuentran en lugares muy distantes o tienen dificultades de movilidad.

- Mediante la comunicación telefónica, los interlocutores tienen una comunicación similar a la oral, pero se pierden ciertos aspectos de *comunicación gestual*, que durante una comunicación oral sí son

explícitos. Una ventaja de esta comunicación es que no existen barreras espaciales. Pero no se permite la transferencia de documentación utilizando este medio (para evitar en parte este problema se utiliza el fax).

- Mediante la comunicación epistolar, se tiene un medio no interactivo de comunicación, ya que el origen de la comunicación envía su mensaje y la forma de transmisión de dicho mensaje hace que su recepción y la respuesta no sean inmediatas. Un factor importante a tener en cuenta en este tipo de comunicación es la *distancia entre los puntos de comunicación*. Sin embargo, a diferencia de la comunicación telefónica, esta sí permite el envío de documentación adjunta.

Con Internet se consiguió salvar la distancia geográfica, ya que mediante esta red (al igual que con la telefónica) se permite la comunicación simultánea de personas situadas en puntos muy distantes. Además se mejoran ciertos aspectos ya que permite la transferencia de todo tipo de documentación, tanto textual como multimedia. Sin embargo no se consigue transmitir la expresión gestual o la intencionalidad del texto que se comunica. La comunicación puede ser escrita (como en el caso del chat y del correo electrónico) o bien visual (como las conexiones de videoconferencia o las retrasmisiones utilizadas últimamente, el streaming).

Además gracias a la popularidad de la tecnología informática y su rápida expansión por todo el mundo, cada vez existen más utilidades y aplicaciones para facilitar la comunicación, se trabaja en entornos universitarios junto con grandes organismos en el diseño de traductores simultáneos y lenguajes naturales que faciliten el uso y el trabajo conjunto de distintas sociedades lingüísticas para fines comunes.

Además, Internet se ha convertido en la gran biblioteca universal, cualquier información que se necesite sobre cualquier tema, se puede localizar mediante los **buscadores**. Esta capacidad de la red, como en todas las disciplinas, puede ser un arma de doble filo, en cuanto a la privacidad o no de ciertos datos, pero a la vez permite un nivel nunca visto antes de aproximación a muy diversos temas, ya que la red contiene todo.

Los gobiernos están haciendo grandes progresos en el desarrollo de plataformas para proveer de servicios *online* a sus ciudadanos. Cada vez se trabaja más en el estudio de formas de identificación remota de los individuos, protocolos de seguridad y firma electrónica. Poco a poco la legislación se va ajustando a los requerimientos que esta nueva red con tanta información requiere, poniendo las limitaciones jurídicas y penales necesarias según el uso que se haga de ella.

CONFIGURAR UN NAVEGADOR (PARTE PRÁCTICA)

La función de un navegador es la de enviar peticiones de archivos a un servidor *Web* y visualizar la información recibida en la estación de trabajo.

La información que se puede mostrar en un navegador son textos, imágenes, sonido, vídeo, etc. Así mismo, pueden utilizarse también para introducir datos sobre formularios y transmitirlos al servidor.

A continuación, se mostrará una breve descripción del explorador que incorpora Windows XP.

Para acceder al navegador, ha de ejecutar **Internet Explorer** desde la barra de inicio rápido o desde **Todos los programas** del menú **Inicio** (previamente, habrá que haber realizado la configuración de la conexión que se va a utilizar), y aparecerá la página de inicio (si es la primera vez, le mostrará una pantalla de aviso en la que le indica que está habilitada la seguridad mejorada en el servidor. Active la casilla **No volver a mostrar este mensaje** y pulse en *Aceptar*).

Esta página es la que está indicada en la configuración como página de inicio (puede modificarse desde **Opciones de Internet** del menú **Herramientas**).

Para poder acceder a otras páginas *Web*, deberá indicar en el apartado **Dirección** los datos correspondientes a la página que desea visualizar.

Por ejemplo, para acceder al servidor *Web* de *Microsoft* en España, deberá escribir *http://www.microsoft.com/Spain*, pulsar [**Intro**] y verá la pantalla siguiente:

Le indica que la página a la que está intentando acceder no se encuentra catalogada como sitio de confianza y la configuración de seguridad estará muy restringida. Puede actuar de dos maneras:

- Si pulsa en **Cerrar**, mantendrá dicha configuración.

- Si pulsa **Agregar**, verá la pantalla siguiente:

Si ahora pulsa en **Agregar**, el sitio pasará a la lista inferior que es donde se encuentran los sitios de confianza y, entonces, la configuración de seguridad será menor.

Cuando haya finalizado, pulse en **Cerrar** dos veces y se cargará la página indicada.

La interfaz del navegador es bastante sencilla de utilizar, está formada por la ventana de navegación (donde se muestran las páginas *Web*), el menú principal de la aplicación y tres barras de utilidades: la de herramientas, la de estado y la del explorador.

Desde el menú principal de la aplicación se pueden realizar todas las acciones que se necesiten (las opciones del menú se muestran en resaltado al situar el puntero del ratón sobre ellas). Este menú principal es muy similar al utilizado en cualquier aplicación de *Microsoft*.

Las barras de herramientas están situadas debajo del menú principal. Constan de una serie de botones que simplifican las acciones a realizar para navegar por las páginas *Web*. A su vez, están formadas por:

- Los **botones estándar** que son los iconos que se ven en dicha barra.
- Las **etiquetas** que son los nombres de cada uno de los iconos anteriores.
- La **barra de direcciones** que sirve para escribir la dirección *URL* de la página que se está mostrando. Se puede introducir directamente la dirección *URL* de una página en este campo (tiene la capacidad de completar la dirección si la encuentra en su historial).
- Los **vínculos** que es un botón que, al pulsar en el signo que hay a su derecha, mostrará los sitios *Web* que se han indicado como de mayor acceso.

- Para añadir entradas se ha de pulsar el icono con forma de **E** que hay en la barra de direcciones a la izquierda de la dirección **URL** de la página deseada y, sin soltarlo, situarlo sobre la palabra **Vínculos**.

- Para eliminarlas hay que situarse encima del vínculo que se desea quitar, pulsar el botón derecho del ratón y seleccionar **Eliminar**.

Una de las opciones más interesantes que presenta este navegador es la posibilidad de ver las páginas *Web* favoritas (en este navegador se llaman **Favoritos**), el historial de páginas visitadas (**Historial**) y la posibilidad de buscar páginas (botón **Búsqueda**), como un panel en la ventana del explorador.

Pulsando cualquiera de estos botones, la ventana del explorador se divide en dos paneles. En el de la derecha se podrá ver la página *Web* actual y en el de la izquierda se mostrará una columna que dependerá de la opción elegida.

Otra característica interesante en este navegador es la posibilidad de mostrar la barra de botones de distintas maneras (con botones grandes o pequeños, pudiéndose mostrar también sin texto si se selecciona **Personalizar** de la opción **Barra de Herramientas** del menú **Ver**).

El icono **Imprimir** realiza la impresión de la página actual pero desde la opción **Imprimir** del menú **Archivo** se puede elegir imprimir los documentos vinculados e, incluso, si una página está formada por varios marcos, se podrá elegir cómo realizar la impresión.

Cómo desplazarse por las páginas

Cuando se encuentre dentro de una página, verá que puede haber palabras que se encuentran destacadas u opciones de menú (al situarse sobre cualquiera de ellas, el puntero del ratón cambiará de forma a una mano con el dedo índice extendido). Cuando pulse el botón izquierdo del ratón sobre dicha palabra, se mostrará la página con la que tiene establecido el vínculo.

Si pulsa el icono de la barra de herramientas que tiene forma de flecha con la punta hacia la izquierda (**Atrás**), retrocederá a la página anterior visitada y si lo hace sobre el icono con forma de flecha con la punta hacia la derecha (**Adelante**), volverá de nuevo a la página.

Para volver a la página de inicio, marque el quinto icono de la izquierda (**Inicio**).

Si una página tarda mucho en mostrarse, puede pulsar el tercer icono de la izquierda para detener el proceso (**Detener**) y si desea volver a reiniciarlo, pulse el cuarto icono de la izquierda para actualizar la información (**Actualizar**).

Cómo buscar texto dentro de una página

Para buscar un texto dentro de la página, abra el menú **Edición**, seleccione **Buscar en esta página**, escriba el texto que desee y marque **Buscar siguiente** las veces que sean necesarias hasta llegar al lugar adecuado.

Cómo cambiar el tamaño de la fuente

Para poder cambiar el tipo de letra a una fuente distinta, abra el menú **Ver**, seleccione **Tamaño de texto** y elija el tamaño que desee.

Cómo guardar el contenido de la página

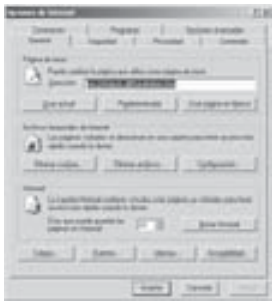
Si abre el menú **Archivo** y selecciona **Guardar como**, podrá guardar la página como un archivo en su propio ordenador para verlo posteriormente con el navegador.

También puede seleccionar el texto que desee para cortarlo, copiarlo y pegarlo en cualquier procesador de textos, seleccionándolo y utilizando las tres primeras opciones del menú **Edición**.

Si pulsa sobre el icono **Imprimir**, imprimirá el contenido de la página activa.

Personalización de Internet Explorer

Utilizando el menú **Herramientas** del menú principal y seleccionando **Opciones de Internet**, se abrirá la ventana de configuración:



Usando las diferentes fichas de la ventana se pueden configurar todas las opciones de este navegador:

- En la ficha **General**:

  En ella se ha de indicar la **Dirección** de la **Página de inicio** (es la página que se verá cada vez que se inicie el programa).

  Si pulsa en **Usar actual**, indicará la página que actualmente tiene en pantalla; si pulsa en **Predeterminada**, volverá a escribir la que tiene por defecto y si pulsa en **Usar página en blanco**, tendrá como página principal una página *HTML* en blanco.

  Si pulsa en **Eliminar archivos** del apartado **Archivos temporales de Internet**, eliminará todo el contenido de la carpeta o carpetas en donde se guardan los archivos con las páginas visitadas para tener un acceso más rápido a ellas.

  Si pulsa en **Eliminar cookies**, eliminará todos los archivos creados por los sitios *Web* en el equipo donde almacenan información como las preferencias al visitar dicho sitio.

  - Si pulsa en **Configuración**, verá la siguiente pantalla:

    En ella podrá indicar si desea que, al actualizar páginas que ya ha visto, compruebe si ha cambiado **Cada vez que se visita la página**, **Cada vez que se inicia Internet Explorer**, **Automáticamente** o no lo haga **Nunca**.

    Puede especificar el porcentaje de espacio en disco que desea utilizar para la **carpeta Archivos temporales de Internet**, **Mover carpeta** para cambiar la ubicación de dicha carpeta, **Ver archivos** para ver el contenido de dicha carpeta o **Ver objetos** para ver la carpeta **Downloaded Program Files** que se encuentra en la carpeta *Windows* que es donde se encuentran los controles **ActiveX** que se han descargado al ordenador.

    Si pulsa en **Aceptar** volverá a la pantalla anterior.

En el bloque **Historial** podrá indicar los días que desea guardar los vínculos a las páginas ya visitadas.

Si pulsa en **Borrar Historial**, vaciará la carpeta en donde se guardan dichos vínculos.

Si pulsa en **Colores**, podrá cambiar los colores predeterminados para el texto y fondo.

Si pulsa en **Fuentes**, podrá cambiar las fuentes que se van a utilizar para ver las páginas *Web*.

Si pulsa en **Idiomas**, podrá cambiar el idioma o idiomas fuentes que va a utilizar para ver las páginas *Web*.

Si pulsa en **Accesibilidad**, podrá conservar e indicar los colores, fuentes y estilos que sustituirán siempre a la del sitio *Web*.

- Si pulsa en la ficha **Seguridad**, verá la pantalla siguiente.

En ella puede indicar distintas configuraciones de niveles de seguridad para las diferentes zonas *Web* a las que se conecta.

En la ventana superior se muestran las posibles zonas de seguridad:

- **Internet**. Es la que se utiliza por defecto cuando el sitio *Web* no está incluido en otra zona. Su nivel de seguridad es mediano.

- **Intranet local**. Corresponde a los sitios *Web* con los que se tiene establecida una conexión directa. Su nivel de seguridad es mediano.

- **Sitios de confianza**. Comprende los sitios *Web* que no van a causar ningún problema. Su nivel de seguridad es bajo.

- **Sitios restringidos**. Comprende los sitios *Web* peligrosos. Su nivel de seguridad es alto.

Si selecciona una zona y pulsa en **Sitios**, pasará a una pantalla en donde podrá definir qué sitios *Web* quiere incluir en la zona elegida:

Cuando haya finalizado, pulse en **Cerrar** para volver a la pantalla anterior.

Si selecciona una zona y pulsa en **Nivel personalizado**, verá la siguiente pantalla:

En ella podrá indicar la configuración de seguridad que desea proporcionar a la zona elegida.

Cuando haya finalizado, pulse en **Aceptar**.

Si pulsa en **Nivel predeterminado**, volverá a establecer los valores que había configurados por defecto para la zona.

- Si pulsa en la ficha **Privacidad**, verá la pantalla siguiente:

En ella podrá indicar la configuración de los **cookies** para la zona seleccionada.

Si pulsa en la barra deslizante que se encuentra en la parte izquierda, cambiará la configuración de privacidad para dicha zona.

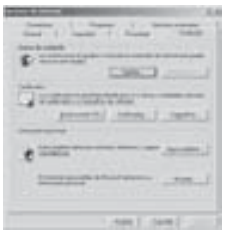
Si pulsa en **Importar**, podrá importar un archivo de privacidad personalizado de organizaciones de privacidad u otros sitios de Internet (deberá indicar su nombre).

Si pulsa en **Opciones avanzadas**, podrá personalizar el manejo de los *cookies* que hará el navegador. Cuando haya finalizado, pulse en *Aceptar*.

Si pulsa en **Predeterminada**, restablecerá el nivel de privacidad al predeterminado para la zona.

Si pulsa en **Editar**, verá una pantalla donde podrá indicar los sitios *Web* a los que se les permitirá o bloqueará, utilizar *cookies* sin importar qué directiva de privacidad tenga la zona. Cuando haya finalizado, pulse en **Aceptar**.

- Si pulsa en la ficha **Contenido**, verá la pantalla siguiente:



En el apartado **Asesor de contenido**, si pulsa en **Habilitar**, verá una pantalla donde podrá indicar el contenido de las páginas *Web* que permite visitar. De esta manera, antes de visitar una página *Web* se comprobará si está clasificada y si su categoría corresponde con las que se han permitido (el inconveniente es que hay pocas compañías que han solicitado la clasificación).

En el caso de que la página *Web* no tenga clasificación o esté fuera de las permitidas, mostrará una pantalla en donde le pedirá la contraseña que puso cuando activó el **Asesor de contenido** (si no se indica la contraseña correcta, no permitirá ver el contenido de la página).

Si selecciona una **categoría RSACi** (**Recreational Software Advisory Council on the Internet**), deberá indicar en la barra deslizante el nivel de restricciones que desea poner a dicha categoría.

Cuando haya finalizado, pulse en **Aceptar** para volver a la pantalla anterior (deberá indicar y confirmar una contraseña. Es conveniente que indique una sugerencia que le ayude a recordar la contraseña, si fuera necesario). Le mostrará una pantalla de aviso en donde le indica que se ha activado el asesor de contenido.

Podrá volver a la pantalla de restricciones, si pulsa en **Configuración** (deberá escribir la contraseña que indicó anteriormente).

Si desea quitar las restricciones, pulse en **Deshabilitar** e indique la contraseña que puso cuando habilitó el asesor de contenido. Le mostrará una pantalla de aviso en donde le indica que acaba de desactivarlo.

El apartado **Certificados** se utiliza para identificarse a sí mismo, a las autoridades emisoras de certificados o compañías de *software*. Los certificados se expiden por una agencia de credenciales que garantiza la identidad de un sitio *Web*, de un usuario o de un *software*. La agencia de credenciales más importante es **Verisign**.

Si pulsa en **Borrar estado SSL**, quitará todos los certificados de autenticación de cliente de la caché de *SSL*, ya que de otro modo, puede permanecer en la caché hasta que se reinicie el equipo.

Si pulsa en **Certificados**, verá la lista de certificados que se pueden utilizar para la autenticación de los usuarios. Esta autenticación se utiliza para conectarse a un sitio *Web* sin necesidad de contraseña ya que se comprueba la identidad mediante el certificado digital. En dicha pantalla podrá realizar las siguientes acciones:

- Si pulsa en **Avanzadas**, podrá establecer distintas opciones como los propósitos del certificado o el formato de exportación. Cuando haya finalizado, pulse en **Aceptar**.

- Si pulsa en **Importar**, traerá un certificado (junto con sus claves) que se encuentra en un archivo (deberá indicar su nombre).

- Si selecciona un certificado y pulsa en **Exportar**, guardará el certificado seleccionado en un archivo.

- Si selecciona un certificado y pulsa en **Quitar**, se eliminará de la lista.

- Si selecciona un certificado y pulsa en **Ver**, mostrará las características del certificado.

Cuando haya finalizado, pulse en **Cerrar** para volver a la pantalla anterior.

Si pulsa en la ficha **Compañías**, verá los editores de confianza en los que confía para recibir *software* certificado (para añadir una entrada, deberá instalar un control *ActiveX* de una compañía). En dicha pantalla podrá realizar las siguientes acciones:

- Si pulsa en **Avanzadas**, podrá establecer distintas opciones como los propósitos del certificado o el formato de exportación. Cuando haya finalizado, pulse en **Aceptar**.

- Si pulsa en **Importar**, traerá un certificado (junto con sus claves) que se encuentra en un archivo (deberá indicar su nombre).

- Si selecciona un certificado y pulsa en **Exportar**, guardará el certificado seleccionado en un archivo.

- Si selecciona un certificado y pulsa en **Quitar**, se eliminará de la lista.

- Si selecciona un certificado y pulsa en **Ver**, mostrará las características del certificado.

Cuando haya finalizado, pulse en **Cerrar**.

En el apartado **Información personal** se indican los datos que se enviarán cuando un sitio *Web* solicite información al visitar sus páginas.

Si pulsa en **Mi perfil**, pasará a una pantalla en donde deberá indicar la entrada de la libreta de direcciones del correo electrónico que desea que se envíe. Cuando haya finalizado, pulse en **Aceptar**.

Si pulsa en **Autocompletar**, podrá indicar la configuración que desea para la información personal que se va a enviar.

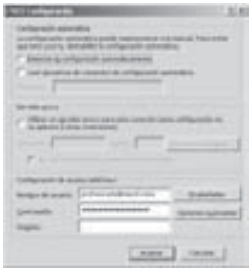
- Si pulsa en la ficha **Conexiones**, verá una pantalla parecida a la siguiente:

En ella se encuentran las siguientes opciones:

- **Instalar**. Activa el **Asistente para conexión nueva** (con él se podrá establecer fácilmente la conexión).

En el apartado **Configuración de acceso telefónico…** muestra las distintas conexiones de acceso telefónico que hay configuradas en el equipo. Puede activar, desactivar o modificar las que desee. También puede activar las casillas que se aplicarán a las distintas conexiones.

- Si pulsa en **Configuración…**, verá la pantalla siguiente:



En ella puede indicar si desea detectar la configuración automática y si desea utilizar un servidor *proxy* para las conexiones de acceso telefónico.

En el apartado **Servidor proxy** se encuentran las siguientes opciones:

- **Utilizar un servidor proxy…** Al activar esta casilla, está indicando que va a utilizar una barrera de seguridad entre su red local e *Internet*. De esta manera, evitará que personas externas a su red local puedan tener acceso a la información que se encuentra en su equipo.

Deberá indicar la **dirección** *URL* y el número de **puerto** del servidor *proxy* que desea utilizar para tener acceso a *Internet*.

- También deberá indicar en **No usar servidor proxy para direcciones locales** si desea utilizar sólo el servidor *proxy* para tener acceso a *Internet* o también desea usarlo para el acceso a la intranet.

- Si pulsa en **Opciones avanzadas**, verá la siguiente pantalla:

En ella deberá indicar la dirección *URL* del servidor *proxy* y el número de puerto que va a utilizar para cada tipo de servidor (si activa la casilla **Usar el mismo servidor proxy para todos los protocolos**, automáticamente pondrá la dirección y el número de puerto que puso en la pantalla anterior).

En la ventana **Excepciones** deberá indicar las direcciones *URL* que no van a utilizar el servidor *proxy*.

Cuando haya finalizado, pulse en **Aceptar** dos veces para volver a la pantalla anterior.

En el bloque **Configuración de acceso telefónico**, deberá indicar el nombre de usuario que le ha asignado el proveedor de servicios, su contraseña y el dominio asignado a la cuenta (si lo solicita el proveedor de servicios).

Si pulsa en **Propiedades**, verá la pantalla de propiedades de la conexión telefónica utilizada para poder cambiar su configuración. Cuando haya finalizado, pulse en **Aceptar**.

Si pulsa en **Opciones avanzadas**, verá una nueva pantalla donde podrá cambiar la configuración de los intentos de conexión y cuándo realizar la desconexión. Cuando haya acabado, pulse en **Aceptar**.

Cuando haya finalizado, pulse en **Aceptar** para volver a la pantalla **Opciones de Internet**.

Si pulsa en **Configuración de LAN**, verá una nueva pantalla donde puede indicar si desea detectar la configuración automática y si desea utilizar un servidor *proxy* para las conexiones a través de la red local. Es parecida a la descrita en **Configuración…** y no se aplicará a las conexiones de acceso telefónico. Cuando haya acabado, pulse en **Aceptar**.

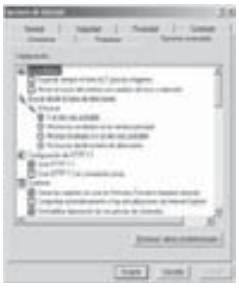
- Si pulsa en la ficha **Programas**, verá una nueva pantalla.

  En el apartado **Programas de Internet**, deberá indicar los programas que se van a utilizar para el **editor HTML**, el **correo**, los **grupos de noticias**, la **llamada por Internet**, etc.

  Si pulsa en **Restablecer configuración Web**, estará indicando que desea restablecer los valores por defecto que tuviera *Internet Explorer* (esta opción únicamente es válida cuando se haya instalado otro explorador después de *Internet Explorer* y hubiera cambiado la configuración predeterminada).

  Si activa la casilla **Comprobar si Internet Explorer es el explorador predeterminado**, estará indicando que desea seguir utilizando este explorador como predeterminado incluso aunque haya instalado otro.

- Si pulsa en la ficha **Opciones avanzadas**, verá la pantalla siguiente:



  En ella podrá modificar la configuración por defecto de **Internet Explorer**.

CONFIGURAR EL CORREO ELECTRÓNICO (PARTE PRÁCTICA)

Con la mensajería podrá enviar y recibir correo electrónico dentro y fuera de su red, así como intercambiar información, mensajes, imágenes y archivos con él.

Windows XP incorpora **Outlook Express** para gestionar el correo electrónico de *Internet* así como acceder a los grupos de noticias e intercambiar mensajes con ellos.

Es importante hacer constar que antes de poder utilizar esta utilidad es necesario disponer de una cuenta en un servidor de correo. Si no dispone de ella deberá ponerse en contacto con un proveedor de acceso a *Internet* o solicitarla a su administrador de la red (si cuenta con un servidor de correo).

Cómo iniciar la mensajería

Para iniciar la mensajería, ejecute la opción **Outlook Express** de **Todos los programas** del menú **Inicio** y verá la pantalla principal de la utilidad.

En ella se observan varias partes diferenciadas:

- **La barra de menús** que es similar a la de todas las aplicaciones Windows.
- **La barra de herramientas** que cuenta con varios iconos que le permitirán realizar distintas operaciones.
- **La lista de carpetas** que se encuentra a la izquierda del centro de la pantalla y muestra todas las carpetas de correo. Siempre hay una carpeta activa que se encuentra resaltada.
- **La lista de mensajes** que se encuentra en la parte superior derecha del centro de la pantalla y muestra la lista de mensajes que hay almacenados en la carpeta activa.
- **Panel de vista previa** que se encuentra en la parte inferior derecha del centro de la pantalla y muestra las primeras líneas del mensaje seleccionado en la **Lista de mensajes**.
- **Contactos** que se encuentra en la parte inferior izquierda del centro de la pantalla y muestra los primeros contactos de la **Libreta de direcciones**.

Las carpetas de correo

Las carpetas que se crean en el proceso de la instalación son cinco:

- **Bandeja de entrada**. Es donde se encuentra el correo que recibe el usuario. Desde aquí es posible responder un mensaje, moverlo a otra carpeta o eliminarlo.

- **Bandeja de salida**. Es donde se encuentra temporalmente el correo enviado a otros usuarios hasta que se realice su entrega (a no ser que tenga activada la casilla **Enviar mensajes inmediatamente** de la ficha **Enviar** de la entrada **Opciones** del menú **Herramientas**).

- **Elementos enviados**. Contiene una copia de los mensajes enviados.

- **Elementos eliminados**. Contiene una copia de los mensajes borrados. Desde aquí es posible recuperar un mensaje que hubiera sido eliminado.

- **Borrador**. Esta carpeta se utiliza para guardar los mensajes que no se han acabado de redactar y, por tanto, no se han enviado.

Es posible crear las carpetas que se deseen con la opción **Carpeta** de **Nuevo** del menú **Archivo**.

Cómo configurar una cuenta de correo nueva

Lo primero que ha de hacer cuando entre por primera vez en esta utilidad, es configurarla para que pueda acceder al servidor de correo.

Para configurar una cuenta de correo siga los pasos siguientes:

1. Abra el menú **Herramientas**, seleccione la opción **Cuentas**, marque **Agregar** y, después, **Correo**. Entrará en el **Asistente para la conexión a Internet** que le ayudará a configurar la cuenta (si es la primera cuenta, le llevará directamente a dicho asistente cuando acceda a la utilidad y seleccione cualquier bandeja). Verá la siguiente pantalla:

2. Deberá indicar el nombre completo que será el que verán los usuarios cuando reciban sus mensajes. Cuando haya finalizado, pulse en *Siguiente* y verá la pantalla:

Indique su dirección de correo electrónica que será la que se enviará a los usuarios con sus mensajes y la que se utilizará cuando ellos respondan a sus mensajes. Cuando haya finalizado, pulse en **Siguiente** y verá la pantalla:

3. Primero deberá indicar si su servidor de correo entrante es **POP3**, **IMAP** o **HTTP**. La diferencia entre ellos está en el protocolo utilizado:

   - **POP3** (**Post Office Protocol versión 3**) es un protocolo de recepción de mensajes que actúa enviando los mensajes completos cuando el usuario se conecta al servidor de correo y, después, los borra de dicho servidor.

   - **IMAP** (**Internet Mail Access Protocol**) es un protocolo de recepción de mensajes que actúa enviando únicamente la cabecera de los mensajes recibidos cuando el usuario se conecta al servidor de correo y mantiene los mensajes completos para que el usuario decida lo que desea hacer con ellos (transferirlo a su ordenador, mantenerlo en el servidor o borrarlo). Este protocolo es más rápido al leer el correo nuevo que **POP3** porque sólo transfiere las cabeceras pero cuenta con el inconveniente de que no se puede usar el filtrado de correo.

   - **HTTP**. Utiliza este protocolo de página *Web* para soporte del servicio de correo.

4. Una vez que haya indicado el tipo de servidor, deberá escribir el nombre del servidor o su dirección *IP* en **Servidor de correo entrante**.

5. Si utiliza el protocolo *POP3* o *IMAP*, deberá indicar el nombre o la dirección *IP* del servidor de correo saliente (puede ser el mismo que el servidor de correo entrante). Este servidor utiliza el protocolo **SMTP** (**Simple MailTransfer Protocol**). Cuando haya finalizado, pulse en **Siguiente** y verá la pantalla:

6. Deberá indicar el nombre de usuario y la contraseña que tiene para acceder a su cuenta en el servidor de correo. Cuando haya finalizado, pulse en **Siguiente** y verá la pantalla de finalización.

7. Pulse en **Finalizar** y volverá a la pantalla de **Cuentas de Internet** (fíjese que la nueva cuenta figura en la lista).

8. Cierre la ventana de cuentas.

Cómo enviar correo

Para enviar correo, marque el icono **Correo nuevo** de la barra de herramientas y verá una pantalla preparada para escribir el mensaje.

En el apartado **De** indica la cuenta por defecto que va a utilizar para el mensaje que está redactando (si pulsa en el triángulo que hay a la derecha del apartado, podrá modificarla). Este apartado únicamente aparecerá si hay creadas más de una cuenta de correo en el equipo.

En el apartado **Para**, deberá indicar el destinatario o destinatarios del mensaje. Si no sabe el nombre exacto, pulse en el icono de la izquierda del campo y verá la libreta de direcciones. Seleccione un usuario de la ventana de la izquierda y marque **Para** (repita el proceso con todos los usuarios a los que desea enviar el mensaje). Cuando haya finalizado, pulse en *Aceptar* y ya estará escrito el nombre o los nombres de los usuarios a los que va a enviar el mensaje.

En el apartado **Cc** (copia de cortesía), indicará el usuario o los usuarios a los que, aunque no sean receptores del mensaje, desea enviárselo para que tengan conocimiento de su envío (siguiendo el mismo proceso indicado en el párrafo anterior pero marcando **Cc** en lugar de **Para**).

En el apartado **Cco** (copia de cortesía oculta), indicará el usuario o los usuarios a los que, aunque no sean receptores del mensaje, desea enviárselo para que tengan conocimiento de su envío pero sin que los demás receptores del mensaje sepan que se le ha enviado a este o estos usuarios (siguiendo el mismo proceso indicado en el párrafo anterior pero marcando **Cco** en lugar de **Para**. Si este apartado no aparece inicialmente, lo hará cuando seleccione un contacto como se ha indicado en este párrafo).

En el apartado **Asunto**, deberá indicar el título que desea dar al mensaje que va a enviar.

En el cuerpo central, deberá escribir el texto que desea incorporar al mensaje.

Puede insertar un archivo. Para ello, marque el octavo icono empezando por la izquierda, indique el nombre del archivo que desea enviar y pulse en **Adjuntar**.

Si selecciona **Establecer prioridad** del menú **Mensaje**, podrá indicar el tipo de importancia (alta, normal o baja) que desea dar al mensaje.

Para enviar el correo, pulse en el icono **Enviar** y el mensaje se enviará directamente o se depositará en la **Bandeja de salida** hasta que establezca la conexión con Internet y seleccione **Enviar y recibir** del menú **Herramientas** (también puede hacerlo marcando en el icono **Enviar y recibir** de la barra de herramientas).

Cómo leer el correo recibido

Para leer el correo recibido, deberá estar situado en la **Bandeja de entrada**. Una vez situado en ella, verá la lista de los mensajes recibidos.

En dicha lista se muestran los siguientes datos (de izquierda a derecha): la prioridad del mensaje (un cierre de admiración indica alta prioridad, una flecha hacia abajo indica baja prioridad y si no hay ninguna de las dos anteriores, es prioridad normal), si lleva objetos incluidos (se indica con un clip), el remitente del mensaje, el asunto de que trata, la fecha y hora en que fue recibido.

Si se sitúa sobre uno de ellos, verá en la parte inferior de la pantalla las primeras líneas del mensaje y si pulsa dos veces el botón izquierdo del ratón, pasará a una pantalla en donde se muestran los datos del mensaje recibido.

Si pulsa en el icono **Imprimir**, el mensaje se imprimirá.

Si abre el menú **Archivo** y selecciona **Guardar como**, guardará el mensaje en un archivo de una carpeta del disco duro (deberá indicar ambos).

Si pulsa en el icono **Eliminar**, se borrará el mensaje sin guardarlo (y sin pedirle confirmación).

Si pulsa en el icono **Responder al remitente**, responderá al usuario que envió el mensaje (enviándole su mensaje entrante también).

Si pulsa en el icono **Responder a todos**, responderá a todos los destinatarios del mensaje (enviándoles el mensaje entrante también).

Si pulsa en el icono **Reenviar**, dirigirá el mensaje a otro u otros usuarios (enviándoles el mensaje entrante también).

Si en el apartado **Adjuntar** indica un nombre, es que tiene insertado un archivo. Si se sitúa sobre dicho nombre y pulsa el botón derecho del ratón, verá su menú contextual. Podrá abrirlo, imprimirlo, guardarlo en un directorio (con el mismo o con otro nombre), hacer una revisión rápida, agregar otro archivo o quitarlo del mensaje.

Si abre el menú **Archivo** y selecciona **Propiedades**, verá datos diversos sobre el mensaje que tiene seleccionado.

Salga de las propiedades del mensaje con **Aceptar** y vuelva a la pantalla principal de la mensajería.

Cómo modificar la presentación del correo

Puede modificar la presentación de la **Bandeja de entrada**, si abre el menú **Ver** y selecciona **Columnas**. Verá la siguiente pantalla:

En ella se ven las columnas que aparecerán en el listado del correo (son las que tienen activada su casilla) y el orden en que lo harán.

Puede alterar el orden en que aparecerán, seleccionándolas y marcando **Subir** o **Bajar**.

Cuando haya finalizado, pulse en **Aceptar**.

También puede modificar el criterio y la clase de ordenación de presentación de los mensajes, si abre el menú **Ver**, pulsa en **Ordenar por** y selecciona el criterio y el orden de ordenación deseado.

La agenda de direcciones

Para trabajar con la agenda de direcciones, abra el menú **Herramientas** y seleccione **Libreta de direcciones**. Verá la pantalla en donde figuran los usuarios dados de alta en el correo.

Si selecciona un usuario y pulsa dos veces el botón izquierdo sobre él**,** verá los datos de dicho usuario repartidos en ocho fichas: **Resumen**, **Nombre**, **Domicilio**, **Negocios**, **Personal**, **Otros**, **Netmeeting** e **Identificadores digitales**.

Puede añadir una nueva entrada a su libreta de direcciones si pulsa en el icono **Nuevo**, selecciona **Nuevo contacto** e introduce sus datos.

Si selecciona un usuario y pulsa en **Eliminar**, se borrará de la libreta de direcciones.

LOS GRUPOS DE CORREO

Un grupo de correo es un grupo de usuarios a los que se les va a enviar el mismo correo.

Un usuario puede formar parte de más de un grupo de correo y, además, estar en forma individual en la libreta de direcciones.

Para crear un grupo de correo, pulse en el icono **Nuevo** y seleccione **Grupo nuevo**.

Indique el nombre del grupo, pulse en **Seleccionar miembros**, seleccione un usuario, pulse en **Seleccionar** (repitiendo el proceso con cada usuario que desee que forme parte del grupo) y pulse en **Aceptar**.

Si selecciona un usuario del grupo y pulsa en **Propiedades**, verá los datos de dicho usuario.

Si lo desea puede quitar algún miembro del grupo. Para ello, seleccione el usuario que desee y pulse en **Quitar**.

Si desea añadir un miembro al grupo pero no quiere que forme parte de la libreta de direcciones, escriba sus datos en los apartados **Nombre** y **Dirección de correo electrónico** y, luego, pulse en **Agregar**.

Cuando haya finalizado, pulse en **Aceptar** y verá que aparecerá en su libreta de direcciones pero con un icono de dos usuarios a su izquierda.

Si desea modificar su grupo ya creado, pulse dos veces el botón izquierdo del ratón sobre él y verá la misma pantalla que cuando se creó. Puede cambiarle el nombre, añadir o eliminar miembros (siguiendo los mismos pasos que cuando se creó). Cuando haya finalizado, pulse en **Aceptar**.

Cómo modificar la configuración de la mensajería

Para modificar la configuración de la mensajería, abra el menú **Herramientas**, seleccione **Opciones** y verá la pantalla siguiente:

- Se encuentra en la ficha **General** y en ella hay diversos aspectos que afectan a la configuración general del programa, tales como:
  - Los minutos que han de pasar para comprobar si han llegado mensajes nuevos.
  - Si se va a reproducir un sonido cuando lleguen nuevos mensajes.
  - Si desea ir directamente a la **Bandeja de entrada** al comenzar con al utilidad.
- Si pulsa en la ficha **Leer**, verá la siguiente pantalla:

En ella se encuentran diversos aspectos que afectan al proceso de lectura de los mensajes, tales como:

- Cuándo se va a considerar un mensaje como leído.
- Cómo resaltar los mensajes leídos.

- Si pulsa en la ficha **Confirmaciones**, verá la siguiente pantalla:

En ella se puede indicar si se desea solicitar confirmaciones de lectura, si se desea devolver confirmaciones de lectura y si desea solicitar confirmaciones seguras (únicamente pueden contener solicitudes de confirmación seguras).

- Si pulsa en la ficha **Enviar**, verá la siguiente pantalla:

En ella se encuentran diversos aspectos que afectan al proceso del envío de los mensajes, tales como:

- El formato que se va a utilizar para el envío del correo y de las noticias.

- Si desea guardar una copia de los mensajes enviados en la carpeta **Elementos enviados**.

- Si va a incluir el mensaje en la respuesta.

- Si va a enviar el mensaje inmediatamente.

- Si pulsa en la ficha **Redactar**, verá la siguiente pantalla:

En ella se encuentran las fuentes, el diseño de fondo y las tarjetas de presentación que se van a utilizar para el correo y las noticias.

- Si pulsa en la ficha **Firmas**, verá una pantalla en donde podrá indicar la firma que se va a adjuntar a los mensajes salientes.

- Si pulsa en la ficha **Ortografía**, verá una pantalla en donde podrá indicar la configuración de la ortografía de los mensajes salientes.

- Si pulsa en la ficha **Seguridad**, verá la siguiente pantalla:

En ella se encuentran diversos aspectos que afectan a la seguridad del correo, tales como:

- El nivel de seguridad de las distintas zonas.

- Si va a firmar digitalmente y cifrar todos los mensajes salientes.

- Si desea obtener un certificado digital.

- Si pulsa en la ficha **Conexión**, verá la siguiente pantalla:

En ella se encuentran diversos aspectos que afectan a la conexión de acceso telefónico, tales como:

- Lo que hará al iniciar el programa.
- Si ha de colgar al finalizar de enviar o recibir mensajes.

- Si pulsa en la ficha **Mantenimiento**, verá la siguiente pantalla:

En ella se encuentran diversos aspectos, tales como:

- Cuándo se deben eliminar los mensajes.
- Si se va a vaciar la carpeta de **Elementos eliminados** cuando se salga de la utilidad.

Las reglas de correo

Los reglas de correo son un conjunto de instrucciones que van a indicar las acciones que se han de ejecutar con los mensajes que cumplan una o unas condiciones determinadas.

CÓMO CREAR UNA REGLA

Para crear una regla de correo siga los pasos siguientes:

1. Abra el menú **Herramientas**, seleccione **Reglas de mensaje** y, después, **Correo**. Si es la primera vez, verá la siguiente pantalla:

2. En la parte superior se encuentran las condiciones que han de cumplirse para que se aplique la regla, en la parte central las acciones que se van a ejecutar y, en la parte inferior, una descripción de la regla junto con las especificaciones que se indiquen para cada condición.

3. Cuando haya finalizado, pulse en **Aceptar** y pasará a la lista de reglas de correo.

4. Puede seguir agregando más reglas, quitar la que desee, modificar sus propiedades o aplicarla a una carpeta que deberá seleccionar.

5. Cuando haya finalizado, pulse en **Aceptar.**

CÓMO TRABAJAR CON LAS REGLAS

Una vez que tenga creadas las reglas de correo que desee, puede desactivarlas o volverlas a activar posteriormente.

Para ello, abra el menú **Herramientas** y seleccione **Reglas de mensaje** y, después, **Correo**.

Verá la pantalla en donde se encuentran las reglas que hay definidas y, a la izquierda de su nombre, una casilla.

Si dicha casilla está marcada, significa que está activa y se va a aplicar a los mensajes entrantes.

Si se desactiva dicha casilla, no se aplicará la regla a ningún mensaje hasta que no vuelva a activarse.

El formato de los mensajes

El formato de los mensajes que se envían puede ser de dos tipos:

- **Mensajes de texto**. Este tipo de formato utiliza únicamente texto sencillo, es decir, no tiene ningún atributo ni estilo.

- **Mensajes HTML**. Este tipo de formato permite crear mensajes con todas las opciones de los documentos *HTML*, es decir, con diferentes tipos de letra, tamaños, imágenes, etc.

Es evidente que el utilizar el formato de mensajes *HTML* es más atractivo pero cuenta con el inconveniente del mayor tamaño del mensaje y que hay programas (como *Microsoft Exchange*) que no soportan este tipo de formato. En ese caso, los mensajes al llegar a dichos programas se trasforman en formato de texto perdiendo todos los atributos).

Se puede establecer el formato de los mensajes de distintas maneras:

- **Formato por defecto**. Se utiliza para definir el formato de todos los mensajes enviados. Se indica abriendo el menú **Herramientas**, seleccionando **Opciones**, marcando **Enviar** y activando la casilla **HTML** o **Texto sin formato**. Después, deberá pulsar el botón correspondiente de su derecha y seleccionar los valores deseados. Cuando haya finalizado, pulse en *Aceptar* para volver a la pantalla anterior.

- **Formato para el mensaje activo**. Se utiliza para cambiar el formato del mensaje que se está redactando. Para ello, una vez está redactando el mensaje, abra el menú **Formato** y seleccione entre **Texto enriquecido (HTML)** o **Texto sin formato**.

- **Formato de los mensajes de respuesta**. Se utiliza para cambiar el formato cuando se responde un mensaje ya que se utiliza el mismo formato que tenía el mensaje original. Para ello, una vez está respondiendo el mensaje, abra el menú **Formato** y seleccione entre **Texto enriquecido (HTML)** o **Texto sin formato**. También puede obligar a que se responda siempre en el formato por defecto, para ello, abra el menú **Herramientas**, seleccione **Opciones**, pulse en **Enviar** y desactive la casilla **Responder a los mensajes en el formato en el que se enviaron**.

- **Formato de los mensajes reenviados**. Se utiliza para cambiar el formato cuando se reenvía un mensaje ya que se utiliza el mismo formato que tenía el mensaje original. Para ello, una vez esté reenviando el mensaje, abra el menú **Formato** y seleccione entre **Texto enriquecido (HTML)** o **Texto sin formato**.

- **Mandar texto sin formato en función del destinatario**. Es posible indicar que, aunque se tenga por defecto establecido el formato **HTML**, a determinados usuarios se envíen los mensajes en texto sin

formato. Para ello, abra la **Libreta de direcciones**, pulse dos veces el botón izquierdo del ratón sobre el usuario que desee y, en la ficha **Nombre**, active la casilla **Enviar correo electrónico sólo con texto sin formato**.

El diseño de fondo

El diseño de fondo se utiliza para designar plantillas predefinidas que el usuario puede utilizar para sus mensajes con formato *HTML*.

Para utilizarlo se puede realizar de dos maneras:

- **Para un mensaje individual**. Si desea utilizar un fondo para un mensaje que está redactando, abra el menú **Formato** y seleccione entre **Texto enriquecido (HTML)**. Vuelva a abrir el menú **Formato**, seleccione **Aplicar diseño de fondo** y se desplegará una lista con fondos *HTML* para que seleccione el que desee y empiece a redactar el mensaje (si selecciona **Más diseños de fondo**, podrá escoger un archivo de la carpeta donde se encuentran todos los fondos).

- **Por defecto para todos los mensajes**. Si desea utilizar fondo para todos los mensajes, abra el menú **Herramientas**, seleccione **Opciones**, pulse en la ficha **Enviar** y escoja **HTML** como **Configuración de formato de envío de correo**. Pulse en la ficha **Redactar**, active la casilla **Correo** del apartado **Diseño de fondo,** pulse en **Seleccionar** y escoja el archivo de diseño de fondo que desee.

Cómo firmar los mensajes

Los mensajes pueden incluir una firma al final del mensaje. Esta firma puede incluir algunos datos personales como su nombre, dirección, teléfono, empresa, dirección de correo, etc.

Para poder firmar los mensajes se ha de crear la firma previamente.

CÓMO CREAR UNA FIRMA

Para crear una firma que se incluya en los mensajes, siga los pasos siguientes:

1. Abra el menú **Herramientas**, seleccione **Opciones**, pulse en la ficha **Firmas** y pulse en **Nueva**.

Se pueden utilizar dos métodos para crear la firma:

- Activar **Texto** y escribir lo que se quiera en el campo que hay a su derecha.

- Activar **Archivo** y escribir el nombre del archivo *TXT* que haya creado previamente conteniendo el texto sin formato que quiera poner como firma.

2. Una vez haya seleccionado el método, deberá activar la casilla **Agregar firmas a todos los mensajes salientes** para que incluya la firma al final de todos los mensajes que se vayan a redactar (si no desea incluir la firma en todos los mensajes salientes, podrá hacerlo manualmente en los mensajes que esté redactando, si selecciona **Firma** del menú **Insertar**).

3. También podrá marcar **No incluir la firma en las respuestas ni en los reenvíos**, si desea que no inserte la firma cuando responda o reenvíe un mensaje.

4. Pulse en **Opciones avanzadas**, indique las cuentas a las que desea agregar la firma y pulse en **Aceptar**.

5. Cuando haya finalizado, pulse en **Aceptar**.

Las tarjetas de presentación

La **tarjeta de presentación o tarjeta vCard** es una especificación que define cómo se ha de codificar un archivo de texto (que tiene la extensión **VCF**) que contiene los datos personales del usuario para que pueda ser entendido por todos los programas de correo que tengan libreta de direcciones.

Outlook Express soporta este tipo de tarjetas que incorpora la misma información de una entrada de la libreta de direcciones.

CÓMO CONFIGURAR UNA TARJETA DE PRESENTACIÓN

Para crear su propia **tarjeta de presentación**, deberá crear una entrada en su **Libreta de direcciones** con todos sus datos.

Cuando lo haya hecho, abra el menú **Herramientas**, seleccione **Opciones**, pulse en la ficha **Redactar** y, en el apartado **Tarjeta de presentación**, active **Correo**.

Pulse en el triángulo que hay a la derecha del campo y seleccione la entrada de la **Libreta de direcciones** que corresponde a sus datos personales.

Si pulsa en **Modificar**, podrá cambiar los datos que considere necesario.

Cuando haya finalizado, pulse en **Aceptar**.

Ahora cuando redacte un mensaje, sus datos personales se incorporarán a todos los mensajes que envíe (si no desea incluir la tarjeta en alguno de los mensajes salientes, podrá hacerlo manualmente en los mensajes que esté redactando. Para ello, abra el menú **Insertar** y seleccione **Mi tarjeta de presentación**).

CÓMO AÑADIR UNA TARJETA DE PRESENTACIÓN A LA LIBRETA DE DIRECCIONES

Cuando reciba un mensaje verá que contiene una tarjeta de presentación si hay incluido un archivo con extensión **VCF** o, también, porque en la parte derecha de la cabecera incluye el icono de dichas tarjetas (es como una hoja de agenda horizontal).

Viendo las primeras líneas del mensaje en el panel de vista previa, pulse el botón izquierdo del ratón sobre el icono que representa a la tarjeta y seleccione abrirlo para ver los datos que incorpora o guardarlo en el disco (deberá hacerlo en un archivo con extensión **VCF**).

Si lo guarda en un archivo con extensión **VCF**, podrá incorporarlo a su **Libreta de direcciones**.

Para ello, siga los pasos siguientes:

1. Abra la **Libreta de direcciones**.

2. Abra el menú **Archivo**, seleccione **Importar** y, después, **Tarjeta de presentación (vCard)**.

3. Seleccione el archivo con extensión **VCF** donde había guardado los datos anteriormente.

4. Verá el contenido del archivo y cuando desee, pulse en **Aceptar** para que se cree una nueva entrada en su **Libreta de direcciones** con dichos datos.

La seguridad en el envío y recepción de mensajes

Outlook Express incorpora distintas características de seguridad en el envío y recepción de mensajes.

Especialmente, incorpora **S/MIME** (**Secure MIME**) que es el sistema de seguridad más utilizado por los programas de correo.

Define una doble protección a los mensajes:

- Autentificación a través de una firma digital.
- Privacidad mediante la encriptación de los mensajes.

Además, puede indicarle si el mensaje ha sido alterado durante la transmisión por *Internet*.

Un sistema criptográfico es un método por el que los mensajes se alteran siguiendo unas determinadas normas para que no pueda ser leído por personas no autorizadas.

En todos los sistemas criptográficos se han de utilizar dos claves: una para cifrar el mensaje y otra para descifrarlo.

Existen dos tipos de sistemas criptográficos:

- **Sistemas de clave simétrica**. Es el que utiliza la misma clave para cifrar y descifrar el mensaje. Por tanto, cuando se descubre una clave, se descubre también la otra.
- **Sistemas de clave asimétrica**. Es el que utiliza una clave distinta para cifrar y descifrar el mensaje. Por tanto, cuando se descubre una clave, no se descubre también la otra.

S/MIME utiliza un sistema híbrido. Es decir, encripta el mensaje con una clave simétrica y dicha clave simétrica se codifica con una clave asimétrica.

Estas dos claves se conocen como **clave pública** y **clave privada**. Son asimétricas y, por tanto, al conocer una no se puede deducir la otra.

La **clave pública** se puede distribuir a todos los destinatarios del mensaje mientras que la **clave privada** es personal y sólo la conoce su propietario.

Un usuario para conseguir su propio par de claves ha de solicitar un identificador digital recurriendo a una **Agencia de Credenciales** (**CA**) que es una compañía especializada en proporcionar certificados a los usuarios.

Cuando recibe su identificador digital, se crea un archivo en su ordenador para cada clave. El archivo de la clave privada está protegido y nunca viaja por **Internet** mientras que el archivo de la clave pública se puede copiar todas las veces que se desee y se envía por **Internet** a los destinatarios de los mensajes.

Este par de claves sirve para realizar dos operaciones distintas:

- **Firma digital**. La firma digital se utiliza para que el destinatario del mensaje esté seguro de que el emisor es realmente quién dice ser. Cuando se envía un mensaje con firma digital, se genera un número utilizando un algoritmo sobre el texto del mensaje y lo encripta utilizando la clave privada del emisor. Cuando llega a su destino, el receptor desencripta el número utilizando la clave pública del emisor, vuelve a generar el número y lo compara con el que previamente había desencriptado.

- **Cifrar el mensaje**. Se utiliza para que únicamente el destinatario del mensaje pueda leerlo. El emisor cifra el mensaje con la clave pública del destinatario y, cuando llega a su destino, el receptor lo descifra utilizando su clave privada.

Utilizando ambas operaciones se puede estar seguro de la identidad del emisor y del destinatario del mensaje.

CÓMO OBTENER UN IDENTIFICADOR DIGITAL

Un usuario particular puede conseguir su identificador digital recurriendo a una **Agencia de Credenciales** (**CA**), por ejemplo, *www.fnmt.es* que es una compañía especializada en proporcionarlos de forma gratuita.

Dichas agencias, además de expedir identificadores digitales para correo, también los expiden para servidores **Web**. Un servidor **Web** seguro manda y recibe toda la información de forma encriptada de forma que no pueda ser interceptada por personas no autorizadas (un servidor **Web** seguro se distingue porque el nombre de su página comienza por **https://** en lugar de por **http://)**.

Cada identificador digital está asociado con una determinada dirección de correo electrónico, por tanto, si posee varias direcciones de correo, deberá solicitar varios identificadores digitales. De la misma manera, es posible tener varios

identificadores para una misma dirección de correo pero cada uno ha de ir expedido por una agencia diferente o por la misma pero con diferente nombre.

Para solicitar un identificador digital abra el menú **Herramientas**, seleccione **Opciones**, abra la ficha **Seguridad** y marque **Obtener Id. digital**.

Se procederá a realizar la conexión con *Internet* para solicitar el identificador digital (siga los pasos que se le indican).

Cuando finalice su solicitud, deberá esperar a recibir un mensaje electrónico (no tarda más de cinco minutos) para proceder a su instalación.

CÓMO ACTIVAR UN IDENTIFICADOR DIGITAL

Una vez se ha instalado un identificador digital, se debe activar antes de utilizarlo.

Para proceder a su activación siga los pasos siguientes:

1. Abra el menú **Herramientas**, seleccione **Cuentas**, elija la cuenta de correo para la que ha solicitado el identificador digital, marque **Propiedades**, elija la ficha **Seguridad** y verá la siguiente pantalla:

2. Pulse en **Seleccionar** y, en la ventana que muestre, seleccione el identificador digital que desea utilizar con esta cuenta de correo (en el caso de no aparecer ninguno, es que no se hizo bien el proceso de solicitud e instalación del identificador).

4. Una vez que esté seleccionado, si pulsa en **Ver certificado**, observará los detalles del identificador.

5. Cuando haya finalizado, pulse en **Aceptar** tres veces y, después, en **Cerrar**.

CÓMO ENVIAR LA CLAVE PÚBLICA

Ahora deberá enviar su clave pública a los usuarios para que puedan leer los mensajes que les va a enviar y para que le puedan cifrar los mensajes que le van a remitir.

Para ello, siga los pasos siguientes:

1. Abra el menú **Herramientas**, seleccione **Opciones**, pulse en la ficha **Seguridad** y pulse en **Opciones avanzadas**.

2. Compruebe que la casilla **Incluir mi identificador digital al enviar mensajes firmados** esté señalada.

3. Cuando haya finalizado, pulse en **Aceptar**.

4. Pulse en **Firmar digitalmente todos los mensajes salientes**.

5. Cuando haya finalizado, pulse en **Aceptar**.

CÓMO RECIBIR UNA CLAVE PÚBLICA

Lo mismo que ha enviado su clave pública a los destinatarios de sus mensajes firmados digitalmente, también deberá recibir sus claves públicas para poder leer sus mensajes firmados y poderles cifrar los mensajes que les va a enviar.

Para ello, siga los pasos siguientes:

1. Cuando haya recibido un mensaje firmado digitalmente (lo sabrá porque a la izquierda del nombre del destinatario aparece un sobre cerrado con la marca de firma digital), selecciónelo, pulse el botón derecho del ratón y elija **Propiedades**.

2. Verá que se muestra una pantalla con tres fichas porque está firmado digitalmente, ya que los mensajes que no van firmados digitalmente no cuentan con la ficha **Seguridad**.

3. Pulse en **Seguridad** y en el apartado **Firma digital**, compruebe que en la opción **Firma de confianza** pone *Sí* que indica que la firma digital está incluida.

4. Si está incluida, pulse en **Ver certificados** y pulse en **Agregar a la Libreta de direcciones** para instalarlo en la entrada correspondiente de dicho usuario (si no existiera la entrada, se crearía una nueva).

5. Pulse en *Aceptar* dos veces para volver a la pantalla principal.

6. Abra la **Libreta de direcciones**, seleccione al usuario, pulse en el icono **Propiedades**, pulse en la ficha **Identificadores digitales** y compruebe que, en el apartado **Identificadores digitales asociados con la dirección de correo electrónico**, aparece una entrada con una marca de color roja a su izquierda (en caso de aparecer una marca verde, significará que ya se confía en dicho certificado).

7. Seleccione el identificador, pulse en **Propiedades** y elija la ficha **Confianza**.

8. Pulse en **Confiar explícitamente en este certificado** (o **Heredar la confianza del emisor** si está expedido por una compañía que emite identificadores fiables como **Verisign**).

9. Pulse en **Aceptar** y verá como la marca se ha sustituido por otra de color verde.

10. Pulse en **Aceptar** y cierre la libreta de direcciones.

ENVIAR MENSAJES FIRMADOS DIGITALMENTE

Una vez que se han seguido todos los pasos descritos en los apartados anteriores, ya se pueden enviar mensajes firmados digitalmente.

Cuando redacte un nuevo mensaje, verá que a la derecha de la cabecera del mensaje aparece un icono de color rojo que indica que está firmado digitalmente.

ENVIAR MENSAJES CIFRADOS

Antes de poder enviar un mensaje cifrado a un usuario, es necesario haber recibido su clave pública y haberla activado en la **Libreta de direcciones**.

Una vez que ya esté realizado este paso, redacte el mensaje nuevo y pulse en el icono **Cifrar** (o seleccione **Cifrar** del menú **Herramientas**).

También puede hacerlo si abre el menú **Herramientas**, selecciona **Opciones**, elige la ficha **Seguridad** y marca **Cifrar contenido y datos adjuntos de todos los mensajes salientes**.

Verá que, además del icono de la firma digital, aparece otro icono en forma de candado de color azul.

RECIBIR MENSAJES FIRMADOS DIGITALMENTE

Cuando reciba un mensaje sabrá que está firmado digitalmente si lleva un icono con forma de sobre cerrado y la marca de firma digital de color rojo en la cabecera.

En el momento de recibirlo, buscará en la **Libreta de direcciones** la clave pública del emisor del mensaje y realizará el proceso para comprobar si la firma digital es correcta.

En caso de ser correcta, verá el mensaje normalmente pero en su cabecera habrá un campo nuevo llamado **Seguridad** que indica que el mensaje está firmado y verificado.

En caso de no ser correcta, el mensaje mostrará un aviso de seguridad que le indicará los problemas detectados (la mayoría de las veces el problema surgirá por no haber recibido la clave pública del emisor y/o no haberla activado en la **Libreta de direcciones**).

RECIBIR MENSAJES CIFRADOS

Cuando reciba un mensaje sabrá que está cifrado si lleva un icono con forma de sobre cerrado y un candado de color azul en la cabecera.

En el momento de recibirlo, buscará la clave pública del receptor (es decir, la suya) y la utilizará para desencriptarlo con el algoritmo **3DES**, a no ser que haya especificado otro en **Preferencias de cifrado** de la ficha **Seguridad** de **Propiedades** de la cuenta de correo utilizada.

Una vez lo haya desencriptado, podrá ver su contenido.

Capítulo 6

SISTEMAS OPERATIVOS

Un sistema operativo es un programa o conjunto de programas que actúa como intermediario entre el usuario y el hardware del ordenador, gestionando los recursos del sistema y optimizando su uso. El sistema operativo presenta al usuario una máquina virtual que es más fácil de manejar y programar que el hardware que está por debajo.

FUNCIONES DEL SISTEMA OPERATIVO

A continuación se muestran las funciones principales que realiza todo sistema operativo:

- **Control de la ejecución de programas**. Para ello, transfiere los programas de cada usuario a la memoria central para que puedan ser utilizados. Además, se encarga de restablecer un punto de control cuando se interrumpe la ejecución de un programa para que pueda reproducirse el estado en el que se encontraba el proceso en el momento de la ejecución.

- **Administración de periféricos**. Se encarga de controlar, cuando recibe una petición de utilización de un dispositivo, si dicho dispositivo está desocupado, establece la conexión y, a continuación, pasa el control al programa correspondiente para que inicie la operación (si el

dispositivo estuviera ocupado, coloca la petición en cola hasta que pudiera ser atendida).

- **Gestión de permisos y de usuarios**. Se encarga de gestionar correctamente los permisos concedidos a los usuarios para que puedan utilizar la información almacenada en sus directorios y archivos. Así mismo, se encarga de autentificar a los usuarios para que puedan conectarse al sistema.

- **Control de concurrencia**. Cuando un archivo es abierto por un usuario, el sistema se encarga de bloquearlo para que no pueda ser utilizado por otro usuario. Este bloqueo estará activo hasta que dicho archivo se cierre.

- **Control de errores**. Al transferir la información de la memoria central al resto de los dispositivos, se encarga de realizar un control para comprobar que el total de los caracteres recibidos coincida con el total de los caracteres enviados. Si dicha cifra no coincide, se encargará de cancelar la operación o de repetirla.

- **Administración de memoria**. Se encarga de proteger la memoria de los errores que se pudieran producir cuando existen varios programas en ejecución. Si se detecta que determinada información no es correcta (debido a problemas de hardware o a alguna transmisión realizada), se encargará de averiguar dónde se ha producido dicho error.

- **Control de seguridad**. Se encarga de gestionar los derechos que tienen los usuarios para realizar distintas tareas en el sistema, de esta manera, se garantiza que cada usuario pueda realizar aquello para lo que ha sido autorizado.

TIPOS DE SISTEMAS OPERATIVOS

Se pueden dar muchos tipos de sistemas operativos, entre ellos se encuentran:

- Los **sistemas operativos monousuario** que son aquéllos que únicamente soportan un usuario a la vez, sin importar las características de la máquina sobre la que está montado el sistema.

- Los **sistemas operativos multiusuario** que son capaces de dar servicio a más de un usuario a la vez, también independientemente de la plataforma *hardware* sobre la que esté montado.

- Los **sistemas operativos multitarea** que son aquellos que permiten al usuario realizar varios trabajos al mismo tiempo. Es común encontrar en ellos interfaces gráficas orientadas al uso de menús y el ratón, lo cual permite un rápido intercambio entre las tareas para el usuario, mejorando su productividad.

- Los **sistemas operativos de red** que son aquellos que mantienen a dos o más ordenadores unidas a través de algún medio de comunicación (físico o no), con el objetivo primordial de poder compartir los diferentes recursos y la información del sistema. En este entorno, cada ordenador mantiene su propio sistema operativo y su propio sistema de archivos local.

SISTEMAS OPERATIVOS DE RED

Los sistemas operativos de red se dividen en dos grupos:

- Sistemas que utilizan el modelo cliente/servidor, éstos funcionan siguiendo el esquema de un servidor principal que proporciona soporte a las estaciones de la red. Entre ellos se va a explicar: **Windows 2000 Server**, **Windows Server 2003** y **Linux**.

- Sistemas que utilizan el modelo entre iguales, en ellos no existe un servidor principal sino que todas las estaciones comparten sus recursos de igual a igual. Entre ellos se va a explicar **Windows XP Professional y Windows Vista**.

Modelos basados en cliente/servidor

Estos sistemas operativos destacan en general por las grandes posibilidades de que disponen y su uso abarca desde una red pequeña hasta una gran red corporativa.

WINDOWS 2000 SERVER

Esta versión cuenta con opciones excelentes y mejora notablemente las funciones de *Microsoft Windows NT 4*.

La familia de servidores *Windows 2000* está formada por tres versiones:

- **Server**. Esta versión permite utilizar hasta 4 procesadores, hasta 4 *GB* de memoria *RAM* e incorpora *Directorio Activo*, herramientas de gestión de *Windows*, infraestructura de seguridad *Kerberos* y *PKI*,

servicios de terminales, servicios de componentes y servicios de *Internet*.

- **Advanced**. Esta versión permite utilizar hasta 8 procesadores, hasta 8 *GB* de memoria *RAM* e incorpora *Directorio Activo*, herramientas de gestión de *Windows*, infraestructura de seguridad *Kerberos* y *PKI*, servicios de terminales, servicios de componentes, servicios de *Internet*, balanceo de la carga de la red y servicios de *cluster*.

- **Datacenter**. Esta versión permite utilizar hasta 32 procesadores, hasta 64 *GB* de memoria *RAM* e incorpora *Directorio Activo*, herramientas de gestión de *Windows*, infraestructura de seguridad *Kerberos* y *PKI*, servicios de terminales, servicios de componentes, servicios de *Internet*, balanceo de la carga de la red y servicios de *cluster* avanzados.

Los requerimientos necesarios para su funcionamiento son:

- Procesador *Pentium* 133 *Mhz* o superior.
- Una configuración mínima de memoria *RAM* de 64 *MB*.
- Una unidad de disco duro con suficiente capacidad de almacenamiento para el tamaño de la red. La capacidad mínima es de 1 *GB*.
- Una tarjeta de red.
- Cableado de red.
- Unidad de *CD-ROM* (a ser posible *SCSI*).
- (Recomendado) Una unidad de cinta u otro dispositivo de respaldo.

Microsoft ha preparado hasta el Service Pack 4 para ir corrigiendo los problemas que fueron apareciendo en el sistema operativo y, además, para incluir distintas mejoras.

Actualmente, Microsoft ya no da soporte para este sistema operativo.

WINDOWS SERVER 2003

La familia de servidores Windows 2003 está formada por cuatro versiones, necesitando cada una de ellas los siguientes requisitos del sistema para equipos basados en *x86*.

Además, las mismas versiones están disponibles para procesadores *Itanium*, teniendo mayores requerimientos tanto en velocidad de la *CPU* como en memoria *RAM*.

Requisito	Web Edition	Standard Edition	Enterprise Edition	Datacenter Edition
Velocidad mínima de la CPU	133 MHz	133 MHz	133 MHz	400 MHz
Velocidad recomendada de la CPU	550 MHz	550 MHz	733 MHz	733 MHz
Memoria RAM mínima	128 MB	128 MB	128 MB	512 MB
Memoria RAM mínima recomendada	256 MB	256 MB	256 MB	1 GB
Memoria RAM máxima	2 GB	4 GB	32 GB	64 GB
Soporte para multiprocesadores	1 ó 2	Hasta 4	Hasta 8	Entre 8 y 32
Espacio en disco necesario para la instalación	1,5 GB	1,5 GB	1,5 GB	1,5 GB

Microsoft ha preparado distintos Services Pack o ampliaciones desde el lanzamiento del sistema operativo. Entre ellas se encuentran:

- **Windows Server 2003 R2** que es una actualización construida sobre Windows Server 2003 con Service Pack 1. Ofrece todos los beneficios de Windows Server 2003 SP1, además de incluir mejoras sobre la administración de identidades y accesos, la administración de capacidades de almacenamiento y el desarrollo de aplicaciones.

- El **Service Pack 2** que incluye las últimas actualizaciones y ofrece mejoras de seguridad y estabilidad. Además, agrega nuevas características y actualizaciones a las incluidas en Windows Server 2003. Se puede instalar directamente en todas las versiones de 32 bits tanto de Windows Server 2003 como de Windows Server 2003 R2.

LINUX

Linux es un sistema operativo multiusuario con todas las características que necesita tener un sistema operativo moderno. De hecho, en los últimos años se ha convertido en una alternativa a los sistemas Windows para computadores basados en arquitecturas Intel y compatibles.

Antes de empezar con aspectos técnicos concretos, conviene analizar tanto su evolución como algunas de las ideas que gobiernan el rumbo de este sistema operativo. Podemos destacar tres fundamentos en los que se apoya el desarrollo y la evolución de Linux:

- **Está basado en el sistema operativo Unix**. A Linux se le ha considerado un clónico de Unix para arquitecturas Intel, y en cierta forma es así. Unix es un sistema operativo multitarea y multiproceso desarrollado a principios de los años 70 y utilizado principalmente en sistemas servidores. Unix evolucionó durante 20 años tanto en ambientes académicos como empresariales, lo que lo convirtió en un sistema operativo robusto y fiable. Linux ha heredado de Unix algunas de esas características que han convertido a Unix en un sistema tan eficiente.

- **Es un sistema operativo multiplataforma**. Inicialmente, Linux se desarrolló para arquitecturas Intel pero con el tiempo se han implementado versiones para otras plataformas hardware más minoritarias, como PowerPC, Alpha, Sparc...

- **Es un sistema operativo de libre distribución.** Esto significa que Linux se distribuye bajo los términos de licencia GPL (*General Public License*), lo que implica que cualquiera puede libremente copiarlo, cambiarlo y distribuirlo pero sin posibilidad de aplicar restricciones en futuras distribuciones. (Más información en **www.gnu.org**). Además, el código fuente de Linux (escrito principalmente en lenguaje C) es también público y de libre distribución.

Distribuciones

Linux es un sistema operativo de libre distribución. En los primeros tiempos se podían encontrar en multitud de servidores conectados a Internet todos los ficheros y programas necesarios para su funcionamiento. Sin embargo, y debido a que la tarea de reunir todos los ficheros necesarios e instalarlos correctamente podía ser bastante compleja, aparecieron empresas que se dedicaron a hacer este trabajo, y aquí surgió el término de distribución.

Una distribución no es más que una recopilación de programas y ficheros (incluyendo la última versión estable del núcleo), organizados y preparados para su instalación. Estas distribuciones se pueden obtener a través de Internet o comprando los CD de las mismas. La mayoría del software que incluyen las distribuciones suele tener licencia GPL.

Normalmente, la obtención de las distribuciones por Internet suele ser gratuita. Y si se obtiene la distribución mediante los CD, suele tener un coste en general bastante aceptable teniendo en cuenta la gran cantidad de software que incluyen, así como manuales e incluso soporte durante un período de tiempo (de 3 a 6 meses gratuitos).

Actualmente, sería difícil precisar el número de distribuciones existente de Linux, no obstante hay datos que apuntan a que son más de 300. A continuación, se describen brevemente algunas de las más conocidas.

Red Hat - Fedora

Red Hat es una de las distribuciones más populares e importantes de Linux. La empresa Red Hat, responsable de la distribución Red Hat Linux, nació en 1994 y durante mucho tiempo fue una de las distribuciones de referencia en el software libre. Red Hat ha desarrollado algunos proyectos que se han convertido en estándar en el mundo del software libre. Su más importante contribución es el formato de software empaquetado llamado RPM, utilizado para la instalación de software en sistemas Linux. Ha servido como base para otras distribuciones, por ejemplo, para Mandrake.

Red Hat desarrolló muchas herramientas para la configuración y administración del sistema incluyendo su propio programa de instalación llamado Anaconda.

La última versión lanzada es Red Hat Linux 9. A partir del año 2003, la estrategia de Red Hat ha sido volcar sus esfuerzos en las versiones más comerciales orientadas a empresas. En esta línea, Red Hat se ha centrado en su versión para empresas **Red Hat Enterprise Linux**, mientras que el desarrollo de la parte no comercial dedicada al software libre ha sido asumido por un proyecto independiente llamado Fedora Project y cuya última versión es **Fedora Core 6**. Esta distribución no incluye todo el software disponible y se debe descargar de los repositorios.

Debian

Debian es la única distribución GNU/Linux no comercial, es decir, no depende de ninguna empresa y su desarrollo no atiende a motivos comerciales.

Está desarrollada por programadores de todo el mundo con el objetivo común de construir un sistema operativo basado en software libre lo más robusto posible. De hecho, es una de las distribuciones más imponentes y poderosas y está formada por más de 15.000 paquetes.

Debian tiene la fama de ser una distribución para usuarios avanzados ya que su principal finalidad es la robustez y estabilidad del sistema y no la facilidad de uso. Los responsables de Debian no incorporan nuevo software a la distribución hasta que no está lo suficientemente probado. En este sentido, su carencia de objetivos comerciales favorece esta metodología de implantación de software.

Es la distribución GNU/Linux que en más arquitecturas está implementada, desde los x86 (Intel, AMD...), Alpha, ARM, Power PC y algunos más. Debian ha desarrollado su propio formato de software empaquetado llamado DEB, diferente del formato RPM de Red Hat.

Dentro de su estrategia para conseguir la máxima estabilidad el proyecto, Debian mantiene tres versiones de forma paralela:

- La versión estable y oficial. Actualmente es la versión 3.1r3 lanzada en septiembre de 2006 y conocida como *sarge*.
- La versión en pruebas o testing. Su denominación es *etch* y será la futura versión estable.
- La versión de desarrollo o unstable. Se denomina de forma permanente *sid*.

Existen muchas distribuciones actuales basadas en Debian; las más conocidas son knoppix y Ubuntu.

SUSE

Es una distribución alemana, cuyo enfoque desde sus inicios ha sido claramente comercial siempre desde el marco de software libre. Una práctica habitual de SUSE ha sido publicar versiones comerciales que se diferenciaban de la versión libre por incluir una extensa documentación impresa y un período de soporte.

Como ocurre con casi todas las distribuciones, tiene su propio software de instalación, que además sirve para la administración del sistema, llamado YaST2. Utiliza el formato de software empaquetado RPM.

En el año 2004, la empresa Novell compra SUSE Linux y a partir de ese momento comienza una política parecida a la llevada a cabo en Red Hat, es decir, SUSE se centra en distribuciones comerciales destinadas a empresas y liberan una distribución para que la comunidad de desarrolladores de Linux sea la encargada de futuros desarrollos. Ésta última toma el nombre de **openSUSE**.

Mandrake – Mandriva

La distribución Mandrake Linux apareció en 1998 y estaba basada a su vez en la distribución Red Hat. Después de un período de incertidumbre sobre la continuidad del proyecto, la distribución cambia su nombre a Mandriva.

Su filosofía inicial era ofrecer un sistema robusto, flexible y fácil de utilizar aunque sin perder toda la potencia de un sistema Linux, por ejemplo, permite montar y administrar un servidor. Esto se ha mantenido en el tiempo convirtiendo esta distribución en una de las más fáciles y la preferida por usuarios noveles. Incluye su propio programa de instalación, que es de los más sencillos e intuitivos, y además algunas herramientas gráficas de configuración, conocidas como Drakes.

Al igual que Red Hat y después de haber superado una época de crisis, esta distribución ya tiene abierta una línea de negocio para empresas y otra para socios, con software comercial (es decir, pagando) aunque mantiene una versión de libre distribución.

La última versión distribuida como software libre es Mandriva Linux 2006, aparecida en octubre de 2005.

Ubuntu

Es una distribución basada en Debian y relativamente nueva pero que ha ganado en popularidad gracias a unir las características de robustez y estabilidad de Debian pero intentando ser una distribución más amigable que ésta.

Está muy vinculada a Debian, ya que algunos de los principales desarrolladores de Ubuntu también participan en Debian. Además, utilizan como entorno gráfico el escritorio GNOME. Esto ha provocado la aparición de Kubuntu, de similares características pero basado en KDE.

Ubuntu nace de la iniciativa de algunos programadores de Debian y GNOME apoyados económicamente por un empresario sudafricano llamado Mark Shuttleworth, que funda la empresa Canonical Ltda. con este fin. La primera versión se lanza en octubre de 2004.

La versión más reciente es la 6.10, lanzada en octubre de 2006.

Knoppix

Es una distribución alemana basada en Debian y cuyo principal logro es ser de las primeras distribuciones que funcionan utilizando el sistema LiveCD.

Una distribución knoppix ejecutada desde un LiveCD se puede utilizar directamente desde el CD sin necesidad de instalarla en el disco duro. Simplemente se debe configurar la BIOS del sistema para arrancar desde la unidad de CD-ROM. En dicho CD se incluye, además de un núcleo estable, una colección de programas GNU/Linux y una gran cantidad de controladores, con un total de casi 2 GB de información, lógicamente comprimida, para adaptarse a la capacidad de un CD convencional. El programa de arranque incluye una herramienta de autodetección de hardware. Las últimas versiones de knoppix también se publican para el formato DVD.

Knoppix proporciona la opción de instalación en disco duro aunque el método de instalación no es tan eficiente y flexible como en otras distribuciones.

El formato de funcionamiento Live tiene varios usos como, por ejemplo, utilizar esta distribución como una demo de Linux, como un CD de aprendizaje o como un sistema de rescate.

La última versión es la 4.0.2, que se puede obtener en **www.knoppix.org**.

Distribuciones nacionales

La primera administración pública en España en desarrollar su propia distribución Linux fue la Junta de Extremadura. El nombre de la distribución es **Linex** (**www.linex.org**) y está muy difundida a nivel académico y de administración en la Comunidad de Extremadura. Está basada en la distribución Debian, a la cual le han añadido herramientas de instalación y configuración, que hacen de esta distribución un sistema fácil de usar. Actualmente, se encuentra en la versión **gnuLinEx 2006 RC2**, lanzada en mayo de 2006.

Aunque Linex fue la pionera, otras Comunidades Autónomas han desarrollado o están en proceso de desarrollar su propia distribución, en la mayoría de los casos con propósitos educativos. Algunos ejemplos son:

- Comunidad de Andalucía: **Guadalinex** (**www.guadalinex.org**). Desarrollada tomando como referencia la distribución Linex y, por tanto, se basa en Debian al igual que ésta última. Actualmente, se encuentra en la versión 3.0.

- Comunidad de Madrid: **MAX (www.educa.madrid.org/web/madrid_linux)**. Está basada en la distribución knoppix. Se ofrecen versiones en CD y DVD y, al igual que knoppix, soporta la característica Live, es decir, se puede ejecutar desde el soporte óptico sin instalación en el sistema. La última versión es la 2.0.

- Comunidad de Valencia: **Lliurex** (**www.lliurex.net**). Distribución basada en Debian y con soporte para Live CD. Uno de sus objetivos es que todas las aplicaciones que incluya estén disponibles tanto en castellano como en valenciano.

- Comunidad de Castilla-La Mancha: **MoLinux** (**www.molinux.info**). Tanto la versión 2.0 (Sancho) como la última, la 2.2 (Rocinante), están basadas en Ubuntu y también incluyen la opción Live para utilizar MoLinux sin instalación en el sistema.

- Cataluña: **Linkat** (**http://linkat.xtec.net**). Recientemente se ha publicado la primera versión Linkcat 1.0, sólo disponible en catalán y basada en OpenSUSE.

Modelos basados en sistemas entre iguales

Estos sistemas operativos destacan por la sencillez de su instalación y por su bajo coste aunque no pueden llegar a competir en posibilidades con los sistemas basados en el modelo cliente/servidor.

Están diseñados para redes que cuentan con un máximo de 10 estaciones de trabajo.

WINDOWS XP

Básicamente es Windows 2000 Professional, pero con un nuevo y mejorado aspecto, así como una mejora notable de las características multimedia e *Internet*. Incorpora DirectX 8 (para juegos 3D y efectos gráficos), Internet Explorer 6, Outlook Express 6 y Windows Media Player 8.

Para utilizarlo se necesita un equipo con las siguientes características:

- Procesador mínimo Pentium a 233 Mhz o Celeron de Intel (recomendado, Pentium III a partir de 500 Mhz), K6 Atlhon o Duron en AMD.
- Memoria RAM mínima de 64 MB (recomendado, 256 MB o superior).
- Disco duro mínimo de 1.5 GB (recomendado, a partir de 3 GB).
- Tarjeta vídeo SVGA a 800x600 con 32 MB de memoria (recomendado, a partir de 64 MB) y soporte 3D Directx 8 o superior.
- Monitor que soporte un mínimo de 800x600 (recomendado, 1024x768).

Microsoft inicialmente sacó a la venta dos versiones:

- **Windows XP Home** que está destinada al mercado doméstico. Originalmente, no proporcionó soporte para SMP, aunque con los Service Pack se ha utilizado dicha función.
- **Windows XP Professional** dispone de características adicionales diseñadas para entornos empresariales, como la autenticación por red y el soporte multiprocesador.

Posteriormente, sacó a la venta dos nuevas versiones de Windows XP para hardware específico:

- **Windows XP Media Center Edition** para equipos *HP Media Center Computer* y la serie *Alienware Navigator*. Esta versión debía venderse con estos ordenadores y no se podía encontrar en las tiendas por separado.
- **Windows XP Tablet PC Edition** para ordenadores portátiles diseñados con una pantalla táctil que admitan escritura a mano y pantallas de pequeño tamaño.

Además, preparó otras tres versiones:

- **Windows XP Corporate Edition** que es similar a Windows XP Professional, pero diseñado especialmente para empresas. Esta edición no está bajo los métodos de ventas tradicionales.
- **Windows XP 64 Bit Edition** para equipos con procesadores AMD 64 e Intel con extensiones de 64 bits.
- **Windows XP Starter Edition** destinado a países con pocos recursos o con altos niveles de copia ilegal. Se puede considerar que es un Windows XP con características limitadas.

Debido a una sentencia judicial de la Unión Europea, Microsoft lanzó otra versión:

- **Windows XP N Edition** para las versiones Home y Professional. Esta versión no dispone de Windows Media Placer y se distribuye únicamente en la Unión Europea.

Microsoft ha preparado distintos Services Pack desde el lanzamiento del sistema operativo:

- El **SP1** cuya novedad más visible fue la incorporación de la utilidad **Configurar acceso y programas predeterminados**, para poder elegir de forma más sencilla qué programas se desean utilizar para las tareas

más comunes. Otras novedades que introdujo fueron el soporte para USB 2.0 y de LBA de 48 bits, por lo que Windows XP podría soportar discos duros de más de 137 GB.

- El **SP1A**, como consecuencia de un pleito con Sun Microsystems, Microsoft se vio forzada a sacar una revisión del SP1, en la que se eliminaba la Máquina virtual Java de Microsoft.
- El **SP2** que incluye todas las correcciones encontradas en el **SP1**, además de varias novedades, centradas sobre todo en dar mayor seguridad al sistema operativo. Dichas novedades son:

    - Un **centro de seguridad**, para controlar el riesgo al que está sometido el sistema operativo.
    - Nueva interfaz del **Firewall de Windows**, además de estar activado por defecto.
    - Se añade un **soporte mejor para WiFi y Bluetooth**.
    - Se incorpora a **Internet Explorer**: un bloqueador de ventanas emergentes (*popups*), la capacidad de bloquear controles ActiveX, el bloqueo de las descargas automáticas y un administrador de complementos.
    - Las **actualizaciones automáticas** están activadas por defecto.
    - El servicio **Windows Messenger** se desactiva por defecto.
    - **Outlook Express** bloquea los archivos adjuntos potencialmente peligrosos (*.exe* o *.vbs*).
    - La ventana de **Agregar o quitar programas** permite mostrar u ocultar las actualizaciones.
    - Incluye el **Reproductor de Windows Media 9**, **DirectX 9.0c**, y **Windows Movie Maker 2.1**.

- El **SP3** que está disponible desde mayo de 2008. Este *Service Pack* no es una gran actualización en cuanto funcionalidades como lo fue el anterior, sino que se concentra básicamente en mejorar la estabilidad, el rendimiento y la seguridad.

  Una de sus grandes novedades es **Network Access Protection**, que permitirá establecer una serie de normas que los equipos que quieran comunicarse a través de la red deberán cumplir.

  Por otra parte, hasta ahora los Service Pack han sido paquetes de actualización acumulativa, no obstante el Service Pack 3 requerirá, al menos, instalarse desde Windows XP Service Pack 1.

Activación del sistema

Mientras que la activación de los productos Windows era habitual en los servidores, la industria del software o los negocios, Windows XP introdujo esta opción también para los usuarios comunes como un medio para frenar la piratería. Esta función requiere que el usuario active el sistema operativo durante un lapso de tiempo. Además, si el sistema informático cambia apreciablemente (por ejemplo, si se sustituye la placa base por otro modelo o se aumenta el número de discos duros), Windows volverá a solicitar que se realice la activación.

Ventajas de Windows Original

Windows Genuine Advantage es una herramienta que verifica la legitimidad de la licencia de Windows XP. Si la clave de producto no es genuina, se desplegarán ventanas de advertencia que solicitan al usuario que adquiera una licencia de Microsoft. Además, restringirá el acceso a actualizaciones de seguridad y otros productos de Microsoft.

En sentido estricto, esta utilidad no es obligatoria y, por tanto, dado que el usuario puede modificar los ajustes del servicio de actualizaciones automáticas para ser informado previamente de su descarga o instalación, puede denegar su instalación aunque tendrá problemas para realizar distintas actualizaciones.

WINDOWS VISTA

Windows Vista es el sistema operativo que sucede a Windows XP. Los requisitos mínimos para su utilización se han dividido en dos: los necesarios para ejecutar Vista sin Aero y los necesarios para ejecutarlo con ello:

	Sin Aero	Completo
Procesador	800 MHz	1.0 GHz
Memoria RAM	512 MB	1 GB
Tarjeta gráfica	DirectX 9	DirectX 9 y GPU con Hardware Pixel Shader v2.0 y soporte del controlador Windows Display Driver Model
Memoria gráfica	N/A	128 MB para soportar hasta 2.756.000 píxeles (por ejemplo, 1920 × 1200) o 512 MB para mayor resolución como 2560x1600
Capacidad HDD	20 GB	40 GB
Espacio libre HDD	15 GB	15 GB

Algunas de las mejoras que proporciona con respecto a Windows XP son:

- Es el primer sistema operativo que garantiza una compatibilidad total con **EFI** (**Extensible Firmware Interface**). Por lo tanto, no empleará MBR (Master Boot Record), sino GPT (GUID Partition Table).
- Utiliza una interfaz gráfica completamente rediseñada, cuyo nombre es **Aero** que incorpora características como la semitransparencia de las ventanas, lo que permite ver lo que hay detrás de ellas. Otra novedad son las mejoras en cuanto a la navegación entre las ventanas que se facilita debido a nuevas características como el **Flip 3D**. Por otro lado, Vista también incorpora iconos más grandes, facilitando el trabajo con el sistema debido a que las altas resoluciones de las pantallas hacen que estos se vean muy pequeños.
  Para activar Aero, emplea un sistema que se ejecuta automáticamente durante la instalación de Vista y cuando se modifica la configuración del PC. El sistema operativo utiliza esta información para determinar, entre otras cosas, qué modalidad de Aero puede ser ejecutada y si la máquina se halla capacitada para reproducir vídeo de alta definición.
  La interfaz Aero sólo está disponible en las versiones Business, Home Premium, Enterprise y Ultimate.
- Para dibujar sus ventanas utiliza gráficos vectoriales. Para ello, utiliza una nueva API, llamada **Windows Presentation Foundation**, cuyo nombre en código es **Avalon**, que requiere una tarjeta gráfica con aceleración 3D compatible con DirectX.
- Utiliza **WinFX** que es una API orientada a reemplazar la API actual (Win32). Esta opción junto con Avalon e Indigo son los pilares de Windows Vista.
- Utiliza una interfaz de línea de comando denominada **Windows PowerShell**, que se ofrece como descarga independiente.
- Incorpora **Internet Explorer 7**.
- Integra directamente en el sistema un lector de noticias **RSS** (**Really Simple Syndication**).
- La utilidad de restauración del sistema se implementa como una herramienta de inicio de sesión, facilitando así el rescate del sistema.
- Utiliza un sistema unificado de comunicaciones llamado **Windows Comunication Foundation**, cuyo nombre en código es **Indigo**.
- Incorpora un sistema antispyware denominado **Windows Defender**.
- Añade al firewall de sistema la capacidad de bloquear conexiones que salen del sistema sin previa autorización.
- Incorpora **Windows Mail** en sustitución de Outlook Express.
- Incluye el nuevo **Windows Sidebar** o **Barra Lateral de Windows** que hace que, al pulsar con el ratón sobre ella, el usuario tenga acceso a una serie de pequeños programas denominados *gadgets*.

- Incorpora la herramienta **BitLocker Drive Encryption**, en las versiones Enterprise y Ultimate, para la protección de datos extraviados.
- Incorpora **User Account Control** por lo que los nuevos usuarios de Windows Vista no tienen derechos de administrador por defecto (para realizar tareas administrativas aparecerá una ventana de confirmación).
- Incluye **Windows Media Player versión 11** (a excepción de las ediciones para Europa que no lo incluyen).
- Incluye **Sync Center** para sincronización con los Pocket PC sin necesidad de instalar el *Active Sync*.
- Incorpora un sistema de protección llamado **Windows Software Protection Platform** (**WSPP**) que es más potente que el actual *Windows Genuine Advantage* (*WGA*). Cuando detecta que la copia es ilegal, lo primero que hace será avisar al usuario y si el usuario no logra obtener una copia auténtica, empezará a ir desactivando opciones del sistema, como son Aero o Windows Defender, hasta dejar sólo activo lo más básico como es el navegador.
- Carga las aplicaciones más rápido que Windows XP gracias a la característica **SuperFetch**.

Microsoft inicialmente sacó a la venta las siguientes versiones (todas están disponibles para 32 y 64 bits, a excepción de Vista Starter Edition que sólo estará disponible en 32 bits):

- **Windows Vista Starter**. Es la versión equivalente a *Windows XP Starter Edition* y está destinada a países con pocos recursos o con altos niveles de copia ilegal.

  Tiene limitaciones importantes, como sólo permitir al usuario iniciar a la vez tres aplicaciones con interfaz gráfica, no aceptar conexiones de red entrantes y un límite en la memoria física que puede manejar de 1 GB. Sólo admite los procesadores Athlox XP, Duron y Geode de AMD y los procesadores Celeron, Pentium III y algunos modelos de Pentium 4 de Intel. La parte utilizable del disco duro está limitada a 250 GB.

- **Windows Vista Home Basic**. Es la versión equivalente a *Windows XP Home Edition*. No incluye *Aero* y admite 8 GB de memoria RAM.

  Sus requisitos mínimos son:
  - 512 MB de memoria RAM.
  - 20 GB de disco duro con al menos 15 GB de espacio disponible.
  - Procesador con 800 MHz (recomendado 1 GHz).
  - Tarjeta gráfica de 32 MB.

- **Windows Vista Home Premium**. Es la versión equivalente a *Windows XP Media Center Edition*. Incluye, además de todo lo contenido en la versión *Home Basic*: *Media Center*, soporte para *Tablet PC*, *HDTV* y hasta 16 GB de memoria RAM. Implementa mejoras como la grabación directa de DVD, *Movie Maker* con compatibilidad de HD, su interfaz incorpora *Aero* y *Mobility Center* para usuarios de ordenadores portátiles.

- **Windows Vista Business**. Es la versión equivalente a *Windows XP Professional*. No incluye *Media Center* y ofrece herramientas orientadas hacia los negocios como: *Tablet PC*, Fax, servidor Web *IIS*, hasta 128 GB de memoria RAM, escritorio remoto, copia de seguridad de archivos, la función *Complete PC* que realiza copias *espejo* del disco duro y *Mobility Center* para usuarios de ordenadores portátiles.

- **Windows Vista Enterprise**. Está basada en *Windows Vista Business* e incorpora, además, *Virtual PC*, *MUI* (*Multilingual User Interface*) y soporte para aplicaciones UNIX. No se vende a través de los medios tradicionales de venta.

- **Windows Vista Ultimate**. Es la versión más completa de *Windows Vista*. Combina todas las características de *Home Premium* junto con las de *Business*. Como novedad, única y exclusiva en esta versión se encuentra *DreamScene* (sólo disponible para usuarios de la última versión de *Ultimate*) que consiste en un fondo de escritorio animado que incrementa la experiencia visual del sistema operativo, *Aero glass* y *Flip 3D*. También incluye el sistema de protección de disco duro (*BitLocker and EFS Enhancements*). Todos los extras se descargan desde el menú *Extras de Windows Vista Ultimate* o desde *Windows Update*.

Además, están disponibles para el mercado europeo las ediciones **Home Basic N** y **Business N**, idénticas a las anteriores, salvo que no incorporan *Windows Media Player*.

Las versiones *Home Basic*, *Home Premium*, *Business* y *Ultimate* se venden en el mismo DVD y, al instalarlo, la clave del producto es la que le dice al programa de instalación qué versión debe instalarse (se podrá pasar a una versión superior simplemente pagando una actualización de la licencia a través del *Windows Anytime Upgrade*).

Windows Vista ha recibido muchas evaluaciones negativas. Entre ellas se incluyen: su bajo rendimiento, las pobres mejoras respecto a Windows XP, su prolongado tiempo de desarrollo, su nueva licencia de uso (aún mas restrictiva que

las anteriores), la inclusión de una serie de tecnologías destinadas a la restricción de la copia de protección de los medios digitales, su seguridad y sus requerimientos de hardware.

Para corregir algunos de estos problemas, Microsoft ha preparado el Service Pack 1 que contiene los cambios centrados en abordar las cuestiones de rendimiento, fiabilidad y seguridad, el apoyo a nuevos tipos de hardware, mejor administración de la memoria, resolver el problema del consumo de energía en las baterías de los portátiles y agregar soporte para varios estándares emergentes.

MONTAR UNA RED ENTRE IGUALES EN WINDOWS (PARTE PRÁCTICA)

Para montar una red entre iguales con equipos Windows, las tareas que habrá que hacer en cada uno de los ordenadores que van a formar parte de la red son las que están descritas en el apartado *Montaje y configuración de una red con un switch* del capítulo 3 (si va a haber una red cableada) o en los apartados *Configuración de un punto de acceso* y *Montaje y configuración de una red inalámbrica* del capítulo 3 (si va a haber una red inalámbrica).

Una vez que los equipos están unidos a la red, deberá compartir los archivos y directorios de los equipos que desee (para ver cómo hacerlo, vea el apartado *Cómo compartir directorios* del capítulo 7).

Para poder imprimir, deberá compartir alguna impresora que esté conectada a algún equipo (para ver cómo hacerlo, vea el apartado *Cómo compartir impresoras* del capítulo 7).

Para crear una unidad de red, vea el apartado *Cómo crear una unidad de red* del capítulo 7).

INSTALAR UN CONTROLADOR DE DOMINIO EN WINDOWS SERVER 2003 (PARTE PRÁCTICA)

Una vez que está acabada la instalación de Windows Server 2003, si dicho servidor va a ser un controlador de dominio, ha de configurarse el servidor y lo primero que hay que realizar es instalar el **Directorio Activo** (previamente el equipo deberá estar unido a un switch). Para ello, siga los pasos siguientes:

1. Inicie una sesión en el servidor como administrador y verá la pantalla siguiente (en caso de que no vea dicha pantalla, seleccione

Administre su servidor de **Herramientas administrativas** del **Panel de control**):

2. Pulse sobre **Agregar o quitar función** y verá la pantalla siguiente:

3. Le mostrará una pantalla con los pasos preliminares necesarios para poder realizar el proceso. Cuando la haya leído y comprobado que todo está preparado, pulse en **Siguiente** y comenzará a detectar la configuración del servidor. Al cabo de un momento, verá la pantalla siguiente:

4. Active la casilla **Configuración típica para un servidor principal**, pulse en **Siguiente** y verá la pantalla:

5 Indique el nombre que desea dar a su dominio (en caso de no tener registrado ninguno en Internet, es conveniente finalizarlo con *local*. En el ejemplo, se indicará *contabilidad.local*). Cuando haya finalizado, pulse en **Siguiente** y verá la pantalla:

6. En ella puede cambiar el nombre *NetBIOS* del dominio (es el que aparecerá con equipos Windows 95/98, Windows Millenium y Windows NT. En el ejemplo, indica *contabilidad*). Cuando la haya leído, pulse en **Siguiente** y verá la pantalla (si, previamente, no ha indicado una dirección IP para el servidor *DNS* en la configuración *TCP/IP*, pasará directamente al punto 7 y no verá la pantalla que se muestra a continuación):

7. En ella deberá indicar (si lo desea) el servidor *DNS* de fuera de su red al que enviará las consultas *DNS* que no pueda resolver el servidor que está configurando (como en todas las estaciones del dominio deberá estar puesta en primera posición la dirección *IP* del servidor *DNS* del dominio, para poder acceder a Internet, deberá poner la dirección IP

del servidor *DNS* de su proveedor de acceso). Cuando lo haya realizado, pulse en **Siguiente**.

8. Le mostrará una pantalla resumen de las selecciones realizadas. Cuando la haya leído, pulse en **Siguiente** y comenzará el proceso (previamente, le mostrará una pantalla en la que le avisa de que cierre todos los programas que tenga abiertos. Cuando los haya cerrado, pulse en **Aceptar**).

9. Le pedirá que inserte el CD de Windows Server 2003 (si no estaba ya colocado en la unidad de CD). Cuando lo haya realizado, continuará el proceso.

10. Al cabo de unos minutos se reiniciará el equipo y continuará con la instalación del Directorio Activo. Cuando haya finalizado, le mostrará la pantalla para que vuelva a iniciar la sesión.

11. Iníciela y realizará los ajustes finales mostrándole la pantalla de progreso de configuración del servidor en la que le indica las operaciones realizadas. Cuando haya finalizado, pulse en **Siguiente** y, después, en **Finalizar**.

12. Le mostrará la pantalla **Administre su servidor** en la que le indica las funciones configuradas del servidor. Active la casilla **No mostrar esta pantalla al iniciar sesión** (se encuentra al final de la pantalla), ciérrela y ya estará instalado el Directorio Activo (recuerde que, además de instalar el Directorio Activo, se ha instalado el servidor *DHCP* y el servidor *DNS*).

CONFIGURAR UN SERVIDOR DHCP EN WINDOWS SERVER 2003 (PARTE PRÁCTICA)

Una vez que se ha instalado el controlador de dominio en Windows Server 2003, es necesario configurarlo para que adjudique las direcciones IP que le pidan los clientes.

Cómo autorizar un servidor DHCP

Los servidores *DHCP* proporcionan un servicio muy útil. Sin embargo, si se introduce en la red un servidor *DHCP* incorrectamente configurado o no autorizado, puede causar problemas (por ejemplo, podría comenzar a conceder direcciones *IP* incorrectas a los clientes o reconocer negativamente a los clientes *DHCP* que intentan renovar sus concesiones actuales de direcciones).

Para evitar estos problemas, Windows Server 2003 comprueba antes de que puedan proporcionar servicios a los clientes la validez de los servidores, así se evitan la mayor parte de los daños accidentales provocados al ejecutar servidores *DHCP* con configuraciones incorrectas o con configuraciones correctas en una red equivocada.

Para autorizar un servidor *DHCP*, siga los pasos siguientes:

1. Seleccione **DHCP** de **Herramientas administrativas** del menú **Inicio** y verá una pantalla parecida a la siguiente:

2. En el panel izquierdo, sitúese sobre **DHCP**, pulse el botón derecho del ratón para que muestre su menú contextual, seleccione **Administrar servidores autorizados** y verá la pantalla siguiente:

3. Pulse en **Autorizar** y verá la pantalla siguiente:

4. Escriba la dirección *IP* del servidor *DHCP* que desea autorizar y pulse en **Aceptar**.

5. Le mostrará una pantalla de confirmación del proceso. Pulse en **Aceptar** y se procederá a autorizar al servidor *DHCP*.

6. Sitúese sobre el servidor *DHCP* que acaba de autorizar y pulse en **Aceptar** para que se añada a la consola de *DHCP* si no estaba ya añadido previamente.

7. Cuando haya finalizado, cierre la utilidad.

Cómo crear un ámbito

Un ámbito es un agrupamiento administrativo de equipos de una subred que utilizan el servicio *DHCP*. Antes de que los clientes puedan obtener una dirección *IP* es necesario crear un ámbito en cada servidor *DHCP*. Normalmente, en el proceso de instalación se ha creado un ámbito. Puede comprobarlo si pulsa en el signo "+" que hay a la izquierda del servidor *DHCP*. También, puede ser necesario crear un ámbito nuevo si desea segmentar la red. Para ello, siga los pasos siguientes:

1. Seleccione **DHCP** de **Herramientas administrativas** del menú **Inicio** y verá la pantalla principal de la utilidad.

2. En el panel izquierdo, sitúese sobre el servidor (en el ejemplo, *principal.contabilidad.empresa.com*), pulse el botón derecho del ratón para que muestre su menú contextual, seleccione **Ámbito nuevo** y entrará en el asistente.

3. Pulse en **Siguiente** y le mostrará una pantalla para que indique el nombre que desea dar al ámbito que está creando (en el ejemplo, *Ámbito de contabilidad*) y una breve descripción.

4. Cuando lo haya hecho, pulse en **Siguiente** y le mostrará la pantalla:

En ella se encuentran los apartados siguientes:

- **Dirección IP inicial**. Permite indicar la primera dirección *IP* que puede conceder.

- **Dirección IP final**. Permite indicar la última dirección *IP* que puede conceder.

- **Longitud**. Permite indicar la máscara de subred en función del número de *bits* a utilizar para el identificativo de equipo (normalmente, las de clase **A** será 8, las de clase **B** será 16 y las clase **C** será 24 pero puede utilizarse cualquier otra, en función de

la segmentación de la red). Fíjese en que al modificar este valor, automáticamente cambia la máscara de subred correspondiente.

- **Máscara de subred**. Permite indicar la máscara de subred (normalmente, las de clase **A** será 255.0.0.0, las de clase **B** será 255.255.0.0 y las clase **C** será 255.255.255.0 pero puede indicarse otras en función de la segmentación de la red). Fíjese en que al modificar este valor, cuando se cambie a otro apartado, cambiará el valor del campo *Longitud*.

5. Cuando haya finalizado, pulse en **Siguiente** y verá la pantalla:

En ella se indicarán todas las direcciones que no serán adjudicadas a nadie, ya sea porque pertenezcan a servidores *DHCP***,** clientes que no van a usar *DHCP***,** estaciones de trabajo sin discos o clientes de acceso remoto, etc. Cuenta con los apartados siguientes:

- **Dirección IP inicial**. Permite indicar la primera dirección que será excluida para la concesión.

- **Dirección IP final**. Permite indicar la última dirección que será excluida para la concesión.

Cuando haya escrito ambas, pulse en *Agregar* y se añadirán a la lista de **Excluir el intervalo de la dirección**. Puede volver a repetir el proceso si hay más intervalos (en el caso de excluir una única dirección, escríbala en **Dirección IP inicial**, deje **Dirección IP final** en blanco y pulse en **Agregar**).

Si desea volver a utilizar una dirección excluida, selecciónela de la lista de **Excluir el intervalo de la dirección** y pulse en **Quitar**.

6. Cuando haya finalizado, pulse en **Siguiente** y verá la pantalla:

En ella podrá indicar la duración que desea otorgar a cada concesión de dirección *IP*.

7. Cuando haya finalizado, pulse en **Siguiente** y verá la pantalla:

8. Pulse en **Siguiente** para continuar configurando las opciones *DHCP* ahora y verá la pantalla:

Indique la dirección *IP* del encaminador o enrutador (puerta de enlace o *router*) y pulse en **Agregar**.

9. Repita el proceso si dispone de más de uno y, cuando haya finalizado, pulse en **Siguiente** y verá la pantalla:

En ella se encuentran los apartados siguientes:

- **Dominio primario**. Permite indicar el dominio principal *DNS*.
- **Dirección IP**. Permite indicar la dirección *IP* del servidor principal *DNS*. Pulse en **Agregar** para que pase al apartado correspondiente.

  Si selecciona una dirección *IP* y pulsa en **Quitar**, pasará al apartado superior para poder modificar la dirección (si desea eliminarla, bórrela).

  Si selecciona una dirección *IP* y pulsa en **Arriba** o **Abajo**, la moverá dentro de la lista.

- **Nombre de servidor**. En caso de no conocer la dirección *IP*, se puede indicar el nombre del servidor *DNS*, pulsar en **Resolver** y, automáticamente, escribirá su dirección *IP*. Pulse en **Agregar** para que pase al apartado correspondiente.

10. Cuando haya finalizado, pulse en **Siguiente** y verá la pantalla*:*

En ella se encuentran los apartados siguientes:

- **Nombre de servidor**. En caso de disponer de servidor *WINS*, puede indicar su nombre, pulsar en **Resolver** y, automáticamente, escribirá su dirección *IP*.

- **Dirección IP**. Permite indicar la dirección *IP* del servidor *WINS*. Pulse en **Agregar** para que pase al apartado correspondiente.

  Si selecciona una dirección *IP* y pulsa en **Quitar**, pasará al apartado superior para poder modificar la dirección (si desea eliminarla, bórrela).

  Si selecciona una dirección *IP* y pulsa en **Arriba** o **Abajo**, la moverá dentro de la lista.

11. Cuando haya finalizado, pulse en **Siguiente** y verá la pantalla*:*

12. Pulse en **Siguiente** para activar el ámbito en este momento y le mostrará la pantalla de finalización del asistente.

13. Pulse en **Finalizar** y volverá a la pantalla principal de la utilidad. Fíjese en que, en el panel izquierdo, le muestra el ámbito que acaba de crear. Si pulsa en el signo "+" que hay a la izquierda de dicho ámbito, se desplegarán sus nodos.

14. Si se sitúa sobre el nodo **Opciones de ámbito**, le mostrará en el panel derecho distintas opciones de su configuración.

15. Puede situarse sobre el resto de los nodos del ámbito y verá todos los demás valores que se indicaron durante la creación del ámbito.

16. Cuando haya finalizado, cierre la utilidad.

Cómo configurar los clientes DHCP

Una vez configurado y activado el servidor *DHCP*, deberá configurar las estaciones para utilizarlo. Para hacerlo vea el apartado *Configuración TCP/IP estática para un equipo* del capítulo 3, pero active las casillas **Obtener una dirección IP automáticamente** y **Obtener la dirección del servidor DNS automáticamente** en lugar de asignar una dirección IP estática.

Cómo ver la configuración IP de la estación

Puede ver la configuración *IP* de un equipo con el comando **ipconfig**. Para ello, siga los pasos siguientes:

1. Seleccione **Símbolo del sistema** de **Programas** del menú **Inicio**.

2. En la pantalla negra que le aparece, escriba **ipconfig /all** y pulse [**Intro**].
3. Le mostrará información diversa sobre la configuración *IP* del equipo y la configuración de su adaptador (incluyendo la dirección *IP*, la dirección física y datos sobre el servidor *DNS* y el servidor *DHCP*).

4. Cuando haya finalizado, cierre la ventana.

CÓMO UNIR UN ORDENADOR A UN DOMINIO (PARTE PRÁCTICA)

Una vez que se ha instalado el servidor, hay que proceder a conectar las estaciones de trabajo a dicho servidor para que autentifique a los usuarios y se puedan utilizar sus recursos.

Previamente, deberán estar unidos los ordenadores que se deseen al switch. Las tareas que habrá que hacer en cada uno de los ordenadores que van a formar parte de la red son las que están descritas en el apartado *Montaje y configuración de una red con un switch* del capítulo 3 (si va a haber una red cableada) o en los apartados *Configuración de un punto de acceso* y *Montaje y configuración de una red inalámbrica* del capítulo 3 (si va a haber una red inalámbrica). Recuerde que lo mejor es que indique que la dirección IP sea asignada de forma dinámica y el servidor DHCP de Windows Server 2003 se la otorgará.

Una vez establecido correctamente el direccionamiento IP en el equipo, para conectarse con Windows Server 2003, estando configurado el Directorio Activo, el servidor DHCP y el servidor DNS, se han de seguir los pasos siguientes:

En **Windows XP**:

1. Cuando se inicie el sistema, le pedirá el nombre y la contraseña para iniciar una sesión en el equipo. Indíquelo, pulse en **Aceptar** y, al cabo de un momento entrará en el escritorio.

2. Sitúese sobre **Mi PC**, muestre su menú contextual y seleccione **Propiedades**.

3. Pulse en la ficha **Nombre de equipo** y verá el nombre del equipo y el grupo de trabajo al que pertenece. Ahora, deberá hacerlo pertenecer al dominio de *Windows Server 2003* al que va a conectarse. Para ello pulse el botón **Cambiar**, active la casilla **Dominio**, escriba el nombre correspondiente y pulse en **Aceptar**. Le pedirá que indique el nombre de una cuenta de usuario con su contraseña con permisos para poder unir el equipo al dominio (ha de ser la cuenta de un administrador del servidor). Indique ambos valores y pulse en **Aceptar**.
4. Al cabo de un momento le dará la bienvenida al dominio. Pulse en **Aceptar** y, después de reiniciar el equipo, indique el nombre del usuario y su contraseña.

En **Windows Vista**:

1. Cuando se inicie el sistema, le pedirá el nombre y la contraseña para iniciar una sesión en el equipo. Indíquelo, pulse en **Aceptar** y, al cabo de un momento entrará en el escritorio.

2. Pulse con el botón derecho del ratón **Equipo** con el botón derecho del ratón, elija **Propiedades**, pulse en **Cambiar la configuración** y pulse en **Continuar** para poder continuar con el proceso (si se lo pide).

3. Pulse en **Cambiar**, active la casilla **Dominio**, escriba el nombre correspondiente y pulse en **Aceptar**. Le pedirá que indique el nombre de una cuenta de usuario con su contraseña con permisos para poder unir el equipo al dominio (ha de ser la cuenta de un administrador del servidor). Indique ambos valores y pulse en **Aceptar**.

4. Al cabo de un momento le dará la bienvenida al dominio. Pulse en **Aceptar** y, después de reiniciar el equipo, indique el nombre del usuario y su contraseña.

Capítulo 7

ADMINISTRACIÓN Y GESTIÓN DE REDES

INTRODUCCIÓN

Los pasos a seguir para instalar y configurar una red son:

- Instalar todo el cableado y las tarjetas de red en los ordenadores.
- Instalar los discos duros, impresoras y otros periféricos.
- Conectar todos los equipos a la red.
- Instalar los sistemas operativos de todas las estaciones de trabajo.
- Instalar el sistema operativo de red en el servidor, identificando cada estación de trabajo y los dispositivos conectados (si es una red con arquitectura cliente/servidor).

Una vez instalados todos los sistemas operativos, se ha de proceder a la configuración de la red, teniendo que realizar, entre otros, los siguientes pasos:

- Desarrollar la estructura de directorios a compartir.
- Copiar los programas de aplicaciones y los datos.
- Conectar las unidades de red.
- Dar de alta a los usuarios y grupos.
- Establecer la configuración de seguridad.
- Localización de problemas.

La responsabilidad de configurar y gestionar el servidor de la red corresponde al administrador, sin embargo, puede ocurrir que los usuarios interfieran en la administración al realizar cambios en las configuraciones de los equipos. Por ello, es necesario que el administrador imponga una serie de restricciones para evitar que los usuarios realicen las modificaciones que les parezcan.

LA ESTRUCTURA DE DIRECTORIOS

Los directorios en Windows

Sin duda, se pueden emplear un número ilimitado de estructuras de directorios en un servidor de ficheros y se debe estudiar cuidadosamente la que mejor se adapta a las necesidades de cada empresa.

Cuando se planea la disposición de los directorios, se deben considerar tres circunstancias importantes:

- **La simplicidad de la estructura**. No se debe hacer que la estructura de directorios sea tan complicada que los usuarios no puedan encontrar los programas ni los archivos de datos.

- **La seguridad**. Muchas de las previsiones de seguridad de un sistema operativo de red son relativas a los directorios y subdirectorios.

- **La lógica**. Los archivos deben estar agrupados lógicamente para aumentar la eficiencia de la red.

Para la utilización por los usuarios, se deberían crear varios directorios en el servidor de ficheros:

- El directorio **PROGRAMAS** que tendrá varios subdirectorios que contendrán los programas de aplicaciones necesarios (en Windows se encuentra en **Archivos de programas**).

- El directorio **UTILIDADES** que proporcionará un almacenamiento a los diversos programas de utilidad.

- El directorio **PRIVADO** que se utilizará para almacenar los archivos de datos individuales de cada usuario de la red local.

- El directorio **GRUPOS** que tendrá subdirectorios que se comparten por individuos del mismo grupo de trabajo.

- El directorio **PUBLICO** que almacenará cualquier archivo cuyo acceso esté permitido a todos los usuarios de la red.

Esta fórmula satisface los criterios establecidos anteriormente para la disposición de un directorio:

1. Es simple. Hay directorios específicos y sus nombres son un claro reflejo de lo que contienen.

2. La estructura de los directorios facilita una seguridad efectiva, permitiendo que los atributos de seguridad se asignen a los usuarios individualmente y a los grupos. Por ejemplo, el acceso a los archivos del directorio **GRUPOS** puede estar restringido a los usuarios individuales de la red que no pertenezcan a un grupo determinado.

3. Los archivos están agrupados lógicamente en los directorios. Los programas de aplicación están separados de los archivos de datos y los datos de cada usuario están separados.

La jerarquía de directorios en Linux

En los sistemas Unix, las ubicaciones de los ficheros en el sistema siguen unas normas determinadas con el objeto de aumentar el nivel de organización. La mayoría de las distribuciones de Linux siguen el llamado estándar de jerarquía del sistema de ficheros, **FHS** (**Filesystem Hierarchy Standard**. Más información sobre este estándar en **www.pathname.com/fhs**). Algunos de los directorios más importantes son los siguientes:

- **/bin** y **/usr/bin**. Estos directorios contienen la mayoría de los ficheros ejecutables y comandos más comunes del sistema Linux.

- **/sbin** y **/usr/sbin**. Estos directorios también contienen comandos y ficheros ejecutables normalmente ejecutados en tareas de administración, con lo cual muchos de ellos sólo son ejecutables para el usuario root o administrador del sistema.

- **/etc**. Este directorio contiene los ficheros de configuración de todo el sistema, con lo cual es de vital importancia. Normalmente, los ficheros que contiene son ficheros de configuración de tipo texto sin formato. Además, suelen tener sólo permisos de lectura para usuarios normales, es decir, sólo el usuario root los puede modificar.

- **/root**. Directorio home del usuario root.

- **/usr**. Directorio destinado a almacenar las aplicaciones, con lo cual su tamaño puede ser elevado si existen muchos paquetes de software instalados. Puede ser una buena opción utilizar una partición separada para este directorio.

- **/home**. Directorio donde se almacenan todos los directorios home de los usuarios del sistema, por tanto, en función del número de usuarios y del uso que hagan del sistema, este directorio puede llegar a necesitar mucho espacio. En sistemas servidores es recomendable utilizar una partición separada para este directorio.

- **/lib** y **/usr/lib**. Directorios que contienen librerías compartidas del sistema.

- **/tmp**. Directorio para almacenar ficheros temporales.

- **/boot**. Directorio que contiene los ficheros necesarios para el arranque del sistema. Por ejemplo, aquí se almacenan los ficheros del gestor de arranque si hubiera alguno instalado (LILO o GRUB). También se suelen almacenar las imágenes del kernel o núcleo del sistema. Algunas distribuciones aconsejan utilizar una pequeña partición separada para este directorio.

- **/dev**. Directorio que almacena ficheros de dispositivos. Estos ficheros no son realmente ficheros sino que es la forma en la que los sistemas Linux implementan los controladores de dispositivos. Se hablará más al respecto de estos archivos en el apartado correspondiente.

- **/var**. Directorio que contiene información variable en general, como colas de impresión, colas de envío y recepción de correos y news, archivos de registro y de eventos del sistema... En sistemas Linux utilizándose como servidores, este directorio puede necesitar mucho espacio, con lo cual es recomendable utilizar una partición propia.

- **/opt**. Directorio opcional donde se pueden instalar aplicaciones, además de /usr. En algunos sistemas Linux no existe.

- **/proc**. Este directorio se corresponde con un sistema de ficheros virtual creado por el kernel en memoria. Sirve de interfaz con los parámetros de configuración del kernel.

- **/mnt**. Directorio usado por defecto por el sistema para realizar el montaje de otros dispositivos de almacenamiento como disquetes, CD-ROM, unidades de almacenamiento USB, etc.

Los ficheros de dispositivo

Una de las características especiales de Linux es su forma de acceder o reconocer los dispositivos físicos para poder hacer uso de ellos. Para Linux, cualquier dispositivo físico depende directamente de los llamados manejadores de dispositivos, que se integran en la estructura de ficheros del sistema dentro del directorio /dev. De esta forma, el acceso a los diferentes dispositivos físicos se hace de una forma homogénea. La entrada/salida se realiza siempre como si se accediera a ficheros.

Para que un dispositivo pueda ser "manejado" a través de estos ficheros es necesario que haya un driver o controlador a bajo nivel instalado. Por tanto, todos los ficheros que contiene el directorio /dev realmente no son ficheros de disco sino que son manejadores de dispositivos creados por los drivers. Los nombres de estos "ficheros" siguen un estándar para identificarlos con los dispositivos físicos a los que están asociados. A continuación se presenta una lista de los más comunes:

- **Disqueteras:**
  /dev/fd0
  /dev/fd1
- **Unidad CD-ROM o DVD:**
  /dev/cdrom
  /dev/dvd
- **Dispositivos conectados a un bus IDE:**
  /dev/hda Primer disco duro del canal IDE 1
  /dev/hda1 Primera partición
  /dev/hda2 Segunda partición
  /dev/hda3 Tercera partición
  /dev/hda4 Cuarta partición
  /dev/hda5 Primera partición lógica
  /dev/hda6 Segunda partición lógica
  ...
  /dev/hdb Segundo disco duro del canal IDE 1
  /dev/hdb1 Primera partición
  ...
  /dev/hdc Primer disco duro del canal IDE 2
  /dev/hdd Segundo disco duro del canal IDE 2

MONTAR Y DESMONTAR DISPOSITIVOS DE ALMACENAMIENTO

Para poder acceder a un sistema de ficheros ubicado en alguno de los dispositivos de almacenamiento que forman parte del sistema, es necesario realizar una operación llamada **montaje**. Montar un sistema de ficheros/dispositivo no es

más que hacerlo disponible en el árbol de directorios de nuestro sistema. Recordar que el árbol de directorios de un sistema Linux es único.

En definitiva, **montar un dispositivo es asociar un directorio del árbol de directorios al sistema de ficheros del dispositivo**. Esta operación se realiza con el comando **mount**:

mount –t <sistema_de_ficheros> <dispositivo> <punto_de_montaje>

El parámetro <dispositivo> es el nombre del dispositivo utilizando el nombre del fichero manejador, por ejemplo */dev/hda1*, */dev/fd0*, */dev/cdrom*.

El parámetro <punto_de_montaje> es el nombre del directorio donde queremos enlazar la estructura de directorios del dispositivo.

Los directorios utilizados como base para montar los diferentes dispositivos removibles del sistema como disquetera y CD-ROM son */mnt* o */media* dependiendo de la distribución utilizada. Sin embargo, el uso de este directorio no es obligatorio; se puede utilizar cualquier directorio. Por ejemplo, en algunas distribuciones existen los directorios */floppy*, */cdrom* y */dvd*.

El siguiente ejemplo monta un disquete formateado con el sistema de ficheros FAT, en el directorio */floppy*. Después de ejecutar el comando, se podrá acceder a la información del disquete accediendo a este directorio.

```
# mount –t vfat /dev/fd0 /floppy
```

El siguiente ejemplo monta un CD-ROM:

```
# mount –t iso9660 /dev/cdrom /cdrom
```

El siguiente comando monta una partición NTFS de Windows XP ubicada en la primera partición de un disco IDE. Primero se crea el directorio o punto de montaje:

```
# mkdir /wxp
# mount –t ntfs /dev/hda1 /wxp
```

El montaje de las particiones Linux que contienen toda la estructura de directorios del sistema se monta en el arranque.

Para desmontar un dispositivo, se utiliza el comando **umount**. Se puede especificar tanto el punto de montaje como el nombre del dispositivo.

Ejemplos:

```
# umount /floppy
# umount /cdrom
# umount /dev/hda1
```

Existe un fichero de configuración donde se pueden especificar los sistemas de ficheros que existen en nuestro sistema y de qué forma se va a realizar el montaje; el fichero es **/etc/fstab .**

Se pueden ver los dispositivos actualmente montados en el fichero **/etc/mtab** o ejecutando el comando *mount* sin parámetros.

Los dispositivos de almacenamiento que sean necesarios para el funcionamiento del sistema han de ser incluidos obligatoriamente en el fichero */etc/fstab* con la opción *auto*, para que sean montados en el arranque.

Para que se monten todos los dispositivos especificados en el fichero */etc/fstab*:

```
# mount –a
```

COPIAR LOS PROGRAMAS DE APLICACIONES Y LOS DATOS

El paso siguiente es cargar en el servidor de ficheros el programa o los programas de aplicaciones, y los datos que puedan ser necesarios.

En general, los procedimientos de una instalación de un programa en cualquier servidor de ficheros son similares a los de una aplicación en un ordenador aislado. La única diferencia está en dónde se cargan los archivos en el disco duro.

Es conveniente asegurarse de que se está utilizando una versión del programa apropiada para funcionar en redes. No es adecuado utilizar versiones para un solo usuario (monopuesto) en una red, ya que tales versiones frecuentemente no funcionan como deben cuando varios usuarios intentan acceder a los mismos archivos.

Para cargar de forma adecuada las aplicaciones, debe seguirse cuidadosamente la documentación de instalación. De otro modo, pueden surgir problemas tales como anomalías en el programa ocasionadas por la señalización incorrecta de los archivos.

LOS PERFILES DE USUARIO

Un **perfil de usuario** es una de las herramientas más potentes de Windows para configurar el entorno de trabajo de los usuarios de red.

Pueden especificar el aspecto del escritorio, la barra de tareas, el contenido del menú **Inicio**, etc. (incluyendo programas o aplicaciones).

Cada usuario puede tener un perfil que está asociado a su nombre de usuario y que se guarda en la estación de trabajo (aquellos usuarios que acceden a varias estaciones pueden tener un perfil en cada una de ellas). Este perfil se denomina **perfil local** porque sólo es accesible desde la estación en que está creado.

Los usuarios que se conectan a un servidor *Windows 2003* pueden tener también perfiles en dicho servidor. De esta manera, se puede acceder al perfil independientemente de la estación en que se esté conectado. Este perfil se denomina **perfil de red** porque se puede acceder a él desde cualquier estación de la red.

Hay dos tipos de perfiles de red:

- **Perfil móvil**. Este tipo de perfil es asignado a cada usuario por los administradores pero puede ser modificado por el usuario y los cambios permanecen después de finalizar la conexión.

- **Perfil obligatorio.** Este tipo de perfil tiene la misma estructura que el **perfil móvil** pero asegura que los usuarios trabajen en un entorno común. Por tanto, puede ser modificado por el usuario pero los cambios realizados se pierden al finalizar la conexión. Sólo puede ser modificado (y guardados sus cambios) por los administradores.

Todos los perfiles locales se guardan por defecto en **\Documents and Settings\<nombre de usuario>**. En dicha ubicación se encuentran los subdirectorios de los usuarios que se crearon en el momento de la instalación (además de los que se hayan creado posteriormente) que son: **Administrador**, **All Users** y **Default User**.

- El perfil del **Administrador** es el que corresponde a dicho usuario.

- El perfil de **All Users** contiene las entradas que se incluirán en los perfiles de todos los usuarios del presente equipo e incluyen los iconos del escritorio y programas del menú **Inicio**, comunes a todos los usuarios.

- El perfil de **Default User** es el que corresponde a todo usuario que se conecta por vez primera o que no tenga asignado un perfil específico para él.

En cada uno de los perfiles puede haber las siguientes carpetas:

- **Datos de programa**. Almacena los datos específicos de los programas.
- **Cookies**. Almacena información sobre las preferencias del usuario.
- **Entorno de red**. Guarda los accesos directos a opciones de **Mis sitios de red**.
- **Escritorio**. Se guardan los iconos que aparecen en el escritorio del usuario incluyendo archivos, carpetas y accesos directos.
- **Favoritos**. Guarda los accesos directos a los programas favoritos y sus ubicaciones.
- **Configuración local**. Almacena los archivos de datos de programas, historial y archivos temporales.
- **Impresoras**. Guarda los accesos directos a los elementos de la carpeta *Impresoras*.
- **Menú Inicio**. Guarda los accesos directos que hay en el menú *Inicio*.
- **Mis documentos**. Guarda los documentos del usuario.
- **Mis imágenes**. Guarda los elementos de imagen del usuario.
- **Plantillas**. Contiene los accesos directos a plantillas del usuario.
- **Reciente**. Guarda los accesos directos usados recientemente.
- **SendTo**. Guarda los accesos directos a las utilidades de control de los documentos.

Las carpetas **Configuración local**, **Datos de programa**, **Entorno de red**, **Impresoras**, **Plantillas**, **Reciente** y **SendTo** están ocultas y no se ven a no ser que se indique expresamente, marcando **Mostrar todos los archivos y carpetas ocultos** de la ficha **Ver** de **Opciones de carpeta** del menú **Herramientas**.

Así mismo, pueden tener hasta tres archivos llamados: **NTuser.dat** (contiene los datos del **Registro** del usuario), **NTuser.dat.LOG** (que es un archivo donde se guardan los cambios anteriores, a la última modificación, por si hubiera algún problema y poder corregir los errores) y **NTuser.man** (contiene los datos del **Registro** del usuario pero es un archivo de sólo lectura y, por tanto, no se guardan los cambios).

Para asignar un perfil de usuario, un archivo de comandos para inicio de la sesión o un subdirectorio particular para la cuenta del usuario, está la ficha **Perfil** de la pantalla de **Propiedades** de cada usuario a la que se puede acceder desde la **Administración de equipos** (si no ha instalado el *Directorio Activo* o eN Windows XP o Vista) o **Usuarios y equipos de Active Directory**.

La ruta de acceso local

Indica el directorio local privado de cada usuario, en donde puede almacenar sus archivos y programas. Así mismo, es el directorio predeterminado que se utiliza en **Símbolo del sistema** y en todas las aplicaciones que no tienen definido un directorio de trabajo.

Facilita la tarea de hacer copias de seguridad de los archivos de cada usuario y su eliminación cuando se quite la cuenta de dicho usuario.

Deberá crearlo antes de especificar su ruta y su utilización es incompatible con **Conectar**.

Conectar a una unidad de red

Indica una conexión con la letra deseada al subdirectorio de red privado de cada usuario, en donde puede almacenar sus archivos y programas, así mismo, es el directorio predeterminado que se utiliza en **Símbolo del sistema** y en todas las aplicaciones que no tienen definido un directorio de trabajo.

Facilitan la tarea de hacer copias de seguridad de los archivos de cada usuario y su eliminación cuando se quite la cuenta de dicho usuario.

Al especificarlo, se crea automáticamente el subdirectorio indicado (en caso de no poder hacerlo, le mostrará un mensaje de error), si no existe.

Su utilización es incompatible con **Ruta de acceso local**.

LA DEFINICIÓN DE LOS USUARIOS DE LA RED

Usuarios en Windows

Las cuentas de usuario representan a una persona y se denominan **principales de seguridad** dentro del *Directorio Activo*, ya que son objetos del directorio a los que se asignan automáticamente identificadores de seguridad para iniciar sesiones en la red y tener acceso a los recursos.

Una cuenta de usuario permite que un usuario inicie sesiones en equipos y/o dominios con una identidad que se puede autentificar y autorizar para tener acceso a los recursos del dominio. Cada usuario que se conecta a la red debe tener su propia cuenta de usuario y su propia contraseña única. Por tanto, una cuenta de usuario se utiliza para:

- Autentificar la identidad del usuario.
- Autorizar o denegar el acceso a los recursos del dominio.
- Administrar otros principales de seguridad.
- Auditar las acciones realizadas con la cuenta de usuario.

Las cuentas de usuario pueden ser de dos tipos:

- **Usuarios globales**. Estas cuentas se crean en equipos Windows Server 2003 que sean controladores de dominio y pueden usarse para conectarse a los dominios en que están creadas y a otros dominios en los que se confía. Se crean, modifican o eliminan con la utilidad **Usuarios y equipos de Active Directory** de **Herramientas administrativas** de la opción **Programas** y se guardan en el *Directorio Activo*.

- **Usuarios locales**. Estas cuentas se crean en equipos con Windows XP, Windows Vista y Windows Server 2003 (que no sean controladores de dominio) y, por tanto, no pueden usarse para conectarse a ningún dominio. Se crean, modifican o eliminan con la utilidad **Administración de equipos** de **Herramientas administrativas** de la opción **Programas** del menú **Inicio**.

Windows proporciona dos cuentas de usuario predefinidas que se crean en el proceso de la instalación y pueden usarse para iniciar una sesión y tener acceso a los recursos. Estas cuentas son:

La **cuenta de usuario del Administrador** que le permite administrar el equipo en el que se creó. Esta cuenta puede ser renombrada pero no puede ser borrada, deshabilitada ni quitada del **grupo local de Administradores**. Es

importante renombrar y proteger esta cuenta con una contraseña especial, así como crear otras cuentas de administradores para proteger mejor la seguridad del servidor.

La **cuenta de usuario del Invitado**. Normalmente, esta cuenta está deshabilitada (y debería permanecer de esta manera) pero puede habilitarse si se desea que alguien pueda conectarse al equipo o dominio con ella (tenga en cuenta que no precisa ninguna contraseña). Esta cuenta puede borrarse y renombrarse.

Usuarios en Linux

Una de las primeras tareas de administración que conviene conocer es la gestión de usuarios. Es el usuario **root** (administrador) el que tiene la posibilidad de crear cuentas para el resto de usuarios del sistema.

La gestión de las cuentas de usuario se lleva a cabo a través de dos ficheros de configuración:

- El fichero **/etc/passwd** que contiene una línea por cada usuario creado en el sistema con la información relevante sobre cada usuario.
- El fichero **/etc/shadow** que se utiliza para almacenar la contraseña de los usuarios y parámetros relacionados con la validez de dichas contraseñas.

El formato de cada línea del fichero */etc/passwd* es el siguiente:

usuario:x:ID:GID:descripción:directorio_home:shell

Por ejemplo:

usuario1:x:500:500:usuario de prueba:/home/usuario1:/bin/bash

Como se puede observar, la información se compone de varios campos separados por el carácter de dos puntos (:):

- **Nombre del usuario** es el nombre o login con el que el usuario accede al sistema.

- **Campo reservado a la contraseña**. En versiones antiguas de Unix, se almacenaba aquí la contraseña encriptada. Sin embargo, en versiones más recientes, en este campo se escribe una x indicando que la contraseña se almacena en el fichero */etc/shadow*. Podemos deshabilitar temporalmente el acceso a un usuario escribiendo un carácter * en este campo.

- **ID** es el identificador de usuario. Debe ser único en el sistema.
- **GID** es el identificador del grupo al que pertenece el usuario por defecto.
- **Texto descriptivo del usuario**. En algunos sistemas este campo se utiliza para incluir el nombre completo del usuario y sus datos personales.
- **Directorio home del usuario**.
- **Nombre de la shell por defecto** para el usuario cuando acceda al sistema.

La tradición en el mundo Linux aconseja trabajar con el usuario *root* el tiempo mínimo imprescindible. Este usuario puede leer, modificar o borrar cualquier fichero en el sistema, cambiar permisos y ejecutar programas peligrosos como pueden ser los que particionan discos o crean sistemas de ficheros. Con esta libertad es fácil cometer errores que tengan consecuencias importantes, incluso catastróficas cuando hablamos de equipos utilizados como servidores.

Para los usuarios que estén acostumbrados al trabajo con el sistema operativo Windows, es otra forma de trabajo completamente diferente, ya que en estos sistemas se tiende a trabajar con usuarios que poseen todos los permisos de administración, mientras que en Linux se propone justo lo contrario: trabajar con usuarios no administradores salvo cuando haya que realizar alguna tarea de administración.

La creación de nuevos usuarios se puede realizar de dos formas, modificando "manualmente" los ficheros de configuración o utilizar los comandos proporcionados por el sistema. Se recomienda esta última opción.

LA CREACIÓN DE GRUPOS

Los usuarios de la red pueden agruparse para permitirles compartir los datos aunque procedan de distintos lugares del árbol del directorio. Concediendo a un grupo privilegios para un subdirectorio, los miembros del grupo pueden acceder a archivos compartidos que no están accesibles a otros usuarios de la red.

Se suelen definir normalmente los grupos incluyendo a todas las personas que realizan una tarea en particular.

El proceso de creación de grupos consta de tres pasos básicos:

1. Crear el grupo que se va añadir.
2. Conceder derechos de archivo y directorio al grupo.
3. Añadir los usuarios al grupo.

Las cuentas de grupo en Windows

Las cuentas de grupo representan a un grupo y se denominan **principales de seguridad** dentro del *Directorio Activo*, ya que son objetos del directorio a los que se asignan automáticamente identificadores de seguridad.

Cada grupo tiene un ámbito que identifica el alcance de aplicación del grupo. Existen cuatro tipos de grupos en función de su ámbito de aplicación:

- **Grupos de ámbito universal**. Éstos (únicamente pueden crearse en equipos con Windows Server 2003 que tengan instalado el *Directorio Activo)* pueden tener como miembros a otros grupos universales, grupos globales y cuentas de cualquier dominio de Windows Server 2003, y se les puede conceder permisos en cualquier dominio. También se les denomina **grupos universales**. Se crean, modifican o eliminan con la utilidad **Usuarios y equipos de Active Directory** de **Herramientas administrativas** de la opción **Programas**, y se guardan en el *Directorio Activo*.

- **Grupos de ámbito global**. Éstos (únicamente pueden crearse en equipos con Windows Server 2003 que tengan instalado el *Directorio Activo)* pueden tener como miembros a grupos globales y cuentas únicamente del dominio en el que se ha definido el grupo, y se les puede conceder permisos en cualquier dominio. También se les denomina **grupos globales**. Se crean, modifican o eliminan con la utilidad **Usuarios y equipos de Active Directory** de **Herramientas administrativas** de la opción **Programas**, y se guardan en el *Directorio Activo*.

- **Grupos de ámbito local de dominio**. Éstos (únicamente pueden crearse en equipos con Windows Server 2003 que tengan instalado el *Directorio Activo)* pueden tener como miembros a grupos universales, grupos globales, grupos locales de dominio de su propio dominio y cuentas de cualquier dominio de Windows Server 2003, y sólo se pueden utilizar para conceder permisos en el dominio que contiene el grupo. También se les denomina **grupos de dominio local**. Se crean, modifican o eliminan con la utilidad **Usuarios y equipos de Active**

Directory de **Herramientas administrativas** de la opción **Programas**, y se guardan en el *Directorio Activo*.

- **Grupos locales**. Únicamente pueden crearse en equipos que ejecutan Windows XP, Windows Vista o que sean servidores miembros o independientes (equipos con Windows Server 2003 que no tienen instalado el *Directorio Activo*). Pueden tener como miembros a cuentas locales del equipo en el que se crean y, si el equipo forma parte de un dominio, podrá tener también cuentas y grupos globales del propio dominio y de los dominios de confianza. Además, se pueden utilizar para conceder permisos en el equipo en el que se crea el grupo. Se crean, modifican o eliminan con la utilidad **Administración de equipos** de **Herramientas administrativas** de la opción **Programas** del menú **Inicio**.

CUENTAS DE GRUPO CREADAS EN LA INSTALACIÓN

Los grupos se utilizan para agregar a los usuarios (o equipos) de forma que se puedan asignar, más fácilmente, privilegios a dichos usuarios (o equipos) y hacer más sencilla su administración. Por tanto, se puede incorporar un usuario (o equipo) a uno o a varios grupos teniendo, en cada uno de ellos, unos permisos determinados que le permitirán realizar distintas funciones.

Cuando se procedió a la instalación se crearon distintos grupos que estaban en función del tipo de instalación realizada (básicamente si se instala o no el *Directorio* Activo). En Windows son los siguientes:

- **Si no se instala el Directorio Activo en Windows Server 2003, son equipos con Windows XP o Windows Vista**. En este caso, los grupos que se crean durante el proceso de instalación son únicamente **grupos locales** y son los siguientes:
  - **Administradores**. Tienen control total sobre el equipo y se les conceden automáticamente todos los derechos y capacidades integradas del sistema. Pueden asignar derechos de usuario y permisos de control de acceso a quien consideren conveniente.
  - **Duplicadores**. Su función es la de realizar la replicación de archivos en el dominio y tendrá un único miembro que será una cuenta de usuario que se utilizará para iniciar los servicios correspondientes (no se deberán agregar a este grupo las cuentas de los usuarios reales).
  - **Invitados**. Este grupo permite a los usuarios ocasionales iniciar una sesión en el equipo utilizando la cuenta de *Invitado* y se le conceden menos capacidades que al **grupo local de Usuarios**.

- **Operadores de configuración de red**. Pueden modificar la configuración TCP/IP, así como renovar y liberar las direcciones IP del equipo.
- **Operadores de copia**. Pueden realizar copias de seguridad y restaurar los archivos en el equipo, independientemente de los permisos que protejan dichos archivos. También pueden iniciar una sesión en el equipo y cerrarlo, pero no pueden cambiar la configuración de seguridad.
- **Operadores de impresión**. Pueden administrar las impresoras y las colas de impresión del equipo.
- **Usuarios**. Realizan, entre otras, las siguientes tareas: ejecutar aplicaciones, utilizar impresoras locales y de red, cerrar y bloquear la estación de trabajo pero no pueden compartir directorios ni crear impresoras locales.
- **Usuarios avanzados**. Crean cuentas de usuario y grupos locales en el equipo pero, únicamente, pueden modificar y eliminar las cuentas que ellos hayan creado.
- **Usuarios del escritorio remoto**. Pueden iniciar sesión en un servidor de forma remota.
- **Usuarios del monitor del sistema**. Supervisan los contadores de rendimiento del servidor, tanto de forma local como de forma remota.
- **Usuarios del registro de rendimiento**. Administran los contadores de rendimiento, registros y alertas del servidor, tanto de forma local como de forma remota.
- **HelpServicesGroup**. Permite que los administradores establezcan permisos comunes para todas las aplicaciones de soporte técnico. De forma predeterminada, el único miembro del grupo es la cuenta **SUPPORT_388945a0** asociada a las aplicaciones de soporte técnico de Microsoft. No añada más usuarios a este grupo.
- **TelnetClients**. Pueden acceder al servidor *Telnet* del sistema.

- **Si se instala el Directorio Activo en Windows Server 2003**. En este caso, los grupos que se crean durante el proceso de instalación son de **dominio local**, **integrado local**, **globales** o **universales**.

  - **Grupos creados en la carpeta Builtin**, del tipo integrado local. Entre ellos se encuentran los siguientes:
    - **Acceso compatible con versiones anteriores de Windows 2000**. Permite, únicamente, el acceso de lectura a todos sus usuarios y grupos en los controladores de dominio. Se proporciona para garantizar la compatibilidad con versiones anteriores en los equipos que utilizan Windows NT 4 o anteriores.

- **Administradores**. Permite a sus miembros tener control total sobre todos los controladores de dominio.
- **Creadores de confianza de bosque de entrada**. Aparece, únicamente, en el controlador de dominio raíz del bosque y permite a sus miembros crear confianzas de entrada unidireccionales en el dominio.
- **Duplicadores**. Permite realizar funciones de replicación de directorio (no se deben agregar a este grupo las cuentas de los usuarios reales).
- **Grupo de acceso de autorización de Windows.** Es un grupo integrado local que permite a sus miembros tener acceso al atributo *tokenGroupsGlobalAndUniversal* calculado en objetos de usuario.
- **Invitados**. Permite a los usuarios ocasionales iniciar una sesión en los controladores de dominio utilizando la cuenta de *Invitado* y se le conceden menos capacidades que al grupo de **Usuarios**.
- **Operadores de configuración de red**. Permite a sus miembros modificar la configuración TCP/IP, así como renovar y liberar las direcciones IP en los controladores del dominio.
- **Operadores de copia**. Sus miembros pueden realizar copias de seguridad y restaurar los archivos en los controladores de dominio, independientemente de los permisos que protejan dichos archivos. También pueden iniciar una sesión en los controladores de dominio y apagarlos, pero no pueden cambiar la configuración de seguridad.
- **Operadores de cuentas**. Sus miembros pueden crear, modificar y eliminar cuentas de usuarios, grupos o equipos que se encuentren en los contenedores *Users*, *Computers* y en las unidades organizativas del dominio (excepto en *Domain Controllers*).
- **Operadores de impresión**. Permite a sus miembros crear, administrar, compartir y borrar impresoras que estén conectadas a los controladores del dominio, así como conectarse y parar los servidores.
- **Operadores de servidores**. Sus miembros pueden administrar los controladores de dominio.
- **Servidores de licencias de Terminal Server**. Permite a sus miembros administrar las licencias de los Servicios de Terminal.
- **Usuarios**. Es un grupo integrado local que posibilita a sus miembros realizar, entre otras, las siguientes tareas: ejecutar aplicaciones, utilizar impresoras locales y de red, cerrar y bloquear el equipo pero no pueden compartir directorios ni crear impresoras locales.

- **Usuarios del escritorio remoto**. Permite a sus miembros iniciar sesión en los controladores de dominio de forma remota.
- **Usuarios del monitor del sistema**. Sus miembros pueden supervisar los contadores de rendimiento de los controladores de dominio, tanto de forma local como de forma remota.
- **Usuarios del registro de rendimiento**. Permite a sus miembros administrar los contadores de rendimiento, registros y alertas de los controladores de dominio, tanto de forma local como de forma remota.

- **Grupos creados en la carpeta Users**, del tipo dominio local, globales o universales, y son los siguientes:
  - **Administradores de DHCP**. Es un grupo de dominio local del que forman parte todos los usuarios que tienen asignada la administración del servicio *DHCP*.
  - **Administradores de esquema**. Es un grupo universal del que forman parte todos los usuarios que tienen asignada la administración del esquema del Directorio Activo.
  - **Administradores de organización**. Es un grupo universal del que forman parte todos los administradores que controlan por completo todos los dominios del bosque.
  - **Administradores del dominio**. Es un grupo global del que forman parte todos los administradores que controlan por completo el dominio.
  - **Controladores del dominio**. Es un grupo global del que forman parte todos los equipos que son controladores del dominio.
  - **DnsAdmins**. Es un grupo de dominio local del que forman parte todos los usuarios que tienen asignada la administración del servidor DNS. Se crea cuando se instala el servidor DNS.
  - **DnsUpdateProxy**. Es un grupo global del que forman parte todos los usuarios clientes *DNS* que tienen permiso para efectuar actualizaciones dinámicas en nombre de otros clientes. Se crea cuando se instala el servidor DNS.
  - **Equipos del dominio.** Es un grupo global del que forman parte todos los servidores (que no sean controladores de dominio) y estaciones del dominio.
  - **Invitados del dominio.** Es un grupo global del que forman parte todos los invitados del dominio.
  - **Propietarios del creador de directivas de grupo**. Es un grupo global del que forman parte todos los usuarios que pueden modificar la directiva de grupo del dominio.

- **Publicadores de certificados**. Es un grupo de dominio local del que forman parte todos los usuarios que tienen permitida la publicación de certificados para usuarios y equipos.
- **Servidores RAS e IAS**. Es un grupo de dominio local del que forman parte todos los servidores que pueden obtener propiedades de acceso remoto de los usuarios.
- **Usuarios de DHCP.** Es un grupo de dominio local del que forman parte todos los usuarios que tienen acceso de sólo lectura al servicio *DHCP*.
- **Usuarios del dominio**. Es un grupo global del que forman parte todos los usuarios del dominio.

Las cuentas de grupo en Linux

Otro elemento de gestión de usuarios en Linux son los **grupos**, que no son más que agrupaciones de usuarios para establecer criterios comunes de accesibilidad. En Linux cada fichero tiene asociado un grupo al que pertenece; además, para cada fichero o directorio se pueden definir los permisos para el grupo al que pertenece. Realmente, ésta es la utilidad de los grupos: poder realizar asignaciones de permisos a ficheros o directorios para un conjunto de usuarios. Un usuario puede pertenecer a varios grupos.

Los grupos de usuarios se gestionan a través del fichero de configuración **/etc/group**.

El formato de este fichero es el siguiente:

nombre:x:GID:usuarios

En donde:

- El campo **nombre** es el nombre del grupo.
- El campo **x** indica que si el grupo tiene contraseña, ésta se almacena en el fichero */etc/gshadow*.
- **GID** es el identificador del grupo.
- **Usuarios**. Aquí se especifican los usuarios que pertenecen a un grupo separados por comas (,).

La creación de grupos se puede realizar de dos formas, modificando "manualmente" los ficheros de configuración o utilizar los comandos proporcionados por el sistema. Se recomienda esta última opción.

ESTABLECER LA ADMINISTRACIÓN DE SEGURIDAD

La administración de seguridad se usa para asignar derechos a los usuarios y grupos que les permitan trabajar dentro de los directorios y archivos, o derechos para administrar objetos y propiedades.

La administración de seguridad en Windows

Hay que distinguir entre permisos estándar y permisos de acceso especial tanto a nivel de directorios como de archivos.

LOS PERMISOS ESTÁNDAR DE DIRECTORIO

Cuando se establecen permisos sobre un directorio, se define el acceso de un usuario o de un grupo a dicho directorio y sus archivos. Estos permisos sólo pueden establecerlos y cambiarlos el propietario o aquel usuario que haya recibido el permiso del propietario y sólo es posible establecer permisos para directorios de unidades formateadas con el sistema **NTFS**.

Una vez establecidos los permisos, afectarán a los archivos y subdirectorios que dependan de él, tanto los que se creen posteriormente como los que ya existían previamente (este hecho se denomina **herencia**). Si no desea que se hereden, deberá indicarse expresamente cuando se indiquen los permisos.

Hay tres modos de realizar cambios en los permisos heredados:

- Realizar los cambios en el carpeta principal y la carpeta secundaria heredará estos permisos.

- Seleccione el permiso contrario (**Permitir** o **Denegar**) para sustituir el permiso heredado.

- Desactivar la casilla de verificación. En Windows XP: **Heredar del objeto principal las entradas de permisos…**, en Windows Vista: **Incluir todos los permisos heredables…** o en Windows Server 2003: **Permitir que los permisos heredables del primario se propaguen a este objeto …**. De esta manera, podrá realizar cambios en los permisos, ya que la carpeta no los heredará de la carpeta principal.

Los permisos estándar para directorios que se pueden conceder o denegar son:

- **Control total**. Es el máximo nivel y comprende todas las acciones tanto al nivel de archivos como de directorios.

- **Modificar**. Comprende todos los permisos menos eliminar los archivos y directorios, cambiar los permisos y tomar posesión.

- **Lectura y ejecución**. Comprende ver los nombres de los archivos y directorios, los datos de los archivos, los atributos y permisos, y ejecutar programas.

- **Listar** o **Mostrar el contenido de la carpeta**. Comprende los mismos permisos que **lectura y ejecución** pero aplicables sólo a las carpetas.

- **Leer** o **Lectura**. Comprende ver los nombres de los archivos y directorios, los atributos, los datos de los archivos y los permisos.

- **Escribir** o **Escritura**. Comprende crear archivos y directorios, escribir los atributos, añadir datos a los archivos y leer los permisos.

Estos permisos son acumulables pero denegar el permiso **Control total** elimina todos los demás.

Para establecer permisos estándar de directorio se utiliza el **Explorador de Windows**.

LOS PERMISOS ESTÁNDAR DE ARCHIVO

Cuando se establecen permisos sobre un archivo, se define el acceso de un usuario o de un grupo a dicho archivo. Los archivos que se crean en un directorio adoptan por defecto los permisos del directorio del que forman parte.

Estos permisos sólo pueden establecerlos y cambiarlos el propietario o aquel usuario que haya recibido el permiso del propietario.

Sólo es posible establecer permisos para archivos de unidades formateadas para ser usadas por el sistema **NTFS**.

Los permisos estándar para archivos que se pueden conceder o denegar son:

- **Control total**. Es el máximo nivel y comprende todas las acciones al nivel del archivo.

- **Modificar**. Comprende todos los permisos menos eliminar el archivo, cambiar los permisos y tomar posesión.

- **Lectura y ejecución**. Comprende ver el nombre del archivo, sus datos, sus atributos y permisos y ejecutarlo.

- **Leer** o **Lectura**. Comprende ver el nombre del archivo, sus datos, los atributos y permisos.

- **Escribir** o **Escritura**. Comprende añadir datos al archivo, escribir sus atributos y ver sus permisos.

Estos permisos son acumulables, pero denegar el permiso **Control total** elimina todos los demás.

Para establecer permisos estándar de archivo se utiliza el **Explorador de Windows**.

LOS PERMISOS ESPECIALES

Generalmente, todo lo que necesitará para proteger los directorios y los archivos son los permisos estándar que se han descrito anteriormente.

Sin embargo, si desea crear un sistema personalizado de permisos, puede utilizar los permisos especiales.

Puede establecer permisos especiales para directorios, para todos los archivos de los directorios seleccionados o para los archivos seleccionados (los no seleccionados mantendrán sus actuales permisos).

Estos permisos sólo pueden establecerlos y cambiarlos el propietario o aquel usuario que haya recibido el permiso del propietario.

Sólo es posible establecer permisos para archivos de unidades formateadas para ser usadas por el sistema **NTFS**.

Los permisos especiales para directorios y archivos son:

- **Recorrer carpeta/Ejecutar archivo**. El permiso **Recorrer carpeta** (sólo afecta a los directorios) comprende el desplazamiento por las carpetas para llegar a otros archivos o carpetas, incluso si el usuario no tiene permisos para las carpetas recorridas (sólo entra en vigor cuando el grupo o usuario no tiene otorgado el derecho de usuario **Saltarse la comprobación de recorrido** en la **Directiva de grupo**). El permiso **Ejecutar archivo** comprende la ejecución de archivos de programa (sólo afecta a los archivos) y al configurar el permiso **Recorrer carpeta**

en un directorio no se define de manera automática el permiso **Ejecutar archivo** en todos sus archivos.

- **Listar** o **Mostrar carpeta/Leer datos**. El permiso **Listar** o **Mostrar carpeta** (sólo afecta a los directorios) comprende ver los nombres de los archivos y subdirectorios de la carpeta. El permiso **Leer datos** comprende ver los datos de los archivos (sólo afecta a los archivos).

- **Atributos de lectura** o **Leer atributos**. Comprende ver los atributos normales de un archivo o directorio.

- **Atributos extendidos de lectura** o **Leer atributos extendidos**. Comprende ver los atributos extendidos de un archivo o directorio (estos atributos se definen mediante programas y pueden variar según el programa).

- **Crear archivos/Escribir datos**. El permiso **Crear archivos** (sólo afecta a los directorios) comprende la creación de archivos dentro de la carpeta. El permiso **Escribir datos** (sólo afecta a los archivos) comprende los cambios en los archivos y la sobrescritura de su contenido.

- **Crear carpetas/Anexar datos**. El permiso **Crear carpetas** (sólo afecta a los directorios) comprende la creación de subdirectorios dentro de la carpeta. El permiso **Anexar datos** (sólo afecta a los archivos) comprende el añadido de contenido del archivo pero no el cambio, eliminación ni sobrescritura de los datos existentes.

- **Atributos de escritura** o **Escribir atributos**. Comprende el cambio de los atributos normales de un archivo o directorio.

- **Atributos extendidos de escritura** o **Escribir atributos extendidos**. Comprende el cambio de los atributos extendidos de un archivo o directorio (estos atributos se definen mediante programas y pueden variar según el programa).

- **Eliminar subcarpetas y archivos**. Comprende la eliminación de subdirectorios y archivos.

- **Eliminar**. Comprende la supresión del archivo o directorio.

- **Permisos de lectura**. Comprende ver los permisos del archivo o directorio.

- **Cambiar permisos**. Comprende el cambio de los permisos del archivo o directorio.

- **Tomar posesión**. Comprende la toma de posesión del archivo o directorio. El propietario de un archivo o carpeta siempre puede cambiar los permisos en la misma, independientemente de los permisos existentes que protejan al archivo o carpeta.

Para establecer permisos especiales se utiliza el **Explorador de Windows**.

La administración de seguridad en Linux

En Linux, los elementos que se encuentran en el sistema de ficheros, es decir, tanto ficheros como directorios, poseen una serie de características o propiedades que pueden visualizarse con el comando **ls –l**:

```
-rw-------    1 root     root        14596 mar 16 01:44 boot.log
-rw-------    1 root     root         3205 mar 16 02:01 cron
drwxr-xr-x    2 lp       sys          4096 mar  5 02:05 cups
-rw-r--r--    1 root     root         5951 mar 16 01:43 dmesg
drwxr-xr-x    2 root     root         4096 mar 16 01:44 gdm
-rw-r--r--    1 root     root        65404 mar 16 01:43 ksyms.0
-rw-r--r--    1 root     root        65404 mar  9 19:50 ksyms.1
-rw-r--r--    1 root     root        65404 mar  8 23:43 ksyms.2
-rw-r--r--    1 root     root        69134 mar  5 01:47 ksyms.3
-r--------    1 root     root     19136220 mar 16 01:49 lastlog
-rw-------    1 root     root         3242 mar 16 01:44 maillog
-rw-------    1 root     root        77967 mar 16 02:02 messages
-rw-r--r--    1 root     root        16109 mar  9 20:56 rpmpkgs
-rw-r--r--    1 root     root        11301 mar  5 01:39
scrollkp.log
-rw-------    1 root     root          841 mar 16 01:45 secure
-rw-------    1 root     root            0 mar  5 01:16 spooler
drwxr-xr-x    2 root     root         4096 feb  4  2006 vbox
-rw-rw-r--    1 root     utmp        53760 mar 16 02:03 wtmp
-rw-r--r--    1 root     root        43584 mar 16 02:02
XFree86.0.lo
-rw-r--r--    1 root     root        46606 mar  9 23:55
XFree86.0.ol
```

Los campos que aparecen en este listado son los siguientes:

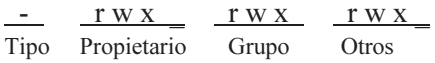
Campo	Descripción
Permisos	Define los permisos sobre el fichero o directorio (descrito a continuación).

Campo	Descripción
NL	Número de enlaces del fichero (descrito en el apartado sobre enlaces). Si es un directorio, indica el número de subdirectorios.
Prop	Nombre del propietario o dueño del fichero o directorio.
Grupo	Nombre del grupo al que pertenece el fichero o directorio.
Tam	Tamaño del fichero, en bytes.
Fecha y Hora	Indica la fecha y la hora de creación o modificación del fichero.
Nombre	Nombre del fichero.

```
Permisos      NL Prop  Grupo  Tam   Fecha  Hora   Nombre
drwxr-xr-x     2 lp    sys    4096  mar 5  02:05   cups
-rw-r--r--     1 root  root   5951  mar 16 01:43  dmesg
drwxr-xr-x     2 root  root   4096  mar 16 01:44   gdm
```

Como se puede observar en cualquier listado generado por el comando *ls*, todos los ficheros tienen asociado tanto un nombre de usuario, que es su propietario, como un nombre de grupo. Un **grupo** no es más que un conjunto de usuarios agrupados para poder establecer permisos de forma conjunta sobre los elementos del sistema de ficheros.

Una de las principales características del sistema de ficheros usado en Linux es que posee un robusto sistema de permisos. Cada fichero del sistema (en este apartado hablaremos de permisos de ficheros pero lo mismo se puede aplicar a directorios) tiene una serie de permisos que definen su accesibilidad a todos los usuarios del sistema. Para ello, se utiliza un grupo de 10 caracteres desglosado de la siguiente forma:



El primer carácter indica el tipo de fichero:

-	Archivo ordinario
d	Directorio
B	Archivo especial tipo bloque
C	Archivo especial tipo carácter

Los otros nueve caracteres indican, en agrupaciones de tres, los permisos de acceso a ese fichero. La primera agrupación son los permisos del propietario del fichero, la segunda agrupación son los permisos del grupo al que pertenece el fichero y la última agrupación son los permisos del fichero para el resto de usuarios.

Cada agrupación tiene tres caracteres con el siguiente significado:

- **Primer carácter**: si aparece una 'r', el permiso de lectura sobre el fichero está activado. Si aparece un '-', significa que no tiene permiso de lectura sobre ese fichero.

- **Segundo carácter**: si aparece una 'w', el permiso de escritura sobre el fichero está activado. Si aparece un '-', significa que no tiene permiso de escritura sobre ese fichero.

- **Tercer carácter**: si aparece una 'x', el permiso de ejecución sobre el fichero está activado. Si aparece un '-', significa que no tiene permiso de ejecución sobre ese fichero.

LA IMPRESIÓN EN LA RED

Cuando se realiza una impresión en la red es necesario distinguir entre los distintos elementos que intervienen en dicha impresión:

- Una **impresora** propiamente dicha es la máquina en la que se va a producir físicamente la impresión de un trabajo. Puede dar soporte a una o varias colas de impresión (es importante distinguir entre **impresora** e **impresora lógica**, que es equivalente a cola de impresión).

- Una **cola de impresión** es un archivo en el que se van a guardar los trabajos que se manden imprimir hasta que la impresora pueda darles salida. Puede dar soporte a una o varias impresoras (es lo que se hace al agregar una impresora). De manera predeterminada, la carpeta donde se guardan los archivos de cola de impresión se encuentran en *\WINDOWS\ system32\spool\PRINTERS*. Si el servidor de impresión únicamente sirve a una o dos impresoras con un volumen de tráfico reducido, esta ubicación predeterminada será suficiente, pero, si se requiere un volumen elevado de impresión (por haber un gran número de impresoras o trabajos de impresión de gran tamaño), será conveniente cambiar la ubicación de la carpeta.

- Un **servidor de impresión** es un ordenador (servidor o estación de trabajo) en el que está conectada físicamente la impresora y que se encarga de solicitar a la cola de impresión que le envíe los trabajos cuando ésta está disponible. Puede dar soporte a varias impresoras y varias colas de impresión.

Utilizar un servidor de impresión proporciona las siguientes ventajas:

- El servidor de impresión administra la configuración del controlador de impresión.
- En todos los equipos que estén conectados a una impresora, únicamente aparece una cola de impresión (lo que permite a los usuarios ver la posición de su trabajo de impresión respecto a los demás trabajos en espera).
- Los mensajes de error aparecen en todos los equipos (por lo que todos los usuarios conocen el verdadero estado de la impresora).
- Parte del proceso de impresión se transfiere del equipo cliente al servidor de impresión por lo que aumenta la capacidad de trabajo de la estación.
- Se puede establecer un registro único para aquellos administradores que deseen auditar los sucesos de la impresora.

- Un **controlador de impresora** es un programa de *software* que utilizan los programas para comunicarse con las impresoras, convirtiendo la información enviada desde el equipo a comandos que pueda entender cada impresora (normalmente, los controladores de impresora no son compatibles entre las distintas plataformas, por lo que se deben instalar diversos controladores en cada servidor de impresión para admitir diferentes componentes de *hardware* y sistemas operativos).

  En general, los controladores de impresora están formados por tres tipos de archivos:

  - **Archivo de configuración** o interfaz de impresora que muestra los cuadros de diálogo *Propiedades* y *Preferencias* cuando se configura una impresora en Windows (tiene la extensión *DLL*).
  - **Archivo de datos** que proporciona información acerca de las capacidades de una impresora específica incluida su capacidad de resolución, si puede imprimir en ambas caras de la página y el tamaño de papel que puede aceptar (en Windows puede tener la extensión *DLL*, *PCD*, *GPD* o *PPD*).
  - **Archivo de controlador de gráficos de impresora** que convierte los comandos de *interfaz de controlador de dispositivo*

(*DDI*) en comandos que pueda entender la impresora. Cada controlador convierte un lenguaje de impresora diferente (en Windows tiene la extensión *DLL*).

- El **procesador de impresión** indica a la cola de impresión que modifique un trabajo en función del tipo de datos del documento. Envía los trabajos de la cola de impresión a la impresora (junto con el controlador correspondiente).

  El procesador de impresión de Windows admite cinco tipos de datos:

  - **NT EMF** (**metarchivo mejorado**). Con este tipo de datos, el documento impreso se convierte a un formato de metarchivo mucho más portátil que los archivos **RAW** que, normalmente, pueden imprimirse en cualquier impresora. El tamaño de los archivos **EMF** suele ser menor que el de los archivos **RAW** que contienen el mismo trabajo de impresión. Referente al rendimiento, sólo la primera parte del trabajo de impresión se altera o se procesa en el equipo cliente, la mayor parte del efecto lo experimenta el equipo servidor de impresión, lo que también permite que la aplicación del equipo de cliente devuelva el control al usuario con más rapidez. Es el tipo de datos predeterminado para la mayoría de los programas basados en Windows (hay varias versiones).

  - **RAW**. Indica a la cola de impresión que no altere de ningún modo el trabajo antes de la impresión. Con este tipo de datos, todo el proceso de preparación del trabajo de impresión se realiza en el equipo de cliente. Es el tipo de datos predeterminado para clientes que no utilizan programas basados en Windows.

  - **RAW [FF appended]**. Actúa igual que el tipo *RAW* pero incluye un carácter de avance de página (es útil para las impresoras *PCL*, ya que omiten la última página del documento si no hay un avance final de página).

  - **RAW [FF auto]**. Actúa igual que el tipo *RAW* pero, además, busca un carácter de avance de página al final del trabajo y, si no lo encuentra, lo añade.

  - **TEXT**. Interpreta todo el trabajo como texto *ANSI* y agrega las especificaciones de impresión mediante la configuración predeterminada de fábrica del dispositivo de impresión (es útil

cuando el trabajo de impresión se ha realizado en texto sencillo y el dispositivo de impresión no es capaz de interpretarlo).

- **Página de separación**. Una página de separación (*banner*) indica el usuario que envió el documento a la impresora, y la fecha y hora de la impresión. Se puede utilizar una de las páginas de separación que incorpora el sistema o crear una página personalizada.

  Las páginas de separación que incorpora Windows se encuentran en la carpeta *\WINDOWS\system32* y son las siguientes:

  - **PCL.SEP**. Cambia la impresora al modo *PCL* e imprime una página de separación antes de cada documento.

  - **PSCRIPT.SEP**. Cambia la impresora al modo *PostScript* pero no imprime ninguna página de separación antes de cada documento.

  - **SYSPRINT.SEP**. Cambia la impresora al modo *PostScript* e imprime una página de separación antes de cada documento (existe una versión en japonés que es **SYSPRTJ.SEP**).

- **Fuentes de impresora**. Las fuentes de impresora permiten mostrar el texto en distinto formato y tamaño. Pueden ser de tres tipos:

  - **Fuentes internas**. Se utilizan principalmente en impresoras láser, matriciales y de inyección de tinta. Se cargan previamente en la memoria de la impresora (*ROM*).

  - **Fuentes de cartucho**. Son fuentes añadidas que están almacenadas en un cartucho o en una tarjeta que se conecta a la impresora.

  - **Fuentes descargables**. Son juegos de caracteres enviados desde el equipo a la memoria de una impresora cuando se necesitan para imprimir (también se pueden llamar **fuentes transferibles**). Se usan principalmente en impresoras láser y otras impresoras de páginas, aunque también en algunas impresoras matriciales.

- **Grupo de impresión**. Se utiliza para distribuir automáticamente los trabajos de impresión a la siguiente impresora disponible. Un grupo de impresión está compuesto por una cola de impresión conectada a varias impresoras a través de varios puertos del servidor de impresión. La impresora física que esté inactiva recibirá el siguiente documento enviado a la cola de impresión (es aconsejable en redes con un alto

volumen de trabajos de impresión, ya que disminuye el tiempo que los usuarios esperan para que se impriman sus documentos. También simplifican la administración, ya que permiten administrar varias impresoras desde la misma cola de impresión de un servidor). Para configurar un grupo de impresión, es necesario tener en cuenta los factores siguientes:

- Todas las impresoras de un grupo deben utilizar el mismo controlador.

- Puesto que los usuarios no sabrán la impresora del grupo en que se imprimirá su documento, todas las impresoras del grupo deben encontrarse en el mismo lugar.

Para poder utilizar una impresora física, es necesario crear una impresora (en Windows o Linux) que tenga los controladores necesarios para poder utilizarla.

Este proceso puede hacerlo el usuario root (en Linux) o un usuario que tenga el permiso **Administrar impresoras** en Windows (por defecto, lo tienen todos los usuarios que pertenezcan a un grupo de **administradores**, **operadores de servidores** u **operadores de impresión**).

LOCALIZACIÓN Y RESOLUCIÓN DE PROBLEMAS

Es necesario controlar el rendimiento del sistema revisando ciertos factores como, por ejemplo, el tiempo que tarda el sistema en recuperar los programas del disco duro del servidor, en clasificar una base de datos, en ejecutar un programa, en guardar un archivo, etc.

Los cambios en el rendimiento ocurren normalmente de forma gradual, aunque no lo note hasta que sucede algo anormal en la red.

Normalmente, debido a la forma de trabajo del sistema operativo de la red, el rendimiento de un disco duro de la red es superior al obtenido con otro tipo de unidades.

Controle de forma periódica el rendimiento del sistema y compare los resultados sucesivos. Será capaz de distinguir las variaciones en el rendimiento cuando la red esté ocupada y, al mismo tiempo, los resultados que produzcan podrán ser la primera pista cuando el rendimiento del sistema empiece a funcionar peor.

Los problemas de funcionamiento de la red que se podrán encontrar pueden depender del *software* o del *hardware*.

Localización y resolución de problemas de software

Generalmente, los problemas de *software* se originan al no ser instalados de forma adecuada o al utilizar programas monousuario en la red. Normalmente, estos problemas afectan solamente a algún programa y pueden ocurrirle a uno o a todos los usuarios de dicho programa.

Si sospecha que el fallo de funcionamiento es debido a un problema de *software*, lo primero que deberá hacer es comprobar los derechos de todos los usuarios que están teniendo problemas.

Un error muy común es instalar y probar el *software* como administrador y, como tiene todos los derechos en todos los directorios, puede ocurrir que después se genere algún error al no contar los usuarios con tantos derechos como él.

Si los derechos de seguridad no son la causa del problema, compruebe la configuración del *software*. Muchos de los programas contienen archivos ejecutables y archivos de configuración, así que deben estar localizados en directorios compartidos.

Si aún sigue dando problemas, vuelva a reinstalar el *software* en un nuevo subdirectorio y siga al pie de la letra el manual sin saltarse ningún paso de la instalación.

Si no se soluciona el problema, consulte con el distribuidor del programa.

Localización y resolución de problemas de hardware

La localización y reparación de los problemas de *hardware* empiezan en la estación de trabajo que produce el error de funcionamiento.

Cuando ocurra un problema de *hardware*, primero ha de inspeccionar la tarjeta adaptadora de red instalada en la estación de trabajo, así como los cables de la red y las conexiones con la tarjeta.

COMPROBACIÓN DE LAS TARJETAS ADAPTADORAS DE RED

Si una estación de trabajo falla al colocarse por primera vez en la red, asegúrese de que la tarjeta está colocada de forma adecuada en el ordenador.

Si la estación sigue fallando, compruebe las especificaciones de la tarjeta adaptadora de red.

Otras tarjetas, como la del ratón, las tarjetas de puerto serie, controladoras, etc., pueden estar interfiriendo con la tarjeta de red. La mayoría de las veces no podrá saber las direcciones de las otras tarjetas que haya. En tal caso, la mejor solución es quitar las tarjetas que no sean esenciales. Después, coloque la tarjeta adaptadora de red en el ordenador e intente conectarse. Si puede hacerlo, empiece a colocar las otras tarjetas, una a una y probando la conexión cada vez, hasta encontrar la que origina el fallo de la estación de trabajo.

COMPROBACIÓN DE LOS CABLES

Los problemas de los cables son muy difíciles de diagnosticar. Si sospecha de un problema con un cable, primero compruebe que está conectado de forma adecuada con la tarjeta adaptadora de red.

Después, compruebe si el cable está partido. Un cable partido interrumpirá el acceso de la estación de trabajo a la red. Un cable dañado puede permitir a la estación de trabajo seguir funcionando, pero de forma deficiente.

También es posible que fallen las conexiones. Es fácil que no hagan buen contacto con el cable y no permitan el correcto funcionamiento.

COMPROBACIÓN DEL RESTO DEL HARDWARE

El *hardware* específico de la red, las tarjetas y los cables, no son siempre los únicos responsables de los problemas de *hardware*. A veces el problema está en el servidor o en una estación de trabajo.

Los tres componentes con más posibilidades de fallo del servidor son la tarjeta controladora del disco, el disco duro y la memoria *RAM*.

La tarjeta controladora y el disco duro del servidor están constantemente en uso y pueden fallar en cualquier momento. Cuando la tarjeta controladora funciona mal, el servidor puede enviar un mensaje de error (normalmente no). Cuando falla el disco duro, casi siempre aparece un mensaje de error en el momento de arrancar el servidor.

Los problemas con la memoria pueden generar algún mensaje. Algunas veces aparecerá un mensaje de error que informa de un problema en la memoria

que produce una paralización del servidor, pero puede que no se repita en un período de tiempo, con lo que es difícil la reparación por parte del servicio técnico.

CÓMO COMPARTIR DIRECTORIOS EN WINDOWS (PARTE PRÁCTICA)

Una vez que está creada la estructura de directorios, es necesario indicar los que se desean compartir para que el resto de los usuarios puedan acceder a ellos. Para compartir un directorio, siga los pasos siguientes:

1. Desde el **Explorador de Windows**, sitúese en el directorio que desea compartir o cree uno nuevo. Pulse sobre dicho directorio el botón derecho del ratón y seleccione **Compartir y seguridad** (en Windows XP) o **Propiedades**, **Compartir** y, después, **Uso compartido avanzado** (en Windows Vista y deberá indicar que desea continuar, si lo pregunta).

2. Active la casilla **Compartir esta carpeta** e indique el nombre de recurso compartido que desee darle.

   En el apartado **Descripción** (Windows XP) o **Comentario** (Windows Vista), indique un breve comentario para este recurso compartido.

   En Windows XP, deje activada la casilla **Máximo permitido** como límite de usuarios o active **Permitir este nº de usuarios** e indique el número de usuarios que pueden conectarse simultáneamente. Cuando haya finalizado, pulse en **Aceptar**.

   En Windows Vista, en **Establecer el límite de usuarios….**, mantenga o modifique el número indicado.

3. Pulse en **Permisos** y verá una pantalla parecida a la siguiente:

4. Fíjese que tiene permitido el permiso **Leer** para la identidad especial **Todos** (corresponde a todos los usuarios y grupos).

5. Puede activar o desactivar las casillas que desee tanto de la columna **Permitir**, se le concede el permiso correspondiente, como de la columna **Denegar**, se le deniega el permiso correspondiente.

6. Si pulsa en **Agregar**, pulsa en **Avanzadas** y pulsa en **Buscar ahora**, se le abrirá una ventana con todos los posibles usuarios, grupos e identidades especiales a las que puede otorgar o denegar permisos.

   Si selecciona elementos de la lista, pulsa en **Aceptar** y vuelve a pulsar en **Aceptar**, se añadirán a los grupos o usuarios que tienen permisos sobre la carpeta. Una vez que estén en la lista, indique los permisos que desea conceder o denegar a cada uno de los usuarios que ha añadido.

7. Si selecciona un usuario, grupo o identidad especial y pulsa en **Quitar**, se eliminará de la lista junto con los permisos establecidos.

8. Pulse en **Aceptar** para salir de la pantalla de **Permisos**.

9. Vuelva a marcar en **Aceptar** para salir de la pantalla de **Propiedades**. Repita todo el proceso con el resto de directorios que desea compartir en cada uno de los dos equipos.

CÓMO CONECTARSE A LOS DIRECTORIOS COMPARTIDOS EN WINDOWS (PARTE PRÁCTICA)

Para poder conectarse a los directorios e impresoras compartidas de red, siga los pasos siguientes:

En Windows XP:

1. Seleccione el icono **Mis sitios de red** y verá una pantalla donde le muestra el servidor o los servidores a los que está conectado. Si no los ve, seleccione **Toda la red**, después, **Red de Microsoft Windows** y, para finalizar, el grupo o dominio al que desea conectarse.

2. Sitúese sobre el equipo que desee y pulse dos veces el botón izquierdo del ratón. Se abrirá una nueva pantalla donde aparecerán los directorios compartidos que hay en ese servidor además de las

impresoras compartidas (sólo aparecerán si se hace como un usuario que esté dado de alta en el servidor).

3. Cuando haya acabado, cierre todas las ventanas que haya abiertas.

En Windows Vista:

1. Seleccione la opción **Red** del menú **Inicio** y verá que se muestran los equipos (en caso de no ver los equipos, vea el apartado *Activar la detección de redes en Windows Vista*).

2. Pulse sobre otro equipo (recuerde que únicamente accederá directamente a dicho equipo si el usuario se encuentra dado de alta en ambos equipos y tiene la misma contraseña. En caso contrario, le mostrará una ventana para que indique el usuario y la contraseña con la que desea conectarse) y verá los directorios que tiene compartidos

3. Cuando haya acabado, cierre todas las ventanas que haya abiertas.

NOTA. Para ver cómo compartir un directorio, vea el apartado *Cómo compartir directorios*.

CÓMO TRABAJAR CON LOS USUARIOS Y LOS GRUPOS (PARTE PRÁCTICA)

En Windows XP:

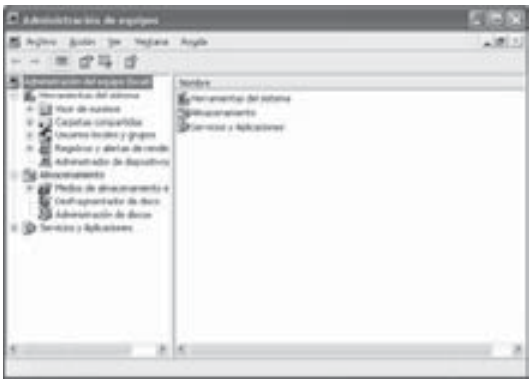
Es posible hacerlo de dos maneras:

- Utilizando **Cuentas de usuario** del **Panel de control**.
- Utilizando **Administrar** del menú contextual de **Mi PC**.

En el libro se va a utilizar esta segunda, ya que es la que se puede utilizar si el equipo pertenece a una red.

Para crear usuarios locales, siga los pasos siguientes:

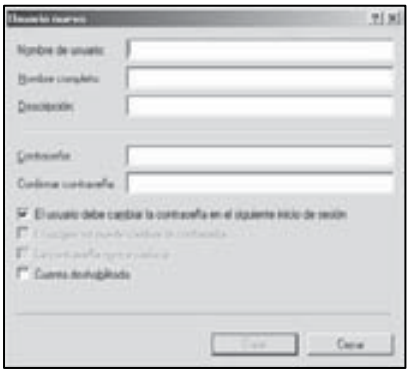
1. Seleccione **Administrar** del menú contextual de **Mi PC** y verá la siguiente pantalla:



2. Pulse el botón izquierdo del ratón sobre el signo + que hay a la izquierda de **Usuarios locales y grupos** y se desplegará su contenido: **Usuarios** y **Grupos**.

3. Pulse el botón izquierdo del ratón sobre **Usuarios** y, en el panel derecho, le mostrará los usuarios que hay dados de alta en el equipo.

4. Pulse el botón derecho del ratón sobre **Usuarios** para que muestre su menú contextual, seleccione **Usuario nuevo** y le mostrará la siguiente pantalla:



5. Indique el nombre que desea dar al usuario para conectarse (con un máximo de 20 caracteres), su nombre completo (es necesario seguir una norma ya que cuando se ordenen por el nombre completo será más fácil su búsqueda, por tanto, que todos empiecen por el nombre del usuario o que todos empiecen por su primer apellido), una breve descripción, su contraseña (con un máximo de 127 caracteres distinguiendo entre mayúsculas y

minúsculas. Si está en una red con equipos Windows 95/98 evite que tengan más de 14 caracteres), la confirmación de la contraseña y active las casillas que desee de las siguientes:

- **El usuario debe cambiar la contraseña en el siguiente inicio de sesión**. Esta opción obligará al usuario a cambiar la contraseña que le puso el administrador al darle de alta en la red la próxima vez que inicie una sesión.

- **El usuario no puede cambiar la contraseña**. Esta opción evita que los usuarios puedan modificar su contraseña.

- **La contraseña nunca caduca**. Al marcar esta opción, evita que la contraseña pueda caducar y deba cambiarla el usuario.

- **Cuenta deshabilitada**. Al marcar esta opción, nadie puede iniciar una sesión con el nombre de este usuario (por ejemplo, cuando el usuario se va de vacaciones, puede deshabilitarla para que nadie pueda tener acceso a sus recursos).

6. Cuando haya finalizado, pulse en **Crear** y ya estará creada la cuenta.

7. Puede repetir el proceso con otro usuario o pulse en **Cerrar** para volver a la lista de usuarios dados de alta en el equipo (fíjese en que el usuario o usuarios que acaba de crear figuran en la lista).

Para modificar usuarios locales y/o hacerlos miembros de algún grupo, siga los pasos siguientes:

1. Seleccione **Administrar** del menú contextual de **Mi PC** y verá la pantalla principal de la utilidad.

2. Pulse el botón izquierdo del ratón sobre el signo + que hay a la izquierda de **Usuarios locales y grupos** y se desplegará su contenido: **Usuarios** y **Grupos**.

3. Pulse el botón izquierdo del ratón sobre **Usuarios** y, en el panel derecho, le mostrará los usuarios que hay dados de alta en el equipo.

4. Sitúese sobre el usuario que desee modificar, pulse el botón derecho del ratón para que muestre su menú contextual, seleccione **Propiedades** y le mostrará la pantalla correspondiente.

5. Se encuentra en la ficha **General** y en ella se encuentran los siguientes apartados:

   - **Nombre completo**. Indica el nombre completo del usuario.

   - **Descripción**. Permite escribir una breve descripción del usuario.

   - **El usuario debe cambiar la contraseña en el siguiente inicio de sesión**. Indica si está establecido que el usuario cambie la contraseña la próxima vez que inicie una sesión.

   - **El usuario no puede cambiar la contraseña**. Evita que los usuarios puedan modificar su contraseña.

   - **La contraseña nunca caduca**. Evita que la contraseña pueda caducar y tiene preferencia sobre la opción **El usuario debe cambiar la contraseña en el siguiente inicio de sesión**.

   - **Cuenta deshabilitada**. Si está activada esta casilla, nadie podrá iniciar una sesión con el nombre de este usuario.

   - **La cuenta está bloqueada**. Normalmente, esta casilla está desactivada y, en caso de estar activada, se utiliza para desbloquear una cuenta que se ha bloqueado por haber intentado iniciar una sesión un número excesivo de veces sin introducir la contraseña correcta (pero no se puede utilizar para bloquearla, para ello está el apartado **Cuenta deshabilitada**).

6. Si pulsa en la ficha **Miembro de**, verá una pantalla en donde se indican los grupos a los que pertenece el usuario (si pulsa en **Agregar**, en **Avanzadas**, en **Buscar ahora**, selecciona los grupos que desea, pulsa en **Aceptar** y vuelve a pulsar en **Aceptar**, podrá añadir más grupos a la lista y, si se sitúa sobre un grupo de la lista y pulsa en **Quitar**, los eliminará).

7. Si pulsa en la ficha **Perfil**, verá una pantalla en donde podrá asignar una ruta de acceso al perfil de usuario, una secuencia de

comandos de inicio de sesión o acceso para el subdirectorio particular del usuario.

8. Cuando haya finalizado, pulse en **Aceptar** y repita el proceso con todos los usuarios que desee modificar. Cuando haya acabado, cierre la utilidad.

Para crear grupos locales, siga los pasos siguientes:

1. Seleccione **Administrar** de menú contextual de **Mi PC** y verá la pantalla principal de la utilidad.

2. Pulse el botón izquierdo del ratón sobre el signo + que hay a la izquierda de **Usuarios y grupos locales** y se desplegará su contenido: **Usuarios** y **Grupos**.

3. Pulse el botón izquierdo del ratón sobre **Grupos** y, en el panel derecho, le mostrará los grupos que hay dados de alta en el equipo.

4. Pulse el botón derecho del ratón sobre **Grupos** para que muestre su menú contextual, seleccione **Grupo nuevo** y le mostrará la siguiente pantalla:

5. Indique el nombre que desea dar al grupo y una breve descripción.

6. Pulse en **Agregar**, en **Avanzadas**, en **Buscar ahora**, seleccione los usuarios, identidades especiales o grupos que desee, pulse en **Aceptar** y vuelva a pulsar en **Aceptar** (fíjese en que aparecerán en la lista de miembros del grupo).

7. Si desea quitar algún miembro de la lista, selecciónelo y pulse en **Quitar**.

8. Cuando haya finalizado, pulse en **Crear**.

9. Repita el proceso con todos los grupos que desee crear y, cuando termine, pulse en **Cerrar** para volver a la lista de grupos dados de alta en el equipo (fíjese que el grupo o grupos que acaba de crear figuran en la lista).

En Windows Vista:

Es posible crear usuarios de dos maneras:

- Utilizando **Cuentas de usuario** del **Panel de control.**
- Utilizando **Administrar** del menú contextual de **Equipo**.

En el libro se va a utilizar esta segunda, ya que es la que se puede utilizar si el equipo pertenece a una red.

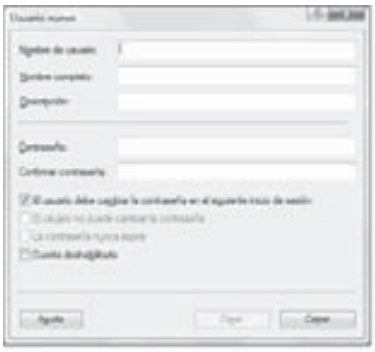
Para crear usuarios locales, siga los pasos siguientes:

1. Seleccione **Administrar** del menú contextual de **Equipo**, pulse en **Continuar** para poder continuar con el proceso (si se lo pide) y verá la pantalla principal de la utilidad.

2. Pulse el botón izquierdo del ratón sobre el signo + que hay a la izquierda de **Usuarios y grupos locales** y se desplegará su contenido: **Usuarios** y **Grupos**.

3. Pulse el botón izquierdo del ratón sobre **Usuarios** y, en el panel derecho, le mostrará los usuarios que hay dados de alta en el equipo.

4. Pulse el botón derecho del ratón sobre **Usuarios** para que muestre su menú contextual, seleccione **Usuario nuevo** y le mostrará la siguiente pantalla:



5. Indique el nombre que desea dar al usuario para conectarse (con un máximo de 20 caracteres), su nombre completo (es necesario seguir una norma ya que cuando se ordenen por el nombre completo será más fácil su búsqueda, por tanto, que todos empiecen por el nombre del usuario o que todos empiecen por su primer apellido), una breve descripción, su contraseña (con un máximo de 127 caracteres distinguiendo entre mayúsculas y minúsculas. Si está en una red con equipos Windows 95/98 evite que tengan más de 14 caracteres), la confirmación de la contraseña y active las casillas que desee de las siguientes:

   - **El usuario debe cambiar la contraseña en el siguiente inicio de sesión**. Esta opción obligará al usuario a cambiar la contraseña que le puso el administrador al darle de alta en la red la próxima vez que inicie una sesión.

   - **El usuario no puede cambiar la contraseña**. Esta opción evita que los usuarios puedan modificar su contraseña.

   - **La contraseña nunca caduca**. Al marcar esta opción, evita que la contraseña pueda caducar y deba cambiarla el usuario.

   - **Cuenta deshabilitada**. Al marcar esta opción, nadie puede iniciar una sesión con el nombre de este usuario (por ejemplo, cuando el usuario se va de vacaciones, puede deshabilitarla para que nadie pueda tener acceso a sus recursos).

6. Cuando haya finalizado, pulse en **Crear** y ya estará creada la cuenta.

7. Puede repetir el proceso con otro usuario o pulse en **Cerrar** para volver a la lista de usuarios dados de alta en el equipo (fíjese en que el usuario o usuarios que acaba de crear figuran en la lista).

Para modificar usuarios locales y/o hacerlos miembros de algún grupo, siga los pasos siguientes:

1. Seleccione **Administrar** del menú contextual de **Equipo**, pulse en **Continuar** para poder continuar con el proceso (si se lo pide) y verá la pantalla principal de la utilidad.

2. Pulse el botón izquierdo del ratón sobre el signo + que hay a la izquierda de **Usuarios y grupos locales** y se desplegará su contenido: **Usuarios** y **Grupos**.

3. Pulse el botón izquierdo del ratón sobre **Usuarios** y, en el panel derecho, le mostrará los usuarios que hay dados de alta en el equipo.

4. Sitúese sobre el usuario que desee modificar, pulse el botón derecho del ratón para que muestre su menú contextual, seleccione **Propiedades** y le mostrará la pantalla correspondiente.

5. Se encuentra en la ficha **General** y en ella se encuentran los siguientes apartados:

   - **Nombre completo**. Indica el nombre completo del usuario.

   - **Descripción**. Permite escribir una breve descripción del usuario.

   - **El usuario debe cambiar la contraseña en el siguiente inicio de sesión**. Indica si está establecido que el usuario cambie la contraseña la próxima vez que inicie una sesión.

   - **El usuario no puede cambiar la contraseña**. Evita que los usuarios puedan modificar su contraseña.

   - **La contraseña nunca caduca**. Evita que la contraseña pueda caducar y tiene preferencia sobre la opción **El usuario debe cambiar la contraseña en el siguiente inicio de sesión**.

   - **Cuenta deshabilitada**. Si está activada esta casilla, nadie podrá iniciar una sesión con el nombre de este usuario.

   - **La cuenta está bloqueada**. Normalmente, esta casilla está desactivada y, en caso de estar activada, se utiliza para desbloquear una cuenta que se ha bloqueado por haber intentado iniciar una sesión un número excesivo de veces sin introducir la contraseña correcta (pero no se puede utilizar para bloquearla, para ello está el apartado **Cuenta deshabilitada**).

6. Si pulsa en la ficha **Miembro de**, verá una pantalla en donde se indican los grupos a los que pertenece el usuario (si pulsa en **Agregar**, en **Avanzadas**, en **Buscar ahora**, selecciona los grupos que desea, pulsa en **Aceptar** y vuelve a pulsar en **Aceptar**, podrá añadir más grupos a la lista y, si se sitúa sobre un grupo de la lista y pulsa en **Quitar**, lo eliminará).

7. Si pulsa en la ficha **Perfil**, verá una pantalla en donde podrá asignar una ruta de acceso al perfil de usuario, una secuencia de comandos de inicio de sesión o acceso para el subdirectorio particular del usuario (se desarrollará posteriormente).

8. Cuando haya finalizado, pulse en **Aceptar** y repita el proceso con todos los usuarios que desee modificar. Cuando haya acabado, cierre la utilidad.

Para crear grupos locales, siga los pasos siguientes:

1. Seleccione **Administrar** del menú contextual de **Equipo**, pulse en **Continuar** para poder continuar con el proceso (si se lo pide) y verá la pantalla principal de la utilidad.

2. Pulse el botón izquierdo del ratón sobre el signo + que hay a la izquierda de **Usuarios y grupos locales** y se desplegará su contenido: **Usuarios** y **Grupos**.

3. Pulse el botón izquierdo del ratón sobre **Grupos** y, en el panel derecho, le mostrará los grupos que hay dados de alta en el equipo.

4. Pulse el botón derecho del ratón sobre **Grupos** para que muestre su menú contextual, seleccione **Grupo nuevo** y le mostrará la siguiente pantalla:

5. Indique el nombre que desea dar al grupo y una breve descripción.

6. Pulse en **Agregar**, en **Avanzadas**, en **Buscar ahora**, seleccione los usuarios, identidades especiales o grupos que desee, pulse en **Aceptar** y vuelva a pulsar en **Aceptar** (fíjese en que aparecerán en la lista de miembros del grupo).

7. Si desea quitar algún miembro de la lista, selecciónelo y pulse en **Quitar**.

8. Cuando haya finalizado, pulse en **Crear**.

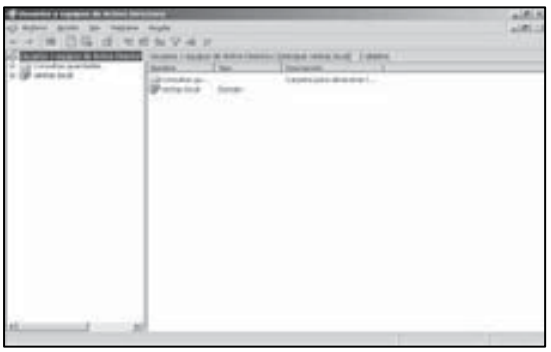
9. Repita el proceso con todos los grupos que desee crear y, cuando termine, pulse en **Cerrar** para volver a la lista de grupos dados de alta en el equipo (fíjese que el grupo o grupos que acaba de crear figuran en la lista).

En Windows Server 2003 con Directorio Activo:

Un usuario global es una cuenta a la que se puede conceder permisos y derechos para el dominio donde se está creando la cuenta. Se crea en el Directorio Activo y se guarda en equipos que disponen de Windows Server 2003 que sean controladores de dominio.

Para crear usuarios globales, siga los pasos siguientes:

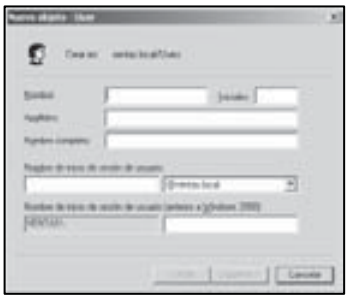
1. Seleccione **Usuarios y equipos de Active Directory** de **Herramientas administrativas** del **Panel de control** y verá la siguiente pantalla:



2. Pulse en el signo + que hay a la izquierda del dominio (en el ejemplo *ventas.local*) y se desplegará su contenido.

3. Pulse el botón izquierdo del ratón sobre **Users** (se encuentra en el panel izquierdo) y, en el panel derecho, le mostrará los usuarios y grupos que hay dados de alta en el Directorio Activo.

4. Pulse el botón derecho del ratón sobre **Users** para que muestre su menú contextual, seleccione **Nuevo**, elija **User** y le mostrará la siguiente pantalla:



En ella se encuentran los siguientes apartados:

- **Nombre**. Corresponde al nombre de pila del usuario. Puede tener una longitud de hasta 28 caracteres, incluyendo mayúsculas y minúsculas.

- **Iniciales.** Corresponde a las iniciales del usuario. Puede tener una longitud de hasta seis caracteres, incluyendo mayúsculas y minúsculas.

- **Apellidos**. Corresponde a los apellidos del usuario. Puede tener una longitud de hasta 29 caracteres, incluyendo mayúsculas y minúsculas.

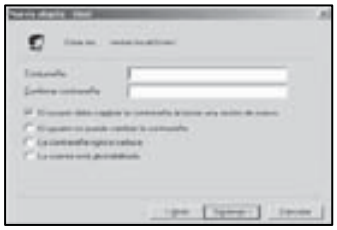
- **Nombre completo**. Corresponde al nombre completo del usuario. Puede tener una longitud de hasta 64 caracteres, incluyendo mayúsculas y minúsculas.

- **Nombre de inicio de sesión de usuario**. Se puede seguir cualquier norma para establecer los nombres de los usuarios pero es importante que todos se rijan por la misma para simplificar el conocimiento de a quién corresponde cada nombre. Es una buena idea el dar a cada usuario la inicial de su nombre más su primer apellido (por ejemplo, el usuario *Ángel Pérez* tendría el nombre de *APerez*).

A su derecha figura el nombre del dominio *DNS* correspondiente al dominio donde se está creando la cuenta (se denomina **sufijo UPN**) pero, si dispone de más de uno, puede pulsar el triángulo que hay a la derecha del campo para seleccionar otro.

- **Nombre de inicio de sesión de usuario (anterior a Windows 2000)**. En este lugar deberá indicar el nombre de usuario que utiliza para iniciar sesiones con *Windows 95/98/NT* (únicamente deberá cambiarlo si es distinto al indicado en el apartado anterior). Puede tener una longitud de hasta 20 caracteres.

5. Cuando haya finalizado (es obligatorio rellenar el nombre de usuario y el nombre de pila), pulse en **Siguiente** y verá la pantalla:



En ella se encuentran los siguientes apartados:

- **Contraseña**. Es la palabra clave que utilizará el usuario (por lo menos, la primera vez que inicie la sesión). Puede tener un máximo de 127 caracteres distinguiendo entre mayúsculas y minúsculas (si está en una red con equipos Windows 95/98 evite que tengan más de 14 caracteres). La contraseña debe reunir las características fijadas en las directivas de contraseñas (por defecto, son longitud mínima de siete caracteres y tener letras, números y signos de puntuación).

- **Confirmar contraseña**. Es la misma palabra clave que la indicada en el apartado anterior (se repite para evitar haber cometido un error en su escritura que puede evitar el iniciar la sesión posteriormente).

- **El usuario debe cambiar la contraseña al iniciar una sesión de nuevo**. Esta opción obligará al usuario a cambiar

la contraseña que le puso el administrador al darle de alta en la red, la próxima vez que inicie una sesión.

- **El usuario no puede cambiar de contraseña**. Esta opción evita que los usuarios puedan modificar su contraseña.
- **La contraseña nunca caduca**. Al activar esta casilla, evita que la contraseña pueda caducar y prevalece sobre una caducidad explícita de la contraseña y sobre el apartado **El usuario debe cambiar la contraseña en el siguiente inicio de sesión**.
- **La cuenta está deshabilitada**. Al activar esta casilla, nadie puede iniciar una sesión con el nombre de este usuario (por ejemplo, cuando el usuario se va de vacaciones, puede deshabilitar la cuenta para que nadie pueda tener acceso a sus recursos).

6. Cuando haya acabado, pulse en **Siguiente** y le mostrará una pantalla con el resumen de lo indicado. Pulse en **Finalizar** y se creará el usuario.

7. Cuando haya acabado, cierre la utilidad.

Para modificar usuarios globales y/o hacerlos miembros de algún grupo, siga los pasos siguientes:

1. Seleccione **Usuarios y equipos de Active Directory** de **Herramientas administrativas** del **Panel de control** y verá la pantalla principal de la utilidad.

2. Pulse en el signo + que hay a la izquierda del dominio (en el ejemplo *ventas.local*) y se desplegará su contenido.

3. Pulse el botón izquierdo del ratón sobre **Users** (se encuentra en el panel izquierdo) y, en el panel derecho, le mostrará los usuarios y grupos que hay dados de alta en el Directorio Activo.

4. Sitúese sobre el usuario que desee modificar, pulse el botón derecho del ratón para que muestre su menú contextual, seleccione **Propiedades** y le mostrará la siguiente pantalla:

5. Se encuentra en la ficha **General** y en ella se encuentran los siguientes apartados:

   - **Nombre**. Indica el nombre de pila del usuario.
   - **Iniciales**. Indica las iniciales del usuario.
   - **Apellidos**. Indica los apellidos del usuario.
   - **Nombre para mostrar**. Indica el nombre descriptivo del usuario y es el que utilizarán distintas aplicaciones (por ejemplo, *Microsoft Exchange*).
   - **Descripción**. Muestra una breve descripción del usuario.
   - **Oficina**. Se utiliza para indicar la ubicación de la oficina del usuario.
   - **Número de teléfono**. Permite indicar el número de teléfono del usuario (si dispone de más de uno, marque en **Otros** y escriba los que sean necesarios. Deberá pulsar en **Agregar** para que pasen a la lista inferior. Cuando haya finalizado, pulse en **Aceptar**).
   - **Correo electrónico**. Permite indicar la dirección del correo electrónico del usuario.
   - **Página Web**. Permite indicar la dirección URL de la página principal del usuario (si dispone de más de una, marque en **Otros** y escriba las que sean necesarias. Deberá pulsar en **Agregar** para que pasen a la lista inferior. Cuando haya finalizado, pulse en **Aceptar**).

6. Si pulsa en la ficha **Dirección**, verá una pantalla en donde podrá indicar los siguientes datos referidos al lugar de domicilio del usuario: **Calle**, **Apartado postal**, **Ciudad**, **Estado o provincia**, **Código postal** y **País o región**.

7. Si pulsa en la ficha **Cuenta**, verá una pantalla en donde se encuentran los siguientes apartados:

   - **Nombre de inicio de sesión de usuario**. Indica el nombre que cada usuario tiene en la red (no puede estar duplicado ni por un usuario ni por un grupo) y, a su derecha, el nombre del dominio *DNS* correspondiente al dominio donde se está creando la cuenta (si dispone de más de uno, puede pulsar el triángulo que hay a la derecha del campo para seleccionar otro).

   - **Nombre de inicio de sesión de usuario (anterior a Windows 2000)**. Indica el nombre que utiliza el usuario para iniciar sesiones con versiones anteriores a Windows 2000 (únicamente deberá indicarlo si es distinto al indicado en el apartado anterior).

   - **La cuenta está bloqueada**. Normalmente, esta casilla está desactivada y, en caso de estar activada, se utiliza para desbloquear una cuenta que se ha bloqueado por haber intentado iniciar una sesión un número excesivo de veces sin introducir la contraseña correcta (pero no se puede utilizar para bloquearla, para ello está el apartado **Cuenta deshabilitada** que se muestra en el apartado **Opciones de cuenta**).

   En el bloque **Opciones de cuenta** se encuentran las siguientes opciones:

   - **El usuario debe cambiar la contraseña en el siguiente inicio de sesión**. Al activar esta casilla, indica que el usuario deberá cambiar su contraseña la próxima vez que inicie una sesión.

   - **El usuario no puede cambiar de contraseña**. Al activar esta casilla, evita que los usuarios puedan modificar su contraseña.

   - **La contraseña nunca caduca**. Al activar esta casilla, evita que la contraseña pueda caducar y prevalece sobre la opción **El usuario debe cambiar la contraseña en el siguiente inicio de sesión**.

- **Almacenar contraseña utilizando cifrado reversible**. Si hay usuarios de equipos *APPLE* que inician sesiones en la red, deberá activar esta casilla para sus cuentas de usuario.

- **Cuenta deshabilitada**. Al activar esta casilla, nadie puede iniciar una sesión con el nombre de este usuario (por ejemplo, cuando el usuario se va de vacaciones, puede deshabilitar la cuenta para que nadie pueda tener acceso a sus recursos).

- **La tarjeta inteligente es necesaria para un inicio de sesión interactivo**. Al activar esta casilla, podrá almacenar de forma segura las claves públicas y privadas, contraseñas e información personal de otro tipo para la cuenta del usuario (es necesario disponer de una tarjeta inteligente, un lector de tarjetas inteligentes conectado al equipo de usuario y éstos deben disponer de un número de identificación personal para poder conectarse a la red).

- **Se confía en la cuenta para su delegación**. Al activar esta casilla, permite a un servicio que se ejecute con esta cuenta, realizar operaciones en nombre de otras cuentas de usuario en la red.

- **La cuenta es importante y no se puede delegar**. Al activar esta casilla, indica que esta cuenta no se puede asignar para su delegación por parte de otra cuenta.

- **Usar tipos de cifrado DES para esta cuenta**. Al activar esta casilla, indica que se utilice el *Estándar de cifrado de datos* (*DES*) que admite varios niveles de cifrado, entre los que se incluyen *MPPE estándar* (40 y 56 *bits*), *MPPE de alto nivel* (128 *bits*), *IPSec DES* (40 y 56 *bits*) y *IPSec Triple DES* (*3DES*).

- **No pedir la autenticación Kerberos previa**. Debe activar esta casilla si la cuenta utiliza otra implementación del protocolo *Kerberos* distinta a la que incorpora *Windows Server 2003* (el protocolo *Kerberos* estándar utiliza la concesión de vales para obtener la autenticación de red en un dominio y la hora a la que se emite un vale de este tipo es importante para *Kerberos*. Sin embargo, la implementación que incorpora *Windows Server 2003* utiliza otros mecanismos para sincronizar la hora, de forma que la opción

de autenticación previa de *Kerberos* no funcionará correctamente entre ambos sistemas).

En el bloque **La cuenta caduca** se encuentran las siguientes opciones:

- **Nunca**. Al activar esta casilla está indicando que la cuenta no caducará nunca (no tiene nada que ver esta opción con la de **La contraseña nunca caduca**, ya que una se refiere a la cuenta y la otra a la contraseña).

- **Fin de**. Al activar esta casilla está indicando que la cuenta caducará en la fecha indicada (se puede modificar pulsando en el triángulo que hay a la derecha del campo).

En el apartado **Horas de inicio de sesión** se puede limitar el número de horas durante las cuales un usuario puede conectarse al dominio.

Al entrar en este apartado se encuentra una matriz en cuya izquierda están los días de la semana y en su parte superior las horas del día.

Puede seleccionar los días (marcando el día correspondiente), una hora (marcando la hora correspondiente) o pulsando el botón izquierdo del ratón y desplazándolo. Cada cuadro corresponde a una hora de un día.

Cuando haya terminado de indicar las horas de conexión, pulse en **Aceptar** y volverá a la pantalla anterior.

En el apartado **Iniciar sesión en** se puede limitar las estaciones desde las que un usuario pueda conectarse al servidor.

Al entrar en este apartado verá la siguiente pantalla:

Active la casilla **Los siguientes equipos**, indique el nombre de la estación de trabajo desde la que desea permitir el inicio de sesión, pulse en *Agregar*, repita el proceso con todas las estaciones desde las que desee permitir el inicio de sesión y, cuando haya finalizado, pulse en **Aceptar** y volverá a la pantalla anterior.

8. Si pulsa en la ficha **Perfil**, verá una pantalla en donde podrá asignar un perfil de usuario, una secuencia de comandos de inicio de la sesión o un directorio particular para la cuenta del usuario.

9. Si pulsa en la ficha **Teléfonos**, verá una pantalla en donde podrá indicar los siguientes datos referidos a los números de teléfono del usuario: **Domicilio**, **Localizador** (busca), **Móvil**, **Fax**, **Teléf IP** (si pulsa en **Otros** de cualquiera de las opciones anteriores, podrá añadir más números de teléfono en cada una de ellas). Así mismo, incluye un apartado para escribir las **Notas** que se consideren necesarias.

10. Si pulsa en la ficha **Organización**, verá una pantalla en donde podrá indicar los siguientes datos del usuario:

    - **Título**. Indica el cargo que ocupa el usuario.

    - **Departamento**. Indica el departamento en el que trabaja el usuario.

    - **Organización**. Indica el nombre de la empresa u organización.

    - En **Nombre** del bloque **Administrador** podrá indica el nombre del usuario que puede administrar al usuario (si pulsa en **Cambiar**, **Propiedades** o **Borrar** podrá indicarlo, modificarlo o borrarlo).

    - **Supervisa a**. Indica los usuarios que administra este usuario.

11. Si pulsa en la ficha **Miembro de**, verá una pantalla en donde se indican los grupos a los que pertenece el usuario (si pulsa en **Agregar**, en **Avanzadas**, en **Buscar ahora**, selecciona los grupos que desea, pulsa en **Aceptar** y vuelve a pulsar en **Aceptar**, podrá añadir más grupos a la lista y, si se sitúa sobre un grupo de la lista y pulsa en **Quitar**, lo eliminará).

Si tiene clientes *Macintosh* y aplicaciones compatibles con *POSIX*, seleccione un grupo de los indicados en la lista anterior y active la casilla **Establecer grupo principal** para indicarlo.

12. Si pulsa en la ficha **Marcado**, verá una pantalla en donde se podrá configurar el uso del **Acceso telefónico a redes** del usuario.

13. Si pulsa en la ficha **Entorno**, verá una pantalla en donde se podrá configurar el entorno de inicio de los **Servicios de Terminal Server** del usuario.

14. Si pulsa en la ficha **Sesiones**, verá una pantalla en donde se encuentran los siguientes apartados:

    - **Finalizar una sesión desconectada**. Indica el tiempo máximo que una sesión desconectada permanece activa en el servidor.

    - **Límite de sesión activa**. Indica la duración máxima de una sesión. Si especifica una duración, la sesión se desconectará o se restablecerá después de transcurrir el tiempo indicado.

    - **Límite de sesión inactiva**. Indica la duración máxima de inactividad de una sesión. Si especifica una duración, la sesión se desconectará o se restablecerá después de que no haya habido actividad durante el tiempo indicado.

    - En el apartado **Cuando se alcanza el límite de una sesión o se pierde la conexión** se encuentran las acciones que se realizarán si se ha establecido un límite horario en cada uno de los apartados anteriores: **Desconectar de la sesión** (el cliente se podrá volver a conectar si es necesario) o **Terminar la sesión** (el cliente no se podrá volver a conectar aunque sea necesario).

    - En el bloque **Permitir volverse a conectar** se encuentran las acciones que se realizarán desde una sesión desconectada: **De cualquier cliente** (el cliente se podrá volver a conectar desde cualquier equipo) o **Sólo del cliente creador** (el cliente únicamente podrá volverse a conectar desde el equipo en el que inició la sesión. Sólo puede utilizarse con clientes basados en *Citrix ICA* que proporcionan un número de serie al realizar la conexión).

15. Si pulsa en la ficha **Control remoto**, verá una pantalla en donde se podrá configurar el control remoto de los **Servicios de Terminal Server** del usuario.

16. Si pulsa en la ficha **Perfil de Servicios de Terminal Server**, verá una pantalla en donde se podrá configurar el perfil de los **Servicios de Terminal Server** del usuario.

17. Si pulsa en la ficha **COM+**, verá una pantalla en donde podrá indicar los conjuntos de particiones *COM+* que se pueden asignar al usuario (una partición *COM+* son grupos de componentes *COM* desarrollados para trabajar conjuntamente para utilizar los servicios *COM+* como colas, seguridad basada en funciones, etc. Hay dos tipos de particiones *COM+*: las almacenadas en el Directorio Activo y las locales almacenadas en servidores de aplicaciones).

18. Cuando haya finalizado, pulsa en **Aceptar** y repita el proceso con todos los usuarios que desee modificar.

19. Cuando haya acabado, cierre la utilidad.

Para crear grupos globales, universales o de dominio local, siga los pasos siguientes:

1. Seleccione **Usuarios y equipos de Active Directory** de **Herramientas administrativas** del **Panel de control** y verá la pantalla principal de la utilidad.

2. Pulse el botón derecho del ratón sobre la carpeta en donde desea crear el grupo (en el ejemplo, se creará en *USERS*) para que muestre su menú contextual, seleccione **Nuevo**, elija **Group** y le mostrará la pantalla siguiente:

En ella se encuentran los siguientes apartados:

- **Nombre de grupo**. Corresponde al nombre que se le va a dar al grupo. Puede tener una longitud de hasta 64 caracteres, incluyendo mayúsculas y minúsculas.

- **Nombre de grupo (anterior a Windows 2000)**. Corresponde al nombre que aparecerá en un sistema operativo anterior a *Windows 2000* y puede incluir mayúsculas y minúsculas.

- **Ámbito de grupo**. Se utiliza para indicar si es un grupo de dominio local, global o universal (esta última opción sólo se podrá utilizar si es un grupo de distribución).

- **Tipo de grupo**. Se utiliza para indicar si es un grupo de seguridad o de distribución.

3. Cuando haya finalizado, pulse en **Aceptar** y se creará el grupo pero no tiene a nadie como miembro de él.

4. Cuando haya acabado, cierre la utilidad

En Linux:

La gestión de usuarios y grupos en Linux puede realizarse utilizando diferentes herramientas. Las más utilizadas en todas las distribuciones de Linux son los comandos *useradd* (creación de usuarios), *userdel* (eliminación de usuarios), *groupadd* (creación de grupos) y *groupdel* (eliminación de grupos). Sin embargo, a no ser que estos comandos se utilicen en *shell-scripts* para gestión de múltiples cuentas, su uso se va restringiendo cada vez más en beneficio de las herramientas gráficas.

En **SuSE Linux** se utiliza la herramienta centralizada *YaST* y *YaST2* para administración de cuentas de usuarios y grupos. En *YaST2*, hay que acceder al grupo de utilidades **Seguridad&Usuarios**. En él se encuentran los siguientes iconos:

- **Crear un nuevo usuario**.

- **Crear un nuevo grupo**.

- **Editar y crear usuarios**.

- **Editar y crear grupos**.

Figura 7.1. Ventana de administración de cuentas de usuario en SuSE Linux

Figura 7.2. Ventana de administración de grupos en SuSE Linux

Las opciones más utilizadas son **Editar y crear usuarios** (cuya ventana principal aparece en la figura 7.1) y **Editar y crear grupos** (su ventana principal aparece en la figura 7.2). Como se puede observar, estas herramientas son, en realidad, una sola. Bastará con seleccionar cualquiera de los botones de opción **Administración de usuarios** y **Administración de grupos** situados en la parte superior de la ventana para cambiar de una a otra.

Si se activa la casilla **Ver también usuarios de sistema** aparecerán todos los usuarios predefinidos en el equipo, además de *root* y cualquier otro usuario que haya creado el administrador del sistema.

La opción **Ver también los grupos del sistema** sirve para ver los grupos definidos automáticamente por el equipo, además del grupo *users* y todos los grupos creados por el administrador del sistema.

En el caso de **Linux Red Hat** se emplea el *panel de control* para administrar las cuentas de usuarios y grupos. La herramienta resulta accesible desde el icono **User Manager** y su ventana principal se muestra en la figura 7.3. Las listas de usuarios y grupos están disponibles en las páginas **Usuarios** y **Grupos** y el cuadro de texto que hay al lado del botón **Aplicar filtro** se utiliza para hacer listados selectivos de usuarios o grupos de acuerdo a un patrón.

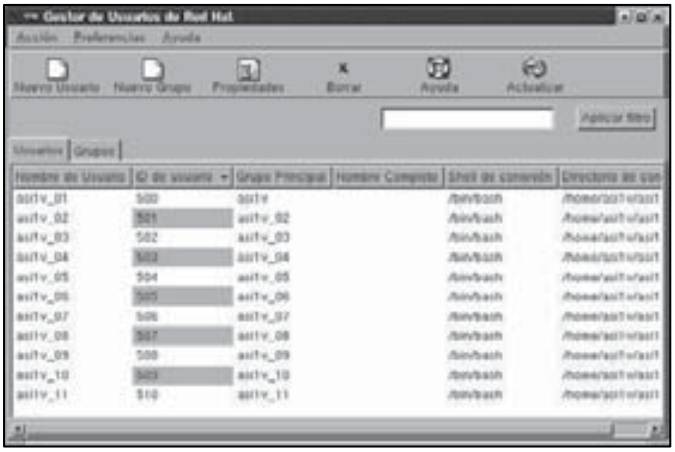


Figura 7.3. Ventana de administración de usuarios y grupos en Linux Red Hat

Un usuario en Linux puede pertenecer a más de un grupo. Cuando se crea un usuario en el sistema, normalmente se le asigna el grupo *users*, aunque se le pueden asignar otros grupos dependiendo de los privilegios que éste necesite en el sistema. Todos los usuarios y grupos creados tienen asociados un identificador, llamado **UID** (**User Identificator**, **Identificador de Usuario**) o **GID** (**Group Identificator**, **Identificador de Grupo**). Estos identificadores son numéricos y se pueden emplear para especificar usuarios o grupos, aunque su uso fundamental es interno al sistema.

CÓMO TRABAJAR LOS PERMISOS (PARTE PRÁCTICA)

En Windows XP y Windows Server 2003:

Para establecer permisos estándar de directorio, siga los pasos siguientes:

1. Desde el **Explorador de Windows**, seleccione el directorio que desee (en el ejemplo, se seleccionará el directorio *PRIVADO* que se creó en prácticas anteriores), pulse el botón derecho del ratón para abrir su menú contextual, seleccione **Propiedades**, después **Seguridad** (si esta ficha no aparece, seleccione **Herramientas**, escoja **Opciones de carpeta**, pulse en la ficha **Ver** y desactive la casilla **Utilizar uso compartido simple de archivos**) y verá la pantalla siguiente:

2. En ella se encuentran los nombres de los usuarios, grupos e identidades especiales que tienen permisos sobre dicha carpeta y, debajo, los permisos estándar de directorio que posee cada uno de ellos.

3. Si desea modificar los permisos de alguno de ellos, sitúese sobre él y verá que en la parte inferior, se muestran los permisos que tiene establecidos (si hay casillas grises, corresponden a permisos heredados). Active la casilla correspondiente al permiso deseado en la columna **Permitir** (se le concede el permiso) o **Denegar** (se le deniega el permiso).

4. Si desea añadir otros usuarios o grupos a la lista de nombres, pulse en **Agregar**, en **Avanzadas** y en **Buscar ahora**. Se le abrirá una ventana con todos los posibles usuarios, grupos e identidades especiales a las que puede otorgar o denegar permisos.

Si selecciona elementos de la lista, pulsa en **Aceptar** y vuelve a pulsar en **Aceptar**, se añadirán a los grupos o usuarios que tienen permisos sobre la carpeta. Una vez que estén en la lista, indique los permisos que desea conceder o denegar a cada uno de los usuarios que ha añadido.

5. Si desea quitar algún usuario o grupo, sitúese sobre él, pulse en **Quitar** (no pedirá ninguna confirmación) y verá como se elimina de la lista.

6. Pulse en **Aceptar** para volver a la pantalla principal de la utilidad.

7. Cuando haya finalizado, cierre la utilidad.

En Windows Vista:

Para establecer permisos estándar de directorio, siga los pasos siguientes:

1. Desde el **Explorador de Windows**, seleccione el directorio que desee (en el ejemplo, se seleccionará el directorio *PRIVADO* que se creó en prácticas anteriores), pulse el botón derecho del ratón para abrir su menú contextual, seleccione **Propiedades**, después **Seguridad** y verá la pantalla siguiente:

2. En ella se encuentran los nombres de los usuarios, grupos e identidades especiales que tienen permisos sobre dicha carpeta y,

debajo, los permisos estándar de directorio que posee cada uno de ellos.

3. Si desea modificar los permisos de alguno de ellos, pulse en **Editar** y verá una nueva pantalla.

4. Sitúese sobre el usuario que desee y verá que, en la parte inferior, se muestran los permisos que tiene establecidos (si hay casillas grises, corresponden a permisos heredados). Active la casilla correspondiente al permiso deseado en la columna **Permitir** (se le concede el permiso) o **Denegar** (se le deniega el permiso).

4. Si desea añadir otros usuarios o grupos a la lista de nombres, pulse en **Agregar**, en **Avanzadas** y en **Buscar ahora**. Se le abrirá una ventana con todos los posibles usuarios, grupos e identidades especiales a las que puede otorgar o denegar permisos.

   Si selecciona elementos de la lista, pulsa en **Aceptar** y vuelve a pulsar en **Aceptar**, se añadirán a los grupos o usuarios que tienen permisos sobre la carpeta. Una vez que estén en la lista, indique los permisos que desea conceder o denegar a cada uno de los usuarios que ha añadido.

5. Si desea quitar algún usuario o grupo, sitúese sobre él, pulse en **Quitar** (no pedirá ninguna confirmación) y verá como se elimina de la lista.

6. Pulse en **Aceptar** para volver a la pantalla principal de la utilidad.

7. Cuando haya finalizado, cierre la utilidad.

En Linux:

Para establecer los permisos de los archivos y carpetas, se puede utilizar el comando **chmod** (véase la ayuda *man*) o el botón derecho del ratón sobre el objeto dentro de la ventana del explorador en entorno gráfico. La figura 7.4 muestra la ventana de configuración de los permisos en entorno gráfico.

Figura 7.4. Ventana para establecer los permisos de archivos y carpetas en el entorno gráfico de Linux

Los sistemas Unix/Linux utilizan unos permisos por defecto a la hora de crear archivos y carpetas. Este valor se puede modificar utilizando el comando **umask** cuya sintaxis es la siguiente:

```
umask [-S] [modo]
```

El comando *umask* sin parámetros muestra el valor de la máscara de permisos por defecto que se aplica en ese momento. Por su parte, el modificador *-S* hace que el valor de la máscara se muestre en formato *rwx*.

La forma más sencilla de trabajar con *umask* es equivalente al comando **chmod**: se especifica a quién se establece el permiso (usuario, grupo y otros) y qué tipo de permisos (lectura, escritura y ejecución). La máscara que se establece para archivos y carpetas es idéntica, con la salvedad de que el permiso de ejecución no tiene efecto en archivos. Esta táctica impide que, por defecto, se puedan crear archivos con derecho de ejecución.

Cuando un usuario accede al sistema Linux, por defecto no tiene permisos para modificar los archivos de configuración. Sin embargo, se le pueden conceder permisos para ello (aunque no es conveniente por cuestiones de seguridad). Lo más lógico es utilizar los usuarios normales para tareas de explotación del sistema y utilizar al usuario *root* solamente para tareas de administración y configuración. Existe

un comando en Linux, llamado **su**, que, ejecutado desde una ventana de terminal, permite cambiar la sesión del usuario actual por la del usuario *root* sin tener que cerrar la sesión anterior. Este comando solicita la contraseña de *root* y, al finalizarlo (pulsando CTRL + D o escribiendo *exit*), se restaura la sesión del usuario anterior.

La solicitud de la contraseña del usuario *root* se puede producir, además de al utilizar el comando *su*, al ejecutar como usuario normal cualquier utilidad de configuración del sistema (*control-panel*, *YaST2*, etc.) o que necesite de ciertos privilegios de ejecución. La figura 7.5 muestra la ventana de solicitud de la contraseña de *root* cuando se ejecuta el programa *YaST2* en entorno gráfico y con un usuario normal. En otros casos, es posible que las utilidades de configuración ni siquiera resulten accesibles para los usuarios y, en ese caso, solamente pueden ser ejecutadas directamente como usuario *root*.

En el caso de archivos ejecutables que tengan el permiso *s* y pertenezcan al usuario *root*, cualquier usuario podrá iniciar esos programas con los privilegios de superusuario sin necesidad de introducir ninguna contraseña. Estos programas se configuran de este modo cuando necesitan ciertos privilegios de acceso al sistema.

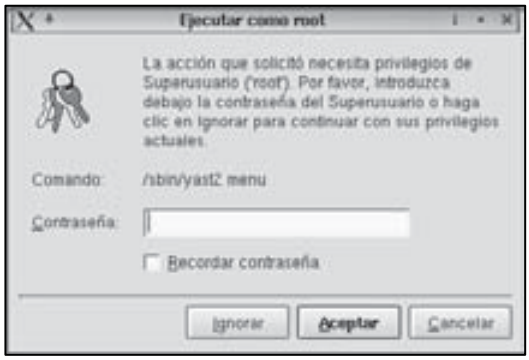


Figura 7.5. Ventana de solicitud de la contraseña de root

El uso que debe darse al usuario *root* en el entorno Linux debe restringirse a tareas de administración. Esto es debido a que cuenta con derechos para realizar cualquier operación sobre el sistema; incluso puede eliminar archivos importantes. Además, si se accede a una red local o extensa utilizando este usuario, el sistema es más vulnerable a ataques externos.

Otras aplicaciones de comunicación por red, como FTP, TELNET y Samba, se basan también en los permisos establecidos a nivel de archivos para generar los derechos que disponen los usuarios, ya que éstos también deben definirse en el sistema. El uso de esas aplicaciones puede contar además con otros derechos que normalmente se establecen en determinados archivos de configuración que se incluyen con ellas.

CÓMO AGREGAR Y COMPARTIR UNA IMPRESORA LOCAL O DE RED EN WINDOWS (PARTE PRÁCTICA)

Una vez que se haya conectado la impresora local al puerto correspondiente del equipo, siga los pasos siguientes:

En **Windows XP**:

1. Ejecute el icono **Impresoras y faxes**, que se encuentra en el **Panel de control** (también puede hacerse desde el menú **Inicio**).

2. Pulse en **Agregar impresora** y entrará en el **Asistente para agregar impresoras**.

3. Pulse en *Siguiente* y le mostrará una pantalla en donde deberá elegir entre:

   - **Impresora local conectada a este equipo**. Si activa esta casilla, está indicando que la impresora está conectada al equipo donde está agregando la impresora (si activa también la casilla **Detectar e instalar mi impresora Plug and Play automáticamente**, el sistema intentará detectar la impresora y, si la encuentra, la instalará).

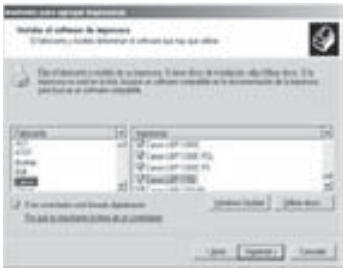
   - **Una impresora de red o una impresora conectada a otro equipo**. Si activa esta casilla, está indicando que la impresora está instalada en otro equipo de la red.

4. Como la impresora está situada en el mismo equipo, se activará la casilla **Impresora local conectada a este equipo** y no se activará la de **Detectar e instalar mi impresora Plug and Play automáticamente** para realizar el proceso de forma manual. Pulse en **Siguiente** y verá la pantalla:

5. En ella ha de indicar en **Usar el puerto siguiente**, el puerto local donde está conectada la impresora (si pulsa en el triángulo que hay a la derecha del apartado, podrá seleccionar uno).

   En caso de necesitar añadir otro puerto, active la casilla **Crear nuevo puerto** y seleccione uno de los disponibles. En este caso y cuando pulse en *Siguiente*, deberá indicar el nombre del puerto o su dirección IP.

   En el ejemplo, se indicará que la impresora se encuentra en **LPT1**, se pulsará en **Siguiente** y mostrará la pantalla:



6. Ahora, deberá seleccionar la impresora que está conectada a dicho puerto para que cargue sus controladores. Para ello, deberá indicar (en la parte izquierda) el nombre del **Fabricante** de la impresora y, a continuación (en la parte derecha), el nombre de dicha impresora (si no apareciese en la lista y dispusiera de sus controladores, pulse en **Utilizar disco** e inserte en la unidad correspondiente el *software* proporcionado por la casa para su instalación).

7. Cuando haya finalizado, pulse en **Siguiente** y le pedirá que indique el nombre (con un máximo de 31 caracteres) que quiere que aparezca para la impresora (en caso de que se hubiere instalado la impresora anteriormente y se hubiera borrado, le mostrará previamente otra pantalla en la que indica que ya hay instalado un controlador para dicha impresora y le pide que indique si desea conservarlo o reemplazarlo). Indíquelo y active la casilla de si desea (o no) que dicha impresora la utilicen los programas como predeterminada (si es

la primera impresora que se instala en el equipo, no le aparecerá esta última opción).

8. Cuando lo haya indicado, pulse en **Siguiente**. En la nueva pantalla, deberá indicar si la impresora va a estar compartida o no. Como en el ejemplo sí lo va a estar, pulse en **Nombre del recurso compartido** y escriba (o acepte) el nombre que va a tener dicho recurso compartido.

9. Cuando lo haya hecho, pulse en **Siguiente** y le mostrará una nueva pantalla en donde deberá indicar la ubicación de la impresora y una breve descripción.

10. Cuando haya acabado, pulse en **Siguiente** y le indicará si desea imprimir (o no) una página de prueba, pulse en **Sí** y le mostrará una pantalla con el resumen de la configuración.

11. Pulse en **Finalizar** y procederá a la instalación. Al cabo de un momento, le aparecerá un nuevo icono con el nombre de la impresora y empezará a imprimirse la página de prueba (pulse en **Aceptar** si se ha impreso bien dicha página o, si no ha sido así, pulse en **Solucionar problemas**).

12. Cuando haya finalizado, cierre la utilidad.

En **Windows Vista**:

1. Ejecute el icono **Impresoras** que se encuentra en el **Panel de control**.

2. Pulse en **Agregar una impresora** y, en la nueva pantalla que le muestra, seleccione **Agregar una impresora local** (si la impresora local que va a conectar es USB, no es necesario que continúe el proceso, ya que se instala automáticamente cuando la conecte al equipo).

3. Le mostrará una pantalla en donde ha de indicar, en **Usar el puerto siguiente**, el puerto local donde está conectada la impresora (si pulsa en el triángulo que hay a la derecha del apartado, podrá seleccionar uno).

   En caso de necesitar añadir otro puerto, active la casilla **Crear un nuevo puerto** y seleccione uno de los disponibles. En este caso y cuando pulse en **Siguiente**, deberá indicar el nombre del puerto o su dirección IP.

   En el ejemplo, se indicará que la impresora se encuentra en **LPT1**, se pulsará en **Siguiente** y mostrará una nueva pantalla para que indique

la impresora que está conectada a dicho puerto para que cargue sus controladores. Para ello, deberá indicar (en la parte izquierda) el nombre del **Fabricante** de la impresora y, a continuación (en la parte derecha), el nombre de dicha impresora (si no apareciese en la lista y dispusiera de sus controladores, marque en **Usar disco** e inserte en la unidad correspondiente el *software* proporcionado por la casa para su instalación).

4. Cuando haya finalizado, pulse en **Siguiente** y le pedirá que indique el nombre que quiere que aparezca para la impresora (en caso de que se hubiere instalado la impresora anteriormente y se hubiera borrado, le mostrará previamente otra pantalla en la que le indica que ya hay instalado un controlador para dicha impresora y le pide que indique si desea conservarlo o reemplazarlo). Indíquelo y active la casilla de si desea (o no) que dicha impresora la utilicen los programas como predeterminada (si es la primera impresora que se instala en el equipo, no le aparecerá esta última opción).

5. Cuando lo haya indicado, pulse en **Siguiente** y le indicará si desea imprimir (o no) una página de prueba.

8. Cuando haya acabado, pulse en **Finalizar** y procederá a la instalación. Al cabo de un momento, le aparecerá un nuevo icono con el nombre de la impresora y empezará a imprimirse la página de prueba (pulse en **Aceptar** si se ha impreso bien dicha página o, si no ha sido así, pulse en **Solucionar problemas de impresora**).

9. Para compartir la impresora que acaba de crear, pulse el botón derecho del ratón sobre ella y seleccione **Compartir**.

10. En la nueva pantalla, si no está disponible la opción **Compartir Impresora**, pulse en **Cambiar opciones de uso compartido** y confirme que desea continuar.

    Si está disponible la opción **Compartir Impresora**, active dicha casilla e indique (o acepte) el nombre que va a tener dicho recurso compartido. Mantenga activada la casilla **Procesar trabajos de impresión en equipos cliente** para descargar a este equipo de los trabajos de impresión que le manden.

11. Cuando lo haya hecho, pulse en **Aceptar** y ya habrá finalizado.

CÓMO AGREGAR UNA IMPRESORA COMPARTIDA EN WINDOWS (PARTE PRÁCTICA)

Para agregar una impresora que ya está instalada en otro equipo, siga los pasos siguientes:

En **Windows XP**:

1. Ejecute el icono **Impresoras y faxes**, que se encuentra en el **Panel de control** (también puede hacerse desde el menú **Inicio**).

2. Pulse en el icono **Agregar impresora** y entrará en el **Asistente para agregar impresoras**.

3. Pulse en **Siguiente** y le mostrará una pantalla en donde deberá elegir entre:

   - **Impresora local conectada a este equipo**. Si activa esta casilla, está indicando que la impresora está conectada al equipo donde está agregando la impresora (si activa también la casilla **Detectar e instalar mi impresora Plug and Play automáticamente**, el sistema intentará detectar la impresora y, si la encuentra, la instalará).

   - **Una impresora de red o una impresora conectada a otro equipo**. Si activa esta casilla, está indicando que la impresora está instalada en otro equipo de la red.

4. Como la impresora está en otro equipo, se activará la casilla **Una impresora de red o una impresora conectada a otro equipo**, pulse en **Siguiente** y verá la pantalla:

5. En ella deberá indicar cómo desea buscar la impresora:

   - **Buscar una impresora en Directorio**. Esta opción sólo estará disponible si se ha iniciado una sesión en un dominio en el que se está ejecutando el Directorio Activo y le permite indicar el nombre de una impresora para buscarla en el directorio.

   - **Conectarse a esta impresora (o para buscar...)**. Esta opción le permitirá indicar el nombre si lo sabe o que le muestre todas las que haya instaladas al pulsar en **Siguiente**.

   - **Conectarse a una impresora en Internet o en su red doméstica u organización**. Esta opción le permitirá buscar una impresora mediante su dirección *URL* (siempre que se tengan los permisos adecuados).

6. En el ejemplo, se activará la casilla **Conectarse a esta impresora (o para buscar…)**, no se indicará ningún nombre, se pulsará en **Siguiente** y mostrará una pantalla parecida a la siguiente:

7. En ella le muestra los dominios o grupos de trabajo que hay en la red (en el ejemplo, *ventas*) y los equipos que hay en dicho dominio (en el ejemplo *principal*). Si pulsa dos veces con el botón izquierdo del ratón sobre el signo + que se encuentra a la izquierda del equipo en donde se encuentra instalada la impresora, le mostrará las impresoras compartidas que hubiera en dicho equipo.

8. Seleccione la que desee (fíjese en que se ha escrito su nombre y el equipo correspondiente en el apartado **Impresora** que se encuentra en la parte superior), pulse en **Siguiente** e indique si desea utilizar dicha impresora como predeterminada.

9. Cuando lo haya hecho, pulse en **Siguiente** y le mostrará una pantalla con el resumen de la configuración.

10. Pulse en **Finalizar**, procederá a la instalación y, al cabo de un momento, le aparecerá un nuevo icono con el nombre de la impresora y el equipo en donde se encuentra.

11. Cuando haya finalizado, cierre la utilidad.

En **Windows Vista**:

1. Ejecute el icono **Impresoras** que se encuentra en el **Panel de control**.

2. Pulse en **Agregar una impresora** y, en la nueva pantalla que le muestra, seleccione **Agregar una impresora de red, inalámbrica o Bluetooth** (la impresora deberá estar conectada y encendida).

3. Pulse en **Siguiente** y le mostrará una pantalla en donde se encuentran las impresoras compartidas que encuentra. Si la que busca no se muestra, pulse en **La impresora deseada no está en la lista** y le mostrará una nueva pantalla para que indique cómo desea buscar la impresora:

   - **Buscar una impresora**. Esta opción le permitirá buscar en los distintos equipos para que seleccione la impresora deseada.

   - **Seleccionar una impresora compartida por nombre**. Esta opción le permitirá indicar el nombre si lo sabe o que le muestre todas las que haya instaladas al pulsar en **Examinar**.

   - **Agregar una impresora por medio de una dirección IP…**. Esta opción le permitirá indicar la dirección IP o el nombre del host de la impresora que desee utilizar y si desea **Consultar a la impresora y seleccionar automáticamente el controlador…**

4. En el ejemplo, se seleccionará una de las impresoras compartidas que se mostraron en la primera pantalla y se pulsará en **Siguiente.**

5. Le mostrará una nueva pantalla para que indique (o confirme) el nombre de la impresora y si desea utilizar dicha impresora como predeterminada. Cuando lo haya realizado, pulse en **Siguiente** y le indicará si desea imprimir (o no) una página de prueba.

6. Cuando haya acabado, pulse en **Finalizar** y procederá a la instalación. Al cabo de un momento, le aparecerá un nuevo icono con el nombre de la impresora y empezará a imprimirse la página de prueba (pulse en **Aceptar** si se ha impreso bien dicha página o, si no ha sido así, pulse en **Solucionar problemas de impresora**).

7. Cuando haya finalizado, cierre la utilidad.

LOS PERMISOS SOBRE LAS IMPRESORAS EN WINDOWS (PARTE PRÁCTICA)

En **Windows XP:**

Si pulsa en la ficha **Seguridad** de las propiedades de una impresora (si esta ficha no aparece, ejecute el **Explorador de Windows**, y desde cualquier carpeta, seleccione **Herramientas**, seleccione **Opciones de carpeta**, pulse en la ficha **Ver** y desactive la casilla **Utilizar uso compartido simple de archivos**), verá una pantalla en la que se encuentran los nombres de los usuarios, grupos e identidades especiales que tienen permisos sobre el objeto y, debajo, los permisos estándar que posee cada uno de ellos.

Hay tres tipos de permisos estándar de impresora: **Imprimir**, **Administrar documentos** y **Administrar impresoras** (de manera predeterminada, todos los usuarios tienen concedido el permiso **Imprimir** como miembros del grupo **Todos**). Además, se encuentra **Permisos especiales** que indica si se han indicado más permisos que los permisos estándar (son los que se obtienen al pulsar en **Opciones avanzadas**).

Para trabajar con los permisos estándar sobre las impresoras y una vez pulsada la ficha **Seguridad**, siga los pasos siguientes:

1. Si desea modificar los permisos de alguno de ellos, sitúese sobre él y verá que en la parte inferior, se muestran los permisos que tiene establecidos. Para ello, active la casilla correspondiente al permiso deseado en la columna **Permitir** (se le concede el permiso) o **Denegar** (se le deniega el permiso).

2. Si desea añadir otros usuarios o grupos a la lista de nombres, pulse en **Agregar**, en **Avanzadas** y en **Buscar ahora**. Se le abrirá una ventana con todos los posibles usuarios, grupos e identidades especiales a las que puede otorgar o denegar permisos.

   Si selecciona elementos de la lista, pulse en **Aceptar** y vuelva a pulsar en **Aceptar**, se añadirán a los grupos o usuarios que tienen permisos sobre la impresora. Una vez que estén en la lista, indique los permisos que desea conceder o denegar a cada uno de los usuarios que ha añadido.

3. Si desea quitar algún usuario o grupo, sitúese sobre él, pulse en **Quitar** (no pedirá ninguna confirmación) y verá cómo se elimina de la lista.

Para trabajar con los permisos especiales sobre las impresoras, siga los pasos siguientes:

1. Pulse en **Opciones avanzadas** y verá una pantalla en la que se encuentran los nombres de los usuarios, grupos e identidades que tienen permisos especiales sobre la impresora junto con una descripción de los permisos y dónde se aplican.

2. Si desea modificar los permisos de alguno de ellos, sitúese sobre él, pulse en **Modificar** y verá una pantalla parecida a la siguiente:

Fíjese en que muestra los permisos especiales que tiene establecidos el usuario o grupo seleccionado.

3. Puede modificar los permisos que desee. Para ello, active la casilla correspondiente al permiso deseado en la columna **Permitir** (se le concede el permiso) o **Denegar** (se le deniega el permiso).

   Indique en el apartado **Aplicar en** el ámbito de los permisos que está marcando (puede modificarlo si pulsa en el triángulo que hay a la derecha del apartado).

4. Cuando haya finalizado, pulse en *Aceptar* y volverá a la pantalla **Configuración de seguridad avanzada** de la impresora.

5. Si desea añadir otros usuarios o grupos a la lista de nombres, pulse en **Agregar**, en **Avanzadas** y en **Buscar ahora**. Se le abrirá una ventana con todos los posibles usuarios, grupos e identidades especiales a las que puede otorgar o denegar permisos.

Si selecciona elementos de la lista, pulse en **Aceptar** y vuelva a pulsar en **Aceptar**, pasará a la pantalla donde deberá indicar los permisos y ámbito de aplicación deseado. Cuando haya finalizado, pulse en **Aceptar** y verá que se añade a la lista de permisos de **Configuración de seguridad avanzada** de la impresora.

6. Si desea quitar algún usuario o grupo, sitúese sobre él, pulse en **Quitar** (no pedirá ninguna confirmación) y verá cómo se elimina de la lista.

7. Cuando haya finalizado, pulse en **Aceptar** para volver a la pantalla de **Propiedades** de la impresora.

En **Windows Vista:**

Pulse en la ficha **Seguridad** de las propiedades de una impresora (para ello, ejecute el icono **Impresoras** que se encuentra en el **Panel de control**, pulse dos veces con el botón izquierdo del ratón sobre la impresora deseada, abra el menú **Impresora** y seleccione **Propiedades**).

Verá una pantalla en la que se encuentran los nombres de los usuarios, grupos e identidades especiales que tienen permisos sobre el objeto y, debajo, los permisos estándar que posee cada uno de ellos.

Hay tres tipos de permisos estándar de impresora: **Imprimir**, **Administrar impresoras** y **Administrar documentos** (de manera predeterminada, todos los usuarios tienen concedido el permiso **Imprimir** como miembros del grupo **Todos**). Además, se encuentra **Permisos especiales** que indica si se han indicado más permisos que los permisos estándar (son los que se obtienen al pulsar en **Opciones avanzadas**).

Para trabajar con los permisos estándar sobre las impresoras y una vez pulsada la ficha **Seguridad**, siga los pasos siguientes:

1. Si desea modificar los permisos de alguno de ellos, sitúese sobre él y verá que, en la parte inferior, se muestran los permisos que tiene establecidos. Para ello, active la casilla correspondiente al permiso deseado en la columna **Permitir** (se le concede el permiso) o **Denegar** (se le deniega el permiso).

2. Si desea añadir otros usuarios o grupos a la lista de nombres, pulse en **Agregar**, en **Avanzadas** y en **Buscar ahora**. Se le abrirá una

ventana con todos los posibles usuarios, grupos e identidades especiales a las que puede otorgar o denegar permisos.

Si selecciona elementos de la lista, pulsa en **Aceptar** y vuelve a pulsar en **Aceptar**, se añadirán a los grupos o usuarios que tienen permisos sobre la impresora. Una vez que estén en la lista, indique los permisos que desea conceder o denegar a cada uno de los usuarios que ha añadido.

3. Si desea quitar algún usuario o grupo, sitúese sobre él, pulse en **Quitar** (no pedirá ninguna confirmación) y verá cómo se elimina de la lista.

Para trabajar con los permisos especiales sobre las impresoras, siga los pasos siguientes:

1. Pulse en **Opciones avanzadas** y verá una pantalla en la que se encuentran los nombres de los usuarios, grupos e identidades que tienen permisos especiales sobre la impresora junto con una descripción de los permisos y dónde se aplican.

2. Si desea modificar los permisos de alguno de ellos, sitúese sobre él, pulse en **Editar** y verá una pantalla en donde se muestran los permisos especiales que tiene establecidos el usuario o grupo seleccionado.

3. Puede modificar los permisos que desee. Para ello, active la casilla correspondiente al permiso deseado en la columna **Permitir** (se le concede el permiso) o **Denegar** (se le deniega el permiso).

   Indique en el apartado **Aplicar en** el ámbito de los permisos que está marcando (puede modificarlo si pulsa en el triángulo que hay a la derecha del apartado).

4. Cuando haya finalizado, pulse en **Aceptar** y volverá a la pantalla **Configuración de seguridad avanzada** de la impresora.

5. Si desea añadir otros usuarios o grupos a la lista de nombres, pulse en **Agregar**, en **Avanzadas** y en **Buscar ahora**. Se le abrirá una ventana con todos los posibles usuarios, grupos e identidades especiales a las que puede otorgar o denegar permisos.

   Si selecciona elementos de la lista, pulsa en **Aceptar** y vuelve a pulsar en **Aceptar**, pasará a la pantalla donde deberá indicar los

permisos y ámbito de aplicación deseado. Cuando haya finalizado, pulse en **Aceptar** y verá que se añade a la lista de permisos de **Configuración de seguridad avanzada** de la impresora.

6. Si desea quitar algún usuario o grupo, sitúese sobre él, pulse en **Quitar** (no pedirá ninguna confirmación) y verá cómo se elimina de la lista.

7. Cuando haya finalizado, pulse en **Aceptar** para volver a la pantalla de **Propiedades** de la impresora.

LAS PROPIEDADES DE LAS IMPRESORAS EN WINDOWS (PARTE PRÁCTICA)

En **Windows XP:**

Para configurar las propiedades de una impresora, sitúese sobre dicha impresora (seleccionando **Impresoras y faxes** del menú **Inicio**), pulse el botón derecho del ratón para abrir su menú contextual, seleccione **Propiedades** y verá una pantalla parecida a la siguiente (el número de fichas y su denominación dependerá del modelo de impresora):

Se encuentra en la ficha **General**. En ella se puede indicar la localización en donde se encuentra (**Ubicación**), escribir una breve descripción sobre la impresora (**Comentario**), ver información diversa sobre sus características, mandar imprimir una página de prueba (**Imprimir página de prueba**) o cambiar las preferencias personales de presentación y otras opciones (**Preferencias de impresión**). Estas últimas opciones dependen de la impresora y pueden ser: orientación del papel, imprimir en ambas caras, orden de las páginas, páginas por hoja, etc. (se describirán posteriormente).

Si pulsa en la ficha **Compartir**, verá una pantalla en la que puede modificar si la impresora está compartida (**Compartir esta impresora**) y el nombre que mostrará (**Nombre de recurso**

compartido), o si no lo está (**No compartir esta impresora**). Podrá indicar si desea **Mostrar lista en el directorio** (esto permitirá a otros usuarios buscar la impresora en el Directorio Activo).

También, puede instalar otros controladores adicionales para la impresora (así, podrá ser usada por otros usuarios que los necesiten y que utilicen otras versiones de Windows). Para ello, pulse en **Controladores adicionales**, active las casillas correspondientes a los entornos que desee y marque en *Aceptar*.

Si pulsa en la ficha **Puertos**, verá una pantalla en la que se muestra la serie de puertos locales donde pueden estar conectadas las impresoras (indicando las impresoras que hay conectadas en cada uno de ellos). Se pueden realizar las siguientes tareas:

- Si desea añadir otro, marque en **Agregar puerto**, seleccione el tipo de puerto disponible y pulse en **Puerto nuevo**. En función del tipo de puerto elegido, deberá actuar de la manera siguiente:
    - Si ha seleccionado **Local Port**, deberá indicar el nombre de puerto local que desee, pulsar en **Aceptar** y pulsar en **Cerrar**.
    - Si ha seleccionado **Standard TCP/IP Port**, entrará en el asistente para que indique la dirección IP que va a darle (siga los pasos indicados hasta su finalización).
- Si desea añadir un nuevo monitor de puerto, pulse en **Nuevo tipo de puerto** y siga los pasos indicados.
- Si desea configurar un puerto, sitúese sobre el puerto deseado, pulse en **Configurar puerto** e indique las características que desee.
- Si desea eliminar alguno de ellos, selecciónelo y pulse en **Eliminar puerto** (le pedirá confirmación del borrado).

Al activar la casilla **Habilitar compatibilidad bidireccional**, podrá utilizar esta característica de impresión que consiste en que un monitor de lenguaje supervisa la comunicación entre el equipo y la impresora y, después, transfiere el trabajo de impresión al monitor de puerto que controla la entrada y salida a la impresora (para poder utilizar la compatibilidad bidireccional, la impresora debe admitirla).

Al activar la casilla **Habilitar la cola de la impresora**, podrá hacer que una cola de impresión preste servicio a dos o más impresoras (de esta manera, cuando una impresora esté imprimiendo un trabajo, el siguiente trabajo se dirigirá a otra impresora). Para ello, una vez activada esta casilla, deberá activar todos los puertos a los que están conectadas todas las impresoras que va a agrupar (**Agrupación de impresoras**).

Si pulsa en la ficha **Opciones avanzadas**, verá una pantalla en la que se encuentran las opciones siguientes:

- **Siempre disponible**. Si activa esta casilla, estará indicando que la impresora va a estar disponible las 24 horas de cada día.

- **Disponible desde**. Si activa esta casilla, deberá indicar desde qué hora **hasta** qué hora estará disponible.

- **Prioridad**. Indica la prioridad predeterminada de esta impresora. Los documentos con mayor prioridad (99) se imprimirán antes que los de menor prioridad (1).

- **Controlador**. Indica el controlador de impresora que se está utilizando (si pulsa en el triángulo que hay a la derecha del apartado, podrá seleccionar otro. En caso de que desee añadir uno nuevo, pulse en **Controlador nuevo** y entrará en el **Asistente para agregar controladores de impresora**. Siga los pasos para seleccionar uno nuevo).

- **Imprimir utilizando la cola para que el programa termine más rápido**. Al activar esta casilla, los trabajos se enviarán a la cola de impresión en lugar de enviarse directamente a la impresora. Cuando ésta esté libre, empezará a imprimir el trabajo.

- **Iniciar la impresión cuando la última página haya entrado en la cola**. Al activar esta casilla, no empezará a imprimir un trabajo hasta que todo él esté almacenado en la cola de impresión (de esta manera, no se bloqueará la impresora si el ordenador que está preparando el trabajo es más lento que la impresión).

- **Empezar a imprimir de inmediato**. Al activar esta casilla, se empezará a imprimir nada más llegar la primera página a la cola de impresión (si la impresora está disponible).

- **Imprimir directamente en la impresora**. Al activar esta casilla, se mandará directamente el trabajo a la impresora (utilice esta

opción sólo cuando no pueda imprimir utilizando la cola de impresión).

- **Dejar pendientes documentos no coincidentes**. Al activar esta casilla, la cola de impresión comprobará que el trabajo que tiene almacenado coincide con el documento antes de ser enviado. Si no coinciden, el documento quedará retenido pero se imprimirán los siguientes trabajos.

- **Imprimir primero los documentos de la cola de impresión**. Al activar esta casilla, se enviarán primero los documentos que estén completos en la cola de impresión incluso si dichos documentos tienen menor prioridad que los otros.

- **Conservar los documentos después de su impresión**. Al activar esta casilla, los documentos no se borrarán de la cola de impresión después de haberse enviado (así, podrá volver a imprimirlos sin necesidad de hacerlo desde la aplicación).

- **Habilitar características de impresión avanzadas**. Al activar esta casilla, se utiliza la cola de impresión por metarchivos (*EMF*) y se habilitarán opciones como: **Orden de páginas**, **Impresión en folleto**, **Páginas por hoja**, etc. (si el modelo de impresora lo permite).

- Si se pulsa en **Valores predeterminados de impresión**, verá una pantalla en la que se pueden indicar los siguientes valores por defecto (se pueden modificar para una impresión personal desde **Preferencias de impresión** de la ficha **General**): la **Orientación**, el **Orden de las páginas** y las **Páginas por hoja** que va a imprimir.

  Si pulsa en la ficha **Papel/Calidad**, verá una pantalla en la que se pueden indicar los siguientes valores por defecto (se pueden modificar para una impresión personal desde **Preferencias de impresión** de la ficha **General**): el **Origen del papel**, la **Configuración de calidad** y el **Color** (éstas últimas no se ven en la pantalla de ejemplo pero pueden aparecer en otras impresoras).

  Si pulsa en **Opciones avanzadas** de la ficha **Presentación** o en **Avanzadas** de la ficha **Papel/Calidad**, verá una pantalla en la que se pueden indicar los siguientes valores por defecto (se pueden modificar para una impresión personal desde **Preferencias de impresión** de la ficha **General**): el **Tamaño del papel**, el **Número de copias**, la **Calidad de impresión**, etc.

Cuando haya finalizado, pulse en **Aceptar** dos veces para volver a la pantalla de **Propiedades** de la impresora.

- Si se pulsa en **Procesador de impresión**, verá una pantalla en la que se puede indicar el tipo de datos predeterminado que utilizará el procesador de impresión.

  Cuando haya finalizado, pulse en **Aceptar** para volver a la pantalla de **Propiedades** de la impresora.

- Si se pulsa en **Página de separación**, verá una pantalla en la que se puede indicar la página de separación que se utilizará al comienzo de cada documento (si pulsa en *Examinar*, podrá seleccionarla).

  Cuando haya finalizado, pulse en **Aceptar** para volver a la pantalla de **Propiedades** de la impresora.

Si pulsa en la ficha **Configuración de dispositivo**, verá una pantalla en la que se encuentran las posibles opciones que hay disponibles para modificar su configuración.

Cuando haya acabado de hacer las modificaciones necesarias, pulse en **Cerrar** y saldrá de la pantalla de **Propiedades**.

En **Windows Vista:**

Para configurar las propiedades de una impresora, sitúese sobre dicha impresora (seleccionando **Impresoras** del **Panel de control**), pulse dos veces el botón izquierdo del ratón, abra el menú **Impresora**, seleccione **Propiedades** y verá una nueva pantalla (el número de fichas y su denominación dependerá del modelo de impresora):

Se encuentra en la ficha **General**. En ella se puede indicar la localización en donde se encuentra (**Ubicación**), escribir una breve descripción sobre la impresora (**Comentario**), ver información diversa sobre sus características, mandar imprimir una página de prueba (**Imprimir página de prueba**) o cambiar las preferencias personales de presentación y otras opciones (**Preferencias de impresión**). Estas últimas opciones dependen de la impresora y pueden ser: orientación del papel, imprimir en ambas caras, orden de las páginas, páginas por hoja, etc. (se describirán posteriormente).

Si pulsa en la ficha **Compartir**, verá una pantalla en la que puede modificar si la impresora está compartida (**Compartir esta impresora**), el nombre que mostrará (**Nombre de recurso compartido**) y si desea **Procesar trabajos de impresión en equipos cliente**. Si las opciones no están activas, pulse en **Cambiar opciones de uso compartido**.

También, puede instalar otros controladores adicionales para la impresora (así, podrá ser usada por otros usuarios que los necesiten y que utilicen otras versiones de Windows). Para ello, pulse en **Controladores adicionales**, active las casillas correspondientes a los entornos que desee y pulse en **Aceptar**.

Si pulsa en la ficha **Puertos**, verá una pantalla en la que se muestra la serie de puertos locales donde pueden estar conectadas las impresoras (indicando las impresoras que hay conectadas en cada uno de ellos). Se pueden realizar las siguientes tareas:

- Si desea añadir otro, marque en **Agregar puerto**, seleccione el tipo de puerto disponible y pulse en **Puerto nuevo**. En función del tipo de puerto elegido, deberá actuar de la manera siguiente:
  - Si ha seleccionado **Local Port**, deberá indicar el nombre de puerto local que desee, pulsar en **Aceptar** y, luego, en **Cerrar**.
  - Si ha seleccionado **Standard TCP/IP Port**, entrará en el asistente para que indique la dirección IP que va a darle (siga los pasos indicados hasta su finalización).
- Si desea configurar un puerto, sitúese sobre el puerto deseado, pulse en **Configurar puerto** e indique las características que desee.
- Si desea eliminar alguno de ellos, selecciónelo y pulse en **Eliminar puerto** (le pedirá confirmación del borrado).

Al activar la casilla **Habilitar compatibilidad bidireccional**, podrá utilizar esta característica de impresión que consiste en que un monitor de lenguaje supervisa la comunicación entre el equipo y la impresora y, después, transfiere el trabajo de impresión al monitor de puerto que controla la entrada y salida a la impresora (para poder utilizar la compatibilidad bidireccional, la impresora debe admitirla).

Al activar la casilla **Habilitar la cola de la impresora**, podrá hacer que una cola de impresión preste servicio a dos o más impresoras (de esta manera, cuando una impresora esté imprimiendo un trabajo, el siguiente trabajo se dirigirá a otra impresora). Para ello, una vez activada esta casilla, deberá activar todos los puertos a los que están conectadas todas las impresoras que va a agrupar (**Agrupación de impresoras**).

Si pulsa en la ficha **Opciones avanzadas**, verá una pantalla en la que se encuentran las opciones siguientes:

- **Siempre disponible**. Si activa esta casilla, estará indicando que la impresora va a estar disponible las 24 horas de cada día.

- **Disponible desde**. Si activa esta casilla, deberá indicar desde qué hora **hasta** qué hora estará disponible.

- **Prioridad**. Indica la prioridad predeterminada de esta impresora. Los documentos con mayor prioridad (99) se imprimirán antes que los de menor prioridad (1).

- **Controlador**. Indica el controlador de impresora que se está utilizando (si pulsa en el triángulo que hay a la derecha del apartado, podrá seleccionar otro. En caso de que desee añadir uno nuevo, pulse en **Controlador nuevo** y entrará en el **Asistente para agregar controladores de impresora**. Siga los pasos para seleccionar uno nuevo).

- **Imprimir utilizando la cola para que el programa termine más rápido**. Al activar esta casilla, los trabajos se enviarán a la cola de impresión en lugar de enviarse directamente a la impresora. Cuando ésta esté libre, empezará a imprimir el trabajo.

- **Iniciar la impresión cuando la última página haya entrado en la cola**. Al activar esta casilla, no empezará a imprimir un trabajo hasta que todo él esté almacenado en la cola de impresión (de esta manera, no se bloqueará la impresora si el ordenador que está preparando el trabajo es más lento que la impresión).

- **Empezar a imprimir de inmediato**. Al activar esta casilla, se empezará a imprimir nada más llegar la primera página a la cola de impresión (si la impresora está disponible).

- **Imprimir directamente en la impresora**. Al activar esta casilla, se mandará directamente el trabajo a la impresora (utilice esta

opción sólo cuando no pueda imprimir utilizando la cola de impresión).

- **Dejar pendientes documentos no coincidentes**. Al activar esta casilla, la cola de impresión comprobará que el trabajo que tiene almacenado coincide con el documento antes de ser enviado. Si no coinciden, el documento quedará retenido pero se imprimirán los siguientes trabajos.

- **Imprimir primero los documentos de la cola de impresión**. Al activar esta casilla, se enviarán primero los documentos que estén completos en la cola de impresión incluso si dichos documentos tienen menor prioridad que los otros.

- **Conservar los documentos después de su impresión**. Al activar esta casilla, los documentos no se borrarán de la cola de impresión después de haberse enviado (así, podrá volver a imprimirlos sin necesidad de hacerlo desde la aplicación).

- **Habilitar características de impresión avanzadas**. Al activar esta casilla, se utiliza la cola de impresión por metarchivos (*EMF*) y se habilitarán opciones como: **Orden de páginas**, **Impresión en folleto**, **Páginas por hoja**, etc. (si el modelo de impresora lo permite).

- Si se pulsa en **Valores predeterminados de impresión**, verá una pantalla en la que se pueden indicar los siguientes valores por defecto (se pueden modificar para una impresión personal desde **Preferencias de impresión** de la ficha **General**): la **Orientación**, el **Orden de las páginas** y las **Páginas por hoja** que va a imprimir.

  Si pulsa en la ficha **Papel/Calidad**, verá una pantalla en la que se pueden indicar los siguientes valores por defecto (se pueden modificar para una impresión personal desde **Preferencias de impresión** de la ficha **General**): el **Origen del papel**, la **Configuración de calidad** y el **Color** (éstas últimas no se ven en la pantalla de ejemplo pero pueden aparecer en otras impresoras).

  Si pulsa en **Opciones avanzadas** de la ficha **Presentación** o en **Avanzadas** de la ficha **Papel/Calidad**, verá una pantalla en la que se pueden indicar los siguientes valores por defecto (se pueden modificar para una impresión personal desde **Preferencias de impresión** de la ficha **General**): el **Tamaño del papel**, el **Número de copias**, la **Calidad de impresión**, etc.

Cuando haya finalizado, pulse en **Aceptar** dos veces para volver a la pantalla de **Propiedades** de la impresora.

- Si se pulsa en **Procesador de impresión**, verá una pantalla en la que se puede indicar el tipo de datos predeterminado que utilizará el procesador de impresión.

  Cuando haya finalizado, pulse en **Aceptar** para volver a la pantalla de **Propiedades** de la impresora.

- Si se pulsa en **Página de separación**, verá una pantalla en la que se puede indicar la página de separación que se utilizará al comienzo de cada documento (si pulsa en *Examinar*, podrá seleccionarla).

  Cuando haya finalizado, pulse en **Aceptar** para volver a la pantalla de **Propiedades** de la impresora.

Si pulsa en la ficha **Configuración de dispositivo**, verá una pantalla en la que se encuentran las posibles opciones que hay disponibles para modificar su configuración.

Cuando haya acabado de hacer las modificaciones necesarias, pulse en **Cerrar** y saldrá de la pantalla de **Propiedades**.

ADMINISTRANDO DOCUMENTOS DE LA COLA DE IMPRESIÓN EN WINDOWS (PARTE PRÁCTICA)

Cuando los usuarios imprimen sus trabajos, si la impresora se encuentra ocupada, se almacenarán en la cola de impresión esperando que puedan ser enviados a la impresora. Dichos documentos pueden ser administrados por los propios dueños de los trabajos y por los usuarios que tengan permiso de **Administrar documentos** tanto desde el servidor de impresión como desde cualquier equipo de la red que tenga instalada dicha impresora.

Para poder administrar unos documentos enviados a una impresora y que se encuentran a la espera de imprimirse, siga los pasos siguientes:

En **Windows XP:**

1. Seleccione **Impresoras y faxes** del **Panel de control**.

2. Pulse dos veces el botón izquierdo del ratón sobre la impresora que se quiere administrar y verá una pantalla en la que se muestra la siguiente información de los documentos que se van a imprimir: **Nombre del documento**, **Estado** en que se encuentra el documento, **Propietario**, **Páginas** que tiene, **Tamaño** que ocupa, la fecha y la hora en que fue **enviado** y el **Puerto** por donde se imprimirá**.**

3. Se pueden realizar las siguientes operaciones:

   - **Parar temporalmente la impresión de todos los documentos**. Si abre el menú **Impresora** y selecciona **Pausar la impresión** (estando está opción sin marcar), dejarán de imprimirse todos los documentos.

   - **Reiniciar la impresión**. Si abre el menú **Impresora** y selecciona **Pausar la impresión** (estando esta opción marcada), volverán a imprimirse los documentos.

   - **Parar la impresión de un documento**. Si elige un documento, abre el menú **Documento** y selecciona **Pausa**, éste dejará de imprimirse.

   - **Reanudar la impresión de un documento**. Si elige un documento, abre el menú **Documento** y selecciona **Reanudar**, éste volverá a imprimirse desde la página en que hizo la pausa (si hay otro documento imprimiéndose, se acabará de imprimir primero antes de reanudar la impresión).

   - **Reiniciar la impresión de un documento**. Si elige un documento, abre el menú **Documento** y selecciona **Reiniciar**, éste volverá a imprimirse desde la primera página (si hay otro documento que se esté imprimiendo, se acabará de imprimir primero antes de reiniciar la impresión).

   - **Cancelar un documento**. Si elige un documento o varios, abre el menú **Documento** y selecciona **Cancelar**, los documentos seleccionados se eliminarán de la cola de impresión.

   - **Cancelar todos los documentos**. Si abre el menú **Impresora** y selecciona **Cancelar todos los documentos**, se eliminarán todos los documentos de la cola de impresión.

   - **Ver y modificar las propiedades de un documento**. Si elige un documento, pulsa el botón derecho del ratón para ver su menú

contextual y elige **Propiedades**, verá una pantalla referida al documento en la que podrá indicar a qué usuario se enviará una notificación cuando se imprima el trabajo, la prioridad que se desea dar (a mayor prioridad, antes se imprimirá) y el momento en que se imprimirá (sin restricción de tiempo o en un intervalo de tiempo que deberá especificar).

Las fichas **Presentación** y **Papel/Calidad** son las mismas que las indicadas en **Valores predeterminados de impresión** del apartado **Propiedades avanzadas de la impresora** y no se pueden modificar.

4. Cuando haya terminado, pulse en **Aceptar** y volverá a la pantalla de la cola de impresión.

En **Windows Vista:**

1. Seleccione **Impresoras** del **Panel de control**.

2. Pulse dos veces el botón izquierdo del ratón sobre la impresora que se quiere administrar y verá una pantalla en la que se muestra la siguiente información de los documentos que se van a imprimir: **Nombre del documento**, **Estado** en que se encuentra el documento, **Propietario**, **Páginas** que tiene, **Tamaño** que ocupa, la fecha y la hora en que fue **enviado** y el **Puerto** por donde se imprimirá**.**

3. Se pueden realizar las siguientes operaciones:

   - **Parar temporalmente la impresión de todos los documentos**. Si abre el menú **Impresora** y selecciona **Pausar la impresión** (estando está opción sin marcar), dejarán de imprimirse todos los documentos.

   - **Reiniciar la impresión**. Si abre el menú **Impresora** y selecciona **Pausar la impresión** (estando esta opción marcada), volverán a imprimirse los documentos.

   - **Parar la impresión de un documento**. Si elige un documento, abre el menú **Documento** y selecciona **Pausa**, éste dejará de imprimirse.

   - **Reanudar la impresión de un documento**. Si elige un documento, abre el menú **Documento** y selecciona **Reanudar**, éste volverá a imprimirse desde la página en que hizo la pausa (si

hay otro documento imprimiéndose, se acabará de imprimir primero antes de reanudar la impresión).

- **Reiniciar la impresión de un documento**. Si elige un documento, abre el menú **Documento** y selecciona **Reiniciar**, éste volverá a imprimirse desde la primera página (si hay otro documento que se esté imprimiendo, se acabará de imprimir primero antes de reiniciar la impresión).

- **Cancelar un documento**. Si elige un documento o varios, abre el menú **Documento** y selecciona **Cancelar**, los documentos seleccionados se eliminarán de la cola de impresión.

- **Cancelar todos los documentos**. Si abre el menú **Impresora** y selecciona **Cancelar todos los documentos**, se eliminarán todos los documentos de la cola de impresión.

- **Ver y modificar las propiedades de un documento**. Si elige un documento, pulsa el botón derecho del ratón para ver su menú contextual y elige **Propiedades**, verá una pantalla referida al documento en la que podrá indicar a qué usuario se enviará una notificación cuando se imprima el trabajo, la prioridad que se desea dar (a mayor prioridad, antes se imprimirá) y el momento en que se imprimirá (sin restricción de tiempo o en un intervalo de tiempo que deberá especificar).

  Las fichas **Presentación** y **Papel/Calidad** son las mismas que las indicadas en **Valores predeterminados de impresión** del apartado **Propiedades avanzadas de la impresora** y no se pueden modificar.

4. Cuando haya terminado, pulse en **Aceptar** y volverá a la pantalla de la cola de impresión.

LA GESTIÓN DE IMPRESORAS EN LINUX (PARTE PRÁCTICA)

CUPS (**Common Unix Printing System**) es el Sistema de Impresión Común de Unix. Ha sido desarrollado para promover una solución de impresión estándar para todos los sistemas de tipo Unix (incluido Linux) y proporciona las tareas básicas de gestión de impresión y de colas de impresión para una gran cantidad de modelos de impresoras. Está basado en el Internet Printing Protocol

(IPP), que es un nuevo protocolo de red que proporciona un conjunto estándar de servicios de impresión en red.

CUPS proporciona, además, los comandos estándar de las implementaciones Berkeley (lpr) y System V (lp), además de un comando de administración: lpadmin.

En sistemas tipo Unix existen otros sistemas de impresión como LPD o LPR/LPRNg, aunque en Linux el más extendido es CUPS.

En todas las distribuciones actuales, CUPS se instala por defecto, sin embargo, para utilizarlo es necesario que el servicio esté activado. Hay que verificar para ello que exista en memoria un proceso llamado *cupsd* o *cups*. Se puede verificar desde una consola de comandos con el comando:

```
ps –ef | grep cupsd
```

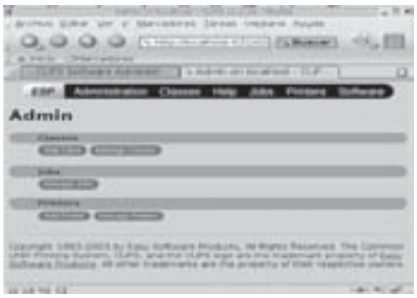
Si no aparece en memoria, hay que arrancar el servicio. Para ello, es necesario ejecutar los siguientes comandos desde una consola como usuario *root*:

```
cd /etc/init.d
./cups start
```

Una vez arrancado el servicio, la gestión del mismo se realiza a través de la herramienta de administración web a la cual se accede a través de un navegador web utilizando la dirección **http://localhost:631**.

Desde esta interfaz web de CUPS se pueden realizar las siguientes acciones:

- Gestión de clases
- Gestión de trabajos de impresión
- Gestión de impresoras



Administración de CUPS

Una clase es simplemente una **agrupación de impresoras**, de forma que si se envía un trabajo de impresión a una clase, éste se imprimirá en la primera impresora libre de la clase.

Gestión de una clase

La principal tarea para la cual se utiliza CUPS es para configurar impresoras, ya que la impresión de trabajos se llevará a cabo desde las propias aplicaciones, como editores de texto, navegadores web, etc.

Los pasos a seguir para configurar una impresora utilizando la interfaz web de CUPS son:

1. En la pantalla de administración de CUPS pulse en **Add printer** y rellene los campos **Name***,* **Location** *y* **Description**. El único importante es el nombre (*Name)* de la impresora. Se puede utilizar cualquier nombre descriptivo de la impresora pero sin espacios en blanco.

2. Configure el modo de conexión de la impresora (**Device**). Aquí CUPS ofrece las siguientes alternativas:

Internet Printing Protocol	Impresora conectada a otro equipo Linux/Unix con CUPS
LPD/LPR Host or Printer	Impresora conectada a otro equipo Linux/Unix con LPD/LPR

Parallel Port	Impresora local conectada al puerto paralelo
SCSI Printer	Impresora local conectada al bus SCSI
Serial Port	Impresora local conectada a un puerto serie
USB Printer	Impresora local conectada al bus USB
Windows Printer via SAMBA	Impresora conectada a otro equipo Windows

3. Elija el fabricante de la impresora:

4. Elija el modelo y el controlador:

Si el modelo de impresora que se quiere configurar no aparece en la lista de CUPS, se puede obtener el controlador en la página **www.linuxprinting.org** (en el siguiente apartado se darán más detalles al respecto).

5. Desde la opción **Printers** se puede ver la impresora recién configurada.

Impresoras no soportadas en CUPS

Si se trabaja con versiones recientes o actualizadas de las diferentes distribuciones, posiblemente no habrá problemas al encontrar la impresora que se desea configurar desde la interfaz web de CUPS. Sin embargo, si se utiliza alguna distribución algo más antigua o un modelo de impresora muy actual, puede ocurrir que en la interfaz web de administración de CUPS no aparezca la impresora que se desea configurar. En este caso, lo más recomendable es acudir a la página web **www.linuxprinting.org** que contiene la base de datos más extensa de los drivers de impresoras de libre distribución. Los pasos a seguir para añadir la impresora a CUPS son los siguientes:

1. Busque el modelo de impresora en la página web de *linuxprinting*, dentro de la opción **Printer listing**.

Página web de linuxprintig.org

2. Elija el driver correspondiente. Hay tres tipos de drivers que son válidos para prácticamente todos los modelos de impresoras. La mayor parte de las distribuciones incluyen estos drivers y, en la mayoría de los casos, sólo hay que descargar un fichero PPD.

a. Ghostscript

Compruebe si ya está el driver instalado, ejecutando el comando *gs –h*. Si no está instalado, se puede descargar el paquete software *ESP Ghostscript* de la página **www.cups.org/espgs/index.php**, aquí se incluyen todos los drivers Ghostscript.

b. Filter

En este caso, el driver es un fichero ejecutable. Para comprobar si está instalado en el sistema, utilice el comando *which* seguido del nombre del driver. Por ejemplo: *which hpijs*.

Si no aparece, habrá que descargarlo de la página indicada. Los drivers más usados suelen estar incluidos por defecto en todas las distribuciones, como, por ejemplo, los drivers *gimp-print* o *hpijs* que se utilizan para más de 500 modelos de impresoras.

c. Postscript

En este caso, no necesita driver; sólo habrá que descargarse el fichero PPD.

3. Descargue el fichero *PPD* (*Postscript Printer Description*). Este tipo de fichero contiene una descripción de las características de un modelo concreto de impresora, como tipo de papel soportado, resolución, soporte de impresión a doble hoja, colores, etc. Estas características se describen en un lenguaje que los drivers saben interpretar de forma que actúan ajustando el comportamiento genérico de los drivers anteriores al modelo concreto de cada impresora. En la mayoría de los casos, configurar en CUPS una impresora que no esté en la lista por defecto se reduce a obtener su fichero PPD.

   Dicha descarga se realiza desde la propia página de *linuxprinting* y este fichero se deberá copiar en el directorio **/usr/share/cups/model** con permiso de lectura para todos los usuarios.

4. Por último, sólo queda reiniciar CUPS desde una consola. Como usuario *root* teclee:

```
cd /etc/init.d
./cups restart
```

Otras herramientas de gestión de impresión

A pesar de la existencia de esta cómoda interfaz web de configuración de impresoras que ofrece CUPS, muchas distribuciones han optado por desarrollar otras herramientas de gestión de impresión, aunque la mayoría de estas aplicaciones utiliza CUPS como gestor de impresión. Se recomienda, sin duda, la utilización de la interfaz web de CUPS que ofrece mucha más homogeneidad entre distribuciones. Un ejemplo es la aplicación de gestión de impresoras desarrollada en el entorno KDE.

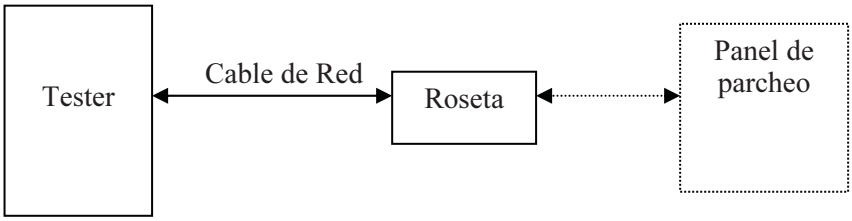
Herramienta de configuración de impresoras de KDE

PASOS A SEGUIR PARA VER DÓNDE SE ENCUENTRA UN FALLO EN EL CABLEADO (PARTE PRÁCTICA)

Ante un fallo del cableado, lo primero que hay que hacer es comprobar el cable que va desde la tarjeta de red del equipo hasta la roseta.

Para ello, se coge el tester, se conecta a ambos extremos del cable y se comprueba si se enciende alguna luz roja o se encienden las 4 verdes. En este caso, deberán encenderse las luces verdes en la secuencia 1-2-3-4, por lo que el cable es correcto.

El siguiente paso será comprobar la roseta. Para ello, se coge el cable que se acaba de comprobar y se conecta un extremo a la unidad principal del tester y el otro extremo a la roseta que estará conectado en el panel de parcheo, se suelta y se conecta en el terminador del tester.



Se vuelve a la unidad principal del tester, se enciende y se comprueba que el botón GND está en OFF y se observa cuántas luces verdes se encienden en el terminador.

Si se encendiesen las 4 verdes, la roseta estaría bien conectada y si se encendiese alguna luz roja, indicaría que hay algún cable mal conectado en la roseta.

Si hubiera algún error, antes de sustituir todo el cable interior por uno nuevo, se desmonta la roseta para ver si el corte está allí.

Una vez encontrada la avería y para comprobar que el cable no está cortado en otro punto de la canalización, se ha de repetir de nuevo la comprobación.

Apéndice

MONTAR UNA RED EN LINUX (PARTE PRÁCTICA)

INSTALACIÓN Y CONFIGURACIÓN DE UN ADAPTADOR ETHERNET

La configuración de un adaptador de red en Linux requiere también de la instalación del controlador de dispositivo asociado. Sin embargo, a diferencia de otros entornos, en Linux todos esos programas se pueden instalar de dos formas distintas:

- Recompilando el núcleo de Linux para dar soporte al dispositivo.
- Incluyendo el controlador como un módulo cargable del núcleo.

La segunda opción suele ser más recomendada, ya que permite activar o desactivar el dispositivo cargando o descargando el módulo. Además, la no inclusión del módulo en el núcleo permite que este último ocupe un tamaño menor, situación que siempre es deseable con el fin de evitar problemas cuando el sistema debe cargarlo al arrancar.

La segunda opción también permite que la carga del módulo se realice de forma automática en el arranque, o de forma manual por los usuarios autorizados (como mínimo, será *root*). Para gestionar los módulos del núcleo, se pueden

utilizar los comandos *lsmod* (muestra los módulos cargados actualmente), *insmod* y *modprobe* (carga un módulo, aunque es más seguro usar este último) o *rmmod* (descarga un módulo), o acceder en el entorno gráfico a la configuración de los módulos cargables del núcleo dentro del panel de control (*control-panel*) de Linux Red Hat. La figura A.1 muestra la ventana gráfica de esta utilidad. Si estamos utilizando SuSE Linux, podemos acceder a las mismas opciones desde las utilidades YaST y YaST2. Todos los cambios que se realicen en estas utilidades serán actualizados en los parámetros correspondientes del archivo de configuración de módulos cargables del núcleo (es */etc/modules.conf*).

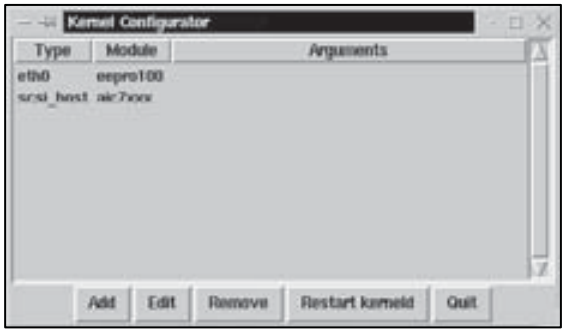


Figura A.1. Ventana de configuración de los módulos cargables del núcleo en Red Hat 6.2

En las últimas versiones de Linux disponibles actualmente no es necesario configurar manualmente el adaptador de red instalado, ya que el núcleo suele detectarlo automáticamente para seleccionar el módulo de carga adecuado. Sin embargo, sí es necesaria esa configuración manual cuando hay problemas en la detección o existe más de una tarjeta instalada. Al finalizar este apartado, se expone más a fondo la configuración manual de un adaptador de red en Linux.

Para las tarjetas de red *Ethernet*, Linux asigna un nombre de controlador al estilo *ethx*, donde *x* es un número entero entre 0 y 3. En realidad, ese nombre es un alias asociado con el controlador específico de la tarjeta (módulo cargable). Si el sistema detecta la tarjeta de red instalada en el primer arranque, el comando siguiente debe devolver un conjunto de parámetros que comienzan con *eth0*[1]:

```
$ ifconfig eth0
```

Una vez detectada la tarjeta, sólo hay que especificar el módulo a cargar (controlador) y los parámetros de TCP/IP. Todo ello se puede configurar desde el

[1] El comando **ifconfig** en Linux es muy parecido al comando *ipconfig* de Windows, aunque este último solamente se utiliza para consultar los parámetros de TCP/IP.

panel de control de Red Hat, a través del icono **Network Configuration** de la ficha **Dispositivos**. La figura A.2 muestra la ventana principal de esta utilidad.

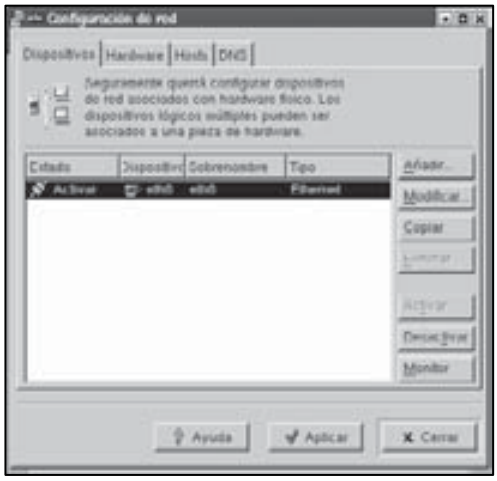


Figura A.2. Ventana principal de configuración de un adaptador de red en Linux Red Hat (versiones 7.0 o superiores)

En esta ventana aparece una lista de los adaptadores de red detectados que pueden activarse o desactivarse en cualquier momento. Utilizando los botones **Agregar** y **Configurar**, es posible establecer los parámetros del dispositivo en lo que se refiere a tipo y fabricante, nombre de controlador, etc.

Si el núcleo detecta algún dispositivo instalado, cargará de forma automática el módulo correspondiente. Puede ocurrir que no detecte el modelo de tarjeta instalada, pero, en ese caso, la podemos seleccionar de una lista desde la ficha **Hardware** pulsando el botón **Modificar**, siempre en la ventana de configuración de red (véase la figura A.3). En caso de que el adaptador de red no aparezca en la lista, habrá que buscar otro compatible o instalar el controlador proporcionado por el fabricante.

Una vez establecido el modelo de adaptador de red, hay que establecer la configuración de los parámetros del protocolo TCP/IP (dirección de red y máscara, dirección de la puerta de enlace, direcciones de los servidores de nombres, etc.). Esto se puede realizar desde las páginas accesibles en la ventana asociada al icono **Network Configuration** (figura A.2).

La dirección IP del adaptador, su máscara y la dirección de la pasarela por defecto se configuran accediendo a la ficha **Dispositivos**, seleccionando el elemento de la lista y pulsando el botón **Modificar**. Puede indicarse también una

dirección asignada por DHCP, si es que disponemos de un servidor de este tipo en la red.

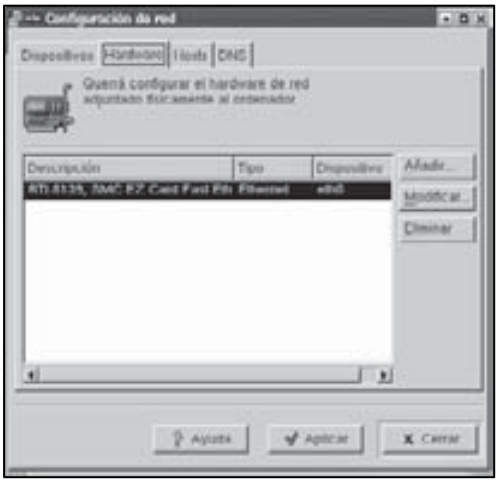


Figura A.3. Configuración hardware de un adaptador de red en Red Hat (versión 7.0)

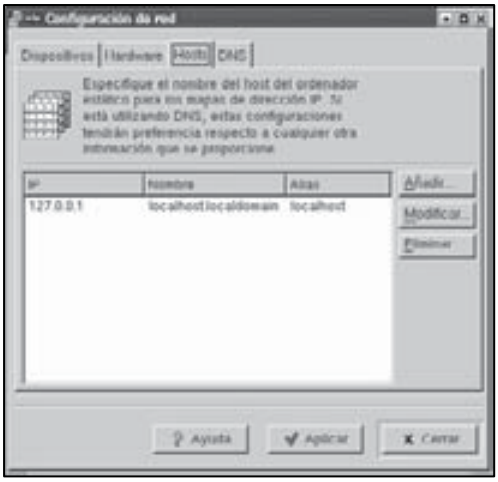


Figura A.4. Configuración de la tabla local de equipos en el cliente DNS en Linux Red Hat

La configuración del servicio DNS en la estación se realiza dentro de las fichas **Hosts**, **DNS** y de la configuración de red (véanse las figuras A.4 y A.5). En la configuración DNS se especifica el nombre de dominio del equipo, algunos nombres de dominio y direcciones IP de equipos conocidos (tabla de *hosts* local) y las direcciones IP de servidores DNS de la red.

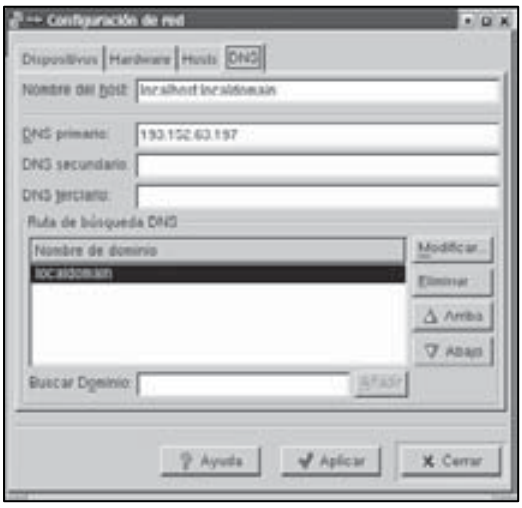


Figura A.5. Configuración de un cliente DNS en Linux Red Hat

En el caso de SuSE Linux, la idea básica de configuración del adaptador es la misma que en Red Hat, pero los programas gráficos son diferentes. Si se dispone de *YaST* o *YaST2*, la configuración resulta bastante sencilla ya que estos programas ofrecen un entorno centralizado con todas las opciones necesarias.

Desde *YaST*, la configuración del módulo de red se realiza seleccionando **Administración del sistema**, **Instalar hardware en el sistema** y **Configurar dispositivo de red**, lo que muestra una ventana como la de la figura A.6. Por su parte, para la configuración de los parámetros de TCP/IP, hay que seleccionar las opciones **Administración del sistema**, **Configuración de red** y **Configuración básica de red**, lo que muestra una ventana como la de la figura A.7.

Figura A.6. Selección del modelo de adaptador de red en YaST

Figura A.7. Configuración de los parámetros TCP/IP en YaST

Desde *YaST2* la configuración es similar, aunque el acceso a las ventanas es distinto. Para establecer el modelo de adaptador de red, hay que acceder a la configuración avanzada desde **Red/Básica** y **Configuración de la tarjeta de red**, y, en la ventana que aparece, marcar la opción **Hardware**. Posteriormente, hay que seleccionar el adaptador y pulsar sobre el botón **Editar**, lo que muestra una ventana como la de la figura A.8. La configuración de TCP/IP en *YaST2* se realiza editando el adaptador de red en la ventana que aparece al seleccionar **Red/Básica** y **Configuración de la tarjeta de red**, salvo que en este caso se pulsa la opción **Interfaz**. Seleccionando el adaptador y pulsando en el botón **Editar**, se accede a su configuración TCP/IP (figura A.9). La opción **Elegir el método de configuración** de esa ventana permite indicar una dirección IP fija (seleccionando **Configuración de la dirección estática** e introduciendo los valores correspondientes en los cuadros **Dirección IP** y **Máscara de subred**) o asignada mediante DHCP [seleccionando **Dirección automática (vía DHCP)**]. La figura A.9 muestra esta ventana de configuración en *YaST2*.

Figura A.8. Configuración hardware de un adaptador de red en YaST2

Figura A.9. Configuración de los parámetros TCP/IP en YaST2

Finalmente, se pueden incluir entradas del protocolo ARP utilizando el comando *arp* (siempre como usuario *root*). Las opciones de este comando son muy parecidas al mismo comando en la versión Windows, aunque con algunas diferencias. Para más información, puede consultarse la ayuda de las páginas del manual (comando *man*). Un ejemplo de añadido de entrada ARP puede ser el siguiente:

```
$ arp -s 10.0.18.218 00:60:08:03:CE:5A
```

Para comprobar que esta configuración funciona correctamente, se puede ejecutar el comando *ping* con la dirección de otro equipo conectado a la red (y activado en ese momento). Si se produce respuesta a los paquetes enviados, entonces es que el adaptador funciona perfectamente. Si se desea realizar una consulta de todos los parámetros de configuración TCP/IP en Linux, se puede escribir el siguiente comando en la ventana de terminal (teniendo en cuenta que *eth0* hace referencia a la configuración TCP/IP asociada con ese adaptador):

```
$ ifconfig eth0
```

INSTALACIÓN Y CONFIGURACIÓN DE UN ADAPTADOR INALÁMBRICO

Debido a que las tecnologías de redes inalámbricas son relativamente recientes, su desarrollo en la comunidad Linux todavía no ha llegado a su culminación, debido sobre todo a la escasez de programas controladores necesarios para que el sistema operativo pueda manejar los adaptadores. Sin embargo, los

programas de configuración y acceso a redes inalámbricas ya han sido plenamente desarrollados e incluidos en todas las distribuciones de Linux.

Los pasos para instalar y configurar el adaptador en Linux son muy parecidos a instalar y configurar un adaptador Ethernet. En primer lugar, se debe acceder a *YaST2* y seleccionar el icono de configuración del adaptador de red. Se van a seguir los pasos sobre la versión 8.2 de SuSE Linux ya que las versiones anteriores no soportan correctamente los adaptadores inalámbricos.

Si todo va correctamente, encontraremos que *YaST2* ha detectado el adaptador inalámbrico y está dispuesto a configurarlo, pulsando en el botón **Configurar** (véase la figura A.10). Si no se ha detectado el dispositivo es porque esta versión no es capaz de manejarlo, aunque existe la posibilidad de intentar configurarlo manualmente seleccionando el icono **Otro (no detectado)**.

La configuración TCP/IP del adaptador inalámbrico se realiza de la misma forma que un adaptador Ethernet. La única diferencia consiste en que deberemos acceder a los parámetros de configuración de la red inalámbrica, que se encuentran dentro de la opción **Detalles del hardware** en el botón **Configuración wireless**.

Figura A.10. Detección de un adaptador de red en YaST2

No hay que olvidar que una vez establecidos los parámetros de configuración de la red inalámbrica hay que configurar también los parámetros TCP/IP y comprobar que todo funciona correctamente.

Además de la herramienta *YaST*, también se pueden utilizar los siguientes comandos para comprobar la detección y configuración de los dispositivos inalámbricos (siendo usuario *root*):

- **cardctl ident**: se utiliza para mostrar la identificación de los dispositivos PCMCIA conectados al equipo.

- **iwconfig**: se utiliza para consultar cuáles son los dispositivos inalámbricos de cualquier tipo detectados por el sistema. Para poder utilizar este comando es necesario instalar el paquete **wireless-tools**.

Figura A.11. Parámetros de configuración de la red inalámbrica en YaST2

ARCHIVOS DE CONFIGURACIÓN DE RED

Independientemente de la herramienta que se utilice para configurar un adaptador de red en Linux, todas las modificaciones realizadas siempre se guardan en los archivos de configuración con formato texto que se encuentran desperdigados por el sistema de archivos. Cuando el usuario que desea configurar los parámetros de red del sistema no tiene conocimientos avanzados en él, entonces siempre es aconsejable recurrir a las utilidades de administración que se han visto en los apartados anteriores.

Sin embargo, cuando nos encontramos con problemas en la configuración de red en Linux o deseamos establecer algunas características avanzadas, la mejor forma de lograrlo es acceder directamente a los archivos de texto que guardan los parámetros del sistema referentes a la red. Dependiendo de la distribución, éstos pueden diferir o encontrarse en diferentes directorios dentro del disco (normalmente en la carpeta */etc*). La mayoría de los expuestos aquí son comunes para las distribuciones Red Hat, SuSE, Mandrake y Debian (a no ser que se indique

lo contrario). Los archivos de configuración básica de red se enumeran a continuación:

- **/etc/modules.conf**. Archivo opcional que guarda información sobre los módulos cargables del núcleo. Para el módulo de la tarjeta de red suele incluirse un alias del nombre genérico *eth0* con el controlador de dispositivo concreto (que dependerá del modelo y fabricante del adaptador y que estará guardado como archivo en la carpeta */dev*).

- **/etc/protocols**. Archivo que guarda los nombres de los protocolos de transporte usados por el sistema.

- **/etc/services**. Contiene una lista de los nombres de los servicios reconocidos por el sistema (protocolos de nivel de aplicación).

- **/etc/pcmcia/config**. Se trata de una base de datos con información sobre los adaptadores PCMCIA reconocidos por Linux.

- **/etc/host.conf**. Este archivo se utiliza para controlar el funcionamiento de la resolución de nombres del cliente DNS en SuSE Linux y Red Hat. En algunas versiones se utiliza el archivo */etc/nsswitch.conf* en vez de éste.

- **/etc/resolv.conf**. Se utiliza para la configuración del cliente DNS. Aquí se especifica el dominio al que pertenece el equipo local, las direcciones IP de los servidores de nombres, etc.

- **/etc/networks**. Este archivo es parecido a */etc/hosts* pero, en este caso, no aparecen nombres de equipos, sino nombres de redes con sus correspondientes direcciones de red.

- **/etc/HOSTNAME**. En él se guarda solamente el nombre del equipo local sin el dominio. No debe incluirse ninguna información adicional.

- **/etc/hosts**. Guarda la tabla local de resolución de nombres en los casos en los que no se usa un servidor DNS.

- **/proc/net/arp**. Archivo que guarda la tabla local de resolución de direcciones ARP.

- **/etc/inetd.conf**. Archivo de configuración de los servicios del demonio *inetd*. Aquí aparecen todos los servicios del sistema, los que se encuentran activos y los desactivados (aquéllos que incluyen un carácter “#” al principio de su línea correspondiente).

- **/etc/sysconfig/network**. Contiene la configuración básica de la red del equipo local en SuSE y Linux Red Hat.

- **/etc/sysconfig/network-scripts/ifcfg-xxx**. *shell-scripts*[2] de configuración de red del equipo local (*xxx* especifica el nombre del archivo controlador de red, que normalmente es *eth0*) en SuSE y Linux Red Hat.

- **/etc/sysconfig/network/wireless**. Contiene la configuración básica de la red inalámbrica del equipo local en SuSE y Linux Red Hat.

- **/etc/rc.config**. Es el fichero principal de configuración de red del sistema en SuSE Linux. Todas las utilidades de configuración (*YaST* y *YaST2*) leen la información en base a este archivo y el resto de ellos se configura a partir de éste. Si se modifica a mano este archivo, es necesario ejecutar *YaST*, *YaST2* o *SuSEconfig* para actualizar los cambios en todos los archivos del sistema necesarios.

- **/etc/nscd.conf**. Es el archivo que se utiliza para configurar el servicio *nscd* (*Name Service Cache Daemon* o *Demonio de Caché del Servicio de Nombres*) en SuSE Linux.

Hay que tener cuidado al modificar de forma manual estos archivos con un editor de texto, ya que cualquier pequeño error al teclear puede hacer que nuestro sistema se comporte de forma anómala. Además, muchos parámetros de configuración de la red se suelen repetir en varios de esos archivos (como la dirección IP), con lo que se debe establecer el mismo valor en ellos para evitar comportamientos anómalos del sistema. En el caso de SuSE Linux, bastará con ejecutar las utilidades *YaST*, *YaST2* o *SuSEconfig* para actualizar todos los archivos con los nuevos cambios establecidos o introducidos directamente en */etc/rc.config*.

COMPARTIR ARCHIVOS EN UNA RED LINUX

La forma en la que se comparte el sistema de archivos de una máquina Linux depende de la máquina cliente que desea tener accesible ese recurso. Si se trata de una máquina Windows, puede consultar el apartado siguiente dentro de este mismo apéndice. Si se trata de una máquina también Linux, será necesario utilizar **NFS** (**Network File System** o **Sistema de Archivos de Red**). Según este sistema, se utiliza el comando *mount* para montar la carpeta remota a la que se desea acceder, especificando el nombre DNS de la máquina remota. Para poder

[2] Un *shell-script* de Linux contiene una secuencia de comandos que se ejecutan uno a continuación del otro como órdenes del sistema operativo u otros archivos ejecutables.

utilizar NFS, hay que instalar el paquete correspondiente, que incluye los módulos *nfsd* y *mountd*. Si se desea utilizar la versión 3 o superior de NFS, hay que disponer del núcleo 2.4 o superior de Linux. Cualquier archivo o carpeta que se desee compartir, deberá especificarse de forma manual dentro del archivo */etc/exports* o a través de alguna herramienta gráfica que no hace más que modificar este archivo.

El sistema de archivos NFS se ha convertido hoy en día en un estándar que permite compartir archivos en una red de forma segura. Su método de configuración es capaz de establecer permisos de acceso a los usuarios y también permite indicar qué equipos pueden acceder a un determinado recurso compartido.

La mayoría de las versiones de Linux llevan el soporte para NFS en la instalación por defecto del sistema. Para comprobar que su versión de Linux está preparada, deberá seguir unos pasos previos a la configuración y uso de este servicio. Lo primero que deberá hacerse es comprobar si la versión del núcleo de Linux tiene soporte para NFS; para ello, deberá ejecutar lo siguiente:

```
root@linux:~# cat /proc/filesystems
```

que deberá devolver una lista con los sistemas de archivos soportados por el núcleo, entre los que deberá aparecer NFS. En caso contrario, hay que instalar una versión más reciente del núcleo que lo soporte. Seguidamente, habrá que comprobar si está instalado el paquete de NFS. Para ello, hay que usar el comando *rmp* o la herramienta gráfica de gestión de paquetes de *YaST2*:

```
root@linux:~# rpm -qa | grep nfs
nfs-utils-1.0.1-89
```

El paquete que aparece contiene tanto el servidor NFS (para compartir una carpeta de nuestro sistema) como el cliente NFS (para acceder a una carpeta compartida de otro equipo). Si el comando anterior no devuelve ningún nombre de paquete, habrá que instalarlo:

```
root@linux:~# rpm -i nfs-utils-1.0.1-89.i586.rpm
```

Una vez instalado el soporte para NFS, es necesario activar los programas demonio que se encargan del manejo del protocolo de comunicación de NFS. Para ello, se puede acceder al editor de niveles de ejecución de *YaST2* e indicar que se deben iniciar los servicios *nfsserver* y *nfslock*. También, se puede hacer esto accediendo a la herramienta **Servidor NFS** en el grupo **Servicios de red** de *YaST2* y pulsar la opción **Arrancar el servidor NFS**.

Una vez activado el soporte para NFS, hay que configurarlo. En caso de que el usuario desee permitir el acceso de otras personas a sus carpetas

compartidas, tendrá que editar el archivo */etc/exports*. Cada fila de este archivo contiene una carpeta compartida, mientras que cada columna contiene la siguiente información (separada por espacios):

- ☑ Ruta completa y nombre de la carpeta compartida.
- ☑ Permisos de acceso, que se establecen con dos parámetros:
  - ➢ Conjunto de equipos que tiene acceso a la carpeta (puede especificarse a través de los nombres de equipos, sus dominios o sus direcciones IP).
  - ➢ Tipo de acceso, que puede ser:
    - **ro**. Sólo se dispone de derecho de lectura (es el valor por defecto). El valor contrario es **rw**.
    - **root_squash**. Si el usuario que está accediendo a la carpeta es *root*, en su equipo no se aplicarán sus derechos, sino los del usuario *nobody*. Esta opción es contraria a **no_root_squash**.
    - **no_subtree_check**. Se utiliza cuando se comparte un sistema de archivos completo para permitir una mayor velocidad en las transferencias de archivos.
    - **sync**. Antes de la versión 1.11 de NFS, si se producía un reinicio del servidor durante la transferencia del archivo, se producía la corrupción de los datos (comportamiento establecido por defecto al valor **async**). Si se usa el valor *sync*, entonces se previene estas situaciones.

Por ejemplo, el archivo */etc/exports* podría contener lo siguiente:

```
# Ejemplo de archivo /etc/exports
/server1(rw) server2(rw,no_root_squash)
/home/usr1*.local.domain(ro)
/home 10.0.1.20(root_squash)
/usr/share10.0.0.0/255.0.0.0(ro)
/var/lib *(ro)
```

La segunda línea especifica que las máquinas cuyo nombre DNS es *server1* y *server2* tienen acceso de lectura y escritura (*rw*) sobre la carpeta raíz (*/*), aunque en el segundo caso el usuario *root* tendrá acceso total a la carpeta (*no_root_squash*).

La tercera línea especifica que cualquier máquina cuyo dominio sea *local.domain* tiene acceso de sólo lectura (*ro*) sobre la carpeta */home/usr*. Por su parte, la cuarta línea especifica que desde la máquina que tiene la IP 10.0.1.20, se tendrá acceso a la carpeta */home* y se mantendrán todos los permisos establecidos (*root_squash*).

La quinta línea indica que se va a compartir la carpeta */usr/share* como sólo lectura para todos los equipos cliente que se encuentren en la red 10.

La última línea indica que cualquier equipo (*) puede acceder a la carpeta */var/lib* con permiso de sólo lectura (*ro*). Recuerde que los nombres DNS pueden especificarse en una tabla local almacenada en el archivo */etc/hosts*, donde existe una correspondencia estática con las direcciones IP. Sin embargo, a no ser que se conozca perfectamente el funcionamiento de DNS, se recomienda especificar direcciones IP en */etc/exports*, ya que es un método más fiable y seguro.

Una vez modificado el archivo */etc/exports*, es necesario que los demonios de NFS apliquen esos cambios. Para ello, se puede acceder al editor de niveles de ejecución y reiniciar los procesos *nfsserver* y *nfslock* o ejecutar el siguiente comando como usuario *root*:

```
root@linux:~# exportfs -ra
```

Para especificar un conjunto de equipos en la misma red, se puede utilizar la opción especificada anteriormente o los números de red como “10.” o “192.168.”. Así mismo, se pueden utilizar nombres de dominio con asteriscos (*) como “*.mired.com” o “*.es”. Sin embargo, hay que tener en cuenta que estos métodos no funcionan bien con versiones del núcleo anteriores a la 2.2.19.

Figura A.12. Ventana principal de configuración del servidor NFS en YaST2

Además de la modificación manual del archivo */etc/exports*, se puede utilizar la herramienta gráfica de configuración **Servidor NFS** del grupo de opciones **Servicios de red** de *YaST2* de SuSE Linux. Ésta permite editar el archivo */etc/exports* y aplicar todos los cambios que se hayan realizado (véase la figura A.12).

Existen algunas consideraciones a tener en cuenta cuando se comparte una carpeta con NFS:

- ✓ No deben compartirse al mismo tiempo las carpetas padre e hijas de ella (en ese caso, se deberá compartir solamente la carpeta padre, de esta forma se accede a todas las hijas).

- ✓ No debe compartirse una carpeta que se encuentra almacenada en una partición de tipo FAT o VFAT, ya que son sistemas que no soportan accesos simultáneos por distintos usuarios.

Los programas demonio involucrados en una comunicación por NFS son los siguientes (deberán estar en ejecución en el servidor para que todo funcione):

- ☑ **portmap**. Mapeador de puertos utilizado también por otros servicios.

- ☑ **nfsd** (o **nfsserver**). Demonio de NFS que realiza la mayor parte del trabajo.

- ☑ **lockd** y **statu**. Se encargan de gestionar el bloqueo de archivos compartidos.

- ☑ **mountd**. Gestiona las solicitudes de montaje.

- ☑ **rquotad**. Demonio encargado de verificar las cuotas de disco.

Para comprobar si todos estos programas demonio están activos en el servidor, hay que ejecutar el siguiente comando como usuario *root*:

```
root@linux:~# rpcinfo -p
```

Para acceder desde un equipo cliente a una carpeta compartida NFS, en primer lugar deberán realizarse las mismas comprobaciones que para el servidor, es decir, si el núcleo tiene soporte para NFS, se encuentra instalado el paquete (*nfs-utils*) y se encuentran en ejecución los demonios *portmap*, *lockd* y *statd*. Después de esto, solamente será necesario montar la carpeta compartida en el sistema de archivos local con el comando *mount*:

```
mount -t nfs equipo:/carpeta-compartida punto-montaje
```

donde *equipo* es el nombre o dirección IP del ordenador que comparte la carpeta (servidor), *carpeta-compartida* es la ruta completa de la carpeta compartida y *punto-montaje* es la ruta completa donde se va a montar (o la ruta relativa a la carpeta actual). La opción *–t nfs* indica que se va a montar un sistema de archivos de tipo NFS.

Las carpetas montadas a través de NFS se pueden incluir también en el archivo */etc/fstab*, lo que simplifica las operaciones y permite funciones adicionales (montaje por usuarios distintos de *root*, montaje automático en el arranque, etc.).

La operación de montaje de una carpeta NFS también se puede realizar desde las herramientas *YaST2* (seleccionando **Servicios de red** y **Cliente NFS**), *Linuxconf* (seleccionando **Configuración** y **Sistemas de archivos (filesystems)**) o *Webmin* (en la opción **Sistema** y **Sistema de archivos de disco y red**). En ellas, se especifican las mismas opciones que para el comando *mount*.

Hay que tener en cuenta que el demonio de NFS también utiliza los archivos */etc/hosts.allow* y */etc/hosts.deny* que especifican qué equipos pueden acceder a las carpetas de la máquina local y cuáles no. Aunque de estas restricciones se pueden realizar en */etc/exports*, se recomienda establecerlas también en estos archivos por cuestiones de seguridad.

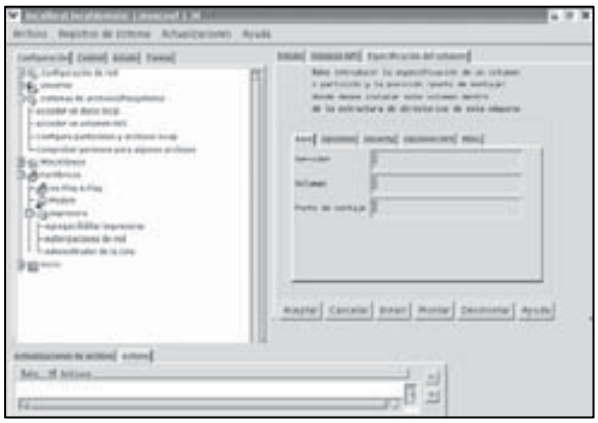


Figura A.13. Manejo de sistemas de archivos NFS en Linuxconf

Los problemas más comunes que se pueden producir durante el acceso a una carpeta compartida por NFS son:

- **No se puede montar la carpeta compartida**. Esta circunstancia puede ser notificada de varias formas:

  - El comando devuelve "Permiso denegado". En este caso, hay que comprobar que la carpeta está compartida (se ha ejecutado el comando *exportfs -ra*) y que el equipo, desde donde se realiza el montaje, tiene permiso para ello (se puede consultar también el archivo */proc/fs/nfs/exports*). También puede ocurrir que se haya compartido una carpeta a la vez que se ha compartido su carpeta hija (una situación que no está permitida). Asimismo, este problema puede ser debido a que existe un encaminador entre el equipo cliente y el servidor que está filtrando algunos mensajes NFS.

  - El comando devuelve "Tiempo de espera agotado" o "Programa no registrado". En este caso, el problema puede estar en que algún proceso demonio no está en ejecución o no puede comunicarse con el cliente. Para comprobar esto, se puede ejecutar el comando *rpcinfo –p* en el servidor y *rpcinfo –p IP_servidor* desde el cliente (donde *IP_servidor* es la dirección IP del equipo servidor). También puede ocurrir que los archivos */etc/hosts.allow* y */etc/hosts.deny* no permitan la conexión NFS del equipo cliente, por lo que también hay que comprobarlos.

  - El comando devuelve "No hay ruta al host". Esto quiere decir que existe algún problema con la configuración de red del equipo cliente o del servidor.

- **No es visible el contenido de la carpeta compartida que se ha montado**. En ese caso, lo primero que hay que comprobar es si realmente se ha montado (con el comando *mount* o editando el archivo */proc/mounts*). En caso afirmativo, hay que comprobar si se ha montado otra unidad o carpeta en el mismo punto de montaje.

- **No existen suficientes permisos para acceder a la carpeta montada**. Esta situación puede ser causada porque no se han establecido correctamente las opciones para compartir la carpeta o porque existe algún problema de correspondencia entre el usuario del equipo cliente y el usuario del equipo servidor.

- **Durante la transferencia de archivos grandes, NFS termina inesperadamente antes de completar la operación**. Este problema es debido probablemente a que se está utilizando un núcleo de Linux

en la versión 2.2, por lo que se recomienda actualizarlo a la versión 2.4.

El sistema de archivos NFS resulta muy flexible, ya que se puede utilizar también como medio para instalar paquetes o un sistema completo de forma remota (por ejemplo, cuando el equipo no dispone de unidad de CD-ROM).

COMPARTIR ARCHIVOS EN UNA RED MICROSOFT

Si se desea acceder a los archivos de una máquina Linux desde una estación que tiene instalado un Windows o al revés, se puede hacer de dos formas:

- ☑ Utilizando el programa de transferencia de archivos FTP y accediendo a la máquina remota como usuario registrado. También se pueden utilizar otros protocolos más seguros, como *scp* (que funciona sobre *ssh*).

- ☑ Utilizando el programa **Samba** para compartir archivos. Este programa permite que Linux pueda acceder a carpetas compartidas de equipos Windows o, incluso, comportarse como un servidor de archivos e impresoras, utilizando los protocolos NetBIOS y SMB de la red Microsoft para comunicarse.

Para que Linux pueda trabajar con *Samba*, es necesario realizar un paso previo de instalación y configuración del servicio. En primer lugar, hay que asegurarse de que la versión del núcleo de Linux que se está utilizando tenga soporte para el sistema de archivos de *Samba* [en las opciones de compilación del núcleo aparecerá como **SMB file system support (to mount Windows shares etc.)**]. En caso de que el núcleo no soporte Samba, cuando se vaya a utilizarlo, se obtendrá mensajes como *fs type smbfs not supported by kernel* (*El sistema de archivos de Samba no está soportado por el núcleo*). En segundo lugar, se deberán instalar los paquetes de *Samba*:

- ☞ **samba**. Paquete que contiene todos los programas, herramientas y protocolos para que Linux se comporte como un servidor de archivos Windows. Gracias a este paquete, cualquier equipo Microsoft Windows o Linux (que tenga *samba-client* instalado) podrá acceder a los archivos y carpetas compartidas.

- ☞ **samba-client**. Paquete que incluye todos los programas necesarios para que el equipo Linux pueda acceder a los recursos compartidos de otro equipo Microsoft Windows o Linux (que haya compartido con *samba*).

Los pasos que se deberán seguir para que un equipo Linux pueda compartir recursos a través de la red Microsoft (como si se tratara de un equipo Windows más) son los siguientes (teniendo en cuenta que ya se han realizado los pasos previos):

1. Buscar el archivo */etc/services* para que incluya las siguientes líneas (que normalmente ya se incluyen por defecto en los archivos instalados):

```
netbios-ns137/tcp  #Servicio de nombres NetBIOS
netbios-ns137/udp
netbios-dgm137/tcp  #Servicio de datagramas NetBIOS
netbios-dgm137/udp
netbios-ssn137/tcp  #Servicio de sesión NetBIOS
netbios-ssn137/udp
```

2. Hay que indicar a Linux que inicie automáticamente el servidor *Samba* al arrancar el sistema a través de algún programa editor de niveles de ejecución. Al iniciar Samba, se ponen en marcha dos demonios: *smbd*, encargado de compartir archivos e impresoras y de la autenticación de los usuarios, y *nmbd*, que realiza la tarea de enviar información de difusión a la red para que el resto de equipos Windows pueda ver a Linux en el *Entorno de Red*. El servidor *Samba* también se puede iniciar y parar manualmente mediante los siguientes comandos[3]:

```
$ /etc/rd.d/init.d/rcsmb start
$ /etc/rd.d/init.d/rcsmb stop
```

3. Cuando se instala *Samba*, se copian al sistema varios archivos, el más importante de ellos es */etc/samba/smb.conf* (también puede encontrarse en */etc*) para su configuración. Un ejemplo de este archivo, con los comentarios para su aclaración, puede ser el siguiente:

```
; Ejemplo de archivo /etc/smb.conf
; Este archivo esta dividido en varias secciones
; que se detallan a continuación.

; Parámetros globales:
[global]
guest account=nobody ;no hay usuario invitado
```

[3] En versiones anteriores de Linux se utilizaban los comandos *smb start* y *smb stop*.

```
load printers=yes
lock directory=/var/lock/samba
printing=bsd
printcap names=/etc/printcap
security=user ;nivel de seguridad de samba
share modes=yes
netbios name=linux ;nombre NetBIOS del equipo
workgroup=migrupo ;grupo de trabajo o dominio

; Para compartir todas las impresoras:
[printers]
comment=todas las impresoras
browseable=no ;solo para usuarios autorizados
create mode=0700 ;permisos utilizados para los
                 ;archivos creados en el spool
path=/var/spool/samba ;carpeta de spool
printable=yes
public=no
writable=no
```

4. El archivo */etc/samba/smb.conf* está dividido en varias secciones, cada una de ellas utilizada para compartir un recurso. Existe también una sección especial denominada *[global]* que contiene todos los parámetros de configuración global de *Samba*. Los parámetros más importantes son:

   - **netbios name**. Es el nombre NetBIOS que va a tener el equipo Linux en la red Microsoft.

   - **workgroup**. Es el grupo de trabajo o dominio al que va a pertenecer el equipo Linux.

   - **security**. Establece el mecanismo que se va a utilizar para autentificar a los usuarios que se conecten a los recursos compartidos del equipo Linux. Este mecanismo puede ser:

     ☑ ***security=share***. Cada elemento compartido tiene una contraseña, de forma que cualquier usuario conectado desde cualquier equipo puede acceder al recurso con sólo poner la contraseña.

- ☑ ***security=user***. El servidor de *Samba* debe tener una lista con los usuarios que tienen derecho de acceso al recurso. El nombre de usuario se especifica con el nombre del equipo Windows y este mismo deberá aparecer registrado con el mismo nombre en Linux (con el comando *useradd* o las herramientas *linuxconf* o *YaST* y en *Samba*, con el comando *smbpasswd*).

- ☑ ***security=server***. Hay otro equipo que se encarga de autenticar a los usuarios.

- **encrypt passwords**. Indica si Linux debe manejar contraseñas cifradas de los usuarios. Se deberá establecer al valor *yes* cuando se espera que Linux vaya a recibir contraseñas cifradas en las conexiones de los equipos cliente Windows que las utilizan en las versiones 9x, NT SP3, 2000 y XP. Si se establece este valor, hay que utilizar el comando *smbpasswd* para crear las contraseñas cifradas en Linux al estilo Windows.

5. Lo siguiente es crear una sección en el archivo */etc/samba/smb.conf* para compartir una carpeta u otro recurso. Esta sección deberá titularse entre corchetes [] como el nombre del recurso que va a estar accesible en la red Microsoft e indicar una serie de parámetros:

   - **browseable**. Indica si el recurso compartido va a aparecer en las ventanas de exploración de la red (*yes*) o no va a aparecer (*no*).

   - **comment**. Se puede utilizar para dar una descripción del recurso al cliente que quiere acceder a él.

   - **create mask**. Se utiliza para establecer qué permisos Linux se van a aplicar cuando el cliente cree un archivo o carpeta dentro de ese recurso compartido.

   - **guest ok**. Se utiliza para indicar si el recurso está accesible para todo el mundo (*yes*) o solamente para usuarios registrados con nombre y contraseña (*no*).

   - **path**. En caso de que el recurso a compartir sea una carpeta, se trata de la ruta local del equipo Linux donde se encuentre.

   - **printable**. Se utiliza para indicar si el recurso compartido es una impresora (se deberá establecer a los valores *yes* o *no*).

- **read only**. Indica si el recurso es de sólo lectura (*yes*) o de lectura-escritura (*no*). El parámetro contrario es **writeable**. Si una carpeta se comparte con acceso de escritura, hay que activar en ella el permiso *salvar texto* (*t*) o, en caso contrario, no se podrá escribir desde un equipo remoto.

- **valid users**. Indica los nombres de los usuarios que están autorizados para acceder al recurso compartido. Cada nombre deberá separarse con espacios.

6. Una vez modificado el archivo */etc/samba/smb.conf*, no es necesario reiniciar el servidor *Samba*, ya que el proceso demonio *smbd* lee la configuración de este archivo cada pocos minutos. En ese momento, el recurso ya está disponible para su uso por los clientes.

Los problemas que pueden surgir a la hora de configurar una carpeta compartida en un equipo Linux que funciona como servidor *Samba* pueden deberse a:

- **Errores de sintaxis en el archivo */etc/samba/smb.conf***. Para encontrarlos se puede utilizar el comando de comprobación de sintaxis *testparm /etc/samba/smb.conf*.

- **Problemas de configuración o conectividad de la red**. Hay que asegurarse de que los dos equipos (tanto el cliente como el servidor) tienen conexión a través de la red.

- **Demonios de Samba inactivos**. Puede ocurrir que los problemas sean debidos a que los procesos demonio de *Samba* (*smbd* y *nmbd*) no se encuentran en ejecución.

- **Problemas de resolución de nombres NetBIOS**. También es necesario asegurarse de que se realiza correctamente la resolución de nombres NetBIOS. Para ello, se puede utilizar el comando *nmblookup* que obtiene un nombre a partir de una dirección IP o al revés.

Por su parte, si queremos que un equipo Linux pueda acceder a un recurso compartido a través de la red Microsoft, hay que asegurarse que el núcleo tiene soporte para *Samba* y que el paquete *samba-client* se encuentra instalado. Para acceder a las carpetas compartidas se puede utilizar el comando:

```
smbclient //servidor/carpeta contraseña
```

Este comando es el más simplificado, aunque también se pueden incluir varias opciones: *-U usuario*, que especifica el nombre de usuario con el que se va a conectar al recurso; *-W grupo*, que especifica el grupo de trabajo (hay que indicarlo en caso de producirse problemas al intentar conectar con el recurso) y *-N*, que suprime la petición de contraseña cuando ésta está vacía (es equivalente a poner dobles comillas como contraseña). Una vez ejecutado ese comando, la carpeta estará disponible para su acceso. Para realizar operaciones sobre éste, se utiliza una interfaz muy parecida al comando FTP, por lo que también se utilizan las mismas instrucciones (véase la tabla A.1 donde aparecen explicados estos comandos).

También se puede utilizar el comando *mount* que permite montar la carpeta compartida en el sistema de archivos local. Su sintaxis es la siguiente:

```
mount -t smbfs //servidor/carpeta carpeta-montaje
```

Las opciones que acepta el comando *smbclient* también pueden ser especificadas en el comando *mount* utilizando la opción *–o* que se indica después del tipo de sistema de archivos (*smbfs*). La opción *–U* es ahora *username=*, la opción *–W* es *workgroup=* y la contraseña se especifica con *password=*. Por ejemplo:

```
mount -t smbfs -o username=usr1 //serv/carpeta /mnt/win
```

Tabla A.1. Comandos para el manejo de archivos y carpetas del programa smbclient

Comando	Descripción
! [*programa*]	Ejecuta un *shell* o un programa del sistema operativo local.
cd [*carpeta*]	Muestra la carpeta actual en el equipo remoto o la cambia a la especificada.
del *patrón*	Elimina los archivos del equipo remoto que coinciden con el patrón especificado.
dir *patrón*	Muestra los archivos de la carpeta actual del equipo remoto que coinciden con el patrón especificado. Es equivalente al comando *ls*.
exit	Finaliza la conexión con el recurso. Es equivalente al comando *quit*.
get *ar_r ar_l*	Obtiene el archivo *ar_r* del equipo remoto y lo guarda en el equipo local con el nombre *ar_l*.
help [*comando*]	Muestra información sobre todos los comandos o el comando especificado. Puede utilizarse también *?*.
lcd [*carpeta*]	Muestra la carpeta actual en el equipo local o la cambia a la especificada.

Comando	Descripción
lowercase	Establece la conversión a minúsculas de los nombres de los archivos obtenidos con los comandos *get* y *mget*.
Mask *patrón*	Los archivos que se copiarán en una operación recursiva serán aquéllos que coincidan con el patrón especificado.
md *carpeta*	Crea una nueva carpeta que cuelga de la actual en el equipo remoto. Es equivalente al comando *mkdir*.
mget *patrón*	Copia todos los archivos que coinciden con el patrón especificado desde el equipo remoto al local.
mput *patrón*	Copia todos los archivos que coinciden con el patrón especificado desde el equipo local al remoto.
print *archivo*	Imprime el archivo en la impresora del equipo remoto.
printmode *modo*	Establece el modo de impresión: *graphics* para imprimir archivos gráficos y *text* para archivos de texto.
prompt	Establece la confirmación en las operaciones de copia.
put *ar_l ar_r*	Copia el archivo *ar_l* del equipo local en el equipo remoto con el nombre *ar_r*.
rd *carpeta*	Elimina la carpeta especificada en el equipo remoto. Es equivalente a *rmdir*.
recurse	Establece la recursión en las operaciones de copia.
rm *patrón*	Elimina todos los archivos que coinciden con el patrón especificado en la carpeta actual.
setmode *atrib*	Establece los atributos de los archivos copiados.
Queue	Muestra el estado de la cola de la impresora remota.

Hay que tener en cuenta que la forma en la que se accede desde Linux a una carpeta compartida en Windows 9x y Windows NT/2000/XP es ligeramente distinta. En el primer caso, el sistema no autentifica al usuario que se conecta (solamente solicita una contraseña si es que se ha establecido una), mientras que en el segundo caso siempre se autentifica al usuario que desea acceder al recurso (independientemente de si el equipo pertenece a un dominio o no). Por lo tanto, para evitar problemas, se recomienda que cuando se desee montar una carpeta compartida de Windows NT/2000/XP se incluyan las opciones para especificar un nombre de usuario, su contraseña y el nombre del grupo de trabajo o del dominio al que pertenece. No hay que olvidar que el usuario especificado deberá haber sido creado en Windows. Estas opciones se establecen con el modificador *–o* de *mount* o *smbmount*. Por ejemplo:

```
$ mount -t smbfs -o username=usuario,password=contraseña,
workgroup=grupo //equipo/carpeta /mnt/samba

$smbmount //equipo/carpeta /mnt/samba -o username=usuario
password=contraseña workgroup=grupo
```

Algunos problemas que pueden surgir en el acceso de cliente son:

- **Problemas con el uso de contraseñas cifradas**. Si se utiliza una versión de Windows 95 o Windows NT que no tiene instalado el *Service Pack 3*, deberemos indicar a Linux que no utilice contraseñas cifradas. Para configurar las contraseñas no cifradas en Windows hay que establecer al valor "1" la clave de registro *EnablePlainTextPassword*.

- **Problemas con Microsoft Windows XP Professional**. Se pueden encontrar varios problemas de acceso como cliente en Linux:

  - Si aparece un error indicando que la contraseña no es correcta, se deberá asegurar que la hemos introducido correctamente. De ser así, entonces se deberá utilizar el **Editor de Políticas de Grupo de Windows** (*GPEDIT.MSC*) y deshabilitar las siguientes opciones de **Local Computer Policy**, **Computer Configuration**, **Windows Settings**, **Security Settings**, **Local Policies** y **Security Options**:

    Domain member: Digitally encrypt or sign secure channel data
    Domain member: Digitally sign secure channel data (when possible)

  - Si aparece el error de sistema 53, es que se ha desactivado el uso de NetBIOS sobre TCP/IP en Windows. Para solucionarlo hay que instalar en Windows XP el *Service Pack 1*.

CONFIGURACIÓN DE UN SERVIDOR DHCP

La configuración de un servidor DHCP resulta bastante sencilla en Linux, aunque hay que tener en cuenta que éste no puede asignar direcciones IP a sí mismo (por lo que deberá tener una dirección IP fija o asignada por otro servidor DHCP). Además, es necesario que el núcleo que se utilice tenga soporte para enviar paquetes de difusión (recuerde 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,* el comando *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.

A continuación, hay que instalar el paquete *rpm* que contiene el proceso servidor DHCP y todos los archivos de configuración necesarios (normalmente, se suele llamar *dhcp-server*).

Seguidamente, deberá añadir una dirección IP en la tabla de encaminamiento del equipo local 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). En primer lugar, se deberá comprobar si esa entrada existe mediante el comando *route*. En caso de que exista ya, deberá aparecer una entrada con la dirección 255.255.255.255 dentro de la columna *Destination*. Si no aparece, habrá que incluirla con el siguiente comando ejecutado como usuario *root*:

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

Si el comando anterior devuelve algún error, habrá 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* el comando:

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

Una vez realizadas estas operaciones, el equipo Linux ya estará preparado para funcionar como servidor DHCP. Lo único que faltará será configurar adecuadamente este servicio. Para ello, se utilizará el archivo de configuración */etc/dhcpd.conf* que está formado por 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 indiquen aquí se aplicarán a todas las subredes que se definan dentro de ella.

- ✓ ***subset***. Se utiliza para definir una subred y puede estar declarada dentro o fuera de la declaración de una red.

- ✓ ***range***. Especifica el rango de direcciones que es asignado a los equipos clientes DHCP que lo soliciten. Puede aparecer más de una declaración de este tipo siempre y cuando 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.

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*, el servidor DHCP asignará direcciones IP a equipos desconocidos; si se especifica *deny unknown-clients*, no se asignarán.

- ✓ **bootp**. Especifica si se van a admitir peticiones de tipo BOOTP, que por defecto sí 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:

- ✓ **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 que contiene el archivo especificado en *filename* (indicado con su nombre o dirección IP).

- ✓ **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 deberán 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 tiempo.

  - **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.

Una vez configurado el servidor DHCP, habrá que iniciar el proceso demonio que lo gestiona que, normalmente, se suele llamar **dhcpd** o **dhcp-server**. Para ello, se pueden utilizar las herramientas del entorno gráfico *YaST2* (opción **Sistema** y **Editor de niveles de ejecución**), *Panel de control de Red Hat* (**Configuración de servicios** o *redhat-config-services*), *Linuxconf* (opción **Configuración** y **Servicios misceláneos**) o *Webmin* (opción **Sistema** y **Configuración Init de SysV**). Para iniciar el servidor DHCP a través de comandos hay que ejecutar como *root*:

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

También se puede usar el siguiente comando:

```
root@linux:~# /usr/sbin/dhcpd &
```

El proceso demonio del servidor DHCP no se iniciará e indicará un mensaje de error en caso de que el archivo de configuración */etc/dhcpd.conf* tenga algún error. Es posible comprobar si el servidor DHCP está funcionando correctamente mediante este comando:

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

O también se puede utilizar este otro:

```
root@linux:~# /usr/sbin/dhcpd -d -f
```

El archivo */var/state/dhcp/dhcpd.leases* 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.

Finalmente, se pueden utilizar los comandos *IPCONFIG* (en Windows) o *ifconfig* (en Linux) para consultar las direcciones asignadas en las estaciones cliente DHCP, o este comando:

```
$ arp -an
```

CONFIGURACIÓN DE UN SERVIDOR DNS

La traducción de direcciones de dominio a direcciones IP en un equipo Linux la realiza el paquete **BIND** (**Berkeley Internet Name Domain**, ***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.

Existen varias versiones del paquete BIND. Actualmente, se incluyen las versiones 8.x y 9.x con las últimas distribuciones de Linux. Si se dispone de una configuración de BIND anterior (4.x), es posible ejecutar un programa *shell-script* que actualice todos los archivos de configuración a las nuevas versiones, llamado */src/bin/named/named-bootconf*. Aquí nos centraremos en la versión 8.1 de BIND.

El inicio del demonio *named* se realiza de forma automática estableciendo el valor *yes* del parámetro *START_NAMED* en el archivo */etc/rc.config* o ejecutando el siguiente comando como *root*:

```
$ rcnamed start
```

Otros modificadores de este comando son *status*, para comprobar el estado del demonio; *reload*, para reiniciar el demonio cuando se modifican sus archivos de configuración y *stop*, para pararlo.

Hay dos opciones de configuración del servidor DNS en Linux:

- **Como caché de nombres exclusivamente**. El demonio *named* recibe las solicitudes y busca en la caché las correspondencias. Si no están, enviará 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 funcionará como una caché de nombres. La definición de las zonas deberá 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 */etc/named.conf* (en las versiones 4.x de BIND era */etc/named.boot*). Se dice por defecto ya que puede utilizarse otro nombre y localización distintos (utilizando el modificador *-b* o *-c* del comando *named*). Existen otros archivos de configuración adicionales que se verán a continuación.

El archivo */etc/named.conf* está formado básicamente por secciones acabadas en punto y coma ";". Éstas pueden aparecer más de una vez dentro de él (excepto las secciones *logging* y *options*). La especificación completa de los parámetros de este archivo no se incluye en este libro por cuestiones de espacio; podrá encontrarla introduciendo la orden *man named.conf* en la línea de comandos de la ventana del terminal o consultando los archivos de ejemplo que se incluyen con el paquete y que están situados en la carpeta */usr/share/doc/packages/bind8/*. Las secciones en que está dividido *named.conf* son:

- *logging*. Especifica qué mensajes notificará el servidor y a dónde los va a enviar.

- *options*. Controla la configuración global del servidor. Algunas opciones importantes que pueden establecerse también a zonas específicas son:

  - *directory*. Directorio de trabajo del servidor.

  - *recursion* ("*yes*"/"*no*"). Indica si las peticiones de resolución de direcciones son recursivas (es decir, se enviarán de unos servidores a otros hasta que se resuelva la dirección).

  - *allow-query*. Especifica las direcciones IP de servidores DNS que pueden solicitar una consulta de dirección a éste.

  - *allow-transfer*. Especifica las direcciones IP de servidores DNS que pueden recibir una *transferencia de zona* de éste.

  - *blackhole*. Especifica las direcciones IP de equipos que pueden enviar consultas y a las que el servidor no contestará.

  - *query-source*. Indica las direcciones IP y puertos de otros servidores de nombres que consultará en caso de no conocer la dirección a resolver.

  - *cleaning-interval*. Especifica el intervalo de tiempo en el que las correspondencias obtenidas van a permanecer en la caché del servidor antes de ser eliminadas. Este parámetro tiene un valor por defecto de 60 minutos.

  - *forward*. Se establece al valor *first* para indicar que primero se consultarán los servidores de la lista *forwarders* y, después, la buscará por sí mismo si no obtiene respuesta; o al valor *only*, para consultar solamente los especificados en *forwarders*.

- *forwarders*. Especifica las direcciones IP de servidores DNS a los que enviará consultas para resolver.

- *notify*. Indica si el servidor notifica a otros servidores DNS que hay cambios en algunos nombres de equipos de la zona. Este mensaje permite a los servidores DNS realizar una transferencia de zona para actualizar sus correspondencias de inmediato.

❍ *zone*. Define una zona (no se utiliza esta sección si el servidor se va a configurar como caché de nombres exclusivamente). Los parámetros principales son: nombre de zona, tipo de dominio (se usa *in* para especificar un dominio de Internet) y otros parámetros adicionales. Entre esos parámetros hay que destacar *file*, que se refiere al archivo donde se guardará la información de la zona y *type*, que especifica el tipo de zona a definir. Existen varios tipos de zonas:

- *master*. El servidor tiene una copia maestra de las correspondencias DNS de la zona. Pueden especificarse, entre otras, las opciones *allow-query*, *allow-transfer* y *file* (archivo donde están almacenados los registros de recursos de la zona).

- *slave*. El servidor tiene una copia de todas las correspondencias DNS de una zona. Pueden especificarse, entre otras, las opciones *allow-query*, *allow-transfer*, *transfer-source* (dirección IP de los servidores DNS que pueden enviar a éste una transferencia de zona), *masters* (especifica las direcciones IP de los servidores DNS maestros desde donde obtendrá copias de las correspondencias) y *file* (archivo donde está almacenada una copia de la información procedente de una transferencia de zona).

- *stub*. Se trata de un servidor esclavo que sólo copia correspondencias de un servidor maestro, no de una zona entera. Pueden especificarse, entre otras, las opciones *allow-query*, *allow-transfer*, *transfer-source* (dirección IP de los servidores DNS que pueden enviar una transferencia de zona a éste), *masters* (especifica las direcciones IP de los servidores DNS maestros desde donde obtendrá copias de las correspondencias) y *file* (archivo donde está almacenada una copia de la información procedente de una transferencia de zona).

- *forward*. Se trata de un servidor que redirige las peticiones a otros servidores DNS. Pueden especificarse las opciones *forwarders* y *forward* para esta zona (véase la lista de opciones que aparece más arriba donde se explican estas dos).

- *hint*. Corresponde a un servidor que posee una lista de direcciones de servidores de nombres raíz. Puede especificarse el parámetro *file* donde se guardará la lista de servidores raíz en forma de registros de recursos. Es necesario que exista, al menos, una entrada de este tipo especificando el dominio raíz "." para poder disponer de direcciones de servidores DNS externos a nuestra red local.

- *acl*. Crea listas de control de acceso donde se especifica una lista de direcciones IP autorizadas para la consulta al servidor. Existen varias listas de control de acceso predefinidas:

  - *any*. Cualquier equipo.
  - *none*. Ningún equipo.
  - *localhost*. Sólo el equipo local.
  - *localnets*. Sólo los equipos de la misma red.

- *key*. Define una clave de autenticación y un identificador asociado.

- *trusted-keys*. Define claves de seguridad de tipo DNSSEC.

- *server*. Establece ciertas opciones de configuración para servidores remotos, identificados por su dirección IP. Éstas son:

  - *bogus*. Indica que ese servidor envía resoluciones incorrectas o defectuosas. Esta opción impide que el servidor envíe consultas a aquél.
  - *transfer-format*. Indica cuál es el formato de las peticiones devueltas por el servidor (*one-answer* para indicar que devolverá una sola respuesta y *many-answers* para indicar que devolverá varias respuestas empaquetadas). Solamente versiones posteriores a la 4.9.5 de BIND reconocen varias respuestas empaquetadas.
  - *keys*. Especifica un identificador de clave que se utilizará para realizar la transacción de información con el servidor remoto.

- *controls*. Declara canales de control para su uso por la utilidad *ndc*, de forma que el servidor DNS se puede administrar de forma remota.

- *include*. Se utiliza para incluir el archivo especificado (entre comillas dobles) en el punto donde aparece esta sentencia. No se puede utilizar dentro de las sentencias vistas anteriormente.

Los archivos que guardan la información de la zona se llaman **archivos de zona** o *archivos maestros*. Estos archivos son manejados por el demonio *named* y están formados por varias directivas más una lista de entradas de registros de recursos (en filas) que poseen varios campos. Las directivas pueden ser:

- *$ORIGIN*. Se utiliza para definir el dominio por defecto de todos los nombres del archivo donde no está especificado.

- *$INCLUDE*. Se utiliza para incluir otro archivo en el punto donde se especifica.

- *$TTL*. Establece el tiempo de vida por defecto de los registros en la caché del servidor.

- *$GENERATE*. Se utiliza para crear registros de recursos cuyos nombres se diferencian solamente en números especificados dentro de un rango (por ejemplo, *server1.dominio.es*, *server2.dominio.es*, *server3.dominio.es*, etc.). Esto facilita la creación de registros de recursos.

Cada registro de recurso está formado por los siguientes campos:

- *domain*. Nombre de dominio completo del equipo. El carácter @ indica que el dominio de ese nombre debe tomarse de la directiva *$ORIGIN*.

- *ttl*. Tiempo de vida del registro en la caché del servidor.

- *class*. Clase de registro. Normalmente se toma la clase de la zona donde se encuentra.

- *type*. Tipo de registro.

- *rdata*. Valor del registro. Depende del tipo especificado.

- *comment*. Comentario aclaratorio.

En los archivos de configuración de zonas hay que incluir también el dominio reservado *in-addr.arpa* que se utiliza para resolver las correspondencias inversas. Delante de este dominio deberá aparecer la dirección IP de red asociada

con los *bytes* escritos en orden inverso y sin los *bytes* reservados para número de estación.

Para comprobar el correcto funcionamiento del servidor DNS, se puede utilizar también el comando *nslookup*, que está implementado en Linux (también se puede ejecutar desde un equipo Windows).

Una vez que se han establecido los archivos de configuración de zona, hay que comprobar si todo funciona correctamente. Una forma sencilla consiste en utilizar el comando de Linux **nslookup**, que realiza consultas a los servidores DNS, tanto directas como inversas. Hay que tener en cuenta que este comando funciona del lado del cliente, por lo que el equipo deberá tener establecida su propia dirección IP para resolver direcciones.

Una vez introducido el comando *nslookup*, aparecerá una línea en la que se puede especificar un nombre o una dirección IP. En el primer caso, devolverá la dirección IP del equipo y en el segundo, devolverá el nombre asociado. En caso de que aparezca algún mensaje, como que no se encuentra el servidor o la dirección, quiere decir que los archivos de configuración de las zonas tienen errores de sintaxis. Si el error aparece al iniciar el demonio *named*, el problema de sintaxis está en */etc/named.conf*.

Hay que tener mucho cuidado a la hora de escribir los archivos de configuración de las zonas, ya que simple hecho de omitir un punto, una coma, etc. hace que el servidor DNS no resuelva las direcciones.

SERVIDOR WEB

Linux también puede funcionar como servidor Web, gracias al paquete *apache* que se incluye en las distribuciones. Con esta utilidad se pueden administrar también varios sitios a la vez.

Para iniciar o parar el servidor *apache*, se pueden utilizar, respectivamente, los siguientes comandos:

```
$ rcapache start
$ rcapache stop
```

El servicio puede configurarse también para que se inicie automáticamente cuando se arranque el equipo, modificando el valor del parámetro *START_HTTPD* del fichero */etc/rc.config*.

El paquete *apache* tiene establecida la configuración por defecto, de forma que, una vez instalado e iniciado, ya puede ser utilizado por los usuarios. Las páginas se guardan en la carpeta */urs/local/httpd/htdocs* y se crea una página de inicio en ella llamada *index.html*.

Todos los archivos de configuración del servidor *apache* se encuentran en la carpeta */etc/httpd* (el más importante de todos ellos es *httpd.conf*). Debido a la cantidad y extensión de estos archivos, no se incluye información adicional sobre ellos, que puede consultarse directamente en ellos o en las páginas del manual (*man*).

ÍNDICE ALFABÉTICO

D

E

F

G

R

S

T

U