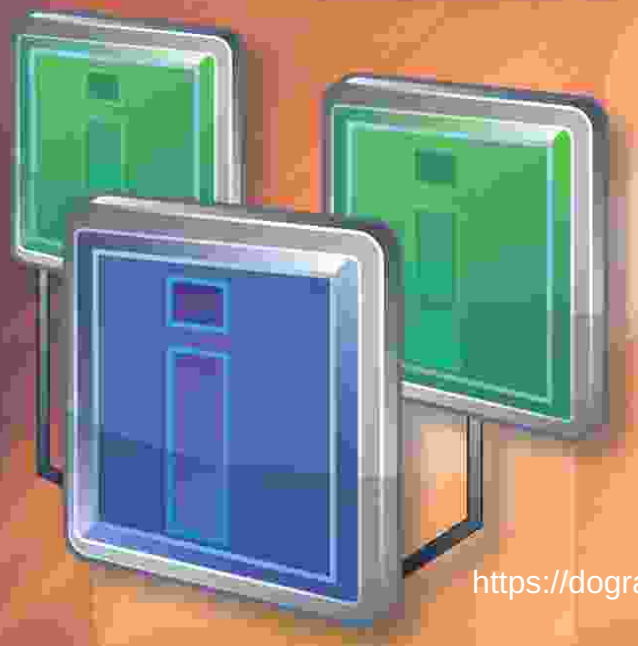
CF GRADO SUPERIOR

CICLOS FORMATIVOS

R.D. 1538/2006

Sistemas Informáticos y Redes Locales



JUAN CARLOS MORENO PÉREZ
MANUEL SANTOS GONZÁLEZ

Ra-Ma®

www.ra-ma.es/cf

La
Copiar o Imprimir este libro

https://dogramcode.com/dogramcode_usuarios/login

SISTEMAS INFORMÁTICOS Y REDES LOCALES

ISBN de Edición en Papel: 978-84-9964-159-1

Editado por:
RA-MA, S.A. Editorial y Publicaciones
Calle Jarama, 33, Polígono Industrial IGARSA
28860 PARACUELLOS DE JARAMA, Madrid
Teléfono: 91 658 42 80
Fax: 91 662 81 39
Correo electrónico: editorial@ra-ma.com
Internet: www.ra-ma.es y www.ra-ma.com

Maquetación: Gustavo San Román Borrueco
Diseño Portada: Antonio García Tomé

ISBN: 978-84-9964-368-7

E-Book desarrollado en España en Septiembre de 2014

Sistemas Informáticos y Redes Locales

JUAN CARLOS MORENO PÉREZ
MANUEL SANTOS GONZÁLEZ

Dedico este libro a mis padres, a mi hermana Mayka y, especialmente, a mi mujer María Amparo y a mi hija Emma.

Juan Carlos.

A toda mi familia.

Manuel.

Especial agradecimiento a: Juan Serrano, Andrés Rosique, Pedro Ruiz, ndevilTV, Intel, elevate_printing, Kylehase, Rafa Espada, Juan Pablo Olmo, Sylvar, Tim Patterson, Girlgeek0001, Erik Charlton, Laihiu, Animaster, viagallery.com, Lordcolus, Okubax, Saquayo y a toda la demás gente que ha hecho posible este libro.

2.4.4 Educación 71
2.4.5 Productividad y negocios 71
2.4.6 Clientes para servicios de Internet 71
2.4.7 Otras categorías de interés 72

RESUMEN DEL CAPÍTULO 72
EJERCICIOS PROPUESTOS 73
TEST DE CONOCIMIENTOS 73

CAPÍTULO 3. MONTAJE Y ENSAMBLADO DE EQUIPOS INFORMÁTICOS DE TELECOMUNICACIONES 75

3.1 PRECAUCIONES Y ADVERTENCIAS DE SEGURIDAD 76
3.1.1 Lugar de trabajo 76
3.1.2 Precauciones sobre la energía eléctrica 76
3.1.3 Precauciones sobre la energía estática 76
3.1.4 Precauciones en sistemas de refrigeración líquida 77
3.1.5 Precauciones sobre los componentes 77
3.1.6 Precauciones generales 79
3.2 HERRAMIENTAS DE MONTAJE 79
3.2.1 El multímetro o polímetro 82
3.3 FASES DE MONTAJE DE SISTEMAS INFORMÁTICOS 86
3.4 MONTAJE DEL EQUIPO 86
3.4.1 Montaje de la placa base en la caja o chasis 86
3.4.2 Ensamblado del procesador y elementos de refrigeración del mismo 89
3.4.3 Fijación de los módulos de memoria RAM 94
3.4.4 Fijación y conexión de las unidades de disco fijo 96
3.4.5 Fijación y conexión de las unidades ópticas de lectura/escritura 103
3.4.6 Fijación y conexión del resto de adaptadores y componentes 104
3.5 VERIFICACIÓN DEL MONTAJE 108

RESUMEN DEL CAPÍTULO 108
EJERCICIOS PROPUESTOS 109
TEST DE CONOCIMIENTOS 110

CAPÍTULO 4. PUESTA A PUNTO Y CONFIGURACIÓN DE UN SISTEMA INFORMÁTICO 113

4.1 SISTEMAS OPERATIVOS EN LA ACTUALIDAD 114
4.1.1 Plataforma Windows® 115
4.1.2 Plataforma GNU/Linux 116
4.1.3 Plataforma MAC OS 117
4.1.4 Sistemas operativos de dispositivos móviles 117
4.2 INSTALACIÓN DE SISTEMAS OPERATIVOS 121
4.2.1 Pasos en la instalación de un sistema operativo 121
4.2.2 Configuración del dispositivo de arranque en la BIOS 121
4.2.3 Particionamiento del disco duro 123
4.2.4 Ejecución del programa de instalación 123
4.2.5 Elección y configuración del usuario o usuarios que van a administrar el sistema 124
4.2.6 Seleccionar los componentes software a instalar 124
4.2.7 Configurar los parámetros de *networking* 124

4.2.8 Instalar el gestor de arranque y el resto del sistema operativo 124
4.2.9 Actualizaciones de seguridad y demás parches 124
4.2.10 Instalar los *plugins* del navegador 125
4.2.11 Instalar los *drivers* de los dispositivos que se vayan a utilizar 126
4.3 VERIFICACIÓN FINAL DEL EQUIPO 126

RESUMEN DEL CAPÍTULO 127
EJERCICIOS PROPUESTOS 128
TEST DE CONOCIMIENTOS 128

CAPÍTULO 5. CONFIGURACIÓN DE SISTEMAS INFORMÁTICOS 131
5.1 ARQUITECTURA CLIENTE/SERVIDOR 132
5.1.1 ¿Qué es una arquitectura cliente-servidor? 132
5.1.2 Características de la arquitectura cliente-servidor 132
5.1.3 Funciones de los clientes y servidores 133
5.1.4 Arquitecturas *peer-to-peer* o P2P 135
5.2 ADMINISTRACIÓN DE SERVICIOS EN SISTEMAS OPERATIVOS 136
5.2.1 ¿Cómo arranca un equipo? 136
5.2.2 ¿Qué es un servicio? 138
5.2.3 Herramientas de configuración de servicios en Linux 138
5.3 CONFIGURACIÓN DE SISTEMAS OPERATIVOS 140
5.4 ADMINISTRACIÓN DE USUARIOS Y PERMISOS 146
5.4.1 Los usuarios en el sistema 146
5.4.2 Los grupos de usuarios 146
5.4.3 Gestionar usuarios y grupos en Linux 147
5.4.4 Los permisos en Linux 149
5.5 VIRTUALIZACIÓN DE ENTORNOS OPERATIVOS 151

RESUMEN DEL CAPÍTULO 152
EJERCICIOS PROPUESTOS 153
TEST DE CONOCIMIENTOS 153

CAPÍTULO 6. IMPLANTACIÓN DE SOFTWARE 155
6.1 TIPOS DE SOFTWARE 156
6.1.1 Componentes de aplicaciones. Arquitecturas del software 159
6.2 INSTALACIÓN, CONFIGURACIÓN Y ELIMINACIÓN DE APLICACIONES 160
6.2.1 Formas de instalación 160
6.3 PASOS BÁSICOS DE UNA INSTALACIÓN 164
6.4 CONFIGURACIÓN DE APLICACIONES 165
6.5 ELIMINACIÓN DE APLICACIONES 165

RESUMEN DEL CAPÍTULO 166
EJERCICIOS PROPUESTOS 167
TEST DE CONOCIMIENTOS 167

CAPÍTULO 7. INTRODUCCIÓN A LAS REDES DE DATOS 169
7.1 ¿QUÉ ES UNA RED DE DATOS? 170
7.2 ¿QUÉ SERVICIOS NOS OFRECEN LAS REDES DE DATOS? 172

7.3 REDES LAN Y REDES WAN 174
7.3.1 Redes LAN 174
7.3.2 Redes WAN 175
7.4 MODELOS DE DISEÑO DE REDES: OSI Y TCP/IP 177
7.4.1 Justificación del uso de un modelo basado en niveles 177
7.4.2 Transferencia de información en un modelo basado en niveles 178
7.4.3 Modelo OSI 179
7.4.4 El modelo OSI frente a TCP/IP 185
RESUMEN DEL CAPÍTULO 186
EJERCICIOS PROPUESTOS 186
TEST DE CONOCIMIENTOS 187
CAPÍTULO 8. CAPA FÍSICA: MEDIOS DE TRANSMISIÓN 189
8.1 MEDIOS DE TRANSMISIÓN 190
8.1.1 Par trenzado 190
8.1.2 Cable UTP 191
8.1.3 Cable STP 193
8.1.4 Cable coaxial 194
8.1.5 Fibra óptica 195
8.1.6 Medios inalámbricos 199
8.1.7 Uso de los medios de transmisión en las redes de datos 201
8.2 OTRAS CARACTERÍSTICAS DEL NIVEL FÍSICO 202
8.2.1 Señalización y codificación 202
8.2.2 Modos de transmisión 204
8.2.3 Topologías de red 205
8.3 CABLEADO ESTRUCTURADO 208
8.3.1 Estándares de cableado estructurado 208
8.3.2 Principales características 209
8.3.3 Arquitectura y subsistemas 209
8.3.4 Instalación y certificación 213
RESUMEN DEL CAPÍTULO 216
EJERCICIOS PROPUESTOS 216
TEST DE CONOCIMIENTOS 217
CAPÍTULO 9. ETHERNET Y DISPOSITIVOS DE INTERCONEXIÓN 219
9.1 INTRODUCCIÓN 220
9.2 ETHERNET, IEEE 802.3 Y EL MODELO OSI 221
9.3 UN PRIMER CONTACTO PRÁCTICO CON ETHERNET 222
9.4 TARJETAS DE RED 226
9.5 ESPECIFICACIONES DEL NIVEL 2 EN ETHERNET 227
9.5.1 Direccionamiento 227
9.5.2 Formato de trama 229
9.5.3 Control de acceso al medio: CSMA/CD 231
9.5.4 Control de errores en Ethernet 232
9.6 10BASE-T: ETHERNET SOBRE PAR TRENZADO 232

9.7 FAST ETHERNET: ETHERNET A 100 MBPS 235
9.7.1 100BASE-TX 235
9.7.2 100BASE-FX 235
9.7.3 100BASE-T4 236
9.8 MEJORANDO ETHERNET: ETHERNET CONMUTADA Y FULL-DÚPLEX 236
9.9 MÁS VELOCIDAD: GIGABIT ETHERNET Y 10-GIGABIT ETHERNET 238
9.9.1 1000BASE-T 238
9.9.2 1000BASE-X 239
9.9.3 10-Gigabit Ethernet 240
9.10 ASIGNACIÓN DE PINES EN UTP PARA ETHERNET: CABLE DIRECTO Y CRUZADO 241
9.11 INTERCONEXIÓN DE DISPOSITIVOS: EL SWITCH O CONMUTADOR 243
9.11.1 Antecedentes 243
9.11.2 Funcionamiento de un *switch* 244
9.11.3 Puertos 247
9.11.4 *Buffers* 250
9.11.5 Técnicas de conmutación 250
9.11.6 Control de bucles: *Spanning tree* 251
9.11.7 Segmentación de tráfico: VLAN 251
9.11.8 *Power Over Ethernet* (POE) 252
9.11.9 *Switches* configurables 253
RESUMEN DEL CAPÍTULO 256
EJERCICIOS PROPUESTOS 256
TEST DE CONOCIMIENTOS 257

CAPÍTULO 10. TCP/IP 259
10.1 INTRODUCCIÓN 260
10.2 ARQUITECTURA TCP/IP 260
10.3 PROTOCOLO DE RED IP 262
10.3.1 Datagrama IPv4 263
10.3.2 Direccionamiento IPv4 265
10.3.3 Subredes 269
10.3.4 Arquitectura IP 272
10.3.5 Ámbitos en el uso de direcciones IP: públicas y privadas 272
10.3.6 Asignación de direcciones IP privadas 274
10.4 OTROS PROTOCOLOS DE TCP/IP: ARP E ICMP 275
10.4.1 Protocolo ARP 275
10.4.2 Protocolo ICMP 275
10.5 PROTOCOLOS DE TRANSPORTE: TCP Y UDP 277
10.5.1 Protocolo UDP 277
10.5.2 Protocolo TCP 278
10.6 CONFIGURACIÓN DE PARÁMETROS DE RED 281
10.6.1 Asignación automática de parámetros IP: servicio DHCP 282
10.6.2 Obtención de direcciones IP de dominios: servicio DNS 283
10.6.3 Configuración de parámetros IP en Windows® 283
10.6.4 Configuración de parámetros IP en Ubuntu 286
10.6.5 *Firewall* 287

10.7 PROTOCOLOS DEL NIVEL DE APLICACIÓN 290
10.7.1 Servicio de acceso a páginas web 291
10.7.2 Servicio de transferencia de correo electrónico: SMTP 292
10.7.3 Servicio de transferencia de archivos: FTP 293
10.7.4 Servicio de Terminal remoto: *Telnet* y *ssh* 293
10.7.5 Servicio de gestión de red: SNMP 293
10.8 DIRECCIONAMIENTO EN EL NUEVO PROTOCOLO IPV6 294
10.8.1 Tipos de direcciones IPv6 294
RESUMEN DEL CAPÍTULO 298
EJERCICIOS PROPUESTOS 298
TEST DE CONOCIMIENTOS 300
CAPÍTULO 11. REDES LAN INALÁMBRICAS 301
11.1 INTRODUCCIÓN 302
11.2 EL ESTÁNDAR IEEE 802.11 Y LA CERTIFICACIÓN WI-FI 302
11.3 ARQUITECTURA DE UNA RED INALÁMBRICA 304
11.3.1 BSS (*Basic Service Set*) 304
11.3.2 ESS (*Extended Service Set*) 305
11.3.3 Modo *bridge* (puente) 307
11.3.4 Identificador de una red inalámbrica: SSID 308
11.4 CANALES 308
11.5 ALCANCE Y NIVELES DE POTENCIA 310
11.6 DIRECCIONAMIENTO 311
11.7 ACCESO AL MEDIO COMPARTIDO: CSMA/CA 311
11.8 SEGURIDAD 312
11.8.1 WEP 312
11.8.2 WPA 312
11.8.3 WPA2 313
11.8.4 Mecanismos de seguridad complementarios 313
11.9 DISPOSITIVOS INALÁMBRICOS 315
11.9.1 Tarjetas de red inalámbricas 315
11.9.2 Puntos de acceso (AP) 316
11.9.3 Puentes inalámbricos 317
11.9.4 *Router* banda ancha con capacidades inalámbricas 318
11.10 CONFIGURACIÓN DE REDES INALÁMBRICAS 319
11.10.1 Configuración de un punto de acceso 319
11.10.2 Configuración de un dispositivo equipado con conectividad inalámbrica 320
RESUMEN DEL CAPÍTULO 322
EJERCICIOS PROPUESTOS 323
TEST DE CONOCIMIENTOS 323
CAPÍTULO 12. MANTENIMIENTO Y PUESTA EN SERVICIO DE SISTEMAS INFORMÁTICOS 325
12.1 AVERÍAS EN SISTEMAS INFORMÁTICOS 326
12.2 MANTENIMIENTO EN SISTEMAS INFORMÁTICOS 326

12.3 NIVELES DE MANTENIMIENTO 328
12.3.1 Factores que pueden afectar al rendimiento o durabilidad de los componentes de un equipo informático 329
12.3.2 Mantenimiento preventivo en equipos portátiles 332
12.4 HERRAMIENTAS DE ANÁLISIS DEL SISTEMA 333
12.4.1 Monitorización de la placa base 333
12.5 PUESTA EN SERVICIO, ANÁLISIS, DIAGNÓSTICO Y LOCALIZACIÓN DE AVERÍAS 334
12.5.1 Puesta en servicio de la computadora una vez montada 335
12.5.2 Tras el montaje de un equipo tenemos problemas 335
12.5.3 Fallos comunes por componentes 337
12.6 REPARACIONES DE EQUIPOS INFORMÁTICOS 340
12.6.1 Reparaciones en equipos portátiles 341
12.7 CLONACIONES 348
12.7.1 Clonación de particiones y de discos 350
12.7.2 Clonación de particiones 350
12.7.3 Clonación de discos 353
12.8 COPIAS DE SEGURIDAD 356
12.8.1 Qué es una copia de seguridad o *backup* 356
12.8.2 Tipos de copias de seguridad 356
12.8.3 Los 10 consejos de las copias de seguridad 358
12.8.4 Utilidades para hacer copias de seguridad en Linux 358
12.9 PLANES DE PUESTA EN SERVICIO DE SISTEMAS INFORMÁTICOS 362
12.10 RENDIMIENTO Y MONITORIZACIÓN DE SISTEMAS INFORMÁTICOS 363
12.10.1 Rendimiento del sistema: *benchmarking* 363
12.10.2 Herramientas de monitorización y medición de parámetros del sistema 364

RESUMEN DEL CAPÍTULO 365
EJERCICIOS PROPUESTOS 366
TEST DE CONOCIMIENTOS 368

CAPÍTULO 13. MANTENIMIENTO Y PUESTA EN SERVICIO DE REDES LOCALES 371
13.1 DIMENSIONADO DE LA RED 372
13.2 PLANOS Y ESQUEMAS 373
13.3 ETIQUETADO 374
13.4 MATERIALES Y EQUIPAMIENTO 376
13.4.1 Cableado horizontal 376
13.4.2 Tomas de usuario 376
13.4.3 Cableado vertical 377
13.4.4 Cableado de campus 377
13.4.5 Armarios de comunicaciones 377
13.4.6 Alimentación 378
13.4.7 Elementos de distribución 378
13.5 DOCUMENTACIÓN 379
13.6 CERTIFICACIÓN DE LA INSTALACIÓN 380

13.7 DIAGNÓSTICO Y LOCALIZACIÓN DE AVERÍAS 381
13.7.1 El comando *ping* como herramienta de diagnóstico 381
13.7.2 Verificación de la conectividad lógica 385
13.7.3 Verificación de la conectividad física 386
13.7.4 La avería más común: fallo en la conexión a Internet 388
13.8 MONITORIZACIÓN 389
13.8.1 Capturadores de tráfico 389
13.8.2 Escaneadores de puertos 391
13.8.3 Supervisión del tráfico de red: *ntop* 392
13.8.4 Protocolo SNMP 393
13.8.5 Supervisión de redes inalámbricas 395
RESUMEN DEL CAPÍTULO 397
EJERCICIOS PROPUESTOS 397
TEST DE CONOCIMIENTOS 398
ÍNDICE ALFABÉTICO 401

Introducción

A la hora de redactar este libro se ha tenido en cuenta el ámbito en el que se encuadra el mismo, que no es ni más ni menos que la Formación Profesional de grado superior. El libro trabaja el fascinante campo de los **Sistemas Informáticos y Redes Locales**. Actualmente estamos rodeados de los mismos y cada vez dependemos más de ellos.

Cualquier profesional de la informática o las telecomunicaciones trata a diario con conceptos como Android, *smartphone*, *firmware*, WLAN, *motherboard*, cliente/servidor, *switch*, servidor, etc. Y, por tanto, este es un libro que trabaja con estos conceptos de una forma sencilla y actualizada con el objetivo que el alumno pueda integrarse en el mundo laboral de una manera efectiva.

Los autores somos profesores y profesionales de las nuevas tecnologías y hemos querido hacer un libro en el que se combinen los contenidos teóricos (que son fundamentales tanto para la experiencia profesional como para los alumnos que deseen dar el paso de incorporarse a la universidad) con el carácter práctico que siempre tiene que tener la formación profesional. Esperamos que los lectores disfruten tanto con contenidos de este libro como los autores cuando lo escribimos.

1 Equipos informáticos de telecomunicaciones

OBJETIVOS DEL CAPÍTULO

- ✓ Valorar y debatir sobre la importancia de los sistemas informáticos en la actualidad.
- ✓ Identificar y caracterizar los elementos que constituyen los bloques funcionales de un equipo microinformático.
- ✓ Describir el papel de los diferentes elementos físicos y lógicos que constituyen un sistema informático.
- ✓ Analizar la arquitectura general de un equipo y los mecanismos de conexión entre dispositivos.
- ✓ Identificar y caracterizar los distintos componentes que constituyen hoy día físicamente un equipo microinformático.
- ✓ Conocer las distintas alternativas tecnológicas para cada tipo de dispositivo.
- ✓ Clasificar los dispositivos periféricos y sus mecanismos de comunicación.

1.1 ESTRUCTURA FUNCIONAL DE UN SISTEMA INFORMÁTICO

En este apartado se va a estudiar los sistemas informáticos desde el punto de vista funcional. La visión funcional de los sistemas informáticos no ha cambiado en gran medida desde que el gran científico von Newmann los describiese hace muchos años atrás. No obstante, hay que diferenciar la estructura funcional con la física o comercial, las cuales son completamente diferentes. De todas formas, el entender conceptualmente la estructura de un sistema informático y su funcionamiento nos va a ayudar a comprender la forma de trabajar de cualquier sistema informático.

1.1.1 DEFINICIÓN DE UN SISTEMA INFORMÁTICO

Vivimos rodeados de sistemas, formando parte de muchos de ellos. En ocasiones lo hacemos inconscientemente y en otras no (ejemplos como sistemas financieros, sistemas políticos, sistemas sanitarios son claras muestras de los mismos).

En su acepción más general, llamamos **sistema** a *aquel conjunto ordenado de elementos que se relacionan entre sí y contribuyen a un determinado objetivo.*

Es evidente que existen múltiples tipos de sistemas pero para lo que nos ocupa, tomamos como punto de partida la idea de los **sistemas de comunicación** entendidos como *aquel conjunto de elementos que emiten, reciben e interpretan información.*

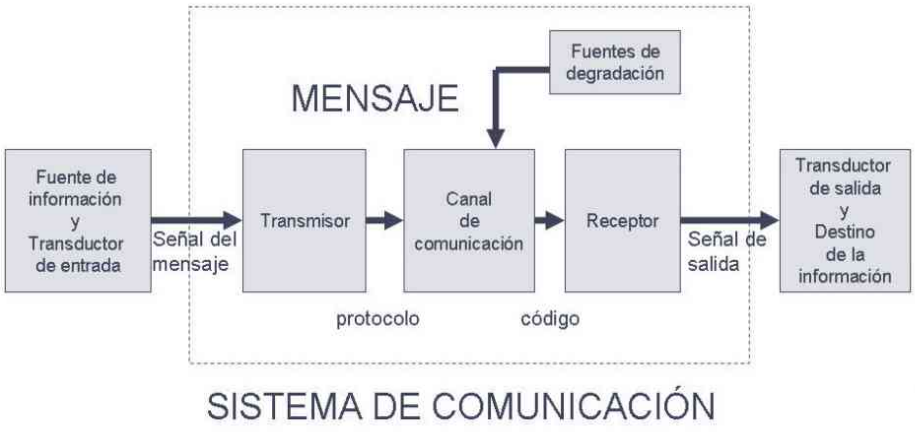


***Figura 1.1**. Esquema sistema de comunicación*

Definición de sistema informático

Un **sistema informático** (**SI**) *es un conjunto de dispositivos, con al menos una CPU o unidad central de proceso, que estarán física y lógicamente conectados entre sí a través de canales, lo que se denomina* **modo local**, *o se comunicarán por medio de diversos dispositivos o medios de transporte, en el llamado* **modo remoto**. Dichos elementos se integran por medio de una serie de componentes lógicos o software con los que puede llegar a interaccionar uno o varios agentes externos, entre ellos el hombre.

El **objetivo** de un sistema informático es el de **dar soporte al procesado**, **almacenamiento**, **entrada y salida de datos** que suelen formar parte de un sistema de información general o específico. Para tal fin es dotado de una serie de recursos que varían en función de la aplicación que se le da al mismo.

Elementos de un sistema informático

Todo SI debe disponer de dos elementos básicos: un **sistema físico o hardware** y un **sistema lógico** o **software**, a los que hay que añadirle un tercero que, sin pertenecer intrínsecamente, no se puede pensar funcionando sin él: los **recursos humanos**.

Tradicionalmente, los elementos que componen un SI son:

- **Hardware**. Formado por aquellos elementos físicos del SI, siendo elementos *hardware* el elemento terminal, los canales y los soportes de la información.
- **Software**. Aquellos elementos del sistema que no tienen naturaleza física y que se usan para el procesamiento de la información.
- **Personal**. Entendido como el conjunto de usuarios finales u operadores del SI.
- **Documentación**. Son todo aquel conjunto de manuales impresos o en formato digital y cualquier otra información descriptiva que explican los procedimientos del sistema informático.

En un SI el software está condicionado por el hardware tanto en su uso como en su evolución.

***Figura 1.2**. Estructura en capas de un sistema informático*

Todo sistema, y por supuesto un SI, se puede contemplar desde dos aspectos: **su descripción física** (cómo es físicamente, analizando los componentes que lo constituyen así como los elementos de interconexión) y su **descripción funcional** (funciones de sus componentes, cómo interactúan unos con otros, reglas o normas de comunicación, etc.).

A lo largo de este capítulo, veremos con más detalle las características funcionales y físicas de un SI entendiendo por:

- **Estructura funcional del SI**. Aquella asociada al soporte físico o hardware que se encarga de estudiar las arquitecturas de organización y funcionamiento de los diversos componentes del mismo. Toma como punto de partida la histórica *Arquitectura de von Neumann*.

- **Estructura física del SI**. También asociada al hardware. En este caso estudiaremos lo que comúnmente se denomina *hardware comercial*. Veremos cómo son físicamente, para qué sirven y qué características tienen los diferentes componentes actuales que componen un PC, integrados a partir de la placa base y recogidos dentro de un chasis, comunicándose con distintos dispositivos de entrada, salida o entrada-salida.

1.1.2 ARQUITECTURA DE VON NEUMANN. ELEMENTOS FUNCIONALES DE UN SI

El elemento central del hardware de un SI es **la UCP** o **Unidad Central de Proceso**, de forma que su arquitectura determina el comportamiento funcional de dicho sistema.

El modelo básico de arquitectura empleada en los computadores digitales fue establecido en 1946 por **John von Neumann**. Su aportación más significativa fue la de construir una computadora con programa almacenado, ya que los computadores existentes hasta entonces trabajaban con programas cableados que se introducían estableciendo manualmente las conexiones entre las distintas unidades.

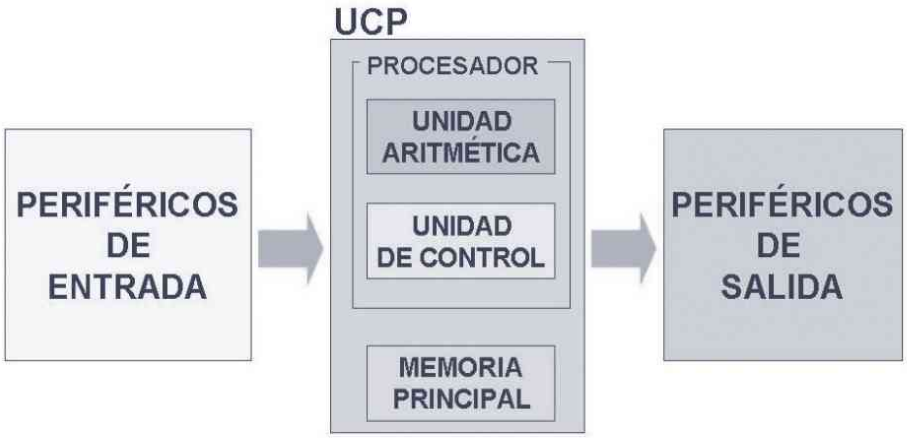


***Figura 1.3**. Estructura funcional de un ordenador*

La idea de von Neumann consistió en conectar permanentemente las unidades de las computadoras, siendo coordinado su funcionamiento por un elemento de control. Esta tecnología sigue estando vigente en la actualidad aunque con pequeñas modificaciones y sigue siendo empleada por la mayoría de los fabricantes.

¿SABÍAS QUE...?

John von Neumann (1903-1957), nacido en Budapest, fue un niño prodigio con gran memoria fotográfica y talento para las matemáticas, pero su padre le prohibió dichos estudios porque pensaba que no era una carrera con la que ganar dinero así que lo engañó y estudiaba química en Berlín, aunque estaba matriculado en Budapest en Matemáticas y sólo iba a los exámenes. En 1930 viaja a EEUU y al comenzar la Segunda Guerra Mundial trabaja para el gobierno americano y viendo las limitaciones del ENIAC y otras máquinas de computación definió un nuevo sistema lógico de computación.

En la imagen anterior observamos la estructura general de un ordenador según la **Arquitectura de von Neumann**. Esta máquina se compone de **cuatro unidades básicas**:

- La **unidad de control** (**UC**), que dispone de un contador de programa (CP) y un registro de instrucción (RI).
- La **unidad aritmético-lógica** (**UAL**), con diversos registros para llevar a cabo operaciones como el registro acumulador (AC) o el registro de estado (RE).
- La **unidad de memoria**, con el registro de palabra (RM) y el registro de dirección (RD).
- La **unidad de entrada-salida**.

Este modelo era capaz de ejecutar una serie de instrucciones elementales que denominó **instrucciones-máquina**, que deben estar almacenadas en la memoria principal con el programa almacenado para poder ser leídas y ejecutadas.

El que se puedan ejecutar diferentes programas hacía que este tipo de máquinas fuesen llamadas de **propósito general**.

Analizando dicha arquitectura observamos como cada elemento tenía una determinada función, era totalmente imprescindible y se comunicaba con otros elementos del sistema para conseguir su objetivo, que no era otro que procesar información y llevar a cabo la tarea para la que se le programó.

La **unidad de control** tenía como función la de leer, una tras otra, las instrucciones-máquina almacenadas en la memoria principal, y generar señales de control necesarias para que toda la máquina funcionase y ejecutase las instrucciones leídas. Para conocer en todo momento la posición de memoria en la que estaba almacenada la siguiente instrucción a ejecutar existía un registro apuntador llamado **contador de programa** que contenía dicha información.

La **unidad aritmético-lógica** se empleaba para llevar a cabo una serie de operaciones elementales como sumas, restas, operaciones lógicas como AND, OR, NOT y otras, e incluso operaciones relacionales. Los datos sobre los que opera esta unidad provienen de la memoria principal y pueden estar almacenados de forma temporal en algunos registros de la propia ALU.

¿SABÍAS QUE...?

En computación juegan un papel fundamental las **operaciones lógicas** o **booleanas** que se implementan mediante dispositivos electrónicos llamados **puertas lógicas**, que son la base de la implementación de los circuitos de conmutación integrados en un chip que trabajan con bits.
Las principales operaciones son:
- AND, donde F = A * B
- OR, donde F = A + B
- NOT, donde F = $\bar{A}$

siendo A y B valores binarios.

La **memoria principal** está formada por un conjunto de celdas de igual tamaño o número de bits que se identifican de forma individual a través de una dirección y sobre las que se podían realizar operaciones de lectura o escritura.

Cada celda suele estar formada por un conjunto de bits, denominándose **punto de memoria**, que son el elemento básico de información y cuyos valores cero o uno se corresponden a estados de tensión diferentes. Las celdas se empleaban para almacenar tanto datos como instrucciones de máquina.

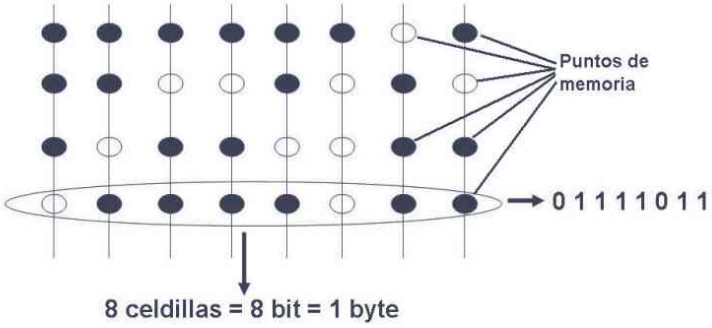


Figura 1.4. *Estructuración de la memoria*

La **unidad de entrada-salida** llevaba a cabo la transferencia de información a través de **canales** asociados a dichas unidades externas que podían estar formadas por **memorias auxiliares o secundarias**, que servían de soporte de almacenamiento de gran capacidad, y otras llamadas **periféricos**, que permitían la comunicación entre el sistema y el medio exterior mediante la carga de datos y programas en la memoria principal o la presentación de resultados, en aquel momento, impresos.

Por último, los *buses* eran *caminos a través de los cuales las instrucciones y los datos circulan entre las distintas unidades del ordenador*.

Teniendo en cuenta que la función principal de un ordenador es ejecutar programas, y que todo este esquema va encaminado a tal fin, para conocer el funcionamiento básico del mismo y cómo interaccionan las distintas unidades entre sí antes hay que dejar claro el concepto de programa.

Un **programa** es un *conjunto de instrucciones que son almacenadas secuencialmente en posiciones o direcciones sucesivas de memoria y que serán ejecutadas una detrás de otra.*

El funcionamiento del ordenador consistirá pues en ir extrayendo sucesivamente instrucciones de la memoria principal, interpretarlas, extraer de memoria los datos empleados en la operación (llamados **operandos**), enviarlos a la unidad que realiza las operaciones y hallar el resultado.

1.2 ESTRUCTURA FÍSICA DE UN SISTEMA INFORMÁTICO

En este apartado vamos a estudiar los componentes del ordenador desde un punto de vista **físico** o lo que algunos han llamado **comercial**, entendiéndolo como la forma en que se pueden percibir y adquirir las distintas piezas que se fabrican y conectan de ese puzle que forma el ordenador.

Los diferentes componentes tienen que cumplir con una serie de configuraciones o **estándares** que deben seguir los diferentes fabricantes de hardware para que sean compatibles entre sí y finalmente se conecten para montar un ordenador con las características que se desee.

Tabla 1.1 Esquema de elementos internos y externos del ordenador

Dispositivos Internos (dentro del chasis)		Dispositivos Externos			
		Periféricos de Entrada	Periféricos de Salida	Periféricos de E/S	Soportes de almacenamiento secundario
Placa base.	CPU, memoria RAM, memoria caché, BIOS, *chipset*, puertos de comunicación, *buses* y ranuras (PCI, PCI-e, EIDE, USB, AGP).	Teclado. Raton. *Joystick*. Escáner. Micrófono. Otros sistemas de reconocimiento óptico. Sensores.	Pantalla. Videoproyector. Impresora. *Plotter*. Altavoces.	Dispositivos de redes (módem, *hub*, *switch*, router, etc.). Impresoras multifuncionales. Pantallas táctiles.	Memorias USB. Discos duros externos. Tarjetas de memoria *flash*.
Unidades de almacenamiento secundario.	Disco(s) duros(s), unidad de disquette, lector/grabador de CD/DVD, lector de tarjetas, etc.				
Tarjetas controladoras.	Tarjeta gráfica, tarjeta de red, controlador SCSI, tarjeta de sonido, tarjeta capturadota de vídeo, sintonizadora de TV, etc.				
Otros componentes auxiliares.	Chasis, fuente de alimentación, sistemas de refrigeración, etc.				

A continuación estudiaremos cada uno de estos elementos profundizando en mayor medida en los más importantes.

1.2.1 CHASIS. ALIMENTACIÓN Y REFRIGERACIÓN

CHASIS

El **chasis**, **caja** o **torre** es el recinto metálico o de plástico que alberga los principales componentes del ordenador y se encarga fundamentalmente de su protección.

¿SABÍAS QUE...?

Los principales materiales con los que se fabrican los chasis son:

- La **chapa troquelada**. De color gris habitualmente, son las más comunes en el mercado. Hay que evitar cajas de este tipo de bajo coste, con la chapa muy fina.
- El **aluminio**. Cada vez son más las cajas que utilizan este material en su construcción pues reúne unas características óptimas para el chasis (es un material rígido y liviano).

Muchas suelen combinar aluminio en los frontales y partes más visibles y chapa troquelada en otras partes.

Otros materiales, como el **acero**, serían adecuados pero el peso hace que no sea operativo utilizarlo.

Formatos más habituales

***Figura 1.5**. Algunos de los formatos de caja más usuales*

Los formatos más habituales de las cajas son:

- **Semitorre ATX**. Este es el formato más vendido con diferencia gracias a su precio y posibilidades de expansión.
- **Torre ATX y EATX**. Es un formato muy empleado cuando se necesitan muchas bahías, sobre todo el EATX, que emplean hasta cinco o más externas de 5 ¼ y admiten otras tantas internas de 3 ½.
- **Micro-ATX**. Este modelo de cajas ocupan muy poco espacio, lo cual implica que suelan llevar solamente una bahía externa de 5 ¼. Las placas soportadas son placas de pequeñas dimensiones (tipo micro-ATX o similares). Es posible que no sea compatible con disipadores más voluminosos que los que vienen de serie con los procesadores.
- **Mini-ITX**. Suelen llevar una bahía de formato *slim* (en portátiles) para lectores ópticos al igual que un alojamiento para un disco duro de portátil (formato ODD). Las placas soportadas son las mini-ITX. Las fuentes de alimentación que llevan estas cajas suelen ser de baja potencia (150 W). Estas cajas no están pensadas para su posible expansión.

Existen cajas más pequeñas que estas como las **pico-ITX**.

***Figura 1.6**. Barebone Shuttle. Fuente ndevilTV*

Es habitual el empleo de chasis de reducidas dimensiones en dispositivos como los **barebones**.

¿SABÍAS QUE...?

Un **barebone** es la solución idónea cuando buscamos un ordenador que ocupe poco espacio.
Su nombre proviene del inglés *barebone*, literalmente hueso desnudo, usado para indicar que algo tiene únicamente lo esencial.

ALIMENTACIÓN

La fuente de alimentación transforma la corriente eléctrica alterna procedente del sistema eléctrico en corriente continua en un voltaje apropiado para los distintos componentes del ordenador. Hoy día suelen incluir un consumo inteligente asociado a la actividad del sistema de forma que casi todos los dispositivos cumplen con la norma **Energy Star** que identifica a productos que usan eficientemente la energía.

Figura 1.7. *Logo de Energy Star*

¿SABÍAS QUE...?

Multiplicando (*potencia en KW*) * (*número de horas*) * (*precio del KWh*) se obtiene el dinero que cuesta mantener cierto aparato encendido un cierto número de horas.
Para averiguar el dinero que cuesta mantener un aparato encendido un cierto número de horas habrá que mirar primero la factura de la empresa que te vende la electricidad (precio del KWh).
Por ejemplo, para una factura de 0,11248 €/KWh con un ordenador que gastase una media de 150 Watios a la hora, que serían 0,150 * 24 = 3,6 kW/día.
Sin entrar en consideraciones legales del tema, son muchos los usuarios que mantienen su ordenador encendido 24 horas al día, descargando vídeos, películas o programas desde redes de intercambio de ficheros. El coste de dejar ese PC siempre encendido sería de 0,402928 €/día, unos 12,147 €/mes.

REFRIGERACIÓN

Mantener el sistema refrigerado es un factor determinante en la longevidad del equipo así como en el aprovechamiento óptimo de las prestaciones del mismo.

Casi todos los componentes internos del ordenador generan calor cuando están funcionando aunque en mayor medida el/los microprocesador(es), la tarjeta gráfica, el *chipset* de la placa base, la memoria RAM o el disco duro.

Un equipo bien refrigerado dura más tiempo que otro que funciona a altas temperaturas. Además, dicho sobrecalentamiento puede provocar pérdida de datos e incluso daños en el equipo.

Hoy día existen dos formas básicas de refrigerar un sistema:

- ✓ Sistemas de refrigeración por aire o sistemas de ventilación.

***Figura 1.8**. Descripción de un sistema de refrigeración por aire*

- ✓ Sistemas de refrigeración líquida o *watercooling*.

  Es una técnica de enfriamiento que usa agua o cualquier líquido refrigerante en lugar de ventiladores y disipadores de calor. Estos líquidos tienen mayor conductibilidad térmica que el aire y la idea consiste en apoyarnos en un circuito cerrado de líquido que extrae el calor fuera del chasis enfriándolo.

¿SABÍAS QUE...?

Una variante del sistema de enfriamiento líquido consiste en utilizar **aceite** en vez de agua. Dado que el aceite común no conduce la electricidad, incluso algunos usuarios han probado con éxito la técnica de sumergir la placa base por completo en un recipiente previamente lleno de aceite mineral.

En caso de querer refrigeración extrema, es conveniente emplear **placas Peltier**. Son una opción muy interesante para los **overclockers** (*gente que sube la frecuencia de reloj de un componente y su voltaje para obtener un mayor rendimiento aunque a consta de aumentar su temperatura*).

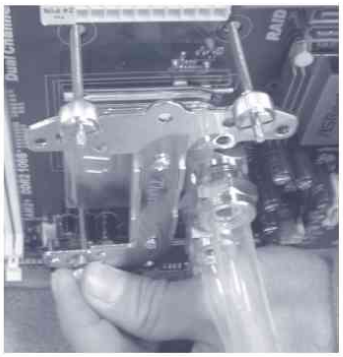


***Figura 1.9**. Instalando un sistema de refrigeración líquida*

Las **ventajas de la refrigeración líquida** son la refrigeración silenciosa y el impacto visual en algunos casos.

1.2.2 DISPOSITIVOS INTERNOS. LA PLACA BASE

DESCRIPCIÓN DE LA PLACA BASE

La **placa base** (*mainboard*) **o placa madre** (*motherboard*) es uno de los elementos principales del ordenador, ya que a ella se conectan todos los demás componentes, siendo conocido como un **componente integrador**.

Físicamente se trata de una gran tarjeta de circuito impreso, a la que se conectan diversos elementos que se encuentran anclados sobre ella entre los que destacan el microprocesador, la memoria RAM, tarjetas y diversos chips de control como la BIOS, que permite realizar funciones básicas de prueba y reconocimiento de dispositivos, carga del sistema de arranque, etc.

Principales Formatos de Placas Base

El formato más empleado es el **ATX** junto al **mini-ATX**. De momento se resiste a ser sustituido por formatos más avanzados y de dimensiones más razonables.

Las ventajas principales de estas placas son una mejor ventilación al situarse la CPU justo debajo de la fuente de alimentación recibiendo aire fresco de esta y menos maraña de cables pues los conectores están más cerca de los discos duros y unidades.

La reducción de tamaño de las **placas mini-ATX**, **micro-ATX** o **micro-BTX** no es mucha, simplemente reducen dos o tres ranuras de expansión y la placa resultante sigue siendo bastante grande.

La reducción real se lleva a cabo por ejemplo en las **placas mini-ITX**, **nano-ITX** y **pico–ITX**. **Mini-ITX** es un formato que tiene mucho éxito. Normalmente estas placas base tienen al menos una ranura de expansión y muchos dispositivos integrados como sonido 7.1, canales con salida digital, red Gigabit, SATA, etc.

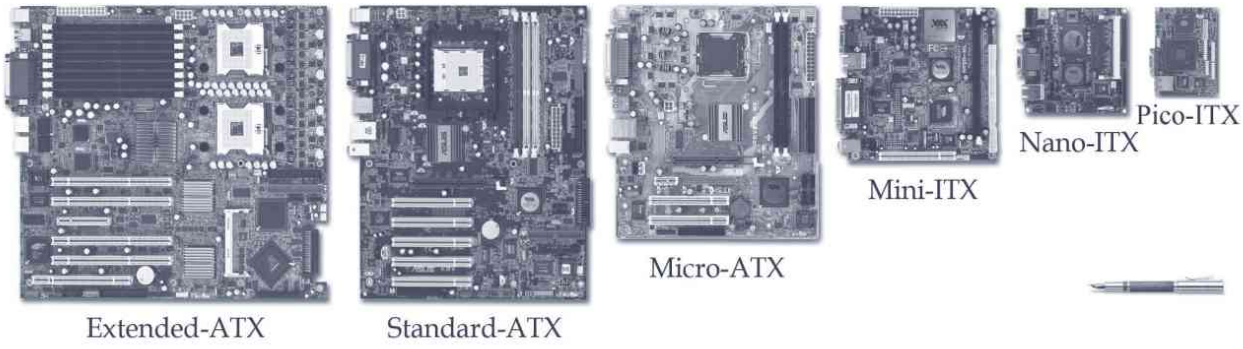


***Figura 1.10**. Distintos factores de forma de motherboard*

Elementos de la Placa Base

Una placa base ATX actual ofrece un aspecto similar al siguiente:

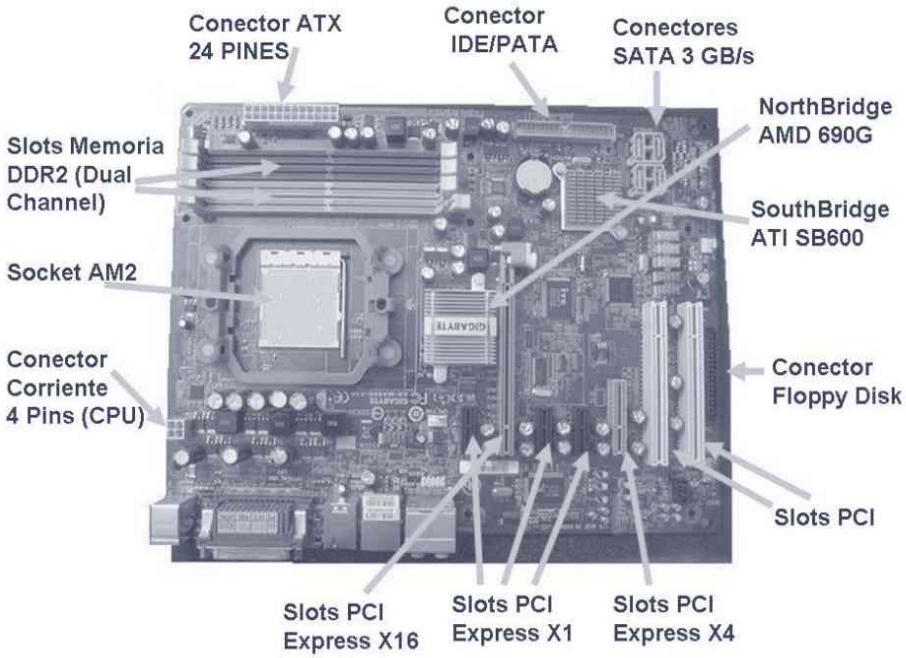


***Figura 1.11**. Elementos de una placa base*

- **El circuito impreso**. También conocido como **PCB** (*Printed Circuit Board*). Es un medio para sostener mecánicamente y conectar eléctricamente componentes electrónicos, a través de rutas o pistas de material conductor grabados en hojas de cobre laminadas sobre un sustrato no conductor.
- **Zócalo del procesador o socket**. Es el conector donde se inserta el microprocesador. Los primeros microprocesadores estaban soldados a la placa base o insertados en zócalos donde era imposibles sacarlos. Los formatos de zócalos actuales más empleados son **PGA** y **LGA**. El formato **ZIF** (zócalo de presión nula, haciendo referencia a la presión requerida para instalar o extraer el microprocesador) puede considerarse un subtipo de zócalos PGA. Veamos algo más de cada uno:
  - **Socket PGA** (*Pin Grid Array*). Utilizado mucho por AMD, estos son *sockets* clásicos utilizados también en microprocesadores que fueron importantes en su tiempo como el 386 y 486. Consiste en una matriz de conectores en los cuales se van insertando las patillas del chip a presión.
  - **Socket ZIF** (*Zero Insertion Force*). Estos *sockets* además de la matriz de conectores, disponen de un mecanismo con una patilla que permite cuando está levantada insertar el microprocesador y, cuando ésta se baja, el micro encaja y hace conexión sin realizar fuerza sobre él.
  - **Socket LGA** (*Land Grid Array*). Utilizado mucho por Intel, en este *socket* los pines están en la placa base en vez de en el micro. El micro tiene una serie de contactos que harán contacto con los pines de la placa base. Estos microprocesadores son menos delicados que los micros con pines dado que los pines se suelen doblar con mucha facilidad.

¿SABÍAS QUE...?

Los **zócalos**, o *sockets*, se emplean en equipos de arquitectura abierta, donde se busca que haya variedad de componentes permitiendo el cambio de la tarjeta o el integrado. En los equipos de arquitectura propietaria, como es el caso de las consolas de videojuegos, los integrados se sueldan sobre la placa base.
En los últimos años el número de pines de estos zócalos ha aumentado de manera sustancial debido al aumento en el consumo de energía y a la reducción de voltaje de operación. En los últimos 15 años, los procesadores han pasado a incrementar sus voltajes y potencias (de 20 vatios a más de 80 vatios).

- **Zócalos de Memoria**. Las placas base tienen entre 1 y 8 zócalos para la inserción de módulos de memoria SIMM o DIMM, este valor dependerá de las características del *chipset* de la placa base. Muchas placas base sólo admiten combinaciones determinadas de los módulos de memoria en sus zócalos.
- **Memoria Caché**. Los ordenadores de 4ª y 5ª generación usaban una caché secundaria, de **nivel 2** o **caché L2** integrada en la placa base. A partir de la sexta generación la caché de nivel 2 se integró en el propio microprocesador.
- **Slots de Buses**. Estas ranuras sirven para aumentar las capacidades del sistema. En ellas se insertan tarjetas y controladoras de entrada-salida. Hoy día los *slots* más habituales son PCI, y PCI-Express.
- **Chipset**. El *chipset* es un conjunto de circuitos integrados diseñados a partir de una arquitectura de procesador determinada que permiten comunicar la placa base donde reside y los componentes que a ésta se conectan con el procesador. En la actualidad está formado por un par de chips denominados **NorthBridge** (Puente Norte) y **SouthBridge** (Puente Sur).

  El **NorthBridge** une los componentes del *bus* primario (*host bus*) y suelen ser los de mayor velocidad de transferencia: el microprocesador, la memoria y el adaptador de vídeo. Este *bus* suele ser de 64 bits y emplea frecuencias elevadas.

  El **SouthBridge** es en realidad un puente para acceder a otros *buses* más lentos, como el PCI, el IDE, el USB y el LPC (*Low Pin Count*), al que se conectan la BIOS, el controlador del ratón y teclado y los puertos serie y paralelos.

  El *Southbridge* se une al *Northbridge* mediante su propio *bus* denominado **Hub Link**.

  El generador de reloj marca el ritmo de los *buses* primario, PCI, USB y *Hub Link*.

¿SABÍAS QUE...?

Ya los primeros procesadores, como el Intel® 4004, venían asociados a *chipset* destinados a facilitar la comunicación y el trabajo entre el microprocesador y la placa base, ya que es el *chipset* el que permite que la placa base funcione como eje del sistema integrador.
En la actualidad los principales fabricants de *chipsets* son AMD®, Intel®, NVIDIA®, SiS® y VIA Technologies®.

- **BIOS** (Basic *Input Output System*). Se implementa mediante memoria ROM o EEPROM (memoria que se puede borrar y escribir) y los datos de configuración se almacenan en una memoria CMOS. Consiste en un conjunto de rutinas básicas que permiten la entrada y salida al sistema, además de permitir configurar determinados parámetros mediante una RAM CMOS. Tiene pues un papel muy importante justo antes de que el sistema operativo tome el control del equipo ya que identifica los componentes principales (RAM, microprocesador, *chipset*, unidades de disco, etc.) y le proporciona acceso y control a todos ellos. Este tipo de memoria es volátil por lo que tiene que estar siendo alimentada permanentemente, para lo cual se emplea una pequeña batería o pila. Existen diversos fabricantes de BIOS como Award o AMI.

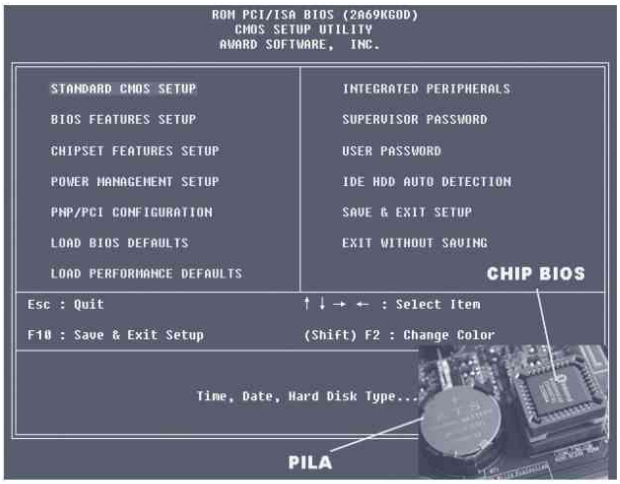


***Figura 1.12**. Esquema de la BIOS*

- **Batería**. El ordenador usa una batería para seguir suministrando corriente y permitir guardar cierta información cuando no está alimentado.
- **Otros componentes**. Como el conector de alimentación, el reloj de tiempo real, reguladores de tensión y condensadores, *jumpers*, conectores de pin y controladores.

EL MICROPROCESADOR

Un microprocesador es un circuito integrado compuesto por millones de transistores que contiene algunos o todos los elementos hardware de una CPU. Se encarga de llevar a cabo todo el procesamiento del ordenador y por ello es considerado el cerebro del mismo.

Hoy día una CPU puede estar soportada por uno o varios microprocesadores, así como un microprocesador puede soportar una o varias CPU. En este sentido ha surgido el concepto de núcleo, o **core**, para referirse a una porción del procesador que lleva a cabo todas las actividades de una CPU real existiendo microprocesadores capaces de integrar varios núcleos.

Parámetros de un Microprocesador

El rendimiento del procesador se puede medir de distintas formas destacando parámetros como la frecuencia de reloj, la velocidad del *bus* o las prestaciones de la memoria caché que emplea.

- **Frecuencia de Reloj**. Aunque impone el ritmo de trabajo del microprocesador y hasta hace unos años ha sido la característica más determinante al elegir un modelo, en los últimos años su valor se ha estabilizado entre los 2-4 GHz, ya que no se han requerido frecuencias más altas para aumentar su capacidad de proceso y se han optimizado el resto de parámetros.

  Además, la tendencia es incorporar más núcleos para aumentar el rendimiento medio de forma que este indicador es cada vez menos determinante. Medir el rendimiento a través de la frecuencia es sólo válido cuando evaluamos procesadores con arquitecturas similares.

  Las principales unidades de medida de la frecuencia son el Hercio (Hz), KiloHercio (KHz), Megahercio (MHz) y Gigahercio (GHz).

- **Velocidad del bus**. El *bus* que comunica el microprocesador con el *northbridge* se denomina *Front Side Bus* (FSB) en los microprocesadores Intel® o FSB *Hipertransport* (HTT), *Lightning Data Transport* (LDT) o simplemente **hipertransport** en procesadores AMD®.

  La prestaciones del *bus* vienen determinadas por el ancho del mismo (64 bits normalmente) y su velocidad, en megahercios. Además, la velocidad del *bus* del microprocesador suele estar relacionada con la de otros *buses* como el de memoria, PCI y PCI *Express* o AGP.

  Normalmente, la velocidad del *bus* de memoria es la misma que la del FSB, al funcionar de forma síncrona, mientras que los otros *buses* funcionan según una fracción del FSB (3/4 por ejemplo).

- **Memoria Caché**. La memoria caché, al ser más rápida que la memoria RAM, acelera el rendimiento, dado que almacena los datos que se prevé que más se van a usar.

  Como ya hemos estudiado existen varios tipos de caché:

  - **Caché L1 o primaria de nivel 1**. Están integradas en el núcleo del microprocesador y funcionan a la máxima velocidad.
  - **Caché L2 y L3 o de nivel 2 y 3**. Conectadas al micro mediante el **back side bus** (*bus* trasero), el cual es más rápido que el *bus* frontal. Pueden estar implementadas en el núcleo, encapsulado o ser externas. La caché L2 es más lenta que la L1 y la L3 que la L2.

- **Disipación del Calor**. Los primeros microprocesadores no tenían ningún sistema de disipación del calor. Sin embargo, a partir del 486, los microprocesadores empezaron a utilizar disipadores (rejillas o aletas que están pegadas al microprocesador) para refrigerarse. Conforme fue necesario, a estos disipadores se le colocó un ventilador que aumentaba la refrigeración al forzar a que el aire recirculara más deprisa.

  Actualmente, para una refrigeración muy exigente se suelen utilizar incluso *heatpipes* (tubos huecos sellados), los cuales tienen un líquido refrigerante en su interior, el cual se evapora y absorbe calor para luego condensarse en otro extremo.

  La refrigeración de los procesadores es sumamente importante, se están investigando materiales y técnicas porque una de las limitaciones de la evolución de los microprocesadores es precisamente la refrigeración.

¿SABÍAS QUE...?

En la actualidad se están investigando nuevos mecanismos para disipar el calor del microprocesador y favorecer su refrigeración, como la **propulsión de aire electrostático** y el **efecto de descarga de corona**, **viento iónico** o **aceleración de fluidos electrostáticos**.

- **Tecnología de fabricación**. La tecnología de fabricación indica el tamaño del elemento más pequeño del chip y da una idea de lo avanzado del mismo. Actualmente, los microprocesadores que se pueden comprar en una tienda están fabricados en una tecnología de 45 nanómetros (nm). Un nanómetro es la millonésima parte de un milímetro.

El *Overclocking*

El *overclocking* es un aumento de la velocidad del microprocesador por encima del establecido en el estándar de fábrica. Se consigue un rendimiento extra de forma gratuita pero produciendo más consumo energético y más calor. El *overclocking*, siempre que se salga de los parámetros fijados por el fabricante, implica la pérdida de garantía del microprocesador.

La fabricación de Microprocesadores

Los microprocesadores se fabrican utilizando técnicas mucho más complejas que la fabricación de otros circuitos integrados más simples. El proceso consiste en depositar en una **oblea**, o lámina de silicio, una serie de materiales conductores, aislantes y semiconductores en forma de bocadillo loncheado (sándwich), superponiendo diferentes capas, para lograr así el deseado microprocesador.

Este proceso es tan preciso que una mota de polvo en un microprocesador lo haría inservible, por tanto, se fabrican en las llamadas salas limpias en las cuales el aire es filtrado y está libre de polvo.

***Figura 1.13**. Proceso de fabricación de microprocesadores. Cortesía Intel*

MEMORIAS INTERNAS

La Memoria RAM

La memoria principal o RAM (*Random Access Memory*, memoria de acceso aleatorio) es el lugar donde el ordenador guarda los datos que está utilizando en el momento actual, con el equipo encendido y operativo. Su capacidad de almacenamiento se mide en **megabytes** (MB) y múltiplos, siendo valores habituales hoy día 2 GB, 4 GB, 16 GB ó 32 GB.

A diferencia de la memoria secundaria, es volátil (se borra la información que contienen al apagar el ordenador) y mucho más rápida.

En la actualidad los ordenadores tienen memoria RAM en muchos componentes internos. Por ejemplo, en el procesador (memoria caché, registros), en los lectores ópticos (*buffer* o caché) o en las tarjetas gráficas (memoria de vídeo o gráfica), aunque cuando hablamos de memoria RAM estamos hablando principalmente de los módulos de memoria que se insertan en la placa base.

Estas memorias se agrupan en módulos de memoria que se conectan a la placa base del ordenador.

Según los tipos de conectores que lleven los módulos, se clasifican en módulos **SIMM** (*Single Inline Memory Module*) con 30 ó 72 contactos, módulos **DIMM** (*Dual In-line Memory Module*) con 168, 184 ó 240 contactos y módulos **RIMM** (*Rambus In-line Memory Module*) con 184 contactos.

Son parámetros fundamentales de este tipo de memoria:

- **Tiempo o Velocidad de Acceso**. Cuanto menor tiempo de acceso tenga la memoria más rápida será. Por ejemplo, una memoria DDR3-1600 puede tener una velocidad de acceso de 5 nanosegundos.
- **Velocidad de reloj**. Las memorias DDR, DDR2 y DDR3 se suelen clasificar atendiendo a dos criterios: según la velocidad del reloj del *bus* (DDR3-1600, DDR3-1333, DDR3-106, etc.) o bien por su ancho de banda teórico (PC3-12800, PC3-10600, PC3-8500, etc.). Normalmente se suelen comercializar atendiendo a la velocidad de reloj del *bus*. El ancho de banda teórico es la máxima capacidad de transferencia del *bus*.
- **Voltaje**. El voltaje viene determinado por el tipo de memoria y tecnología.
- **Tecnologías soportadas**. Con el uso de técnicas como *Single Memory Channel* (un solo canal de intercambio de información entre módulos de memoria y *bus*), *Dual Memory Channel* (dos canales simultáneos diferenciados de intercambio, la CPU funciona con dos canales independientes y simultáneos, con lo cual las cifras de ancho de banda efectivo se disparan) o incluso *Triple Channel*.

¿SABÍAS QUE...?

Bill Gates dijo en los años ochenta: "**640 KB de memoria RAM deberán ser suficientes para hacer cualquier cosa**". Hoy día lo normal es instalar entre 4 GB y 8 GB, unas 64.000 veces más cantidad. Estuvo bastante alejado de la realidad actual pero aquel joven entonces justificó sus palabras en el hardware y software de entonces, con sistemas operativos sin entornos gráficos y aplicaciones muy elementales.

En la actualidad se usan básicamente los módulos **DIMM** en ordenadores de escritorio, con *bus* de datos de 64 bits, y los módulos **SO-DIMM** en portátiles como un formato miniaturizado de DIMM. Estos últimos tienen 100, 144 y 200 contactos y las características en voltaje y prestaciones de la memoria son las mismas que las de un equipo convencional.

También existe un formato más pequeño, pero menos utilizado, que es el **Micro-DIMM**.

Las **principales memorias** usadas hoy día son las **DDR3 SDRAM** que tienen similares tiempos de acceso a DDR2 y trabajan en el rango de frecuencias de 800-2.600 MHz. Son físicamente incompatibles con memorias anteriores (DDR2 y DDR).

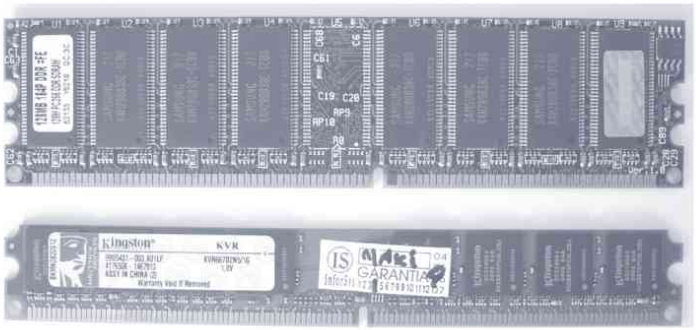


***Figura 1.14**. Módulos de memoria RAM (DDR y DDR2)*

Memorias de Vídeo o Gráfica

Dentro de las memorias internas merece también ser nombrada la memoria de vídeo o gráfica. Es aquella memoria empleada por el controlador de la tarjeta gráfica para poder manejar toda la información visual que le manda la CPU del sistema.

Hace unos años las tarjetas de vídeo se basaban en el empleo de memoria DDR. Actualmente los fabricantes se han decantado por otros tipos de memoria más eficientes como DDR2 y DDR3, que son memorias RAM convencionales y otras **memorias especificas de vídeo** como son **GDDR3**, **GDDR4** y **GDDR5** (GDDR = *Graphics Double Data Rate*). Este último tipo de memorias, aunque es muy parecido a las memorias DDR2 y DDR3, tienen algunas características que las hacen más apropiadas para las tarjetas de vídeo.

¿SABÍAS QUE...?

Los **módulos GDDR** son chips de memoria insertadas directamente en las tarjetas gráficas o en la placa base (en el caso de gráficas integradas en placa base que utilicen este tipo de memoria), siendo controlados directamente por el procesador de la gráfica, no interviniendo para nada en este proceso la placa base.
Se trata de memorias muy rápidas, con velocidades actualmente en torno a los 1,5 GHz, con acceso directo al procesador gráfico y un ancho de banda enorme (alrededor de 75 GB/s).
Si tenemos en cuenta que es una memoria totalmente independiente de la memoria del sistema, no existe ningún tipo de incompatibilidad entre ésta y la propia del sistema, pudiendo ser por tanto diferentes.

EL CHIPSET

El *chipset* es un conjunto de procesadores situados en la placa base que están pensados para que funcionen como si fueran únicos y realizan las funciones de la placa base. Cada uno tiene una misión específica, esto hace que sean los responsables de la comunicación entre los demás elementos del equipo informático (disco duro, microprocesador, memoria, etc.).

La arquitectura actual del *chipset*, denominada **Puente Norte-Puente Sur** (**NorthBridge-SouthBridge**), está basada en una doble división estratégica funcional del mismo en base a la velocidad de los tipos de dispositivos que se pueden conectar.

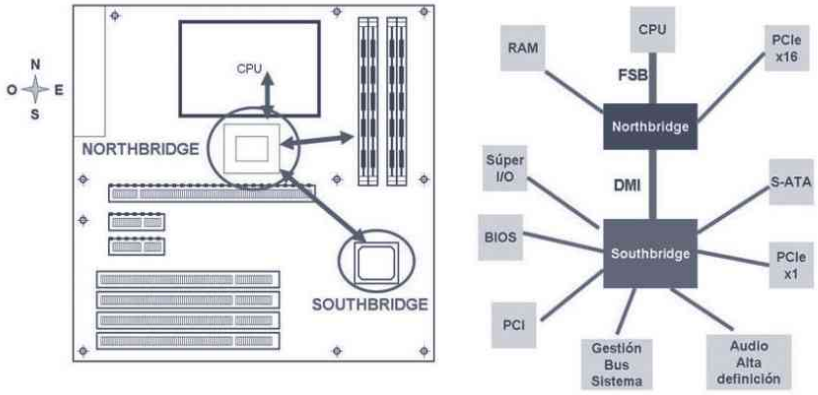


***Figura 1.15**. Arquitectura Puente Norte-Puente Sur*

EL NORTHBRIDGE

Aparece con las placas ATX y se sitúa en la parte norte de la placa, junto a la CPU y la memoria. Se encarga de gestionar la memoria, comunicación con el procesador, los puertos gráficos (AGP) y la comunicación con los demás componentes del equipo a través del *Southbridge*. Antiguamente los *Northbridge* también gestionaban los puertos PCI, aunque ahora los puertos PCI los gestiona el *Southbridge*.

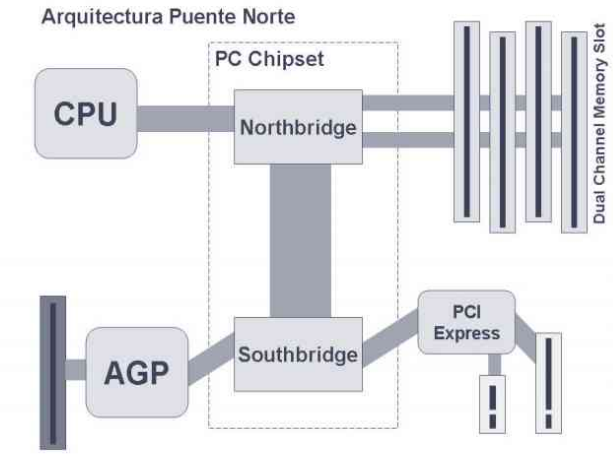


***Figura 1.16**. Arquitectura Puente Norte*

Como se puede observar en la figura anterior, del tipo de *Northbridge* dependerá el tipo de procesador que admite la placa, la frecuencia del *front side bus*, el adaptador gráfico y el tipo y frecuencia de la memoria.

EL SOUTHBRIDGE

El *Southbridge* no está directamente conectado a la CPU. La conexión a la CPU es a través del *NorthBridge* mediante el **DMI** (*Direct Media Interface*).

Se suele llamar concentrador de controladores de entrada-salida o **input/output controller hub** porque se encarga de controlar casi la totalidad de los elementos de entrada salida del equipo y algunas otras funcionalidades de baja velocidad.

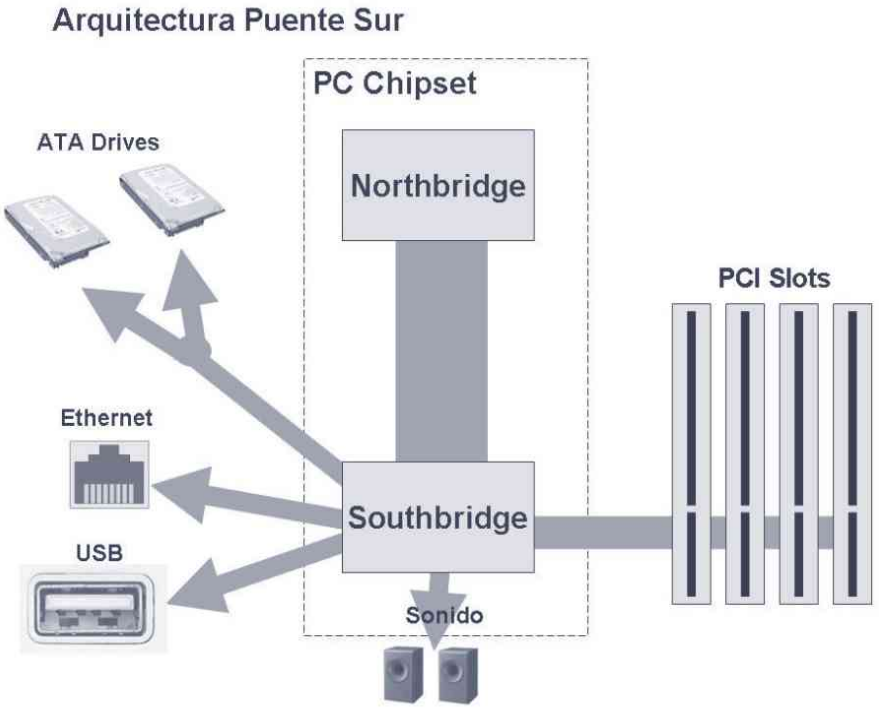


Figura 1.17. *Arquitectura Puente Sur*

Se encarga de controlar los siguientes elementos: la administración de potencia eléctrica, la BIOS, *bus* PCI, *bus* ISA, controlador DMA, controlador SATA o PATA, controlador de interrupciones, interfaz de sonido AC97, puente LPC, reloj en Tiempo Real, soporte Ethernet, soporte RAID y soporte USB.

Aunque algunos de los elementos anteriores son controlados por un chip independiente, como el puerto *Ethernet* o la interfaz de sonido, es el *Southbridge* el que se encarga de la coordinación de estos.

CONECTORES DE LA PLACA BASE

Buses y ranuras de expansión

Los *buses* son líneas de interconexión que interconectan el procesador con los distintos dispositivos del equipo. Aunque existen muchos *buses* (FSB, *Hipertransport*, *Back Side Bus*…) en este apartado solo vamos a trabajar los relacionados con las tarjetas de expansión o *slots*.

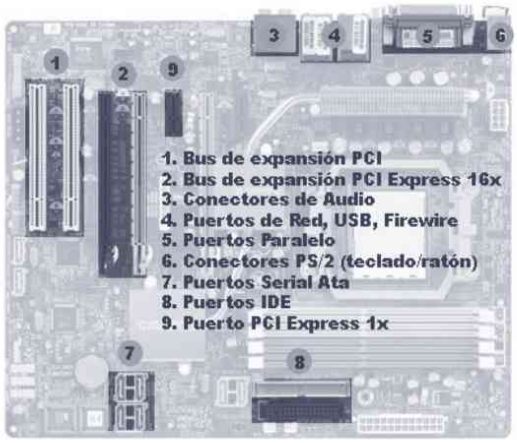


***Figura 1.18**. Buses y ranuras de expansión de una placa base*

BUS PCI

El *bus* PCI, o *Periphreal Component Interconnect* (inteconexión de componentes periféricos), fue creado en 1993 por Intel®, este tipo de *bus* está desapareciendo dando paso al PCI Express.

BUS PCI EXPRESS

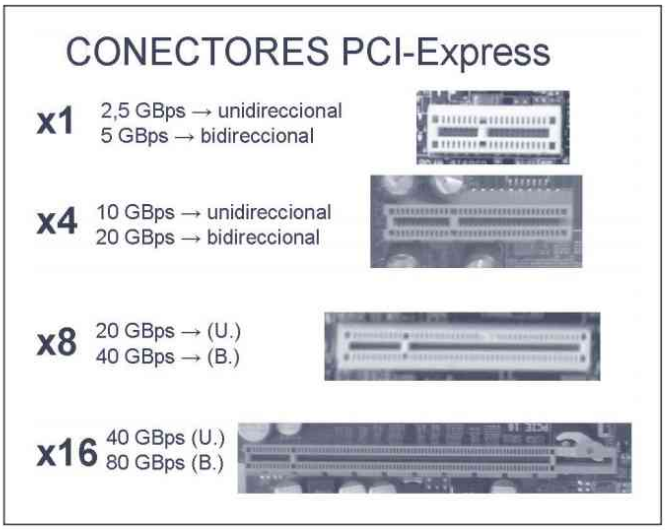


***Figura 1.19**. Algunos de los conectores PCI-Express*

El puerto PCI resultaba escaso para las necesidades de algunas tarjetas como las gráficas actuales o las Gigabit Ethernet, ante lo que surgió este nuevo puerto. El puerto está formado por uno o más enlaces punto a punto de tipo bidireccional. En realidad se mandan muy pocos bits a la vez pero a mucha velocidad (2,5 ó 5 Gbits/s).

Existen *slots* con uno (X1), cuatro (X4), ocho (X8), diecisésis (X16) o treinta y dos (x32) enlaces de datos. Para hacerse una idea, un enlace X1 es más rápido que el PCI normal y un enlace X8 es igual de rápido que la versión más rápida de AGP.

¿SABÍAS QUE...?

Inicialmente, a finales de los 70, se desarrollaron *buses* capaces de trabajar con 8 bits de forma simultánea denominados XT. Con el avance de la informática aparecieron procesadores capaces de manejar 16 bits de datos, pero si los *buses* aún continuaban a 8 bits se producía un **cuello de botella**. Aparecieron entonces los *buses* del tipo ISA y se volvió a repetir el problema, solucionándose con la llegada de nuevos estándares como PCI, útil para conectar tarjetas que no requieran una gran capacidad de transmisión de datos como módems o tarjetas de sonidos sencillas, AGP, ante las necesidades gráficas o el actual PCI Express en sus distintas versiones.

1.2.3 UNIDADES DE ALMACENAMIENTO SECUNDARIO

El almacenamiento secundario lo conforman el conjunto de dispositivos y medios o soportes que almacenan memoria secundaria, entendida como almacenamiento masivo y permanente.

En la actualidad, para almacenar información se usan las siguientes tecnologías: la **tecnología magnética** (discos duros, disquetes, cintas magnéticas), **tecnología óptica** (CD, DVD, *Blu-ray*), **tecnología magneto-óptica** (discos *zip*) y **tecnología flash** (tarjetas de memorias *flash*).

Las principales unidades y soportes de almacenamiento secundario son:

Tabla 1.2 Dispositivos o unidades con sus respectivos soportes o medios

Dispositivos o Unidades	Soportes o Medios
Disquetera o unidad de discos flexibles	Discos flexibles o disquetes (3 ½ y 5 ¼)
Unidad de disco rígido (*Hard Disk Drive*)	Discos rígidos o discos duros
Unidad de cintas magnéticas (*Tape Drive*)	Cintas magnéticas de datos, audio o vídeo
Lector/grabador de discos ópticos	CD, DVD y *Blu-ray*
Lector de tarjetas de memoria	Tarjeta de memoria *flash*

A la hora de elegir una unidad o soporte de almacenamiento hay que observar una serie de características entre las que destacan la **capacidad** (MB, GB o TB), la **velocidad de transferencia** (MB/s) y los **tiempos medios de acceso**, **búsqueda** y **lectura/escritura** (nanosegundos o ns).

1.2.4 TARJETAS DE EXPANSIÓN

Las tarjetas de expansión son dispositivos con diversos circuitos integrados que se insertan en ranuras de expansión de la placa base con el fin de ampliar la capacidad del ordenador.

Dichas tarjetas de expansión emplean puertos **PCI**, **AGP** (ya en desuso) y **PCI Express**, además de las **PCMCIA** y **Expresscard** de los portátiles.

Hoy día cada vez se emplean menos debido al avance de la tecnología USB y de que muchas funciones, como la conectividad Ethernet, el audio y el vídeo están ya integradas en la placa base.

Entre las tarjetas de expansión más utilizadas están la *tarjeta capturadora o sintonizadora de vídeo y/o televisión*, *tarjeta de red* (cableada o inalámbrica), *tarjeta de sonido*, *tarjeta gráfica*, *tarjeta PCI-SCSI*, *tarjeta PCI-RAID*, *tarjeta PCI-IDE*, *tarjeta expansión SATA*, *tarjeta expansión USB*, *tarjeta expansión Firewire*, etc.

LA TARJETA GRÁFICA

La tarjeta gráfica, tarjeta de vídeo y/o aceleradora gráfica juega un papel fundamental y merece ser objeto de estudio en los ordenadores actuales, donde el contenido multimedia está constantemente presente con una calidad y resolución gráfica tan exigente.

Es la encargada de procesar los datos que provienen de la CPU y transformarlos en información comprensible y representable en un dispositivo de salida como un monitor o un videoproyector.

Además de las tarjetas gráficas habituales, entendidas como tarjetas dedicadas y separadas de la placa base, se conoce también como tarjeta gráfica a las **GPU** (*Graphics Proccessing Unit*, procesador de tarjetas gráficas) integradas en la placa base.

Dada la exigencia gráfica de los videojuegos, aplicaciones 3D o programas de edición de vídeo, se hace necesario un procesador que aligere la carga de trabajo que tiene el procesador central. La GPU se encarga de gran parte de las tareas para gráficos mientras que la CPU está realizando otra serie de tareas.

Una GPU está especializada en procesamiento gráfico y en ejecución de operaciones en coma flotante, típicas en los gráficos 3D, pudiendo llegar a alcanzar velocidades elevadas de proceso pero nunca será capaz de reemplazar a una CPU.

Existen múltiples técnicas empleadas por las tarjetas gráficas en la mejora de la imagen como el **antialiasing**, que consiste en el suavizado de los bordes de los objetos, importante para obtener imágenes realzadas. Normalmente, al aplicar algún tipo de *antialiasing* la calidad de la imagen mejora sensiblemente.

En la actualidad existen dos grandes empresas, **NVIDIA** y **ATI**, que lideran el mercado de este componente a través de sus respectivos chips gráficos *GeForce* y *Radeon*.

¿SABÍAS QUE...?

Las **tarjetas de vídeo** normalmente siguen para cada marca una serie de numeraciones y sufijos, por ejemplo, en el caso de NVidia, el modelo 9800 es mejor que el 9600 (cuanto más alto mejor), y dentro del mismo modelo una GTX es mejor que una GT (de peor a mejor en el caso de NVidia, tenemos LE, G, GS, GT, GTS, GTX y Ultra).

1.2.5 DISPOSITIVOS EXTERNOS DE ENTRADA-SALIDA. PERIFÉRICOS

Se puede considerar un periférico a todo aquel dispositivo que se pueda conectar al sistema y que transmita o reciba información.

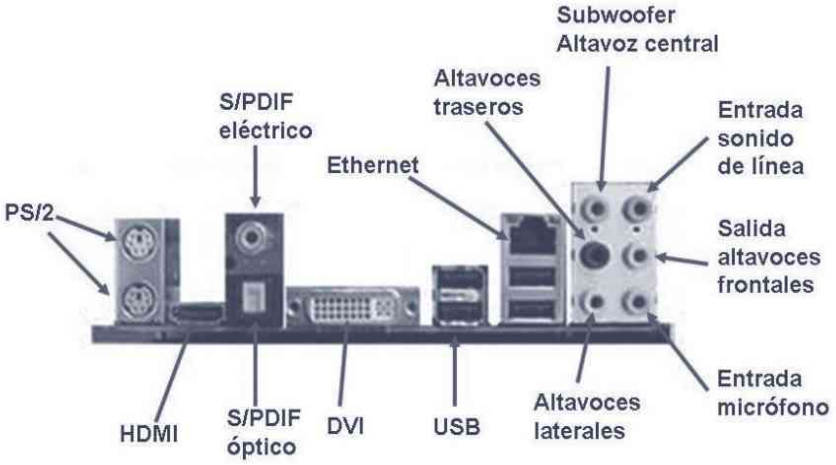


***Figura 1.20**. Relación entre la memoria principal, el sistema operativo y el periférico*

En el periférico la información se transforma. Por ejemplo, en un disco las señales magnéticas se transforman en impulsos eléctricos y en una impresora pasarán cosas parecidas, se transformará en caracteres, puntos… El sistema operativo es un intermediario, es el encargado de recibir y enviar esta información desde y hasta el periférico y almacenarla en la memoria principal o RAM.

1.3 DISPOSITIVOS Y SISTEMAS DE ALMACENAMIENTO

Actualmente la información se almacena de forma definitiva en los sistemas informáticos en dispositivos que utilizan tecnologías diferentes:

- **Tecnología magnética**. Es la utilizada en los discos duros y otros dispositivos. La información se almacena magnetizando la superficie del disco. Se puede almacenar gran volumen de información en estos dispositivos. Estos dispositivos son reescribibles.
- **Tecnología óptica**. Utilizada en los CD y DVD. El coste por BIT es muy bajo. La mayoría de estos soportes son de solo lectura y no permiten su reescritura.
- **Memorias sólidas**. El coste por bit cada vez es menor. De momento estos dispositivos no tienen mucha capacidad pero ésta cada vez es mayor. Su uso se está popularizando cada vez más y en un futuro esta tecnología puede llegar a tener más uso que las dos anteriores.

***Figura 1.21**. Características de los dispositivos de almacenamiento*

1.3.1 DISPOSITIVOS MAGNÉTICOS

El sistema operativo y los programas necesitan estar en memoria para ejecutarse. No es posible ejecutar un programa si no está en memoria central o RAM. La memoria RAM es volátil, esto quiere decir que cuando se deja de suministrar energía eléctrica a la misma esta pierde su información. Dada esta situación se necesita algún dispositivo como discos duros, CD, DVD… que almacene la información de forma definitiva (dispositivos no volátiles) para que ésta no se pierda.

Estos dispositivos de almacenamiento definitivo de la información han ido mejorando con el tiempo permitiendo almacenar mucha más información, con un tiempo de acceso mucho menor y velocidades de transmisión mayores conforme la tecnología ha evolucionado.

Los dispositivos magnéticos más importantes son:

- **Disco duro**. Son los más utilizados en la actualidad. La tecnología va evolucionando hacia discos SSD.
- **Disco flexible**. El tradicional disquete ya ha quedado obsoleto. Está en desuso.
- **Cinta**. Utilizados para la realización de *backup* en entorno empresarial. Cada vez se utiliza menos este tipo de tecnología.

¿De qué están compuestos los dispositivos magnéticos?

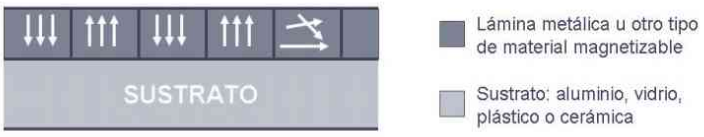


***Figura 1.22**. Composición del plato de un disco duro*

Los dispositivos magnéticos (discos duros, disquetes, cintas....) están formados por un sustrato al que en su superficie se ha depositado algún material magnetizable.

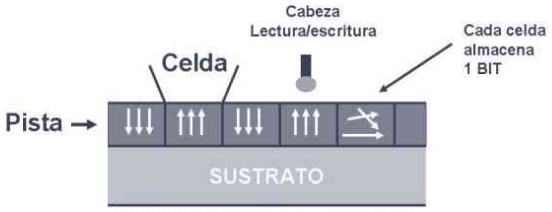


***Figura 1.23**. Organización del material magnetizable de un disco*

El material magnetizable está agrupado en celdas. Dependiendo del tamaño de cada celda se podrá almacenar más o menos información en la misma superficie. Cada celda va a representar un bit y el material en cada celda puede estar magnetizado en alguno de los dos estados estables o bien puede estar sin magnetizar, como se puede apreciar en la figura anterior. La cabeza de lectura/escritura permitirá leer el soporte reconociendo la magnetización de las celdas y escribir la información magnetizando la superficie del mismo.

EL DISCO DURO

Características de un disco duro

A continuación se citarán algunas de las características de un disco duro:

- ✓ Es el dispositivo donde reside normalmente el sistema operativo.
- ✓ Al contrario que la memoria RAM, es un dispositivo de almacenamiento no volátil.
- ✓ La información reside en la superficie de unos platos metálicos los cuales están encerrados en una carcasa.
- ✓ Contiene partes mecánicas y electrónicas.
- ✓ Es un sistema de grabación de forma magnética y digital.
- ✓ El acceso a la información es un acceso aleatorio.

Algunos elementos que componen un disco duro

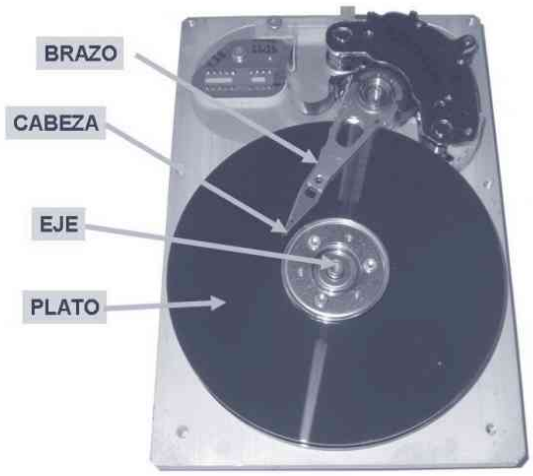


***Figura 1.24**. Estructura interna de un disco duro*

- **Platos**. Están fabricados en algún material metálico como puede ser aluminio, o incluso otros tipos de material como puede ser la cerámica o el vidrio. Las caras externas de los platos están cubiertas de material magnetizable (oxido de hierro u otro) o bien tienen una película metálica que también es magnetizable.
- **Brazos**. También llamados brazos actuadores. Es donde van montadas las cabezas. Las cabezas son el elemento de más precisión y, por tanto, más importantes del disco. El brazo se desplaza de derecha a izquierda. Con este movimiento y el de la rotación de los platos puede accederse a toda la información del disco.
- **Cabezas**. Las cabezas son el dispositivo electromagnético que se encarga de leer, escribir y borrar los datos del dispositivo magnético. Las cabezas aunque parezca que están en contacto con el disco no lo están. Las cabezas vuelan sobre la superficie del disco pero sin tocarla.

¿SABÍAS QUE...?

Si la cabeza llegara a tocar la superficie del disco éste se estropearía.

Las cabezas se sitúan siempre al final del brazo actuador y a través de impulsos magnéticos se encargan de leer y escribir la información en el plato.

Dependiendo del número de platos que tenga el disco así será el número de cabezas. Los platos tienen cabezas en ambas caras del disco. Esto es obvio, puesto que no se va a desaprovechar una de las caras de un plato. Si un disco tiene 2 platos deberá de tener 4 cabezas (2 por cada plato). El número de cabezas está limitado por la BIOS a 16. No obstante hay discos que tienen más de 2 cabezas por plato gracias a la tecnología *sector translation*, la cual permite tener hasta 12 cabezas en un solo plato.

¿SABÍAS QUE...?

A pesar de la tecnología sector translation, un disco no podrá tener más de 16 cabezas.

La interfaz del disco duro

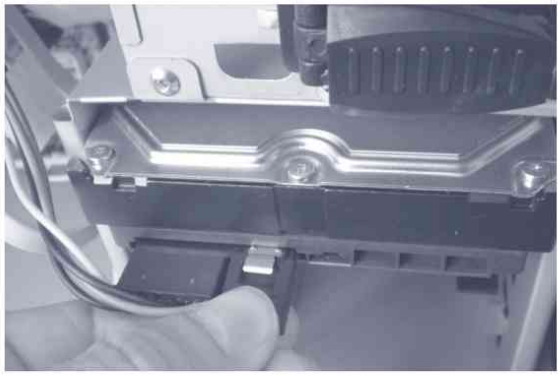


***Figura 1.25**. Instalando un disco duro SATA*

Las interfaces de un disco duro pueden ser:

- **IDE o PATA**. Es la interfaz de los discos antiguos.
- **SATA**. Es la interfaz actual por excelencia. A su buen rendimiento se le une que los discos SATA tienen un precio muy ajustado.
- **SCSI**. Son los más rápidos y se utilizan en entornos profesionales que requieren dispositivos de almacenamiento veloces. Estos discos son más caros que los convencionales.

***Figura 1.26**. Detalle de la parte posterior de un disco duro IDE*

La interfaz SATA

Serial ATA reduce los 16 de ancho del *bus* ATA paralelo (PATA) a solo 1 bit, pero transmite a velocidades muy altas (1,5 Gbit/s ó 3 Gbit/s). Dada la velocidad de esta interfaz, se utiliza un sistema de codificación que da mayor seguridad a la transmisión de datos y la velocidad efectiva al final se queda en un 80% de las cifras citadas anteriormente.

IMPORTANTE

Una cosa es la velocidad máxima de la interfaz y otra es la velocidad efectiva del disco. Los discos nunca llegan a ser tan rápidos como su interfaz, siempre son más lentos.

La velocidad de esta interfaz es de 150 MB/s (SATA I o SATA 150) ó 300 MB/s (SATA II o SATA 300) frente a los 133 MB/s como máximo que ofrece el PATA. Los discos y controladoras SATA II son compatibles con los sistemas más lentos (nunca se alcanzarán los 150 MB/s).

En un futuro se espera tener SATA 600, pero de momento como los discos no llegan ni a la tercera parte de lo que ofrece SATA 300 no hay mucha prisa.

Velocidad de rotación

La velocidad de rotación de los discos duros varía mucho. Hay discos que rotan a 4.500 ó 5.400 revoluciones por minuto (como los discos de los portátiles), hasta discos SCSI que pueden rotar a 15.000 revoluciones por minuto (RPM). Normalmente, los discos de los equipos de sobremesa funcionan a 7.200 RPM. En los portátiles el aumento de RPM lleva consigo un aumento en el consumo de batería, por esa razón esos discos trabajan a menos revoluciones.

¿SABÍAS QUE...?

Los discos duros de alto rendimiento que rotan a altas velocidades 10.000/15.000 RPM son más ruidosos, consumen y se calientan mucho más que un disco estándar. En ocasiones eso implica una vida útil más corta.

Tamaño del *buffer* o caché

La caché sirve como almacén entre un medio muy lento (la parte interna del disco la cual es mecánica y magnética) y uno rápido (la controladora de disco). Los datos se almacenan en el *buffer* y en caso de que se vuelvan a leer por segunda vez es posible que todavía estén allí, por tanto, no hace falta acceder al disco y la operación será mucho más rápida.

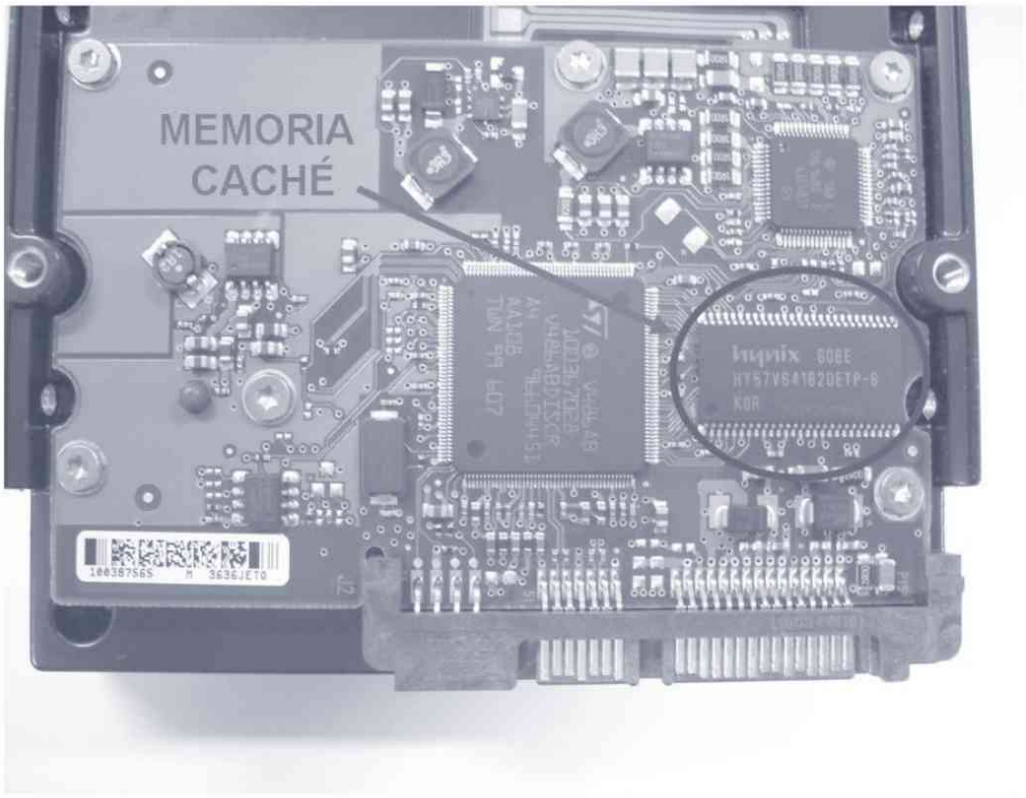


***Figura 1.27**. Detalle de la circuitería electrónica de un disco duro*

Obviamente, cuanto mayor sea la capacidad del *buffer* mejor será el rendimiento del disco. Por regla general los discos cuentan con 8, 16 ó 32 MB de *buffer*.

¿SABÍAS QUE...?

Un tamaño de *buffer* grande puede representar cierto peligro teórico. Un corte de corriente inesperado puede suponer una mayor pérdida de datos.

ESTRUCTURA LÓGICA DE UN DISCO

Las particiones

Prácticamente todos los discos incluso los dispositivos con memoria *flash* se pueden particionar.

IMPORTANTE

Una partición es una división del disco duro que puede tener un sistema de archivos independiente. Un disco puede tener varias particiones con varios sistemas de archivos.

Existen tres tipos de particiones principales:

- **Primaria**.
- **Extendida**. Las particiones extendidas pueden albergar particiones lógicas.
- **Lógica**.

Las particiones extendidas son necesarias porque si no un disco solamente podría tener 4 particiones.

¿SABÍAS QUE...?

Los sistemas operativos generalmente se instalan en particiones primarias.

En el particionamiento se siguen una serie de reglas y limitaciones que se van a ver a continuación:

- ✓ **Regla 1**: un disco solo puede tener hasta 4 particiones primarias.
- ✓ **Regla 2**: las particiones extendidas cuentan como si fueran particiones primarias.
- ✓ **Regla 3**: no puede existir más de una partición extendida.
- ✓ **Regla 4**: dentro de una partición extendida pueden existir una o varias particiones lógicas.

EJERCICIO 1.1

1. ¿Puedo tener un disco con 2 particiones primarias y 2 extendidas?
   No, según la regla 3 no puede existir más de una partición extendida.
2. ¿Puedo tener un disco con 2 particiones primarias y 5 lógicas?
   No, puesto que no existe ninguna partición extendida.
3. ¿Puedo tener en un disco 3 particiones primarias, 1 partición extendida y 4 particiones lógicas?
   Sí, siempre que las particiones lógicas estén dentro de la partición extendida.
4. ¿Puedo tener en un disco 7 sistemas de archivos diferentes o repetidos?
   Sí. El disco anterior podría tener todos esos sistemas.

IMPORTANTE

El formateo

El formateo implica la pérdida de información que había en el disco. Primero se particiona y luego se formatea lógicamente.

Las particiones activas

Las particiones primarias son las utilizadas para instalar los sistemas operativos. Si un equipo no tiene ninguna partición activa, al arrancar dará un fallo. El sistema operativo de la partición activa será el que se cargue al arrancar desde el disco duro.

RECUERDA

Para que un disco duro se pueda utilizar y arrancar tiene que tener al menos una partición primaria activada y con un sistema operativo instalado en ella.

El sector de arranque

Un disco se compone de un sector de arranque y una serie de particiones y, opcionalmente, espacio sin particionar.

El sector de arranque es el primer sector del disco (cabeza 0, cilindro 0 y sector 1). Dentro de él está la tabla de particiones y el *Master Boot* o gestor de arranque. Este programa lee la tabla de particiones y cede el control al sector de arranque de la partición activa. Como se ha dicho antes si no hay partición activa, el equipo da un error al arrancar.

***Figura 1.28**. Estructura del master boot record*

El sector de arranque tiene 512 *bytes* (446 + 64 + 2 = 512) como se puede observar en la figura anterior.

1.3.2 DISPOSITIVOS DE ALMACENAMIENTO ÓPTICO

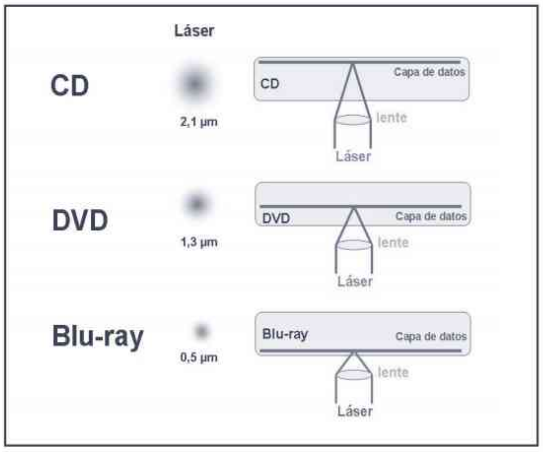


***Figura 1.29**. Comparativa entre los diferentes soportes ópticos*

Los dispositivos de almacenamiento óptico tienen una serie de ventajas frente a otros tipos de dispositivos:

- El coste por bit; su coste reducido hace que sean un producto sumamente utilizado.
- El soporte dura indefinidamente debido a que la lectura no desgasta el disco. La información no se degrada con el paso del tiempo. Tampoco disminuye la calidad con el tiempo salvo que se deteriore físicamente el soporte.
- Los campos magnéticos no afectan a los datos.
- Los materiales del soporte aguantan la humedad.
- Pueden aguantar golpes siempre que la superficie de datos no se dañe.

¿SABÍAS QUE...?

Existe un hongo de tipo Geotrichum que se alimenta del carbono y el nitrógeno de la capa plástica de policarbonato del CD y destruye las pistas de información grabadas en la capa de aluminio.

Los dispositivos de almacenamiento óptico, lectoras y regrabadoras, utilizan un haz láser para leer y escribir los datos en los soportes ópticos. Como se puede ver en la figura anterior, el láser del *Blu-ray* es mucho más preciso que el del DVD, y el del DVD es a su vez más preciso que el del CD (no hay nada más que ver el diámetro de ancho de los tres y su capacidad).

DISCOS O UNIDADES SSD

El termino SSD (*Solid State Drive*) tiene su traducción en "unidad de estado sólido". Aunque seguramente se les va a seguir denominando discos de estado sólido no tiene sentido llamarlos discos, puesto que ya no existe el disco propiamente dicho, sino que es sustituido por componentes electrónicos.

Estos discos o dispositivos de almacenamiento utilizan:

- **Memoria no volátil** como *flash*. Esta memoria tiene la ventaja de no ser volátil, no necesitar refresco y tener un bajo consumo eléctrico.
- **Memoria volátil** como la SDRAM, que le confiere sobre todo velocidad.

Una gran diferencia de estos discos frente a los tradicionales es que al no tener partes móviles la posibilidad de rotura o que se estropee por las vibraciones desaparece. Dada sus características, los tiempos de búsqueda y latencia son menores que los discos duros tradicionales.

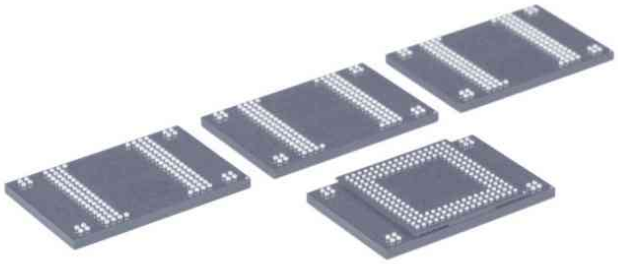


***Figura 1.30**. Memoria PATA SSD de Intel®. Fuente Intel®*

Ventajas de los discos SSD frente a los HD tradicionales

- ✓ Al no tener partes mecánicas el consumo de energía es mucho menor. También se produce menos calor.
- ✓ Son silenciosos al no tener partes mecánicas.
- ✓ Tienen un peso menor.
- ✓ El tiempo de búsqueda es constante frente al tiempo de búsqueda variable de los discos tradicionales.
- ✓ La lectura es mucho más rápida.
- ✓ El rendimiento no baja cuando el disco se va llenando.

Desventajas de los discos SSD frente a los HD tradicionales

- ✓ En lecturas y escrituras secuenciales pueden llegar a ser más lentos que los tradicionales.
- ✓ En caso de fallo la celda se destruye, con lo cual la posibilidad de recuperación es más remota.
- ✓ De momento estos discos son más caros pero en un futuro esto no será así.

***Figura 1.31**. Parte trasera de un disco SSD. Fuente Intel®*

1.4 LA FUENTE DE ALIMENTACIÓN

1.4.1 ¿QUÉ ES UNA FUENTE DE ALIMENTACIÓN?

La fuente de alimentación transforma la corriente alterna de la red en corriente continua, que es la que soporta un PC.

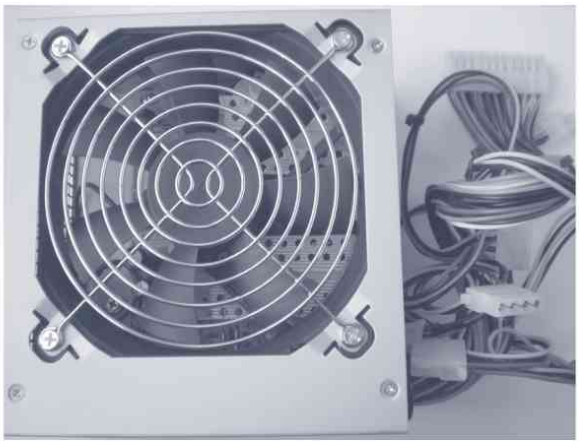


***Figura 1.32**. Fuente de alimentación*

1.4.2 CARACTERÍSTICAS DE LAS FUENTES DE ALIMENTACIÓN

Las fuentes que se utilizan en la actualidad son las fuentes ATX. Algunas características de una fuente de alimentación son las siguientes:

- **PFC** (*Power Factor Correction*): factor de corrección de potencia. Todas tienen PFC pero puede ser activo o no activo. Las fuentes con *active PFC* (activo) son más eficientes (95% o superior) y la calidad de la corriente es mejor, así como la reducción de la emisión de interferencias electromagnéticas.
- **Eficiencia**: normalmente la eficiencia la da el fabricante en %. Cuanto más eficiente sea la fuente de alimentación mejor. Más de un 80% ó 90% suelen ser valores aceptables.
- **Nivel de ruido**: cuanto menor sea el nivel de ruido mejor será la fuente. Las fuentes silenciosas tienen unos ventiladores de mejor calidad y de ahí su bajo nivel sonoro.
- **Conectores SATA**: cuantos más conectores SATA traiga la fuente mejor. De esa forma no habrá que utilizar adaptadores. Actualmente todos los discos duros y lectores ópticos son SATA.
- **Single fan**, **Dual Fan**...: número de ventiladores que tiene la fuente de alimentación. A mayor número de ventiladores más refrigerada estará.

RECUERDA

Las fuentes que no especifican PFC activo es porque no lo son (son PFC no activo). Las fuentes con PFC activo son mucho más caras y de mejor calidad.

Conectores ATX de las fuentes de alimentación

Existen dos tipos de conectores:

- ATX. Conector de 20 pines.
- ATX 2.2. Conector de 24 pines.

***Figura 1.33**. Conector hembra ATX*

- Conector ATX 12V con 4 y 8 pines.

***Figura 1.34**. Conector ATX 12V de 8 pines*

Las placas base que funcionan con conectores ATX de 24 pines suelen admitir conectores de 20 pines siempre que se estén conectados por los pines 1 y 13.

Las fuentes de alimentación, además de con el botón de encendido, también pueden activarse mediante el módem o la tarjeta de red.

RECUERDA

No confunda un conector 24 + 4 con uno 20 + 4. El conector extra de 4 pines de 12 voltios es para alimentar al micro mientras que esos 4 pines extra son para reforzar voltajes que suelen utilizar algunos componentes.

EJERCICIO 1.2

POSIBLE FALLO EN UNA FUENTE DE ALIMENTACIÓN. LA PRUEBA DEL VENTILADOR

Esta prueba no sirve para ver si la fuente de alimentación funciona correctamente, para ello deberíamos de verificar las tensiones. Esta prueba nos servirá para ver si la fuente no está muerta y en ese caso le podríamos echar la culpa de un mal funcionamiento del equipo a otro componente (micro, placa...). En muchas ocasiones cuando no se enciende el equipo es una forma rápida de encontrar el fallo (fuente rota).

Paso 1. Desconectar la fuente de la corriente.
Siempre hay que manipular los equipos con la fuente desconectada (desconectando el cable de corriente y el botón de encendido si tiene).

Paso 2. Puentear la fuente de alimentación.
Con un clip u otro objeto hay que puentear el cable verde (PS_ON) con cualquier negro (GND) como se muestra en la figura.

***Figura 1.35**. Puenteo del conector macho ATX*

Paso 3. Conectar la fuente de alimentación.
Conectar el cable de alimentación y pulsar el botón de encendido.

***Figura 1.36**. Encendido de la fuente de alimentación*

En este momento pueden pasar dos cosas:

- **El ventilador da vueltas**. Esto quiere decir que es posible que la fuente esté funcionando correctamente.
- **El ventilador no funciona**. Signo de que la fuente está averiada.

EJERCICIO 1.3

TESTEO DE LAS TENSIONES EN UNA FUENTE DE ALIMENTACIÓN

Este ejercicio va a servir para comprobar que la fuente de alimentación proporciona los voltajes esperados. Para ello se va a utilizar un polímetro y algún clip para puentear la fuente. La fuente tiene que estar funcionando para poder medir los voltajes.

Paso 1. Desconectar la fuente de la corriente.
Siempre hay que manipular los equipos con la fuente desconectada (desconectando el cable de corriente y el botón de encendido si tiene).

Paso 2. Puentear la fuente de alimentación.
Con un clip u otro objeto hay que puentear el cable verde (PS_ON) con cualquier negro (GND).

Paso 3. Conectar la fuente de alimentación.
Conectar el cable de alimentación y pulsar el botón de encendido.

Paso 4. Conectar y configurar el polímetro.
Colocar las puntas en la posición correspondiente y el conmutador rotativo en el rango adecuado a la tensión que, en este caso serán 20 voltios, en corriente continua, pues el valor máximo que se va a medir son 12 voltios.

Figura 1.37. Detalle de la configuración del rotor conmutativo

En nuestro caso 20 voltios.

Paso 5. Medir los voltajes.
Hay que medir los voltajes colocando la punta negra en el cable negro del conector ATX y la punta roja en el cable que se quiere testear.

El voltaje a veces no es exacto al valor de referencia pero tiene que ser muy parecido. Si los voltajes medidos son muy diferentes al de referencia o fluctúan, la fuente podría estar averiada.

EJERCICIO 1.4

TESTEO DE LAS TENSIONES EN UNA FUENTE DE ALIMENTACIÓN CON UN TESTER

Los *tester* de fuentes de alimentación son herramientas específicas que permiten testear todos los conectores de una fuente de alimentación de una forma rápida. Como ya se ha visto con anterioridad, no es difícil testear los voltajes de una fuente de alimentación pero tampoco es una operación muy rápida. Una herramienta de este tipo va a permitir al técnico ganar tiempo y precisión en este tipo de funciones.

***Figura 1.38**. Tester de fuentes de alimentación*

Para testear la fuente basta con realizar la conexión macho-hembra de los conectores de la fuente y el *tester*. Una vez conectados se pone en funcionamiento la fuente conectándola a la corriente y se comprueban los indicadores led.

***Figura 1.39**. Tester conectado a una fuente de alimentación*

En este caso se puede ver que los led indican que la fuente está en correcto funcionamiento.

Con este tipo de aparatos se pueden testear los conectores Molex, ATX, ATX 12V, SATA y Berg, entre otros.

RECUERDA

Para medir los voltajes de una fuente de alimentación de una forma rápida existen *testers* que permiten insertar en ellos todos los conectores ATX de 24 y 20 pines, Molex o conector de alimentación SATA y realizan de una manera rápida y sencilla la comprobación (incluso informando mediante leds verdes/rojos su funcionamiento).

1.5 LOS PERIFÉRICOS

El avance de la Informática en la actualidad tiene su más visible forma de expresión en la enorme cantidad de artilugios tecnológicos que surgen en torno al ordenador y que nos permiten cada vez más aumentar la interacción con éste, así como la cantidad de procesos que se pueden desarrollar.

Llamamos periférico a cualquier dispositivo informático que no es parte del ordenador esencial (procesador-memoria interna-*buses*), de su CPU, pero está situado relativamente cercano a ésta (en la periferia) y son de gran utilidad e incluso imprescindibles para su uso y manejo.

Un sinónimo empleado habitualmente es el de dispositivo externo de entrada-salida, ya que permiten realizar tareas de entrada y salida de información complementando las que realizan la CPU.

Se consideran periféricos tanto a los dispositivos a través de los cuales la CPU se relaciona con el mundo exterior como a los sistemas de almacenamiento, como se verá posteriormente al describir su clasificación. Algunos periféricos están montados dentro del chasis y ya han sido objeto de estudio, como la unidad de disco duro, la unidad lectora de CD-ROM, etc.

Es fundamental conocer toda la gama de periféricos que existen en la actualidad así como sus características y poder argumentar su elección idónea, ya que eso conlleva a mejorar el rendimiento y manejo del ordenador al permitirnos una enorme gama de procesos y actividades.

¿SABÍAS QUE...?

Las primeras computadoras carecían de monitor y su forma de comunicarse era bien por luces en un panel de control o por impresión.
Por otro lado, hasta 1981 no se lanzó el primer ordenador que incluía ratón (Xerox Star 8010).

Los periféricos son imprescindibles en la explotación y uso de un sistema informático, ya que son los elementos con los que éste interactúa.

Todo periférico tiene dos partes claramente diferenciadas:

- **Parte mecánica**. Formada por dispositivos electromecánicos (conmutadores, electroimanes, motores y otros), que son controlados por elementos eléctricos.
- **Parte electrónica**. Encargada de controlar las ordenes que lleguen desde la CPU y de generar las órdenes necesarias para manejar esas partes mecánicas.

Todo dispositivo de entrada-salida tendrá que "traducir" la información que llega desde la CPU (salida) o envía hacia la misma (entrada) en forma de señales codificadas que se detectan, transmiten, interpretan, procesan y almacenan de forma transparente.

En ocasiones algunos periféricos requieren de unos controladores hardware que se presentan en forma de tarjetas y que suelen incluir una potente electrónica para descargar de tareas a la CPU. También necesitan de un *driver* o "controlador de dispositivo", que es un pequeño programa que facilita la comunicación entre el Sistema Operativo y el periférico, abasteciendo a la CPU de instrucciones para poder comunicarse con el nuevo dispositivo.

Existen diversas clasificaciones de los periféricos atendiendo a múltiples criterios, pero la más clara y extendida es atendiendo a su funcionalidad:

- **Periféricos de entrada**. Aquellos que introducen información en el ordenador (teclado, ratón, detectores ópticos, escáner, micrófono, etc.).
- **Periféricos de salida**. Aquellos que muestran información generada o contenida en el ordenador (monitor, impresora, altavoz, etc.).
- **Periféricos de E/S o mixtos**. Incluyen en un solo dispositivo elementos para dar la entrada y salida de información (pantalla táctil, impresora multifuncional, cámara *ip*, etc.).
- **Periféricos de comunicación**. Estarían dentro de la categoría de entrada/salida, pero dado su carácter específico merecen una categoría aparte (módem, *switch*, *router* y otros).
- **Periféricos de almacenamiento**. Pueden también considerarse como periféricos de E/S pero también merecen de una categoría propia.

Tabla 1.3 Clasificación de periféricos

Periféricos de ENTRADA	Teclado, ratón, detectores ópticos (de marcas, de barras impresas, de carácteres manuscritos o impresos, de huellas digitales, de pupilas, escáner de imágenes, cámara digital de fotos o vídeo, *webcams*), micrófono, sensores (de movimiento, de luz, etc.), lápiz óptico, *joystick, gamepad,* tableta gráfica o digitalizadora.
Periféricos de SALIDA	Monitor (CRT, LCD o Plasma), impresora (inyección, láser, térmica, etc.), visualizadores o *displays, plotter,* altavoz, auricular.
Periféricos de ENTRADA-SALIDA o MIXTOS	Pantalla táctil, impresora multifuncional, dispositivos de realidad virtual (traje, guante, gafas, casco, CAVE, etc.).
Periféricos de ALMACENAMIENTO	**Tecnología óptica**: dispositivos lectores/grabadores y soportes de CD, DVD, *Blu-Ray*. **Tecnología magnética**: cintas y discos magnéticos, discos duros, etc.
Periféricos de COMUNICACIÓN	Modem, *hub, switch, router, router adsl,* etc.

1.6 EQUIPAMIENTOS Y TECNOLOGÍAS APLICADAS A SISTEMAS INFORMÁTICOS DE TELECOMUNICACIONES

Los dispositivos de comunicaciones permiten que el ordenador se conecte con otros sistemas informáticos a través de diversos medios cableados o inalámbricos.

Entre los principales periféricos de comunicación destacan los siguientes:

- **Módem**. Permite conectar ordenadores remotos usando la línea telefónica tanto analógica como móvil. Se encarga, como su propio nombre indica, de **mo**-dular y **dem**-odular, convirtiendo las señales digitales del ordenador en señales analógicas adaptadas al medio y viceversa. Actualmente son muy comunes los módem USB que dan acceso a Internet los cuales permiten tener conectado el equipo en cualquier lugar. Estos módem cuentan con memoria interna, son autoinstalables y permiten conexiones HSDPA, UMTS, EDGE o GPRS.
- **Tarjeta de Red**. Permite la conexión entre diferentes ordenadores a través de un medio cableado o inalámbrico para compartir información o recursos. Cada tarjeta de red tiene un número de identificación de 48 bits expresado en hexadecimal por seis números de dos cifras hexadecimales separados por dos puntos llamada **dirección MAC**, que es única y viene de fábrica. Es un elemento fundamental para poder formar parte de una red local o conectarse a la misma. Se puede presentar de múltiples formas: como una tarjeta cableada Ethernet interna, una tarjeta Wi-Fi interna, una tarjeta PCMCIA de red o un adaptador USB-Wi-Fi.
- **Concentrador** (*Hub*). Permite canalizar el cableado de una red local para ampliarla y repetir la misma señal a través de diferentes puertos. El funcionamiento está basado en repetir un mismo paquete de datos en todos sus puertos de manera que todos los equipos conectados accedan a la misma información y al mismo tiempo.
- **Conmutador** (*Switch*). Interconecta dos o más partes de una red local funcionando como un puente que transmite datos de un segmento de la red a otro. El mismo dispositivo tiene capacidad de aprender y almacenar direcciones de red de componentes de la misma, de forma que, a diferencia de lo que ocurre con el concentrador, el *switch* hace que la información dirigida a un dispositivo vaya sólo desde un puerto origen a otro destino.
- **Enrutador** (*Router*). Permite que varias redes u ordenadores se conecten entre sí. El *router* tiene múltiples usos entre los que el más común es que en una casa u oficina varios ordenadores aprovechen la misma conexión a Internet. De esta forma, el *router* funciona como receptor de la conexión de red para encargarse de distribuirla a todos los equipos.

Existen también toda una gama de periféricos de comunicación en constante avance como son el **teléfono IP** (para Skype, por ejemplo), el **adaptador USB-bluetooth**, un **hub USB** o determinadas **antenas domésticas**.

RESUMEN DEL CAPÍTULO

En este capítulo se explica el funcionamiento básico de un sistema informático (estructura funcional) y la estructura física (hardware comercial).

Se estudian uno a uno los componentes de la arquitectura de von Neuman: la unidad central de proceso, la memoria, los *buses* y los subsistemas de entrada-salida, siempre desde un punto de vista funcional u operativo.

En el estudio del hardware comercial se van a tratar todos los componentes que se encuentran dentro del chasis, incluido él mismo.

Los dispositivos de almacenamiento se van a estudiar en un apartado independiente, dado que se verán más en profundidad.

En este tema también se profundiza en la fuente de alimentación y a ella se le dedica un apartado del tema.

Por último, se enumeran y detallan los principales componentes fuera del chasis (los periféricos), clasificándolos para tal fin en periféricos de entrada, salida, entrada-salida o mixtos y almacenamiento.

EJERCICIOS PROPUESTOS

- **1.** Elabore una línea cronológica donde señale desde el ábaco hasta la actualidad los principales acontecimientos históricos relacionados con la historia de la informática y de los ordenadores. Investigue qué aportaciones se han llevado a cabo por españoles.
- **2.** Investigue todo lo que pueda sobre el conector eSATA. Realice un informe detallado de sus características.
- **3.** Investigue sobre los principales sistemas de codificación de color (RGB, CMYK y otros), su modo de empleo y para qué se emplean.
- **4.** ¿Cuáles son las ventajas e inconvenientes de los formatos gráficos de mapa de bits frente a los formatos vectoriales? Investigue sobre los diferentes estándares en el mercado.
- **5.** Realice una comparativa de los micros core i3, i5 e i7.
- **6.** Investigue en la Red cuáles son las arquitecturas RISC y CISC. Enumere ventajas e inconvenientes de la arquitectura RISC frente a la CISC. Busque ejemplos de máquinas actuales que basen su arquitectura en cada una de ellas.
- **7.** ¿Qué es el *pipeline*? Busque otras técnicas similares que persigan optimizar el procesamiento del microprocesador.

8. Estudie las características, ventajas e inconvenientes de la tecnología magnética frente a la óptica y averigüe dispositivos y soportes de cada tipo.

9. Investigue sobre las características técnicas del suministro eléctrico y la fuente de alimentación de los ordenadores que emplee (tipo de fuente, consumo en watios, conectores que posee, valores de corriente que maneja, etc.).

10. Estudie los sistemas de refrigeración por aire y líquido indicando componentes, funcionamiento, precios y ventajas e inconvenientes. Si los recursos lo permiten, trate de llevar a cabo la instalación de ambos sistemas en grupos de trabajo elaborando un material multimedia (vídeo y/o imágenes) de dicho proceso.

11. *Overclocking*. Investigue en qué consiste y cómo llevarlo a cabo.

12. Investigue sobre las nomenclaturas DDR2-xxx y PC2-yyyy, indicando qué valores indican las cantidades *xxx* e *yyyy*. Averigüe los modelos más comercializados en la actualidad, así como sus características técnicas.

TEST DE CONOCIMIENTOS

1 Elija la afirmación falsa:

a) Los zócalos o *sockets* se emplean en equipos de arquitectura abierta.
b) Las ventajas de la refrigeración líquida son la refrigeración silenciosa y el impacto visual en algunos casos.
c) Un sistema informático (SI) es un conjunto de dispositivos, con al menos una CPU o unidad central de proceso.
d) El modelo básico de arquitectura empleada en los computadores digitales fue establecido en 1946 por Paul Neumann.

2 Elija la afirmación falsa:

a) El elemento central del hardware de un Sistema Informático es la UCP o Unidad Central de Proceso.
b) Una variante del sistema de enfriamiento líquido consiste en utilizar aceite en vez de agua.
c) El *Southbridge* se une al *Northbridge* mediante su propio *bus* denominado *Hub Link*.
d) Las cajas Mini-ITX son un poco más grandes que las Micro-ATX.

3 Elija la afirmación falsa:

a) El *Socket* PGA es un *socket* clásico utilizado ya con los micros 386 y 486.
b) El modelo básico de arquitectura empleada en los computadores digitales fue establecido en 1946 por John von Neumann.
c) El *bus* que comunica el microprocesador con el *Northbridge* se denomina *Front Side Bus*.
d) Un microprocesador es un circuito integrado compuesto unos miles de transistores.

4 Elija la afirmación falsa:

a) Hoy día una CPU puede estar soportada por uno o varios microprocesadores, así como un microprocesador puede soportar una o varias CPU.
b) La idea de von Neumann consistió en conectar permanentemente las unidades de las computadoras, siendo coordinado su funcionamiento por un elemento de control.
c) En caso de querer refrigeración extrema, es conveniente emplear placas Peltier.
d) Energy Star identifica cualquier producto que use energía, en especial los equipos informáticos.

5 Elija la afirmación falsa:

a) PCB son las iniciales de *Principal Circuit Board*.
b) Un nanómetro es la millonésima parte de un milímetro.
c) La unidad de control de la máquina de von Newmann tenía como función la de leer, una tras otra, las instrucciones-máquina almacenadas en la memoria principal.
d) El *overclocking* es un aumento de la velocidad del microprocesador por encima del establecido en el estándar de fábrica.

6 Elija la afirmación falsa:

a) Las caché L2 y L3 o de nivel 2 y 3 están conectadas al micro mediante el *Back Side Bus*.
b) Los primeros microprocesadores no tenían ningún sistema de disipación del calor.
c) Las prestaciones de un *bus* vienen determinadas por el ancho del mismo y su velocidad.
d) Un programa es un conjunto de instrucciones que son almacenadas secuencialmente en posiciones o direcciones sucesivas de memoria y que serán ejecutadas una detrás de otra.

7 Elija la afirmación falsa:

a) El *bus* que comunica el microprocesador con el *Northbridge* se denomina *Norbridge Bus*.
b) Muchas de las cajas de los ordenadores están fabricadas con chapa troquelada.
c) Las cajas Mini-ITX son más pequeñas que las Micro-ATX.
d) Las cajas Pico-ITX son más pequeñas que las Mini-ITX.

8 Elija la afirmación falsa:

a) La memoria RAM es no volátil y muy rápida.
b) La fuente de alimentación transforma la corriente eléctrica alterna procedente del sistema eléctrico en corriente continua.
c) Los módulos GDDR son chips de memoria insertados directamente en las tarjetas gráficas.
d) Un microprocesador es un circuito integrado compuesto por millones de transistores.

9 Elija la afirmación falsa:

a) Un *barebone* es un equipo de reducidas dimensiones.
b) El formato más empleado de placa base es el ATX junto al mini-ATX.
c) El puerto PCIe está formado por uno o más enlaces punto a punto de tipo bidireccional.
d) Los *heatpipes* son unos tubos que absorben el vapor del aire introducido en su interior, el cual se condensa y, a su vez, absorbe calor para luego evaporarse en otro extremo.

10 Elija la afirmación falsa:

a) Energy Star identifica a productos que usan eficientemente la energía.
b) El *chipset* en la actualidad está formado básicamente por un par de chips denominados *NorthBridge* y *SouthBridge*.
c) El *NorthBridge* une los componentes de mayor velocidad de transferencia.
d) Un nanómetro es la milmillonésima parte de un milímetro.

2 Arquitectura software de los equipos informáticos de telecomunicaciones

OBJETIVOS DEL CAPÍTULO

- ✓ Conocer las características del software.
- ✓ Catalogar los tipos de software según su tipo de licencia, distribución y propósito.
- ✓ Analizar las necesidades específicas de software asociadas al uso de sistemas informáticos en diferentes entornos productivos.
- ✓ Proporcionar diferentes soluciones software para determinados requisitos.
- ✓ Comparar diferentes aplicaciones.
- ✓ Conocer el concepto de sistema operativo.

2.1 CONCEPTO DE SISTEMA OPERATIVO

2.1.1 EL ENTORNO OPERATIVO

Con el término **entorno operativo** englobamos al **sistema operativo**, **a su interfaz de usuario asociada y algunas aplicaciones** que suelen venir con él (administrador de archivos, programas de configuración y optimización y otros).

El sistema operativo es el software básico que controla una computadora. A grandes rasgos tiene tres grandes **funciones**: **coordinar y manipular el hardware** del sistema informático (memoria, impresoras, unidades de almacenamiento, periféricos, etc.), **organizar los archivos** en los dispositivos de almacenamiento y **gestionar los diferentes errores** que se generen.

2.1.2 FUNCIONES DE LOS SISTEMAS OPERATIVOS

A continuación vamos a enumerar las principales funciones de los sistemas operativos:

- **Control de Recursos**. Coordinar y manipular el hardware del sistema informático. Se encarga del funcionamiento coordinado de todos los componentes para que funcionen como una sola máquina.
- **Control y Manejo de los dispositivos de E/S**. Controla y organiza los dispositivos conectados al sistema.
- **Ejecución y secuenciación de tareas**. Controla la ejecución de varios programas a la vez, repartiendo los recursos del ordenador (procesador, memoria, espacio almacenamiento…) a los distintos programas que se están ejecutando.
- Ofrece una **base estándar sobre la que ejecutar** otros programas permitiendo diseñar software de aplicación sin necesidad de tener en cuenta el hardware particular de cada sistema.
- Administra y mantiene los **sistemas de archivo de disco**, permitiendo guardar la información en las unidades de almacenamiento en forma de ficheros y directorios.
- Permite la interacción entre el sistema y los usuarios, permitiendo su manejo de forma fácil e intuitiva a través de la **interfaz gráfica** o **GUI**.
- **Detecta e informa** al usuario de los errores que se produzcan.

Un buen sistema operativo aprovechará toda la potencia que ofrece el hardware tratando de que funcione de forma óptima.

Para poder ejecutar cualquier otra aplicación es necesario tener cargado el sistema operativo con el que es compatible. Para ello, el sistema operativo es el primer programa o software que se carga y ejecuta al arrancar o reiniciar el sistema siendo automática su ejecución.

Los programas son creados para que funcionen en una o varias **versiones y/o distribuciones** del mismo sistema operativo.

En un mismo sistema informático se pueden tener varios sistemas operativos, aunque sólo uno puede cargarse a la vez, eligiéndose mediante un menú de arranque, como **GRUB** (para entornos Linux).

2.1.3 COMPONENTES DE UN SISTEMA OPERATIVO

Todo sistema operativo, SO en adelante, tiene una serie de módulos o componentes encargados de diversas **funciones**:

1. **Gestión de Procesos**. Un proceso es un programa en ejecución que necesita recursos para realizar su tarea: tiempo de CPU, memoria, archivos, dispositivos de E/S.

   El SO será el responsable de parar y reanudar los procesos y ofrecer mecanismos para que se comuniquen y sincronicen.

   La gestión de procesos podría ser comparable a un trabajo de oficina. Se puede tener una lista de tareas a realizar y a éstas fijarles distinto grado de prioridades. Debemos comenzar haciendo las tareas de prioridad mayor primero y, cuando se terminen, seguir con otras de prioridad inferior. Una vez realizada la tarea se elimina de la lista. Esto puede traer un problema, que las tareas de más baja prioridad tarden mucho en ejecutarse, pero existen mecanismos para controlar esto.

2. **Gestión de la Memoria Principal**. El SO es responsable de conocer las partes de la memoria usadas y por quién, controlar el espacio libre, decidir qué procesos se cargarán en memoria cuando haya espacio libre y asignar o reclamar espacio de memoria cuando sea necesario.

3. **Gestión del almacenamiento secundario**. Se encarga de traspasar y mantener en memoria secundaria aquella información de memoria principal que no sea necesaria. También se encarga de planificar los discos, gestionar el espacio libre y asignar el almacenamiento.

4. **Gestión de la entrada-salida**. El SO debe gestionar el almacenamiento temporal de los dispositivos de E/S así como servir las interrupciones de estos.

5. **Gestión de Archivos**. Los archivos son colecciones de información que almacenan programas y datos como imágenes, textos, etc.

   El SO es el responsable de construir y eliminar archivos y directorios, ofrecer funciones para manipular archivos y directorios, realizar copias de seguridad de archivos, etc.

6. **Mecanismos de Protección**. Deberán ofrecer mecanismos que controlen el acceso de los programas o los usuarios a los recursos del sistema.

7. **Gestión de Comunicaciones**. Controlan el envío y recepción de información a través de las interfaces de red, crean y controlan puntos de comunicación y conexiones virtuales entre aplicaciones en ejecución local o remota.

8. **Utilidades de Sistema**. Ofrecen un entorno útil para el desarrollo y ejecución de programas dando soporte a diferentes lenguajes de programación, controlando el estado del sistema, etc.

***Figura 2.1**. Componentes del sistema operativo*

2.1.4 ENTORNOS OPERATIVOS EN LA ACTUALIDAD

Cualquier sistema operativo actual está en completa evolución. Se puede decir que la cuota de mercado de los sistemas operativos de sobremesa se la llevaría Windows®, Linux y, en menor medida, el sistema operativo de Apple.

***Figura 2.2**. Logos de sistemas operativos libres basados en Linux*

Los sistemas operativos antes citados no son funcionales en los dispositivos móviles como puedan ser *smartphones*, MID, *tablets*, PDA, etc. Estos dispositivos necesitan un sistema operativo ligero y que cuente con muchos de los servicios que proporcionaban los sistemas operativos tradicionales. Entre estos sistemas operativos móviles destacan **Android**, **BoottoGecko** (**B2G**), **BADA**, **MeeGo**, **Symbian OS**, **Palm OS**, **iPhone OS** y **Windows® Mobile**.

***Figura 2.3**. Logos de sistemas operativos libres de dispositivos móviles*

¿SABÍAS QUE...?

Google Chrome está pensado para *netbooks* y es código abierto. La interfaz de usuario es mínima ya que están pensados básicamente para trabajar sobre Internet. Pretende rediseñar la arquitectura de seguridad que lo soporta para estar blindado de virus y de software malicioso.

***Figura 2.4**. Ficha personal de Linux Torvalds. Fuente: Kylehase*

Hay que decir que muchos sistemas operativos móviles basan su filosofía en Linux. Esto tiene mucho de lógica dado que es un sistema operativo libre y cualquier desarrollo partiendo desde cero sin tener en cuenta lo ya realizado por Linux no tiene mucho sentido.

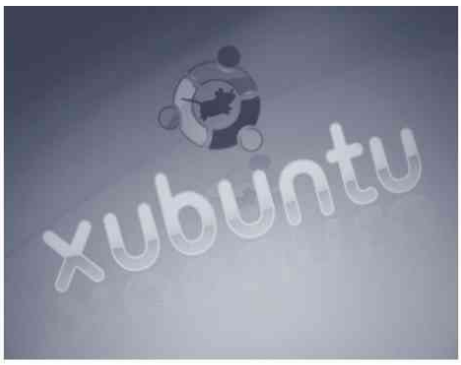


***Figura 2.5**. Instalación de XUbuntu. Fuente: Rafa Espada*

***Figura 2.6**. Mac OS X Leopard. Fuente: Juanpol (Juan Pablo Olmo)*

El futuro de los sistemas operativos está basado en el *cloud computing* trasladando lo que eran los servicios que ofrecía nuestro sistema a Internet. En un futuro será Internet la que proveerá de servicios y almacenará los datos de los clientes. Los equipos informáticos harán de caché y trabajarán con esos datos, pero su almacenamiento realmente estará en servidores de Internet. Habrá muchos servicios basados en la web y los clientes podrán acceder a ellos teniendo un abanico de posibilidades muy variado y seguramente se establecerá el sistema de pago por consumo.

Los sistemas operativos del futuro se van a basar cada vez más en el navegador (el primero en girar hacia esta filosofía fue Google Chrome y Windows® 8 se está desarrollando de esta manera). Muchas personas, aunque reconocen las bondades de esta tecnología, no son partidarias de esta idea pues se genera una dependencia de los proveedores de servicios y del acceso a Internet.

2.2 TIPOS DE APLICACIONES INFORMÁTICAS

Llamamos *software de aplicación* y, en general, *aplicación*, a aquel tipo de software diseñado como una herramienta que permita al usuario realizar una tarea específica, a diferencia de los sistemas operativos, que hacen funcionar al ordenador, o las utilidades, que realizan tareas de mantenimiento o uso general y el software de programación, con el que se crean los programas informáticos.

En general, una aplicación es un programa compilado o interpretado escrito en algún lenguaje de programación que necesita de un sistema operativo soporte para poder funcionar y requiere unas condiciones determinadas para su instalación y ejecución, y que hacen referencia a espacio en disco, procesador y memoria RAM.

Suelen ser aplicaciones que solucionan ciertas tareas humanas complicadas como la gestión de un almacén, la redacción de documentos o el diseño de planos, donde la máquina se convierte en una enorme ayuda evitando en ocasiones tareas repetitivas o tediosas.

Este tipo de software se puede desarrollar en forma de **software estándar y de uso generalizado** o como **software a medida**, siendo estos últimos más costosos pero ofreciendo mayor potencia, ya que están exclusivamente desarrollados para resolver un problema específico.

Dentro de las aplicaciones también podemos hablar de aplicaciones **verticales** cuando su campo de empleo es específico, para uso cerrado por parte de un perfil determinado de usuarios (abogados, administradores, médicos, policías, etc.) y de aplicaciones **horizontales** cuando son de utilidad para un amplio sector de usuarios.

Algunas empresas agrupan diversos programas de uso similar o complementario entre sí, para que forme un conjunto de programas a los que se les llama **paquete integrado** o **suite**.

Existen paquetes integrados o *suites* de diversas índoles como **herramientas ofimáticas** (Microsoft Office®, OpenOffice, etc.) o **Suites Gráficas** (Corel®, Adobe®, etc.).

***Figura 2.7**. Imágenes de suites ofimáticas y gráficas*

Todas las aplicaciones están desarrolladas para ser ejecutadas en una única plataforma o sistema operativo, con el que son compatibles y se pueden comunicar, y no son funcionales directamente en las otras, aunque muchas aplicaciones ofrecen diferentes versiones para distintas plataformas.

Son **software** de aplicación:

- **Aplicaciones de productividad empresarial**. Son aplicaciones empleadas para fines empresariales de mejora de la productividad en diversos sectores. Son ejemplos las aplicaciones ofimáticas, aplicaciones gráficas, gestión de proyectos, etc.
- **Aplicaciones de ámbito doméstico**. Son aplicaciones usadas sin un fin profesional para el entretenimiento o la formación. Juegos, Enciclopedias Multimedia, etc.
- **Aplicaciones profesionales horizontales**. Diseñadas para gestionar y ejecutar una función o proceso empresarial de forma estándar. Engloban aplicaciones de contabilidad profesional, gestión de recursos, diseño web y otras.
- **Aplicaciones verticales**. Software para la realización de unas determinadas funciones concretas dentro de un sector determinado.
- **Aplicaciones utilitarias**. Son programas que realizan una tarea muy específica siendo de menor tamaño, coste y complejidad que todas las anteriores. Serían aplicaciones de rendimiento y diagnóstico, compresores, antivirus o programas de grabación.

2.3 LICENCIAS DE SOFTWARE

Una **licencia de software** es un contrato en el que se especifican todas las normas que rigen el uso de un determinado programa, entre el propietario de la licencia, que puede ser el autor o titular de los derechos de explotación o distribución del producto, y el que la adquiere, usuario o empresa, que empleará la aplicación cumpliendo una serie de términos y condiciones establecidos en forma de cláusulas en dicho contrato.

En estas cláusulas se determinan entre otras cosas el **plazo de cesión de los derechos** (6 meses, un año, dos años, etc.), el **ámbito geográfico** de validez del contrato, los **límites en la responsabilidad por fallos**, el **tipo de mantenimiento** que se le da soporte y los **compromisos** que debe adquirir el propietario (número de copias licitadas, no cesión del programa a otros o incluso la no reinstalación de la aplicación en equipos distintos al original).

Las licencias de uso de software generalmente caen en alguno de estos tipos:

- **Licencia propietaria**. Uso en una o varias máquinas por el pago de un precio.
- **Shareware**. Uso limitado en tiempo o capacidades tras el cual habrá que pagar un precio.
- **Freeware**. Uso y copia ilimitados con precio cero.
- **Software libre**. Permite el uso, copia, modificación y distribución libre con acceso al código fuente.

La siguiente tabla resume los tipos de software que hay según su licencia de uso, modificación, copia y redistribución, así como el coste y las posibles limitaciones.

Tabla 2.1 Tipos de licencias software

Tipo de licencias de software	Limitaciones	Precio cero	Permiso de copia y redistribución	Código fuente y permiso para modificarlo (sin ánimo de lucro)	Código fuente y permiso para modificarlo (con fines comerciales)
Propietario	Ninguna.	No	No	No	No
Shareware o evaluación	No 100% funcional. Uso por tiempo limitado.	Sí	Sí	No	No
Freeware	Ninguna.	Sí	Sí	No	No
Semilibre	Ninguna.	Sí	Sí	Sí	No
Libre/*Open Source*/GPL	Ninguna.	Sí*	Sí	Sí	Sí

(*) Hay veces que dentro de un mismo producto se mezclan algunas partes libres y otras no (sobre todo distribuciones de Linux). Es habitual que estos productos tengan un precio no cero debido a las partes que no son libres.

2.3.1 CLASIFICACIÓN DE LAS LICENCIAS SOFTWARE

Las licencias pueden ser de **usuario final o de distribuidor** para el caso de una empresa que se encargue de su distribución.

Según los derechos que cada autor reserva sobre su obra podemos tener licencias:

1. **Licencia de Software de Código Abierto con permisos**. Permite crear una aplicación derivada sin que requiera protección alguna. Ejemplos: *PHP License v.30*, *Apache Software License v.1.1.*, *Perl License*, *etc*.
2. **Licencia de Software de Código Abierto Robustas (con restricciones)**. Aplican determinadas restricciones a las obras derivadas. Pueden ser:
   - 2.1. **Robustas o con restricciones fuertes**, **CopyLeft fuerte**. **Licencias GPL**. La Licencia Pública General (*GPL*), contiene una cláusula que obliga a que las obras derivadas o modificaciones posteriores se deban licenciar bajo los mismos términos y condiciones de la licencia original.

     Adopta el principio de la no ocultación, respaldando el concepto moral que establece que todo software desarrollado con el uso de material licenciado bajo GPL debe estar disponible para ser compartido por todos.

     Ejemplos: *OpenSSL License*, *GNU General Public License v.2.0*, *etc*.

2.2. Débiles o con restricciones débiles. CopyLeft Débil, Suave o Híbrido. Licencia LGPL.

La Licencia Pública General Menor (*Lesser GPL*), es una modificación de la licencia GPL, e indica que las obras derivadas deben licenciarse bajo los mismos términos aunque las modificaciones posteriores pueden ser licenciadas bajo otros términos y condiciones distintas.

La LGPL permite que los desarrolladores usen programas bajo la GPL o LGPL sin estar obligados a someter el programa final bajo dichas licencias.

Ejemplos: *Mozilla Public License*, *Open Source License*, *etc.*

3. **Licencias de software de Código Cerrado**. También se conocen con el nombre de **software propietario** o **privativo**. En ellas los propietarios establecen derechos de uso, distribución, redistribución, copia, modificación, cesión y cualquier otra consideración que estimen oportuna.

   Este tipo de licencias no permiten que el software sea modificado, desensamblado, copiado o distribuido fuera de lo estipulado en las condiciones de la licencia incurriéndose en tal caso en lo que se conoce como la piratería de software.

   Suelen ofrecer servicios de soporte técnico y actualizaciones durante el tiempo de vida del producto otorgado en la licencia.

4. **Software de dominio público** (**sin licencia**). En este tipo de aplicaciones se permite el uso, copia, modificación y distribución del producto con o sin fines de lucro.

   Aquí se incluye la **licencia BSD** (Distribución de Software de Berkeley), que no impone ninguna restricción a los desarrolladores de software en lo referente al uso posterior del código en derivados y licencias de estos programas.

¿SABÍAS QUE...?

Si una empresa o un particular emplea el modelo de desarrollo de **código fuente abierto**, entonces las licencias de código abierto sin restricciones tales como la licencia BSD son más aconsejables que las licencias de software libre tales como la GPL. Las licencias sin restricciones permiten a los desarrolladores de software más libertad a la hora de utilizar el código recogido bajo la licencia para desarrollar software nuevo y para elegir los términos de la licencia bajo los que se regirá su programa.

Las licencias propietarias restringen en gran medida las libertades del usuario, a diferencia de las licencias libres. En el caso de las licencias con **copyleft**, sus restricciones buscan precisamente garantizar la libertad del software. En ningún caso se puede hablar, basado netamente en términos de la licencia, de que los software con licencias libres son más convenientes o no que los de licencia propietaria.

Lo que sí es cierto es que, en ocasiones, las libertades están fuertemente restringidas en el software de licencia propietaria. En muchos casos existen cláusulas que restringen fuertemente las libertades del usuario y otorgan privilegios abusivos a la empresa proveedora.

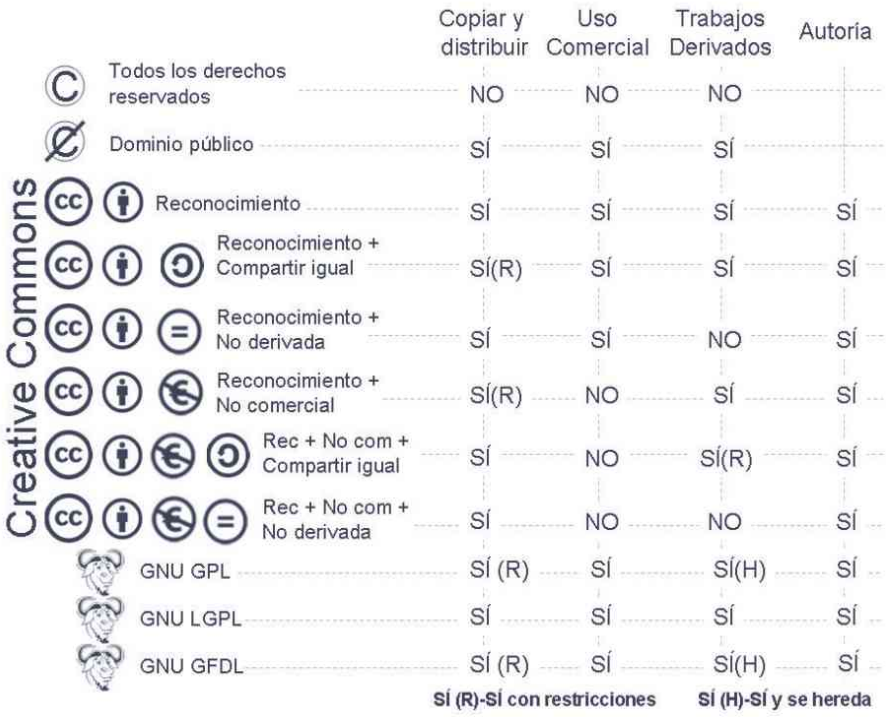


Figura 2.8. *Tipos de licencias software*

2.4 SOFTWARE DE PROPÓSITO GENERAL

Lo constituyen todos aquellos programas diseñados para un uso común y generalizado por parte de un gran número de usuarios de diferentes perfiles y ámbitos.

El software específico es aquel que está diseñado para una tarea en especial, muy específica y concreta, como el software de un TPV, de un banco o de un cibercafé.

2.4.1 OFIMÁTICA Y DOCUMENTACIÓN ELECTRÓNICA

Es el tipo de aplicaciones más extendido y usado ya que los ordenadores se han convertido en herramientas ideales para el trabajo diario de oficina. Han revolucionado el trabajo de oficina, mejorando los resultados y ahorrando recursos.

Dentro del software de ofimática tenemos varios tipos de aplicaciones:

- **Procesadores de texto**. Se usan para crear documentos de texto con gran riqueza tipográfica. Permiten cambiar tipos de letra, tamaño, márgenes, crear tablas, insertar imágenes, gráficos, sonidos, vídeos, etc.

  Ejemplos: *MS Word*, *OpenOffice.org Writer*.

- **Hojas de cálculo**. Mediante una estructura de celdas organizadas en hojas, filas y columnas permiten realizar gran cantidad de cálculos de forma rápida y sencilla y presentarlos adecuadamente con gran facilidad y acompañadas de gráficos. Se emplean para elaborar facturas, calcular presupuestos, balances, estadísticas, etc.

  Ejemplos: *MS Excel*, *OpenOffice.org Calc*, *Lotus 123*.

- **Gestores de Bases de Datos**. Permiten el almacenamiento y la consulta de datos organizados de forma estructurada, almacenándose para ello los datos y las relaciones entre ellos.

  Ejemplos: *MS Access*, *OpenOffice.org Base*, *Sybase*, *SQL Server*, *Oracle*.

- **Editores de Presentaciones**. Permiten crear presentaciones con textos, gráficos, sonidos, animaciones y vídeos, para ser vistas en ordenadores o mediante videoproyectores.

  Ejemplos: *MS Powerpoint*, *OpenOffice.org Impress*.

- **Agendas y Organizadores**. Son auténticas agendas electrónicas que almacenan citas, fechas, contactos, direcciones o teléfonos e incluyen funciones como aviso de citas, organización de contactos en grupos, etc.

  Ejemplos: *MS Outlook*, *Evolution*.

- **Visualizadores de Documentos**. El formato PDF (*Postcript Document File*) se ha convertido en el estándar de documento electrónico. Para ver este tipo de formato y otros menos extendidos se hace necesaria una aplicación de visualización. El más extendido y empleado es el *Adobe Reader*.

- **Suites Ofimáticas**. Son paquetes de software que incluyen una aplicación de cada uno de los tipos citados con anterioridad cubriendo todas las necesidades de una oficina.

  Ejemplos: *MS Office* y *OpenOffice.org*.

2.4.2 IMAGEN, SONIDO Y VÍDEO. SOFTWARE MULTIMEDIA

Este grupo está formado por aquellos programas dedicados a la creación, edición y reproducción de contenidos multimedia (gráficos, sonido, vídeo, animaciones, etc.).

Para tal fin son necesarios los **entornos de reproducciones multimedia**, capaces de reproducir tanto archivos de audio como de vídeo en múltiples formatos y en algunos casos hasta imágenes. Suelen incluir algunas otras funciones como la grabación de CD, etc. Destacan *Windows® Media Player*, *Real Player*, *MusicMatch Jukebox*, *SlowView*, *Totem* o *VideoLan*.

Gráficos

Son programas para la creación, adquisición, modificación, visualización e impresión de archivos gráficos. Pueden ser:

- **Visualizadores**. Muestran los archivos gráficos. Permiten ver carpetas completas de archivos gráficos en diapositivas, tener un catálogo de imágenes etc. Destacan *ACDSEE*, *SlowView*, *XnView*, *IrfanView*.

- **Editores de imágenes de mapa de bits**. **Retoque Fotográfico**. Sirven para crear y sobre todo retocar imágenes permitiendo desde cambiar el tamaño o las propiedades de la imagen hasta aplicar efectos y crear fotomontajes. Destacan *Adobe Photoshop*, *Paint Shop Pro*, *GIMP*, *CorelPhoto Paint*.

- **Editores de imágenes vectoriales**. **Maquetación**. Utilizan imágenes vectoriales para la creación de carteles, tarjetas de visitas, etc. Destacan *Corel Draw*, *Macromedia Freehand*, *Inkscape*, *QuarkXpress*.

- **Programas CAD** (*Computer Aided Design*, diseño asistido por ordenador). Son las aplicaciones empleadas por los ingenieros para elaborar planos, etc. Son ejemplos aplicaciones como *Autodesk Autocad* y *Orcad*.
- **Diseño 3D**. Son aplicaciones empleadas para la construcción de objetos tridimensionales en un espacio virtual y animarlos. Destacan *3D StudioMax*, *SoftImage XSI*, *Maya*.
- **Escaneo y OCR**. Son programas que sirven para adquirir imágenes de un escáner. Los programas OCR (*Optical Character Recognition*) escanean texto en un documento físico y lo convierten a texto en un editor de textos. Suele ser software que acompaña a un escáner o impresora multifuncional cuando se adquiere.

Sonido

Son aplicaciones dedicadas exclusivamente al tratamiento del sonido en el ordenador:

- **Reproductores de Sonido**. Reproducen sonido en archivos de sonido o CD musicales permitiendo crear listas de reproducción, manejar ecualizadores, llevar una base de datos (biblioteca) de la música que se posee y tener un acceso inmediato a cualquier tema.

  Ejemplos: *Winamp*, *Sonique*, *Windows® Media Player*, *VideoLan*.
- **Editores de Sonido**. Se usan para modificar un archivo de sonido a través de la manipulación del dibujo de su onda. Permiten aplicar efectos, cambiar parámetros de audio e incluso capturar sonido a través de un micrófono conectado.

  Ejemplos: *CoolEdit, Adobe Audition, Audacity.*
- Existen **otras muchas utilidades** de sonido como por ejemplo aquellas que se dedican a ripear (convertir a fichero) archivos de sonido desde un CD o viceversa.

Vídeo

Son aplicaciones con una funcionalidad similar a las de sonido, pero de mayor complejidad dadas las mayores posibilidades que ofrece el tratamiento de vídeo respecto al sonido:

Destacan:

- **Reproductores de vídeo** como *DivXPlayer*, *VLC* (*Video Lan Client*), *BSPlayer.*
- **Editores de vídeo** como *Adobe Premier*, *Pinnacle Video Studio* o *ULead Media Studio*.
- **Reproductores de DVD**. Aplicaciones capaces de reproducir DVD como *PowerDVD*, *WinDVD*, etc.
- Otras muchas utilidades, entre las que destacan *DVDShrink* para hacer un *backup* de un DVD, etc.

2.4.3 PROGRAMACIÓN

Lo constituyen el conjunto de herramientas que permiten al programador desarrollar programas informáticos empleando lenguajes de programación. Lo constituyen editores de texto, compiladores e intérpretes, enlazados, depuradores y los Entornos de Desarrollo Integrados (entornos IDE).

Destacan como entornos de desarrollo integrados *Eclipse*, *Borland C++*, *Visual C++* o *Delphi.*

2.4.4 EDUCACIÓN

El software de educación es aquel que, como su nombre indica, sirve para la educación o el aprendizaje. En éste se encuentran las enciclopedias electrónicas, los programas interactivos para aprender matemáticas, física, anatomía, etc., incluyendo además los programas que ayudan a aprender el uso de un tipo de software en especial.

Dentro de esta categoría tenemos pues, desde programas orientados al aprendizaje, diccionarios y enciclopedias multimedia, hasta sistemas operativos completos destinados a la educación, como las distintas distribuciones GNU/Linux orientadas a la enseñanza.

Podríamos mencionar aplicaciones como la *Enciclopedia Multimedia Interactiva Encarta*, *la colección Aprende con Pipo*, etc.

2.4.5 PRODUCTIVIDAD Y NEGOCIOS

Aquí se encuentran programas que ayudan a mejorar nuestra productividad de forma que sirven para llevar las finanzas de un negocio, por ejemplo, un programa que registre los artículos vendidos en un determinado tiempo y después muestra las ganancias.

Pertenecerían a esta categoría programas del tipo:

- ✓ Agenda de Contactos: *ContactKeeper*, *Outlook Express*, *etc.*
- ✓ Calculadoras.
- ✓ Contabilidad: *Contahogar*, *Contaplus*, *etc*.
- ✓ Gestión de Proyectos: *Microsoft Project®*.
- ✓ Terminales de Punto de Venta o TP.
- ✓ Rellenar Formularios: *FormFax Filler 3.5*.

2.4.6 CLIENTES PARA SERVICIOS DE INTERNET

Este grupo lo constituyen aquellos programas que sirven para la conexión a Internet o que usan servicios de esta red.

- **Navegadores**. Se usan para acceder a multitud de servicios de Internet a través del servicio *World Wide Web* o *www*, mostrando contenidos en HTML u otros lenguajes. Destacan *Internet Explorer*, *Firefox*, *Opera*.
- **Clientes de correo electrónico**. Empleados para recibir y enviar correos electrónicos a través de un servidor de correo. Destacan *MS Outlook Express*, *Eudora*, *Thunderbird*.
- **Programas de chat o Mensajería instantánea**. Sirven para tener conversaciones escritas en tiempo real con los contactos registrados. Destacan *MSN Messenger*, *Mirc*.
- **Reproductores multimedia de Internet**. Permiten ver contenidos multimedia transmitidos por Internet. Destacan *Real Player*, *Windows® Media Player*, *Flash Player*.
- **Aplicaciones P2P**. Son aplicaciones que permiten compartir archivos en Internet con otros usuarios. Destacan *emule*, *BitTorrent* o *Pando*.
- **Software Firewall**. Son aplicaciones que impiden el intrusismo en nuestro equipo a través de Internet, además de establecer restricciones en nuestro propio equipo al usar Internet. Destacan *Zone Alarm*, *Norton Internet Security*.

2.4.7 OTRAS CATEGORÍAS DE INTERÉS

Existen otras categorías de software entre las que podrían destacar:

- **Software de tiempo real**. Está íntimamente relacionado con el mundo exterior, debiendo responder a un problema en éste en un tiempo determinado, crítico en muchas ocasiones. Debido a que este software debe operar bajo restricciones de rendimiento muy rigurosas su diseño está guiado por la arquitectura hardware y software soporte. Son ejemplos los programas que gestionan los planes de vuelo de compañías aéreas, controladores de procesos industriales, sistemas médicos de diversa índole, como el software que gestiona un respirador artificial, etc.
- **Software científico y de ingeniería**. Está caracterizado por los algoritmos de manejo de números. Las aplicaciones van desde la astronomía a la vulcanología, desde el análisis de la presión de los automotores a la dinámica orbital de los lanzadores espaciales y desde la biología molecular a la fabricación automática.
- **Software empotrado**. Reside en memoria de solo lectura y se utiliza para controlar productos y sistemas de los mercados industriales y de consumo. El software empotrado puede ejecutar funciones muy limitadas y curiosas (p. e. el control de las teclas de un horno de microondas) o suministrar una función significativa y con capacidad de control (p. e. funciones digitales en un automóvil, tales como control de la gasolina, indicaciones en el salpicadero, sistemas de frenado, etc.).
- **Software de Inteligencia Artificial**. El software de inteligencia artificial o IA hace uso de algoritmos no numéricos para resolver problemas complejos para los que no son adecuados el cálculo o el análisis directo. El área más activa de la IA es la de los sistemas expertos, también llamados sistemas basados en el conocimiento.

RESUMEN DEL CAPÍTULO

En este capítulo se estudia y analiza el otro gran componente de un sistema informático, el software. Primeramente se introduce el concepto de sistema operativo como software básico. Una vez visto esto, se analizan las necesidades de software asociadas a diferentes entornos productivos y cómo se puede usar software estándar o a medida, también se catalogan los diferentes tipos de software estudiando los entornos operativos básicos (plataformas Linux, Windows®, Mac y móviles). También se estudian los distintos tipos de software atendiendo al tipo de licencia que emplean tanto en uso como en distribución, hablando de software libre en distintas categorías y software propietario.

EJERCICIOS PROPUESTOS

- **1.** Elabore un cuadro cronológico en el que recoja la evolución de los principales lenguajes de programación, haciendo especial hincapié en los últimos veinte años.
- **2.** Identifique en un sistema operativo Linux y/o Windows® diferentes componentes asociados a las funciones del sistema operativo estudiadas en el libro (ejemplo: el Explorador de Archivos se emplea para la gestión de archivos).
- **3.** Enumere las diferentes versiones de Windows® por las que se ha pasado tratando de identificar el período de vigencia y las características más relevantes.
- **4.** Describa las principales distribuciones Linux a nivel mundial, así como las diferentes distribuciones Linux que se ofrecen en España por comunidades.
- **5.** Estudie los requerimientos y prestaciones de las principales distribuciones en las diferentes plataformas: Windows® 7, Ubuntu 9.10, MAC OS X.
- **6.** Defina GPL, LGPL y BSD enumerando diferencias así como ventajas e inconvenientes de unas y otras.
- **7.** Indique la utilidad y si son software libre o propietario de las aplicaciones que se enumeran a continuación: *ACDSee*, *mirc*, *Adobe Premiere*, *Winrar*, *Ahead Nero*, *OpenOffice Base*, *Outlook Express*, *Microsoft Project*, *Adobe Dreamweaver*, *Delphi*, *Opera*, *emule*, *Videolan*, *AutoCAD*, *3D Studio*, *Inkscape*, *Quake*, *Adobe Audition*. Trate de averiguar para cada tipo de aplicación otra que tenga la misma funcionalidad.
- **8.** Elabore un historial de los diversos sistemas operativos que haya manejado, así como las distintas aplicaciones que haya utilizado. Desde que empezó a hacer uso del software, ¿cuáles han sido las diferencias más significativas que ha encontrado con respecto al software actual?

TEST DE CONOCIMIENTOS

1 Elija la afirmación correcta:

a) El software de tiempo real reside en memoria de solo lectura y se utiliza para controlar productos y sistemas de los mercados industriales y de consumo.
b) GUI e interfaz gráfica de usuario son dos programas distintos entre sí pero relacionados entre ambos.
c) Las aplicaciones utilitarias son aplicaciones empleadas para fines empresariales de mejora de la productividad en diversos sectores.
d) El GRUB es un cargador de arranque que permite ejecutar varios sistemas operativos en una misma máquina.

2 Elija la afirmación correcta:

a) Con GRUB es posible que en una máquina coexistan Linux y Windows®.
b) Un sistema operativo multiusuario permite ejecutar varios programas (procesos) de forma simultánea.
c) Una licencia de software semilibre no permite el acceso al código fuente y permiso para modificarlo.
d) La gestión del almacenamiento secundario del sistema operativo es responsable de conocer las partes de la memoria usadas y por quién, controlar el espacio libre, decidir qué procesos se cargarán en memoria cuando haya espacio libre y asignar o reclamar espacio de memoria cuando sea necesario.

3 Elija la afirmación correcta:

a) El sistema operativo Windows® fue el primer entorno operativo que contó con una interfaz gráfica.

b) El entorno operativo engloba al sistema operativo, la interfaz de usuario y algunas aplicaciones.

c) Las aplicaciones profesionales horizontales son software para la realización de unas determinadas funciones concretas dentro de un sector determinado.

d) La licencia BSD es una licencia GPL.

4 Elija la afirmación correcta:

a) El software a medida es más potente pero más costoso.

b) Una licencia propietaria permite el uso limitado en tiempo o capacidades tras el cual habrá que pagar un precio.

c) Con el control de recursos, el sistema operativo controla y organiza los dispositivos conectados al sistema.

d) El sistema operativo no administra los sistemas de archivos de disco, sino que es una aplicación aparte llamada *administrador de archivos*.

5 Elija la afirmación correcta:

a) En la gestión del almacenamiento secundario del sistema operativo, el SSOO es el responsable de construir y eliminar archivos y directorios, ofrecer funciones para manipular archivos y directorios, realizar copias de seguridad de archivos, etc.

b) Entre los mecanismos de protección del sistema operativo, éste suele ofrecer servicios de *phishing*, cortafuegos, *spam* y antivirus.

c) La BIOS es la primera parte del sistema operativo que se ejecuta.

d) GUI o interfaz gráfica es lo mismo.

6 Elija la afirmación correcta:

a) Las aplicaciones que vienen con el sistema operativo no se consideran parte del entorno operativo, en todo caso se considerarían accesorios.

b) El *freeware* permite el uso, copia, modificación y distribución libre con acceso al código fuente.

c) Las aplicaciones profesionales horizontales están diseñadas para gestionar y ejecutar una función o proceso empresarial de forma estándar.

d) OS X es una distribución Linux.

7 Elija la afirmación falsa:

a) El sistema operativo de Apple fue el primer entorno operativo que contó con una interfaz gráfica.

b) Las aplicaciones necesitan del sistema operativo para funcionar.

c) La gestión del almacenamiento secundario del sistema operativo se encarga de traspasar y mantener en memoria secundaria aquella información de memoria principal que no sea necesaria.

d) El GRUB es un cargador de arranque que permite ejecutar varios sistemas operativos a la vez en una misma máquina.

8 Elija la afirmación falsa:

a) El software a la medida o enlatado son aplicaciones que se realizan de acuerdo a los requerimientos de las instituciones o empresas.

b) Microsoft® fue una de las primeras compañías en desarrollar software para Apple.

c) La LGPL permite que los desarrolladores usen programas bajo la GPL o LGPL sin estar obligados a someter el programa final bajo dichas licencias.

d) El software de dominio público permite el uso, copia, modificación y distribución del producto con o sin fines de lucro.

9 Elija la afirmación falsa:

a) Delphi es un IDE.

b) La licencia de software de Código Abierto con permisos no permite crear una aplicación derivada sin que requiera protección alguna.

c) El control de recursos de un sistema operativo permite coordinar y manipular el hardware del sistema informático.

d) La interfaz de Windows® se basó en la interfaz de Macintosh.

10 Elija la afirmación falsa:

a) El sistema operativo se deberá de encargar de gestionar los diferentes errores que se generen a nivel operativo.

b) Visual C++ es un entorno de desarrollo integrado.

c) La Licencia Pública General (GPL), contiene una cláusula que obliga a que las obras derivadas o modificaciones posteriores se deban licenciar bajo los mismos términos y condiciones de la licencia original.

d) Un programa ejecutable se ejecuta en la máquina para la cual ha sido diseñado sin importar el sistema operativo.

3 Montaje y ensamblado de equipos informáticos de telecomunicaciones

OBJETIVOS DEL CAPÍTULO

- ✓ Va a aprender a cómo montar un equipo informático desde cero. Conocerá los componentes necesarios para el funcionamiento del equipo y cómo hacerlos funcionar.
- ✓ Deberá seguir y tener muy en cuenta las precauciones en el montaje para evitar accidentes y preservar los componentes.
- ✓ Recordará que cualquier manipulación incorrecta de un componente anula su garantía.
- ✓ Aprenderá los pasos y verificaciones a seguir una vez montado el equipo.

El montaje de un sistema informático no es una operación complicada. Hace años los equipos se compraban a la carta, hoy en día esto no siempre es así. No obstante, como técnico superior, el alumno debe aprender el montaje de equipos así como realizar operaciones de mantenimiento y actualización de los mismos. Aunque en el libro nos centramos en equipos de sobremesa no hay que preocuparse, todos los equipos son muy parecidos y tienen muchas partes en común (memoria, procesador, placa base, disco duro, etc.).

3.1 PRECAUCIONES Y ADVERTENCIAS DE SEGURIDAD

3.1.1 LUGAR DE TRABAJO

Una buena iluminación del sitio de trabajo es fundamental. No hay que descartar el utilizar una luz adicional tipo flexo o portátil para iluminar ciertas partes del interior del ordenador que haga falta que estén mejor iluminadas. Además, el espacio de trabajo deberá estar despejado y acondicionado para las operaciones que se vayan a realizar.

3.1.2 PRECAUCIONES SOBRE LA ENERGÍA ELÉCTRICA

Nunca manipular los componentes con el ordenador encendido, hay que asegurarse de que el ordenador esté apagado. Esto quiere decir que se debe desconectar el cable de alimentación al aparato y el interruptor de la fuente de alimentación si tiene (incluso batería si es un portátil).

Utilizar siempre enchufes con toma de tierra. Evitar utilizar enchufes que no tengan toma de tierra.

3.1.3 PRECAUCIONES SOBRE LA ENERGÍA ESTÁTICA

La energía estática puede hacer que se dañen los componentes electrónicos. La electricidad estática puede producir descargas de **4.000 o incluso más voltios** que hacen que se estropee un componente electrónico. Muchas de estas descargas que se producen no son visibles al ojo humano.

Acciones que evitan problemas con la energía estática:

- ✓ Tocar un grifo (las tuberías cuando son metálicas hacen de toma de tierra).
- ✓ Tocar continuamente la parte metálica de la carcasa para descargarse.
- ✓ Utilizar una pulsera con toma de tierra y utilizarla correctamente.
- ✓ Utilizar un espray antiestático. Rociar un trapo con el espray y frotar el monitor, caja y teclado.

Acciones que pueden provocar problemas con la energía estática (**hay que evitar**):

- ✓ Trabajar en moquetas que no sean antiestáticas.
- ✓ Utilizar zapatos con suela de goma.
- ✓ Utilizar pulseras conductoras (metálicas).
- ✓ Coger los componentes por zonas que no sean los cantos.
- ✓ No descargarse estáticamente antes y mientras se está trabajando.

3.1.4 PRECAUCIONES EN SISTEMAS DE REFRIGERACIÓN LÍQUIDA

Todas las empresas de componentes hacen pruebas de sus productos antes de su distribución, no obstante para evitar problemas que se pudieron producir en la distribución se recomienda hacer una **prueba de estanqueidad** fuera del chasis antes de montarla dentro del mismo.

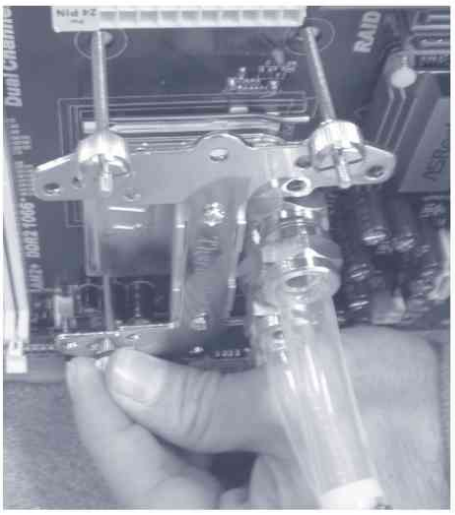


***Figura 3.1**. Instalación de una refrigeración líquida*

La pérdida de líquido del sistema de refrigeración elevará la temperatura del sistema y puede provocar algún problema si dicho líquido llega a los demás componentes.

3.1.5 PRECAUCIONES SOBRE LOS COMPONENTES

Microprocesador

- No poner a funcionar el equipo con el microprocesador montado sin el disipador del microprocesador.
- Cuando se cambie el disipador hay que limpiar la pasta térmica anterior y volver a aplicar pasta nuevamente antes de montar otra vez el disipador.
- Nunca manipular el procesador por los pines o patillas.
- Nunca instalar un disipador en un microprocesador sin pasta térmica.
- Normalmente, los disipadores de los microprocesadores tienen ya un material con pasta térmica preaplicado. Si se decide utilizar otro tipo de material consultar si es apropiado utilizarlo o no en ese microprocesador.

Fuente de alimentación

- No desenchufar el cable de tensión cuando el equipo está funcionando. Puede ocurrir que dañe la fuente y los demás componentes. Recuerde que un equipo suspendido o en *standby* está funcionando.
- No ubicar el equipo o la fuente de alimentación en un lugar con alta temperatura o humedad.

- Las fuentes de alimentación tienen altos voltajes en su interior (¡incluso después de desconectadas!). Con lo cual, se aconseja mucho cuidado en su manipulación y si no se está seguro de lo que se hace, mejor no tocar.

***Figura 3.2**. Parte posterior de la fuente de alimentación*

Placas base

Cuando compramos una placa base viene protegida en su parte inferior por un material que impide que se deterioren los contactos situados en esa cara y envuelta en una bolsa antiestática.

- No agarrar la placa por los componentes, siempre agarrarla por los cantos.
- No sacar la placa de la bolsa hasta que haya que montarla, cuanto menos se maneje mejor.
- No poner la placa encima de la bolsa puesto que puede haberse almacenado la carga electrostática en la zona externa.
- No apilar las placas unas encima de otras pues se pueden dañar. Colocarlas encima de algún material aislante.
- No tocar los componentes con la mano.

Memoria

Hay que seguir los mismos consejos que con la placa base. Al igual que la placa base, evitar manejar en exceso la memoria dado que es uno de los componentes más sensibles del equipo. La energía estática es uno de los peores enemigos de las memorias.

Discos duros

- Manejar los discos a temperatura ambiente.
- La placa con circuitería electrónica es muy sensible a la energía estática, por tanto, hay que manejar el disco por los cantos.
- Su uso debe ser en posición horizontal (preferentemente).
- No tocar nunca la circuitería electrónica del disco.
- No manipular el disco conectado a la corriente.
- No golpear, ni manejar el disco de forma brusca pues las cabezas pueden dañar el plato.

- No exponer los discos a fuentes magnéticas pues dañan la información que contienen.
- No abrir el disco bajo ningún concepto.
- No utilizar tornillos muy largos cuando se fije a la caja.

3.1.6 PRECAUCIONES GENERALES

Con carácter general habrá que tomar las siguientes precauciones:

- No forzar nunca los componentes. No hacer fuerza a la hora de atornillar, fijar una memoria, insertar la placa en su zócalo…
- Evitar el contacto de los líquidos con el equipo. En caso de que se derrame cualquier líquido sobre algún componente electrónico dejarlo secar algunos días en ambiente lo más seco posible. Muchos líquidos provocan cortocircuito.
- Evitar la acumulación de polvo en el interior de los equipos. Para eliminarlo utilizar un pincel suave, un aspirador pequeño o un espray limpiador específico para eliminar polvo de componentes electrónicos.
- Ante todo, y para problemas que no se han enumerado, utilizar el sentido común.

3.2 HERRAMIENTAS DE MONTAJE

Las siguientes herramientas y aparatos de medida son los más utilizados por los técnicos a la hora de manipular sistemas informáticos:

Destornilladores

Se utilizarán destornilladores de distintos tamaños y puntas (Phillips o estrella y planos). También podemos tener algún destornillador tipo Tork (estrella de 6 puntas) para la apertura de discos duros.

Así mismo, se recomienda en el caso de que tengamos que montar o reparar varios equipos el tener un destornillador eléctrico pues facilita y agiliza el trabajo.

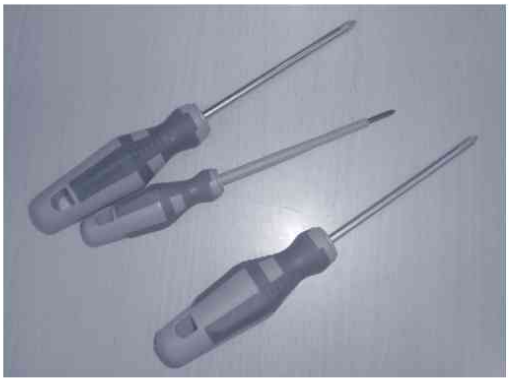


***Figura 3.3**. Juego de destornilladores*

Alicates

De derecha a izquierda: mordaza, alargados y de corte.

***Figura 3.4**. Juego de alicates*

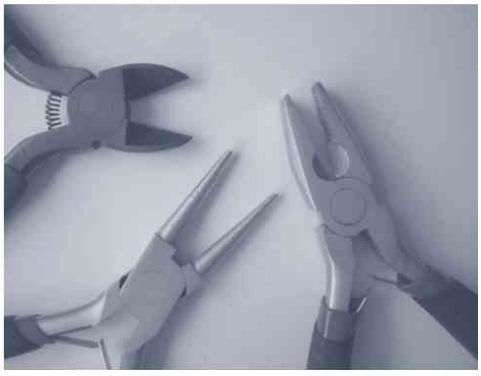


***Figura 3.5**. Juego de alicates (detalle)*

Bridas

Las bridas de plástico o nailon nos servirán para organizar el cableado interior del equipo evitando roces con ventiladores y demás elementos.

***Figura 3.6**. Brida*

Polímetro

Para verificar el correcto funcionamiento de los componentes se necesitará un polímetro con el cual se podrán medir principalmente los voltajes de los componentes como la fuente de alimentación, transformadores de portátiles, etc.

***Figura 3.7**. Multímetro*

Pasta térmica

La superficie del disipador y el procesador no son estrictamente lisas. Es por eso que hay que aplicar pasta térmica para cubrir esos **huecos** que quedan entre ambas superficies cuando se montan en la placa base. En los huecos entre el microprocesador y el disipador quedaría aire y la pasta térmica conduce mejor el calor que el aire, por eso se aplica.

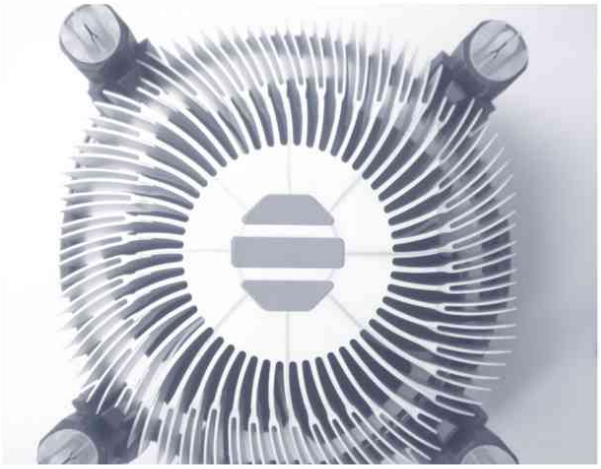


***Figura 3.8**. Disipador Intel®. Detalle de la zona de contacto con el procesador*

Se debe aplicar solamente la cantidad justa sobre la superficie superior del microprocesador y extender posteriormente con una tarjeta de visita, carné o similar para que quede bien distribuida.

No hay que aplicar pasta térmica en exceso, pues es mucho menos conductora que el aluminio y bastante peor que el cobre. También decir que hay pastas térmicas que contienen partículas metálicas y, por tanto, hacen de conductor eléctrico, por lo que un exceso de pasta podría provocar problemas.

Hay disipadores, como el de la figura anterior, que ya vienen con pasta térmica de fábrica, con lo cual no hace falta aplicarla.

***Figura 3.9**. Jeringa de pasta térmica*

En cuanto al tipo de pasta térmica a utilizar, únicamente decir que cuanto más conductora sea mejor, puesto que podemos reducir unos cuantos grados menos la temperatura del microprocesador.

RECUERDA

La pasta térmica es diferente de la silicona térmica. La silicona térmica no transmite tan bien el calor pero pega mucho más, con lo cual nos será más difícil separar el microprocesador del disipador.

3.2.1 EL MULTÍMETRO O POLÍMETRO

Qué es un polímetro o multímetro

Un multímetro o polímetro es un instrumento de medida con el cual podemos medir entre otras:

- Voltaje en corriente continúa y alterna (**voltímetro**).
- Intensidad en corriente continúa (**amperímetro**).
- Resistencia (**óhmetro**).
- Probar diodos y transistores.
- Probar la continuidad de un circuito.

***Figura 3.10**. Multímetro*

Cómo funciona el multímetro

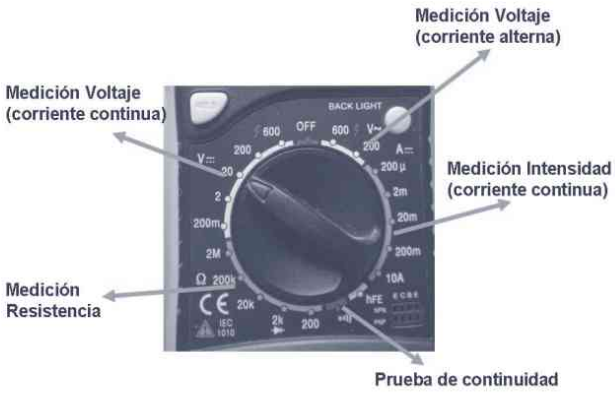


***Figura 3.11**. Detalle del selector rotatorio del multímetro*

Medir voltajes

***Figura 3.12**. Detalle de los conectores de las puntas del multímetro*

1 Hay que colocar las puntas en los terminales correspondientes.

2 Colocar el conmutador rotativo en el rango adecuado a la tensión que se va a medir (si se desconoce el valor de tensión a medir, se recomienda comenzar por el valor más alto del conmutador e ir bajando las escalas hasta conseguir un valor de lectura en pantalla. No olvidar desconectar las puntas en cada cambio de escala).

3 Conectar las puntas al circuito o fuente sometida a prueba.

4 Cuando el aparato indique que está fuera de rango subir al rango superior.

5 Tener en cuenta las polaridades cuando se están efectuando mediciones en corriente continua.

Consejos para un uso correcto

- ✓ No tocar las puntas metálicas al hacer mediciones.
- ✓ No exceder los márgenes indicados para cada valor de escala.
- ✓ Regular la función y el rango a valores apropiados en concordancia con las mediciones.
- ✓ Desconectar las puntas antes de cambiar la escala.
- ✓ No realizar pruebas de resistencias en circuitos alimentados.
- ✓ No realizar medidas de capacidades sin comprobar antes que el condensador está descargado.
- ✓ No utilizar el multímetro con las manos mojadas o en un ambiente muy húmedo.

EJERCICIO 3.1

MEDIR EL VOLTAJE DE SALIDA DE UN TRANSFORMADOR DE PORTÁTIL

Paso 1
Antes de realizar la lectura hay que averiguar cuál es el voltaje de salida del transformador. Por la información "DC Output: 19 V" ya se sabe que el voltaje de salida es de 19 voltios.

Paso 2
Insertar las puntas negra y roja en los terminales COM y VΩMa.

***Figura 3.13**. Detalle de la conexión de las puntas del multímetro*

Paso 3
Colocar el conmutador rotativo en el rango adecuado a la tensión.

***Figura 3.14**. Configuración del selector rotatorio*

En nuestro caso 20 voltios en corriente continua puede ser suficiente, de todas formas es posible que si el voltaje supera esa cantidad nos aparezca un "1" en pantalla avisando que se está fuera de rango y hay que pasar al nivel superior "200 v".

Paso 4
Enchufar el transformador y medir la tensión.

***Figura 3.15**. Medición del conector del transformador de un portátil*

Para medir el voltaje hay que ayudarse de un clip u otro objeto metálico.

***Figura 3.16**. Detalle del resultado de la medición*

En este caso aparece un valor ligeramente superior al valor de referencia del aparato lo cual puede darse por bueno. Los valores medidos suelen ser aproximados y es común que varíen ligeramente por encima o por debajo del valor de referencia.

3.3 FASES DE MONTAJE DE SISTEMAS INFORMÁTICOS

PASOS EN EL MONTAJE

1. Apertura de la caja.
2. Montaje de la placa base.
3. Montaje del microprocesador y disipador.
4. Montaje de las unidades ópticas.
5. Montaje del disco duro.
6. Montaje de las tarjetas de expansión (si son requeridas).
7. Conexionado del resto de componentes.
8. Verificación final de la instalación.

CONSEJO

Generalmente es más cómodo montar el microprocesador y el disipador en la placa base antes de fijar ésta al chasis.

3.4 MONTAJE DEL EQUIPO

3.4.1 MONTAJE DE LA PLACA BASE EN LA CAJA O CHASIS

Fijado de la placa base al chasis de la caja

IMPORTANTE

Sujete la placa base por los bordes. No toque la circuitería con los dedos.

La tornillería que viene con la caja incluye piezas de plástico o metal que evitan que la placa base esté en contacto directo con la caja.

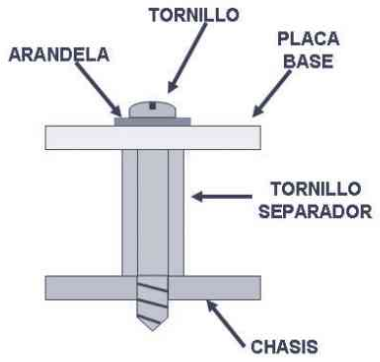


***Figura 3.17**. Sistema de sujeción de la placa base al chasis (tornillos)*

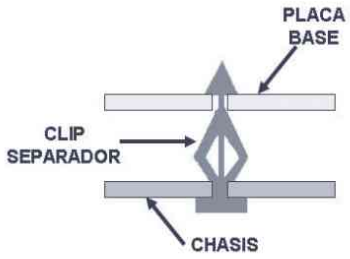


***Figura 3.18**. Sistema de sujeción de la placa base al chasis (clips)*

Normalmente son tornillos macho hembra o clips de plástico que tendrán que colocarse en los huecos apropiados dependiendo de las dimensiones de nuestra placa.

RECUERDA

Compruebe antes de fijar la placa base que todos tornillos macho-hembra o clips quedan perfectamente alineados con los orificios de la placa y no queda ninguno libre. De esta manera no tendremos que desmontar y volver a montar la placa de nuevo.
No deje separadores sin atornillar pues pueden producirse falsos contactos.
Atornille la placa al chasis por todos los sitios marcados.
Se aconseja poner arandelas de cartón o plástico antes de introducir y atornillar los tornillos.

Una vez que tenemos fijados los tornillos macho-hembra o clips en el chasis de la caja se fijará la placa base a la caja utilizando los orificios rodeados de estaño de la misma.

***Figura 3.19**. Detalle de la zona de sujeción de la placa base al chasis*

Los tornillos harán que la placa quede firmemente fijada al chasis de la caja.

Conexionado de la placa base a la fuente de alimentación

RECUERDA

Antes del conexionado de alimentación de la placa base, consulte el **manual** de la misma para hacerlo de forma correcta.

***Figura 3.20**. Conector ATX hembra de la placa base*

Los conectores **ATX** de las placas base actuales son de **24 pines**. Si se tiene una fuente antigua de 20 pines también se puede instalar pero tiene que hacerse en los primeros 20 pines dejando libres los 4 últimos (deberemos conectar el conector ATX de la fuente de alimentación utilizando los pines 1 y 13).

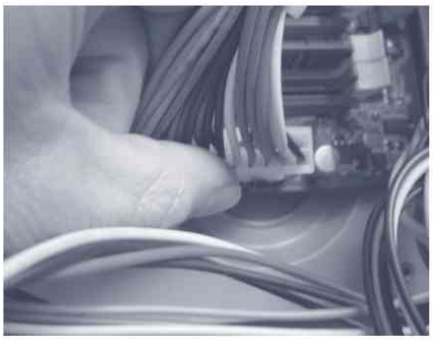


***Figura 3.21**. Conectando el conector ATX hembra de la placa base*

En ocasiones es difícil encajar el conector de alimentación ATX a la placa base. No hay que forzar demasiado la placa base pues se puede dañar.

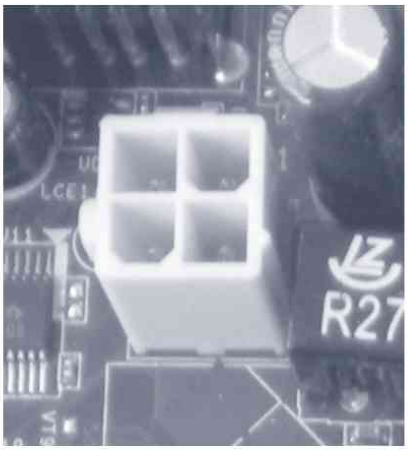


***Figura 3.22**. Conector ATX 12V de la placa base*

Cerca del microprocesador hay un conector **ATX de 12 voltios** de 4 u 8 pines que va a servir para proporcionar la suficiente electricidad al mismo. Hay que colocar el conector ATX 12 V macho de cuatro u ocho pines de la fuente de alimentación al conector hembra de la placa base.

3.4.2 ENSAMBLADO DEL PROCESADOR Y ELEMENTOS DE REFRIGERACIÓN DEL MISMO

RECUERDA

Si se va a instalar una CPU ya utilizada hay que limpiarla bien. Para ello habrá que limpiar tanto la superficie del microprocesador como la base del disipador con alcohol isopropílico que eliminará la pasta o compuesto térmico que ya tenía anteriormente.

CONSEJO

Instalar el microprocesador y disipador antes de fijar la placa base al chasis de la caja.

Existen diferentes tipos de zócalos y formatos de instalación, aunque todos suelen ser similares. Consulte el manual del fabricante para conocer la forma de instalación. Leyendo detenidamente las instrucciones del fabricante no le resultará difícil montar el microprocesador y sistema de refrigeración.

La instalación requiere realizar los siguientes pasos:

1. Leer antes de ensamblar el microprocesador.
2. Preparación del zócalo para recibir el microprocesador.
3. Instalación del microprocesador en el zócalo.
4. Fijación del disipador al zócalo y conexión del ventilador.

Leer antes de ensamblar el microprocesador

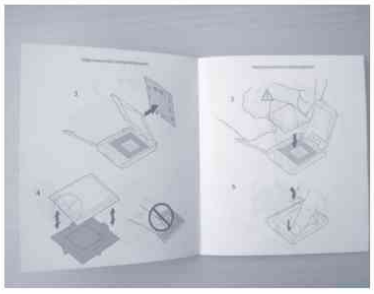


***Figura 3.23**. Manual de instalación del micro y disipador*

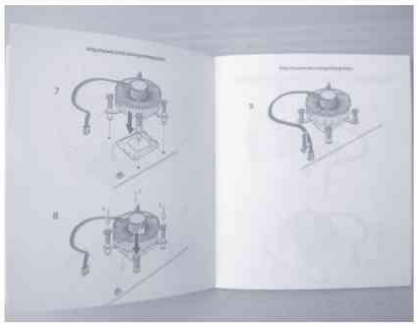


***Figura 3.24**. Manual de instalación del micro y disipador*

Hay que leer detenidamente las instrucciones del fabricante antes de instalar el microprocesador pues es uno de los componentes más sensibles del equipo. Una mala manipulación o instalación dañaría el microprocesador.

En las instrucciones se explicará cómo montar el microprocesador y su disipador.

RECUERDA

Compruebe que la placa base y el microprocesador que va a montar son compatibles. Los micros Intel® y AMD® utilizan diferentes placas base. Consulte antes la documentación del fabricante.

Preparación del zócalo para recibir el microprocesador

1 Liberar la patilla del zócalo.

***Figura 3.25**. Zócalo para procesador Intel®*

2 Retirar el plástico protector.

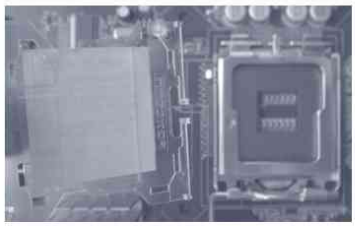


***Figura 3.26**. Zócalo para procesador Intel® sin el plástico protector*

3 Abrir el zócalo.

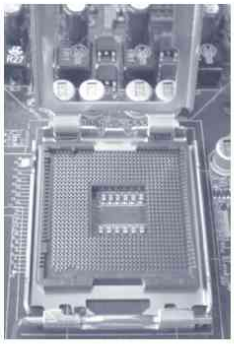


***Figura 3.27**. Zócalo dispuesto para colocar el micro*

RECUERDA

El zócalo suele llevar un plástico que le previene del contacto con los pines del mismo. Quite el plástico justo cuando vaya a instalar el microprocesador. Si retira el microprocesador del zócalo vuelva a colocar el plástico en el zócalo para que no se dañe.

RECUERDA

Zócalo **ZIF** (*Zero Insertion Force*, fuerza de inserción cero). Estas siglas significan que no hay que forzar o hacer fuerza sobre el micro hacia el zócalo.

Instalación del microprocesador en el zócalo

RECUERDA

Alinee correctamente el microprocesador al zócalo. El indicador de la Conexión 1 debe coincidir con el Pin 1 del zócalo de la CPU. Compruebe que las muescas o chaflán del zócalo coinciden con las del microprocesador. Los microprocesadores sólo encajan en una posición determinada.

1 Colocar microprocesador suavemente en la posición correcta dentro del zócalo.

***Figura 3.28**. Colocación del micro en el zócalo*

2 Cerrar la portezuela del zócalo.

***Figura 3.29**. Micro ya alojado en el zócalo*

3 Ajustar la patilla para que el micro haga contacto con los pines del zócalo.

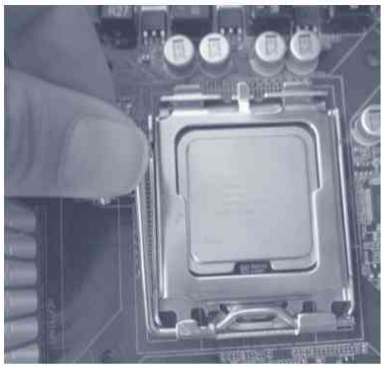


***Figura 3.30**. Colocación de la pata de sujeción del micro en el zócalo*

Fijación del disipador al zócalo

NO OLVIDES

Colocar pasta térmica en el microprocesador antes de instalar el disipador en caso de que el disipador **NO** venga con compuesto térmico de fábrica.
Procure colocar pasta térmica (la justa) y distribuir una capa fina por toda la superficie del microprocesador.

1 Colocar el disipador ajustándolo correctamente. Hay que tener cuidado de no pinzar los cables del ventilador con el disipador.

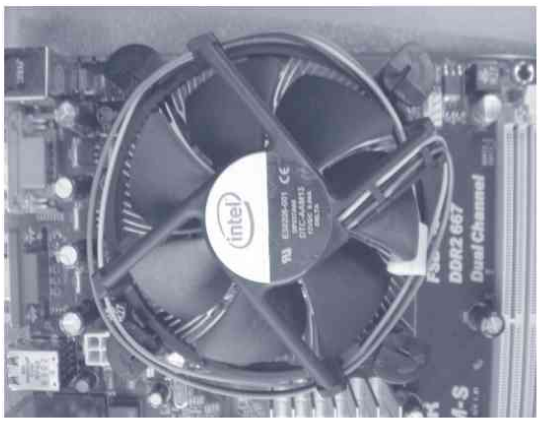


***Figura 3.31**. Detalle del fan del disipador*

2 Anclarlo a la placa base. Para ello en algunos casos habrá que ayudarse con un destornillador.

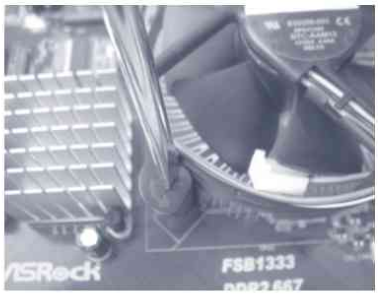


***Figura 3.32**. Fijación del disipador a la placa base*

3 Nótese que el ventilador está colocado de tal forma que hace que el calor ascienda. Expulsa el aire caliente del disipador y lo saca fuera del mismo.

***Figura 3.33**. Conexión de alimentación del fan del disipador de la CPU*

El ensamblaje del ventilador tiene un conector de alimentación de 3 pines (normalmente en las placas viene marcado como CPU FAN). Si el conector tiene 4 (con control PWM), este cuarto contacto es para instalar un ventilador silencioso y poder controlar la velocidad del ventilador mediante el contacto extra (si es de solo 3 pines, este conector se conectará generalmente en los 3 primeros -del 1 al 3-. No obstante, consultar con el manual de la placa base para su correcta instalación).

NO OLVIDES

Conectar el cable del disipador al conector de la placa base. Consulte el manual del fabricante para saber en qué pines irá conectado el ventilador.

3.4.3 FIJACIÓN DE LOS MÓDULOS DE MEMORIA RAM

Pasos antes de montar la memoria

1 Consultar en el manual de la placa base si la memoria que se va a instalar es compatible.

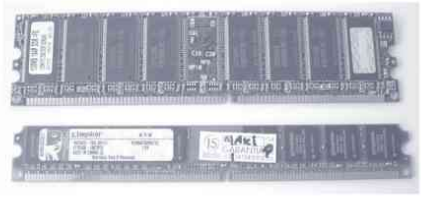


***Figura 3.34**. Memorias de tipo DDR*

2 Consultar en el manual en qué bancos de memoria se deben colocar los módulos de RAM.

Instalación física

Seguiremos los pasos que se indican a continuación.

1 Alinear las muescas de la RAM con las muescas del banco de memoria.

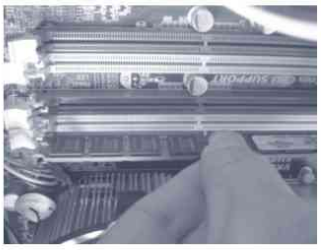


***Figura 3.35**. Instalación de la memoria RAM*

2 Empujar suavemente hasta que la RAM haya encajado perfectamente.

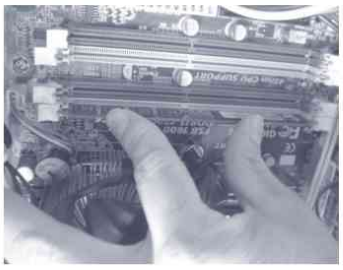


***Figura 3.36**. Fijación de la memoria RAM al zócalo*

3 Fijar la RAM con las pestañas para que quede bien asegurada.

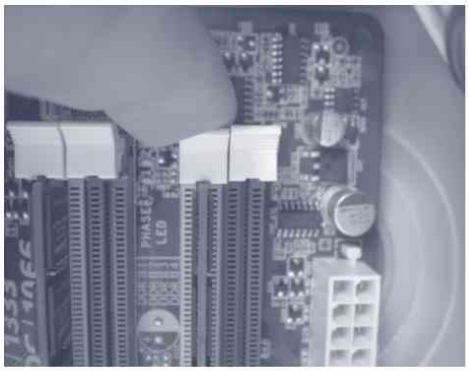


***Figura 3.37**. Ajustando las patillas de la memoria RAM al zócalo*

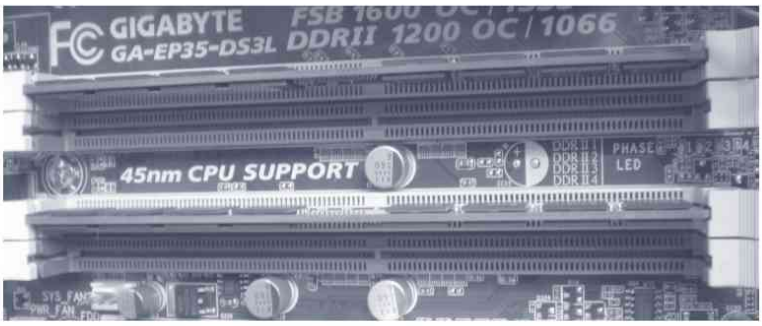


***Figura 3.38**. Detalle de 2 módulos de memoria en una placa base*

En el caso de que se tenga que montar más de un módulo el procedimiento es el mismo. Como se dijo antes, consultar en el manual de la placa base los bancos de memoria donde tienen que ir colocados.

RECUERDA

Hay placas que admiten más de un tipo de memoria pero no se aconseja colocar tipos de memoria diferentes en una placa.
Procure montar memorias iguales (misma marca, tamaño…), sobre todo si va a hacer *Dual Channel*.

3.4.4 FIJACIÓN Y CONEXIÓN DE LAS UNIDADES DE DISCO FIJO

RECUERDA

Para la instalación y manipulación del disco siga las recomendaciones dadas al principio de este capítulo.

Pasos a seguir

Los pasos a seguir en la instalación de un disco duro de una manera muy simplificada son los siguientes:

1 Configuración de los *jumpers* (solo discos PATA). Muchos discos PATA vienen de fábrica configurados en la posición *cable-select*. Dependiendo de la configuración particular deseada puede ser necesario que haya que modificarlo a la posición de maestro o esclavo. Más adelante se mostrarán las distintas configuraciones de un disco duro PATA.

2 Instalar físicamente el disco en la bahía conectando el cable de datos.

3 Ver que se autodetecta correctamente el disco duro desde la BIOS.

4 Crear una partición y formatearla si es un disco que no alberga el sistema y si no instalar el sistema operativo.

Configuración de los jumpers (sólo en los discos IDE/PATA)

IMPORTANTE

No todos los discos tienen la misma configuración de *jumper*. Consulte las instrucciones del fabricante en cada caso.

En los discos SATA no es necesario configurar ningún tipo de *jumper*:

***Figura 3.39**. Configuración de jumper de un disco duro*

Tipos de configuraciones:

- **Maestro o único disco** (*master or single drive*). Éste es el caso de que solamente tengamos un disco o el disco sea maestro y tenga un esclavo.
- **Esclavo** (*slave*). Se configura de esta forma cuando ya existe un maestro.
- **Maestro con un esclavo no ATA compatible** (*master with a non-ATA-compatible*). Éste es un caso raro. Configurar de esta forma cuando el disco esclavo no se está reconociendo correctamente.
- **Selección por cable** (*Cable Select*). Se autoconfigura a partir de la posición que ocupa en el cable.
- **Limitar la capacidad a 32 GB** (*Limit capacity to 32 GB*). Si el sistema no permite la instalación de discos de capacidad mayor a 32 GB se configurará de esta manera. Si el sistema lo soporta no configurar de esta manera.

La siguiente figura muestra la configuración de un disco barracuda de *Seagate*:

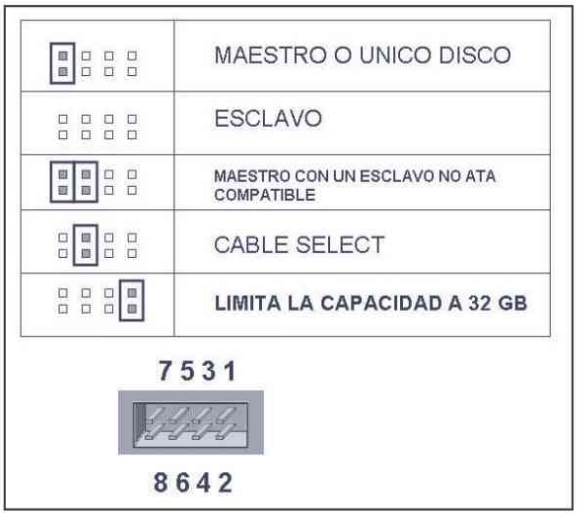


***Figura 3.40**. Tabla de configuración de jumper de un disco duro*

En este otro disco, vemos que la configuración es diferente:

***Figura 3.41**. Tabla de configuración de jumper de un disco duro*

EJERCICIO 3.2

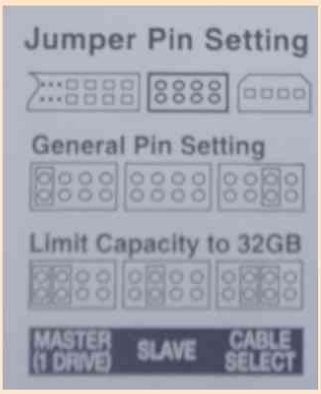


***Figura 3.42**. Tabla de configuración de jumper de un disco duro*

Atendiendo a la configuración de *Jumper* de este disco. Explique cuáles son las siguientes configuraciones que se han dispuesto:

- **Configuración 1**

***Figura 3.43**. Configuración de jumper de un disco duro*

- **Configuración 2**

***Figura 3.44**. Configuración de jumper de un disco duro*

EJERCICIO 3.3

***Figura 3.45**. Tabla de configuración de jumper de un disco duro*

Atendiendo a la configuración de *Jumper* de este disco, se necesita configurar el disco como *Master* pero con la limitación que tiene el sistema de 32 GB. Describa la configuración de los *jumpers*.

Conexionado del cable PATA y SATA

CABLE PATA

A diferencia del cable SATA el cual se conecta al puerto SATA de la placa y al del disco, el cable PATA se instala en una posición determinada. El disco dependiendo si es maestro (o único) o esclavo se conectará en un conector determinado.

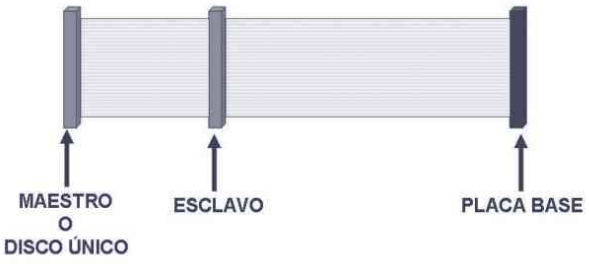


***Figura 3.46**. Conector PATA*

El cable PATA es un cable plano y ancho. Tiene 40 u 80 hilos (ya es prácticamente imposible ver uno de 40 hilos).

Generalmente los cables PATA tienen los conectores que se ven en la figura anterior. Un extremo del cable irá a la placa base y el otro a la unidad maestra o única. Si se quiere montar un segundo dispositivo en el mismo cable irá en el conector central.

El conector que va a la placa base generalmente es de otro color (azul). También los conectores para conectar las unidades están más juntos que el conector que va a la placa base.

Normalmente, las placas base tienen 1 ó 2 conectores PATA (o puertos IDE) en los que se pueden instalar 2 ó 4 unidades PATA como máximo.

CABLE SATA

***Figura 3.47**. Conector SATA*

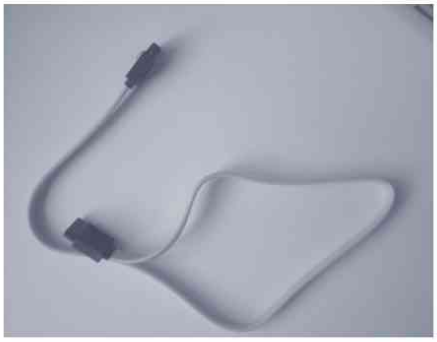


***Figura 3.48**. Conector SATA*

Los cables de datos SATA van conexionados al disco y a la placa base. Tienen sólo dos conectores con lo cual únicamente se puede conectar una unidad (disco duro, lector óptico…) por cable.

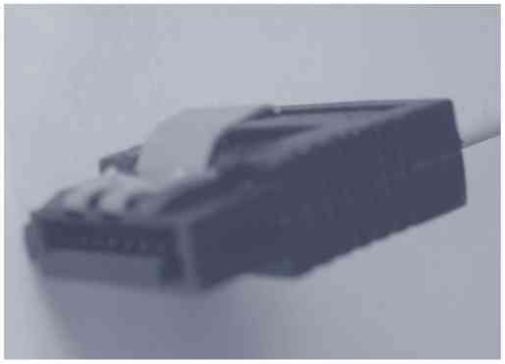


***Figura 3.49**. Detalle del conector SATA*

Conector de datos SATA

Los conectores de los cables de datos SATA tienen un conector de 7 pines. Un extremo del cable se conectará a la placa base y el otro extremo al conector de datos SATA del disco.

Instalación física

1 Desenchufar de la corriente.

2 Quitar las tapas laterales del ordenador.

3 Introducir el disco en una de las bahías disponibles de 3 ½.

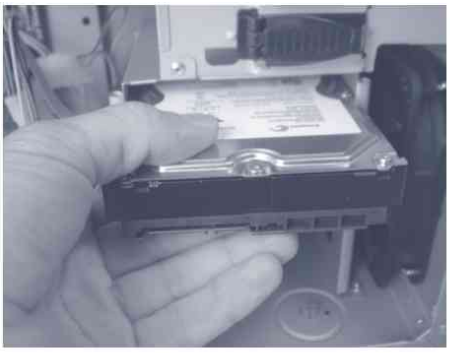


***Figura 3.50**. Alojando un disco duro en una bahía de 3 ½*

4 Fijar el disco al chasis con los tornillos o presas. Dependiendo de la caja tendrá un sistema u otro.

***Figura 3.51**. Detalle del sistema de sujeción de unidades rígidas/ópticas*

El sistema de presas permite un montaje y desmontaje más rápido.

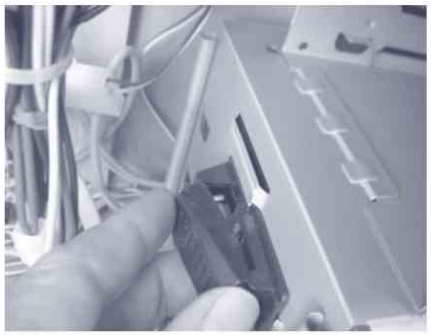


***Figura 3.52**. Fijando la unidad al chasis*

El disco tiene que quedar bien fijo pues gira a mucha velocidad (normalmente a 7.200 RPM).

5 Conectar el conector Molex/SATA de corriente.

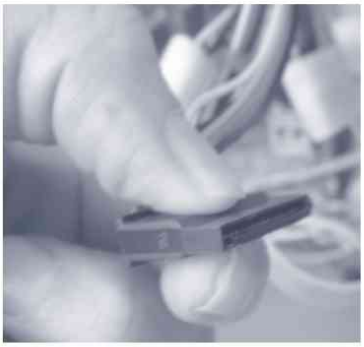


Figura 3.53. *Conector SATA de corriente*

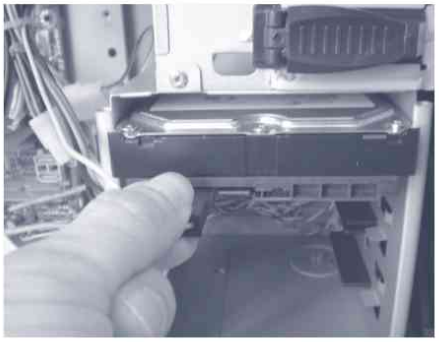


Figura 3.54. *Conectando el conector SATA de corriente*

6 Conectar el cable PATA/SATA de datos (un extremo a la unidad o disco y el otro al puerto SATA de la placa base).

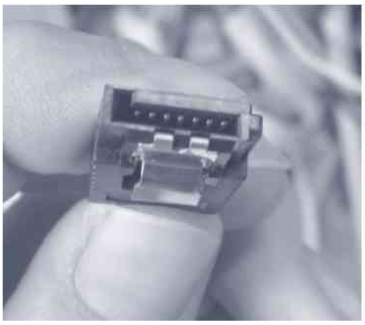


Figura 3.55. *Conector SATA de datos*

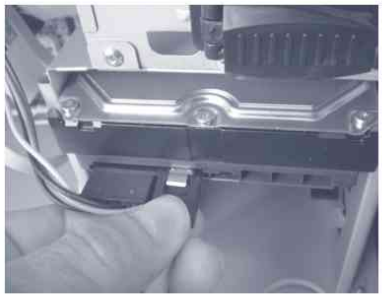


Figura 3.56. *Conectando el conector SATA de datos*

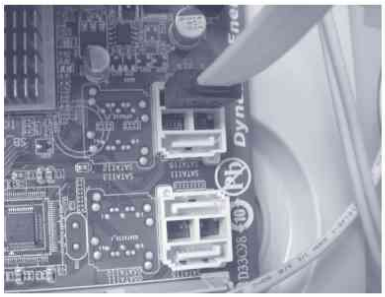


Figura 3.57. *Conexión del cable SATA a la placa base*

RECUERDA

Los cables SATA de corriente y datos sólo encajan en una posición, pues tienen forma de "L". No fuerce la conexión pues se puede dañar el conector.

3.4.5 FIJACIÓN Y CONEXIÓN DE LAS UNIDADES ÓPTICAS DE LECTURA/ESCRITURA

Pasos a seguir

Los pasos a seguir en la instalación de una unidad óptica de una manera muy simplificada son los siguientes:

1 Configuración de los *jumper* (solo discos PATA). Muchas unidades PATA vienen de fábrica configuradas en la posición *cable-select*. Dependiendo de la configuración particular deseada puede ser necesario que haya que modificarla a la posición de maestro o esclavo. Esta configuración es igual que en los discos duros.

2 Instalar físicamente la unidad en la bahía conectando el cable de datos.

3 Detectar o ver que se autodetecta correctamente la unidad desde la BIOS.

EJERCICIO 3.4

Figura 3.58. *Detalle de la configuración de una unidad óptica*

Atendiendo a la configuración de *jumper* de esta unidad óptica, explique las unidades PATA que puede tener el equipo y cómo están configuradas.

RECUERDA

El conexionado de los cables **PATA** y **SATA** y la instalación física es igual que en los discos duros, la única variación es que las unidades ópticas se instalan en bahías de 5 ¼.

RECUERDA

Los cables **SATA** de corriente y datos en un lector óptico sólo encajan en una posición pues tienen forma de "L". No fuerce la conexión pues se puede dañar el conector.

3.4.6 FIJACIÓN Y CONEXIÓN DEL RESTO DE ADAPTADORES Y COMPONENTES

Instalación de la tarjeta de vídeo

Una tarjeta de vídeo es el elemento electrónico que permite que el equipo se comunique con un monitor. Las tarjetas de vídeo más recientes son las **PCI Express** (PCIe) aunque también se pueden encontrar en el mercado tarjetas **AGP** o **PCI** (menos veloces y más obsoletas). La instalación de todo este tipo de tarjetas es similar.

Para la instalación física se seguirán los siguientes pasos:

1 Retirar el cable de corriente del equipo.

***Figura 3.59**. Retirando la placa metálica del slot*

***Figura 3.60**. Placa metálica liberada*

2 Liberar un *slot* de la plaquita metálica. Utilizar para ello un alicate de mordaza y un destornillador. Cuidado con esta chapa pues puede provocar cortes en las manos.

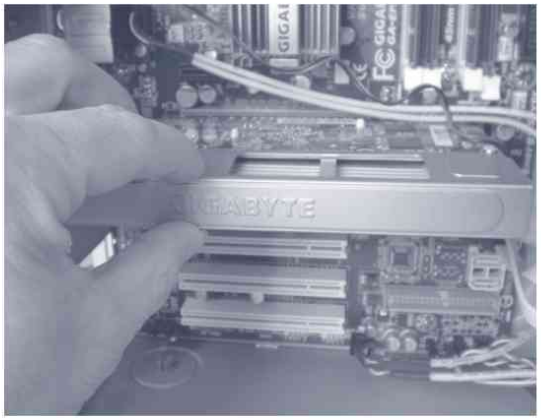


***Figura 3.61**. Insertando la tarjeta de vídeo en su ranura*

3 Alinear la tarjeta de vídeo con el *slot* y la ranura de expansión de la placa base.

RECUERDA

Algunos conectores **AGP** o **PCIe** tienen un mecanismo de seguridad para fijar mejor la tarjeta. Tenga cuidado y no lo fuerce para no romper la fijación.

4 Presionar de manera suave la tarjeta de vídeo hasta que quede encajada correctamente. No forzar en exceso.

***Figura 3.62**. Fijando la tarjeta al slot*

5 Fijar la tarjeta con un tornillo o bien con el sistema que traiga la caja o chasis.

Algunas tarjetas de alta gama necesitan un conector eléctrico suplementario pues el voltaje suministrado por la placa base no es suficiente. En ese caso no hay que olvidarse de conectarlo.

RECUERDA

Si necesita instalar más de una tarjeta en una placa base para que funcionen de forma agrupada mediante **Crossfire®** o **SLI®** deberá unirlas mediante un puente o conectar la tarjeta maestra a la esclava. Consulte el manual del fabricante en todo caso para comprender correctamente la forma de instalación.

Instalación de una tarjeta de expansión USB

Una tarjeta de expansión de USB es un dispositivo bastante barato a comparación de otras tarjetas y permite ampliar los puertos USB de un equipo sin necesidad de utilizar concentradores u otros elementos. También permitirá disponer de algún USB interno para conectar algún dispositivo como *displays*, paneles…

Para la instalación física se seguirán los siguientes pasos:

1 Retirar el cable de corriente del equipo.

2 Liberar un *slot* de la plaquita metálica. Utilizar para ello un alicate de mordaza y un destornillador. Cuidado con esta chapa pues puede provocar cortes en las manos.

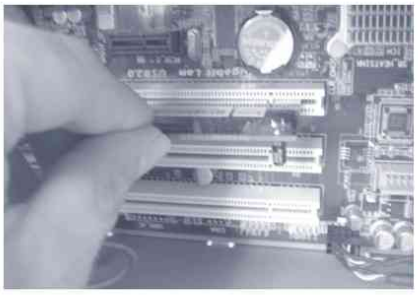


***Figura 3.63**. Insertando la tarjeta de expansión en su ranura*

3 Alinear la tarjeta expansora con el *slot* y la ranura de expansión de la placa base.

4 Presionar de manera suave la tarjeta de expansión hasta que quede encajada correctamente. No forzar en exceso.

***Figura 3.64**. Fijando la tarjeta al slot*

5 Fijar la tarjeta con un tornillo o bien con el sistema que traiga la caja o chasis.

ACTIVIDADES 3.1

Instalación de varias NIC

Por regla general, las placas base ya tienen integradas la NIC (*Network Interface Card*). No obstante, en caso de servidores o equipos que necesiten otro adaptador de red adicional porque se van a conectar a más de una red, se le puede instalar una o varias tarjetas adicionales. Igualmente si la NIC de la placa base deja de funcionar se puede instalar una adicional que supla las funciones de la que se ha estropeado.

Las NIC utilizan las ranuras de expansión PCIe y PCI de la placa base.

- Como actividad se pide que instale las siguientes NIC:
  a. NIC instalable en el puerto PCI Express (PCIe) x1.
  b. NIC PCI inalámbrica.

Recuerde que para instalar una tarjeta de expansión deberá seguir los siguientes pasos:

a. Retirar el cable de corriente del equipo.
b. Liberar un *slot* de la plaquita metálica. Utilizar para ello un alicate de mordaza y un destornillador. Cuidado con esta chapa pues puede provocar cortes en las manos.
c. Alinear la tarjeta con el *slot* y la ranura de expansión de la placa base.
d. Presionar de manera suave la tarjeta hasta que quede encajada correctamente. No forzar en exceso.
e. Fijar la tarjeta con un tornillo o bien con el sistema que traiga la caja o chasis.

Una vez instalada la tarjeta compruebe que ésta funciona correctamente, para ello deberá previamente configurarla.

Conexionado del resto de los cables del chasis

1 Conectar los conectores Molex que alimenten a los distintos ventiladores.

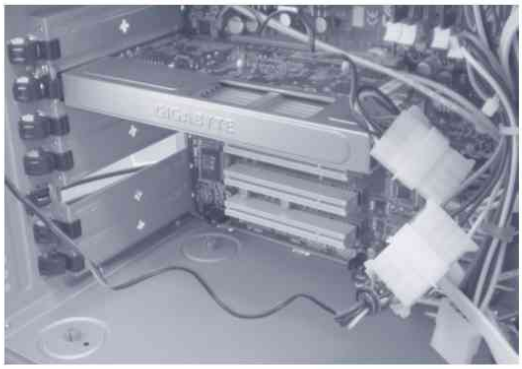


***Figura 3.65**. Conectando los molex de los ventiladores de la caja*

2 Conexión de los demás cables del chasis:

- *Speaker* del chasis.
- Conectores USB.
- Panel del sistema (*power* o encendido de la torre, *reset*, led del disco duro, etc.).
- Conector de los demás ventiladores del chasis.

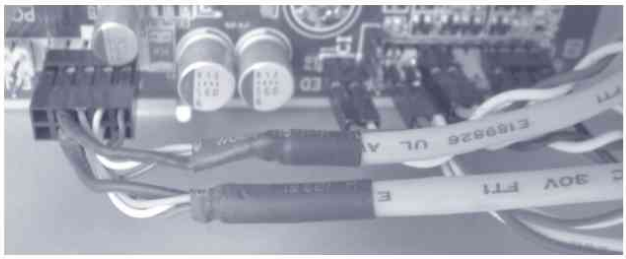


***Figura 3.66**. Conectando los demás conectores de la placa base*

RECUERDA

Los cables de los indicadores **led** tienen **polaridad**. Si observa que no encienden quizás tenga que cambiarlos de orientación.

3.5 VERIFICACIÓN DEL MONTAJE

Antes de enchufar el cable de alimentación y encender el ordenador hay que parar un momento para comprobar las siguientes cosas.

- ✓ ¿Está la RAM correctamente instalada en el banco correspondiente y cerradas las pestañas de fijación?
- ✓ ¿Está correctamente fijada la placa al chasis?
- ✓ ¿Está el disco duro correctamente fijado y con sus conectores de datos y alimentación?
- ✓ ¿Está el microprocesador correctamente fijado a la placa y al disipador con pasta térmica?
- ✓ ¿Están conectados el conector ATX y ATX 12V a la placa base?
- ✓ ¿Está correctamente conectado el cable del ventilador de la CPU?
- ✓ ¿Están correctamente conectados los cables de encendido, *reset*, leds, USB…?
- ✓ ¿Los demás conectores eléctricos de la placa están correctamente conectados?

Además de estas comprobaciones, dependiendo la configuración particular del equipo se deberán hacer algunas otras comprobaciones complementarias.

CONSEJO

Utilice un live CD para realizar comprobaciones de que todo funciona correctamente.

RESUMEN DEL CAPÍTULO

En este capítulo se explica de forma general cómo se monta un equipo informático con todos sus componentes. Siempre que se manipulan componentes y equipos electrónicos hay que hacerlo con las herramientas adecuadas y con seguridad, por tanto, hay que tener muy en cuenta estas precauciones.

Todos los equipos suelen utilizar el mismo tipo de componentes (memoria, placa base, fuente de alimentación, procesador…), lo único que cambia es el formato y los modelos. Obviamente, no se utilizará el mismo procesador para un *netbook* o un servidor pero lo que sí es importante es que ambos utilizan un procesador. El alumno deberá entender el montaje también de forma conceptual pues los componentes variarán con el tiempo y según las características del equipo.

Es importante hacer una buena verificación del equipo una vez montado el mismo antes de su puesta en funcionamiento.

EJERCICIOS PROPUESTOS

1. Montaje y desmontaje de un equipo informático.

En este ejercicio deberá de tomar nota de cómo está montado el equipo para volverlo a montar. No hace falta separar el disipador del microprocesador o cualquier otro elemento como clips de sujeción, etc., si cree que puede dañarse en su desmontaje. Consiga el manual de la placa, pues le va a hacer falta para entender la configuración del equipo. Compruebe el sistema antes del desmontaje y después, comprobando que funcionen todos los elementos del mismo (lectores ópticos, disco duro, leds, puertos USB…). Recuerde las recomendaciones de seguridad que se hicieron al comienzo del capítulo.

2. Montaje de un equipo informático desde cero.

Este ejercicio consistirá en el montaje de un equipo desde cero. Al contrario que en el primer ejercicio, ahora no tiene la referencia del sistema ya montado.

Lea atentamente toda la información disponible (placa base, microprocesador…) antes de empezar con el montaje. Recuerde las recomendaciones de seguridad que se hicieron al comienzo del capítulo.

3. Montaje de una segunda unidad óptica.

Una segunda unidad óptica puede sernos de utilidad cuando se requiere copiar o clonar discos con *backups* o datos personales. Si es posible y el equipo lo soporta, instale una segunda unidad SATA y otra PATA.

4. Ampliación de la RAM.

Se ampliará la RAM para un portátil y para un equipo de sobremesa.

Antes de la instalación, cerciorarse si la RAM a instalar es compatible y en qué banco de memoria se ha de instalar.

5. Sustitución del procesador.

Se sustituirá el procesador de un equipo de sobremesa. Habrá que tener cuidado en no dañar los componentes. Antes de fijar el microprocesador, verificar en el manual de la placa base si el zócalo soporta ese tipo de microprocesadores. No olvidar añadir material termoconductor (pasta térmica) entre disipador y microprocesador.

6. Sustitución o ampliación del disco duro en un portátil.

Ésta es una situación cada vez más frecuente. Cada vez existen más portátiles en el mercado y este tipo de operaciones se demandan con más frecuencia.

7. Sustitución de la fuente de alimentación.

Ésta es una situación muy común en la reparación de equipos informáticos. Las fuentes de alimentación se deterioran con el paso del tiempo o con un mal uso. Compruebe que la nueva fuente de alimentación tiene las mismas dimensiones y, al menos, igual potencia que la antigua. Recuerde las recomendaciones de seguridad que se hicieron al comienzo del capítulo.

8. Sustitución del disipador y ventilador de la CPU por otro más silencioso.

Normalmente existen disipadores y ventiladores mejores que los que vienen de serie cuando compramos el microprocesador. Habrá que comprobar la temperatura antes y después de haber instalado el nuevo componente para ver las ventajas del mismo. Si es posible, instalar un controlador de ventiladores o controlador de temperatura para la CPU.

9. Averigüe de qué está compuesta la pasta térmica.

TEST DE CONOCIMIENTOS

1 Elija cuál de estas afirmaciones es verdadera:
- a) Hay que evitar el contacto del disipador con cualquier líquido o alcohol para evitar la oxidación del mismo.
- b) La pasta térmica no debe ser conductora pues puede producir problemas con los componentes del equipo.
- c) Muchas de las descargas de energía electrostática que se producen no son visibles al ojo humano.
- d) Antes de instalar un disco PATA o SATA hay que verificar la configuración de los *jumpers*.

2 Elija cuál de estas afirmaciones es verdadera:
- a) Hay que evitar instalar un disipador en un microprocesador con pasta térmica.
- b) Hay que evitar no poner la placa base o *motherboard* encima de la bolsa que la contiene puesto que puede haberse almacenado la carga electrostática en la zona externa.
- c) Para evitar la electromigración hay que evitar coger los componentes por zonas que no son los cantos.
- d) Nunca hay que manipular el procesador por los pines o patillas.

3 Elija cuál de estas afirmaciones es verdadera:
- a) Es posible instalar un Athlon en una placa base Intel®, basta con cambiar el zócalo Intel® y ponerle un AM2.
- b) Un voltímetro permite medir la intensidad en corriente continua.
- c) Para evitar la electromigración hay que evitar utilizar pulseras conductoras (metálicas).
- d) En caso de que se derrame cualquier líquido sobre algún componente electrónico dejarlo secar algunos días en un ambiente lo más seco posible.

4 Elija cuál de estas afirmaciones es verdadera:
- a) Para hacer *Dual Channel* se aconseja utilizar memorias de la misma marca, tamaño y velocidad.
- b) La pasta térmica no debe ser conductora pues puede producir problemas con los componentes del equipo.
- c) La silicona térmica es un material compuesto en un 75% por cianocrilato, el resto son materiales conductores.
- d) Hay que evitar no poner la placa base o *motherboard* encima de la bolsa que la contiene puesto que puede haberse almacenado la carga electrostática en la zona externa.

5 Elija cuál de estas afirmaciones es verdadera:
- a) El conector ATX 12V tiene 4, 6 u 8 pines.
- b) En un cable pata con 3 conectores se pueden instalar hasta 2 discos duros.
- c) El conector ATX 12V tiene 20 ó 24 pines.
- d) Para medir la corriente continua puedo utilizar un multímetro o bien un óhmetro.

6 Elija cuál de estas afirmaciones es verdadera:
- a) El tercer contacto de un ventilador con control PWM permite poder controlar la velocidad del ventilador.
- b) El conector ATX 12 V tiene 8 ó 4 pines.
- c) Los zócalos ZIF (*Zero Installation Force*) permiten instalar un micro sin hacer fuerza sobre el micro hacia el zócalo.
- d) Una vez pegado con silicona térmica el microprocesador y el disipador no pueden separarse pues la silicona contiene *epoxy*.

7 Elija cuál de estas afirmaciones es verdadera:
a) Para evitar la electromigración hay que evitar utilizar pulseras conductoras (metálicas).
b) Los cables PATA tienen 60 u 80 hilos.
c) En un cable pata con 3 conectores se pueden instalar hasta 3 discos duros.
d) Existen esprays antiestáticos que evitan la acumulación de energía estática.

8 Elija cuál de estas afirmaciones es verdadera:
a) Antes de instalar un disco PATA o SATA hay que verificar la configuración de los *jumpers*.
b) Hay que evitar el contacto del disipador con cualquier líquido o alcohol para evitar la oxidación del mismo.
c) El conector ATX tiene 20 pines.
d) La pasta térmica no debe ser conductora pues puede producir problemas con los componentes del equipo.

9 Elija cuál de estas afirmaciones es verdadera:
a) La silicona térmica es un material compuesto en un 75% por cianocrilato, el resto son materiales conductores.
b) Hay que evitar no poner a funcionar el equipo con el microprocesador montado sin el disipador del microprocesador.
c) Para medir intensidades hay que colocar el multímetro en serie en el circuito.
d) Las pulseras metálicas evitan la acumulación de energía estática.

10 Elija cuál de estas afirmaciones es verdadera:
a) Hay que evitar instalar un disipador en un microprocesador sin pasta térmica.
b) Hay que evitar el contacto del disipador con cualquier líquido o alcohol para evitar la oxidación del mismo.
c) Hay que evitar no poner a funcionar el equipo con el microprocesador montado sin el disipador del microprocesador.
d) Hay que evitar no poner la placa base o *motherboard* encima de la bolsa que la contiene puesto que puede haberse almacenado la carga electrostática en la zona externa.

11 Elija cuál de estas afirmaciones es verdadera:
a) Para medir la corriente continua puedo utilizar un multímetro o bien un óhmetro.
b) La silicona térmica es un material similar a la pasta termica.
c) Para evitar la electromigración hay que evitar utilizar pulseras conductoras (metálicas).
d) Un voltímetro permite medir la intensidad en corriente continua.

12 Elija cuál de estas afirmaciones es verdadera:
a) Tocar un grifo evita la acumulación de energía estática.
b) Hay que evitar no poner a funcionar el equipo con el microprocesador montado sin el disipador del microprocesador.
c) Hay que evitar instalar un disipador en un microprocesador con pasta térmica.
d) Para evitar la electromigración hay que evitar coger los componentes por zonas que no son los cantos.

13 Elija cuál de estas afirmaciones es verdadera:
a) Hay que evitar no poner la placa base o *motherboard* encima de la bolsa que la contiene puesto que puede haberse almacenado la carga electrostática en la zona externa.
b) Es posible instalar un Athlon en una placa base Intel®, basta con cambiar el zócalo Intel® y ponerle un AM2.
c) El conector ATX 12V tiene 4, 6 u 8 pines.
d) La electricidad estática puede producir descargas de 4.000 o incluso más voltios.

14 Elija cuál de estas afirmaciones es verdadera:
a) La silicona térmica es un material compuesto en un 75% por cianocrilato, el resto son materiales conductores.
b) Las pulseras metálicas evitan la acumulación de energía estática.

c) Hay que evitar no poner la placa base o *motherboard* encima de la bolsa que la contiene puesto que puede haberse almacenado la carga electrostática en la zona externa.
d) La configuración *cable-select* de los discos duros hace que el disco se autoconfigure a partir de la posición que ocupa en el cable.

15 Elija cuál de estas afirmaciones es verdadera:
a) El conector ATX tiene 24 pines.
b) Antes de instalar un disco PATA o SATA hay que verificar la configuración de los *jumpers*.
c) La pasta térmica no debe ser conductora pues puede producir problemas con los componentes del equipo.
d) Hay que evitar el contacto del disipador con cualquier líquido o alcohol para evitar la oxidación del mismo.

16 Elija cuál de estas afirmaciones es verdadera:
a) Existe un zócalo universal TRX-10 que permite instalación de micros Intel® o AMD® sin distinción.
b) Un disco se puede configurar en modo *Master* o bien en *Single drive* si lo que se quiere es instalar un segundo disco.
c) Los cables PATA o SATA envían y reciben datos de la placa al disco, y viceversa, en serie.
d) Los cables SATA no tienen 40 u 80 hilos.

4 Puesta a punto y configuración de un sistema informático

OBJETIVOS DEL CAPÍTULO

- ✓ Conocer los sistemas operativos más utilizados en la actualidad y reconocer las diferencias existentes entre ellos.
- ✓ Conocer los sistemas operativos de sistemas móviles y reconocer su importancia y evolución.
- ✓ Estudiar los pasos a realizar en la instalación de los sistemas operativos.
- ✓ Saber los parámetros y software que hay que instalar y configurar en una instalación estándar.
- ✓ Conocer las herramientas y software básico más utilizadas así como su utilización.
- ✓ Verificar la instalación de un sistema operativo.

4.1 SISTEMAS OPERATIVOS EN LA ACTUALIDAD

Los sistemas operativos siguen evolucionando aunque hoy día y desde hace unos años ofrecen unas **características básicas** comunes:

- En computadoras, el SO empieza a funcionar cuando finaliza el trabajo de la BIOS al encenderse o reiniciar la máquina.
- Poseen una **interfaz** que puede ser gráfica (entornos GUI) o de texto (línea de comandos).
- Son **multiusuario** (permite el manejo por parte de diferentes usuarios cada uno con su configuración personalizada).
- Son **multitarea** (pueden ejecutar varios programas, llamados "procesos", simultáneamente).
- Forman parte de una familia o **plataforma**, donde diferentes aplicaciones y herramientas son compatibles entre sí.
- Soportan uno o varios **sistemas de archivos**, destacando FAT, FAT32 y NTFS (Windows®), HFS, HFS+ (Mac), Ext2, Ext3, Ext4 (Linux).
- Ofrecen **herramientas** similares con distintos nombres: Administrador de Archivos, Panel de Control, Utilidades de diagnóstico y seguridad, etc.

En la actualidad son tres plataformas las que abarcan casi todo el mercado de computadores: **Plataforma Windows®**, **Plataforma GNU/Linux y Plataforma MAC OS®** aunque se van abriendo camino otras propuestas como **Google Chrome**, **Craythur**, **Desktoptwo**, **EyeOS**, **Glide**, **Goowy**, **Orca**, **etc**.

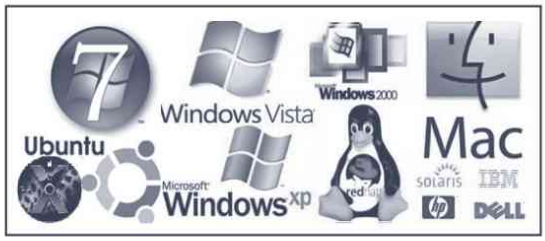


***Figura. 4.1**. Imágenes corporativas de sistemas operativos sobremesa*

Por otro lado existen también sistemas operativos concebidos para dispositivos móviles como *smartphone*, *tablet* o PDA, entre los que destacan **Android** (basado en núcleo Linux), **BADA®**, **Symbian OS®**, **Palm OS®**, **iPhone OS®** y **Windows® Mobile**.

***Figura 4.2**. Imágenes corporativas de sistemas operativos en dispositivos móviles*

¿SABÍAS QUE...?

Google Chrome está creado en la filosofía *cloud computing* (cómputo en la nube, nube en referencia a Internet), la cual se basa en un paradigma con el propósito de crear servicios a través de Internet. La idea es que los usuarios accedan a estos servicios y que en algunos casos sean de pago.

4.1.1 PLATAFORMA WINDOWS®

La Plataforma Windows® es sin duda la más empleada en el sector de usuarios más extenso, el usuario doméstico, con conocimientos informáticos escasos o nulos, aunque también está muy presente en la pequeña y mediana empresa.

Dicha plataforma fue desarrollada por **Microsoft®**, empresa fundada por Bill Gates y Paul Allen en 1975 dedicada al sector de la informática, con sede en Redmond (Washington), que creó en 1981 su primer sistema operativo, el PC DOS 1.0, que llegó a evolucionar hasta su última versión, MS-DOS 6.22 (1994). Este sistema operativo fue reemplazado por distribuciones que ofrecían una interfaz gráfica de usuario estándar (GUI), con ventanas, iconos, botones y un empleo intensivo del ratón, desde Windows® 3.0 (1990) hasta el actual **Windows® 7** (2009), pasando por innumerables distribuciones y versiones: Windows® 95/98/2000/XP/NT/Me/Vista /Server 2003/otras.

¿SABÍAS QUE...?

Increíble pero cierto: **Microsoft®** fue una de las primeras compañías en desarrollar software para **Apple**. Su fundador, **Steve Jobs**, tenía muy claro que necesitaba software para que **Macintosh®** fuese un éxito, y **Microsoft®** era la solución. En sus orígenes, la empresa de **Bill Gates** se especializaba en los lenguajes de programación y son creadores de Basic y Fortran. Más tarde comprarían y revenderían a **IBM** el **DOS** accediendo al mercado de los **Sistemas Operativos**.
Para poder escribir un programa de ordenador, es necesario conocerlo todo sobre él, por lo que Jobs tuvo que mostrar a **Microsoft®** los primeros prototipos de Macintosh®. A Bill Gates le causó muy buena impresión el sistema operativo de **Apple**, y comenzó a buscar la forma de emplear los **iconos**, **ventanas** y **ratón** en la plataforma **IBM PC**.
Según cuentan algunos, **Gates** presionó a **Jobs** para que le permitiera utilizar partes de la **interfaz** de **Macintosh®** en **PC**, a cambio de no demorar el lanzamiento de las aplicaciones que **Apple** necesitaba. Esto sería el detonante para lo que luego se llamaría **Windows 1.0**. Todas las futuras demandas legales de **Apple** contra **Microsoft®** por el uso de algunos elementos de la **GUI** se vieron debilitadas debido a este antiguo acuerdo entre ambas empresas.

Existen diferentes distribuciones del sistema operativo según su uso: **personal**, **empresarial** o **servidores**. Es el sistema operativo que más amplia gama de aplicaciones disponibles ofrece destacando aquellas con capacidad multimedia y de comunicación.

4.1.2 PLATAFORMA GNU/LINUX

Es uno de los términos empleados para referirse al sistema operativo **libre** similar a Unix que utiliza el núcleo Linux y herramientas de sistema GNU.

Fue creado por **Linus Torvalds** en 1991 que creó el primer núcleo Linux. Por aquel entonces, el Proyecto GNU, iniciado por **Richard Stallman** en 1983, ya había creado muchos de los componentes para conseguir un entorno operativo en software libre.

¿SABÍAS QUE...?

GNU es un acrónimo recursivo que significa *GNU no es Unix* (**GNU is Not Unix**), puesto que en inglés "*gnu*" se pronuncia igual que "*new*".
Richard Stallman recomienda pronunciarlo "*guh-noo*". En español, se recomienda pronunciarlo "*ñu*" como el animal o fonéticamente deletreado (G-N-U) para su mejor comprensión.
En sus charlas, Richard Stallman, finalmente dice siempre: "*Se puede pronunciar de cualquier forma, la única pronunciación errónea es decirle Linux*".

Desde entonces han aparecido diferentes distribuciones de éste sistema operativo entre las que destacan **Debian**, **Slackware**, **Gentoo** o **Ubuntu**.

Muchas distribuciones permiten el arranque del sistema directamente desde un CD, DVD o unidad de almacenamiento USB o de red (llamados **livecd**), sin modificar el disco duro del ordenador en el que se ejecuta.

Algunas **características** de GNU/Linux son:

- ✓ Soporta tecnología *Plug&Play*.
- ✓ Amplia gama de aplicaciones disponibles y cada vez mayor con el respaldo de compañías como Nero, Java, Google o Adobe.
- ✓ Herramientas avanzadas de seguridad y administración de redes.
- ✓ Prácticamente inmune a los virus y otras amenazas.
- ✓ Es software libre lo que ha permitido cambiarlo, modificarlo y volverlo a distribuir con la configuración y apariencia que se quiera.

Hoy día hay varias empresas que comercializan soluciones basadas en GNU/Linux (IBM, Novell -SuSe-, Red Hat, Canonical Ltd -Ubuntu-), y existen ya muchas empresas que ofrecen productos o servicios basados en esta tecnología.

***Figura. 4.3**. Distribuciones Linux principales*

4.1.3 PLATAFORMA MAC OS

Mac OS es el nombre del entorno operativo creado por **Apple** para sus equipos. Fue el primer entorno operativo que contó con una interfaz gráfica concebida para la interacción con el ratón y que empleaba ventanas, iconos y menús.

Su primera versión vio la luz en 1984. Ha pasado por diferentes distribuciones (System 6, System 7, Mac OS 8, Mac OS 9 y Mac OS X) y que ha pasado por diferentes versiones (Mac OS X v10.1"Puma" -2001-) hasta llegar a **Mac OS X v10.8 "Mountain Lion"** (2012).

***Figura. 4.4**. MacOS-X Leopard*

MAC OS X ofrece una plataforma muy estable y segura con elementos como la multitarea preventiva y la memoria protegida, así como una interfaz gráfica llamada *Aqua*, con elementos de efectos de agua y empleo de la tecnología *antialiasing*, muy atractiva e intuitiva.

4.1.4 SISTEMAS OPERATIVOS DE DISPOSITIVOS MÓVILES

Palm OS

Es un sistema operativo de la compañía Palm que lleva mucho tiempo en el mercado, al igual que las PDA que lo utilizan. No es software libre y esta desarrollado por PalmSource Inc. Existen multitud de aplicaciones que pueden funcionar en este sistema operativo (más de 19.000, incluso algunas con código abierto). Su última versión es webOS y se incorpora en su teléfono Palm Pre. La empresa espera en el futuro crear más teléfonos que incorporen este sistema operativo.

Windows® Mobile

Es el sistema creado desde cero por Microsoft® para teléfonos móviles. También se puede encontrar este sistema operativo en Pocket PC o PDA y *media center* portátiles. Aunque estos dispositivos comparten el sistema operativo y tiene una apariencia común, existen aplicaciones que funcionan en un dispositivo y no en el otro. Como casi todos los productos de Microsoft®, Windows® Mobile no es código libre.

iPhone OS

Es el sistema operativo que utiliza el iPhone y también el iPod Touch. Ni qué decir tiene que todos estos nombres precedidos por una *i* provienen de la empresa Apple. El sistema operativo es una variante de su sistema operativo Mac OS X.

El sistema operativo es de código cerrado pero mediante iTunes (la tienda en Internet de Apple) se pueden conseguir actualizaciones de forma gratuita para el iPhone.

BlackBerry OS

Sistema operativo desarrollado por RIM (*Research In Motion*) para sus dispositivos BlackBerry. Es un sistema operativo multitarea y solo pueden ejecutarse en él aplicaciones proporcionadas por RIM o firmadas por ellos.

Symbian

Es un sistema operativo muy extendido. Esta desarrollado en base a la alianza de una serie de compañías como son Nokia®, Sony Ericsson®, PSION, Samsung®, Siemens®, Arima®, Benq®, Fujitsu®, Lenovov, LG®, Motorola®, Mitsubishi Electric®, Panasonic®, Sharp®, etc.

Está desarrollado bajo licencia EPL (*Eclipse Public License*), la cual puede considerarse como código abierto.

Android

Sistema operativo desarrollado por el grupo Open Handset Alliance, formado por más de 30 empresas de tecnología y móviles, entre ellas Google. Es una plataforma móvil completamente abierta y gratuita y desde su web te animan a desarrollar software para Android. Este sistema operativo esta basado en Linux y Java. Algunos expertos dicen que es el sistema operativo del futuro para este tipo de aparatos.

¿SABÍAS QUE...?

Oracle Corp®, empresa que compro Sun Microsystems® y propietaria de los derechos sobre Java, demandó a Google por la violación de la propiedad intelectual en la utilización de Java en su sistema operativo Android.

Si algun programador quiere realizar una aplicación para Android, puede desarrollarla con un SDK (*Software Development Kit* - kit de desarrollo de software) y Java aunque puede también utilizar el NDK (*Native Development Kit* o kit de desarrollo nativo) en el que se puede programar en C y que proporciona Google.

Las versiones de Android se llaman con nombres de postres. Las últimas versiones actualmente son la 4.1 (*Jelly Bean*), 4.0 (*Ice Cream Sandwich*), 3.x (*Honeycomb*) y la 2.3 (*Gingerbread*).

Como se explicaba anteriormente, Android es un sistema operativo libre y, por tanto, se puede tener acceso al código fuente pero muchas veces no se pueden actualizar los dispositivos a la última versión porque se requieren los *drivers* del dispositivo para esa versión de sistema operativo. Un *driver* es un software que hace que el sistema operativo se pueda comunicar con el hardware del dispositivo.

Android corre sobre varias plataformas hardware como la x86 o microprocesadores Intel®, los procesadores MIPS que son unos procesadores RISC fabricados por MIPS Technologies o los famosos procesadores ARM (*Advanced Risc Machines*) que son procesadores diseñados por la empresa Acorn Computers.

***Figura 4.5**. Arquitectura de Android*

La arquitectura, como se puede observar en la figura anterior, está compuesta de una serie de aplicaciones (SMS, brújula, calendario, mapas, contactos, navegador, etc.) similares a las que pueda tener un iPhone en su sistema iPhone OS. Esta serie de aplicaciones funciona sobre un Framework de aplicaciones tiene una serie de API (*Application Programming Interface*) que son una serie de funciones y procedimientos que permiten que los desarrolladores puedan realizar aplicaciones sin conocer a fondo las "tripas" de Android. Sin estas API sería imposible obtener tantas aplicaciones como se tienen actualmente. El Framework hace uso de las librerías de Android que están escritas en C y C++, lenguajes muy utilizados en el desarrollo de sistemas operativos. El *Android runtime* son una serie de librerías que contienen funciones de librerías base de Java. Por último, está el núcleo o kernel de Linux que es el que ejecuta las funciones básicas del sistema (gestión de la memoria, gestión de los procesos, seguridad, etc.).

***Figura 4.6**. Interfaz del sistema Android. Fuente Laihiu*

Bada

BADA es un sistema operativo para dispositivos móviles desarrollado por Samsung®. *Bada* es una palabra coreana que significa *océano*, este nombre supuestamente representa la filosofía que quiere Samsung® para su sistema operativo (potencial sin limitaciones). El primer dispositivo que ha utilizado este sistema operativo es el *smartphone* de Samsung® Wave S8500. Samsung® en principio desarrolló aplicaciones para este sistema operativo pero cualquier desarrollador puede realizar aplicaciones para Bada.

Samsung® siempre ha realizado desarrollos de sistemas operativos para dispositivos móviles pero de carácter propietario. Bada cambia toda esta filosofía hacia una plataforma de desarrollo abierto.

Para más información sobre este sistema operativo se puede acceder a *www.bada.com*. En este sitio está disponible el SDK (kit de desarrollo de software) de Bada para cualquier programador.

***Figura 4.7**. Sistema Bada de Samsung®*

La figura anterior muestra un *smartphone* Samsung® con Bada, el cual tiene cierto parecido al sistema operativo iPhone OS.

BoottoGecko (B2G) de Mozilla

Es una plataforma totalmente abierta, lo cual cambia la filosofía actualmente existente de sistemas operativos para móviles. El problema que hay actualmente en el mundo de los sistemas operativos para móviles es que no hay una plataforma verdaderamente abierta. Aunque se etiqueten como abiertas, algunas plataformas están monopolizadas por una empresa con intereses comerciales concretos y que, a la postre, toma las decisiones sobre el sistema operativo.

Esta plataforma se basa sobre el estándar HTML5, javascript y otras tecnologías de código abierto. La ventaja que ofrece este sistema es el poder acceder a todos los elementos del teléfono.

Otros sistemas

Aparte de estos sistemas operativos móviles que hemos visto hay numerosos proyectos como Maemo y Moblin, que son sistemas basados en Linux. A partir de estos dos sistemas aparece MeeGo que es la unión de ambos y es el sistema de Nokia e Intel® para hacerle la competencia al Android de Google. MeeGo es básicamente una distribución Linux que da soporte a microprocesadores Intel® Atom y ARM.

Figura 4.8. *Sistema MeeGo. Fuente Animaster*

4.2 INSTALACIÓN DE SISTEMAS OPERATIVOS

En esta sección se van a dar una serie de consejos y pasos de cómo se instalan la mayoría de sistemas operativos. Generalmente, los sistemas operativos convencionales (Windows® o Linux) son similares en su instalación.

4.2.1 PASOS EN LA INSTALACIÓN DE UN SISTEMA OPERATIVO

1. Configuración del dispositivo de arranque en la BIOS.
2. Particionamiento del disco duro.
3. Ejecución del programa de instalación.
4. Elección y configuración del usuario o usuarios que van a administrar el sistema.
5. Seleccionar los componentes software a instalar.
6. Configurar los parámetros de *networking*.
7. Instalar el gestor de arranque y el resto del sistema operativo.
8. Actualizaciones de seguridad y demás parches.
9. Instalar los *plugins* del navegador.
10. Instalar los *drivers* de los dispositivos que se vayan a utilizar.

4.2.2 CONFIGURACIÓN DEL DISPOSITIVO DE ARRANQUE EN LA BIOS

La secuencia de arranque de un equipo es el orden que seguirá el equipo para la búsqueda y carga del sistema operativo. Generalmente, los equipos arrancan el sistema operativo que está instalado en el disco duro pero podrían arrancar un sistema operativo contenido en un DVD/CD o bien pueden arrancar desde un dispositivo USB, tarjeta de red…

Una operación frecuente es reemplazar en el equipo el sistema operativo. Para ello eliminaremos el sistema operativo instalado en el equipo por uno contenido en un DVD.

EJERCICIO 4.1

CAMBIO DE LA SECUENCIA DE ARRANQUE DEL EQUIPO

Paso 1. El primer paso consistirá en entrar en la BIOS. Para ello durante el arranque y después del pitido aparece el mensaje "*Press Del to Enter BIOS Setup*". En ese mismo momento pulsaremos la tecla **Supr** y entraremos en la BIOS. Hay que ser rápido pues no hay mucho tiempo desde que aparece el mensaje hasta que la BIOS continúa con la secuencia de arranque. Es posible que el mensaje o la tecla sean diferentes de las comentadas en este paso.

***Figura 4.9**. Detalle de la BIOS*

Paso 2. Una vez dentro de la BIOS (*CMOS BIOS Setup*), que es el famoso programa de fondo azul, elegiremos la opción **Advanced Setup** o **Advanced features** y verificaremos que en la opción **First Boot Device** tenemos configurado nuestro lector óptico como primera opción de arranque o un dispositivo USB que actúe como disco de arranque si nuestro equipo carece de lector óptico.

***Figura 4.10**. Opción "Advanced BIOS Features" de la BIOS*

Paso 3. Una vez que hemos comprobado que la secuencia de arranque es la deseada habrá que grabar los cambios y salir de la BIOS (**Save and Exit**).

Es posible que el nombre de las opciones difiera de una BIOS a otra. En ese caso elija la opción correcta.

¿SABÍAS QUE...?

Cada vez más ordenadores portátiles (todos los *netbook* y *tablet*) vienen sin lector de CD por razones de tamaño y peso. Estos equipos deben de ser instalados mediante un dispositivo USB que actúe como disco de arranque.

4.2.3 PARTICIONAMIENTO DEL DISCO DURO

Como ya se vio anteriormente, cualquier dispositivo es susceptible de ser particionado. En el particionamiento hay que tener claro cuales son las necesidades futuras que se van a tener en el equipo y realizar la configuración óptima para dicha máquina. No obstante, siempre se podrán modificar estas particiones utilizando la herramienta Gparted u otra parecida.

IMPORTANTE

En los sistemas Linux hay que hacer como mínimo una partición donde colocar el sistema de archivos y cuyo punto de montaje sea la raíz del sistema de archivos y una partición de *swap* o intercambio. Es aconsejable también realizar una partición donde residan las cuentas de usuarios y montar el directorio */home*.

Las ventajas de un buen particionamiento son la seguridad al poder separar sistema operativo de datos, la posibilidad de poder instalar varios sistemas operativos en la misma máquina o simplemente el orden (al tener varias particiones se pueden separar mejor los contenidos).

4.2.4 EJECUCIÓN DEL PROGRAMA DE INSTALACIÓN

Una vez realizado el particionamiento, el programa de instalación empieza a realizar el proceso de instalación del sistema en sí mismo.

***Figura 4.11**. Detalle del proceso de instalación de Ubuntu*

4.2.5 ELECCIÓN Y CONFIGURACIÓN DEL USUARIO O USUARIOS QUE VAN A ADMINISTRAR EL SISTEMA

Durante la instalación es cuando se tienen que crear las cuentas de superusuario o administrador del sistema junto con sus *passwords*. En los sistemas Unix y Linux el superusuario se denomina *root* mientras que en sistemas Windows® el superusuario se denomina *Administrador* (*Administrator* si el sistema está en inglés).

4.2.6 SELECCIONAR LOS COMPONENTES SOFTWARE A INSTALAR

Generalmente en las instalaciones el sistema se puede ajustar a las necesidades del usuario. Por defecto, el sistema se instalará con las opciones más típicas, pero en muchas ocasiones es aconsejable modificar esa propuesta inicial por otra que se ajuste mejor a las necesidades de uso que se le vayan a dar al equipo.

4.2.7 CONFIGURAR LOS PARÁMETROS DE NETWORKING

Generalmente todos los parámetros de red se reciben de forma automática debido a que el equipo recibe la IP y demás parámetros de forma dinámica mediante el protocolo DHCP. En caso contrario, estos datos se deberán de ajustar de manera manual. Los parámetros mínimos que se deberían de configurar son los siguientes:

- Dirección IP.
- Mascara de subred.
- *Gateway* o puerta de enlace.
- DNS.

4.2.8 INSTALAR EL GESTOR DE ARRANQUE Y EL RESTO DEL SISTEMA OPERATIVO

El gestor de arranque se instala y configura automáticamente durante el proceso de instalación. En instalaciones duales, donde van a coexistir Windows® y Linux, se aconseja instalar primero Windows® y después Linux dado que Grub que es el gestor de arranque de Linux detecta la existencia de otros sistemas operativos y los añadirá en su arranque como posibles sistemas operativos a cargar. NTLDR que es el cargador de Windows® no respeta esto y dejará Windows® como único sistema operativo disponible en la máquina.

CONSEJO

Si se quiere instalar primero Linux y luego Windows en una máquina, habrá que recuperar el Grub para poder acceder a ambos sistemas. La mejor manera de realizar esto es utilizar la herramienta SuperGrub o Rescatux (*http://www.supergrubdisk.org/*).

4.2.9 ACTUALIZACIONES DE SEGURIDAD Y DEMÁS PARCHES

Este paso es uno de los más importantes en la instalación de un sistema operativo. Desde que se generó el sistema operativo que se va a instalar hasta la fecha pasó quizás mucho tiempo y el sistema es ahora vulnerable a posibles intrusos, virus, agujeros del sistema operativo y del navegador, etc. Es el momento de aplicar todas las actualizaciones

de seguridad creadas hasta el momento. En Windows® será *Windows® update* el proceso para actualizar estos parches de seguridad (cuando hay muchos parches Windows® distribuye un *service pack* con todas las actualizaciones). Linux funciona de manera análoga.

4.2.10 INSTALAR LOS PLUGINS DEL NAVEGADOR

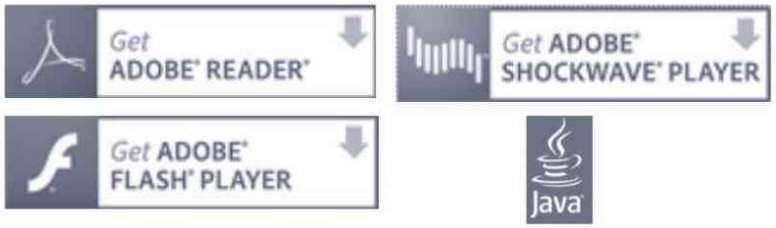


***Figura 4.12**. Plugins del navegador*

Los *plugins* se pueden considerar como complementos del navegador. Generalmente los navegadores vienen sin ellos y se instalan a posteriori. Algunos complementos del navegador son:

- **Adobe flash/Adobe sockwave**. Permiten visualizar el contenido multimedia en el navegador. Descargables en *www.adobe.com*. El *plugin sockwave player* está menos extendido que el *flash player*. Ambos realizan las mismas funciones, quizás el segundo tiene un mejor rendimiento y ciertos contenidos desarrollados para *sockwave* no son reproducibles con *flash player*.
- **Adobe reader**. Si se quiere visualizar contenido PDF en el navegador (cosa bastante común por cierto) hay que instalar este *plugin*. Descargable en *www.adobe.com*.
- **Java**. Permite jugar *on line*, utilizar *chats*, ejecutar aplicaciones, visualizar objetos tridimensionales, etc. Descargable en *http://www.java.com/es/download/*.
- **Otros complementos del navegador**. Aparte de los anteriormente mencionados, que son los más utilizados, los navegadores permiten la instalación de múltiples complementos los cuales aumentan las funcionalidades del navegador con motores de búsqueda, diccionarios, cambios de apariencia, etc.

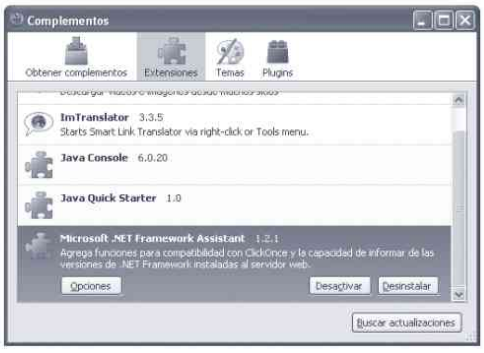


***Figura 4.13**. Otros complementos del navegador*

4.2.11 INSTALAR LOS DRIVERS DE LOS DISPOSITIVOS QUE SE VAYAN A UTILIZAR

Se aconseja que siempre que se instala un equipo se actualicen los *drivers* a las últimas versiones del mismo. De esta manera se subsanarán posibles problemas que puedan tener los *drivers* o una ejecución mucho más rápida del sistema. Generalmente, todo el hardware viene de fábrica con sus *drivers* correspondientes. Si se quiere descargar la última versión bastará con acceder a la página web del fabricante.

Se necesitarán instalar en el equipo los *drivers* de la placa base, controladora de vídeo, controladora de red, tarjeta de sonido, sintonizadora de TV, impresoras, etc.

4.3 VERIFICACIÓN FINAL DEL EQUIPO

IMPORTANTE

Dependiendo de la configuración del equipo las comprobaciones son diferentes. Por ejemplo, en el caso de un equipo que tenga una unidad de cinta para *backup* deberíamos de hacer un *backup* y una restauración para comprobar que todo funciona correctamente.

Una vez instalado el sistema, el siguiente paso es verificar que la instalación ha sido exitosa. Generalmente, si durante el proceso de instalación el sistema operativo no ha mostrado ningún mensaje de error o problema, lo más seguro es que la instalación haya ido bien. A continuación se van a detallar una serie de pasos que, como mínimo, se deberán realizar tras una instalación.

Verificar el acceso a la red

Para verificar el acceso a la red una de las herramientas fundamentales es la utilidad *ping*.

RECUERDA

En ocasiones, antes de seguir los pasos del ejercicio anterior, basta con abrir un explorador y probar a conectarnos a alguna página web muy utilizada. Si podemos navegar si problemas por la página se entiende que la conexión de *networking* funciona.

Probar Adobe flashplayer

En Internet mucho contenido de páginas web y demás es *flash*. En la siguiente dirección se puede comprobar este *plugin* del navegador.

http://www.adobe.com/es/shockwave/welcome/

Verificar sonido y vídeo

La mejor manera de verificar este punto es reproducir un vídeo (que tenga sonido, por supuesto).

Verificar la instalación de Java

Java lo vamos a necesitar si tenemos que hacer operaciones con el navegador que hagan uso del mismo. Muchas páginas web necesitan que el cliente tenga Java instalado. En la siguiente dirección se puede comprobar si tenemos java instalado en el equipo y si estamos utilizando la última versión.

http://www.java.com/es/download/installed.jsp

Comprobar la impresora

El mejor consejo sobre impresoras es el de instalar la última versión del *driver*. En muchas ocasiones el *driver* que proporciona el fabricante junto con la impresora no es la última versión y podríamos tener algún pequeño problema en su utilización. Generalmente, la mejor opción para comprobar una impresora es utilizando el software que distribuye el fabricante y que tiene utilidades con esta finalidad.

Otras comprobaciones

En este paso se deberían de comprobar todos los periféricos del equipo y su funcionamiento, así como las posibles características particulares de la configuración del equipo.

IMPORTANTE

Si vamos a actualizar el sistema operativo de un equipo hay que verificar si existen los *drivers* para este nuevo sistema operativo.

RESUMEN DEL CAPÍTULO

Este capítulo tiene como objetivo el que el alumno conozca los distintos sistemas operativos existentes en la actualidad así como sus características y en qué dispositivos se instalan.

En la actualidad el uso de los sistemas operativos de sistemas móviles se está extendiendo cada vez más y es importante que el alumno se familiarice con ellos y sepa de sus características.

Generalmente, en la instalación de sistemas operativos se siguen una serie de pasos y a lo largo del Apartado 4.2 de este capítulo se detallan cada uno de ellos.

Una vez que se instala el sistema operativo lo más común es instalar un antivirus (obligatorio en Windows®), alguna utilidad de grabación, algún cortafuegos, etc. En el tercer apartado del capítulo se muestran algunas utilidades muy comunes.

El último paso de todos es la verificación de la instalación, en el capítulo se ofrecerán una serie de consejos para la misma. La verificación de la instalación será diferente dependiendo las características del sistema montado.

EJERCICIOS PROPUESTOS

1. Enumere las diferentes versiones de Windows® por las que se ha pasado tratando de identificar el período de vigencia y las características más relevantes.

2. Describa las principales distribuciones Linux a nivel mundial así como las diferentes distribuciones Linux que se ofrecen en España por comunidades.

3. Estudie los requerimientos y prestaciones de las principales distribuciones en las diferentes plataformas: Windows® 7, Ubuntu 9.10, MAC OS X.

4. Elabore un historial de los diversos sistemas operativos que ha manejado, así como las distintas aplicaciones que haya utilizado. Desde que empezó a hacer uso del software, ¿cuáles han sido las diferencias más significativas que ha encontrado con respecto al software actual?

5. Cálculo MD5 de una distribución.

Descárguese la última distribución de Ubuntu en cualquiera de sus versiones y realice la comprobación MD5 del archivo. Compárela con las firmas proporcionadas por Canonical.

6. Antivirus en Linux.

Instale algún antivirus para Linux tipo NOD32 o similar. Escanee tanto su equipo como alguna unidad de red en la que se compartan ficheros.

TEST DE CONOCIMIENTOS

1 ¿Cuál de las siguientes afirmaciones es falsa?

a) Adobe reader es otro *plugin* de *flash* necesario para leer ficheros PDF.
b) Bada es un sistema operativo basado en núcleo Linux.
c) WMA es un formato de compresión con pérdida desarrollado por Microsoft®.
d) El primer sistema operativo que utilizó interfaz gráfica fue Mac OS.

2 ¿Cuál de las siguientes afirmaciones es falsa?

a) Paul Allen fue fundador de Microsoft®.
b) WMV es un *codec* de audio.
c) Una firma MD5 es como un resumen digital de un archivo.
d) Cuando se salva una imagen como JPG, la imagen resultante pierde calidad.

3 ¿Cuál de las siguientes afirmaciones es falsa?

a) Cuando se desea reproducir un vídeo o audio se necesitará el *codec* con el cual fue comprimido dicho audio o vídeo y no otro.
b) Symbian está desarrollado bajo licencia EPL, la cual puede considerarse como código abierto.
c) Oracle es la propietaria de Java.
d) El proyecto GNU fué iniciado por Linus Torvalds en 1991.

4 ¿Cuál de las siguientes afirmaciones es falsa?

a) El algoritmo del formato *7-zip* es un algoritmo de compresión sin pérdida.
b) Es posible tener más de 4 particiones en un disco.
c) MeeGo es una distribución Linux.
d) La interfaz gráfica de MS-DOS era más básica que la de Windows® 1.

5 ¿Cuál de las siguientes afirmaciones es falsa?

a) El formato *zip* utiliza un algoritmo de compresión con pérdida.
b) El algoritmo *7-zip* es mejor que el algoritmo *zip*.
c) Con los algoritmos de compresión con pérdida una vez descomprimidos los datos no se obtienen los datos originales.
d) Es posible tener más de 4 particiones en un equipo.

6 ¿Cuál de las siguientes afirmaciones es verdadera?

a) Un disco no puede tener más de 4 particiones.
b) Es posible tener un disco con 2 particiones primarias y 5 lógicas.
c) *Adobe flash* y *Adobe shockwave flash* realizan prácticamente las mismas funciones nada más que el primero está menos extendido.
d) Un fichero *mp3* pierde calidad de sonido frente a uno *wav*.

5 Configuración de sistemas informáticos

OBJETIVOS DEL CAPÍTULO

- ✓ Conocer las características de la arquitectura cliente-servidor.
- ✓ Conocer las fases del arranque de un sistema operativo.
- ✓ Identificar qué es un servicio y cuáles son los fundamentos de configuración de los mismos.
- ✓ Conocer las posibilidades y herramientas de configuración de sistemas operativos y, más concretamente, Linux.
- ✓ Reconocer la importancia de la seguridad en un sistema.
- ✓ Conocer las implementaciones de grupos y permisos para establecer un sistema de seguridad en un sistema.
- ✓ Estudiar qué es la virtualización y conocer las herramientas de virtualización más utilizadas.

5.1 ARQUITECTURA CLIENTE/SERVIDOR

5.1.1 ¿QUÉ ES UNA ARQUITECTURA CLIENTE-SERVIDOR?

Hace mucho tiempo la mayoría de los ordenadores trabajaban *standalone*, esto quiere decir que estaban desconectados del mundo. Eran, por así decirlo, autónomos. En el caso de estar interconectados, cada uno hacía un trabajo normalmente siendo parte de una cadena y los datos se intercambiaban en ficheros y estos en muchas ocasiones dentro de un soporte. Estas eran las funciones de los centros de cálculo en donde vivían unos seres computacionales llamados *mainframes*. Antiguamente los *mainframes* eran los reyes de la informática (al igual que los dinosaurios en la tierra). Los clientes no tenían capacidad de cómputo. Los *mainframes* eran unas máquinas muy costosas y con una capacidad de cálculo muy grande. Ellos lo hacían todo, los clientes se limitaban simplemente a ser una mera pantalla. Esto empezó a cambiar con la irrupción y generalización del PC u ordenadores de bajo coste. En ese momento empezaron a aparecer los servicios o equipos dedicados a una tarea concreta (servidor de bases de datos por ejemplo). El precio y la capacidad de cálculo eran tan altos que valía la pena aligerar el peso de los servidores y dejar que los clientes hiciesen más trabajo para lo cual estaban perfectamente preparados.

Se puede entender la arquitectura cliente-servidor como una forma de explotar las aplicaciones divididas en dos partes, una de las cuales provee los servicios (servidor) y otra es la que demanda dichos servicios (cliente). Esta arquitectura es hardware y software puesto que el hardware condiciona al software, por así decirlo. Las funciones de todo el sistema están divididas y la línea que separa dónde está el lado del cliente y del servidor no está del todo fija. Generalmente los clientes operan en hardware distinto del servidor y a través de la Red.

5.1.2 CARACTERÍSTICAS DE LA ARQUITECTURA CLIENTE-SERVIDOR

- ✓ Un servidor suele ser un *host* que posee una gran capacidad de cómputo. Este equipo comparte sus recursos con los clientes.
- ✓ Los clientes no comparten sus recursos, su papel es el de pedir contenidos a los servidores o pedir servicios a dichos servidores.
- ✓ Generalmente, esta relación cliente-servidor se da en los programas que se ejecutan en los sistemas. Los programas cliente que residen en los *hosts clientes*, demandan servicios a los programas servidores que residen en los *hosts servidores*. La arquitectura cliente-servidor define la relación entre dos programas (cliente y servidor). Generalmente, el programa servidor está alojado en solo una máquina, aunque pudiese darse el caso de estar alojado en varias.
- ✓ Muchísimos servicios como el *email*, las páginas web, acceso a bases de datos, FTP... están basados en el modelo cliente-servidor.
- ✓ Por regla general, los servidores son equipos con mayor capacidad de procesamiento que los clientes.
- ✓ Los servidores pueden interactuar con múltiples tipos de clientes. Por ejemplo, un servidor web puede ser accedido por muchos clientes como *smartphones*, portátiles, PDA, *tablets*...

Actualmente, la arquitectura cliente-servidor está en vigor y muchas aplicaciones se desarrollan teniendo en cuenta este tipo de arquitectura. El funcionamiento de una arquitectura software cliente-servidor es bien sencillo, el cliente hace una petición a uno o varios servidores los cuales están interconectados. Estos servidores reciben las peticiones que son aceptadas o rechazadas. En el caso de que las peticiones sean aceptadas, éstas se procesan y se envían de vuelta a los clientes.

Tabla 5.1 Ejemplos de programas clientes y servidores

Cliente	Servidor
Clientes de *chat*	Servidores de impresión
Navegadores	Servidores de correo
Clientes de correo electrónico	Servidores DNS
	Servidores de bases de datos
	Servidores FTP
	Servidores web
	Servidores de aplicaciones

***Figura 5.1**. Arquitectura cliente servidor en un servidor de páginas estáticas*

En la anterior figura se puede apreciar la típica arquitectura cliente servidor. Este sistema consiste en un servidor web y un *browser*, navegador o cliente *http*. En el primer paso de todos, el cliente efectúa la petición de la página. En el segundo paso el servidor localiza la página solicitada y en el paso tres el servidor envía dicho documento en formato HTML o un mensaje de error en caso de que la página no sea encontrada. Por último, en el cuarto paso, el navegador interpreta el documento y presenta en pantalla la página resultante.

5.1.3 FUNCIONES DE LOS CLIENTES Y SERVIDORES

La división de las funciones entre los clientes y los servidores no es algo estricto. En ocasiones los clientes realizan muchas funciones o aquellas que requieren una mayor capacidad de procesamiento y, en ese caso, se podrían denominar **clientes gruesos o pesados**, y en otras ocasiones los clientes realizan pocas funciones o las que realizan son una mera visualización de los datos con pocos requerimientos de procesamiento y podríamos denominar a los clientes como **clientes livianos o ligeros**.

RECUERDA

En ocasiones los clientes livianos lo único que corren es un navegador web, mientras que los clientes pesados hacen tantas tareas como sea posible pasando solamente datos al servidor para su recuperación o almacenaje.

***Figura 5.2**. Cliente liviano o thin client. Fuente www.viagallery.com*

En la siguiente tabla se ofrecen una serie de funciones realizadas por los clientes y los servidores:

Tabla 5.2 Funciones de los clientes y servidores en una arquitectura cliente-servidor

Cliente	Servidor
Gestión de la interfaz de usuario. El cliente es el encargado de gestionar la interfaz del cliente. El servidor solamente envía los datos y es el cliente el que tiene que organizarlos y mostrarlos de forma adecuada.	Control de accesos. Se realizarán los controles de accesos a los servicios, aplicaciones, se controlarán también los accesos concurrentes a bases de datos compartidas, etc.
Captura y validación de los datos de entrada. El cliente se encargará de que los datos enviados al servidor estén validados correctamente.	Comunicaciones. En el caso de que los servicios tengan que comunicarse con otros servicios en la misma red o en otras redes, será función del servidor realizar estas tareas.
Otro tipo de tareas como generación de consultas sobre base de datos, generación de informes, almacenaje local de información, etc.	Gestión de periféricos compartidos. Generalmente los servicios compartidos (impresoras, fax, etc) son gestionados por los servidores.

5.1.4 ARQUITECTURAS PEER-TO-PEER O P2P

En las arquitecturas *peer to peer* cualquier cliente puede ser cliente y servidor a la vez. Cada *host* en una red P2P tiene las mismas funciones. Son los mismos programas los que funcionan como cliente y servidor (Emule es un claro ejemplo de ello). Las arquitecturas cliente-servidor suelen denominarse centralizadas mientras que las arquitecturas P2P se denominan descentralizadas. Estas arquitecturas descentralizadas en ocasiones suelen ser más robustas debido a que la pérdida de un nodo no implica la paralización del sistema. También en el caso de que el servidor acepte mucho tráfico, éste puede congestionarse, lo cual sería más difícil que ocurriera en una red P2P donde no existen estos cuellos de botella.

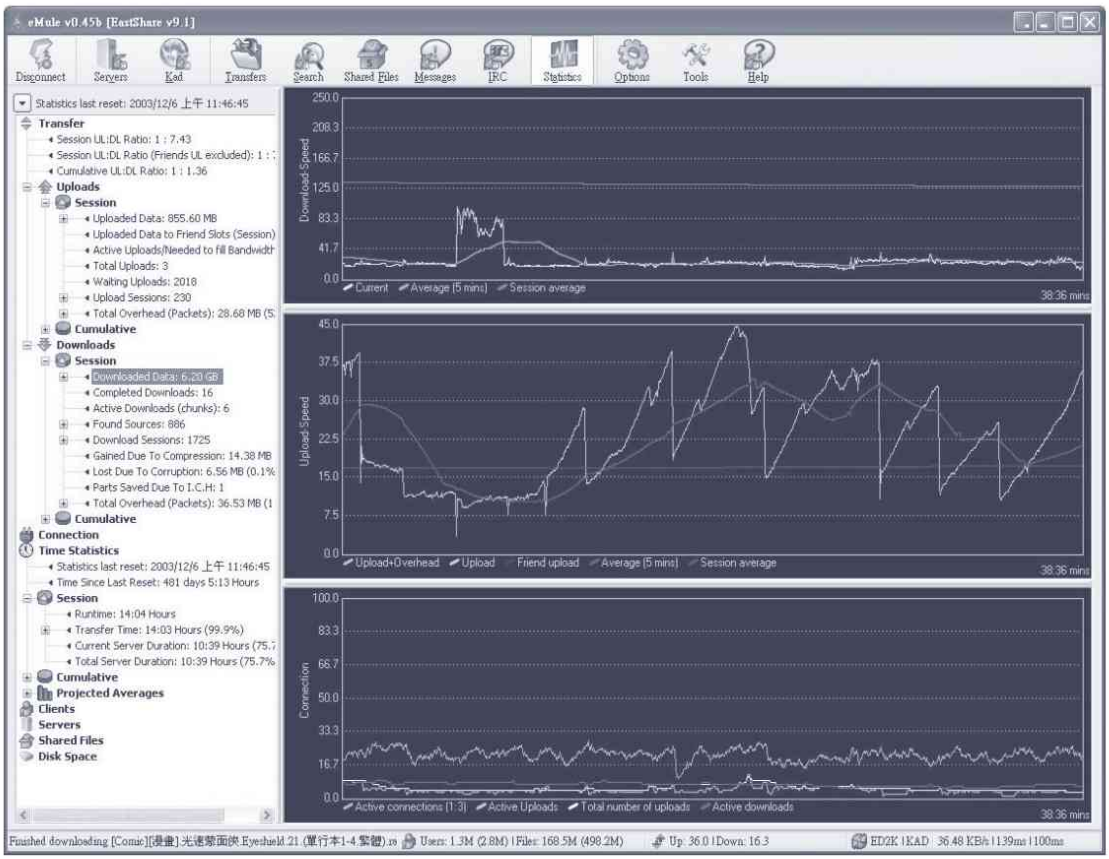


***Figura 5.3**. Emule funcionando. Información de tráfico. Fuente Lordcolus*

CONSEJO

Si lo que se desea es la seguridad de la información, la arquitectura cliente-servidor suele ser más adecuada que la distribuida (como las redes P2P) porque los datos están centralizados y se pueden aplicar mejor mecanismos de seguridad. La actualización de datos también es más sencilla en una arquitectura C/S dado que no hay que replicar información al estar ésta centralizada.

5.2 ADMINISTRACIÓN DE SERVICIOS EN SISTEMAS OPERATIVOS

Para este apartado vamos a centrarnos en un sistema operativo concreto. Se ha elegido Linux y más concretamente Ubuntu Linux. En sistemas Windows® la filosofía es parecida aunque las herramientas de configuración sean diferentes.

5.2.1 ¿CÓMO ARRANCA UN EQUIPO?

Antes de ver qué es un servicio vamos a ver cómo es la secuencia de arranque de un equipo con sistema operativo Linux y en qué momento se cargan los servicios, de esa forma será más fácil ubicar su importancia y ponerlos en contexto.

***Figura 5.4**. Secuencia de arranque de un equipo*

En la figura anterior se puede ver cuáles son los pasos en la secuencia de arranque de un equipo Linux. A continuación se explicará cada uno de estos pasos más en detalle.

1 (**BIOS**): la BIOS realiza el POST (*Power On Self Test*), el cual se encarga de realizar un autodiagnóstico del hardware del equipo. Si encuentra algún problema, el POST avisará del mismo con una secuencia de pitidos, cada secuencia indicará un error u otro. Una vez realizado el POST, la BIOS busca el dispositivo de arranque según la secuencia de búsqueda que está predeterminada en la misma (esta secuencia se puede modificar en la propia BIOS, haciendo que arranque primero desde el disco duro, lector de DVD…). Esta unidad debe estar marcada como *bootable* o arrancable. El sector de arranque es el primer sector de todo disco. Cada sector contiene 512 bytes y el primer sector o sector 0 es el sector de arranque del disco. Está situado en la pista más externa del disco. Es aquí donde buscará la BIOS para arrancar el sistema operativo. Normalmente, en esos 512 bytes se encuentra un pequeño programa (*Boot Manager*) que realiza la carga del sistema operativo. Como 512 bytes es muy poco, normalmente en este espacio sólo se almacena parte del *Boot Manager*, la otra parte se almacena en otra parte del disco.

2 (**BOOT**): en esta fase se cargará el *Boot Manager*. El *Boot Manager* es un pequeño programa que permite cargar el sistema operativo. Su función es cargar el sistema operativo elegido por el usuario en el caso de que haya varios sistemas operativos instalados en dicha máquina. Gracias a este programa nos permite tener varios sistemas operativos en una misma máquina. Existen múltiples programas de este tipo dependiendo del sistema operativo, los más conocidos son los siguientes:

- Sistema operativo Linux:
  - LILO
  - GRUB
- Sistema operativo Windows®:
  - NTLDR

El Boot Manager en Linux se encuentra en */boot*.

ACTIVIDADES 5.1

» Eche un vistazo al directorio */boot* de su sistema Linux.

3 (**KERNEL**): en esta fase se cargará el Kernel. El kernel entre otras cosas verificará la configuración hardware, configurará los *drivers* necesarios para el sistema y montará el sistema de archivos. En esta parte de la ejecución se muestran muchos mensajes informativos.

4 (**INIT**): tras la carga del kernel se ejecutará el proceso Init. Init está iniciado por el kernel y tiene un PID (*Process IDentificator*) o identificador de proceso número 1. Es el primer proceso del sistema y padre de los demás procesos del sistema. El funcionamiento de Init se configura en */etc/inittab*. El cometido de Init es ejecutar una serie de *scripts* (programas) que activan los servicios que hacen funcionar el sistema.

En este paso, Init ejecutará todos los *scripts* genéricos por orden alfabético que se encuentran en el directorio */etc/rcS.d* y comiencen por *S* (*start*).

5 (**CARGA DE SERVICIOS Y APLICACIONES**): una vez ejecutados los *scripts* genéricos, se ejecutarán los *script* correspondientes al *runlevel* o nivel de ejecución. Existen una serie de *runlevels* del 0 al 6 que no son ni más ni menos que diferentes configuraciones de arranque (ejecución de diferentes servicios). El *runlevel* 0 se ejecuta para parar el sistema, el 1 para arrancar en modo monousuario y sirve para realizar tareas de administración en el sistema, del 2 al 5 sirven para un arranque normal y el 6 se ejecuta para reiniciar el sistema (*reboot*). El nivel de ejecución por defecto o *runlevel* por defecto en Ubuntu es el 2 (los demás se utilizan en situaciones especiales). El *runlevel* por defecto se configura en el fichero */etc/inittab*.

Una vez que se ejecuta el *runlevel* deseado se ejecutarán los *script* situados en */etc/rcX.d*, donde *X* es el nivel de ejecución que se quiere ejecutar. Se ejecutarán de forma ordenada primero los *scripts* que comiencen por *K* (*kill* o *stop*) y luego los que comiencen por *S* (*start* o arranque). Cada uno de estos *scripts* arrancará o parará un servicio (los *scripts* que comienzan por *K* lo paran y los que comienzan por S lo arrancan).

Si se quiere cambiar de nivel de ejecución se puede ejecutar el comando *telinit* indicando el *runlevel* que queremos que se ejecute. Por ejemplo, ejecutando *telinit 6* en el *prompt* se reiniciará el equipo.

ACTIVIDADES 5.2

» Eche un vistazo al fichero */etc/inittab* de su sistema Linux.

6 (**LOGIN**): una vez que se ha cargado el sistema operativo es el momento de identificarse y entrar en la máquina. Este proceso identificará al usuario en el sistema y permitirá que él mismo acceda a su escritorio.

CURIOSIDAD

Desde el intérprete de comandos en Linux ejecute *init 0* ó *telinit 0* y espere a ver qué ocurre.

5.2.2 ¿QUÉ ES UN SERVICIO?

Un servicio es un programa que se ejecuta al inicio del sistema operativo o bien lo puede ejecutar un usuario con los privilegios suficientes y proporcionan funcionalidades al sistema. Algunos servicios son los siguientes:

- **atd**. Ejecuta tareas programadas.
- **httpd**. Permite servir paginas web.
- **inetd**. Internet super daemon (super demonio de Internet). Proporciona las funcionalidades básicas de la Red, sin él no podría funcionar un *firewall*, un proxy, etc.
- **lpd**. Demonio de impresión.
- **smb**. Samba. Demonio que permite intercambiar ficheros y servicios de impresión con equipos Windows®.
- **sendmail**. Demonio que permite transportar *emails* de una máquina a otra.

5.2.3 HERRAMIENTAS DE CONFIGURACIÓN DE SERVICIOS EN LINUX

La activación y desactivación de servicios son operaciones que se pueden realizar en Linux desde un terminal con privilegios de *root*. Son operaciones sencillas y fáciles de acometer por un administrador de sistemas. No obstante, para una mayor comodidad, existen herramientas que permiten realizar estas tareas desde una interfaz gráfica y pueden resultar más cómodas.

Una herramienta muy útil para estas cuestiones es BUM (*Boot-Up Manager*), que es una herramienta desarrollada en Perl y que permite gestionar la configuración de los *runlevels* o niveles de ejecución de cualquier distribución derivada de Debian como puede ser Ubuntu.

Toda la información sobre BUM se puede encontrar en la siguiente dirección:

http://www.marzocca.net/linux/bum.html

La forma más cómoda de instalar BUM es mediante el comando *apt*:

```
sudo apt-get install bum
```

Una vez instalado BUM aparecerá dentro del menú principal en **Sistema → Administración → BootUp-Manager**.

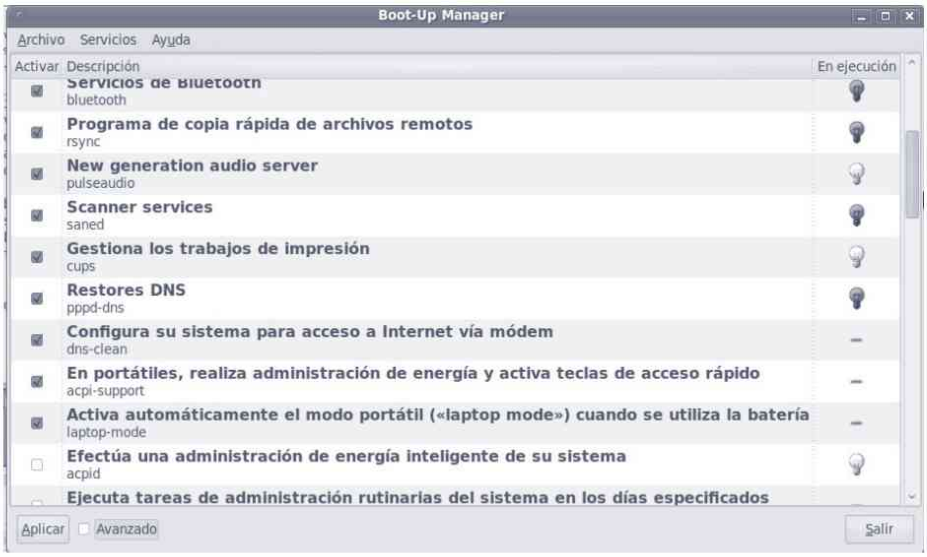


***Figura 5.5**. Herramienta de administración BootUp Manager (modo normal)*

El funcionamiento de la herramienta es simple (activar/desactivar) y tiene dos modos de ejecución, un modo normal y un modo experto en el que aparecen dos pestañas más y permite realizar más operaciones.

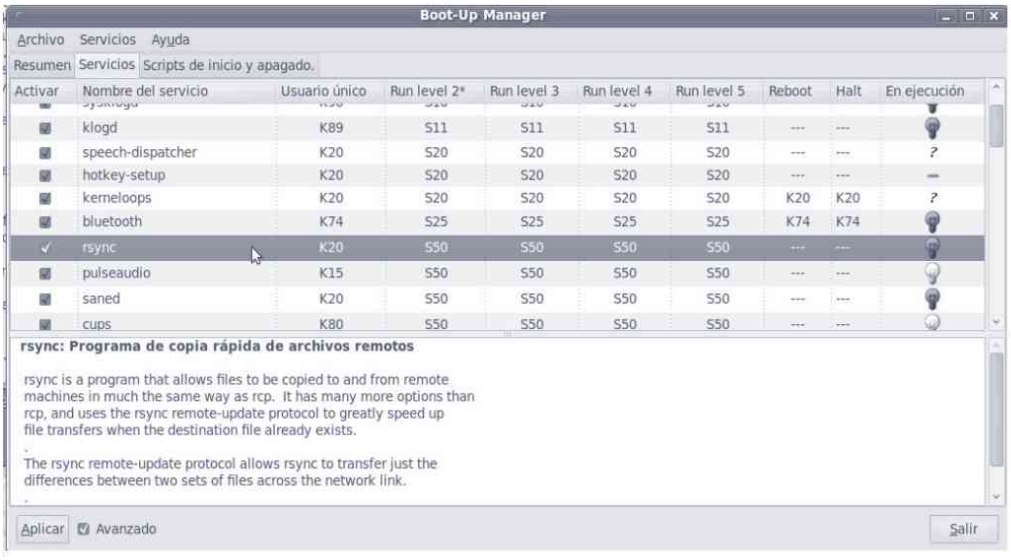


***Figura 5.6**. Herramienta de administración BootUp Manager (modo experto)*

Además de esta herramienta, existe la herramienta *rcconf*. Esta herramienta se puede instalar desde el gestor de paquetes Synaptic o de forma más comoda mediante línea de comandos con el comando *apt*:

```
sudo apt-get install rcconfig
```

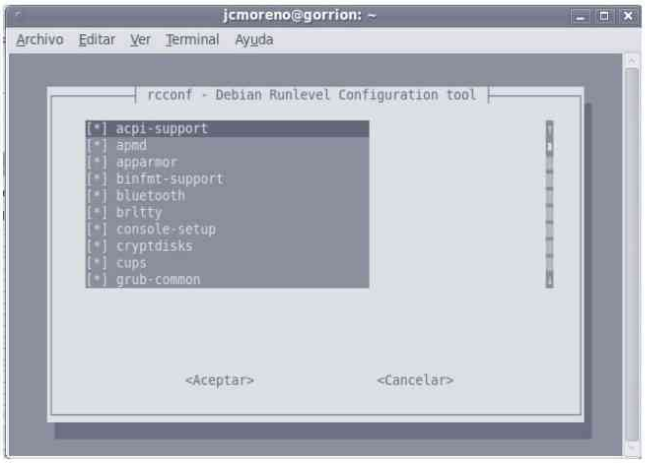


***Figura 5.7**. Herramienta de administración rcconfig*

La diferencia entre ambas herramientas está clara, *rcconfig* hay que ejecutarla desde línea de comandos como superusuario (comando *sudo rcconfig*) mientras que BUM se incorpora al menú principal. Además, BUM se ejecuta en modo gráfico, lo cual hace que BUM sea una herramienta más cómoda y útil que *rcconfig*.

ACTIVIDADES 5.3

- Instale BUM y *rcconfig* en su sistema y evalúe ambas herramientas. ¿Con cuál se queda?

5.3 CONFIGURACIÓN DE SISTEMAS OPERATIVOS

La configuración en sistemas Linux es bastante sencilla. Generalmente hay dos opciones para cambiar la configuración en un sistema Linux, la primera es editar un fichero de configuración (que en la mayoría de los casos está en el directorio */etc*) o bien utilizar una herramienta (que lo que hará será modificar ella misma ese fichero). Muchos administradores de sistemas prefieren modificar directamente los ficheros para tener un mayor control de lo que están haciendo. Una vez modificado el archivo de configuración se reinicia el servicio en cuestión y éste funcionará con la nueva configuración. En Linux no vamos a encontrarnos con ningún registro como en Windows®, ni con ficheros *ini* o *bat* y mucho menos con las famosas DLL que más de un dolor de cabeza nos han dado a más de uno.

Los ficheros de configuración son ficheros ASCII y pueden editarse con *gedit* o cualquier editor de texto. En estos ficheros de texto las líneas que comienzan por almohadilla (#) nunca se ejecutan y suelen ser comentarios o líneas de configuración comentadas para descomentarlas cuando se requiera.

A continuación se va a dar una relación de archivos junto con una explicación de su contenido.

Tabla 5.3 Algunos de los ficheros de configuración más importantes de Linux

Fichero	Contenido
Sistema de archivos	
/etc/fstab	En el fichero *fstab* está la configuración de los sistemas de ficheros que se tienen que montar al arranque del sistema.
/etc/mtab	Listando este fichero se muestra los sistemas de archivos que están montados en ese mismo momento. Es un fichero dinámico y por lo tanto su contenido va a variar si se monta o se desmonta un dispositivo o sistema de ficheros. Este fichero lo inicializa *init* y lo actualiza *mount*. *Mount* es el programa dedicado a montar sistemas de archivos.
Administración del sistema	
/etc/passwd	En este fichero se almacena la base de datos de todos los usuarios del sistema en la cual se almacena el nombre, contraseña, identificador de usuario, identificador del grupo del usuario, nombre del usuario, directorio de trabajo y *shell* del usuario. Las contraseñas no aparecen en este fichero aunque antiguamente sí. Actualmente las contraseñas se almacenan en el fichero */etc/shadow*.
/etc/group	Este fichero almacena la información de los grupos del sistema, junto con el fichero */etc/passwd* son los ficheros más utilizados en la gestión de usuarios.
/etc/shadow	Este fichero contiene entre otros campos las contraseñas cifradas, la antigüedad de las mismas, los días que hace que la contraseña fue cambiada por última vez, etc.
/etc/motd	Los administradores lo utilizaban cuando querían mostrar un mensaje a todos los usuarios de un servidor. MOTD = *Message Of The Day* (Mensaje del Día). Actualmente es más cómodo y efectivo utilizar el *email*.
/etc/crontab	Cron es un demonio que ejecuta comandos programados. La configuración de cron está en este fichero y le dice que comandos hay que ejecutar. Cron se despierta cada minuto y revisa si tiene que ejecutar algún comando y si es así lo ejecuta, en caso contrario volverá a dormir.
/etc/shells	Contiene una lista con los intérpretes de comando del sistema. Las aplicaciones lo utilizan para ver si el intérprete de comandos es válido o no.
Configuración del arranque	
/etc/inittab	Este es el primer archivo que se ejecuta al arrancar una máquina UNIX. En este archivo se encuentra la configuración para el comando *init* y en él se determina el nivel de ejecución del sistema o *runlevel* y se definen los *scripts* de arranque.
Networking	
/etc/hosts.conf	Es el archivo de configuración del cliente DNS. Permite entre otras cosas decidir si se va a utilizar el fichero *hosts* para resolución de nombres y cuál va a ser el orden y sistema a utilizar en la resolución de nombres de dominio (DNS).

/etc/hosts	Contiene una lista de *hosts* conocidos. Generalmente los *host* se conocen por nombres en vez de por direcciones IP. Para mí y para muchas personas es más fácil teclear en un navegador *http://www.google.com* que *http://66.249.92.104/.*
	Un ejemplo de archivo *host* puede ser el siguiente:
	`#Archivo /etc/hosts de ejemplo`
	`#localhost`
	`127.0.0.1 localhost`
	`#red local`
	`192.168.0.5 servidorlocal`
	`#Internet`
	`66.249.92.104 www.google.com`
	Generalmente el archivo */etc/hosts.conf* se configura para que mire este archivo antes de preguntar al DNS o NIS. No se ha dicho pero resulta obvio, si las direcciones son dinámicas no tiene sentido apuntarlas en este archivo.

/etc/networks	En el fichero *networks* aparecen las redes accesibles a las que está conectada la máquina. Este fichero lo utiliza el comando *routed.*

/etc/network/interfaces	Este fichero contiene la configuración de la red. En este fichero se configura cómo el sistema se conecta a la red.
	Un ejemplo de este fichero es el siguiente:
	`iface eth0 inet static`
	`address 192.168.0.5`
	`netmask 255.255.255.0`
	`gateway 192.168.0.1`
	En este fichero, como se puede observar, aparecerán las interfaces de red con sus direcciones, máscaras y *gateways* por defecto.

/etc/resolv.conf	En este fichero aparece el dominio de Internet al que pertenece la máquina y las direcciones IP de los DNS a utilizar cuando se quiere resolver una dirección IP.
	Un ejemplo de este fichero es el siguiente:
	`domain ra-ma.es`
	`dnsuno 194.178.5.1`
	`dnsdos 194.179.45.30`

/etc/services	En este archivo se encuentra la traducción entre los números de puerto y los protocolos. Este archivo es utilizado por *telnet*, *inetd* y otros programas.
/etc/inetd.conf	Este es el archivo que contiene la configuración de *inetd*. *Inetd* es un superdemonio ya que va a gestionar las conexiones de varios demonios. La ejecución de este demonio es más efectiva para el sistema que si los demonios se gestionasen de forma individual. En este fichero se pueden habilitar y deshabilitar servicios como el *ftp, pop3, imap,* etc. Actualmente se utiliza el *xinetd* que es una versión más segura y moderna que el servicio *inetd*. La filosofía es la misma, además este demonio permite realizar cosas como limitar la cantidad de servicios que se ejecutan o proteger al sistema de un escaneo de puertos.
/etc/sendmail.cf	Es el archivo de configuración de *sendmail*. *Sendmail* es el MTA (*Mail Transfer Agent*- Agente de transporte de correo) más utilizado y permite encaminar los mensajes de correo. La configuración de *sendmail* no es sencilla y va desde configurar un simple mail *forwarder* hasta configuraciones mucho más complicadas.
Demonios	
/etc/httpd.conf	En este archivo reside la configuración del servidor web Apache. Dependiendo de la instalación de Apache este fichero residirá en un lugar u otro.

¿Qué ocurre si queremos configurar el sistema operativo sin tener que editar los ficheros de configuración? **¿Y si queremos configurar el sistema operativo desde la misma o desde otra máquina**? La solución a estas preguntas puede ser *webmin*. *Webmin* es una interfaz web para la administración de sistemas Linux. Con cualquier navegador se pueden modificar las configuraciones de Apache, DNS, cuentas de usuario, apagado del equipo, compartir archivos, etc.

En el Material adicional del libro y en la siguiente página web podemos encontrar una guía paso a paso de instalación de *webmin*:

http://sliceoflinux.com/2009/09/07/instalar-webmin-en-ubuntu-paso-a-paso/

Una vez instalado, el programa pedirá que el usuario se identifique en el sistema. Obviamente el usuario que acceda al equipo a administrar deberá tener permisos de administración en el mismo.

***Figura 5.8**. Acceso a webmin*

A *webmin* se accederá por *https* para trabajar con más seguridad que con *http* y se accederá por el puerto 10.000. El aspecto de la interfaz es el que se muestra en la siguiente figura:

***Figura 5.9**. Herramienta webmin*

Las ventajas que tiene *webmin* son muchas y cada vez que se utiliza más esta herramienta se le encuentran más ventajas todavía. Por citar algunas:

- ✓ *Webmin* permite administrar un equipo desde cualquier navegador.
- ✓ *Webmin* permite administrar cualquier Linux. Si aprende *webmin* puede administrar una máquina con SUSE, Ubuntu, Gentoo, Knoppix, etc.
- ✓ Se puede administrar una máquina independientemente de dónde se encuentren los ficheros de configuración. No hace falta aprenderse ni nombres de archivos ni rutas.
- ✓ *Webmin* permite administrar un equipo de forma remota sin importar el sistema operativo o el navegador que se esté utilizando.

ACTIVIDADES 5.4

- Instale *webmin* en su máquina y acceda a *webmin* desde un navegador de otra máquina en la misma red. Navegue por las diferentes opciones de administración.

EJERCICIO 5.1

CAMBIAR LA HORA DEL EQUIPO CON WEBMIN

Cambiar la hora del sistema es una tarea que realizan de vez en cuando los administradores de sistemas. Para cambiar la fecha y hora del sistema se utiliza el comando *date* desde un terminal. No obstante, puede ser más sencillo ajustar la hora mediante una interfaz gráfica como *webmin*.

La hora en *webmin* se puede ajustar accediendo a la opción **system time** del menú **hardware**.

***Figura 5.10**. Opción de menú system time de webmin*

Una vez que se accede a esta opción de menú aparecen 2 fechas y horas distintas, *system time* y *hardware time*. La razón de ello es la siguiente, el hardware, y más concretamente la BIOS CMOS, mantiene entre otra información la hora del sistema. Cuando se apaga el equipo y la fuente de alimentación deja de proporcionar suministro eléctrico al equipo, ese reloj se mantiene funcionando porque la BIOS CMOS tiene una pila de tipo botón que hace que siga funcionando. Esa hora almacenada en la CMOS será la *hardware time* mientras que Linux mantiene su propio reloj y la hora del sistema operativo será *system time*.

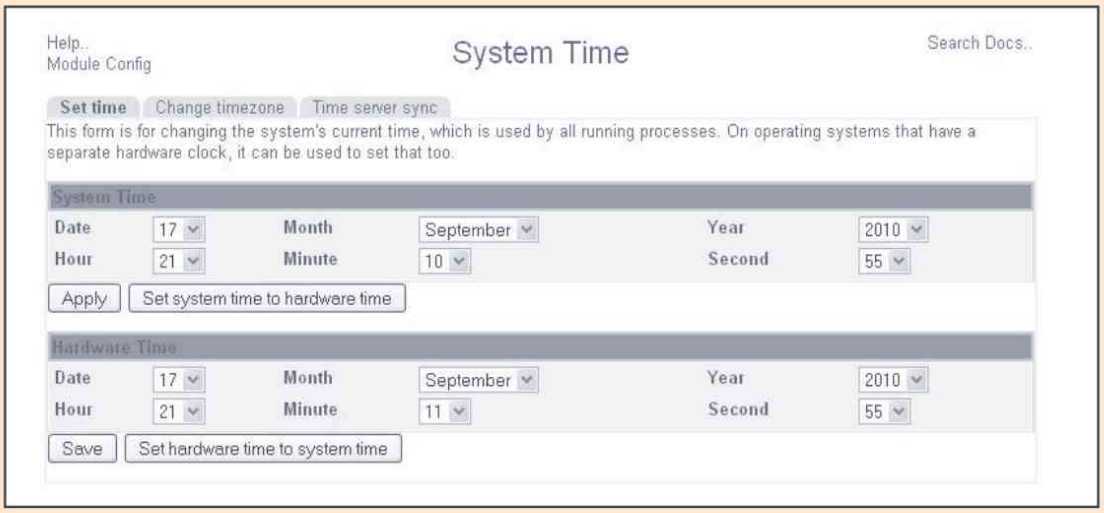


***Figura 5.11**. Interfaz para cambiar la hora en webmin*

Como se puede observar en la imagen anterior el funcionamiento es muy intuitivo y la herramienta permite sincronizar ambas horas (*system time* y *hardware time*).

ACTIVIDADES 5.5

- Cambie la hora de su equipo a la hora actual.

CONSEJO

Si cada vez que encendemos un equipo ha reiniciado la hora o ésta se atrasa seguramente haya que cambiar la pila de la BIOS.

5.4 ADMINISTRACIÓN DE USUARIOS Y PERMISOS

En esta sección nos vamos a centrar en el sistema de usuarios y permisos de Linux. Las explicaciones sirven prácticamente para cualquier distribución Linux, pero los ejemplos se van a hacer sobre Ubuntu Linux.

5.4.1 LOS USUARIOS EN EL SISTEMA

Linux permite trabajar con múltiples usuarios a la vez y también permite realizar varias tareas al mismo tiempo, con lo cual puede considerarse un sistema operativo multiusuario y multitarea, como prácticamente todos los sistemas operativos actuales.

En Linux existen tres tipos de usuarios.

- **Root o superusuario**. Es el usuario encargado de administrar el sistema, pudiendo realizar cualquier tipo de tarea sin restricción alguna. Es igual al usuario administrador de Windows®.
- **Usuarios normales**. Generalmente son personas físicas teniendo algunos usuarios más privilegios que otros. Yo, por ejemplo, accedo al sistema identificándome como *jcmoreno*.
- **Usuarios de sistema**. Son usuarios utilizados por procesos o servicios los cuales necesitan una cuenta de usuario para realizar sus funciones. Al listar el fichero */etc/passwd* podemos ver algunos de ellos (FTP, *mail*, etc.).

RECUERDA

Los usuarios en un sistema Linux se almacenan en el fichero */etc/passwd*.

5.4.2 LOS GRUPOS DE USUARIOS

Imaginemos que tengo el siguiente problema. Tengo dos grupos de personas a mi cargo, el grupo de comerciales los cuales trabajan con una serie de listados de precios, ventas y clientes y el grupo de técnicos, los cuales trabajan con documentación técnica de la empresa en la que trabajamos. Necesito que las únicas personas que accedan a los listados de precios, ventas y clientes sean los comerciales. Ellos necesitan trabajar con estos documentos pero no deben de acceder a la documentación técnica. Sin embargo, el grupo de los técnicos quiero que acceda a la documentación técnica pero no a los listados de precios, clientes y ventas.

Una solución a este problema es crear en mi sistema una carpeta por usuario y darle el permiso correspondiente a la carpeta de cada usuario. Dado que son 30 empleados no parece muy operativo, es más, hay archivos como la lista de ventas que tiene que poder actualizarse por cualquier comercial. En ese caso cualquier actualización de un comercial tiene que replicarse en los demás 29 archivos de sus compañeros lo cual lo hace inviable.

Se me ocurre otra solución y es crear un grupo de comerciales, el cual tendrá acceso a la carpeta comerciales y el grupo técnicos, el cual podrá acceder a la carpeta *docu_técnica*. Cada usuario estará en el grupo correspondiente y yo, que soy el jefe, perteneceré a los dos grupos, lo cual me permite acceder a toda la información.

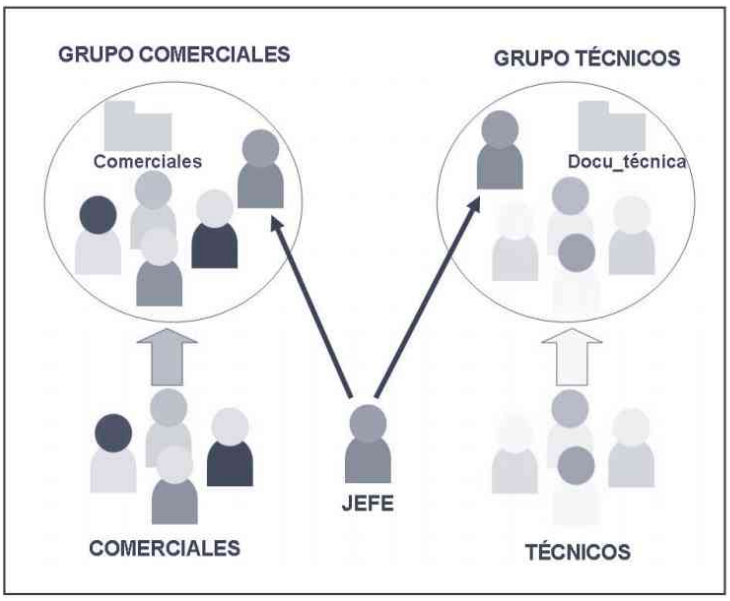


***Figura 5.12**. Ejemplo de grupos de usuarios*

5.4.3 GESTIONAR USUARIOS Y GRUPOS EN LINUX

Gestionar grupos y usuarios en Linux se puede hacer de las siguientes maneras:

- Mediante **comandos**. Lo cual permitirá dar de alta, baja y modificar usuarios en cualquier sistema Linux con los mismos comandos.
- **Editando los ficheros** */etc/passwd* o */etc/group*. Este método puede dar algún problema si no se edita el fichero correctamente.
- Con una **herramienta administrativa**. Es más cómodo, pero las herramientas cambian con el tiempo y pueden diferir de una distribución a otra, mientras que los comandos no.

Los grupos y los usuarios son tareas administrativas que hace el usuario *root* o administrador del sistema. Una de las operaciones más comunes es crear un usuario, que se puede hacer con los siguientes comandos:

```
$ usaradd emma
$ passwd emma
```

Con el primer comando anterior se crea el usuario *Emma* y con el segundo el sistema pedirá una contraseña para el nuevo usuario. El comando *useradd* permite muchos parámetros, con el comando *man useradd* podrá conocer la potencia de este comando. Si lo que se desea es borrar el usuario se utilizará el comando *userdel*. Con el siguiente comando se borrará el usuario *Emma*:

```
$ usardel emma
```

Si lo que se quiere es crear el grupo *alumnos*, se deberá de ejecutar el siguiente comando:

```
$ groupadd alumnos
```

Una vez creado el grupo haremos que *Emma* sea miembro de ese grupo.

```
$ gpasswd -a emma alumnos
```

Para borrar un grupo se puede utilizar el comando *groupdel* seguido del nombre del grupo a borrar.

CONSEJO

Sobre contraseñas

Nunca hay que utilizar contraseñas que sean fáciles de adivinar (sobre todo la de *root*). Generalmente se utilizan contraseñas con los nombres de los hijos, de la novia, con la fecha de nacimiento, etc. Estas contraseñas son fáciles de averiguar. Las contraseñas hay que memorizarlas y no escribirlas en archivos, cuadernos, etc.
Es buena costumbre cambiar las contraseñas de vez en cuando.
Mejor elegir contraseñas con mayúsculas, minúsculas y números y con al menos 8 caracteres (si se utiliza algún símbolo de puntuación mejor).

En la siguiente figura se puede observar la herramienta de gestión de usuarios de Ubuntu. Como se puede observar, la interfaz es sencilla e intuitiva y todas las posibilidades que se pueden hacer mediante comandos se podrán realizar con la interfaz. Esta herramienta está disponible en el menú **Sistema → Administración**:

***Figura 5.13**. Herramienta de administración de usuarios de Ubuntu*

La gestión de grupos y asignación de usuarios a grupos se puede realizar desde la misma herramienta:

***Figura 5.14**. Herramienta de administración de grupos de usuarios de Ubuntu*

5.4.4 LOS PERMISOS EN LINUX

Linux, como se vio en el apartado anterior, tiene un sistema de seguridad basado en usuarios y grupos. Los ficheros y directorios en Linux tienen seguridad a tres niveles. Se establecerán permisos a los ficheros o directorios al usuario creador del mismo al grupo al que pertenece el fichero o directorio y a los demás usuarios del sistema.

En Linux existen tres tipos de permisos para archivos y directorios:

- **r**. Lectura. Se puede acceder al contenido del archivo o listar el contenido del directorio.
- **w**. Escritura. Permite borrar y modificar un archivo y en un directorio crear y borrar ficheros dentro de él.
- **x**. Ejecución. A diferencia de Windows®, en Linux los ficheros no hace falta que sean *.exe* para poder ejecutarse. Los directorios con permiso de ejecución permiten realizar operaciones sobre ellos mediante los otros permisos de lectura y escritura.

Cuando se lista una serie de archivos y directorios (con el comando *ls –l*) se puede observar algo parecido a la siguiente figura:

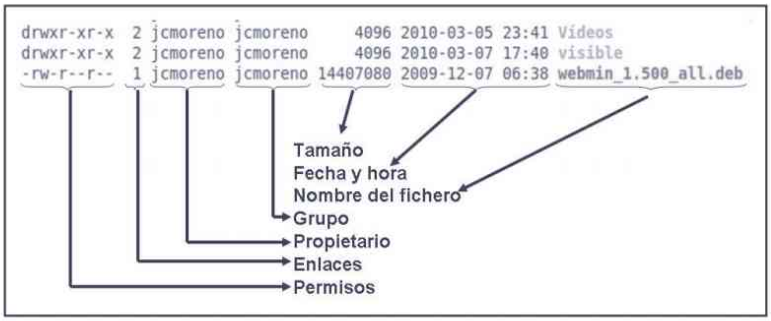


***Figura 5.15**. Listado de una serie de archivos*

Como se puede observar, en la zona izquierda de la figura aparecen los permisos de dichos archivos o directorios. A continuación se comentarán estos permisos:

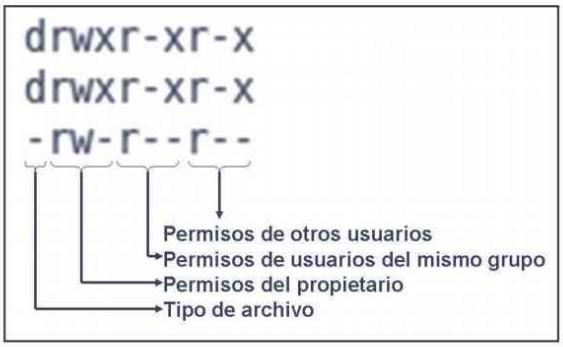


***Figura 5.16**. Detalle de los permisos*

El primer dígito muestra si es un fichero regular (-) o un directorio (*d*). Los permisos (*r*, *w* ó *x*) aparecen en tres grupos y cada permiso tiene una posición (si aparece un guión "–" es ausencia de dicho permiso), el primero son los permisos del usuario seguido de los permisos de los usuarios que pertenezcan al grupo al que pertenece dicho archivo o directorio y, por último, los permisos que tienen los demás usuarios del sistema sobre dicho archivo o directorio.

Existen unos comandos bastante útiles para el manejo de ficheros y directorios que son los siguientes:

- **chown**. Permite cambiar el propietario al directorio o archivo.
- **chgrp**. Permite cambiar el grupo al directorio o archivo.
- **chmod**. Permite cambiar los permisos del directorio o archivo.

RECUERDA

Para cambiar los permisos de un fichero o directorio hay que tener permiso de escritura sobre él.

Sobre el cambio de permisos de un directorio o archivo hay que decir que se pueden cambiar de dos maneras:

- De forma **alfabetica**.
- De forma **numérica** (octal). Esta es la más utilizada.

La forma numérica es la más utilizada, a cada permiso se le asigna un valor (*r* = 4, *w* = 2 y *x* = 1) y por orden (propietario, grupo y otros), de tal manera que si ejecuto el siguiente comando:

```
chmod 754 script.sh
```

Asignará al propietario del fichero *script.sh* permisos de lectura, escritura y ejecución (7 = 4 + 2 + 1), al grupo permisos de lectura y ejecución (5 = 4 + 1) y a los demás usuarios permiso de lectura solamente (4 = 4).

RECUERDA

Aparte de los terminales, muchos usuarios utilizan los exploradores de archivos, de forma que el cambio de permisos se puede realizar de manera más cómoda.

5.5 VIRTUALIZACIÓN DE ENTORNOS OPERATIVOS

En los últimos años, asociado a los entornos operativos se ha desarrollado el concepto de la **virtualización**, permitiendo ejecutar distintos sistemas operativos de forma virtual sobre uno solo.

La **virtualización de plataforma** se lleva a cabo en una plataforma de hardware mediante un software anfitrión, que es un programa de control que simula un entorno computacional (**máquina virtual**) para su software invitado.

Generalmente, este software invitado es un SO completo que se ejecuta como si estuviera instalado en una plataforma de hardware autónoma.

Virtualizar el SO es una opción interesante si no queremos instalar dos sistemas operativos en el mismo ordenador. En este caso no se necesita un gestor de arranque para elegir el sistema operativo a utilizar, y si estando en uno queremos cambiar a otro no tenemos por qué reiniciar el equipo.

***Figura 5.17**. XP ejecutándose sobre Ubuntu Hardy vía Virtualbox. Fuente: Okubax*

Entre los programas de control para virtualizar, algunos son de pago, como **VMWare**, que es uno de los referentes en el mercado y ofrece una versión más básica gratuita, **VMWare Player**, que permite virtualizar a través de una máquina virtual ya configurada.

Dentro de los programas gratuitos tenemos **VirtualPC** de Microsoft®, y además como programas de código libre **Xen**, **OpenVZ** y **VirtualBox**, que funcionan tanto en Windows® como en Linux.

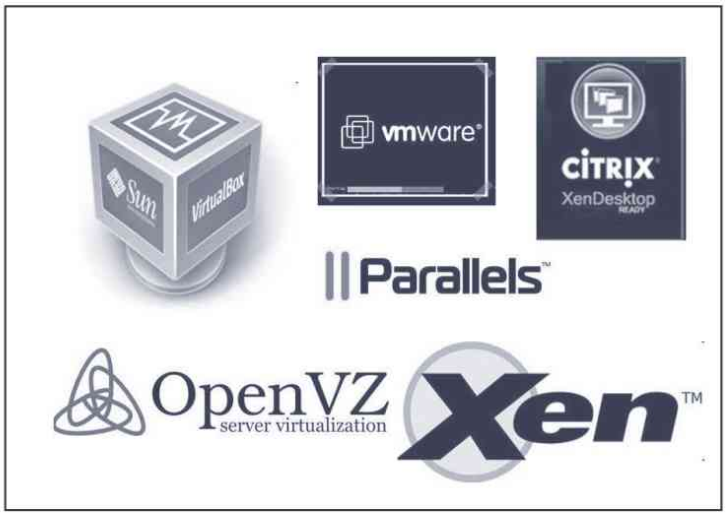


***Figura 5.18**. Software de virtualización*

RESUMEN DEL CAPÍTULO

En este tema se estudiarán los principios básicos de los sistemas informáticos.

En primer lugar se estudia la arquitectura cliente/servidor, la cual es utilizada abundantemente en sistemas telemáticos, servicios de Internet, etc.

Una vez visto esto se estudia cómo funciona esta arquitectura en los equipos comunes. La configuración de un sistema operativo reside en gran parte en configurar sus servicios. La mayoría de estos servicios responde a la arquitectura cliente/servidor. Aparte de esto, se aprenderán los principios básicos de la configuración de sistemas operativos.

A la administración de usuarios y permisos se le dedica un epígrafe de este tema. Por temas de seguridad, los sistemas operativos utilizan usuarios, grupos y permisos para protegerse de un uso indebido del mismo. En este tema se estudiarán los principios básicos de los mismos.

Por último, se estudiará la virtualización. Esta técnica es muy utilizada actualmente ya que permite en una máquina tener múltiples sistemas operativos y arrancarlos y pararlos al antojo del administrador.

EJERCICIOS PROPUESTOS

1. Investigue cómo funcionan los dominios en Windows®. Haga una descripción detallada de cómo gestionaría los dominios en una empresa que tiene tres tipos de empleados (*jefes*, *empleados de administración y comerciales* e *informáticos*).

2. ¿Averigüe qué es *Samba*, cómo se configura y para qué sirve?

3. ¿Qué es un *mail forwarder*? ¿Cómo se crearía uno en Linux?

4. ¿Cómo se distingue una unidad arrancable de una que no lo es?

5. ¿Qué versiones de Grub existen actualmente?

6. En Linux, utilice la herramienta *at* para programar un apagado de su equipo para dentro de 1 hora.

7. En Linux, utilice la herramienta *mount* para montar y desmontar un *pendrive*. Liste el fichero de configuración *mtab* para comprobar si está montado o no el *pendrive*.

8. En Linux, modifique el fichero */etc/hosts* para añadir una entrada de un *host* de la red local (utilice un alias en vez de su verdadero nombre). Compruebe que funciona la modificación anterior.

9. En Linux, utilice la herramienta de administración correspondiente para crear un usuario en el sistema y acceder al mismo utilizando dicho usuario.

10. Cree un fichero en Linux, *prueba.txt*, que tenga permiso de lectura, escritura y ejecución para el usuario y ningún permiso para los demás usuarios del sistema.

TEST DE CONOCIMIENTOS

1 Elija la afirmación falsa:

a) Un servidor suele ser un *host* que posee una gran capacidad de cómputo. Este equipo comparte sus recursos con los clientes.
b) El *PID* de *Init* es siempre 1.
c) Los clientes no comparten sus recursos, su papel es el de pedir contenidos a los servidores o pedir servicios a dichos servidores.
d) El comando *telinit 6* apagará el equipo.

2 Elija la afirmación falsa:

a) El *POST* realiza un autodiagnóstico del hardware del equipo.
b) *GRUB* es un *boot* manager.
c) El *boot* manager de Linux se encuentra en */boot*.
d) Cliente liviano es lo opuesto a *thin client*.

3 Elija la afirmación verdadera:

a) El comando *init 0* apagará la máquina.

b) El sector de arranque comprende los primeros 512 MB del disco y es ahí donde reside el sistema operativo.

c) *POST* es el acrónimo de *Power Operating System Test*.

d) El funcionamiento de *init* se configura en */boot/inittab*.

4 Elija la afirmación verdadera:

a) En la arquitectura C/S el cliente es el encargado del control de acceso.

b) httpd es el demonio servidor de páginas web o Apache.

c) La arquitectura C/S es una arquitectura distribuida (distribuida entre el cliente y el servidor).

d) El *PID* de *Init* es siempre 0 al ser el primer proceso que se ejecuta.

5 Elija la afirmación verdadera:

a) En la arquitectura C/S la generación de consultas y *report* la realiza el servidor por tener mayor capacidad de cálculo.

b) El comando *chgrp* permite cambiar el propietario al directorio o archivo.

c) El comando *telinit 6* reiniciará el equipo.

d) El *POST* realiza un autodiagnóstico del hardware y software del equipo.

6 Elija la afirmación verdadera:

a) *Atd* es el demonio que permite transportar *email* de una máquina a otra.

b) Muchísimos servicios como el *email*, las páginas web, acceso a bases de datos, FTP… Están basados en el modelo P2P.

c) El comando *chown* permite cambiar el grupo al directorio o archivo.

d) *Man useradd* muestra la ayuda del comando *useradd*.

7 Elige la afirmación falsa:

a) *Lpd* es el demonio de impresión de Linux.

b) En el arranque de un equipo, primero se ejecuta el proceso *Init*, el cual es el primer proceso a cargar en memoria y luego se carga el *kernel* del sistema operativo.

c) El comando *chmod* permite cambiar los permisos del directorio o archivo.

d) El *PID* de *Init* es siempre 1.

6 Implantación de software

OBJETIVOS DEL CAPÍTULO

- ✓ Conocer las características del software y sus dificultades en el desarrollo.
- ✓ Recordar las diferentes etapas por las que pasa toda aplicación desde que se encarga hasta que deja de usarse.
- ✓ Saber instalar, configurar y desinstalar aplicaciones en diferentes entornos operativos.
- ✓ Verificar la repercusión de la eliminación, modificación y/o actualización de aplicaciones instaladas en el sistema.

6.1 TIPOS DE SOFTWARE

Por software entendemos al equipamiento o soporte **lógico** de un sistema informático. Lo constituyen el conjunto de componentes lógicos y, por tanto, no tangibles y no físicos, necesarios para llevar a cabo una tarea específica en nuestro sistema.

Es un componente **imprescindible** en todo sistema informático que comunicará y dará órdenes al hardware para que se lleven a cabo todas las tareas que el usuario del sistema le encomiende.

Podemos definir el software como el **conjunto de los programas de cómputo**, **procedimientos**, **reglas**, **documentación y datos asociados** que forman parte de las operaciones de un sistema de computación (definición extraída del **estándar 729 de IEEE**).

El concepto ya fue empleado por **Charles Babbage** como parte de su **máquina diferencia**l en forma de diferentes secuencias de instrucciones leídas desde memoria.

Posteriormente, **Alan Turing**, con su **máquina de Turing** y su **teoría de la computación**, desarrolló la teoría que forma la base del software moderno.

¿SABÍAS QUE...?

Alan Turing (1912-1954) fue un matemático, informático teórico y criptógrafo inglés considerado uno de los padres de la Ciencia de la Computación, siendo el primer antecedente de la informática moderna. Formuló la **Teoría de la Computación**, hoy día ampliamente aceptada, y contribuyó a combatir a los alemanes en la Segunda Guerra Mundial ayudando a descifrar su potente máquina **Enigma**.
Su emergente carrera se cortó bruscamente cuando fue acusado y procesado por ser homosexual siendo castrado químicamente y suicidándose al poco tiempo.

El software es un elemento con una serie de características muy particulares que lo llevan a que diferentes acciones sobre el mismo como el desarrollo o el mantenimiento sean también muy particulares. Estas características son:

- El software **es lógico**, **no físico**.
- El software **se desarrolla**, **no se fabrica**.
- El software **no se estropea**.
- En ocasiones, **se puede construir a medida**.

¿SABÍAS QUE...?

La palabra **software** como tal, fue empleada por primera vez en 1957 por **J.W. Tukey** (1915-2000), donde en un artículo de 1958 en la publicación *American Mathematical Monthly*, empleó por primera vez el término **computer software** en un contexto computacional donde hablaba de la necesidad de aprovechar las capacidades de cálculo de las computadoras, permitiendo a los programadores escribir y organizar complejos conjuntos de instrucciones que luego se traducirán a un lenguaje comprensible por las máquinas pudiendo ser ejecutadas.
J.W. Tukey también acuñó otro término imprescindible en la Tecnología Computacional, la palabra **bit** como contracción de **Digito Binario**, por sus palabras en inglés **Binary Digit**.

Todo software en su creación y desarrollo pasa por una serie de etapas, lo que es conocido como las **fases del ciclo de vida del software** dentro de la disciplina encargada de tal fin, llamada **Ingeniería del Software**.

El objetivo de la Ingeniería del Software es proporcionar un marco de trabajo para construir software con mayor calidad.

El término **ciclo de vida del software** describe el desarrollo de software, desde la fase inicial hasta la fase final. El propósito de este modelo es definir las distintas fases intermedias que se requieren para la **validación** del desarrollo de la aplicación (garantizar que el software cumpla los requisitos para la aplicación) y la **verificación** de los procedimientos de desarrollo (asegurar que los métodos utilizados son apropiados).

Este tipo de modelos se desarrollan tomando como punto de partida que es muy costoso rectificar los errores que se detectan tarde dentro de la fase de implementación. El ciclo de vida permite que los errores se detecten lo antes posible y, por tanto, permite a los desarrolladores concentrarse en la calidad del software, en los plazos de implementación y en los costes asociados.

Figura 6.1. *Ciclo de vida del software*

En general, todo ciclo de vida de un software consta de las siguientes etapas:

- **Definición de necesidades**: consiste en realizar una primera aproximación al proyecto y definir en grandes rasgos las necesidades.
- **Análisis**: consiste en recopilar, examinar y formular los requisitos del cliente y examinar cualquier restricción que se pueda aplicar. En este paso se realiza un análisis en profundidad de la arquitectura hardware y software del sistema.
- **Diseño**: se determinarán los requisitos generales de la arquitectura de la aplicación y se dará una definición precisa de cada subconjunto de la aplicación.
- **Codificación** (programación e implementación): consiste en la implementación del software en un lenguaje de programación para crear las funciones definidas durante la etapa de diseño.
- **Pruebas**: se llevará a cabo una prueba individual de cada subconjunto de la aplicación para garantizar que se implementaron de acuerdo con las especificaciones y se garantizará que los diferentes módulos se integren con la aplicación.

- **Validación**: se garantizará que el software cumple con las especificaciones originales y se instalará el software en el entorno real de uso.
- **Mantenimiento y evolución**: se realizarán los procedimientos correctivos (mantenimiento correctivo) y las actualizaciones secundarias del software (mantenimiento continuo).

El orden y la presencia de cada uno de estos procedimientos en el ciclo de vida de una aplicación dependen del tipo de modelo de ciclo de vida acordado entre el cliente y el equipo de desarrolladores.

Existen múltiples **clasificaciones del software** pero la más común suele ser la siguiente:

- **Software de Sistema**. Es el conjunto de programas o rutinas cuyo objetivo es facilitar el uso de la computadora, permitiendo administrar y asignar los recursos del sistema.

  Proporciona al usuario adecuadas interfaces, herramientas y utilidades de apoyo que permiten el uso y mantenimiento del sistema.

  Incluyen herramientas como sistemas operativos, controladoras de dispositivos, herramientas de diagnóstico y reparación, herramientas de optimización y utilidades varias. Hoy día todas estas herramientas se recogen en los llamados **entornos operativos**.

- **Software de Aplicación**. Una vez que un sistema informático tiene instalado el software de sistema entonces se le puede agregar el software de aplicación.

  Son aquellos programas que permiten a los usuarios llevar a cabo una o varias tareas específicas en diversos campos como el educativo, industrial, comercial, servicios, etc.

- **Software de Programación**. Es el conjunto de herramientas que permiten al programador desarrollar programas informáticos. Lo forman distintas herramientas como editores de texto, compiladores, intérpretes, enlazadores, depuradores aunque en la actualidad todos ellos se recogen en los **entornos de desarrollo integrados** (**IDE**).

  Se emplean lenguajes de programación para crear los programas en dichos entornos. Un **lenguaje de programación** es una notación para escribir programas. Un lenguaje viene definido por una gramática o conjunto de reglas que se aplican a un alfabeto constituido por el conjunto de símbolos utilizados. Son ejemplos de lenguajes de programación C/C++, Basic, Pascal, PHP o Javascript.

  Existen diferentes **clasificaciones de los lenguajes**. Una de ellas es atendiendo a su proximidad al hardware, hablamos entonces de **lenguajes de bajo nivel** (aquel que es aquel fácil de ser procesado por el microprocesador, ocupa poco lugar en memoria y de muy difícil programación para el hombre) y de **lenguajes de alto nivel** (de difícil acceso al hardware, ocupa mucho más espacio de memoria y es fácil de programar por un programador).

***Figura 6.2**. Esquema tipo cebolla Hw-SO-Sw Aplicación*

Hoy en día **el software tiene un doble papel**, es un producto y, al mismo tiempo, el vehículo para hacer entrega de un producto.

Como **producto** hace entrega de la potencia informática del hardware informático. Si reside dentro de un teléfono móvil u opera dentro de una computadora central, el software es un transformador de información, produciendo, gestionando, adquiriendo, modificando, mostrando o transmitiendo información que puede ser tan simple como un solo bit, o tan compleja como una simulación en multimedia.

Como **vehículo** utilizado para hacer entrega del producto, el software actúa como la base de control de la computadora (sistemas operativos), la comunicación de información (redes), y la creación y control de otros programas (herramientas de software y entornos).

El software se ha convertido en el **elemento clave** de la evolución de los sistemas y productos informáticos.

En las últimas cuatro décadas, el software ha pasado de ser una herramienta para resolver problemas específicos (casi todos de ámbito científico) y una herramienta de análisis de información, a ser una industria por sí misma. Pero la breve e intermitente historia de la programación ha creado un conjunto de problemas que persisten todavía como ya veremos.

6.1.1 COMPONENTES DE APLICACIONES. ARQUITECTURAS DEL SOFTWARE

Ya hemos estudiado que toda aplicación informática está desarrollada por un programador empleando un lenguaje de programación.

En un principio, la programación se consideró todo un arte dada la dificultad que exigía cualquier aplicación por pequeña que fuese y era una disciplina al alcance de muy pocos.

Con el tiempo, la **evolución de los lenguajes de programación** (donde los lenguajes de alto nivel han desplazado a los de bajo nivel y tuvo lugar la aparición de la programación modular y estructurada), y el **auge y dependencia de los sistemas informáticos**, se han ido descubriendo y desarrollando formas y guías generales de crear aplicaciones basadas en módulos y componentes que en muchos casos ya se encuentran implementados. Es lo que se conoce como **arquitectura del software**.

La **arquitectura de software** establece los fundamentos para que analistas, diseñadores, programadores, etc., trabajen en una línea común que permita alcanzar los objetivos del sistema informático cubriendo todas las necesidades. Es el diseño de más alto nivel de la estructura de una aplicación.

La arquitectura de software define, de manera abstracta, los componentes que llevan a cabo alguna tarea de computación en una aplicación, sus interfaces y la comunicación entre ellos.

En cualquier arquitectura de software existen al menos **tres vistas fundamentales**:

- **Visión estática**. Describe los componentes que tiene la arquitectura.
- **Visión Dinámica**. Describe cómo se comportan los componentes a lo largo del tiempo y cómo interactúan entre sí.
- **Visión Funcional**. Describe qué hace cada componente.

Estas vistas o modelos de arquitecturas pueden expresarse mediante uno o varios lenguajes y herramientas como el lenguaje natural, los diagramas de estado, los diagramas de flujo de datos y otros, cada uno apropiado para un tipo de vista. Existe además otro lenguaje, UML (lenguaje unificado de modelado) que permite implementar todos los modelos o vistas.

En base a cómo están organizados los componentes del software existen diferentes arquitecturas, entre las que destacan:

- **Arquitectura Monolítica**. El software se estructura en componentes funcionales muy acoplados.
- **Arquitectura Cliente-Servidor**. El software reparte su carga de cómputo en dos partes independientes pero sin reparto claro de funciones.
- **Arquitectura de tres niveles**. Es un tipo concreto de arquitectura cliente-servidor donde la carga se divide en tres partes o capas, que se relacionan únicamente con la inmediata, con un reparto claro de funciones. Una capa para la presentación (interfaz de usuario), otra para el cálculo y otra para el almacenamiento. Existen incluso arquitecturas de cuatro o más niveles.

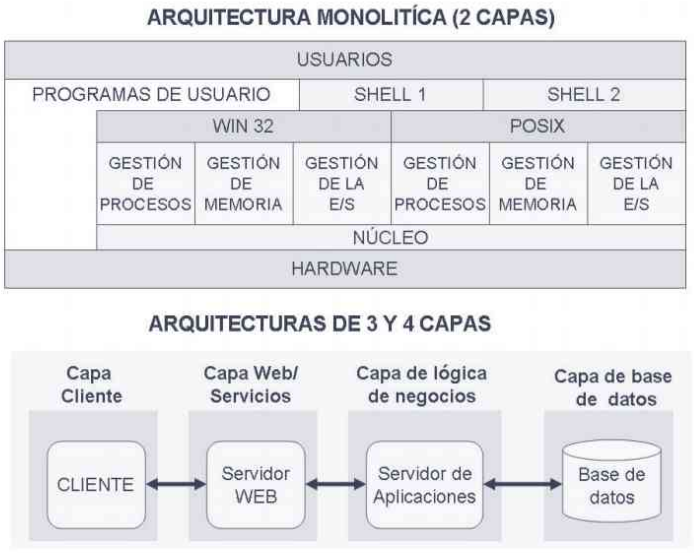


***Figura 6.3**. Diferentes esquemas de arquitecturas*

6.2 INSTALACIÓN, CONFIGURACIÓN Y ELIMINACIÓN DE APLICACIONES

6.2.1 FORMAS DE INSTALACIÓN

La instalación de software y su configuración es el **primer paso y una condición necesaria** para el uso de un programa tras su adquisición.

Es fundamental que este paso tenga éxito dado que si el proceso falla, aunque solo sea parcialmente, es probable que la aplicación directamente no funcione o lo haga de forma incorrecta.

Es necesario, sobre todo en instalaciones de software complejo, que contenga muchos archivos con gran dispersión física e interdependencias con otros componentes, que dicho proceso sea **seguro y confiable**.

En los últimos años se han desarrollado normas y técnicas cada vez más potentes para simplificar y estandarizar el proceso de instalación de software, siendo básicamente los descritos a continuación.

Instalación por copia directa

Este sistema de instalación es fácil e intuitivo y el preferido en MAC OS X. Los programas en Mac suelen usar librerías comunes del propio MAC OS X para todas ellas (diferentes aplicaciones comparten las mismas librerías).

Se organizan en el directorio **Aplicaciones** y se presentan como un paquete simple con todo lo necesario para que el programa funcione y, en ocasiones, una lista de preferencias que se aloja en el mismo directorio para todos los programas (*home/librería/Application Support*).

***Figura 6.4**. Instalación directa en MAC*

Este modelo hace que aunque instalemos y desinstalemos gran cantidad de software el funcionamiento general del sistema operativo no se vea alterado, además de evitar los conflictos de incompatibilidad entre diferentes aplicaciones.

Tiene el inconveniente de que olvidamos versiones antiguas de aplicaciones ocupando espacio en disco al instalar las posteriores.

Los programas en MAC OS X para su instalación se presentan en **formato comprimido** (*.zip*, *.rar*, *.tar*, *.gz*, etc.), **como imagen de disco** (*.dmg* o *.iso*) que se montará y aparecerá en el **finder**, **como paquete de extensión** *.app*, en el que habrá que arrastrar el fichero a la carpeta *Aplicaciones* y hacer doble clic en él para ejecutarlo **y en muy pocas ocasiones como instalador ejecutable**, ya que necesitan instalarse a nivel de administrador o requieren componentes especiales (es el caso del Microsoft Office® para Mac, la *suite* Adobe Photoshop® y Dreamweaver®, iLife u otros).

Instalación mediante un instalador

Emplean un **archivo ejecutable** o **instalador** (fichero *.exe* normalmente), que viene soportado en un medio de almacenamiento, un CD o DVD, o bien en un archivo que nos hemos descargado de Internet, que posteriormente instala el software deseado en un determinado lugar y deja constancia de ello al Sistema Operativo (*Agregar/Quitar Programas*).

En la plataforma **Windows®** es habitual el uso de instaladores de forma que cada programa instalado va repartiendo diversos ficheros por diferentes subdirectorios, añadiendo líneas al **registro del sistema** (editor de registro o **regedit.exe**), e instalando nuevas librerías, habitualmente con formato DLL, en los directorios *windows/system* y *windows/system32*.

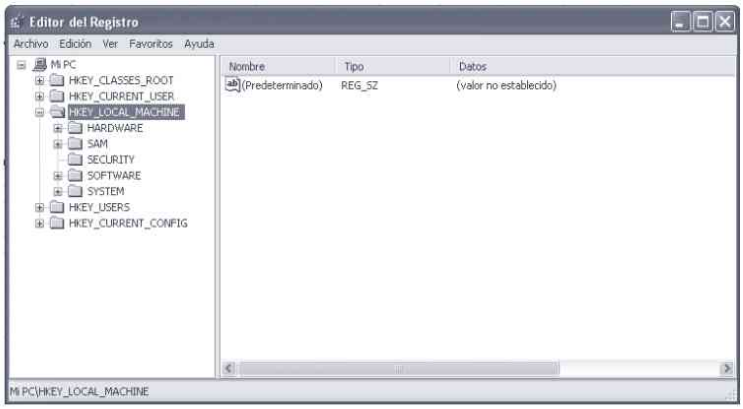


***Figura 6.5**. Editor del registro de Windows*

Los instaladores son el mejor método para hacer este proceso **transparente** al usuario. Los ejecutables y componentes principales de los programas se suelen almacenar en los directorios **Archivos de Programa** (*Program Files*) o en la propia **raíz del disco**.

Este tipo de instalación hace necesario el uso de desinstaladores para tratar de no dejar rastro de dicha aplicación al quitarla y que no haya ningún elemento de la misma que afecte al rendimiento.

¿SABÍAS QUE...?

La instalación de nuevos programas en Windows® afecta al rendimiento del mismo y puede desestabilizar el funcionamiento por lo que no es aconsejable instalar y desinstalar aplicaciones de forma permanente.

Instalación usando un sistema o gestor de paquetes

El Sistema Operativo o algún software específico se ocupan de instalar un paquete de software con todos los archivos requeridos. Para tal fin se emplean una colección de herramientas que sirven para automatizar el proceso de instalación, actualización, configuración y eliminación de paquetes de software.

Se emplean básicamente en **plataformas Linux**, donde el software se distribuye en forma de paquetes, que pueden ser descargados o accedidos directamente desde Internet a través de los **repositorios** que incluyen, además del propio software, información llamada *metainformación*, que incluye datos como el nombre completo, descripción de funcionalidad, número de versión, distribuidor, suma de verificación (para comprobar la autenticidad del paquete, comparando dicho valor con el valor de la versión oficial) y lista de paquetes requeridos para un correcto funcionamiento. En muchos casos se deben resolver dependencias para garantizar que el software funcione correctamente.

Esta metainformación se suele almacenar en una base de datos de paquetes local.

Son sistemas basados en paquetes binarios:

- **dpkg**, usado por la distribución Linux Debian y otros, emplea el formato *.deb* y fue el primero en emplear una herramienta gestor de paquetes, **APT**.
- **fink**, para Mac-Osx, pretende hacer más sencilla la instalación de programas libres.
- **Sistema rpm**, creado por la distribución Linux Red Hat y usado por gran número de distribuciones Linux a través de herramientas como **urpmi** (Mandriva), **Yast** (Suse) o **Yum** (Fedora).
- **Sistema tgz**,usado por la distribución Linux Slackware, emplea *.tar* y *.gzip*, con herramientas como *slapt-get*, *slackpkg*.
- **Pacman**, para archivos Linux, emplea *.tgz*.

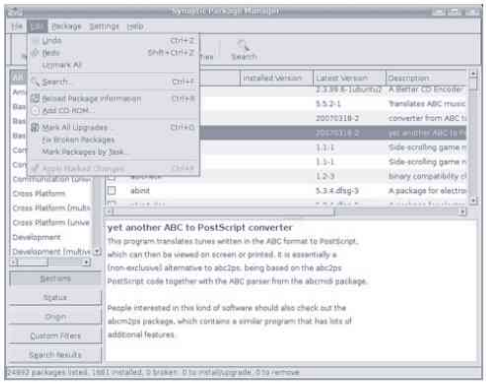


***Figura 6.6**. Gestor de paquetes Synaptic en una instalación Linux*

Instalación usando una aplicación portable

La ventaja que tienen las aplicaciones portables frente a las convencionales es su ausencia de instalación. Estas aplicaciones portables pueden funcionar sin tener que instalar ninguna librería adicional en el equipo destino. Generalmente, se almacenan en un *pendrive* y pueden ejecutarse en cualquier equipo con sistema operativo compatible. En el caso de que se quieran dejar en el equipo de forma permanente basta con copiar una carpeta de la memoria USB al equipo destino.

En muchos sistemas operativos el concepto de portátil no tiene sentido puesto que las aplicaciones son portátiles de por sí. Un ejemplo de esto es el sistema MAC OS X o AmigaOS. El sistema operativo con aplicaciones que se instalen menos portables es Windows® dado que la idea de registro hace imposible este concepto.

Para realizar una aplicación portátil, lo que debe conseguir el desarrollador es que el programa no necesite de librerías que no se puedan encontrar en el equipo destino, también deberán dejar el equipo intacto sin modificar el registro o crear algún archivo en un directorio distinto del directorio de instalación.

***Figura 6.7**. Aplicaciones portables*

6.3 PASOS BÁSICOS DE UNA INSTALACIÓN

En todo modelo de instalación se llevan a cabo unos **pasos de instalación básicos**:

1 **Comprobar** si se cumplen los **requisitos de instalación** en cuanto a hardware y software. A veces requiere la desinstalación de versiones antiguas del mismo software.

2 **Verificación** de que el **software es original**, para evitar la instalación de programas maliciosos.

3 **Creación de los directorios** necesarios para la instalación de los archivos necesarios.

4 **Creación de usuarios y permisos necesarios**, en ocasiones por petición explícita de la aplicación o como recomendación para delimitar responsabilidades y limitar daños en caso necesario.

5 **Copia**, **desempaquetado y descompresión** de los archivos del paquete de software. Habitualmente para ahorrar ancho de banda y tiempo en la transmisión por Internet o espacio en disco duro los paquetes vienen empaquetados y comprimidos.

En dichos paquetes se incluyen los archivos principales, archivos de datos, archivos de configuración, bibliotecas o librerías, documentación, etc.

6 **Compilación y enlace con las bibliotecas** requeridas ya presentes o que se instalaron con anterioridad.

7 **Configuración de la aplicación** y definición de las variables de entorno, por medio de archivos para tal fin. Se lleva a cabo de forma manual, editando ficheros de texto o de forma guiada por medio de ventanas.

8 **Registro de la instalación** en el caso de software comercial. Se puede presentar en distintas formas: *on line*, relleno de formulario, inserción de número de serie y/o clave de activación, etc.

La instalación de aplicaciones en grandes sistemas empresariales, en los que además es probable que no pueda dejar en ningún momento de funcionar el sistema informático, es bastante más compleja. Normalmente, hablamos de software a medida y la realiza la empresa que desarrolló el software (es una etapa más del ciclo de vida del software, una tarea dentro de la etapa de implementación, cuyo objetivo era la puesta en marcha del sistema desarrollado y evaluación de su funcionamiento). En tal caso la aplicación deberá acompañarse de una completa documentación: guía de instalación, especificaciones de la aplicación, manual de procedimiento, manual de administración del sistema.

Se pueden presentar dos casos:

- Que sea el primer sistema automatizado que se implanta en la empresa.
- Que no sea así y haya traspaso de un sistema antiguo a otro más nuevo, para lo cual se pueden presentar distintas formas de proceder:
  - **Proceso encadenado**. Continúa funcionando el antiguo de forma que los resultados del nuevo se contrastan y comparan con el antiguo.
  - **Proceso directo**. Desactivación del antiguo y activación directa del nuevo.
  - **Proceso en paralelo**. Ambos conviven a la vez hasta comprobar la fiabilidad del nuevo.
  - **Proceso por subsistemas**. Ambos sistemas, antiguo y nuevo, se reparten el trabajo.

6.4 CONFIGURACIÓN DE APLICACIONES

La configuración de aplicaciones la forman aquel conjunto de acciones que determina el valor de algunas variables de una aplicación en su ejecución. Estas opciones son cargadas en su inicio y en ocasiones habrá que reiniciar la aplicación para poder ver los cambios, ya que no pueden ser cargados mientras se está ejecutando.

Existen por tanto dos configuraciones típicas:

- **Configuración predeterminada**. Es la que se carga cuando no se ha definido ninguna y no suele ser la más idónea cuando se da una configuración personalizada como opción. Esta configuración pretende ser lo más adaptada posible a todos los perfiles de usuarios (de diferentes edades y sexos, en diferentes idiomas, suele cargar el idioma del sistema operativo) y con unas exigencias de recursos del ordenador en cuanto a memoria y espacio en disco medias.
- **Configuración personalizada**. Es aquella determinada de forma específica por el usuario y suele incluir elementos como selección de idioma, ruta de instalación y trabajo, componentes a instalar, etc.

Las opciones de configuración suelen almacenarse en un archivo o base de datos que puede presentarse en forma de texto plano, en sistemas Unix sobre todo, para que sea editable desde fuera del programa, o de forma cifrada para que solo pueda ser modificada por el programa a configurar.

¿SABÍAS QUE...?

En el proceso de configuración pueden ocurrir **errores de configuración** que lleven a la imposibilidad de ejecución o a una ejecución defectuosa. Para que esto no ocurra es importante leer los requerimientos mínimos de una configuración y que los valores elegidos estén por debajo de estos umbrales.

6.5 ELIMINACIÓN DE APLICACIONES

Para eliminar una aplicación del ordenador hay que seguir un proceso muy sencillo que se llama **desinstalación**, y que será distinto dependiendo del modelo de instalación que se siguió.

En el caso de haber empleado un instalador, como ocurre en Windows®, será necesario un **desinstalador** que seguirá los siguientes pasos:

1. Eliminación automática de los archivos que constituyen la aplicación.
2. Ajustes necesarios de configuración del sistema operativo, de forma automática.

3 Eliminación de iconos en el escritorio y en el menú de acceso a aplicaciones, también de forma automática.

Para lanzar el proceso de desinstalación de un programa hay que acceder a una parte específica del sistema, no se debe borrar directamente.

La desinstalación de programas en ordenadores Mac es muy simple y basta con arrastrar el icono de la aplicación a desinstalar a la papelera, aunque en muy pocas ocasiones también se almacenan pequeños archivos de configuración con preferencias que habrá que eliminar.

La desinstalación en los sistemas Linux mediante gestión de paquetes es la más simple, ya que basta con acceder a dicho sistema y marcar el paquete a desinstalar para que de forma automática se elimine todo rastro del mismo.

¿SABÍAS QUE...?

Existen pequeñas aplicaciones encargadas de analizar el sistema en busca de rastros en forma de librerías y archivos de configuración de aplicaciones ya desinstaladas y que están afectando al rendimiento del sistema. Son los programas **Cleaners** que, en el caso de Windows®, también limpian el registro de sistema. En MAC también están presentes con aplicaciones como *Appzapper*, *Appcleaner o Appdelete.*

RESUMEN DEL CAPÍTULO

En este capítulo se estudia y analiza el otro gran componente de un sistema informático, el software, para lo cual, partiendo de sus características básicas tan peculiares, se profundiza sobre su forma de desarrollo e implantación (ciclo de vida).

Aparte de esto, se estudia cómo llevar a cabo operaciones como la instalación, eliminación, actualización o configuración de aplicaciones en un sistema operativo.

EJERCICIOS PROPUESTOS

1. Investigue sobre otros modelos de ciclos de vida del software, aparte del ciclo de vida clásico que se recoge en el libro, y analice las diferencias que encuentre en los mismos.

2. Elabore un cuadro cronológico en el que recoja la evolución de los principales lenguajes de programación, haciendo especial hincapié en los últimos veinte años.

3. Trate de llevar a cabo alguna instalación y desinstalación mediante un instalador y un gestor de paquetes e indique las ventajas e inconvenientes que ha observado en uno y otro.

TEST DE CONOCIMIENTOS

1 Elija la afirmación falsa:

a) En la arquitectura Cliente-Servidor, el software reparte su carga de cómputo en dos partes independientes pero sin reparto claro de funciones.

b) El editor del registro de Windows® se puede invocar ejecutando el programa *regedit.exe*.

c) El software es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados que forman parte de las operaciones de un sistema de computación

d) J.W. Tukey acuñó el término "bit" por primera vez.

2 Elija la afirmación falsa:

a) Los lenguajes de programación de bajo nivel son más sencillos de programar al tener un nivel bajo de complejidad.

b) Existen lenguajes de programación de alto nivel y de bajo nivel.

c) El software de arquitectura monolítica se estructura en componentes funcionales muy acoplados.

d) Existen varios ciclos de vida del software dependiendo del método de desarrollo.

3 Elija la afirmación falsa:
- a) Alan Turing en su teoría de la computación desarrolló la teoría que forma la base del software moderno.
- b) PHP se considera un lenguaje de programación de alto nivel.
- c) Fink es un gestor de paquetes usado por la distribución Linux Debian y otros.
- d) Los lenguajes de programación de bajo nivel ocupan poco espacio en memoria.

4 Elija la afirmación falsa:
- a) Un IDE es una implementación de desarrollo extendido.
- b) El objetivo de la Ingeniería del Software es proporcionar un marco de trabajo para construir software con mayor calidad.
- c) El gestor de paquetes rpm fue creado por la distribución Linux Red Hat.
- d) El software es el equipamiento o soporte lógico de un sistema informático.

5 Elija la afirmación falsa:
- a) Un IDE es un entorno de desarrollo integrado.
- b) Steve Jobs inventó la máquina de Turing.
- c) Una DLL es una librería estática de Windows®.
- d) La instalación de nuevos programas en Windows® afecta al rendimiento del mismo y puede desestabilizar el funcionamiento por lo que no es aconsejable instalar y desinstalar aplicaciones de forma permanente.

6 Elija la afirmación verdadera:
- a) El ensamblador se considera un lenguaje de bajo nivel.
- b) Andrew Tanenbaum en su teoría de la computación desarrolló la teoría que forma la base del software moderno.
- c) El software en su creación y desarrollo pasa por una serie de etapas conocidas como las fases del ciclo empírico del software.
- d) Las pruebas de unidad del software permiten garantizar que los diferentes módulos se integren con la aplicación.

7 Elija la afirmación verdadera:
- a) Existen pruebas alfa y beta del software.
- b) En los sistemas MAC OS X los instaladores modifican el registro a la hora de instalar programas.
- c) En plataformas Windows® el software se distribuye en forma de paquetes, que pueden ser descargados o accedidos directamente desde Internet a través de los repositorios.
- d) La palabra software como tal, fue empleada por primera vez en 1957 por Alan Turing.

8 Elija la afirmación falsa:
- a) El software de sistema es el conjunto de programas o rutinas cuyo objetivo es facilitar el uso de la computadora, permitiendo administrar y asignar los recursos del sistema.
- b) En plataformas Linux el software se distribuye en forma de paquetes.
- c) El análisis de requisitos la viabilidad de un software consiste en definir el resultado del proyecto y su papel en la estrategia global.
- d) El *firmware* es un tipo de software.

7 Introducción a las redes de datos

OBJETIVOS DEL CAPÍTULO

- ✓ Entender qué es una red de datos y sus principales funciones.
- ✓ Conocer los principales servicios proporcionados por las redes de datos.
- ✓ Conocer la diferencia entre redes LAN y redes WAN.
- ✓ Justificar la aplicación de un modelo en capas para el diseño de redes de datos.
- ✓ Entender el funcionamiento general de un modelo de capas.
- ✓ Conocer el modelo OSI y las funciones de sus niveles.
- ✓ Relacionar el modelo OSI con el modelo de la arquitectura TCP/IP.

7.1 ¿QUÉ ES UNA RED DE DATOS?

De una manera general, una **red de datos** (o en este contexto, simplemente **red**) se podría definir como la infraestructura que posibilita que varios dispositivos intercambien datos entre sí, conectados para ello a algún medio físico que permita la transmisión de dichos datos. Los dispositivos que forman parte de la red también reciben el nombre de nodos. En cuanto a los medios físicos, a través de los cuales viajan los datos, estos pueden ser medios guiados (como el clásico cable de cobre o la fibra óptica) o se pueden utilizar ondas electromagnéticas transmitidas a través del aire.

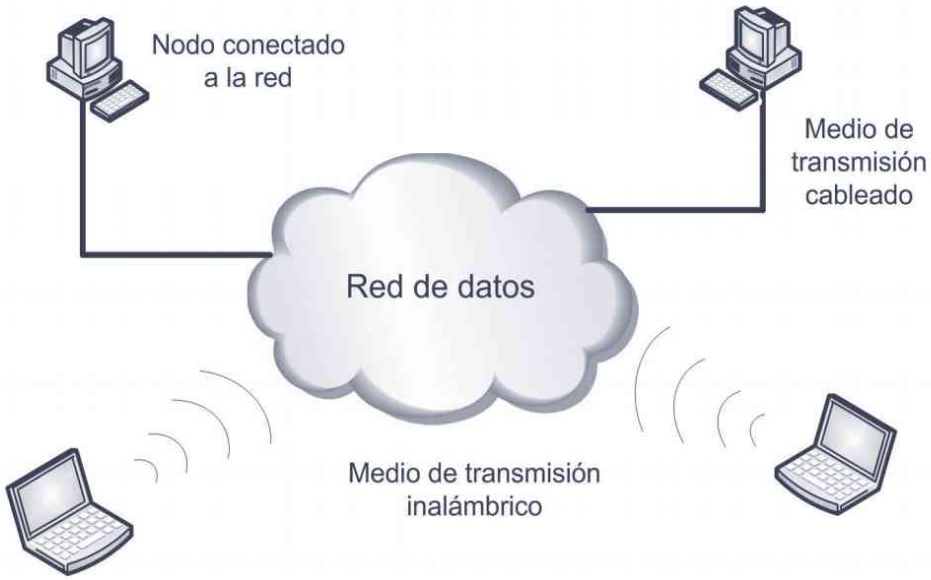


***Figura 7.1**. Varios dispositivos conectados a una red de datos*

En las primeras redes de datos, los nodos que formaban parte de las mismas eran en su gran mayoría ordenadores de sobremesa, grandes servidores o impresoras. En la actualidad, sin embargo, el abanico de dispositivos que pueden conectarse a dichas redes es más amplio, incluyendo ordenadores portátiles, *smartphones*, *tablet* PC, NAS (almacenamiento accesible por red), escáneres, etc.

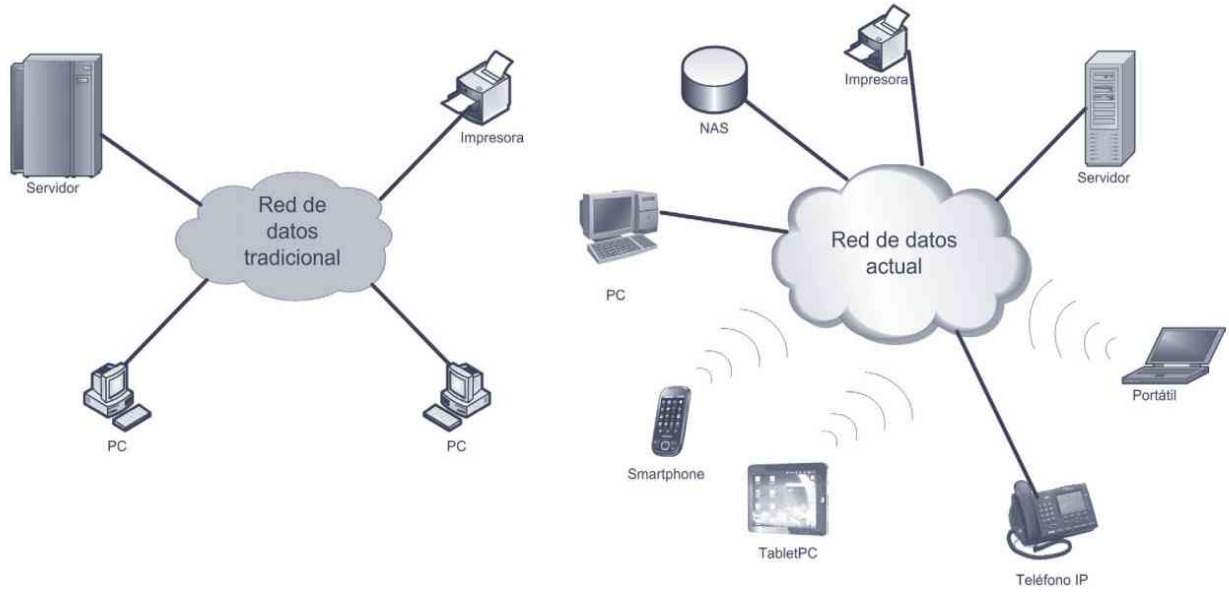


Figura 7.2. *Aumento del tipo de dispositivos que se pueden conectar a las redes telemáticas actualmente*

Y, después de la definición, la siguiente pregunta es, ¿para qué sirven las redes de datos? En un principio, las redes de datos se comenzaron a desarrollar con el objetivo de compartir recursos y de acceder a información a distancia. Derivados de estos primeros objetivos han surgido multitud de servicios telemáticos que actualmente han adquirido una gran importancia, como puede ser, el correo electrónico, el acceso a páginas web, videoconferencia, compartición de recursos como impresoras y unidades de almacenamiento, etc. A dichos servicios, derivados directamente de la aparición de las redes de datos, hay que añadir los servicios de telecomunicación clásicos como la telefonía, radio o televisión, ya que en la actualidad, dichos servicios pueden ser proporcionados por las actuales redes telemáticas.

Ya tenemos, a grandes rasgos, la definición y los objetivos de las redes de datos. Ahora se podrían plantear algunas dudas al intentar aplicar estos conceptos a nuestra realidad diaria. Por ejemplo, "*si yo me conecto en casa o en mi trabajo a Internet, ¿me estoy conectando a una red de datos?*", "*¿es Internet una red de datos?*", "*¿cuándo un establecimiento público, como un restaurante, ofrece conexión Wi-Fi gratuita significa que tienen algún tipo de red datos?*". Bueno, la respuesta a todas esas preguntas es **sí**.

La primera cuestión que conviene aclarar es que **Internet** sí es una red de datos, de hecho es la mayor y más importante red de datos del mundo. Aunque lo cierto es que es una gran red de datos pero un poco especial, porque la principal función de Internet no es permitir conectar dispositivos sino permitir conectar redes. Internet posibilita la interconexión de millones de redes esparcidas por todo el mundo. Internet es la red de datos que une el resto de redes de datos del mundo. Por ello es conocida como la Red de redes.

En sus inicios, Internet era una red de datos que se ajustaba a la definición ofrecida en este apartado, es decir, conectaba dispositivos generalmente alejados geográficamente, incluso hasta en miles de kilómetros. El desarrollo tecnológico en las telecomunicaciones y la aparición de las redes de área local ha producido un cambio de su "función" a la interconexión de redes.

Por lo tanto, hay que tener claro que cuando nos conectamos a Internet en casa, o en el trabajo, o en un restaurante, realmente nos estamos conectando a una red de datos que a su vez estará conectada al resto de las redes que forman Internet.

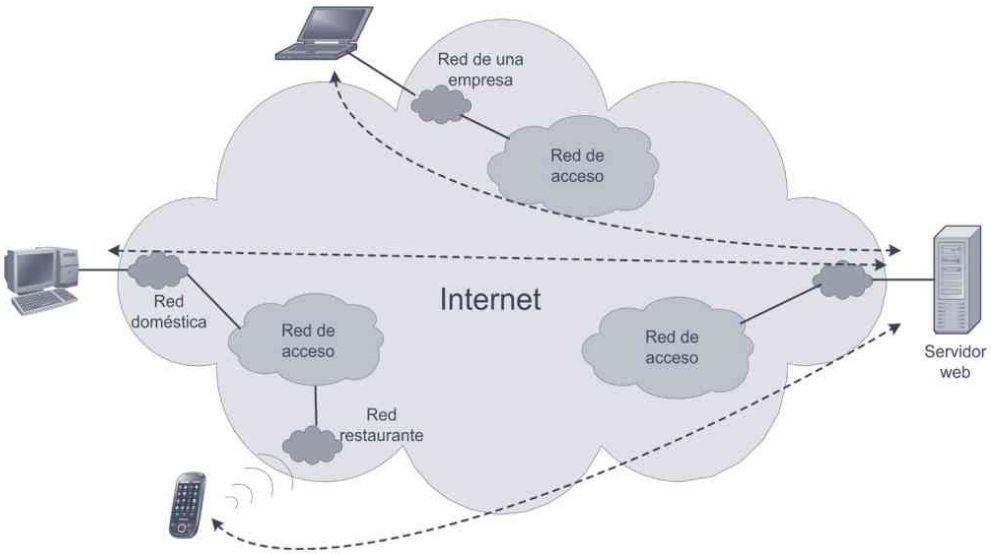


Figura 7.3. *Interconexión de redes de datos formando Internet*

Es importante no perder la perspectiva de lo que realmente ocurre cuando "nos conectamos" a Internet. Para la gran mayoría de personas, "entrar" en Internet es abrir en el ordenador un navegador web (Internet Explorer, Firefox, Chrome…) y acceder a alguna página web. Precisamente en ese punto se produce la comunicación entre dos dispositivos que forman parte de redes de datos. Un dispositivo es mi ordenador y el otro dispositivo es un servidor (también un ordenador pero con mucha potencia y prestaciones) ubicado en algún lugar del mundo. Esta perspectiva se puede visualizar en la Figura 7.3.

7.2 ¿QUÉ SERVICIOS NOS OFRECEN LAS REDES DE DATOS?

O dicho de otra manera, ¿qué podemos hacer cuando nos conectamos a una red de datos? Principalmente, los servicios ofrecidos por las redes se pueden clasificar en función del ámbito de la red:

- **Servicios ofrecidos en redes privadas**

  El escenario de este tipo de servicios es una red que conecta los ordenadores de una empresa dentro de un ámbito geográfico limitado, por ejemplo, un edificio. En este caso, los servicios principales son:

  - Compartir información (archivos).
  - Compartir recursos hardware (impresoras, escáneres, fotocopiadoras…).
  - Acceso al servicio web de la empresa (lo que se conoce como **intranet**) o a aplicaciones corporativas (de gestión, bases de datos, etc.).
  - Servicio de directorio para la gestión de recursos de red y nombres de usuario.
  - Acceso a otras redes, típicamente Internet.

Es decir, desde el ordenador del empleado de una empresa que tenga su propia red, se podrá acceder a archivos ubicados en otros ordenadores de la empresa, podrá enviar trabajos de impresión a las impresoras de la empresa o podrá acceder tanto a la intranet de la empresa como a Internet.

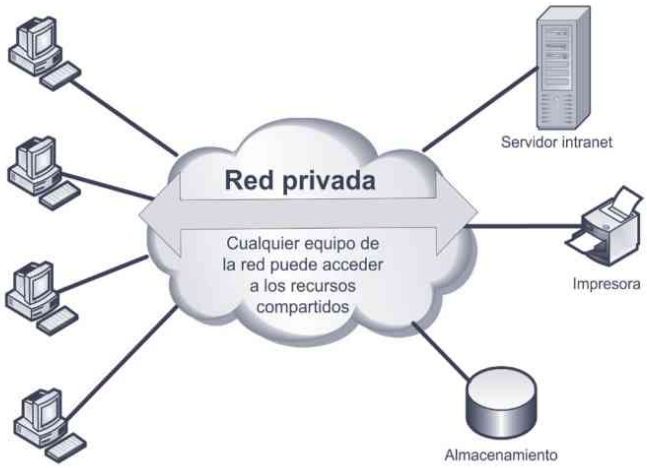


***Figura 7.4**. Esquema general de una red privada*

IMPORTANTE

El termino **intranet** se aplica habitualmente al servicio de páginas web proporcionado por una empresa de forma interna. Para acceder a la intranet de una empresa se utiliza un navegador web. Normalmente el acceso a una intranet solo es posible desde un equipo ubicado dentro de la propia empresa

Servicios ofrecidos a través de Internet (red pública)

Actualmente, la mayor parte de los servicios que se proporcionan en Internet se hacen mediante el servicio web, es decir, el acceso a los servicios se hace utilizando un navegador web. Algunos ejemplos son:

- Acceso a páginas web.
- Servicio de correo electrónico.
- Servicio de mensajería instantánea (*chat*).
- Servicios multimedia como la visualización de programas de televisión, radio, películas o música.
- Comercio electrónico.
- Acceso a las denominadas redes sociales.

Aunque lo más extendido sigue siendo el uso de un PC (de sobremesa, portátil o *notebook*) para conectarnos a las redes de datos, cada vez es más común el uso de otros dispositivos como teléfonos móviles de última generación (*smartphones*), *tablets*, consolas o televisiones.

En este apartado no se han mencionado todos los servicios que pueden proporcionar las redes de datos pero sí algunos de los más representativos.

7.3 REDES LAN Y REDES WAN

La principal clasificación que se hace actualmente de las redes de datos es en función del ámbito o alcance geográfico de la red. Y, en función de este factor, podemos distinguir entre dos tipos de redes: LAN y WAN.

7.3.1 REDES LAN

El término **LAN** (*Local Area Network* o red de área local) se aplica a una red de datos cuando los dispositivos unidos en dicha red se encuentran ubicados en un área geográfica limitada. Las distancias entre dispositivos conectados a una red de área local pueden variar entre unos pocos metros hasta varios cientos de metros o incluso kilómetros. En este caso, lo importante es que toda la infraestructura que forma la red pertenezca a una misma unidad organizativa, por ejemplo, una empresa, institución educativa, organismo público...

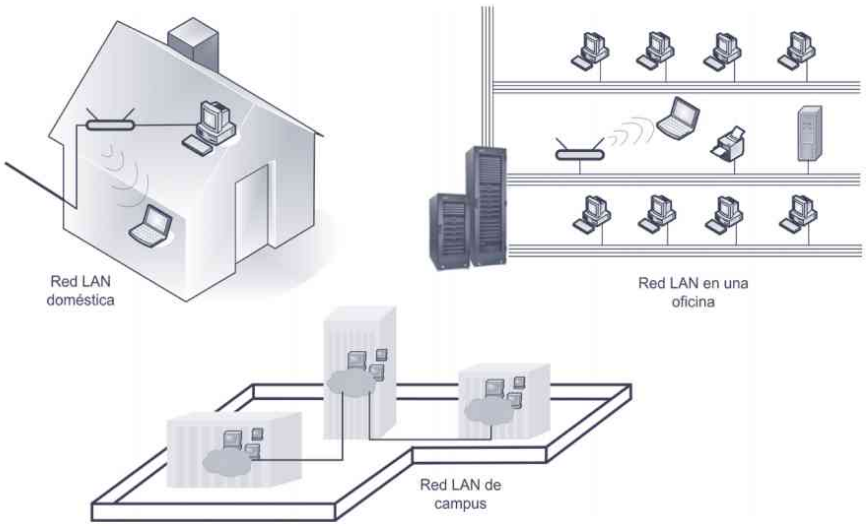


***Figura 7.5**. Diferentes ejemplos de redes LAN*

Se han desarrollado tecnologías específicas para implementar este tipo de redes, por ello, otro criterio habitual de identificación de una red LAN es el uso de una tecnología específica para redes LAN. Los estándares actuales de redes LAN son Ethernet y Wi-Fi, que se estudiarán con detalle más adelante.

Lo cierto es que la aparición de diferentes estándares de Ethernet sobre fibra óptica ha facilitado que Ethernet extienda su uso no solo ha redes LAN sino también a redes WAN.

7.3.2 REDES WAN

El término **WAN** (*Wide Area Network* o red de área extensa) se aplica realmente a la infraestructura que permite la conexión de redes o dispositivos ubicados en diferentes zonas geográficas sin límite de distancia. En resumidas cuentas, todo lo que no sean infraestructuras pertenecientes a redes LAN serán redes WAN. Una característica muy significativa en este tipo de redes es el uso de las infraestructuras proporcionadas por los operadores de telecomunicación cuyo ámbito de actuación esté dentro de las zonas que cubren este tipo de redes. Existen tecnologías específicas para redes WAN, como Frame Relay, ATM, xDSL, etc.

Es necesario destacar la expresión "sin límite de distancia", es decir, se puede utilizar una red WAN para unir dispositivos (o redes) dentro de, por ejemplo, la misma ciudad. O se podría utilizar una red WAN para unir dispositivos (o redes) separados miles de kilómetros.

Veamos los dos principales ejemplos del uso de redes WAN: la conexión de una LAN a Internet y la conexión privada de dos o más LAN. En el primer caso, se desea conectar una red doméstica con la red de un **ISP**. Esta conexión necesita utilizar infraestructuras de algún operador de telecomunicaciones, que podría ser la misma empresa que proporciona el acceso a Internet.

***Figura 7.6**. Ejemplo de red WAN para conectar una red LAN a Internet*

ISP: *Internet Service Provider*. Empresa que proporciona el servicio de conexión a Internet, por ejemplo, Telefónica, Jazztel, Ono...

En el segundo caso, se utilizan las infraestructuras de redes WAN para unir diferentes sedes de una empresa ubicadas en distintas ciudades.

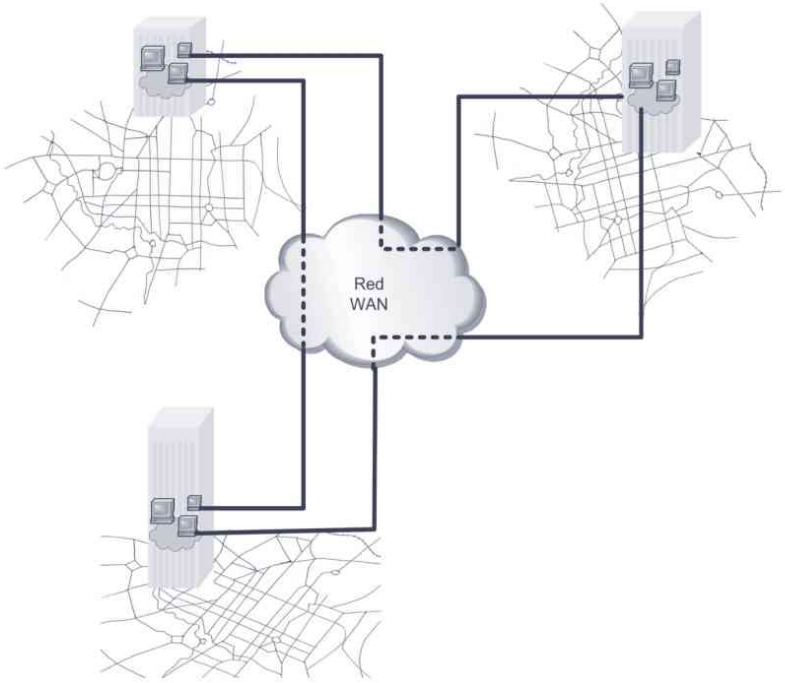


Figura 7.7. *Conexión de varias sedes ubicadas en diferentes núcleos urbanos mediante una red WAN*

Existe bibliografía que añade un tercer tipo de redes llamadas **MAN** (*Metropolitan Area Network* o red de área metropolitana). Este término se aplica a redes que unen redes LAN o dispositivos dispersos en varias ubicaciones dentro de un núcleo de población o de varios núcleos cercanos entre sí. Se suelen utilizar las infraestructuras de operadores de telecomunicaciones que dan servicio en la zona de cobertura de la red MAN.
Lo cierto es que la tendencia actual es la de utilizar las mismas infraestructuras, tecnologías y protocolos para redes MAN y redes WAN, por lo que la única diferencia entre ellas es el ámbito geográfico.

7.4 MODELOS DE DISEÑO DE REDES: OSI Y TCP/IP

7.4.1 JUSTIFICACIÓN DEL USO DE UN MODELO BASADO EN NIVELES

Antes de empezar a profundizar en las tecnologías, técnicas y procedimientos que forman parte de las redes de datos hay que tener en cuenta una idea importante: el proceso de comunicación llevado a cabo en las redes es **complejo**.

Para afrontar esta complejidad, el diseño dichas redes se lleva a cabo utilizando el concepto de capas o niveles. La idea fundamental de este tipo de diseño es dividir el proceso de comunicación en niveles. Cada uno de estos niveles deberá implementar una serie de funciones concretas sin tener en cuenta el resto de funciones, que serán resueltas en otros niveles.

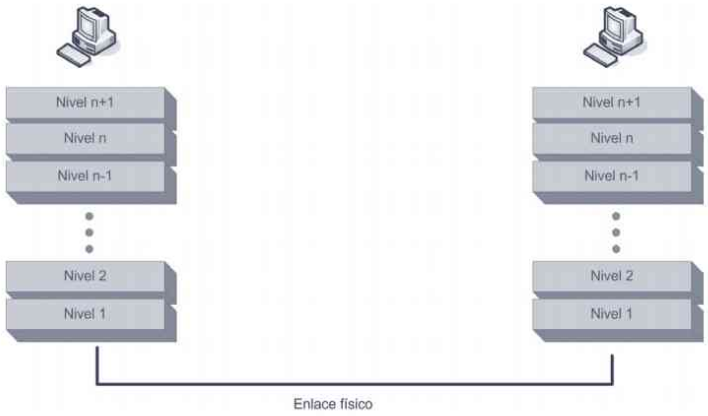


Figura 7.8. *Arquitectura de red por niveles*

RECUERDA

El proceso de comunicación en las redes de datos es complejo. Una posible estrategia para afrontar esta complejidad es agrupar todas las funciones de la comunicación en capas o niveles.

El diseño de una arquitectura en niveles está basado en los siguientes principios:

- Cada nivel lleva a cabo una serie de funciones de la comunicación. Estas funciones deben estar claramente definidas.
- El número de niveles y su función puede ser diferente en cada arquitectura de red. El número de niveles debe ser suficiente para separar las funciones de forma eficiente pero un número demasiado alto de niveles complicaría en exceso el diseño.

- Cada nivel n conoce la existencia de los niveles adyacentes, es decir, el nivel superior $n + 1$ y el nivel inferior $n - 1$.
- La comunicación entre niveles adyacentes se lleva a cabo por medio de servicios. Se dice, por tanto, que cada nivel ofrece servicios al nivel superior y utiliza servicios del nivel inferior.
- Una interfaz define básicamente qué información y servicios ofrece un nivel determinado al nivel superior. Es muy importante que las interfaces estén muy bien definidas. Cuando esto ocurre, la implementación específica de las funciones de un nivel puede ser modificada o reemplazada sin realizar ningún cambio en los niveles adyacentes, característica que se conoce como modularidad. Unas interfaces bien definidas proporcionan modularidad a la arquitectura de red.
- El diseño de las interfaces debe hacerse de forma que se minimice el flujo de información entre los niveles, en definitiva, las interfaces deben ser lo más sencillas posible.

A lo largo del tiempo, ha habido dos modelos de arquitectura de red que se han convertido en referencia dentro de las redes de datos y que debemos conocer y entender: uno teórico, el modelo OSI, y otro práctico, el modelo TCP/IP. Más adelante en este capítulo, se proporcionarán algunas nociones básicas del modelo OSI y en el Capítulo 10 se abordará en profundidad el modelo que siguen prácticamente todas las redes en la actualidad, el modelo TCP/IP.

7.4.2 TRANSFERENCIA DE INFORMACIÓN EN UN MODELO BASADO EN NIVELES

El fin último de cualquier modelo de red es transferir datos de un sistema a otro. En el caso de un modelo basado en niveles, el flujo de información se lleva a cabo según lo mostrado en la Figura 7.9. Cuando un nivel tiene que transferir datos, estos deben pasar obligatoriamente por todos los niveles inferiores hasta alcanzar el destino de la comunicación, donde la información transmitida deberá pasar igualmente por los niveles inferiores hasta alcanzar el nivel de destino.

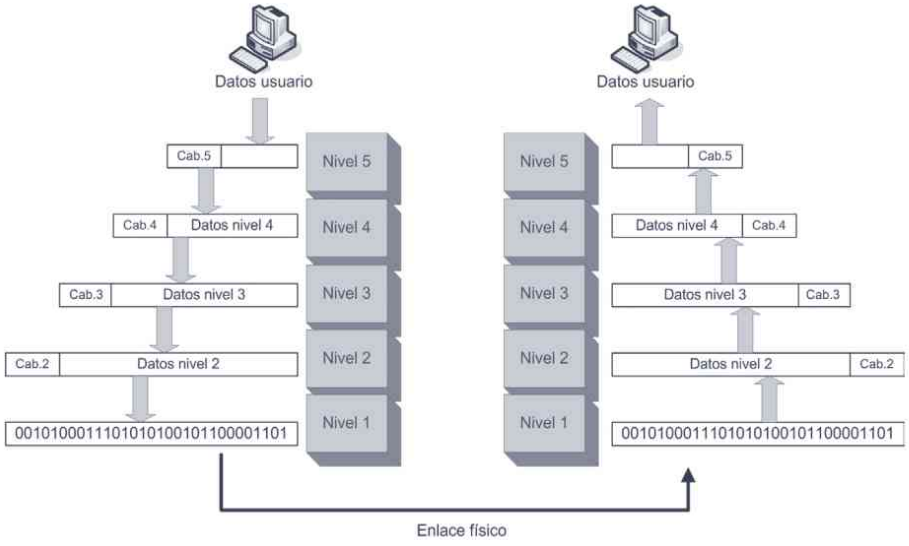


Figura 7.9. *Transferencia de datos en un modelo basado en niveles*

Cada uno de los niveles tiene asignado una serie de funciones y algunas de esas funciones necesitan el envío de cierta información de control. Esta información de control se añade al comienzo del bloque de datos y se conoce como **cabecera**. Es fácil deducir que debe haber cierta correspondencia en lo que se hace en el nivel *n* del emisor y el nivel *n* del receptor, a los que se conoce como **niveles homónimos**. Es decir, los niveles homónimos deben "entenderse" para que la comunicación sea efectiva. De hecho, la información de control que contiene la cabecera de un determinado nivel de la comunicación será tratada por el nivel inferior como datos sin ningún significado especial y solo el nivel homónimo en el receptor será capaz de interpretarlos.

En la jerarquía de niveles del receptor el proceso será el inverso. Los datos llegarán al nivel más bajo, éste utilizará la información de la cabecera para llevar a cabo sus funciones y pasará los datos al nivel superior suprimiendo su cabecera. Este procedimiento se repite hasta alcanzar el nivel más alto que entrega los datos al proceso destino.

El mecanismo que permite el "entendimiento" entre dos niveles homónimos de la comunicación se denomina protocolo y es uno de los conceptos clave en la implementación de las redes telemáticas. Un **protocolo** se puede definir como un conjunto de reglas que se establecen para llevar a cabo una comunicación. Muy importante, hay que tener en cuenta que estas reglas se establecen siempre entre niveles homónimos. Así, si dos dispositivos que desean comunicarse mediante una red de datos utilizan diferentes protocolos en un determinado nivel, la comunicación simplemente, no será posible. A la lista de protocolos empleados en un sistema, con un protocolo por nivel como mínimo, se le denomina **pila de protocolos**.

Se podría decir, por tanto, que en un modelo por niveles existen dos comunicaciones. Una real, llevada a cabo entre niveles adyacentes y cuya implementación a través de servicios se denomina interfaz, y otra virtual, llevada a cabo entre niveles homónimos a través de los llamados protocolos.

RECUERDA

Los protocolos son reglas que se establecen para llevar a cabo la comunicación en los niveles homónimos. Este término suele emplearse para referirse a la comunicación en los niveles superiores de los modelos de red.

7.4.3 MODELO OSI

El modelo **OSI** (*Open System Interconnection*, interconexión de sistemas abiertos) fue publicado en 1983 por el organismo de estandarización ISO. Este modelo recibe el código ISO 7498 y también forma parte de las recomendaciones de la ITU-T como recomendación X.200.

OSI es un modelo basado en niveles para el diseño de sistemas de red. Este modelo además permite la interconexión de sistemas abiertos, o lo que es lo mismo, permite que dos sistemas diferentes se puedan comunicar independientemente de su arquitectura. Es importante resaltar que OSI es un modelo, no un protocolo. Además, el modelo OSI no especifica los servicios ni los protocolos que forman parte de cada nivel.

Los niveles definidos en el modelo OSI son siete: **físico**, **enlace**, **red**, **transporte**, **sesión**, **presentación**, **aplicación**.

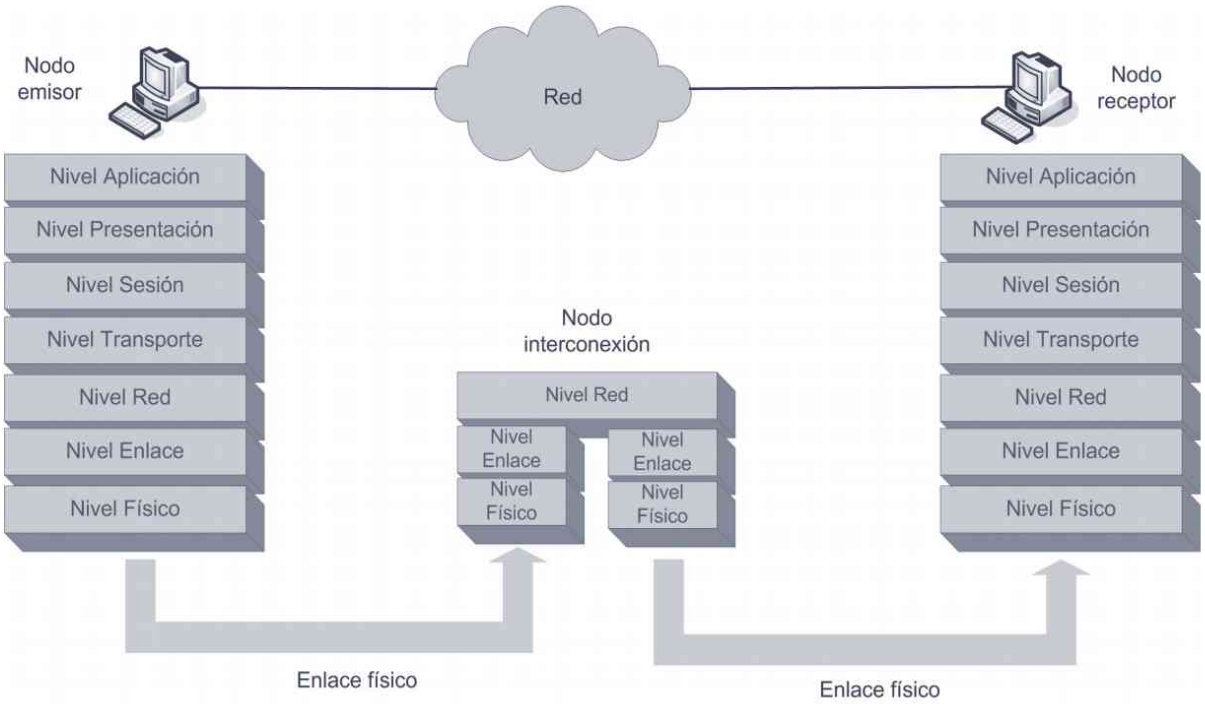


***Figura 7.10**. Modelo OSI*

En el modelo OSI, los niveles superiores se implementan por software mientras que los inferiores suelen llevar un alto componente hardware. El nivel físico es principalmente hardware.

En el gráfico anterior se tiene en cuenta la existencia de sistemas intermedios entre el emisor y receptor que pueden requerir la implementación de uno o varios niveles. Los sistemas intermedios más sofisticados podrán tener implementados los tres primeros niveles de la arquitectura, es decir, hasta el nivel de red.

En los próximos apartados se exponen brevemente las funciones que deben ser cubiertas por cada uno de los niveles del modelo OSI.

Nivel 7. Aplicación

El nivel de aplicación es el nivel de la comunicación en el que un usuario interactúa con la red. Este es el nivel más alto del modelo y, por tanto, es el nivel donde se generan los datos que luego viajarán por las redes. En este nivel se define lo que se conoce como **servicios de red**. Cuando un usuario quiere transferir un archivo de un equipo a otro, utiliza un servicio de red de compartición de archivos (por ejemplo, el servicio proporcionado por Windows® para compartir archivos). O si desea acceder a la información que una empresa proporciona en su página web utiliza el servicio web para acceder a dicha información. Tanto la compartición de archivos en red como el acceso a páginas web son ejemplos de servicios proporcionados por el nivel de aplicación.

Nivel 6. Presentación

El nivel de presentación se encarga básicamente de aislar las capas inferiores del formato de los datos del nivel de aplicación. Este nivel implementa características que tienen que ver con la sintaxis y la semántica de la información que se intercambia entre un emisor y un receptor.

Para ello, las principales funciones que se llevan a cabo son:

- **Conversión de formatos**. Si fuese necesaria cuando el emisor y el receptor utilizan sistemas de codificación diferentes.
- **Cifrado**. Algunos procesos de red necesitan que la información se transmita cifrada para asegurar su privacidad. Los datos son transformados en función de los algoritmos de cifrado y en el receptor se realiza el proceso inverso para recuperar los datos originales.
- **Compresión**. Para aumentar las prestaciones de la transferencia de datos, sobre todo para volúmenes altos.

Nivel 5. Sesión

El nivel de sesión organiza y sincroniza el intercambio de datos entre procesos de aplicación. Las funciones que se llevan a cabo son:

- **Gestión de sesiones**. Para ello implementa las funciones necesarias para crear, mantener y finalizar sesiones de comunicación.
- **Sincronización**. Funciona con el nivel de aplicación para proporcionar conjuntos de datos sencillos llamados puntos de sincronización, que permitirá a una aplicación conocer cómo está progresando la transmisión y recepción de datos. En caso de pérdida de transmisión o de errores es capaz de resincronizar el flujo de información.

Este nivel asume que los dos extremos de la comunicación tienen la misma categoría, algo que no es muy frecuente en los servicios de red, los cuales son en su gran mayoría de tipo cliente-servidor.

Nivel 4. Transporte

El nivel de transporte se encarga de realizar la entrega completa y sin errores del mensaje desde el origen hasta el destino. Para ello debe desarrollar las siguientes funciones:

- **Control de la conexión**. El nivel de transporte puede proporcionar servicios orientados a la conexión. En este caso, el envío de los datos del emisor al receptor se lleva a cabo en tres pasos: *establecimiento de la conexión*, *transferencia de los datos* y *finalización de la conexión*. Este tipo de servicios proporciona fiabilidad a la comunicación ya que antes de enviar los datos se comprueba que el receptor está preparado para recibirlos. Un ejemplo de protocolo del nivel de transporte orientado a conexión es TCP. Por el contrario, en los protocolos no orientados a conexión está función no se lleva a cabo. Un ejemplo de protocolo del nivel de transporte no orientado a conexión es UDP.
- **Control de flujo**. En una transmisión puede ocurrir que el receptor no sea capaz de procesar la información a la velocidad a la que la recibe y, por tanto, hay que implementar un mecanismo para que el emisor envíe datos solo cuando el receptor los pueda procesar. El nivel de transporte se encarga de llevar a cabo la función de control de flujo de extremo a extremo de la comunicación.
- **Control de errores**. Otra función importante del nivel de transporte es proporcionar mecanismos para detectar y corregir los errores que se produzcan en la comunicación de extremo a extremo. La información en este nivel se envía fragmentada en paquetes y el nivel de transporte se encarga de que los paquetes enviados lleguen sin errores, sin pérdidas y sin duplicados.
- **Direccionamiento**. Un equipo conectado a una red puede tener varios procesos, normalmente en la capa de aplicación, que llevan a cabo comunicación de datos a través de la red. Por ello, es necesario distinguir qué procesos dentro de cada equipo emisor y receptor están intercambiando información. Este direccionamiento se lleva a cabo en el nivel de transporte a través de la llamada dirección de **punto de servicio o dirección de puerto**.

Nivel 3. Red

El nivel de red se encarga de todas las funciones necesarias para encaminar la información a través de varias redes. Sus funciones son necesarias cuando el emisor y el receptor están en redes diferentes. Este nivel recibe un paquete de datos del nivel superior y se encarga de que llegue a su destino siendo necesario llevar a cabo mecanismos de encaminamiento. Las funciones básicas que realiza son:

- **Encaminamiento o enrutamiento de los paquetes**. El nivel de red proporciona los mecanismos para la identificación de la ruta que deben llevar los paquetes de datos hasta alcanzar su destino.

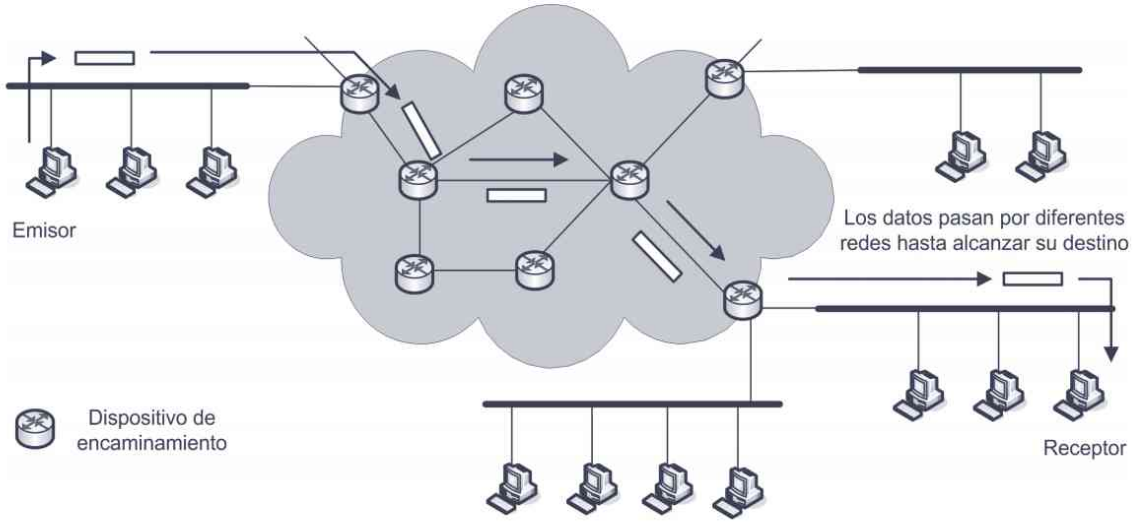


Figura 7.11. Encaminamiento en el nivel de red

- **Proporcionar un direccionamiento lógico**. Es necesario establecer un mecanismo de direccionamiento utilizado para identificar cada dispositivo en la red. Además, este direccionamiento debe ser jerárquico, incluyendo información de la red a la que está conectado dicho dispositivo. Por lo tanto, cada equipo debe identificarse a través de una dirección lógica.
- **Control de la congestión**. La congestión se produce en las redes cuando los dispositivos de enrutamiento no son capaces de manejar el volumen de tráfico presente en la red. El control de la congestión podría confundirse con el control de flujo. La diferencia es que el control de la congestión se implementa para asegurar que la red es capaz de transportar el tráfico ofrecido mientras que el control de flujo está referido solo a la conexión entre dos dispositivos concretos.

Nivel 2. Enlace

La transmisión de los datos se lleva a cabo en el nivel físico, aunque dicho nivel no proporciona ningún mecanismo para asegurar que los datos (bits) que se envían llegarán libres de errores al receptor. El objetivo del nivel físico es llevar a cabo la transmisión de los datos con la mayor fiabilidad posible pero sin llevar a cabo ningún control de errores, función de la que se encarga el nivel de enlace. La principal función del nivel de enlace es, por tanto, proporcionar fiabilidad a la transmisión entre dos dispositivos unidos mediante un enlace.

Además, el nivel de enlace lleva a cabo las siguientes funciones:

- **Encapsulación de datos: tramado.** Para llevar a cabo las funciones del nivel de enlace se hace necesario dividir el flujo de datos que llega del nivel superior en bloques de datos llamados *tramas*, a las cuales se añaden la cabecera con información de control del nivel de enlace. Una de las informaciones de control más importante que se añade es un código de comprobación de errores. Este código no se incluye en la cabecera, sino que suele ir al final de la trama.
- **Proporcionar un direccionamiento físico.** Esto es necesario en los enlaces multipunto donde hay varios dispositivos conectados a una red y cualquiera de ellos puede ser el receptor de los datos. En este caso es necesario proporcionar un mecanismo de identificación del receptor. De hecho, tanto la dirección física del emisor como del receptor es una información incluida en la cabecera que se añade a los datos en el nivel de enlace.
- **Control de acceso al medio.** Esta función no es siempre necesaria, solo cuando el enlace es compartido por varios dispositivos. En este caso, es el nivel de enlace el encargado de determinar qué dispositivo puede acceder al medio para transmitir.
- **Control de flujo.** El control de flujo llevado a cabo en este nivel se refiere al control del flujo de información en un enlace. El objetivo de esta función es que el emisor envíe información a través del enlace solo cuando el receptor pueda procesarla.
- **Control de errores.** Como ya se ha apuntado, ésta es la principal función del nivel de enlace, detectar y corregir los errores de transmisión producidos en un enlace. Esta función incluye la capacidad de detectar y retransmitir tramas con error y tramas perdidas, así como detectar tramas duplicadas.

Es importante diferenciar las funciones de control de flujo y de errores llevadas a cabo en el nivel de enlace y en el nivel de transporte. El nivel de enlace lleva a cabo estas funciones en un enlace y el nivel de transporte lo hace pero para la comunicación de extremo a extremo.

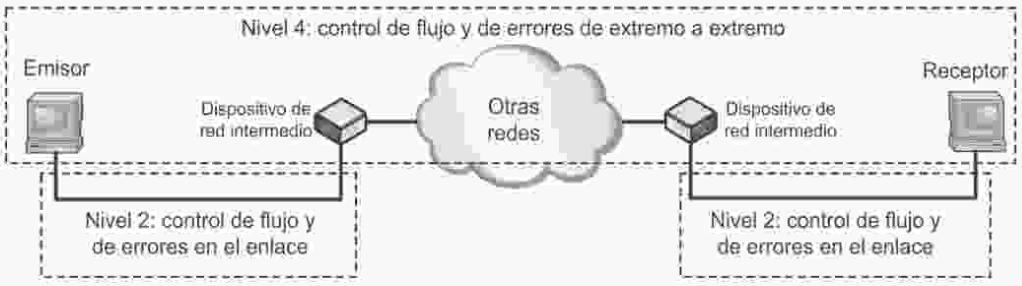


***Figura 7.12.** El control de flujo y de errores se aplica en dos niveles*

Se puede observar que existen 3 niveles en los que se llevan a cabo funciones de direccionamiento aunque en cada nivel la función de la dirección es diferente. En el nivel de enlace, la dirección (llamada *dirección física*) sirve para identificar un dispositivo en un enlace donde puede haber varios dispositivos conectados. En el nivel de red, la dirección (llamada dirección lógica) se utiliza para identificar un dispositivo de forma única en un conjunto de redes. En el nivel de transporte, la dirección (llamada dirección de puerto) sirve para identificar dentro de un dispositivo a qué aplicación van dirigidos los datos. Todas las direcciones son transmitidas en sus correspondientes cabeceras.

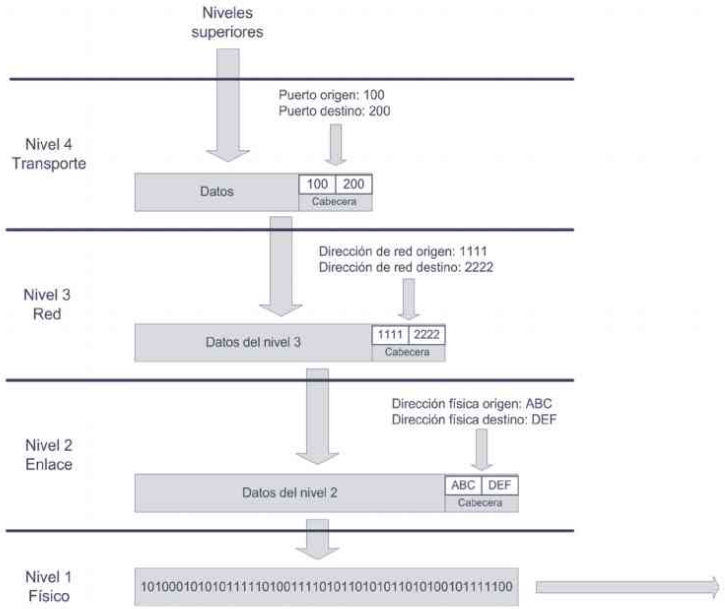


***Figura 7.13**. Direccionamiento en los distintos niveles del modelo OSI*

Nivel 1. Físico

El nivel físico se encarga de la transmisión de la información a través de un medio físico, es decir, el nivel físico debe ser capaz de enviar datos (bits) a través de un canal de comunicaciones (cable de cobre, fibra óptica, aire) procurando que esos datos no sufran alteraciones y puedan ser correctamente interpretados en el receptor. Para lograr este propósito se llevan a cabo las siguientes funciones:

- **Definición de las características físicas de las interfaces con el medio de transmisión**. Por ejemplo, las especificaciones de los conectores (interfaces con el medio de transmisión), tanto eléctricas (nivel de señal, impedancia…) como mecánicas (tipo de conector, dimensiones físicas, distribución del patillaje…) y funcionales (función de cada patilla en el conector…).
- **Definición de las características del medio de transmisión**. En el caso de medios guiados (cable y fibra óptica) será necesario definir las características físicas y mecánicas de dichos medios.
- **Codificación de los datos digitales**. Este proceso consiste en representar los datos digitales, unos y ceros, en señales eléctricas que pueden ser transmitidas por el medio.
- **Configuración de la línea**. Que está referido a la forma en la que se conectan los dispositivos al medio. Puede ser punto a punto o multipunto.
- **Topología física**. La topología se refiere a la forma en la que están conectados entre sí los dispositivos de una red telemática.
- **Modo de transmisión**. Puede ser *símplex*, *half-dúplex*, *full-dúplex*.
- **Velocidad de transmisión**. Con todas las características anteriores se establece la velocidad a la que se pueden transmitir los datos, es decir, la tasa de bits de la comunicación.

La mayor parte de las funciones que aparecen en la lista anterior serán ampliadas en los próximos capítulos. Los principales organismos dedicados a estandarizar las distintas implementaciones del nivel físico han sido la EIA y la ITU-T.

7.4.4 EL MODELO OSI FRENTE A TCP/IP

En el contexto en el que se desarrolló, el modelo OSI parecía una solución a la interconexión de sistemas debido a la existencia de grandes empresas con arquitecturas propietarias e incompatibles, como SNA de IBM y DECnet de Digital.

Sin embargo, la complejidad que supuso el desarrollo de los protocolos que implementarán este modelo y el auge de la arquitectura TCP/IP, que ya tenía sus protocolos desarrollados y estaban suficientemente probados en entornos académicos, supuso el progresivo declive de la implementación del modelo OSI a favor del modelo TCP/IP que ha sido el que se ha impuesto definitivamente propiciado sobre todo por el auge de Internet.

Uno de los principales problemas del modelo OSI es que fue desarrollado sin tener en cuenta los protocolos que luego se deberían utilizar. De esta forma, hay algunos niveles donde apenas se desarrollaron protocolos, como el nivel de sesión, y otros, como el nivel de enlace, en los que fue necesario desarrollar protocolos complejos e incluso dividir sus funciones en subniveles.

La arquitectura TCP/IP propone la existencia de cinco niveles: físico, enlace, red, transporte y aplicación. Como se observa, la diferencia más obvia es que en este modelo no aparecen los niveles de sesión y presentación. Lo que ocurre es que cualquier función por encima del nivel de transporte en TCP/IP se implementa en el nivel de aplicación. Los niveles con más similitudes entre el modelo OSI y el modelo TCP/IP son los de red y de transporte.

La principal aportación del modelo OSI es servir como referencia al desarrollo de arquitecturas de red. En dicho modelo se establecen de forma clara los conceptos de servicio, interfaz y protocolo, cosa que no ocurre en TCP/IP. Por ello, este modelo tiene gran valor pedagógico en el estudio de arquitecturas de red.

Por el contrario, aunque la arquitectura TCP/IP es la que se ha impuesto en la actualidad, su modelo no es un modelo general y solo sirve para describir su propia arquitectura. Como ejemplo, en el modelo TCP/IP no se hace una distinción entre las capas física y de enlace (por lo que, en realidad el modelo TCP/IP consta de cuatro niveles), cosa que desde el punto de vista del diseño de redes no es muy aceptable. Esto es debido a que primero se desarrollaron los protocolos y el modelo TCP/IP es tan solo una descripción de dichos protocolos.

Se puede concluir, por tanto, que la referencia en interconexión de sistemas como modelo es el modelo OSI y como protocolos, son los protocolos de la arquitectura TCP/IP.

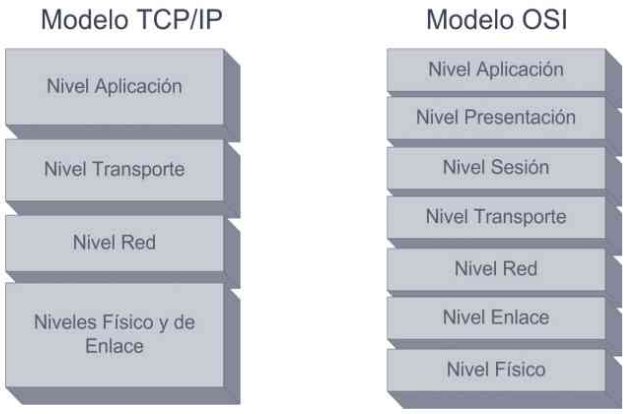


***Figura 7.14**. El modelo TCP/IP frente al modelo OSI*

RESUMEN DEL CAPÍTULO

Este capítulo sirve como introducción a las redes de datos. Se empieza por exponer la definición y las características más generales de las mismas, incluyendo los servicios que proporcionan. Además, se incluye la definición y características de los dos tipos de redes de datos actuales, las redes LAN y las redes WAN.

En la segunda parte del capítulo se ofrece una explicación del modelo de capas o niveles utilizado para el diseño de las redes de datos. En concreto, el modelo utilizado como referencia es el modelo OSI. Además, se incluye una primera comparación con el modelo de la arquitectura de red predominante en la actualidad, como es TCP/IP.

EJERCICIOS PROPUESTOS

1. Aplicar los conceptos que aparecen en la jerarquía por niveles del modelo OSI a una empresa de logística que envía paquetes de todo tipo a cualquier lugar del mundo. Para ello, definir primero las funciones, los niveles y asignar cada función en uno de los niveles definidos. Aplicar en alguno de los niveles definidos el concepto de interfaz y de protocolo. A continuación se sugieren algunos aspectos que se deben tener en cuenta en la definición de las funciones:

- Identificación del destinatario: nombre, dirección, localidad…
- Reglas de tratamiento de los paquetes: frágiles, voluminosos, peligrosos…
- Tipo de embalaje.
- Métodos de comprobación de los destinatarios.
- Etiquetado de paquetes.
- Prioridades.
- Elaboración de rutas de envío.
- Tipos de medios de transporte: camión, coche, avión, barco…
- Elementos físicos: carreteras, calles…

2. Con la ayuda de los diferentes materiales de apoyo como libros, revistas e Internet y el apoyo del profesor, elabore una lista de protocolos y tecnologías utilizados en las redes de datos, indicando la arquitectura de red a la que pertenece y el nivel correspondiente.

TEST DE CONOCIMIENTOS

1 La principal diferencia entre los diferentes tipos de redes telemáticas es:
- a) La velocidad de transmisión, siendo más elevada en las redes LAN que en las WAN.
- b) El número de dispositivos conectados. Las redes LAN tienen limitaciones de varios cientos de dispositivos mientras que las WAN no tienen limitación.
- c) La distancia cubierta. Las redes LAN tienen limitación geográfica y las WAN no.
- d) El tipo de medio de transmisión utilizado. Cable de cobre y coaxial en redes LAN y fibra óptica en redes WAN.

2 Las redes WAN:
- a) Se pueden utilizar para unir redes LAN.
- b) Suelen ser implementadas por los operadores de telecomunicaciones.
- c) Permite la conexión de dispositivos o redes sin límite de distancia.
- d) Todas las respuestas anteriores son correctas.

3 Para que haya comunicación entre dos niveles homónimos en el modelo OSI es necesario que utilicen:
- a) El mismo protocolo.
- b) La misma interfaz.
- c) El mismo lenguaje de programación.
- d) El mismo sistema operativo.

4 Uno de los principales servicios ofrecidos por las redes privadas es:
- a) Comercio electrónico.
- b) Compartir recursos hardware.
- c) Acceso a redes sociales.
- d) Todas las respuestas anteriores son correctas.

5 La información contenida en una cabecera la procesa:
- a) El nivel superior.
- b) El nivel inferior.
- c) El nivel homónimo.
- d) El nivel más alto.

6 El nivel que asegura la transmisión fiable de datos en un enlace simple es:
- a) El nivel físico.
- b) El nivel de enlace.
- c) El nivel de transporte.
- d) El nivel de aplicación.

7 La dirección física de los dispositivos se define:
- a) En el nivel físico.
- b) En el nivel de enlace.
- c) En el nivel de transporte.
- d) En el nivel de sesión.

8 Las direcciones de puerto se definen en el:
- a) Nivel de enlace.
- b) Nivel de red.
- c) Nivel de aplicación.
- d) Nivel de transporte.

9 ¿Cuál de los siguientes niveles no incluye en sus funciones ningún tipo de direccionamiento?
- a) Nivel de enlace.
- b) Nivel de transporte.
- c) Nivel de red.
- d) Nivel de aplicación.

10 La transferencia de ficheros es un servicio proporcionado por el:
a) Nivel de enlace.
b) Nivel de transporte.
c) Nivel de red.
d) Nivel de aplicación.

11 Actualmente, la mayor parte de las redes:
a) Utilizan arquitecturas basadas en el modelo OSI en redes WAN.
b) Utilizan arquitecturas basadas en el modelo OSI en redes LAN.
c) Utilizan la arquitectura TCP/IP.
d) Utilizan la arquitectura TCP/IP y arquitecturas basadas en el modelo OSI conjuntamente.

8 Capa física: medios de transmisión

OBJETIVOS DEL CAPÍTULO

- ✓ Conocer los principales medios de transmisión utilizados en las redes de datos.
- ✓ Entender algunas características básicas relacionadas con el nivel físico como son la codificación, los modos de transmisión y las topologías de red.
- ✓ Conocer la función y las principales características de los sistemas de cableado estructurado como una de las infraestructuras para redes de datos más utilizadas.

En el capítulo anterior planteamos que, para afrontar la complejidad de las redes de datos, era necesario aplicar un modelo de capas que permitiera agrupar en niveles menos complejos las múltiples funciones que es necesario resolver. Utilizando el modelo OSI como referencia, el único nivel en el que se produce el "movimiento" real de la información es en el nivel físico. En este capítulo repasaremos los medios de comunicación utilizados en las redes de datos. También veremos algunos conceptos aplicables a este nivel como la codificacón, señalización y las topologías. Para acabar se repasará la normativa de cableado estructurado utilizada para la implantación de redes locales.

8.1 MEDIOS DE TRANSMISIÓN

Los medios de transmisión son el elemento por el que viajan los datos en las redes. La función proporcionada por los medios de transmisión está englobada en el nivel 1 (nivel físico) del modelo OSI y conocer las características, propiedades y comportamiento de los medios de transmisión disponibles es fundamental para entender el funcionamiento de las redes. Como ya se mencionó en el Capítulo 7 existen dos tipos de medios de transmisión: medios guiados y medios no guiados.

- En los **medios guiados** los datos son transportados a través de un material que canaliza la señal que transporta. Es lo que se conoce habitualmente como medios cableados o simplemente cables. Cuando conectamos dos dispositivos mediante un cable, la información viaja de un dispositivo a otro canalizada en dicho cable. Existen dos tipos de señales que se pueden utilizar para transportar datos a través de un medio guiado: las señales eléctricas y las señales ópticas. Cada uno de estos tipos de señales utiliza un material diferente:
  - **Medios guiados de cobre**. El cobre es el material que se emplea para transportar señales eléctricas. Sin ninguna duda, es el medio actualmente más utilizado en las redes de datos y en general, en cualquier sistema que necesite transportar señales eléctricas. Sus principales propiedades son:
    - Conductividad. El cobre es el mejor conductor de la corriente eléctrica que se conoce.
    - Ductilidad o capacidad para dividirse en finos hilos sin romperse.
    - Maleabilidad o facilidad para darle forma.

    En las redes de datos se utilizan dos tipos de cableado de cobre: el cable de *par trenzado* y el *cable coaxial*.
  - **Medios guiados de fibra óptica**. La fibra óptica es el medio que se emplea para transportar señales ópticas. La fibra óptica es el medio más utilizado en la transmisión de datos a larga distancia. Su funcionamiento está basado en el envío de luz a través de una fina canalización de fibra de vidrio o algún material plástico de similares características.
- En los **medios no guiados** los datos viajan en forma de ondas electromagnéticas utilizando el aire como medio de transmisión. En este caso, los datos se propagan sin estar sujetos a ninguna canalización que guíe la señal. También reciben el nombre de medios inalámbricos. El uso de medios inalámbricos está muy extendido en las telecomunicaciones ya que los principales servicios ofrecidos, como la televisión, radio o telefonía móvil usan medios inalámbricos.

8.1.1 PAR TRENZADO

El **cable de par trenzado** es un tipo de cable de cobre utilizado en los sistemas telefónicos y en la gran mayoría de redes de datos de área local. El elemento básico de un cable de par trenzado es el llamado **par**, formado por dos

hilos o cables de cobre. El par es el elemento necesario para transmitir una señal eléctrica. Los pares están trenzados para proporcionar protección frente a una fuente de interferencias llamada **diafonía** generada por pares adyacentes.

***Figura 8.1**. Cable de par trenzado*

Un cable de par trenzado puede estar formado por uno o varios pares. Por ejemplo, para telefonía se emplea cable de par trenzado con un solo par o con dos pares (dos o cuatro hilos de cobre). El cable de par trenzado más utilizado en redes de área local (LAN) tiene cuatro pares, es decir, ocho hilos de cobre. Existen dos tipos de cable de par trenzado, conocidos por sus siglas en inglés: UTP y STP.

8.1.2 CABLE UTP

El **cable UTP** (*Unshielded Twisted-Pair*) o cable de par trenzado sin apantallar es el medio de transmisión más empleado en redes de área local. La razón principal de su extenso uso es que es el medio cableado más barato para transmitir datos. Es flexible y por tanto sencillo de instalar (otros tipos de cables son más rígidos y, por tanto, más difíciles de manipular), el conector utilizado en este tipo de cable es también barato, es relativamente ligero y de poco diámetro y las velocidades soportadas se ajustan a las necesidades de la mayor parte de las redes.

El cable UTP está formado por cuatro pares trenzados (ocho hilos de cobre), cada uno de los hilos está cubierto por una funda protectora de un color determinado para identificar su función (todo el conjunto está cubierto por otra funda plástica exterior). El conector utilizado en redes de datos con cable UTP se conoce como **conector RJ-45**.

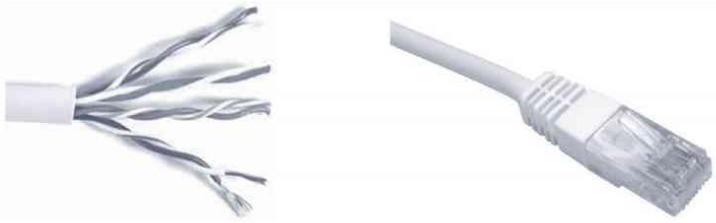


***Figura 8.2**. Cable UTP formado por cuatro pares trenzados y el conector utilizado, el RJ-45*

Por otra parte, el cable UTP presenta dos desventajas, primero que no incorpora ningún elemento para protegerse del ruido eléctrico y las interferencias (como ocurre con otros tipos de cable de cobre como el STP o el cable coaxial), y segundo, que no permite las transmisión de datos para distancias largas (la mayor parte de los estándares que utilizan cable UTP limitan su longitud máxima a 100 metros).

RECUERDA

El cable UTP o par trenzado sin apantallar es el medio de transmisión dominante actualmente en las redes de área local aunque la longitud máxima que se puede cubrir con este tipo de cable es de 100 metros.

Debido al aumento de las prestaciones de las redes de datos a lo largo de los últimos años, la industria de cableado ha tenido que desarrollar cables UTP que ofrecieran cada vez mejores características. Por ello, existen varios tipos de cable UTP conocidos como **categorías**. Se han ido desarrollando nuevas categorías de cable UTP donde el principal objetivo era proporcionar mayor ancho de banda y consecuentemente, mayor velocidad de transmisión. Las primeras categorías de cable UTP, conocidas como Categoría 1 (CAT 1) y Categoría 2 (CAT 2) se consideran extinguidas. En la siguiente tabla aparecen las categorías existentes en la actualidad:

Nombre	Ancho de banda	Velocidad de transmisión	Estado
CAT 3	16 MHz	16 Mbps	Utilizado en las primeras redes locales Ethernet a 10 Mbps. Actualmente ya no se utiliza en redes de datos.
CAT 5	100 MHz	100 Mbps	Utilizado en muchas de redes locales Ethernet aunque actualmente ha sido desplazado por la categoría CAT 5e.
CAT 5e	100 MHz	1.000 Mbps	Utilizado en redes Ethernet tanto a 100 Mbps como a 1 Gbps.
CAT 6	250 MHz	1.000 Mbps	Utilizado principalmente para redes Ethernet a 1 Gbps. Existe una mejora llamada CAT 6e que admite velocidades de 10 Gbps con 500 MHz de ancho de banda.
CAT 7	600 MHz	10 Gbps	Realmente es cable de par trenzado apantallado.

IMPORTANTE

Cuidado con confundir el cable UTP con el cable de par trenzado con uso exclusivo para voz. Suele ser un cable con uno o dos pares y el conector es del tipo RJ-11 con solo cuatro pines (y no ocho como el RJ-45) y lógicamente más estrecho que el RJ-45.

Figura 8.3. *Comparación entre los conectores RJ-11 y RJ-45*

8.1.3 CABLE STP

El **cable STP** (*Shielded Twisted-Pair*), o cable de par trenzado apantallado, es otro tipo de cable de cobre utilizado en las redes de datos aunque su uso en la actualidad es más bien escaso. Al igual que el cable UTP está formado por cuatro pares trenzados y cada par está recubierto de una malla metálica o pantalla cuya función es reducir el efecto de las interferencias. Además, todo el conjunto lleva otra malla o lámina metálica para aumentar su inmunidad frente al ruido eléctrico y las interferencias. Existe además un tipo de cable STP que solo lleva la lámina metálica exterior, es decir, los pares no van apantallados.

***Figura 8.4**. Cable STP*

La inmunidad que presenta este tipo de cable mejora sus prestaciones pero por el contrario proporciona algunos inconvenientes, como mayor coste y mayor dificultad de instalación. Hay que tener en cuenta que el blindaje metálico debe estar conectado a tierra, y si esto no se hace correctamente, el efecto puede ser justo el contrario ya que los blindajes metálicos sin conexión a tierra son muy sensibles a las interferencias.

En la práctica, solo es justificable utilizar cable STP en instalaciones con fuerte nivel de interferencias y lo cierto es que en la actualidad muy pocas instalaciones están preparadas para el uso de cables STP y éste apenas se utiliza.

Una **conexión a tierra**, o una toma de tierra, es un elemento que aparece en prácticamente en todas las instalaciones eléctricas y cuyo principal uso es la protección de los usuarios de los dispositivos eléctricos y electrónicos ante voltajes eléctricos no deseados. La descripción formal de la tierra en una instalación eléctrica es:

Una conexión conductora, ya sea intencional o accidental, por medio de la cual un circuito eléctrico o equipo se conecta a la tierra o a algún cuerpo conductor de dimensiones relativamente grandes que cumpla la función de la tierra.

En la práctica, una conexión a tierra es simplemente una pieza metálica enterrada en el suelo y conectada al llamado cable de tierra. También se puede conectar a las partes metálicas de la estructura del edificio. Además de esta función de protección, la conexión a tierra también proporciona una trayectoria alternativa a las corrientes inducidas y, por tanto, minimiza el ruido eléctrico en los cables, que es el efecto que se busca en los cables STP.

8.1.4 CABLE COAXIAL

El **cable coaxial** es otro medio de transmisión de cobre. Consta de un conductor de cobre en su parte central por donde circula la señal, el cual se encuentra rodeado por un material aislante. Este material está rodeado a su vez por un conductor cilíndrico presentado como una malla de cobre trenzado que hace de masa. El conductor externo está cubierto por una capa de plástico protector. Esta construcción le confiere un elevado ancho de banda y excelente inmunidad al ruido.

***Figura 8.5**. Cable coaxial*

La figura anterior muestra la estructura de un cable coaxial. La velocidad de transmisión de este cable depende de su longitud y en cables de 1 km se pueden obtener velocidades entre 1 y 2 Gbps. Los cables coaxiales solían utilizarse en los troncales del sistema telefónico, pero ahora se les ha reemplazado por fibra óptica. También se utilizó ampliamente para las primeras implementaciones de redes Ethernet. Actualmente, el cable coaxial todavía se utiliza para la televisión por cable y para los tramos locales de algunos tipos de líneas de datos. Los proveedores de acceso a Internet por cable utilizan este tipo de cable para la conexión de sus clientes a la red. Hay varios tipos de cable coaxial, los más conocidos son:

- **RG-8**, conocido como coaxial grueso, con alrededor de 1 cm de diámetro y 50 Ω de impedancia. Este tipo se ha utilizado ampliamente en las redes de área local, aunque actualmente no se usa.
- **RG-58**, conocido como coaxial fino, con un diámetro de 0,5 cm y 50 Ω de impedancia. Al igual que el anterior, se ha utilizado para redes de área local, aunque actualmente no se usa.
- **RG-59**, este tipo de unos 0,6 cm de diámetro y 75 Ω de impedancia se utiliza actualmente en las redes de transmisión de señales de televisión por cable.
- **RG-6**, es un cable de 0,69 cm de grosor y 75 Ω de impedancia. Es el más utilizado actualmente para la conexión a los proovedores de acceso a Internet por cable.

El conector que se utiliza para el cableado coaxial se conoce como **conector BNC**.

***Figura 8.6**. Conector BNC*

Fuera del ámbito de las redes de datos podemos encontrar cable coaxial en aplicaciones relacionadas con el vídeo, tomas de antena de TV y de satélites.

En la actualidad, un uso típico del cable coaxial es en la red de acceso a los proveedores de servicios de televisión y datos por cable, como por ejemplo: Ono, R, Euskaltel, Telecable. En estos casos, el cable que une el punto de acceso a la red del operador con la red interna del usuario (normalmente un *router* o módem de cable) suele ser cable coaxial

Uno de los parámetros que podemos encontrar dentro de las características de los cables de cobre es el diámetro del hilo de cobre. Este diámetro se suele especificar utilizando el sistema americano conocido como **AWG** (*American Wire Gauge*, medición americana de cable). Para indicar el diámetro de un tipo de cable utiliza una numeración relacionada con el diámetro en pulgadas. Los cables de cobre más habituales van desde el tipo AWG 14 (1,6 mm de diámetro) hasta el AWG 24 (0,51 mm de diámetro). Los cables más utilizados en redes de datos suelen estar entre AWG 23 y AWG 24.

8.1.5 FIBRA ÓPTICA

A diferencia de los anteriores medios de transmisión guiados, la fibra óptica utiliza rayos de luz en lugar de señales eléctricas para el envío de datos. Para ello se utiliza en uno de los extremos de la transmisión un elemento que genere luz, con la longitud de onda adecuada, a partir de la información digital que se quiere transmitir. La luz generada en el emisor se canaliza por un cable formado por un material adecuado para guiarla, normalmente fibra de vidrio. En el otro extremo del sistema de transmisión existirá un elemento que convierte la luz en impulsos eléctricos. Por lo tanto, un sistema de transmisión por fibra óptica está formado por tres elementos: *transmisor*, *cable de fibra óptica* y *receptor*.

El cable de fibra óptica está cuidadosamente diseñado para transportar señales de luz. Se trata de un cilindro de pequeña sección flexible, conocido como **núcleo**, con un diámetro del orden de 8 a 125 μm por el que se transmite la luz. Como comparación, el diámetro del cabello humano es del orden de 50 μm. El núcleo está recubierto de un material similar al del propio núcleo pero con un índice de refracción menor a fin de mantener toda la luz en el interior de él. Recibe el nombre de **revestimiento**. A continuación viene una cubierta plástica (normalmente PVC) para proteger el revestimiento e impedir que cualquier rayo de luz del exterior penetre en la fibra.

Figura 8.7. *Cable de fibra óptica*

Entre el revestimiento y la cubierta exterior suele existir otra capa cuya función es dar consistencia y protección contra las sobretensiones. Normalmente, se utiliza Kevlar en forma de hilos que rodean el revestimiento. Dependiendo de las condiciones de uso de la fibra, se pueden añadir cubiertas exteriores para proporcionar rigidez y protección extra al cable de fibra. También existen en el mercado cables que contienen varios haces de fibra óptica, protegidos por una cubierta exterior común, utilizados sobre todo en los enlaces troncales de grandes redes LAN y en las redes WAN.

***Figura 8.8**. Cable de fibra con varios haces*

IMPORTANTE

Algunos datos sobre el elemento transmisor en la fibra óptica: la luz

La luz es un tipo de energía electromagnética que puede desplazarse en forma de onda a través de diferentes medios, como el aire, el vacío o el vidrio. La principal propiedad de la luz (y, en general, de cualquier tipo de onda) es su longitud de onda. La **longitud de onda** se puede definir como la distancia lineal entre dos puntos equivalentes de ondas sucesivas. Se mide en metros y sus múltiplos y submúltiplos. Se suele representar con la letra griega λ (lambda).

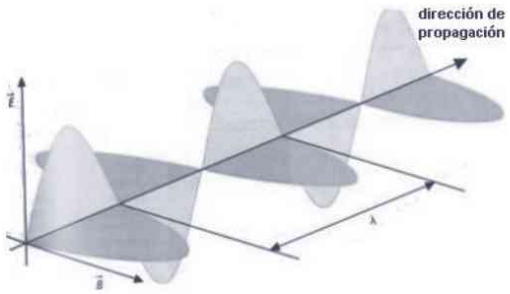


***Figura 8.9**. Longitud de onda*

Dependiendo del rango de la longitud de onda de la luz, ésta recibe diferentes nombres. Por ejemplo, la luz visible son ondas electromagnéticas con una longitud de onda entre unos 400 nm y 700 nm (1 nm equivale a 0,000000001 m o 10^{-9} m). La luz utilizada en las transmisiones con fibra óptica está fuera del alcance de la luz visible. Pertenece al rango denominado **luz infrarroja**. Las longitudes de onda, dentro del rango de la luz infrarroja, que tienen un mejor comportamiento para su transmisión con fibra óptica son tres: 850 nm, 1.310 nm y 1.550 nm.

Normalmente, por un cable de fibra se puede enviar información en un solo sentido, es decir, es una transmisión *símplex*. Para obtener una transmisión *full-dúplex* es necesario utilizar dos cables de fibra óptica. Esta configuración se utiliza mucho en las redes LAN.

***Figura 8.10**. Cable de fibra óptica dúplex*

Los cables de fibra óptica utilizados en las redes telemáticas pueden transmitir la luz de dos formas diferentes:

- **Fibra monomodo**: la luz se propaga en el interior del núcleo siguiendo un solo camino (modo). Para conseguir esta característica es necesario construir el núcleo de un diámetro muy pequeño. En las fibras monomodo el núcleo tiene un diámetro que oscila entre 8 y 10 micras, aunque el valor más habitual es de 9 micras. En estos casos, el diámetro del revestimiento suele ser de 125 micras. En el etiquetado de la fibra suelen aparecer estos dos valores, el diámetro del núcleo y del revestimiento. En el caso de fibras monomodo lo habitual es que estén etiquetadas como 9 µ/125 µ.
- **Fibra multimodo**: la luz se propaga en el interior del núcleo siguiendo varios caminos o modos. Esto se debe a que el diámetro en este tipo de fibras es sensiblemente mayor. Los valores más utilizados son de 50 o 62,5 micras. Para compensar el desfase que se produce en el receptor entre los diferentes modos se utiliza un tipo de fibra de vidrio llamado fibra de vidrio de índice gradual, cuyo índice de refracción va disminuyendo gradualmente desde el núcleo hasta la parte más exterior. El revestimiento en este tipo de fibra también suele ser de 125 micras, por lo que los tipos más habituales de fibras multimodo se suelen etiquetar como 62,5 µ/125 µ ó 50 µ/125 µ.

La fibra óptica es el medio de transmisión que más se utiliza en transmisiones en largas distancias o en transmisiones que requieran un gran flujo de información. Las principales **características de la fibra óptica** como medio de transmisión son:

- ✓ Es el medio de transmisión con **mayor ancho de banda**, por lo que es el medio que más información puede transportar.
- ✓ **Inmunidad frente a perturbaciones electromagnéticas**. Las señales ópticas no se ven afectadas por este tipo de perturbaciones.
- ✓ **Menor atenuación**. Gracias a que la atenuación de la señal óptica es menor que la atenuación de las señales eléctrica por medios de cobre, se pueden cubrir distancias mayores sin utilizar repetidores o regeneradores de señal.
- ✓ Es el medio de transmisión **más adecuado para grandes distancias**, ya que en este caso es más barato que el cobre, es más ligero y resiste mejor elementos medioambientales como el agua.

Emisores y receptores

En la actualidad, lo habitual es que el cableado que conecta los dispositivos de los usuarios finales a una red de datos sea cable de cobre. Sin embargo, en algunas ocasiones, esta infraestructura de cableado de cobre debe conectarse a infraestructura formada por fibra óptica, como puede ser en los troncales de las grandes redes LAN o en los enlaces WAN. Por lo tanto, son necesarios elementos que transformen las señales eléctricas que viajan por el cable de cobre en señales ópticas que viajan por la fibra óptica.

El emisor en un sistema de transmisión de fibra óptica es el elemento encargado de convertir una señal de datos eléctrica a una señal de datos óptica equivalente, apta para ser transmitida por la fibra de vidrio. Existen dos tipos de transmisores:

- **Emisores LED** (*Light Emitting Diodes*, diodos electroluminescentes). Este tipo de transmisor genera luz infrarroja con longitudes de onda de 850 ó 1.310 nm y, por tanto, se utiliza en la fibra multimodo instalada habitualmente en las redes LAN. Son emisores relativamente baratos.
- **Emisores Láser**. Este tipo de transmisor genera luz infrarroja con longitudes de onda de 1310 ó 1.550 nm y, por tanto, se utiliza para fibra monomodo. Además, el láser puede recorrer distancias más largas que la luz generada por los emisores LED, por tanto, es el tipo de transmisor utilizado en los enlaces WAN. Este tipo de conectores son mucho más costosos que los emisores LED.

Por otra parte, los receptores son los elementos encargados de convertir la señal óptica transmitida por la fibra en una señal eléctrica. Para ello se utilizan los llamados **fotodiodos**, que son dispositivos electrónicos sensibles a una longitud de onda concreta y que produce corriente eléctrica cuando llega un pulso de luz.

Tanto los emisores como los receptores de fibra óptica pueden estar incluidos en los dispositivos utilizados dentro de las redes telemáticas como *switches* o *routers*. A continuación se presenta una tabla resumen de las características de los dos tipos de cables de fibra óptica.

Tipo	Diámetro núcleo / revestimiento	Longitud de onda	Tipo de luz	Distancia máxima de cable	Uso
Fibra monomodo	9 µ/125 µ	1.310 nm 1.550 nnm	Láser	más de 10 Km	Redes WAN y troncal de redes LAN
Fibra multimodo	50 µ/125 µ 62,5 µ/125 µ	850 nm 1.310 nm	LED	Unos 2 Km	Redes LAN

Conectores

Existen varios tipos de conectores utilizados para conectar el cable de fibra óptica a los equipos. Los más utilizados en las redes de datos son:

- **Conector ST**. Uno de los conectores de fibra óptica más utilizados en redes LAN aunque en la actualidad se tiende a su sustitución por los conectores SC. Tiene un mecanismo de acople de tipo bayoneta similar a algunos conectores de cable coaxial.

Figura 8.11. *Conector ST*

- **Conector SC**. Este tipo de conector se ha ido imponiendo al conector ST debido a sus mejores prestaciones y facilidad de conexión. Es fácil de identificar por su perfil cuadrado en lugar del perfil circular del ST. Existe una varidad *dúplex* con dos conectores SC unidos.

***Figura 8.12**. Conector SC*

Se puede encontrar una lista completa de conectores usados en fibra óptica en el siguiente enlace: *www.fibraoptica.com/informacion-tecnica/identificacion-de-conectores*

8.1.6 MEDIOS INALÁMBRICOS

Las redes de datos también pueden utilizar medios inalámbricos para transmitir información. Realmente, cuando hablamos de medios inalámbricos nos referimos al aire (aunque también se considera un medio inalámbrico el vacío). En este caso, la información se propaga mediante ondas electromagnéticas sin estar confinadas en ninguna canalización, por ello también se conocen como medios no guiados.

Los medios de transmisión inalámbricos han sido utilizados tradicionalmente en las telecomunicaciones para ofrecer diferentes servicios como televisión, radio, telefonía móvil, etc. En los últimos años se ha producido un auge del uso de este medio para las redes de datos debido a su versatilidad y su bajo coste de instalación en comparación con las redes cableadas.

Al igual que en los rayos de luz en la fibra óptica, el principal parámetro que define las ondas electromagnéticas propagadas por el aire es su **longitud de onda** (λ). Aunque en este caso, tambien se emplea como parámetro característico la **frecuencia** (**f**). La relación entre frecuencia y longitud de onda viene expresada por la siguiente ecuación:

$$v = \lambda \cdot f$$

Donde v es la velocidad de propagación de la onda electromagnética. Es muy frecuente utilizar como referencia de velocidad de propagación la velocidad de la luz en el vacío: $3 \cdot 10^8$ m/s.

El conjunto de todas las posibles longitudes de onda (o frecuencias) constituye el llamado **espectro electromagnético**. Este espectro se divide en bandas en función de la frecuencia. El rango de frecuencias utilizadas en telecomunicaciones va desde los 3 KHz hasta alrededor de los 300 GHz. A este rango se le conoce como **espectro de radiofrecuencia** y abarca las siguientes bandas:

- **Ondas de radio**. Son fáciles de generar, pueden viajar largas distancias, penetran en los edificios sin problemas y viajan en todas direcciones desde la fuente emisora. El rango de frecuencias que cubre va desde las frecuencias más bajas, alrededor de los 10 KHz hasta frecuencias entorno a los 300 MHz. Existen dos tipos de ondas de radio:
  - **Ondas de radio de baja frecuencia**: se caracterizan porque en su recorrido siguen la curvatura de la Tierra y pueden atravesar con facilidad los edificios. Sin embargo, su ancho de banda solo permite velocidades de transmisión bajas.
  - **Ondas de radio de alta frecuencia**: estas ondas tienden a ser absorbidas por la Tierra, por lo que deben ser enviadas a la ionosfera, donde son reflejadas y devueltas de nuevo, con lo que se consigue transmitir a largas distancias.
- **Microondas**. Además de su aplicación en hornos, las microondas permiten transmisiones tanto terrestres como con satélites. Sus frecuencias están comprendidas entre 300 MHz y 300 GHz. A diferencia de las ondas de radio, las microondas no atraviesan bien los obstáculos, de forma que es necesario situar antenas repetidoras cuando queremos realizar comunicaciones a largas distancias. En el caso de las comunicaciones por satélite, hay que tener en cuenta que siempre existe un pequeño retardo en las transmisiones debido a que la señal tarda aproximadamente 0,3 segundos en llegar y volver. Para algunas aplicaciones de envío y recepción de datos, este tiempo de espera puede resultar inaceptable.
- **Ondas infrarrojas**. Este tipo de ondas se utiliza para la comunicación de corto alcance, en controles remotos de televisores, y en general de dispositivos electrónicos. También es posible encontrar un puerto de comunicación infrarroja en los ordenadores portátiles. Estos controles son relativamente direccionales, baratos y fáciles de construir, pero tienen un inconveniente importante: no atraviesan los objetos sólidos. Este inconveniente también resulta a veces una ventaja en el sentido de que ofrecen más seguridad, precisamente porque la comunicación no atraviesa las paredes de un edificio. Además, el uso de frecuencias en la banda de los infrarrojos no está regulado por las administraciones comno ocurre con otras bandas de frecuencia.

La mayor parte de las comunicaciones inalámbricas en las redes de datos se llevan a cabo en la banda de las microondas.

El uso del espacio radioeléctrico está regulado por las administraciones de los diferentes países. En la página web del Ministerio de Industria, Turismo y Comercio se puede obtener la asignación de frecuencias del espectro radioeléctrico en España:
www.mityc.es/telecomunicaciones/Espectro/Paginas/CNAF.aspx

8.1.7 USO DE LOS MEDIOS DE TRANSMISIÓN EN LAS REDES DE DATOS

En los apartados anteriores se ha dado un repaso a los diferentes medios de transmisión existentes. En este apartado se ofrece una síntesis de cómo y dónde se usan estos medios de transmisión dentro de las redes de datos más comunes en la actualidad. Recordemos que podemos establecer dos grandes tipos, las redes LAN y las redes WAN.

Empecemos con las redes LAN. En este ámbito, la gran mayoría de redes están constituidas por alguno de estos medios de comunicación:

- **Cable de par trenzado**. La inmensa mayoría de las redes LAN cableadas actuales utilizan cable UTP. La tendencia es utilizar cable UTP de categoría 5e ó 6 aunque podemos encontrar aún muchas redes funcionando con cables UTP de categoría 5. La categoría 3 prácticamente ha desaparecido y la categoría 7 aún no está muy extendida.

- **Fibra óptica**. La fibra óptica se encuentra con frecuencia en las redes LAN formando parte de lo que se conoce como el troncal de la red, que es la parte de la red local que soporta mayor volumen de información. Además, es necesario utilizar fibra cuando la distancia es mayor de 100 metros. Habitualmente, se utiliza fibra multimodo ya que las distancias a cubrir no son excesivamente grandes y este tipo de fibra es más barata que la fibra monomodo.

- **Medio inalámbrico utilizando señales electromagnéticas en el rango de las microondas**. El estándar actual para establecer redes LAN inalámbricas es Wi-Fi, cada vez más utilizado tanto en entornos domésticos como profesionales. Su punto fuerte es la flexibilidad y facilidad de instalación ya que no requiere cableado. Las desventajas son la potencial falta de seguridad respecto a las redes cableadas y unas menores prestaciones respecto a éstas.

El uso de cable STP o cable coaxial en las redes LAN hoy en día es prácticamente inexistente.

Para redes WAN sin duda el medio de transmisión más utilizado en la actualidad es la **fibra óptica**, aunque, como veremos más adelante, en una de las partes de las redes WAN que es la conexión del usuario final a la red WAN (que se suele denominar *red de acceso*) se utilizan otras opciones:

- **Par trenzado telefónico**. Usado por los proveedores de acceso a Internet (ISP) a través del par telefónico. Habitualmente usando tecnologías de banda ancha xDSL.

- **Cable coaxial**. Usado para proporcionar acceso a Internet por los operadores de cable.

- **Enlaces inalámbricos WiMAX**. Proporciona una conexión inalámbrica entre un abonado y un proveedor de servicio de datos.

- **Satélite**. También basado en el uso de tecnologías inalámbricas, habitualmente en el rango de las microondas.

- **Telefonía móvil**. La mayor parte de los operadores de telefonía móvil también proporcionan acceso a Internet mediante las redes inalámbricas de telefonía móvil utilizando GSM ó 3G.

8.2 OTRAS CARACTERÍSTICAS DEL NIVEL FÍSICO

8.2.1 SEÑALIZACIÓN Y CODIFICACIÓN

La información que se transmite en las redes de datos es información digital. Esto significa que toda la información transmitida se representa utilizando solo dos estados, llamados 1 y 0. Esta información digital se puede representar utilizando señales eléctricas. La relación que se establece entre información digital y señales eléctricas puede llegar a ser muy intuitiva, ya que puede consistir en asignar un voltaje eléctrico al estado 1, y otro voltaje eléctrico al estado 0. A cada uno de estos estados se le conoce como bit. De esta forma podemos obtener una señal eléctrica que representa información digital, como se observa en la siguiente figura.

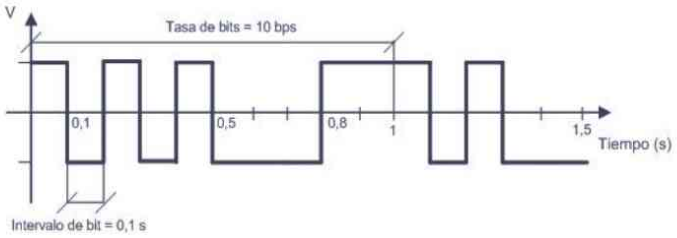


Figura 8.13. *Representación gráfica de una señal digital*

En la figura anterior uno de los estados se representa con un valor positivo de tensión eléctrica y el otro estado se representa con un valor negativo. Los parámetros característicos de una señal digital son:

- **Intervalo de bit**. Es el tiempo necesario para transmitir un bit. Se mide en segundos o submúltiplos.
- **Tasa de bits**. Es el número de bits transmitidos en un segundo. Este parámetro da una idea de la velocidad con la que se transmiten los datos, por ello la tasa de bits también se conoce como **velocidad de transmisión**. Se mide en bits por segundo (bps) o múltiplos como Kbps, Mbps…

Al proceso de representar información digital (unos y ceros) en señales eléctricas se le conoce como *señalización* o *codificación*. La **codificación**, por tanto, sería la representación de la información digital mediante una señal digital. Básicamente consiste en traducir los ceros y unos binarios que se desea transmitir a una secuencia de pulsos de voltaje, adecuada para su transmisión.

Uno de los entornos más propicios para codificar la información digital es en las redes locales cableadas. Sin embargo, no siempre se puede aprovechar la simplicidad de codificar la información en una señal eléctrica digital. Esto solo es posible cuando las condiciones de transmisión lo permitan. Por ejemplo, las transmisiones inalámbricas necesitan transportar la señal que se desea transmitir a una frecuencia determinada. En este caso no se puede utilizar la codificación.

Tampoco se puede utilizar la codificación cuando hace falta aplicar técnicas analógicas para transmistir las señales eléctricas. Por ejemplo, la tecnología ADSL lleva a cabo técnicas analógicas, como la modulación, para obtener al máximo rendimiento de la línea.

Existen muchos tipos de codificaciones, algunos ejemplos serían:

- **Codificación unipolar**. Es el tipo de codificación más sencilla y primitiva y que, actualmente, se considera obsoleta. Su principal ventaja es su sencillez. Para codificar información digital (ceros y unos) mediante esta técnica, se asigna a cada nivel lógico un nivel de voltaje usando únicamente una polaridad. Por ejemplo, los "unos" se codifican con un valor de voltaje positivo y los "ceros" se codifican con el valor de voltaje cero.

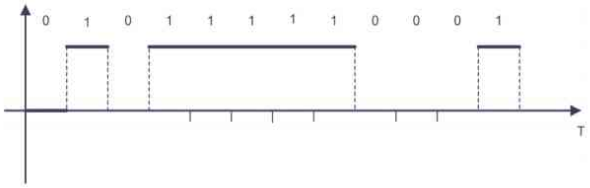


***Figura 8.14**. Codificación unipolar*

- **Codificación NRZ-I**. Este tipo de codificación utiliza dos niveles de voltaje con diferente polaridad. El nivel lógico 1 se representa con una inversión del nivel de voltaje, y un nivel lógico 0 se representa sin ningún cambio de polaridad. En la siguiente figura se muestra un ejemplo de codificación NRZ-I.

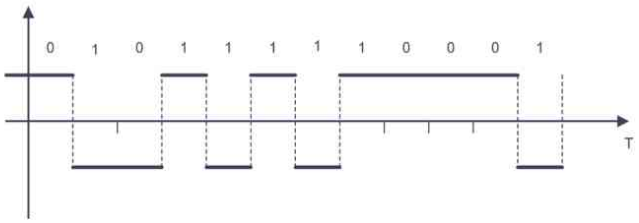


***Figura 8.15**. Codificación NRZ-L*

- **Codificación Manchester**. También conocida como codificación bifásica. También se utilizan dos niveles de voltaje con diferente polaridad, pero en este caso se usa una inversión de la polaridad de la señal en mitad de cada intervalo de bit. El sentido de la inversión es el que indica el valor del bit codificado. Una transición de negativo a positivo representa un 1 binario y una transición de positivo a negativo representa un 0 binario. En el ejemplo siguiente se puede apreciar este funcionamiento.

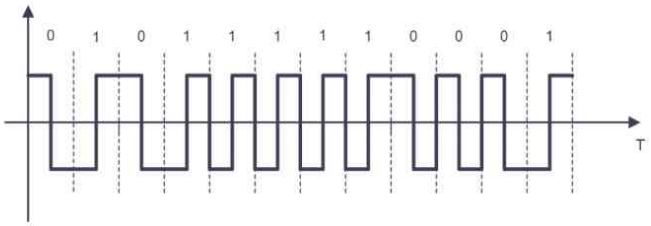


***Figura 8.16**. Codificación Manchester*

8.2.2 MODOS DE TRANSMISIÓN

El intercambio de información entre dos dispositivos conectados mediante un medio de transmisión se puede hacer de varias formas en función de la dirección del flujo de las señales enviadas entre los dos dispositivos enlazados, lo que se conoce como **modos de transmisión**:

- **Símplex**: cuando se establece una comunicación unidireccional entre los dos dispositivos. Un dispositivo solo recibe y el otro solo envía. Un ejemplo de comunicación símplex podría ser la radio o la televisión.
- **Half-dúplex o semidúplex**: cada dispositivo puede enviar y recibir datos pero no al mismo tiempo. Cuando un dispositivo envía, el otro solo puede recibir y viceversa. Un ejemplo de este tipo de comunicación son los *walkie talkies*.
- **Full-dúplex o dúplex**: cuando los dos dispositivos que llevan a cabo la comunicación pueden enviar y recibir de forma simultánea. Para ello debe haber dos caminos físicos diferentes o se tiene que dividir la capacidad del enlace en dos canales. Un ejemplo de comunicación *dúplex* es la que se lleva a cabo en un ordenador conectado a una LAN.

Existen dos forman de conectar los dispositivos de una red a un enlace. El enlace es el medio físico por el que se transfieren los datos. A este concepto se le conoce como **configuración de línea**.

- **Punto a punto**. La conexión recibe este nombre cuando existe un enlace dedicado entre dos dispositivos. Toda la capacidad del enlace se reserva para la transmisión entre ambos dispositivos. También se conoce como *conexión dedicada*. Esta configuración es la más habitual en las redes cableadas actuales.

***Figura 8.17**. Enlace punto a punto*

- **Multipunto**. La conexión recibe este nombre cuando varios dispositivos comparten el mismo enlace. En esta configuración, la capacidad del enlace está compartida en el espacio o en el tiempo. Esta configuración se puede utilizar sobre todo en redes inalámbricas. La tecnología de redes LAN cableadas conocida como Ethernet, que se estudiará en el Capítulo 9, hace uso de la configuración multipunto en sus primeras versiones. Hoy en día prácticamente está en desuso.

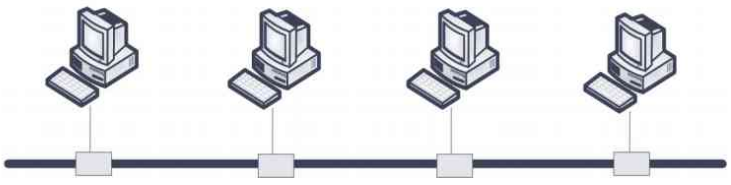


***Figura 8.18**. Enlace multipunto*

8.2.3 TOPOLOGÍAS DE RED

En el contexto de las redes de datos, la topología se refiere a la forma en que está diseñada la red, bien físicamente o bien lógicamente. Dos o más dispositivos se conectan a un enlace. Dos o más enlaces forman una topología. Por tanto, en función de cómo estén conectados los diferentes dispositivos que forman una red existen varias topologías:

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

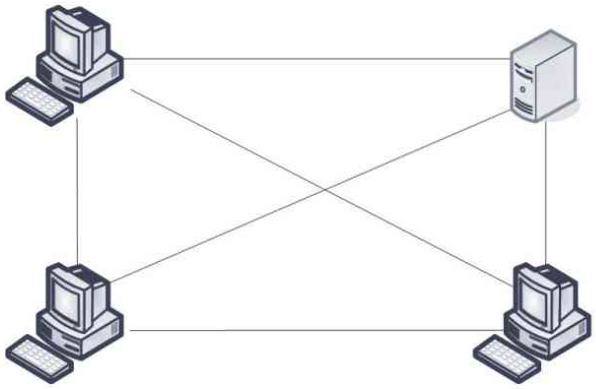


***Figura 8.19**. Topología en malla*

Aunque esta topología es la más eficiente en cuanto 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.

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

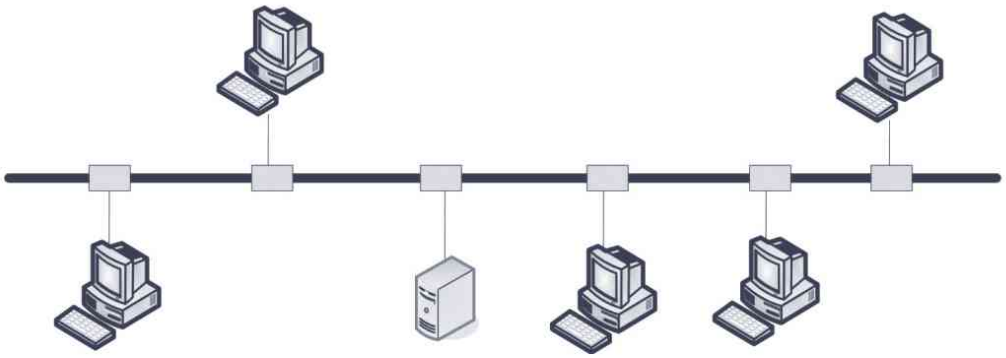


***Figura 8.20**. Topología en bus*

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

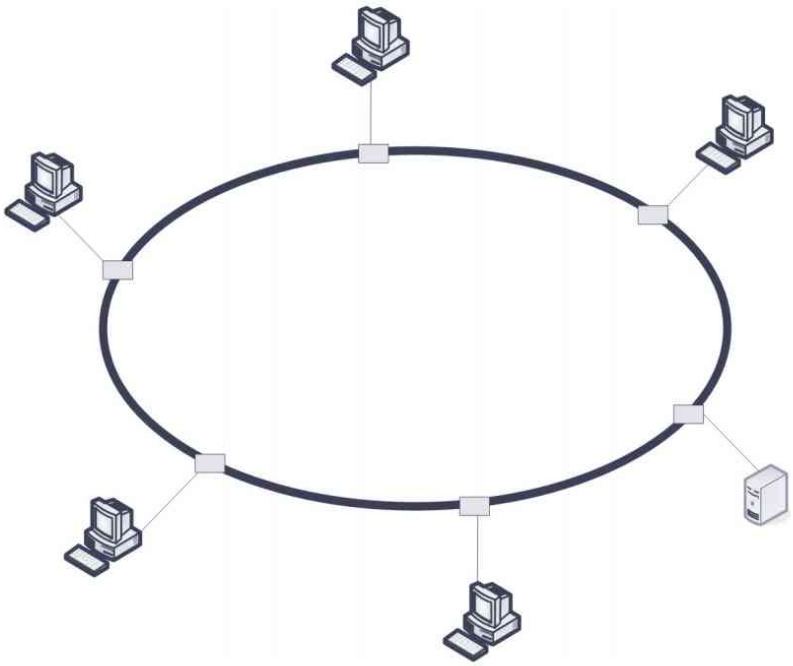


***Figura 8.21**. Topología en anillo*

- **Estrella**. En este caso, cada dispositivo solamente tiene un enlace dedicado con el controlador central, llamado *concentrador*.

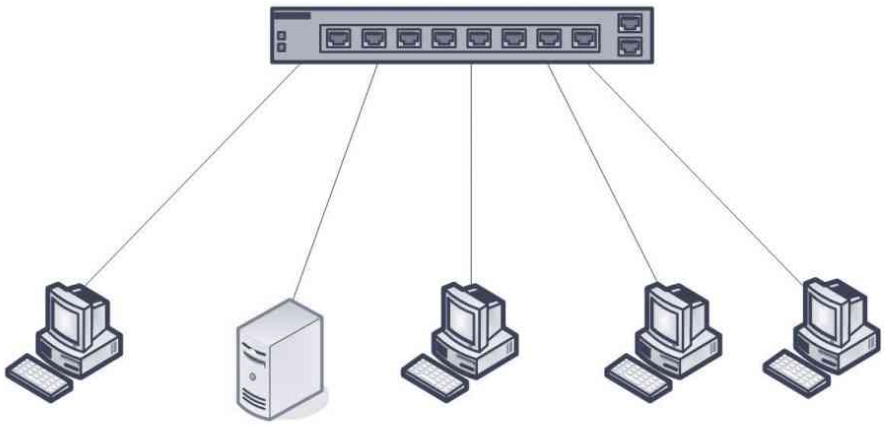


***Figura 8.22**. Topología en estrella*

- **Árbol**. Esta topología es una variante de la topología en estrella.

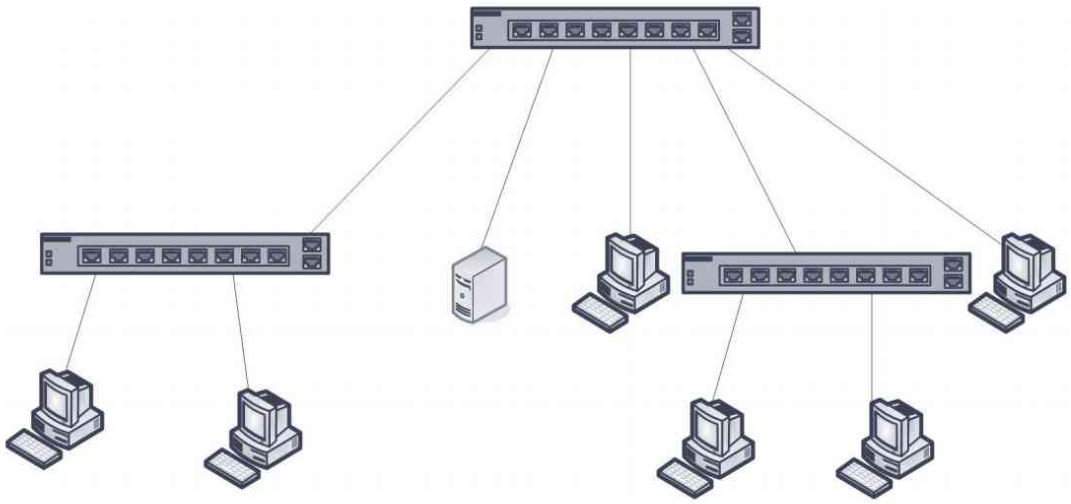


***Figura 8.23**. Topología en árbol*

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

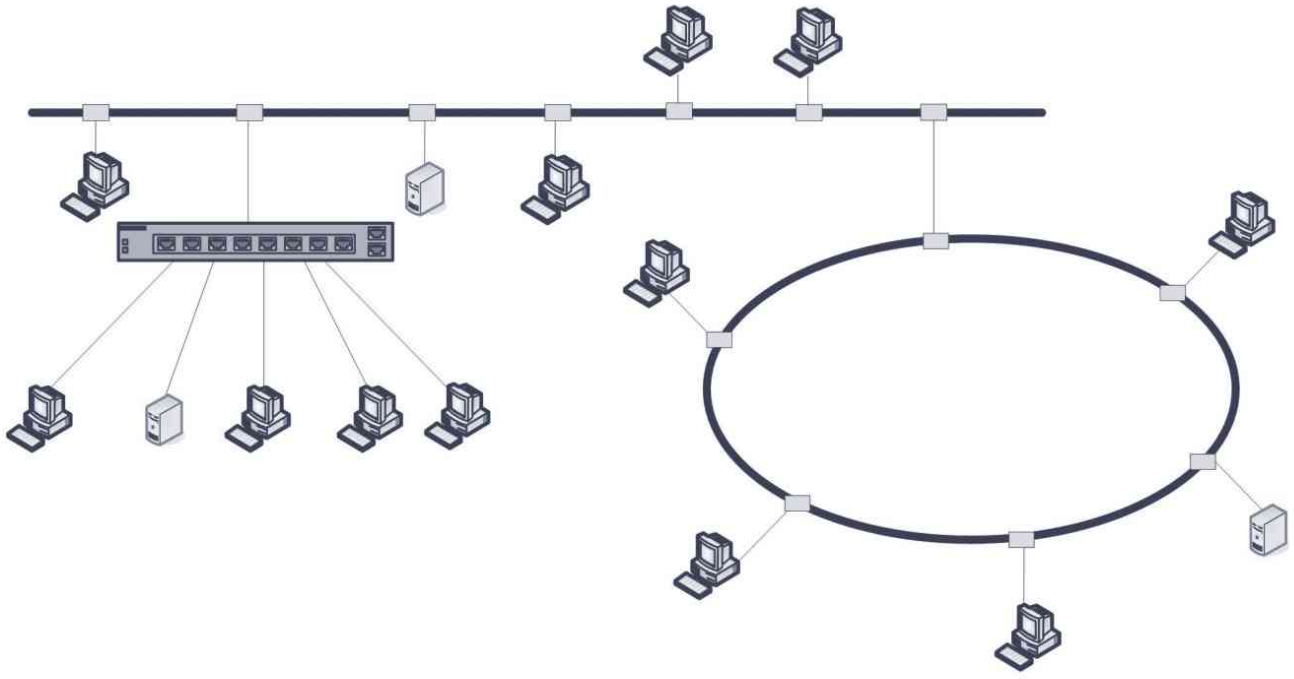


***Figura 8.24**. Topología híbrida*

8.3 CABLEADO ESTRUCTURADO

8.3.1 ESTÁNDARES DE CABLEADO ESTRUCTURADO

Cuando el número de equipos que se quieren conectar en una red es alto y estos equipos están ubicados en edificios de oficinas con varias plantas y/o estancias, es necesario estructurar adecuadamente la instalación del cableado que formará la red de área local. Afortunadamente, existen estándares que proporcionan las pautas e indicaciones adecuadas y que facilitan enormemente la instalación y el mantenimiento de las redes locales, estos estándares se conocen como **estándares de cableado estructurado**.

El principal estándar de cableado estructurado lo ha desarrollado el organismo de estandarización norteamericano llamado **TIA** (*Telecommunication Industry Association*) y, por tanto, su ámbito de aplicación es en la región de Norteamérica. Dicho estándar es el **TIA/EIA-568-A** y fue publicado en 1995. Posteriormente, en 2001, se llevó a cabo una revisión del mismo, publicada como **TIA/EIA-568-B**. Este estándar se conoce como **Norma de cableado de telecomunicaciones para edificios comerciales** (*Commercial Building Telecommunication Cabling Standard*).

Debido al éxito de este estándar, otros organismos de estandarización lo han adoptado prácticamente sin cambios. Así, el equivalente estándar utilizado en Europa es el **EN 50173** publicado por el CENELEC, organismo de estandarización europeo. Así mismo, y con un ámbito de aplicación mundial, se publicó el estándar **ISO/IEC 11801**, publicado por el ISO.

IMPORTANTE

AENOR ha publicado el equivalente a la norma europea EN 50173 con el código **UNE-EN 50173**. Esta norma es de obligado cumplimiento para la instalación de redes de datos en la mayor parte de las administraciones públicas.

Existen algunas pequeñas diferencias entre los estándares TIA/EIA e ISO/IEC, aunque se pueden considerar compatibles. Habitualmente se utiliza como referencia por parte de la industria (fabricantes, instaladores…) el estándar TIA/EIA-568-B por ser el más restrictivo.

Un estándar de cableado estructurado contiene un conjunto de normas para el diseño y la implementación de la infraestructura de cableado, de forma que facilite el uso de la mayor cantidad posible de servicios de telecomunicaciones. El objetivo del estándar es proporcionar una infraestructura de telecomunicaciones altamente adaptable a los cambios, es decir, escalable.

Los sistemas de cableado estructurado definen aspectos que forman parte del nivel físico del modelo OSI, como son tipos de medios de transmisión, conectores, distancias, topología, etc. Lógicamente, su principal uso es como infraestructura para redes locales de datos.

8.3.2 PRINCIPALES CARACTERÍSTICAS

El estándar original EIA/TIA-568 se diseñó para proporcionar una infraestructura válida para instalaciones de hasta 3 Km de longitud máxima, 1.000.000 m^2 de supercifie de trabajo y hasta 50.000 usuarios. Por lo tanto, las normas de cableado estructurado cubren un amplio abanico de diferentes requisitos ya que también se pueden utilizar de forma eficiente para redes más pequeñas con unos pocos de cientos de usuarios.

Otros de los aspectos que se persigue en la norma es que la infraestructura de cableado que siga el estándar sea válido un período mínimo de 10 años. Esto significa que el sistema de cableado estructurado debería ser capaz de soportar todos los servicios de comunicaciones necesarios durante ese período de tiempo y además puede afrontar de forma sencilla posibles ampliaciones del número de usuarios.

El sistema de cableado estructurado está ideado para que sea independiente de la aplicación, es decir, que dé soporte a cualquier tipo de comunicación de datos, por tanto, no solo se puede utilizar para redes locales, sino que dicha infaestructura es válida para cualquier sistema que requiera la transmisión de datos, como pueden ser sistemas de telecontrol y de televigilancia.

Por último, hay que destacar que una de las principales ventajas de los sistemas de cableado estructurado es su gran flexibilidad, ya que permite una gran movilidad de los puestos de trabajo sin apenas esfuerzo. Esto supone un importante ahorro en los costes de mantenimiento de las redes.

8.3.3 ARQUITECTURA Y SUBSISTEMAS

Para proporcionar un alto índice de flexibilidad, los sistemas de cableado estructurado están basados en el desarrollo de una estructura jerárquica formada por niveles de jerarquía conocidos como subsistemas. Se puede encontrar hasta tres niveles jerárquicos o subsistemas, subsistemas de campus, subsistema vertical y subsistema horizontal. En la siguiente figura se puede observar la estructura física del sistema de cableado y la ubicación de cada uno de los subsistemas.

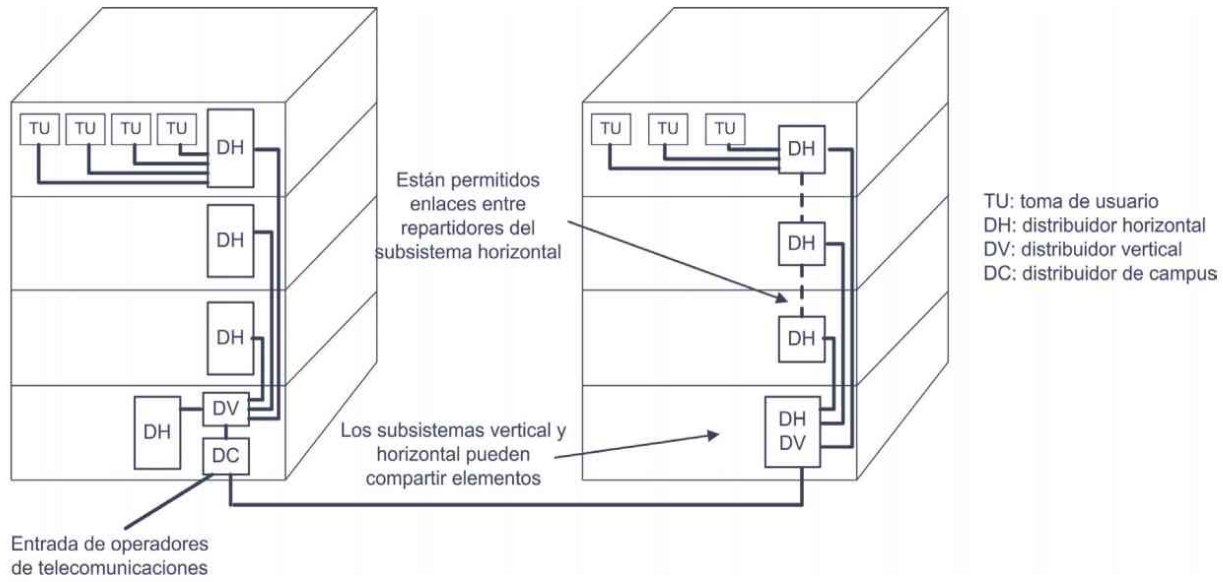


***Figura 8.25**. Estructura física de un sistema de cableado estructurado*

Los elementos que pueden existir en un sistema de cableado estructurado son los siguientes:

- **Repartidor o distribuidor de campus**. Es el elemento del sistema desde donde se distribuye el cableado que forma parte del subsistema de campus. Solo puede haber uno.
- **Cableado troncal de campus o backbone de campus**. Como su nombre indica, es el cableado que forma parte del subsistema de campus. Se utiliza para unir los diferentes edificios que forman parte de la infraestructura.
- **Distribuidor vertical o de edificio**. Es el elemento del sistema desde donde se distribuye el cableado que forma parte del subsistema vertical. Habrá un distribuidor vertical por cada edificio que forma parte del sistema.
- **Cableado troncal de edificio, vertical o backbone de edificio**. Es el cableado que forma parte del subsistema vertical. Su función es interconectar los diferentes subsistemas horizontales.
- **Distribuidor horizontal o de planta**. Es el elemento del sistema desde donde se distribuye el cableado que forma parte del subsistema horizontal. Habrá un distribuidor horizontal por cada planta del edificio.
- **Cableado horizontal**. Es el cableado que forma parte del subsistema horizontal y se encarga de conectar los puestos de trabajo al sistema de cableado.
- **Toma de usuario, toma de telecomunicaciones o toma de área de trabajo**. Es el punto de unión del equipo de usuario con el sistema de cableado estructurado. Se ubican en las áreas de trabajo.
- **Punto de transición (opcional)**. Punto de interconexión intermedio utilizado en alguna conexión horizontal que debe cubrir demasiada longitud. No es muy frecuente su uso.

Otros elementos:

- **Punto de demarcación (demarc) o acometida exterior**. Es el punto del sistema donde se conectan las líneas externas a la infraestructura de cableado y que proporcionan las comunicaciones con el exterior.
- **Sala de equipos o sala de telecomunicaciones**. Es el espacio donde se encuentran los equipos de interconexión que forman parte del sistema de cableado así como otros equipos que formen parte de la infraestructura de comunicaciones, como *routers*, servidores, etc.

En la siguiente figura se puede observar la estructura lógica de un sistema de cableado estructurado donde se puede apreciar como sigue una estructura jerárquica en estrella.

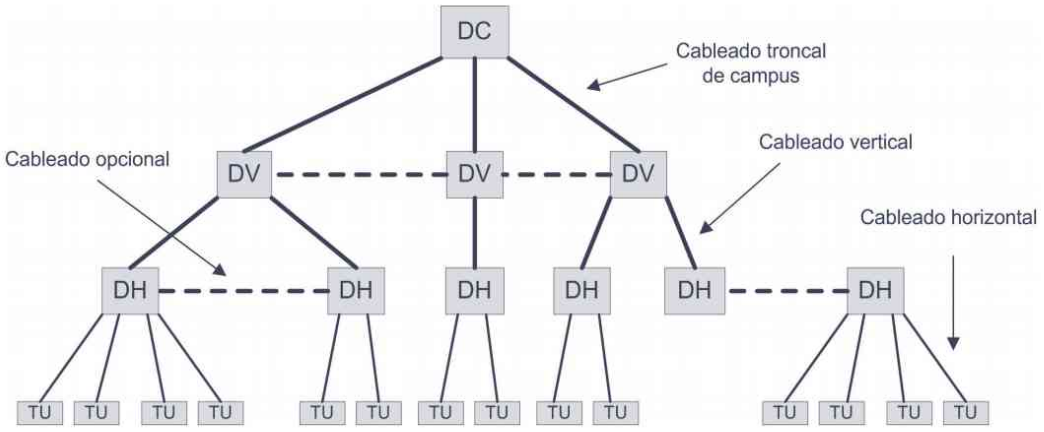


***Figura 8.26**. Estructura lógica de un sistema de cableado estructurado*

Subsistema de distribución de campus

El subsistema de distribución de campus es la parte del sistema de cableado estructurado utilizado en la unión de diferentes edificios. Normalmente, es el subsistema que cubre mayores distancias. Los medios de transmisión utilizados son la fibra óptica y los radioenlaces. Está formado por el distribuidor de campus, que estará situado en uno de los edificios, y el cableado troncal de campus. Lógicamente, este subsistema solo se implementará en los sistemas que necesiten conectar más de un edificio.

Subsistema de distribución vertical

El subsistema de distribución vertical también conocido como backbone se encarga de suministrar la interconexión entre los diferentes subsistemas horizontales. Habitualmente el cableado que forma parte del subsistema vertical recorre el edificio en sentido vertical, de ahí su nombre. Está formado por el distribuidor vertical y el cableado vertical. Sus principales características son:

- ✓ Como medio de transmisión se utiliza fibra óptica o cable de par trenzado.
- ✓ Se permiten conexiones entre dos subsistemas horizontales directamente. Dichas conexiones se consideran que forman parte del cableado vertical.
- ✓ La distancia máxima entre el distribuidor de campus y el distribuidor vertical es de 2.000 metros.
- ✓ La distancia máxima entre el distribuidor vertical y el horizontal es de 500 metros.

Subsistema de distribución horizontal

El subsistema de distribución horizontal es la parte del sistema de cableado estructurado que suministra la conectividad a los puestos de trabajo en las diferentes áreas de trabajo que cubre dicho sistema. Frecuentemente, el área cubierta por un subsistema de distribución horizontal es una planta del edificio donde está ubicada la instalación. Todo el cableado que forma parte de este subsistema está en una misma planta de la instalación, de ahí su nombre. Los elementos que forman parte del subsistema:

- **Cableado horizontal**. El cableado que forma parte de este subsistema es el cableado que va desde el distribuidor horizontal hasta la toma de usuario en el área de trabajo. Normalmente, el tendido de este cable se hace por falsos suelos y techos o por canaletas.
- **Latiguillos**. Además del cableado horizontal propiamente dicho, hay que incluir un cable de unión entre el distribuidor horizontal y la electrónica de red, y otro cable de unión entre la toma de usuario y el equipo. Estos cables de unión se conocen como *latiguillos*. Un latiguillo es un cable UTP con un conector RJ-45 en cada uno de sus extremos.

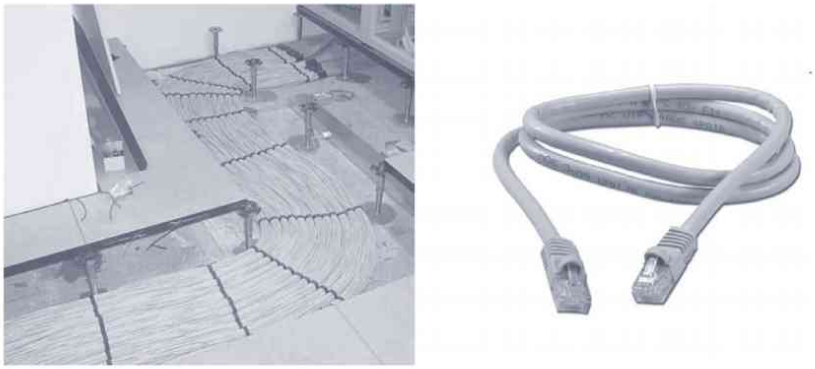


***Figura 8.27**. Cableado horizontal en un falso suelo y un típico latiguillo de red*

- **Rosetas**. Con este nombre se conoce al elemento que hace las funciones de toma de usuario. Una roseta es un conector hembra RJ-45 y, por tanto, en una roseta se conectará un latiguillo para unir el equipo del usuario a la red.

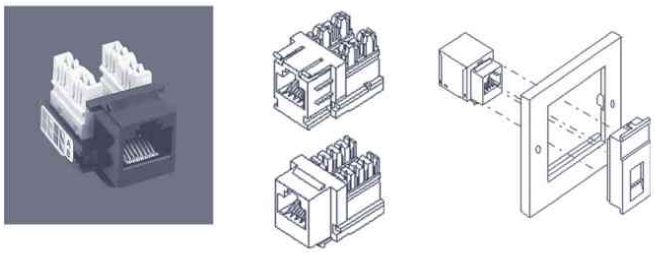


***Figura 8.28**. Roseta*

- **Patch Panel**. Son los elementos que hacen la función de distribuidor horizontal ya que es donde va conectado el cableado horizontal que llega de cada uno de los puestos de trabajo. Los *patch panel* (o paneles de parcheo) van montados en armarios de comunicaciones especialmente diseñados para alojar este tipo de elementos junto con otros auxiliares.

***Figura 8.29**. Patch panel de 24 puertos*

- **Electrónica de red**. Son los dispositivos electrónicos que proporcionan las funciones de red propiamente dichas. Actualmente esta función la proporcionan los dispositivos conocidos como *switches*. Dichos dispositivos no forman parte del sistema de cableado propiamente dicho.

***Figura 8.30**. Partes que componen el subsistema horizontal*

Las características más destacadas de este subsistema son:

- ✓ La distancia máxima que pude cubrir el cableado horizontal es de 90 metros.
- ✓ La suma de las longitudes de los lantiguillos de cada punto de interconexión no debe ser superior a 10 metros.
- ✓ El tipo de cable de cobre utilizado es UTP de categoría 5e ó 6. La norma también permite utilizar cable STP si las condiciones lo requieren.
- ✓ Cada puesto de trabajo debe tener dos tomas de usuario para prevenir ampliaciones del sistema y futuros nuevos servicios.

8.3.4 INSTALACIÓN Y CERTIFICACIÓN

La instalación de un sistema de cableado estrcuturado requiere de una adecuada planificación y el conocimiento de los espacios físicos donde se va a ubicar. En este apartado se ofrecen algunas nociones básicas referidas, sobre todo a la parte del subsistema horizontal, que es la parte del sistema de cableado estructurado que mejor conviene conocer.

En el apartado anterior ya se hablaba sobre los armarios de comunicaciones, que son los espacios donde estará ubicado el distribuidor horizontal junto con la electrónica de red. Existen en el mercado multitud de modelos de armarios de comunicaciones, los más usados son los armarios de 19" de cuerpo entero y los armarios murales de 19" utilizados en pequeñas instalaciones o en instalaciones auxiliares.

***Figura 8.31**. Armarios de comunicaciones para alojar los sistemas de distribución y la electrónica de red*

Las herramientas más utilizadas en la instalación del sistema de cableado estructurado son:

- **Crimpadora**. También se puede encontrar bibliografía que la denomina *grimpadora*. Esta herramienta se utiliza para unir un conector RJ-45 con un cable UTP.
- **Herramienta de impacto o de inserción**. Utilizada para conectar el cableado UTP al *patch panel* por la parte posterior del mismo.

***Figura 8.32**. Herramienta de inserción y crimpadora*

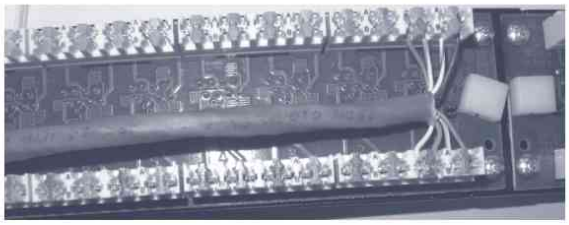


***Figura 8.33**. Detalle de un cable UTP crimpado en un patch panel*

- **Téster de red**. Dispostivo formado por dos unidades que se utilizan para comprobar que no haya ningún par del cableado que no tenga conectividad. Una unidad se conecta en un extremo del cable y la otra unidad al otro extremo. Normalmente, la comprobación se hace mediante algún sencillo sistema de luces indicadoras.

***Figura 8.34**. Tester de red*

Hay fabricantes de dispositivos electrónicos que han desarrollado herramientas para comprobar que una instalación cumple con los parámetros exigidos en las normas de cableado estructurado. Estas herramientas se conocen como **certificadores de cableado** y lo cierto que en la actualidad son dispositivos electrónico, con funciones muy potentes. Una instalación de cableado que ha sido comprobada por un dispositivo de este tipo se dice que es una instalación certificada, esto significa que se ha comprobado que la conexión de todas las tomas de usuario al sistema de cableado cumple los requisitos exigidos por las normas de cableado estructurado.

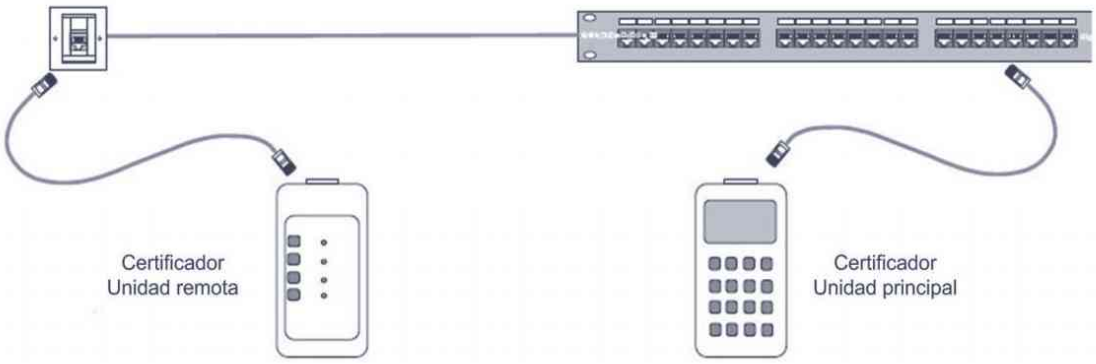


***Figura 8.35**. Certificador de cableado*

RESUMEN DEL CAPÍTULO

Este capítulo incluye un repaso de los diferentes medios de transmisión existentes, como son el cable de par trenzado, el cable coaxial, el cable de fibra óptica, los medios inalámbricos y el uso que de ellos se hace en las redes de datos.

Así mismo, se proporciona información sobre algunos conceptos de interés referentes al nivel físico como son la codificación, los modos de transmisión y las topologías de red.

En la parte final del capítulo se habla de las principales características de los sistemas de cableado estructurado, utilizados como infraestructura para muchas redes locales instaladas en la actualidad.

EJERCICIOS PROPUESTOS

- **1.** Buscar información sobre los medios de transmisión utilizados por las tecnologías LAN y WAN utilizadas en la actualidad.
- **2.** Buscar en catálogos y páginas web de fabricantes de cableado las principales características de cableado comercial, tanto de cobre como de fibra óptica. Obtener información de los precios.
- **3.** Buscar información en catálogos y páginas web de fabricantes, sobre los diferentes elementos relacionados con las instalaciones cableado estructurado vistos en esta unidad, como *pach panel*, armarios de comunicaciones, canaletas, bandejas… Así mismo, obtener información sobre el precio de estos elementos.

TEST DE CONOCIMIENTOS

1 ¿Qué topología utiliza un elemento central llamado concentrador?
- a) *Bus*.
- b) Anillo.
- c) Estrella.
- d) Malla.

2 La mayor parte de la comunicaciones inalámbricas en los sistemas telemáticos utilizan:
- a) Ondas de radio de baja frecuencia.
- b) Ondas de radio de alta frecuencia.
- c) Microondas.
- d) Ondas infrarrojas.

3 La principal diferencia entre las categorias de cable de cobre existentes es:
- a) El tipo de conector utilizado: RJ-11, RJ-45…
- b) La distancia máxima que pueden cubrir.
- c) El tipo de red en el que se pueden utilizar.
- d) El ancho de banda y, por tanto, la velocidad de transmisión.

4 El tipo de medio de transmisión más empleado en las redes LAN es:
- a) Exclusivamente cable de par trenzado UTP.
- b) Principalmente cable de par trenzado UTP y cable coaxial para la parte troncal.
- c) Cable de par trezado, tanto UTP como STP.
- d) Principalmente cable de par trenzado UTP, aunque también es posible utilizar fibra óptica.

5 ¿Qué elemento se utiliza en la fibra óptica monomodo para transmitir?
- a) Emisores LED.
- b) Emisores Láser.
- c) Fotodiodos.
- d) Fotorresistencias.

6 La topología física que no requiere ningún dispositivo controlador central es:
- a) Anillo.
- b) Malla.
- c) *Bus*.
- d) Todas las respuestas anteriores son correctas.

7 El cable de cobre UTP utilizado en redes locales está formado por:
- a) Un par.
- b) Dos pares.
- c) Tres pares.
- d) Cuatro pares.

8 Los medios no guiados se utilizan especialmente:
- a) En redes LAN.
- b) En la red de acceso de las redes WAN.
- c) En la red de transporte de las redes WAN.
- d) Tanto en redes LAN como en la red de acceso de las redes WAN.

9 La principal diferencia entre cable categoría 5 y categoría 6 es:
- a) El ancho de banda.
- b) La resistencia a la humedad y corrosión.
- c) El tipo de datos que se pueden transmitir.
- d) Todas las respuestas anteriores son correctas.

10 La ventaja del uso de cable de fibra óptica respecto al cable de cobre es:
- a) La fibra óptica tiene mayor ancho de banda.
- b) La fibra óptica tiene mayor inmunidad frente a perturbaciones.
- c) Las señales ópticas sufren una menor atenuación que las señales eléctricas.
- d) Todas las respuestas anteriores son correctas.

11 El subsistema del cableado estructurado que proporciona conectividad a los puestos de trabajo de los usuario es:

a) El subsistema horizontal.
b) El subsistema vertical.
c) El subsistema de campus.
d) Cualquier subsistema puede hacer esa función.

12 El tipo de cableado más común utilizado en el subsistema horizontal es:

a) Fibra óptica multimodo.
b) Fibra óptica monomodo.
c) Cable UTP categoría 3 ó 5.
d) Cable UTP categoría 5e ó 6.

9 Ethernet y dispositivos de interconexión

OBJETIVOS DEL CAPÍTULO

- ✓ Relacionar adecuadamente las funciones de Ethernet con el modelo OSI.
- ✓ Conocer los elementos que forman parte de una red Ethernet.
- ✓ Conocer las principales características de Ethernet.
- ✓ Entender las diferencias entre las distintas versiones de Ethernet.
- ✓ Conocer los principios de funcionamiento de un *switch* así como sus principales características.

Como vimos en el Capítulo 7, existen principalmente dos tipos de redes de datos conocidos como LAN y WAN. La principal diferencia entre ellos es que los dispositivos conectados a una red LAN se encuentran ubicados en un área geográfica limitada, mientras que las redes WAN no tienen esa limitación.

Sin ninguna duda se puede afirmar que Ethernet es una de las tecnologías más importantes en el ámbito de las redes de datos. Actualmente es la tecnología dominante en las redes LAN cableadas. Ethernet tuvo que competir a mediados de los años 80 con otras tecnologías LAN como **Token Ring** o **Token Bus**, pero salió claro ganador y hoy en día el porcentaje de utilización de Ethernet en redes LAN cableadas debe estar muy cerca del 100%. El éxito de Ethernet está basado fundamentalmente en su simplicidad, bajo coste y a su alta capacidad de adaptación. En su primera versión Ethernet proporcionaba una velocidad de apenas 3 Mbps y en la actualidad existen especificaciones de Ethernet para trabajar a 10 Gbps. Desde luego, toda una evolución.

9.1 INTRODUCCIÓN

Ethernet es una tecnología desarrollada para ser utilizada en redes LAN, en las cuales cubre las funciones del nivel físico y del nivel de enlace del modelo de referencia OSI. Recordemos que las redes LAN proporcionan conexión a dispositivos en un ámbito geográfico limitado, lo cual es una de las condiciones de diseño. Además, para desarrollar Ethernet se tuvo en cuenta otras necesidades importantes de las redes LAN, como son alcanzar altas velocidades de transferencia de datos con una baja tasa de errores y que la instalación y mantenimiento sean lo más sencillos posible.

Actualmente, nadie pone en duda las ventajas que se generan al interconectar equipos próximos entre sí o que pertenezcan a una misma unidad organizativa en un edificio (o varios próximos entre sí), es decir, al implementar una LAN. Desde pequeñas oficinas, naves o talleres hasta grandes empresas con cientos o miles de empleados, se utilizan las tecnologías de las redes LAN para interconectar sus equipos y aprovecharse de todas las ventajas que ello supone, principalmente el uso compartido de archivos, impresoras y otros periféricos, así como el acceso compartido a Internet, el acceso a aplicaciones corporativas... Incluso cada vez son más frecuentes los hogares donde montan sus redes LAN a pequeña escala, con dos o tres ordenadores, una impresora y un *router* de acceso a Internet.

La tecnología Ethernet fue desarrollada inicialmente por la empresa **Xerox** en 1973 y funcionaba a una velocidad de 2,94 Mbps. Posteriormente, la colaboración entre las empresas Xerox, Intel y Digital (conocida como DIX) dio lugar a su primera versión oficial que fue publicada en 1980, donde ya se especificaba una velocidad de 10 Mbps.

Ethernet no fue un desarrollo cerrado, Xerox permitió el uso de esta tecnología mediante el pago de una pequeña cuota, de forma que cualquier empresa pudo utilizarlo, propiciando su rápida difusión. En 1982 se publicó la segunda versión de Ethernet conocida como **Ethernet II**. Esta versión fue la última especificada por DIX y de hecho ese mismo año Xerox liberó la marca registrada sobre el nombre Ethernet.

La organización IEEE utilizó las características de Ethernet como base para desarrollar su estándar IEEE 802.3. Actualmente se utiliza la denominación Ethernet para referirse tanto a la especificación original como a la especificación IEEE 802.3.

Ethernet fue un éxito desde su comienzo, y el éxito ha continuado gracias a su gran capacidad de evolución. Durante algunos años se trabajó con redes Ethernet a 10 Mbps pero en 1995 se publicó una nueva extensión de la norma para velocidades de 100 Mbps, conocida como Fast Ethernet. Pocos años más tarde, en 1998 se publicó la extensión de la norma Ethernet, llamada Gigabit Ethernet, para velocidades de 1 Gbps sobre fibra óptica y en 1999 para cable UTP. Desde el año 2002 se han ido publicando varias ampliaciones de la norma Ethernet para velocidades de 10 Gbps.

9.2 ETHERNET, IEEE 802.3 Y EL MODELO OSI

Como se ha mencionado en el apartado anterior, el organismo IEEE decidió crear un comité (conocido como comité 802) para estandarizar las redes de datos. Fruto de este trabajo, en 1985 se publicó la norma IEEE 802.3 que definía una tecnología abierta (cualquier fabricante podía adoptarla) para redes de área local. El comité del IEEE utilizó la tecnología Ethernet como referencia para desarrollar la norma IEEE 802.3 pero a su vez intentó encajar esta tecnología en el modelo de referencia OSI (publicado solo un par de años antes, en 1983). Debido a ello, la norma IEEE 802.3 presentaba algunas pequeñas diferencias respecto a Ethernet, aunque se consideraron tecnologías compatibles.

Además del estándar IEEE 802.3 fueron publicados otros estándares de redes locales como el IEEE 802.4, conocido como *Token Bus*, y el IEEE 802.5, desarrollado a partir de la tecnología de redes locales usada en esa época por IBM y llamada *Token Ring*. Durante unos años estas tecnologías de redes locales convivieron hasta que se impuso el estándar basado en Ethernet.

El organismo IEEE ha seguido desarrollando estándares relacionados con las redes telemáticas, muchos de ellos basados en transmisiones inalámbricas como IEEE 802.11 (Wi-Fi), IEEE 802.15.1 (*Bluetooth*) o IEEE 802.16 (WiMAX). Así mismo, el IEEE ha seguido publicando revisiones y actualizaciones del estándar IEEE 802.3 para adaptarlo a las nuevas exigencias de prestaciones de las redes locales.

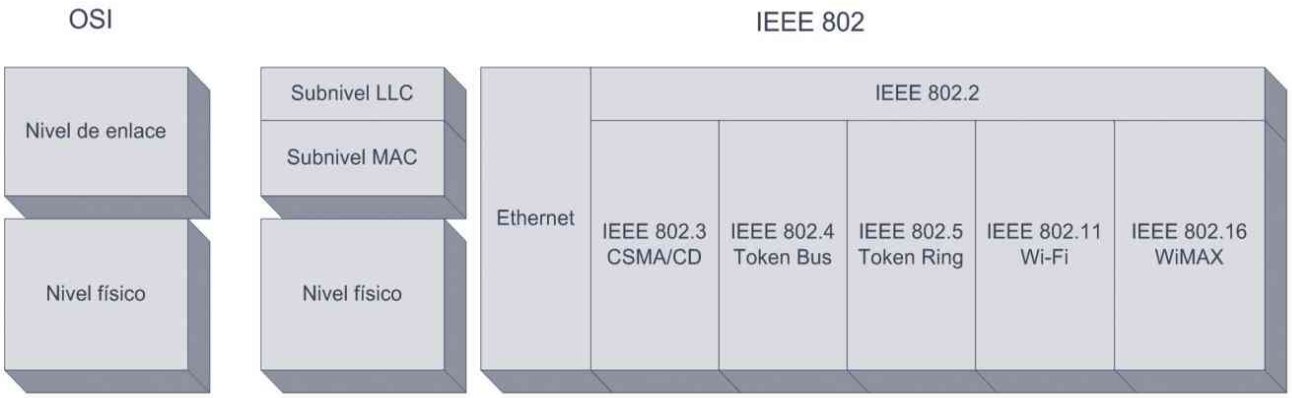


Figura 9.1. *Estándares para redes del IEEE*

Como se observa, el nivel de enlace en las redes LAN definidas por el proyecto IEEE 802 se subdivide de dos niveles, uno superior y común a todas las implementaciones LAN, llamado **LLC** (*Logical Link Control* o control de enlace lógico), y otro inferior llamado **MAC** (*Medium Access Control* o control de acceso al medio), que depende de cada implementación.

Control de enlace lógico (LLC): 802.2

El subnivel **LLC** (*control de enlace lógico*) está definido dentro del estándar **IEEE 802.2**. Es el subnivel superior del nivel de enlace en todas las tecnologías de red definidas por el IEEE. Es decir, este subnivel no depende de ninguna implementación de red concreta y es común a todas ellas.

La principal función de este subnivel es proporcionar un formato único de datos y una interfaz común al nivel superior, es decir, al nivel de red. De esta forma se esconden al nivel de red las diferencias de formatos en los diferentes tipos de redes. Para ello, este nivel implementa una encapsulación de datos añadiendo una cabecera.

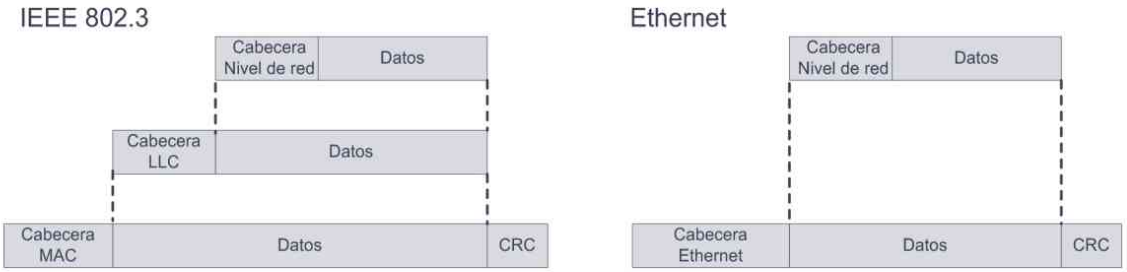


***Figura 9.2**. El subnivel LLC situado entre el nivel de red y el subnivel MAC*

Las funciones que proporciona Ethernet son las funciones que cubren los niveles físico y de enlace del modelo de referencia OSI. Por una parte, Ethernet especifica todos los aspectos relacionados con el nivel físico, como puede ser el tipo de cableado, conectores, velocidad, codificación de los datos, etc. Pero, además, especifica funciones del nivel de enlace como métodos de acceso al medio, direccionamiento físico, tramado o control de errores.

La evolución de Ethernet ha supuesto desarrollar nuevas especificaciones, sobre todo en las funciones del nivel 1 (físico). Sin embargo, algunas de las funciones del nivel 2 (enlace) han permanecido sin variaciones desde las primeras versiones. Después de dedicar un apartado sobre el primer contacto práctico con una red basada en Ethernet, dedicaremos los siguientes a estudiar todas las funciones que proporciona Ethernet.

9.3 UN PRIMER CONTACTO PRÁCTICO CON ETHERNET

Antes de profundizar en los aspectos técnicos relacionados con Ethernet, se ofrecerá en este apartado una visión más práctica de lo que nos vamos a encontrar cuando estemos delante de una red que utilice Ethernet.

En muchas ocasiones se utiliza la expresión **red Ethernet** para referirise a una red LAN que utiliza la tecnología Ethernet que, por otra parte, son la gran mayoría de las redes. Emplearemos esta expresión en la presente obra.

La primera característica importante a tener en cuenta sobre las redes Ethernet es su topología, es decir, cómo están conectados los elementos que forman parte de la red. Actualmente Ethernet utiliza una **topología en estrella**, y dado que admite un cierto nivel de anidamiento es frecuente encontrar redes Ethernet siguiendo topologías en árbol o estrella anidada.

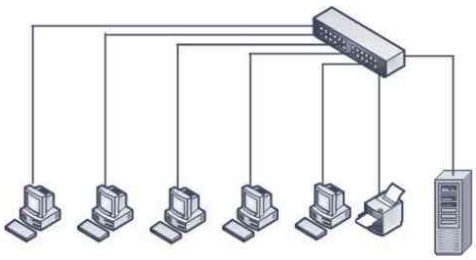


***Figura 9.3**. Topología en estrella de las redes Ethernet actuales*

Es prácticamente seguro que cuando estemos en algún lugar que tenga una red local en funcionamiento, ésta utilice Ethernet. ¿Cuáles son los elementos visuales que nos encontraremos en una red Ethernet?

- **Cableado y su infraestructura de distribución**. Si nos encontramos en un lugar donde existe una instalación de cableado de datos, dicha instalación contará con unos puntos de conexión llamados **rosetas** o tomas murales, situadas en cada área de trabajo.

***Figura 9.4**. Roseta y latiguillo en una red Ethernet*

Desde este punto de conexión existirá un cable que conectará dicho punto al ordenador. Este cable habitualmente es de tipo UTP de 4 pares y se conoce como **latiguillo de red**. Los latiguillos de red se identifican por sus extremos, que cada uno tiene un conector RJ-45.

Los puntos de conexión, o rosetas, a su vez estarán unidos a la infraestructura de comunicaciones mediante el cableado distribuido por canaletas, bandejas, falsos suelos o techos. Todo el cableado de distribución acaba en los armarios de comunicaciones donde se conectan a los dispositivos de interconexión, típicamente *switches*.

***Figura 9.5**. Cableado de red distribuido por un falso suelo*

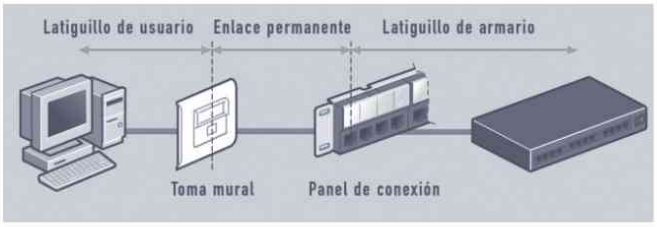


***Figura 9.6**. Enlace completo en una instalación de red Ethernet*

La infraestructura del cableado en redes Ethernet se adapta perfectamente a las normas de cableado estructurado vistas en el capítulo anterior.

El uso del cable UTP en redes LAN basadas en Ethernet está tan extendido que es frecuente escuchar el término **cable Ethernet** para referirse a un cable UTP de cuatro pares.

- **Tarjetas de red**. El punto de entrada de la red a los equipos es la tarjeta de red. Podemos encontrar tarjetas de red que se instalan en los *slots* PCI de la placa del equipo, aunque la mayor parte de las tarjetas de red están incluidas en la propia placa base del equipo. El único elemento identificativo en este caso es el conector de red, que para el cable UTP es el conector RJ-45. En el próximo apartado se dan algunos detalles más sobre las tarjetas de red.

- **Dispositivo de interconexión**. Habitualmente, el dispositivo de interconexión utilizado para formar redes LAN se conoce como **switch** o **conmutador**. En la mayor parte de las redes, el *switch* (o los *switches*) suele estar ubicado en un espacio reservado o una sala técnica hasta donde llega todo el cableado. Más adelante en este capítulo se darán más detalles del funcionamiento de los *switches*.

***Figura 9.7**. Dos switches en funcionamiento en una red local Ethernet*

En las pequeñas instalaciones domésticas no existe una infraestructura de cableado. El *router* de acceso a Internet proporcionado por el provedor de acceso a Internet suele integrar la funcionalidad de un *switch* de cuatro puertos, por lo que dicho *router* hace las funciones de dispositivo de interconexión. La conexión de los puertos Ethernet del *router* a los equipos se hace directamente con un latiguillo de red.

***Figura 9.8**. Router ADSL con cuatro puertos Ethernet formando una red local de cuatro equipos*

9.4 TARJETAS DE RED

Las tarjetas de red, también conocidas por sus siglas en inglés **NIC** (*Network Interface Card*) son elementos electrónicos que posibilitan la conexión de un equipo a una red local. Las primeras tarjetas de red se conectaban en un equipo a través de un *slot* de expansión en la placa base del equipo.

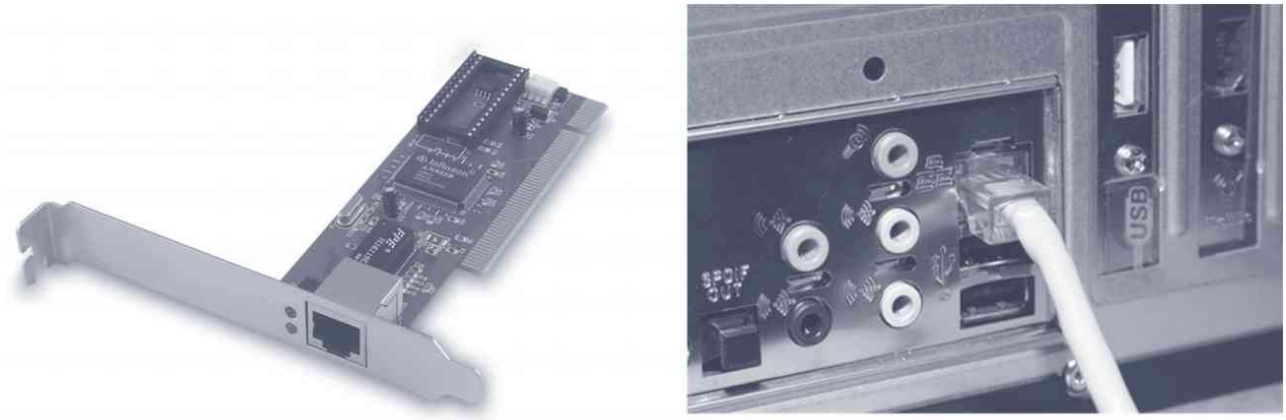


***Figura 9.9**. Tarjeta de red para conectar en un slot PCI y tarjeta de red incluida en la placa base*

En la actualidad, todas las placas base incluyen ya la circuitería relativa a la tarjeta de red, por lo que no es necesario conectar al equipo ninguna tarjeta de red a menos que la tarjeta de red incluida en la placa base se estropee o necesitemos una con características especiales.

El diseño y las funciones implementadas en una tarjeta de red dependen de la tecnología para la que se va a utilizar. Actualmente, la tecnología dominante es Ethernet, por tanto, todas las tarjetas de red que se pueden encontrar son tarjetas Ethernet. La mayor parte de ellas utilizan cable UTP y, por tanto, el conector que llevan incorporado es de tipo RJ-45. Sin embargo, existen especificaciones Ethernet que utilizan fibra óptica, por lo que también existen en el mercado tarjetas de red Ethernet con un conector para fibra óptica.

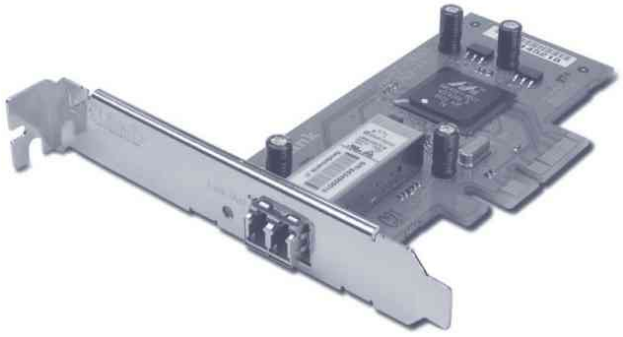


***Figura 9.10**. Tarjeta Gigabit Ethernet (DLink DGE-560SX) que utiliza fibra óptica en lugar de cable UTP*

La dirección física en las redes Ethernet es un número binario formado por 48 bits (6 *bytes*) y almacenado en la propia tarjeta de red. La dirección física tambien se conoce como **dirección MAC**.

Esta dirección debe ser única para toda la red; para conseguir esto cada tarjeta de interfaz de red se configura de fábrica con una dirección física diferente. De esta forma se asegura que no va a haber dos tarjetas conectadas en la misma red con la misma dirección física. Los 24 bits de mayor peso los asigna el IEEE e identifica a la empresa fabricante de la tarjeta de red. Este número de 24 bits se conoce como **OUI** (*Organizationally Unique Identifier*). Los 24 bits de menor peso los asigna el fabricante a cada tarjeta durante el proceso de fabricación.

Un ejemplo de dirección física podría ser el siguiente:

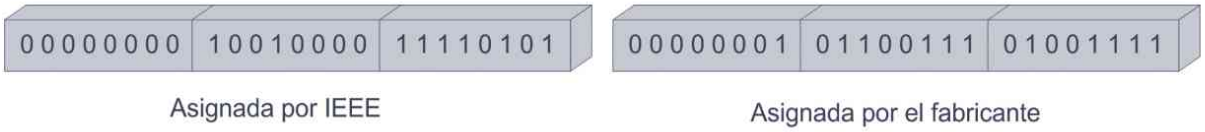


***Figura 9.12**. Dirección MAC en binario*

La notación binaria utilizada en el ejemplo anterior es incómoda de manejar, por lo que normalmente se utiliza la notación hexadecimal. En dicha notación se utilizan guiones (-) o dos puntos (:) como separadores de cada dos dígitos hexadecimales. El ejemplo anterior se representaría en formato hexadecimal de la siguiente forma **00-90-F5-01-67-4F** o bien utilizando el carácter "dos puntos" como separador: **00:90:F5:01:67:4F**.

Se ha definido una dirección especial llamada **dirección de broadcast o de difusión** utilizada para enviar una trama a todos los dispositivos de una red. Es la dirección FF:FF:FF:FF:FF:FF, es decir, todos los bits a valor 1.

Todos los equipos conectados a una red Ethernet deben tener asignada una dirección MAC. Incluso puede darse el caso de equipos que tienen más de una tarjeta de red. En este caso, cada tarjeta de red tendrá su dirección MAC. Para equipos que utilizan como sistema operativo Windows® 7 (o XP) se puede consultar la dirección MAC con el comando *ipconfig/all* ejecutado mediante la herramienta *Símbolo del sistema*.

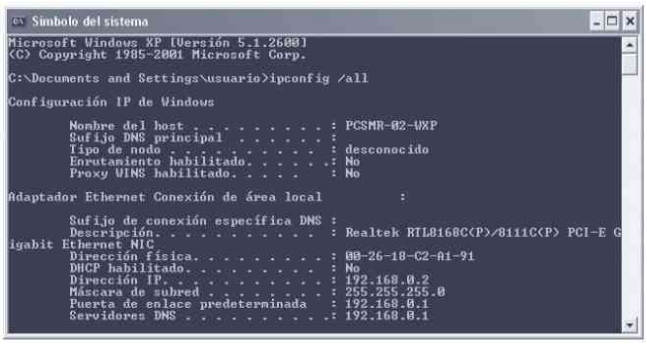


***Figura 9.13**. Ejecución del comando ipconfig para ver la dirección MAC*

En sistemas Linux se puede consultar la dirección MAC mediante el comando *ifconfig* ejecutado desde un terminal de comandos.

La dirección física es asignada por el fabricante a una tarjeta de red en el proceso de fabricación y no puede ser cambiada. Sin embargo, en la actualidad existen mecanismos que permiten llevar a cabo un cambio ficticio de la dirección física por software, normalmente a través de los sistemas operativos más actuales como Windows® XP, Windows® 7 o Linux. En este caso, la dirección física de la tarjeta no se altera pero los servicios de red del sistema operativo proporcionan una dirección física ficticia, es decir, enmascaran la verdadera dirección. En la siguiente figura se puede observar la ventana de configuración de la tarjeta de red de un equipo y el parámetro con el que se puede modificar la dirección física de dicho equipo.

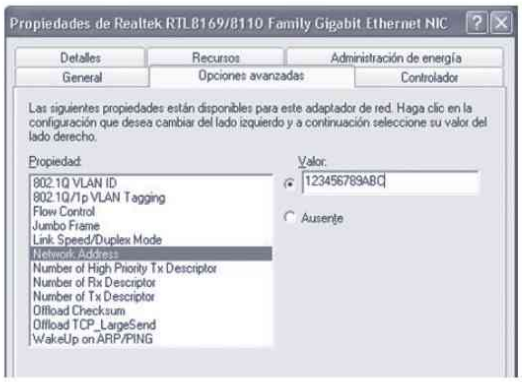


***Figura 9.14**. Enmascaramiento de la MAC de una NIC desde Windows® XP*

9.5.2 FORMATO DE TRAMA

Una de las funciones cubiertas en el nivel de enlace es el tramado de la información que se quiere transmitir. El tramado consiste en dividir dicha información en fragmentos denominados tramas y añadir a cada fragmento información de control en lo que se conoce como cabecera. Veamos primero cómo es el formato de la trama especificada en el estándar IEEE 802.3.

***Figura 9.15**. Formato de la trama IEEE 802.3*

La trama IEEE 802.3 se divide en campos o bloques de información. La información real que se quiere transmitir y que proviene del nivel superior se incluye en el campo **Datos**, el resto es información de control. A continuación se describe la función de cada campo:

- **Preámbulo**. Está formado por 7 *bytes* (56 bits) con valores 0 y 1 alternados. Es decir, cada *byte* contiene los bits 10101010. Este campo se utiliza para realizar la sincronización entre el emisor y el receptor.
- **SFD** (*Start Frame Delimiter*) o delimitador del comienzo de trama. Es 1 *byte* con el valor 10101011. Este campo indica el inicio de la trama.
- **Dirección de destino**. Campo con un tamaño de 6 *bytes* que contiene la dirección física (dirección MAC) del dispositivo de destino.

- **Dirección fuente u origen**. Campo con un tamaño de 6 *bytes* que contiene la dirección física (dirección MAC) del dispositivo que envía la trama.
- **Longitud**. Este campo está formado por 2 *bytes* que indican la longitud de los datos. El valor mínimo es 0 y el máximo es 1.500.
- **Datos**. Este campo tiene un tamaño variable entre 46 y 1.500 *bytes* dependiendo lógicamente de la información recibida del nivel superior. El tamaño mínimo de este campo debe ser de 46 *bytes*, por tanto, si el número de *bytes* para enviar es inferior, se envían *bytes* de relleno hasta completar este tamaño mínimo. Esto se debe a que el tamaño mínimo total de la trama debe ser de 64 *bytes* por cuestiones relacionadas con la temporización en el uso del medio de transmisión.
- **FCS** (*Frame Check Sequence*) o secuencia de verificación de trama. Este campo contiene un valor de 4 *bytes* (32 bits) conocido como **CRC** o código de redundancia cíclica y que es utilizado para detección de errores en la transmisión. El campo FCS no se considera parte de la cabecera, ya que se añade al final de la trama, sin embargo, sí forma parte de la inforrmación de control.

Veamos ahora cúal es el formato de la trama Ethernet II:

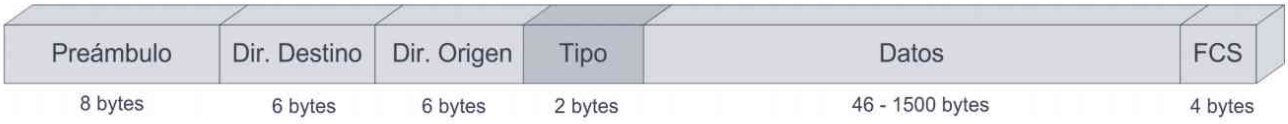


***Figura 9.16**. Formato de la trama Ethernet II*

Se puede observar que hay pocas diferencias entre las tramas IEEE 802.3 y Ethernet II. Por una parte, el campo SFD de IEEE 802.3 está incluído en el preámbulo en Ethernet II pero su contenido es el mismo. Por otra parte, el campo **Longitud** en IEEE 802.3 se ha convertido en el campo **Tipo** en Ethernet II. El campo **Tipo** es un código de 2 *bytes* que indica el protocolo de nivel superior (nivel de red).

Los protocolos de nivel de red más utilizados en redes LAN basadas en TCP/IP son IP y ARP. Además para IP existen dos versiones, la actual IPv4 y la futura IPv6. Los códigos en valor hexadecimal utilizados en el campo *Tipo* para estos protocolos son:

- IPv4 0800
- IPv6 86DD
- ARP 0806

Además, hay que tener en cuenta que en la trama IEEE 802.3 el campo *Datos* contiene la información del nivel superior, que en este caso es el subnivel LLC. Este subnivel, como se ha comentado anteriormente, añade una cabecera de 3 *bytes*. En el caso del formato Ethernet II, el campo *Datos* contiene información que proviene directamente del nivel de red, ya que en este caso no se utiliza el subnivel LLC.

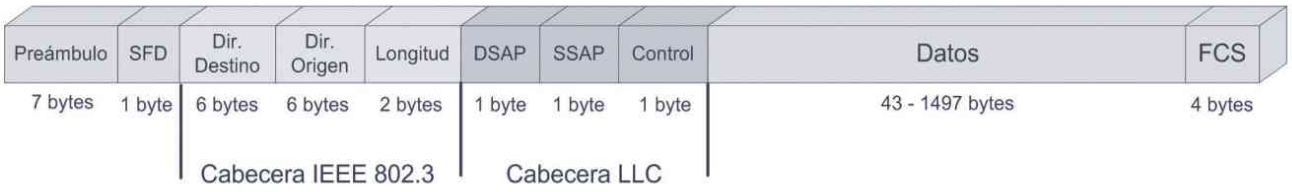


***Figura 9.17**. Formato de la trama IEEE 802.3 incluyendo la cabecera LLC*

Estos dos formatos de trama han coexistido en las redes Ethernet hasta que en 1997 el IEEE incluyó el formato Ethernet II en el estándar IEEE 802.3, por lo que desde entonces ambos formatos de trama forman parte del estándar, pasándose a denominar el campo que marcaba la diferencia como *Longitud / Tipo*. En cualquier caso, la mayor parte de los dispositivos de red en la actualidad utilizan el formato Ethernet II.

La forma en la que las tarjetas de red manejan los dos tipos de tramas es simplemente analizando los dos siguientes *bytes* de la dirección origen. Si es un número igual o inferior a 1.500 es una trama IEEE 802.3 y este campo indica la longitud de la trama y si es un número superior a 1.500 (05DC en hexadecimal) es una trama Ethernet II y este campo indica el tipo de protocolo de nivel superior.

Los campos *preámbulo* y *SFD* son campos utilizados para sincronización y realmente no forman parte de la trama. De hecho, las últimas versiones no necesitan estos mecanismos de sincronización y estos campos no son necesarios, aunque se mantienen en el estándar por motivos de compatibilidad.

9.5.3 CONTROL DE ACCESO AL MEDIO: CSMA/CD

Las primeras versiones de Ethernet utilizaron enlaces multipunto en los que varios dispositivos estaban conectados en el mismo enlace (por ejemplo, en la implementación 10BASE-T), por ello fue necesario establecer un mecanismo de arbitraje para resolver el conflicto ocasionado cuando dos equipos quieren acceder al mismo tiempo al medio de transmisión.

Las técnicas utilizadas para esta función se denominan técnicas de **contienda** y se han desarrollado varias a lo largo de la historia. Todas ellas se basan en el tratamiento de un estado que se puede producir en el medio de transmisión llamado colisión. Una **colisión** se produce cuando dos dispositivos transmiten datos simultáneamente. Las señales enviadas por cada dispositivo se mezclan y se pierde la información que contienen.

La técnica de contienda utiliza en Ethernet es **CSMA/CD** (*Carrier Sense Multiple Access with Collision Detection*, acceso múltiple por detección de portadora y con detección de colisiones) y sus principios de funcionamiento son los siguientes:

- ✓ Cuando un equipo quiere transmitir una trama comprueba si el medio de transmisión está libre, es decir, no hay otro dispositivo enviando información. Por lo tanto, si el medio está libre, dicho equipo comienza la transmisión de su trama.
- ✓ Si el medio está ocupado, el equipo espera hasta que quede libre y transmite su trama.
- ✓ Mientras se transmite la trama el equipo comprueba continuamente si se produce alguna colisión.
- ✓ Si se detecta una colisión se deja de transmitir inmediatamente, se espera un tiempo aleatorio y se intenta la transmisión de nuevo.

Solamente se comprueba si hay colisión mientras se transmite la trama, por lo que es importante que los sistemas que utilicen CSMA/CD estén correctamente diseñados para que no se produzcan colisiones después de que el transmisor deje de transmitir. En el caso de Ethernet, esta situación puede ocurrir para la transmisión de tramas muy cortas, por esta razón las tramas Ethernet necesitan un número mínimo de *bytes*, concretamente 64 *bytes*, ya que con tramas más pequeñas no se garantizaría la detección correcta de colisiones.

El uso de medios de transmisión compartidos, donde es necesario utilizar **CSMA/CD convierte a Ethernet en una tecnología half-dúplex**, ya que solo puede haber una trama simultáneamente en el medio de transmisión.

9.5.4 CONTROL DE ERRORES EN ETHERNET

En las redes Ethernet pueden aparecer diferentes tipos de errores, algunos de ellos relacionados con las colisiones (colisiones atrasadas) y otros relacionados con tamaños incorrectos de trama. Estos errores aparecen de forma esporádica.

Como se ha visto anteriormente, en la trama Ethernet existe un campo llamado *FCS* utilizado para el control de errores. Los errores detectados con este campo se refieren a errores de transmisión en los datos y normalmente son producidos por tarjetas de red defectuosas, controladores defectuosos o cableado en malas condiciones.

La técnica utilizada para la detección de errores FCS se basa en obtener a partir de un bloque de datos una secuencia de bits, llamada **CRC** (*Cyclic Redundancy Code*, o código de redundancia cíclica). En este caso, el bloque de datos es la propia trama Ethernet, incluida la información de control. Esta secuencia de bits es calculada por el emisor siguiendo un algoritmo determinado y transmitida en el campo *FCS* de la trama Ethernet. El receptor, cuando recibe los datos, realiza el mismo cálculo. Si el CRC calculado por el receptor coincide con el recibido es que los datos no han sido alterados en la transmisión, es decir, no ha habido errores y, por tanto, la trama se acepta. Cuando el CRC calculado no coincide con el recibido es que ha habido errores en la transmisión, con lo cual la trama se descarta.

9.6 10BASE-T: ETHERNET SOBRE PAR TRENZADO

Ya hemos visto como la implementación de muchas de las funciones del nivel 2 desarrolladas en Ethernet se ha mantenido a lo largo del tiempo. No ha ocurrido lo mismo con la implementación de las funciones del nivel 1. Es en las funciones del nivel 1, donde se definen aspectos como tipo de cableado, conectores, velocidad de transmisión y longitud máxima de los cables, etc., donde se ha llevado a cabo la evolución de Ethernet para conseguir adaptarse a las nuevas exigencias de prestaciones de las redes actuales.

En los primeros años se publicaron varios estándares que utilizaban diferentes topologías y medios de transmisión, aunque el que se acabó imponiendo y se tomó como referencia para desarrollar las sucesivas versiones del estándar fue el conocido como **10BASE-T** o **Ethernet sobre par trenzado**.

El nombre de la implementación se descompone en tres partes. La primera indica la velocidad máxima (10 indica 10 Mbps). La segunda parte indica el tipo de transmisión (BASE indica banda base). Y la tercera parte indica la longitud máxima de un segmento (5 indica 500 metros) para las primeras implementaciones o un código referido al tipo de medio de transmisión en las más recientes.

Las primeras implementaciones de Ethernet 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 roturas 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 equipo 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 solo afectarían al equipo al 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 568** en 1991. Esta circunstancia propició aún más el despliegue de redes 10BASE-T. Actualmente, las dos normativas más utilizadas en cableado estructurado son la EIA/TIA 568-A y la ISO/IEC 11801 publicadas en 1995. A continuación se enumeran las principales características de 10BASE-T:

- ✓ La topología física es en estrella física aunque a nivel lógico se sigue comportando como un *bus*.

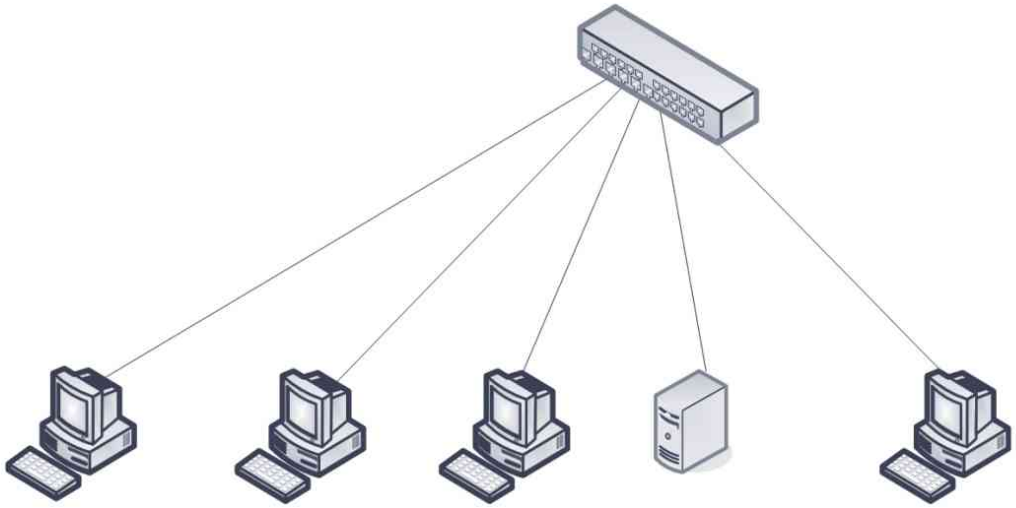


***Figura 9.18**. Topología en estrella física en 10BASE-T*

- ✓ Se utiliza cable de par trenzado sin apantallar (UTP) de categoría 3 o superior. Las categorías de cables están definidas en la norma EIA/TIA 568.

- Los cables UTP utilizados son de cuatro pares (ocho conductores) con conectores RJ-45 en ambos extremos. De estos cuatro pares solo se utilizan dos.

***Figura 9.19**. Cable UTP con conectores RJ-45*

- La velocidad de transmisión es de 10 Mbps.
- La codificación utilizada es Manchester en banda base con valores de tensión de +/- 5 v.
- Todas las operaciones de red se sitúan en un dispositivo de red llamado **concentrador** o **hub**, el cual tiene un puerto de entrada de tipo RJ-45 por cada equipo. Todos los equipos de la red se conectan al *hub*. En el interior del hub se implementa un *bus* lógico.

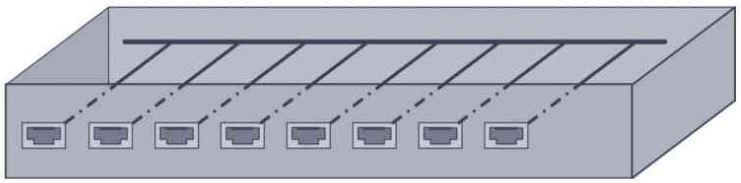


***Figura 9.20**. Implementación de un bus lógico en un hub*

- La longitud máxima del cable entre un equipo y el *hub* es de 100 metros. Esta limitación viene impuesta por las características físicas del cable de par trenzado, de calidad inferior al cable coaxial.
- El *hub* retransmite todas las tramas recibidas a los equipos que están conectados al mismo. Cada tarjeta de red comprueba si la trama le pertenece comprobando la dirección de destino. Si no coincide con la dirección física la trama se desecha. Con este modo de operación la topología lógica sigue siendo en *bus*, ya que cualquier trama enviada por un equipo se propagará por el resto de equipos. Lógicamente se seguirán produciendo colisiones.

RECUERDA

El *hub* o concentrador es el elemento central de las redes 10BASE-T. Retransmite la trama recibida por un puerto al resto de los puertos.

9.7 FAST ETHERNET: ETHERNET A 100 MBPS

El rápido crecimiento y utilización de las redes Ethernet produjo a su vez un aumento de los requerimientos de velocidad. Las redes Ethernet estaban formadas cada vez por más equipos y las transferencias de información a través de las mismas también iban en aumento. La solución adoptada por el IEEE fue **Fast Ethernet**, publicada en 1995 como **IEEE 802.3u**. Su principal característica es el aumento de la velocidad de transmisión de 10 a 100 Mbps.

Fast Ethernet utiliza la especificación 10BASE-T como referencia, de forma que se intenta mantener las características de ésta. Por ejemplo, se mantiene la topología en estrella física y lógica en *bus*, se sigue utilizando CSMA/CD como método de acceso al medio y se mantiene el formato de la trama. Para dar diferentes alternativas en función de los medios de transmisión disponibles, el IEEE publicó tres alternativas de redes Fast Ethernet que se verán a continuación.

9.7.1 100BASE-TX

Esta versión de Fast Ethernet es la que se ha impuesto y actualmente es uno de los tipos de redes más utilizados. Uno de los cambios necesarios en esta implementación es el tipo de cable. Se utiliza cable de cobre de par trenzado sin blindaje (UTP) de categoría 5. La principal diferencia entre categoría 3 y categoría 5 es la frecuencia máxima, que lógicamente debe ser mayor en categoría 5. Se utilizan dos pares, uno para transmisión y otro para recepción de forma que este tipo de redes admite operaciones *full-dúplex* (esta característica se verá en el próximo apartado). La distancia máxima entre un equipo y el *hub*, al igual que en 10BASE-T, es de 100 metros. Resumen de características de 100BASE-TX:

- ✓ Velocidad de transmisión 100 Mbps.
- ✓ Topología física en estrella y lógica en *bus* con modo de transmisión *half-dúplex*.
- ✓ Necesidad de un elemento de interconexión central (*hub*).
- ✓ Cableado UTP de categoría 5, cada enlace puede tener una distancia máxima de 100 metros.
- ✓ Conectores RJ-45.
- ✓ Codificación 4B/5B y codificación de línea MLT-3.

9.7.2 100BASE-FX

Esta versión de Ethernet, al igual que la siguiente, no ha tenido mucha repercusión y actualmente no hay muchas redes que la utilicen. Sus principales características son:

- ✓ Utiliza como medio de transmisión fibra óptica multimodo.
- ✓ Utiliza conectores SC o ST.
- ✓ La codificación utilizada es 4B/5B y NRZ-I. Elegida por compatibilidad con las redes FDDI.
- ✓ Distancia máxima entre el concentrador y un equipo es de 2.000 metros en modo *full-dúplex*.

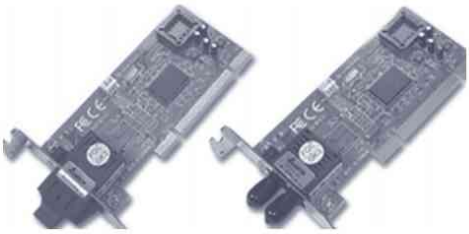


***Figura 9.21**. Tarjetas de red 100BASE-FX*

9.7.3 100BASE-T4

Esta versión de Fast Ethernet se especificó para dar la opción de aprovechar cableado instalado de categoría 3. Aunque, al igual que la anterior, no tuvo mucha penetración en el mercado.

- Utiliza cables de par trenzado categoría 3. Sin embargo, utiliza cuatro pares en lugar de dos para repartir el flujo de datos a 100 Mbps en tres de 33,3 Mbps. Dos de los pares utilizados se utilizan en modo *half-dúplex*, por lo que este tipo de redes no admite operaciones *full-dúplex*.
- La distancia máxima entre un equipo y el *hub*, al igual que en 100BASE-TX, es de 100 metros.
- Utiliza codificaciones 8B/6T y NRZ-I. La codificación 8B/6T sustituye un grupo de 8 bits en seis símbolos ternarios, es decir, se utilizan tres niveles de tensión diferentes en lugar de dos.

9.8 MEJORANDO ETHERNET: ETHERNET CONMUTADA Y FULL-DÚPLEX

Las redes Ethernet conmutadas se basan en la utilización como elemento central de la topología física en estrella un *switch* o conmutador, en lugar de un *hub*.

Un **switch** o **conmutador** es un dispositivo de interconexión que posee varios puertos de entrada, normalmente de tipo RJ-45. Externamente es parecido a un *hub*, sin embargo, y a diferencia de éste, un *switch* es capaz de leer las tramas Ethernet que recibe por cualquiera de sus puertos, analizar la dirección física de destino y reenviar la trama solo al puerto donde esté conectado el equipo con dicha dirección. Es decir, no hace una simple difusión de las señales eléctricas al resto de puertos. De esta forma se reduce drásticamente el número de colisiones. En un apartado posterior, en este mismo capítulo se verán en detalle las características más importantes de los *switches*.

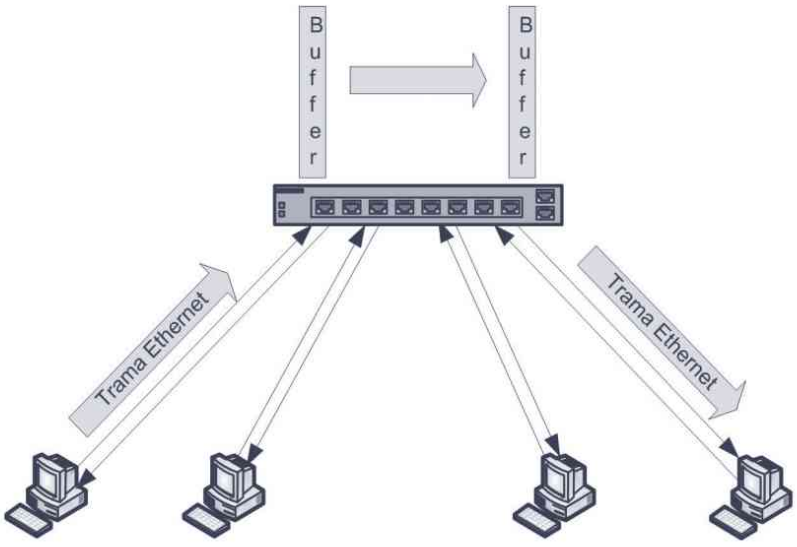


***Figura 9.22**. En la Ethernet conmutada no se produce difusión de las tramas en el switch*

La otra característica interesante que añaden los *switches* es que permiten comunicación *full-dúplex*. Para que este funcionamiento sea posible tanto la tarjeta de red (NIC) como el *switch* deben estar diseñados para ello. En el modo de funcionamiento *full-dúplex* no se utiliza el método de acceso al medio CSMA/CD por ser innecesario, ya que la conexión de cada NIC al *switch* utiliza un canal dedicado por cada sentido de la comunicación.

RECUERDA

En modo *full-dúplex* no es necesario utilizar el método CSMA/CD de acceso al medio, ya que cada conexión equipo-*switch* se comporta como una línea punto a punto.

El modo de funcionamiento *full-dúplex* está definido dentro del estándar IEEE en la especificación **IEEE 802.3x** (publicada en el año 1997), donde además se incluye un método de **control de flujo**. Esto es necesario ya que es posible que un dispositivo transmita tramas más rápido de lo que el receptor puede procesarlas, lo que provocaría pérdidas de información. Este control de flujo se implementa mediante el envío de una trama de control llamada **trama PAUSE** desde el receptor, donde le indica al emisor el tiempo que debe permanecer sin enviar datos. Durante el tiempo de inactividad el receptor puede volver a enviar *tramas PAUSE* para prolongar, reducir o suprimir la pausa inicial. Las *tramas PAUSE* se identifican porque contienen el valor 8808 (hexadecimal) en el campo *Tipo*.

El buen funcionamiento de esta operación depende sobre todo de lo rápido que se identifiquen las tramas de control de flujo. El comité IEEE comprobó que el formato Ethernet original era el más adecuado para este propósito, ya que permitía identificar las tramas de control de flujo mediante el campo *Tipo* mientras que en el formato IEEE esta información debe incluirse en la trama LLC. Por lo tanto, IEEE decidió estandarizar el formato de trama Ethernet. Este formato forma parte del estándar desde 1997 utilizando el campo *Tipo / Longitud* para distinguir el tipo de trama utilizado.

El ancho de banda efectivo de las redes que utilizan el modo *full-dúplex* se duplica respecto al modo *half-dúplex*. Así, una red *half-dúplex* funcionando a 100 Mbps aumentará su velocidad a 200 Mbps si utiliza el modo *full-dúplex*, ya que cada equipo conectado podrá tener un flujo máximo de información de 100 Mbps en un sentido y otros 100 Mbps en el sentido contrario de forma simultánea.

A partir de la versión IEEE 802.3x, publicada en 1997, se incluye en el estándar el formato de trama Ethernet II, por tanto, en la actualidad, ambos formatos de trama están incluídos en el estándar. El más utilizado es el formato Ethernet II (también conocido como DIX) principalmente por reducir la sobrecarga, eliminando la cabecera LLC.

Una de las características incluidas en la especificación IEEE 802.3u fue la capacidad de **autonegociación** entre el *switch* y los equipos para determinar principalmente dos características, la velocidad de transmisión 10/100 Mbps y el modo de transmisión *half-dúplex* o *full-dúplex*.

La mayor parte de los dispositivos de interconexión admiten esta característica, de forma que la comunicación entre los mismos y los equipos de la red es autoconfigurable de forma transparente al usuario. El controlador de la

En cualquier caso, tanto si tenemos un equipo con tarjeta de red como si ésta está integrada en la placa base, lo más habitual es el uso de cable UTP y, por tanto, en la parte trasera de dicho equipo encontraremos un conector hembra RJ-45 utilizado para conectar el equipo a la red.

Las tarjetas de red llevan a cabo todo el procesamiento de las funciones 1 y 2 del modelo de referencia OSI en el equipo. Muchas de las funciones, que veremos en los próximos apartados, se llevan a cabo precisamente en las tarjetas de red.

Para que una tarjeta de red funcione adecuadamente en un equipo con el sistema operativo Windows® o Linux es necesario que exista un **controlador** o **driver**. Dicho controlador posibilita que el sistema operativo pueda intercambiar información con la tarjeta, es decir, permite la comunicación entre el sistema operativo y la propia tarjeta de red. Los sistemas operativos contienen internamente controladores para muchos modelos diferentes de tarjetas de red pero en algunas ocasiones será necesario instalar dicho controlador, que deberá ser suministrado por el fabricante de la tarjeta de red.

Una vez instalado correctamente el controlador, es posible acceder a algunos parámetros de configuración avanzados de la tarjeta de red. En la siguiente figura se puede observar la ventana de configuración en Windows®:

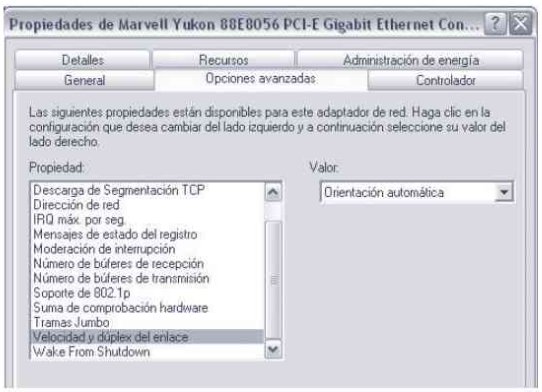


***Figura 9.11**. Ventana de configuración de la tarjeta de red en Windows®*

9.5 ESPECIFICACIONES DEL NIVEL 2 EN ETHERNET

Algunas de las especificaciones sobre funciones del nivel 2 del modelo de referencia OSI desarrolladas para las primeras versiones de Ethernet se han mantenido a lo largo del tiempo y siguen siendo válidas en la actualidad. Éstas son el *direccionamiento físico*, el *formato de la trama* y el *control de errores*. Sin embargo, la función de control del enlace utilizado en las redes Ethernet tradicionales hoy en día está prácticamente en desuso, aunque se ha mantenido en las especificaciones por motivos de compatibilidad.

9.5.1 DIRECCIONAMIENTO

En los próximos apartados se repasará la forma en que se implementan las principales funciones del nivel 2 del modelo OSI en Ethernet. Empecemos con el **direccionamiento físico**, que consiste en proporcionar un mecanismo para identificar cada equipo conectado a la red.

tarjeta de red suele tener la posibilidad de configurar las características de la tarjeta en modo autoconfiguración o se puede forzar un modo determinado de funcionamiento.

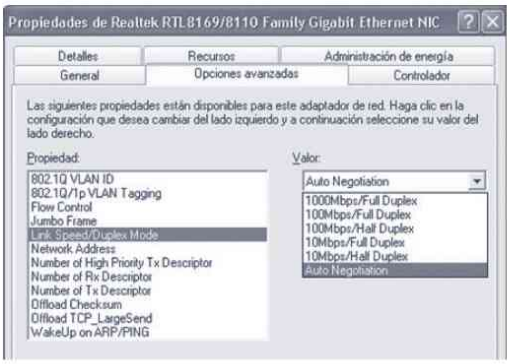


***Figura 9.23**. Configuración del modo de funcionamiento de la tarjeta de red en Windows® XP*

9.9 MÁS VELOCIDAD: GIGABIT ETHERNET Y 10-GIGABIT ETHERNET

Entre los años 1998 y 1999 el IEEE amplió el estándar IEEE 802.3 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 **IEEE 802.3z** o también **1000BASE-X**, que utiliza fibra óptica. La segunda desarrollada en 1999 llamada **IEEE 802.3ab** también conocida como **1000BASE-T** que utiliza cable de cobre de par trenzado. La principal característica de Gigabit Ethernet es que la velocidad de transmisión es de 1.024 Mbps o 1 Gbps.

1000BASE-X está basado en la utilización de fibra óptica como medio de transmisión. Además, utiliza las especificaciones a nivel físico del estándar **Fiber Channel** (ANSI X3 T11), pero mantiene la compatibilidad con Ethernet en el nivel de enlace. La arquitectura Fiber Channel utiliza cuatro capas, aunque la especificación 1000BASE-X utiliza solo las dos primeras llamadas FC-0 y FC-1.

9.9.1 1000BASE-T

El estándar 1000BASE-T permite la transmisión de datos a 1 Gbps ó 1.024 Mbps utilizando cable UTP pero manteniendo todas las funciones de Ethernet del nivel 2.

El estándar permite el uso de cable UTP de categoría 5 que cumpla la norma EIA/TIA 568 revisada en 1995. Para cableado de categoría 5 fabricado anterior a este año (y que siguiera la norma original EIA/TIA 568 publicada en 1991) no se recomienda su uso en 1000BASE-T. Para simplificar la adopción de criterios de cableado en muchas ocasiones se recomienda el uso de cable UTP de categoría 5e (5 mejorado) o superior.

Gigabit Ethernet puede funcionar tanto en modo *half-dúplex* como en modo *full-dúplex*. En modo *half-dúplex* se sigue usando el método CSMA/CD de acceso al medio como en las implementaciones anteriores de 10 y 100 Mbps, aunque en la práctica casi todos los sistemas que utilizan Gigabit Ethernet lo hacen exclusivamente en modo *full-dúplex*.

En resumen, las principales características de 1000BASE-T son:

- ✓ Cable de cobre de par trenzado categorías 5e ó 6.
- ✓ Velocidad de transmisión: 1024 Mbps ó 1 Gbps.
- ✓ Longitud máxima del cable: 100 metros.
- ✓ Técnica de transmisión PAM-5 con codificación 8B/10B.
- ✓ Transmisión *half-dúplex* o *full-dúplex*.

9.9.2 1000BASE-X

Las implementaciones 1000BASE-X utilizan como medio de transmisión la fibra óptica. A continuación se proporcionan las principales características de los dos tipos de implementaciones 1000BASE-X publicadas:

- **1000BASE-SX**
  - Emplea las codificaciones 8B/10B y NRZ-I.
  - Se utiliza fibra óptica multimodo.
  - La distancia máxima es de 275 metros para fibra de 62,5/125 µm o de 550 metros para fibra de 50/125 µm.
- **1000BASE-LX**
  - Emplea las codificaciones 8B/10B y NRZ-I.
  - Se utiliza tanto fibra óptica monomodo como multimodo.
  - La distancia máxima para fibra multimodo es de 550 metros o de 5 Km para fibra monomodo.

Ambas implementaciones de Gigabit Ethernet son utilizadas en modo *full-dúplex* principalmente para dar soporte al troncal (*backbone*) de las redes Ethernet de mediana o gran envergadura.

***Figura 9.24**. Tarjeta Gigabit Ethernet con conectores SC*

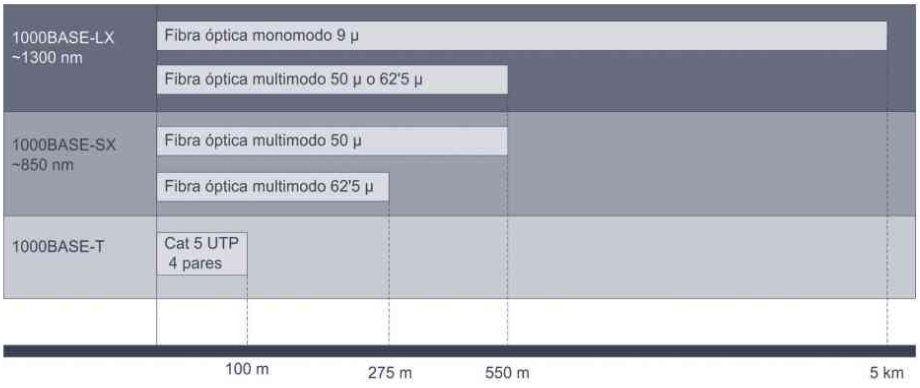


***Figura 9.25**. Distancias máximas en Gigabit Ethernet*

Implementación	Estándar IEEE	Año	Velocidad (Mbps)	Codificación	Tipo de cable	*Full-dúplex*
10BASE-T	802.3i	1990	10	Manchester	UTP Cat.3	Sí*
100BASE-TX	802.3u	1995	100	4B/5B y MLT-3	UTP Cat.5	Sí*
100BASE-FX	802.3u	1995	100	4B/5B y NRZ-I	Fibra óptica	Sí*
100BASE-T4	802.3u	1995	100	8B/6T y NRZ-I	UTP Cat.3	No
1000BASE-T	802.3ab	1999	1.000	PAM-5 y 8B/10B	UTP Cat.5, 5e ó 6	Sí
1000BASE-X	802.3z	1998	1.000	NRZ-I y 8B/10B	Fibra óptica	Sí

*El modo *full-dúplex* no está especificado en el estándar original. Este modo es admitido a partir del estándar IEEE 802.3x en el año 1997.

9.9.3 10-GIGABIT ETHERNET

En el año 2002 se publicó un nuevo estándar llamado **10-Gigabit Ethernet** (IEEE 802.3ae), abreviado como 10GbE y que funciona a velocidades de 10 Gbps sobre fibra óptica. Las implementaciones físicas que incluye el estándar IEEE 802.3ae son:

- **10GBASE-SR**, utiliza fibra óptica multimodo para distancias de hasta 300 metros.
- **10GBASE-LR**, utiliza fibra óptica monomodo para distancias de hasta 10 Km.
- **10GBASE-LX4**, utiliza multiplexación por división de onda (WDM) tanto para fibra óptica multimodo como monomodo.
- **10GBASE-ER**, utiliza fibra monomodo para cubrir distancias hasta 30 Km.
- **10GBASE-SW**, **10GBASE-LW**, **10GBASE-EW**, son similares a las implementaciones SR, LR y ER, pero con la posibilidad de interconectase con equipos que utilicen estándares sobre fibra óptica de redes WAN.

Posteriormente han aparecido algunas ampliaciones del estándar 10-Gigabit Ethernet:

- **10GBASE-LRM** (IEEE 802.3aq), publicada en 2006 para proporcionar compatibilidad con el cableado de las redes FDDI.
- **10GBASE-CX4** (IEEE 802.3ak), publicada en 2004. Es la primera especificación de 10-Gigabit Ethernet que utiliza cable de cobre (un tipo especial llamado InfiniBand) con una longitud máxima de 15 metros.
- **10GBASE-T** (IEEE 802.3an), publicada en 2006. Utiliza cable de cobre de categoría 6a para cubrir una distancia máxima de 100 metros.

InfiniBand es una interfaz de comunicaciones punto a punto de altas prestaciones cuyas primeras especificaciones fueron desarrolladas por varias empresas entre las que se encuentran Intel, AMD, Sun, IBM, Dell, Cisco o Silicon Graphics y que se publicaron en el año 2000.

El desarrollo de la tecnología 10-Gigabit Ethernet se ha enfocado principalmente al uso de Ethernet para redes WAN, gracias sobre todo a las distancias cubiertas por las especificaciones que utilizan fibra óptica. Por lo tanto, se puede decir que la evolución de Ethernet está enfocada a introducirse como tecnología en redes WAN. Uno de los principales reclamos es la posibilidad de que los operadores de telecomunicaciones puedan ofrecer a sus clientes conectividad Ethernet de extremo a extremo con el ahorro en costes y la simplicidad de gestión que ello supone.

9.10 ASIGNACIÓN DE PINES EN UTP PARA ETHERNET: CABLE DIRECTO Y CRUZADO

Como se ha visto anteriormente, los estándares 10BASE-T y 100BASE-TX utilizan cable UTP de cuatro pares de los cuales se utilizan dos, uno para transmisión y otro para recepción. En los estándares de cable UTP para Gigabit Ethernet y 10-Gigabit Ethernet, sin embargo, fue necesario utilizar los cuatro pares simultáneamente tanto en recepción como en transmisión.

La asignación de pines en el cable UTP y su correspondiente conector RJ-45 (su nombre formal es **8P8C**) sigue el estándar **EIA/TIA 568** de cableado estructurado. Realmente en este estándar hay dos asignaciones, conocidas como **T568A** y **T568B**. La asignación T568B es la más reciente y la más utilizada en la actualidad. Estas asignaciones siguen un código de colores utilizado en la cubierta plástica de cada hilo de un cable UTP. El uso habitual es la conexión de un equipo (a través de su tarjeta de red o NIC) a un *switch*. En este caso, el par utilizado por el equipo para transmitir es asignado como *par de recepción* en el *switch*, y el par de recepción en el equipo será el *par de transmisión* en el *switch*.

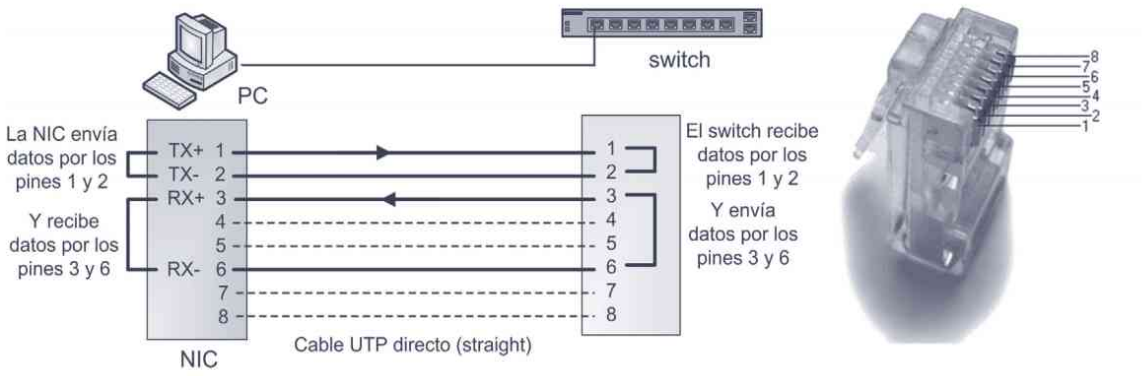


***Figura 9.26**. Conexión entre una NIC y un switch mediante cable UTP*

Los cables UTP utilizados en redes Ethernet con la configuración anterior se conocen como **cable UTP directo**. La mayor parte de los cables utilizados en redes Ethernet siguen esta configuración y se utilizan para conectar un equipo de red (a través de su NIC) a un dispositivo de interconexión, típicamente un *switch*. Sin embargo, existe un caso en el que este tipo de cable no funcionará y es cuando sea necesario conectar dos *switches* entre sí.

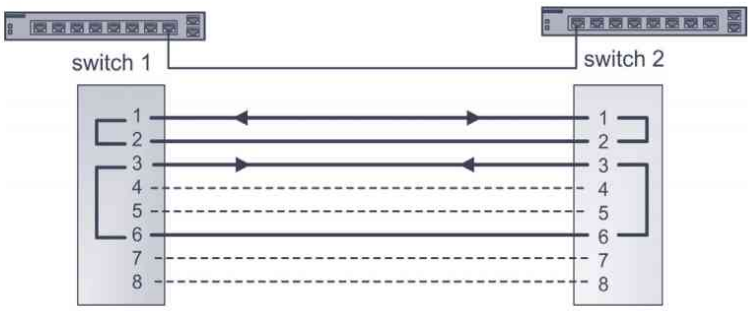


***Figura 9.27**. Conexión entre dos switches utilizando un cable UTP directo*

Como se observa en la figura anterior, al conectar dos *switches* utilizando la configuración de un cable UTP directo, los dos *switches* intentan transmistir por el mismo par (por los pines 3 y 6) por lo que sus datos "colisionarán". Además, intentarán recibir datos por el mismo par (por los pines 1 y 2). Para solucionar este problema se utiliza una configuración llamada **cable UTP cruzado**, que consiste en cruzar los pares de transmisión y recepción.

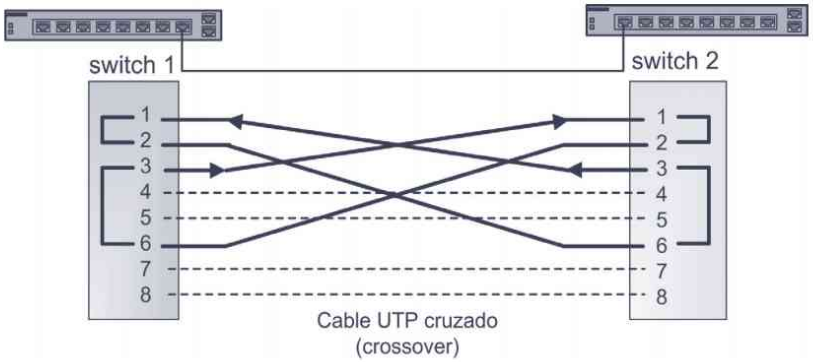


***Figura 9.28**. Conexión entre dos switches utilizando un cable UTP directo*

La configuración de cable UTP cruzado también se puede utilizar para conectar dos tarjetas de red Ethernet directamente sin utilizar un *switch*. Esta característica puede ser útil cuando queramos conectar dos equipos y no tengamos un *switch*.

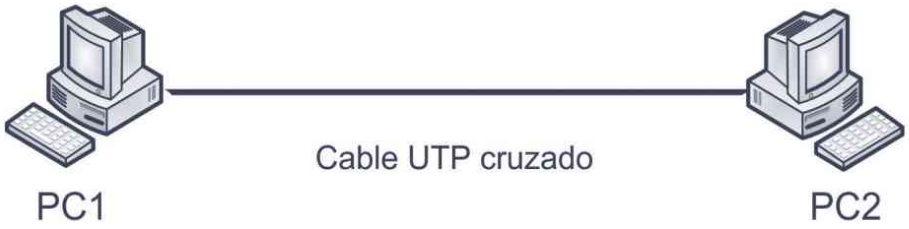


***Figura 9.29**. Conexión entre dos PC utilizando un cable UTP cruzado*

La función de los pares en una tarjeta de red se conoce formalmente como **MDI** (*Medium Dependent Interface*) y la función de los pares en un dispositivos de interconexión como un *switch* (o como en los antiguos *hubs*) se conoce como **MDI-X** (*Medium Dependent Interface Crossover*).

Para evitar el uso de cable UTP cruzado algunos modelos de hubs incluían un puerto especial que podía ser configurado como MDI (si se iba a conectar a otro hub) o como MDIX (si se iba a conectar a un PC). Posteriormente, se han desarrollado puertos que detectan automáticamente que tipo de configuración necesitan para funcionar correctamente con el dispositivo al que esté conectado; esta característica se conoce como **puerto Auto MDI/MDI-X**.

9.11 INTERCONEXIÓN DE DISPOSITIVOS: EL SWITCH O CONMUTADOR

9.11.1 ANTECEDENTES

En las redes actuales el *switch* es el dispositivo utilizado como elemento de interconexión de los equipos que forman parte de las mismas, existiendo una gran variedad de modelos para cubrir todas las necesidades de las redes actuales, tanto de pequeñas redes con unos pocos equipos, como de grandes redes con cientos o incluso miles de equipos.

Sin embargo, su uso no se ha hecho extensivo a prácticamente todas las redes hasta hace unos años cuando su precio permitió utilizarlo de forma masiva. Repasemos brevemente los dispositivos utilizados hasta ese momento.

- **Hub o concentrador**

  En las primeras redes 10BASE-T el dispositivo utilizado como elemento central de interconexión era el *hub* o concentrador. Un *hub* se puede considerar un dispositivo de interconexión de nivel 1 ya que opera exclusivamente en el nivel 1 del modelo OSI. Como ya se ha comentado anteriormente, cuando un *hub* recibe datos por uno de sus puertos lo que hace es simplemente retransmitir esos datos por el resto de los puertos, es decir, lleva a cabo una simple transferencia de niveles eléctricos.

  Con la llegada de la Ethernet conmutada y el abaratamiento de los *switches*, los *hubs* dejaron de utilizarse y, actualmente, prácticamente no se utilizan.

***Figura 9.30**. El modelo de hub 3com Superstack II de 24 puertos fue muy utilizado en redes LAN*

- **Puente (Bridge)**

  Un puente, a diferencia de un *hub*, operaba en el nivel físico y de enlace, por lo que se les considera dispositivos de interconexión de nivel 2. Su función principal era la de dividir una red grande en segmentos más pequeños. Para llevar a cabo esta función los puentes contienen la lógica necesaria para separar el tráfico de cada segmento.

  El rendimiento de las primeras redes Ethernet que utilizaban CSMA/CD dependía en gran medida del número de equipos conectados, ya que cuantos más equipos, más colisiones y más reintentos sucesivos penalizando dicho rendimiento si el número de colisiones era muy elevado. En esta situación se utilizaban los puentes, dividiendo la red en dos segmentos, repartiendo el número de equipos y, por tanto, la carga de datos. Se dice que los puentes reducen **el dominio de colisión**. Un dominio de colisión está formado por todos los equipos que propagan sus tramas por un medio común y que, por tanto, son susceptibles de producir colisión.

No confundir un dominio de colisión con un dominio de difusión. Un **dominio de difusión** está formado por todos los equipos que recibirían una trama de *broadcast* dentro de una red. Los puentes reducen los dominios de colisión pero mantienen los dominios de difusión.

Los puentes normalmente tienen dos puertos, en cada uno de los cuales se conecta un segmento de red. Cuando se recibe una trama por uno de los puertos, el puente lee la trama para obtener la dirección de destino, si dicha dirección se corresponde a un equipo conectado al segmento de red desde el que se envió la trama, ésta no se propaga al otro segmento. Si la dirección de destino se corresponde con un equipo conectado al otro segmento, reenvía la trama por el puerto correspondiente.

La otra gran función de los puentes era de conectar dos redes LAN que utilicen protocolos diferentes en el nivel de enlace, como por ejemplo, Ethernet y Token Ring, aunque en la actualidad esto tampoco sería necesario. Con la aparición de los conmutadores, los puentes han ido progresivamente desapareciendo y actualmente se pueden considerar extinguidos

9.11.2 FUNCIONAMIENTO DE UN SWITCH

Un *switch* es el dispositivo de interconexión utilizado en Ethernet que posibilita el uso de la conmutación Ethernet. Externamente un *switch* es muy similar a un *hub*, y se utiliza en los mismos casos que los *hubs*, es decir, como elemento de interconexión de las redes Ethernet en estrella. Sin embargo, internamente un *switch* es un dispositivo con unas prestaciones muy superiores a los *hubs*.

Aunque el término *switch* tiene su traducción al español, que sería **conmutador**, lo cierto es que apenas se utiliza.

***Figura 9.31**. Moderno switch de 52 puertos (48+4) de la marca D-Link*

Al *switch* se le considera un dispositivo de interconexión de nivel 2, ya que opera tanto en el nivel 1 como en el nivel 2 del modelo OSI. Su funcionamiento es muy similar a un puente multipuerto. Cuando un *switch* recibe una trama por uno de sus puertos, en lugar de redirigir la trama al resto de los puertos como hacen los *hubs*, la reenvia solo al puerto donde está conectado el dispositivo al que va dirigida la trama.

Los *switches* utilizan una sencilla técnica para conocer qué dispositivos están conectados a sus puertos. Esta técnica se basa en almacenar la dirección MAC de los dispositivos y asociar dicha dirección al puerto en el que están conectados. Esta asociación se almacena en una tabla interna en la memoria del *switch*.

Puerto	Dirección MAC
8	00:04:3B:8C:A5:73
3	00:0C:29:95:1F:B1
1	00:17:D8:65:20:03
2	00:09:7D:27:77:A8
4	00:24:98:C2:23:44

La técnica para generar la tabla de direcciones MAC sigue el siguiente procedimiento:

- Inicialmente la tabla estará vacía.

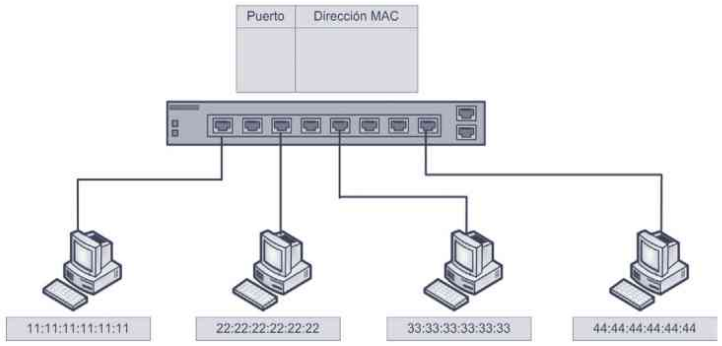


***Figura 9.32**. Estado inicial de un switch con la tabla de direcciones MAC vacía*

- Cuando el *switch* recibe una trama por uno de sus puertos con una dirección de destino que no está en la tabla, reenvía la trama al resto de los puertos (igual que un *hub*).

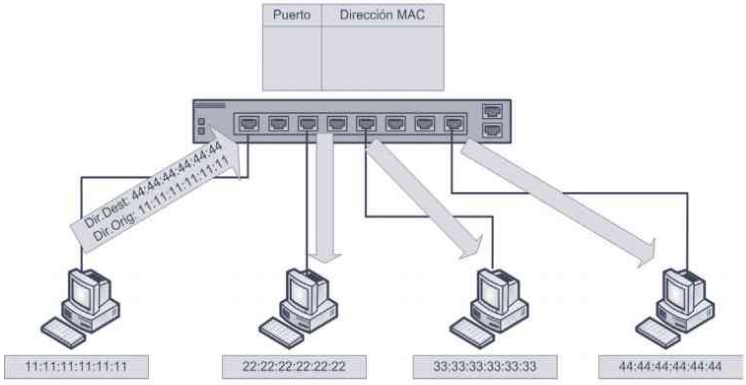


***Figura 9.33**. Reenvío de una trama a todos los puertos*

- Si la dirección origen de una trama no está en la tabla, almacena dicha dirección y el puerto desde el que ha recibido la trama.

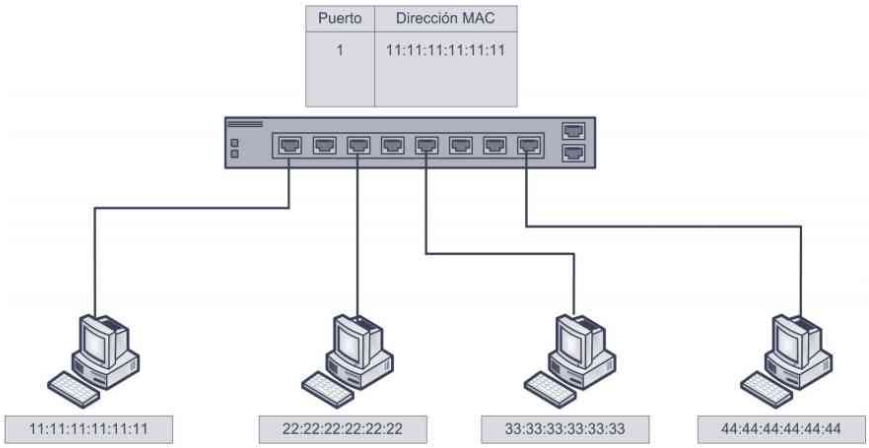


***Figura 9.34**. Almacenamiento de la dirección origen en la tabla*

- Si la dirección destino está en la tabla, envía dicha trama directamente al puerto de destino.

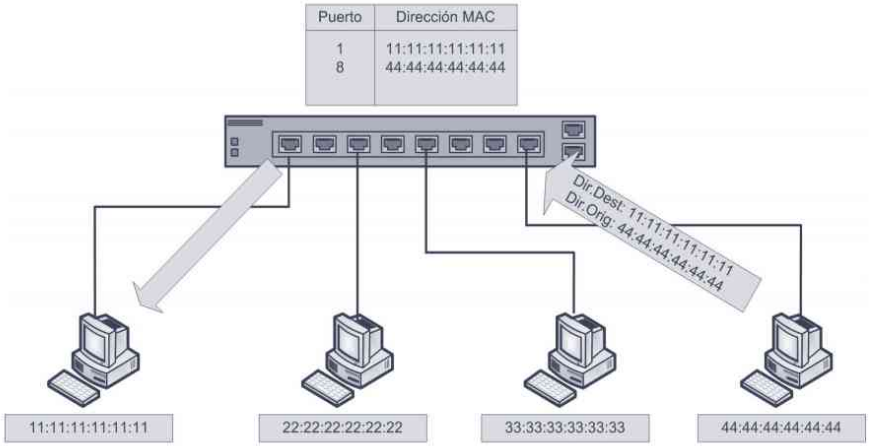


***Figura 9.35**. Reenvío directo al puerto de destino*

- Cada cierto tiempo los datos de la tabla de direcciones se invalidan para actualizar posibles cambios en la topología de la red, por ejemplo, que un dispositivo cambie de puerto.

Esta técnica considera la posibilidad de que exista más de una dirección MAC en un puerto. Esta situación se puede dar cuando lo que hay conectado en el puerto es otro *switch* (o *hub*). Por ello, cuando recibe una trama con una dirección destino que no está en la tabla de direcciones, reenvía la trama al resto de los puertos aunque algunos de ellos ya tuvieran entrada en la tabla.

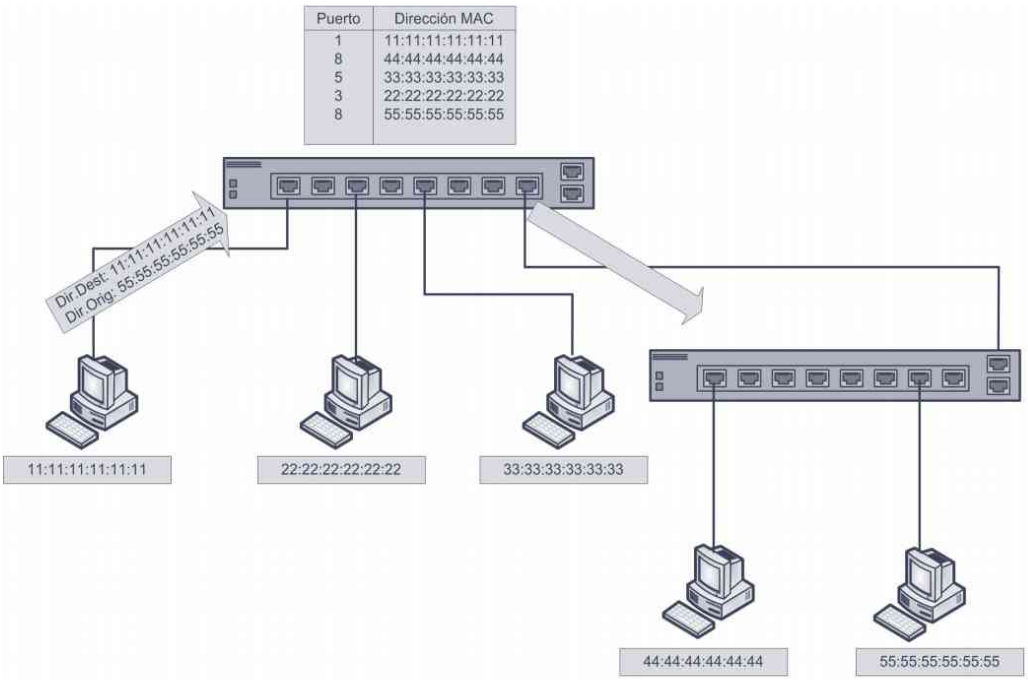


***Figura 9.36**. Tabla de direcciones con varias entradas por puerto*

El reenvío que hace el *switch* de una trama cuando no encuentra la dirección MAC de destino en la tabla de direcciones no se hace realmente como en un *hub*. En los *switches* cada puerto tiene asociado un *buffer* de memoria. Lo que hace el *switch* es copiar la trama a los *buffers* del resto de los puertos. De esta forma nunca habrá más de una trama en ninguno de los enlaces que unen el *switch* y los dispositivos y, por tanto, no habrá colisiones.

Al igual que en los puentes, cada puerto en un *switch* es un dominio de colisión separado, con lo cual no propaga colisiones. Si se conectan equipos a cada uno de los puertos del *switch*, cada equipo forma su propio dominio de colisión. Al igual que los puentes, todos los equipos conectados a un *switch* pertenecen al mismo dominio de difusión.

Una de las características de los *switches*, al igual que en los *hubs*, es el número de puertos que ofrecen para la conexión de los dispositivos a la red. Existen *switches* de 4 y 8 puertos para pequeñas redes domésticas, aunque en entornos más profesionales los valores típicos suelen oscilar entre 24 y 48 puertos. En los próximos apartados se mostrarán algunas de las principales características de los *switches*.

9.11.3 PUERTOS

Uno de los aspectos básicos que define las prestaciones de los *switches* son los puertos, que son los elementos que permiten la conexión del *switch* a otros dispositivos. El primer dato sobre los puertos es su número. En el mercado podemos encontrar *switches* con diferente cantidad de puertos que van desde 4 puertos los más básicos hastas varios cientos de puertos los más sofisticados. Además del número de puertos que proporciona un *switch* conviene tener en cuenta otras características.

Velocidad y medio de transmisión

Dado que Ethernet permite varias velocidades y medios de transmisión, otras de las características destacables sobre los puertos de los *switches* son precisamente la velocidad a la que pueden trabajar y el medio de transmisión utilizado. Podemos encontrar puertos definidos como **10/100**, es decir, que pueden funcionar bajo los estándares 10BASE-T y 100BASE-TX. Otra posibilidad es encontrar puertos **10/100/1000**, es decir, añaden el estándar 1000BASE-T. También se pueden encontrar puertos que utilicen fibra óptica utilizando conectores hembra de algún formato para fibra óptica. Existen puertos 100BASE-FX y 1000BASE-X.

Por último, los *switches* de altas prestaciones pueden ofrecer puertos que cumplan con el estándar 10 GbE, tanto en fibra como en cable UTP.

Funcionamiento *Half/Full-dúplex*

Como se ha visto en los apartados anteriores, el método de acceso al medio CSMA/CD obliga a que las comunicaciones en una LAN sean *half-dúplex*. Sin embargo, el uso de *switches* permite las comunicaciones *full-dúplex*, por lo que el ancho de banda efectivo respecto a redes con *hub* se duplica. Así, una red Fast Ethernet con una velocidad de 100 Mbps aumentará a 200 Mbps utilizando un *switch* que permita el modo *full-dúplex*. Lógicamente, este modo de funcionamiento también lo deben soportar las tarjetas de red de los dispositivos conectados al *switch*. Todos los *switches* fabricados en la actualidad admiten ambos modos. Habitualmente la selección del modo se hace de forma automática negociando con la NIC del equipo conectado al puerto mediante el método de autoconfiguración del estándar IEEE 802.3.

Algunos *switches* admiten la posiblidad de configurar manualmente el modo de transmisión y la velocidad de cada uno de sus puertos.

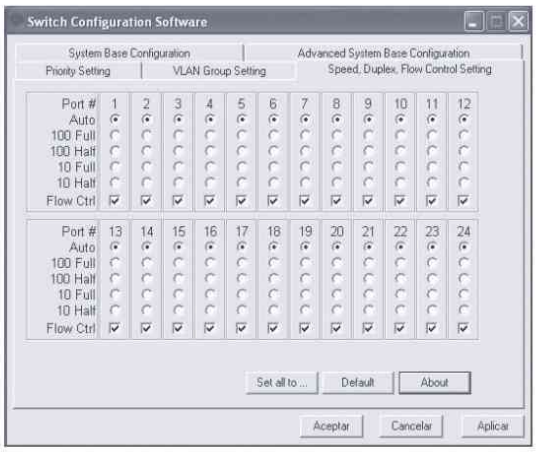


***Figura 9.37**. Configuración por software de los puertos de un switch*

Modo Auto MDI/MDI-X

En el apartado 4.10 se explicaban los dos tipos de configuraciones de cable UTP utilizadas en redes Ethernet. La configuración de cable UTP directo se utiliza para conectar equipos a un *switch*. Pero también existe la configuración de cable UTP cruzado necesaria para conectar dos *switches* entre sí o dos PC entre sí.

Los primeros *hubs* o *switches* tenían puertos especiales que realizaban el ajuste necesario en la asignación de los pines para poder utilizar un cable UTP directo. Este tipo de puertos se conocían como **puertos MDI/MDI-X** o **puertos uplink**.

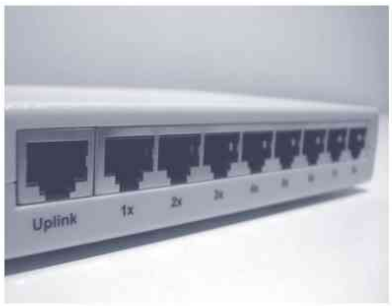


Figura 9.38. *Puerto MDI/MDI-X o uplink en un switch*

En la actualidad, la mayor parte de los *switches* y NIC funcionan con el llamado modo **Auto MDI/MDI-X** que detecta de forma automática el tipo de cable conectado y realiza la asignación conveniente de los pines del conector. De esta forma, si utilizamos un *switch* que esta característica no es necesario tener en cuenta el tipo de cable utilizado en una conexión.

Puertos modulares: GBIC y SFP

La mayor parte de los *switches* de gamas media y alta ofrecen los llamados puertos modulares. Estos puertos realmente no tienen ningún conector específico si no que a ellos se conecta un módulo que contiene el puerto. De esta forma podemos adaptar el puerto al tipo de medio y velocidad que necesitemos. Es habitual que los fabricantes ofrezcan módulos de diferentes tipos con conectores RJ-45 o de fibra óptica. Los puertos modulares proporcionan flexibilidad en la configuración de los *switches*.

Existen dos tipos de módulos para conectar a los puertos modulares: el primer tipo de módulo que apareció es el módulo **GBIC** (*Gigabit Interface Converter*) diseñado para ofrecer flexibilidad en la elección del medio de transmisión para Gigabit Ethernet. Posteriormente apareció el módulo **SFP** (*Small Form-factor Puggable*) que es algo más pequeño que GBIC (de hecho también se denomina **mini-GBIC**) y que ha sido utilizado por los fabricantes para ofrecer módulos tanto Gigabit como 10 GbE en fibra o en cable UTP.

Figura 9.39. *Módulos SFP y GBIC*

9.11.4 BUFFERS

El elemento clave en los *switches* para llevar a cabo el proceso de conmutación son los *buffers*, que son zonas de memoria donde las tramas son almacenadas antes de ser reenviadas al puerto correspondiente. Esta característica, además, permite al *switch* conectar puertos que trabajen a diferentes velocidades.

Los *buffers* pueden ser implementados en la salida de los puertos, en la entrada de los puertos o una combinación de ambos. Lo más habitual es implementarlos en la salida, ya que es el modo más eficiente, consiguiéndose unos índices de eficacia cercanos al 98%.

Los *buffers* se implementan en memorias RAM integradas en la circuitería del dispositivo, como se observa a la siguiente fotografía.

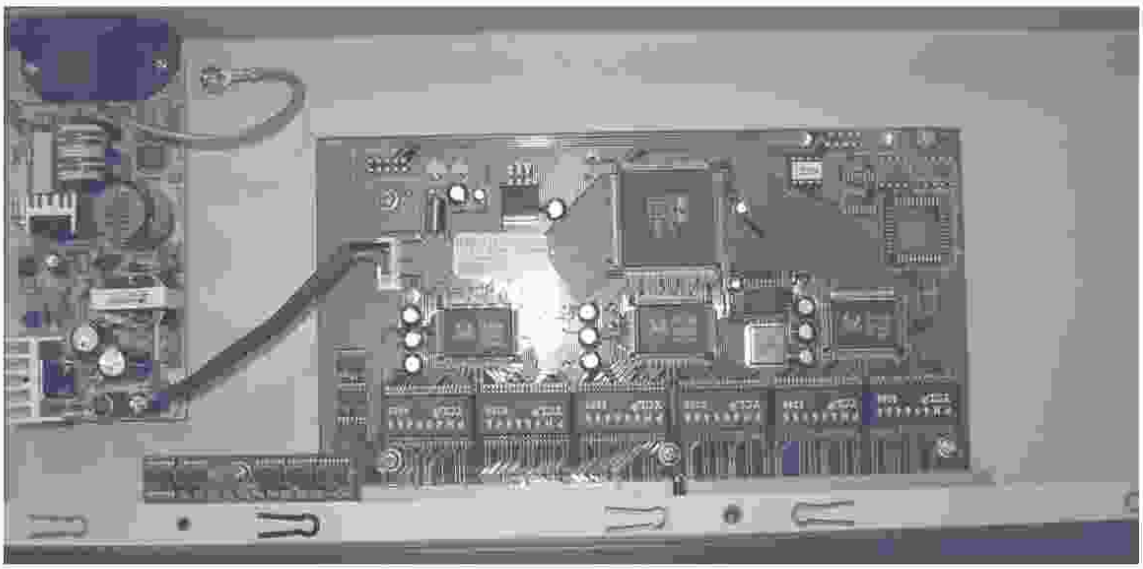


Figura 9.40. *Circuitería de un switch donde se observan los seis chips de memoria para los buffers en la zona inferior*

9.11.5 TÉCNICAS DE CONMUTACIÓN

Existen dos técnicas para llevar a cabo la transferencia de los datos entre puertos de un *switch*:

- **Reenvío directo** (**cut-through**). En esta técnica, cuando un *switch* comienza a recibir datos por un puerto, no espera a leer la trama completa para reenviarla al puerto destino. En cuanto lee la dirección de destino de la trama MAC, comienza a transferir los datos al puerto destino.

  Esta técnica proporciona unos tiempos de retardo bastante bajos, sin embargo, tiene como inconveniente que solo puede usarse cuando las velocidades de todos los puertos son iguales.

  Otro problema que plantea la técnica *cut-through*, debido a su forma de funcionamiento, es que los *switches* propagan tramas erróneas o tramas afectadas por colisiones. Una posible mejora para evitar la propagación de tramas con colisiones es retrasar el reenvío hasta que se lean los primeros 64 *bytes* de trama, ya que las colisiones solo se pueden producir en los primeros 64 *bytes* de la trama. Esta mejora, sin embargo, aumenta el tiempo de retardo.

- **Almacenamiento y reenvío** (*Store and Forward*). En este caso, cuando un *switch* recibe datos por un puerto, almacena la trama completa en el *buffer* para luego reenviarla al puerto destino. La utilización de esta técnica permite realizar algunas comprobaciones de error antes de ser enviada al puerto de destino.

  El tiempo de retardo introducido es variable, ya que depende del tamaño de la trama, aunque suele ser superior al proporcionado por la técnica *cut-through*. Sin embargo, es imprescindible utilizar esta técnica cuando existen puertos funcionando a diferentes velocidades.

9.11.6 CONTROL DE BUCLES: SPANNING TREE

El algoritmo **Spanning tree** (árbol de expansión) se utiliza en los *switches* para prevenir los bucles lógicos que pueden aparecer en una red. Los bucles se producen cuando existen varios caminos distintos entre dos puntos de la red y su efecto es que las tramas pueden circular de forma indefinida atrapadas en un bucle sin conseguir alcanzar su destino, lo que además afectará negativamente al rendimiento de la red. El algoritmo *Spanning tree* ayuda a los *switches* a elegir el camino más idóneo y, por tanto, elimina los bucles.

El uso de este algoritmo está especificado en el estándar **IEEE 802.1D**. En 1998 se hizo una revisión del mismo añadiendo variaciones para optimizar su funcionamiento, el resultado se llamó **Spanning tree rápido** y está especificado en la norma **IEEE 802.1w**.

9.11.7 SEGMENTACIÓN DE TRÁFICO: VLAN

Una de las características más importantes que añaden los conmutadores es la posibilidad de configurar redes LAN virtuales, también llamadas VLAN. El funcionamiento **VLAN** se basa en agrupar los dispositivos conectados al *switch* en subredes virtuales o segmentos VLAN. Dichos segmentos, a todos los efectos, se comportan como subredes diferentes y forman dominios de difusión separados. Un equipo situado en una VLAN determinada no podrá comunicarse con otro equipo situado en otra VLAN diferente, aunque, lógicamente compartan el medio de transmisión o el dispositivo de interconexión. Para poder comunicar dos equipos situados en dos VLAN diferentes será necesario utilizar un dispositivo de interconexión de red de nivel 3, es decir, un *router*. Se dice que los *switches* con la funcionalidad VLAN llevan a cabo una segmentación de la red a nivel lógico.

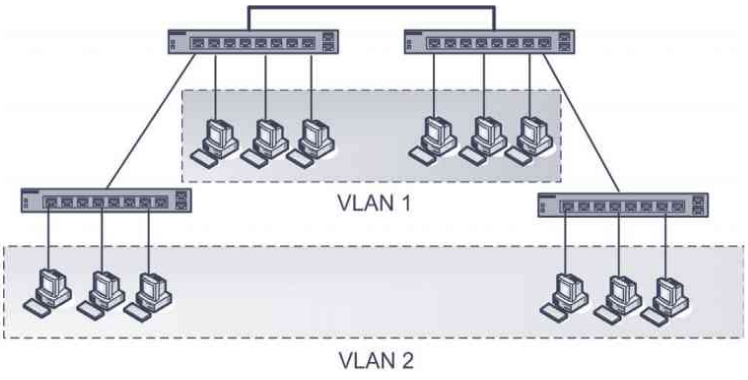


***Figura 9.41**. Ejemplo de VLAN por puerto*

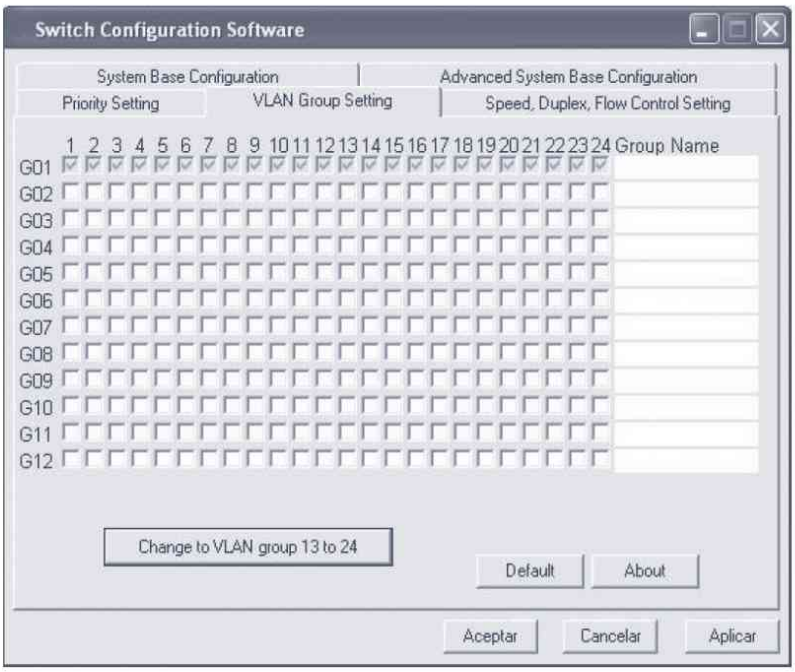


***Figura 9.42**. Software para configurar redes VLAN en un switch*

9.11.8 POWER OVER ETHERNET (POE)

Power Over Ethernet (*Alimentación eléctrica por Ethernet*), también conocido como **PoE**, es una tecnología que permite el envío de alimentación eléctrica junto con los datos en el cableado de una red Ethernet. La primera versión de esta tecnología se publicó en el estándar **IEEE 802.3af** en 2003 y en el año 2009 se publicó una revisión y ampliación en el estándar **IEEE 802.3at**.

La tecnología PoE permite suministrar alimentación eléctrica a dispositivos conectados a una red Ethernet, simplificando por tanto la infraestructura de cableado para su funcionamiento. Un dispositivo que soporte PoE obtendrá tanto los datos como la alimentación por el cable de red Ethernet.

Los dispositivos que utilizan esta característica son puntos de acceso inalámbricos Wi-Fi, cámaras de vídeo IP, teléfonos de VoIP, *switches* remotos y en general cualquier dispositivo que esté conectado a una red Ethernet, que no tenga un consumo energético muy elevado y que su ubicación física dificulte la instalación de cableado. En el estándar PoE se distinguen dos dispositivos:

- **PSE** (*Power Sourcing Equipment*). Son los dispositivos que generan la alimentación que viajará por los cables de datos Ethernet. Hay a su vez dos tipos:
  - **Endspans**, son *switches* Ethernet que incluyen la electrónica para la transmisión de la señal de alimentación eléctrica.
  - **Midspans**, son inyectores de potencia que se ubican entre un *switch* sin PoE y el dispositivo que requiere alimentación por PoE.

- **PD** (*Powered Devices*). Son los dispositivos que reciben alimentación eléctrica mediante la tecnología PoE.

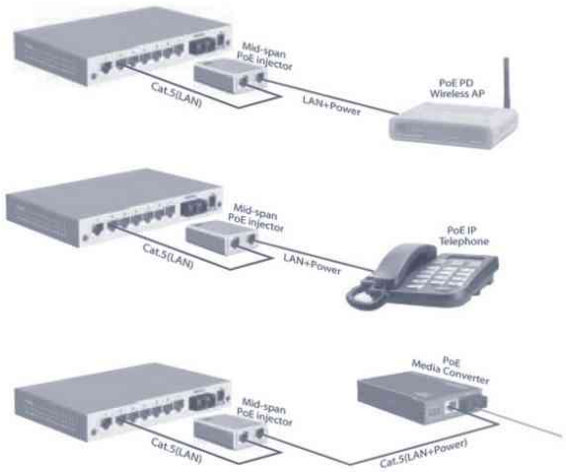


***Figura 9.43**. Inyector de potencia PoE*

El estándar IEEE 802.3at especifica dos tipos de sistemas PoE: Tipos I y II. El Tipo I cumple las características de la primera versión del estándar IEEE 802.3af y el Tipo II es el nuevo sistema PoE con características mejoradas. El siguiente cuadro muestra un resumen de las características de los dos tipos.

	Tipo I (IEEE 802.3af)	Tipo II (IEEE 802.3at)
Categoría mínima de cableado	Categoría 3	Categoría 5
Potencia suministrada por el PSE	15,4 W	30 W
Potencia máxima disponible para el PD	12,95 W	25,5 W
Rango de tensión de salida del PSE	44 – 57 V cc	50 – 57 V cc
Tensión nominal de salida del PSE	48 V cc	53 V cc
Corriente máxima	350 mA por par	600 mA por par

9.11.9 SWITCHES CONFIGURABLES

La función básica que llevan a cabo los *switches* que es la conmutación de tramas Ethernet no necesita ninguna configuración manual. Sin embargo, las funciones avanzadas que ofrecen algunos modelos (como por ejemplo, la configuración de redes VLAN) sí requieren una configuración manual. A los *switches* que proporcionan mecanismos de configuración y gestión se conocen como *switches* gestionables (*managed switches*).

El acceso a la configuración de dichos *switches* se puede hacer bien por un puerto especial de configuración, o por un servicio web interno que proporciona el propio *switch*. En el primer caso, es necesario conectar un PC a dicho puerto y acceder mediante algún software específico (como, por ejemplo, un programa de terminalo de comandos). En el segundo caso basta con utilizar un navegador web en algún PC conectado en un puerto Ethernet del *switch*. El acceso al servicio web interno de gestión del *switch* requiere que se configure en el mismo una dirección IP dentro del rango de la red donde esté conectado.

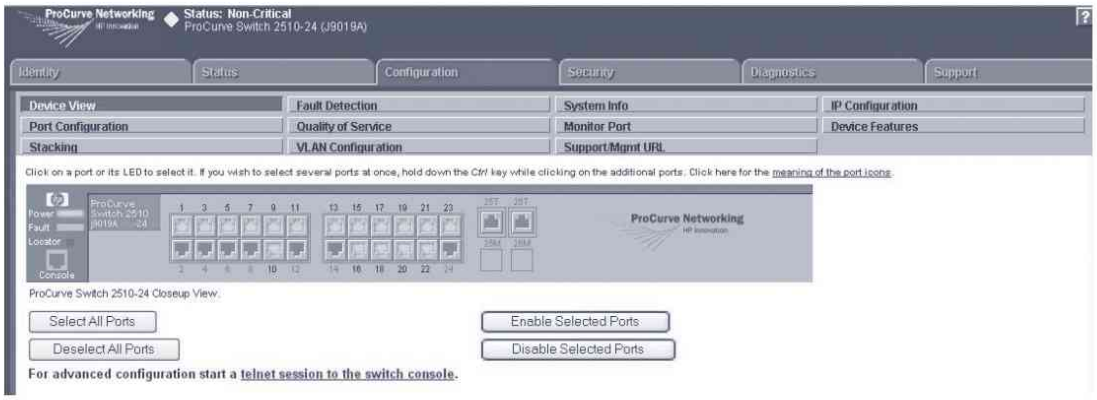


***Figura 9.44**. Configuración de un switch HP mediante el servicio web*

EJEMPLO 9.1

CONFECCIÓN DE LATIGUILLO DE RED

El objetivo es confeccionar un latiguillo de red para ser utilizado en una red Ethernet.

- Para llevar a cabo esta actividad es necesario disponer de cable UTP y de conectores RJ-45, así como de una crimpadora para unir el conector al cable y un alicate de corte.
- Obtener información por Internet para conocer la asignación de pines en el conector RJ-45 para la confección de un latiguillo Ethernet. Recuerde que hay dos posibles configuraciones conocidas como T568A y T568B.
- Antes de insertar los cables al conector deben estar todos los cables bien igualados:

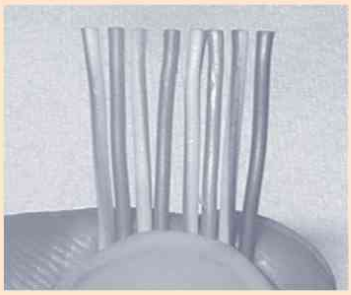


***Figura 9.45**. Igualar bien todos los cables antes de introducirlos en el conector RJ-45*

- Cuidado con la longitud de los cables. No deben quedar los pares fuera del conector:

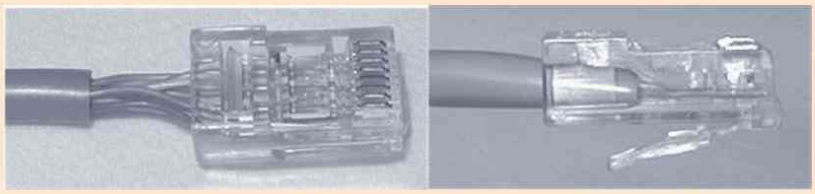


Figura 9.46. *A la izquierda, conexión incorrecta. A la derecha, conexión correcta*

Repetir la actividad pero confeccionando un latiguillo de red cruzado

EJEMPLO 9.2

MEDIR LA VELOCIDAD EN UN ENLACE ETHERNET

- Para llevar a cabo esta actividad se utilizarán dos PC conectados a un *switch* o bien dos PC conectados directamente mediante un cable de red cruzado.
- Se trata de medir la velocidad de transferencia de un archivo entre dos equipos. Para ello se utilizará un programa llamado **LAN Speed Test** que hace uso del servicio de compartir archivos en redes Windows®.
- *LAN Speed Test* es software *freeware* por lo que se puede descargar de Internet sin problema. No requiere instalación.
- Este programa hace un test de velocidad copiando un archivo de prueba en una carpeta compartida de otro equipo (*writing*, escritura) y luego descargando ese mismo archivo (*reading*, lectura). El programa permite seleccionar la carpeta compartida donde se guardará el archivo de prueba, así como el tamaño de dicho archivo.
- Haga tres test con los tamaños 50, 100 y 200 MB y anote los resultados.

IMPORTANTE

Para que LAN Speed Test funcione correctamente es necesario compartir la carpeta utilizada para hacer el test en modo escritura.

RESUMEN DEL CAPÍTULO

Sin ninguna duda, Ethernet es el estándar dominante como tecnología utilizada en las redes locales cableadas. En este capítulo se ha hecho un extenso repaso de sus características más importantes así como de las diferentes versiones que se utilizan de la misma. Todas las funciones que proporciona Ethernet cubren los niveles físico y de enlace del modelo OSI.

En la segunda parte del capítulo se estudia el dispositivo de red más utilizado en las redes locales, que es el *switch*, considerado el dispositivo de interconexión de nivel 2 por excelencia. Así mismo, se repasan tanto su funcionamiento como sus principales características.

EJERCICIOS PROPUESTOS

1. Con un capturador de tramas se ha obtenido la siguiente información, expresada en formato hexadecimal. No se incluye el preámbulo y el *byte* de comienzo de trama.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00	FF	FF	FF	FF	FF	FF	00	00	48	B7	E7	B2	00	2B	E0	E0
16	03	FF	FF	00	28	00	01	00	00	00	00	FF	FF	FF	FF	FF
32	FF	04	53	00	00	00	00	00	00	48	B7	E7	B2	57	FD	00
48	01	FF	FF	FF	FF	00	00	00	00	00	00	00	B3	78	12	C9

¿De qué tipo de trama se trata? Obtener los valores de todos los campos de la cabecera y su función.

2. Repetir el ejercicio anterior con las siguientes capturas:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00	00	A0	C5	38	70	70	00	13	8F	73	76	DA	08	00	45	00
16	00	28	AA	99	40	00	80	06	81	42	0A	0C	02	0D	D4	AA
32	EE	30	09	FE	00	50	BD	B2	FF	5E	7B	EB	A8	89	50	10
64	44	70	B0	9B	00	00	00	00	00	00	00	00	F6	A1	06	BA

- **3.** Obtener información en Internet sobre lo que son las **tramas Jumbo**.
- **4.** Algunos fabricantes de equipos de red ofrecen unos dispositivos llamados **conversores de medios**. Obtener información sobre su función en las redes Ethernet, así como sus principales características. Incluir información de las características de dos modelos concretos de conversores.
- **5.** Buscar en Internet algunos modelos de *switches* e indicar sus principales características. Así mismo, indicar algunos modelos de *switches* que incluyan funciones avanzadas como puertos modulares, VLAN y PoE.

TEST DE CONOCIMIENTOS

1 La conmutación Ethernet se puede utilizar:
- a) Sobre cualquier red 10BASE-T.
- b) Sobre cualquier red Fast Ethernet.
- c) Sobre cualquier red Fast Ethernet o Gigabit Ethernet.
- d) Sobre cualquier red Ethernet que utilice un *switch* en lugar de un *hub*.

2 La dirección MAC de las tarjetas de red Ethernet las configura:
- a) El usuario del equipo.
- b) El administrador de la red.
- c) Cualquier usuario con permisos de administración.
- d) No se puede cambiar.

3 La diferencia entre una trama Ethernet II y una trama IEEE 802.3 es:
- a) El tercer campo de la cabecera es el Tipo en Ethernet, y la Longitud en IEEE 802.3.
- b) No hay diferencia en la trama MAC, la diferencia es que la trama IEEE 802.3 encapsula una trama LLC.
- c) Las direcciones de la trama Ethernet son de 6 *bytes* y en IEEE 802.3 son de 2 *bytes*.
- d) La trama Ethernet necesita una longitud mínima de los datos de 46 *bytes* y la trama IEEE 802.3 no.

4 El modo de operación *full-dúplex*:
- a) No funciona utilizando un *hub*.
- b) No necesita CSMA/CD.
- c) Se puede utilizar tanto en Fast Ethernet como en Gigabit Ethernet.
- d) Todas las respuestas anteriores son correctas.

5 Una de las características de funcionamiento de CSMA/CD es que:
- a) Se pueden configurar los dispositivos con una mayor prioridad de transmisión.
- b) Una señal de congestión indica que se ha borrado la colisión y que los medios no se encuentran ocupados.
- c) Antes de transmitir, un dispositivo escucha y espera hasta que los medios no se encuentren ocupados.
- d) Cuando ocurre una colisión, el dispositivo manda una trama de error a los niveles superiores.

6 Los *switches* utilizan principalmente dos métodos para la conmutación de tramas. ¿Cuál de estos métodos se fija en la dirección de destino y reenvía inmediatamente la trama?
- a) CSMA/CD.
- b) *Full-dúplex*.
- c) *Cut-through*.
- d) *Store and forward*.

7 ¿Cuál de las siguientes es un ejemplo de dirección MAC de nivel 2?
- a) 192.201.63.251
- b) 19-22-01-63-25
- c) 0000.1234.FEG
- d) 00-00-12-34-FE-AA

8 ¿Cuáles de los enlaces siguientes soportan una conexiòn Ethernet *full-dúplex*?
- a) *Switch* a PC.
- b) *Hub* a *hub*.
- c) *Switch* a *hub*.
- d) *Hub* a PC.

9 ¿Cómo funciona un dispositivo de nivel 2 como un *switch*?
- a) Mantiene una tabla con las direcciones IP de los equipos conectados.
- b) Reenvía las tramas cuyo destino no tenga almacenado en la tabla de direcciones a la puerta de enlace.
- c) Comprueba la dirección de destino de la trama en su tabla de la direcciones y envía la trama hacia su destino.
- d) Mantiene la tabla de direcciones del nivel de enlace y del nivel de de red para los equipos conectados con su segmento de red.

10 La conmutación en Ethernet:
- a) Proporciona mayor velocidad a la conexión a Internet.
- b) Permite la conexión de un número mayor de equipos.
- c) Permite el uso del modo *full-dúplex*.
- d) Permite el uso del estándar Gigabit Ethernet.

11 Cuando una tarjeta de red detecta una trama con errores utilizando la información del campo FCS:
- a) Descarta la trama.
- b) Pide la retransmisión de la trama.
- c) Notifica del error al nivel superior.
- d) Gracias a CSMA/CD no puede haber errores.

12 La característica de autonegocación incluida en el estándar IEEE 802.3u permite la negociación automática de:
- a) El tipo de trama.
- b) La velocidad.
- c) El modo de transmisión *half-dúplex* o *full-dúplex*.
- d) Tanto el modo de transmisión como la velocidad.

10.1 INTRODUCCIÓN

En los dos capítulos anteriores se han estudiado las dos tecnologías utilizadas en redes LAN para cubrir las funciones del nivel 1 (nivel físico) y del nivel 2 (nivel de enlace) del modelo OSI. Dichas tecnologías son Ethernet para redes cableadas y Wi-Fi para redes inalámbricas.

Este capítulo se dedicará a exponer el resto de niveles utilizados en las redes actuales. A partir del nivel 3 (nivel de red) ya no hablaremos de tecnologías, sino más bien de protocolos y, por tanto, el conocimiento de los niveles superiores supone el conocimiento de los protocolos utilizados en dichos niveles. Entre ellos, posiblemente el más importante de todos sea el protocolo IP. Junto a éste aparecen otros protocolos utilizados actualmente en las redes como TCP, UDP, ARP, ICMP. El uso de estos protocolos no se limita a las redes LAN, sino que se utilizan en todo tipo de redes. Además, al final del capítulo se incluye un apartado sobre la nueva versión del protocolo IP, conocido como IPv6.

10.2 ARQUITECTURA TCP/IP

En la arquitectura TCP/IP realmente no existe un modelo de red dividido en niveles, fundamentalmente porque su diseño se enfocó a implementar protocolos que solucionasen los requisitos de interconexión que se plantearon en su desarrollo inicial, y para ello no se partió de ningún modelo concreto. Así pues, el modelo en niveles de la arquitectura TCP/IP es un intento de acercamiento al modelo OSI y se puede considerar solo como una descripción de los protocolos existentes.

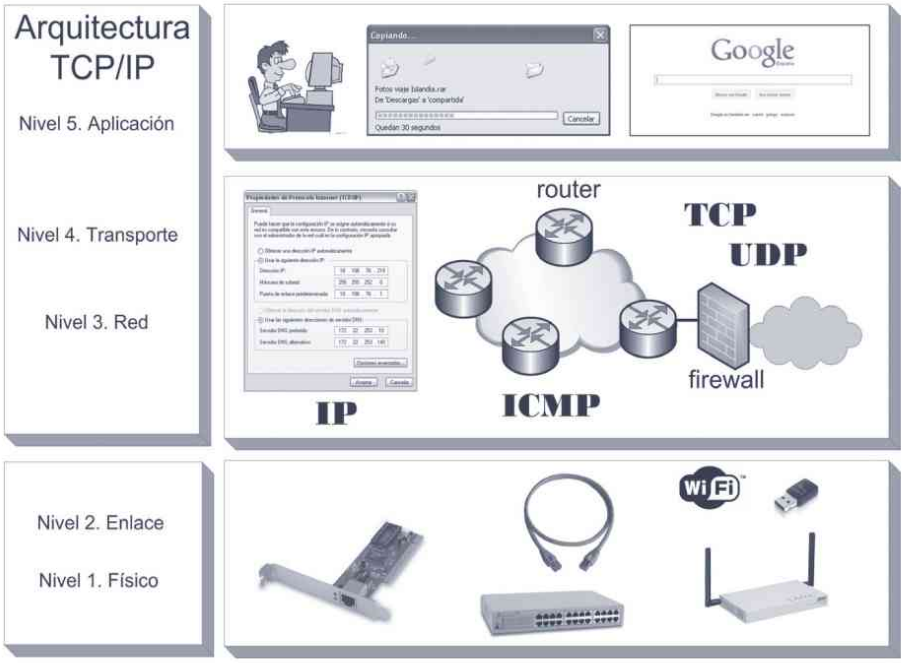


Figura 10.1. *Comparativa de niveles entre el modelo OSI y la arquitectura TCP/IP*

10 TCP/IP

OBJETIVOS DEL CAPÍTULO

- ✓ Asociar el modelo OSI con la arquitectura TCP/IP.
- ✓ Conocer las principales características de los protocolos que forman parte de la arquitectura TCP/IP como son IP, ARP, ICMP, TCP y UDP.
- ✓ Entender el mecanismo para establecer subredes.
- ✓ Conocer cómo configurar los prámetros de red en los equipos.
- ✓ Conocer los principales protocolos utilizados en el nivel de aplicación en TCP/IP.
- ✓ Conocer las principales características de direccionamiento del nuevo protocolo IPv6.

Aunque en el Capítulo 7 se hizo una comparación en la que los modelos OSI y TCP/IP parecían muy similares, la siguiente figura se acerca más a la realidad.

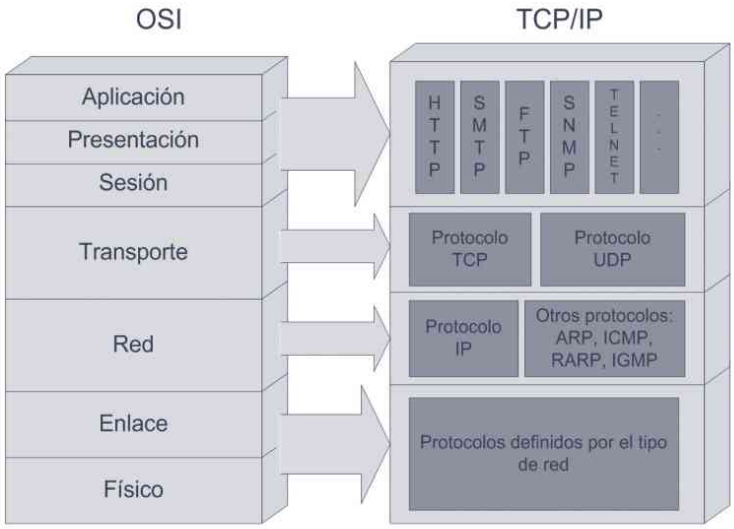


***Figura 10.2**. Comparativa de niveles entre el modelo OSI y la arquitectura TCP/IP*

El modelo TCP/IP no diferencia los niveles físico y de enlace. Los protocolos TCP/IP propiamente dichos comienzan en el nivel 3, de forma que se puede utilizar cualquier protocolo y cualquier tecnología en estos niveles inferiores. Posiblemente éste sea uno de los factores que más ha ayudado a la expansión de la arquitectura TCP/IP.

Como se observa, el grueso de la arquitectura se encuentra en los equivalentes a los niveles de red y de transporte, los cuales curiosamente cubren prácticamente las mismas funciones que sus homónimos en el modelo OSI. A partir de ahí, todo pertenece al nivel de aplicación.

También se puede establecer un cierto paralelismo con el modelo OSI, en la forma en la que se pasan los datos entre los diferentes niveles en la arquitectura TCP/IP. Como ocurre en el modelo OSI, los dispositivos de interconexión solo implementan funciones hasta el nivel de red. Por lo tanto, dichos dispositivos de interconexión no necesitan implementar la complejidad del protocolo de transporte, encargado de proporcionar fiabilidad a la comunicación. Esto tiene una importante consecuencia, las comunicaciones intermedias entre nodos de la red (normalmente llevadas a cabo por los llamados encaminadores o *routers*) son relativamente fáciles de hacer y esto proporciona eficacia y rapidez a las operaciones de encaminamiento de datos, algo que también ha sido crucial en el desarrollo de esta arquitectura.

Todas las especificaciones técnicas sobre los protocolos y procedimientos usados en Internet se publican en unos documentos llamados **RFC** (*Request For Comment*), que se pueden obtener en *www.ietf.org*. Muchos de estos documentos están traducidos al español en *www.rfc-es.org*.

10.3 PROTOCOLO DE RED IP

El principal protocolo que utiliza la arquitectura TCP/IP en el nivel de red es el **protocolo IP** (*Internet Protocol*). IP es un protocolo del nivel de red no orientado a conexión, basado en datagramas y no fiable.

- Se dice que un protocolo está **basado en datagramas** cuando la información que debe transmitir se divide en fragmentos. Por lo tanto, cada uno de los paquetes o fragmentos de información que transporta IP se le denomina *datagrama*.
- IP es un protocolo **no orientado a conexión**, es decir, no se establece un camino previamente, con lo cual cada datagrama viaja de forma independiente pudiendo llegar al destino fuera de secuencia o duplicado. No se crean circuitos virtuales.
- Y, además, es un protocolo **no fiable**, es decir, no ofrece comprobaciones ni seguimientos. IP intenta que los datos lleguen a su destino lo mejor que puede pero sin ofrecer garantías.

RECUERDA

La unidad básica de información en el nivel 2, o nivel de enlace, se denomina **trama**. La unidad básica de información en el nivel 3, o nivel de red, es el **datagrama**.

Se puede comparar IP con el servicio de correo postal donde, al igual que en IP, no se realiza ningún seguimiento de que una carta se reciba correctamente. Deben ser el remitente o el destinatario los que estén pendientes de que el envío llegue correctamente.

Si se necesita llevar a cabo una comunicación fiable utilizando IP, es necesario añadir otro protocolo que le dé fiabilidad a la transmisión; este protocolo es TCP en la arquitectura TCP/IP. Del mismo modo, para dar más fiabilidad a la entrega del correo postal, se puede utilizar el envío postal con acuse de recibo. En esta modalidad, cuando la carta llega a su destino, se envía un acuse de recibo al remitente. Si no se recibe acuse de recibo, el remitente puede suponer que la carta no llegó correctamente y volver a enviarla.

Aunque pueda parecer que IP es un protocolo con carencias, realmente no es así. Este funcionamiento permite gran flexibilidad para implementar los servicios en los niveles superiores.

La versión actualmente implantada en la mayor parte de los sistemas es la versión 4, conocida como IPv4. Sin embargo, algunas limitaciones de la versión 4 llevaron al desarrollo de la versión 6 (hay una versión 5 experimental no utilizada de forma comercial). La versión 6 de IP, conocida como **IPv6** (en sus inicios también fue conocida como **IPng** de *IP Next Generation*), fue adoptada por el organismo encargado de la publicación de los estándares en Internet llamado **IETF** (*Internet Engineering Task Force*) en 1994.

Hasta ahora el nuevo protocolo IPv6 apenas ha sido utilizado, aunque el agotamiento de las direcciones IPv4 está obligando a empezar a utilizarlo de forma cada vez más masiva. Más adelante en este tema se expondrán las principales características de esta nueva versión del protocolo IP.

10.3.1 DATAGRAMA IPV4

La transmisión de los datos en el nivel de red utilizando el protocolo IP se realiza en unidades de información llamadas **datagramas**. Como es de suponer, un datagrama consta de dos partes, una cabecera y los datos. La longitud de un datagrama es variable, pudiendo alcanzar un tamaño máximo de 65.535 *bytes*. A continuación se muestra la estructura de un datagrama IP. Los números mostrados en la parte inferior de la figura son los tamaños de los campos de la cabecera expresados en bits.

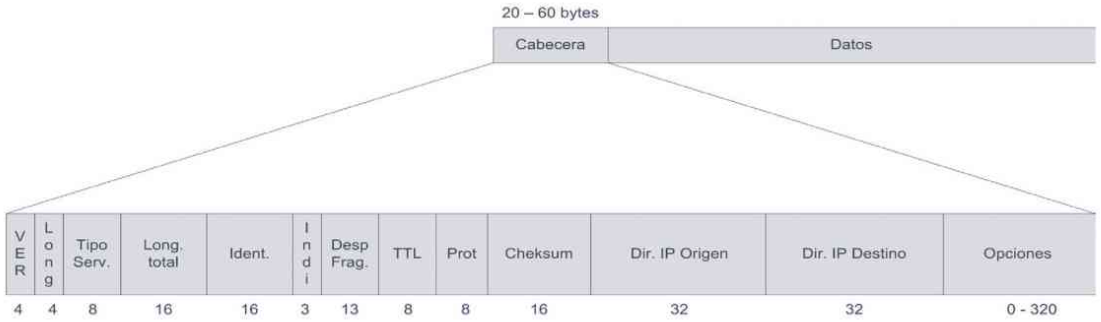


***Figura 10.3**. Datagrama IP*

La descripción de cada uno de los campos es la siguiente:

- **Versión**. Se incluye la versión del protocolo IP. Actualmente, la mayor parte de las redes utiliza la versión 4, por tanto, este campo contiene el valor 4 en binario: 0100.
- **Longitud de la cabecera**. La cabecera de un datagrama IP no tiene un tamaño fijo. Su longitud puede estar entre 20 y 60 *bytes*. En este campo se define la longitud de la cabecera en un valor múltiplo de 4, es decir, el valor almacenado en este campo se multiplica por 4 para obtener el número total de *bytes* de la cabecera.
- **Tipo de servicio** (**actualmente ECN**). En la especificación original de IP este campo se utilizaba para incluir información sobre el nivel de retardo, fiabilidad y prestaciones, en función del tipo de servicio que se estuviera utilizando. En la práctica este campo apenas ha sido utilizado, de forma que el IETF redefinió su uso como **ECN** (*Explicit Congestion Notification*), utilizado para enviar información sobre congestión de la red (RFC 3168 publicado en 2001).
- **Longitud total**. Almacena la longitud total del datagrama IP incluyendo la cabecera y los datos. Es un campo de 16 bits por lo que puede almacenar hasta una longitud de 65.535 *bytes*.

IMPORTANTE

Aunque la longitud máxima que admite el protocolo IP es de 65.535 *bytes*, en la práctica el tamaño del datagrama IP utilizado en las redes suele ser bastante inferior y depende de la tecnología de red empleada en los niveles inferiores. Esto es así para evitar la fragmentación de los datagramas, lo que ocasionaría una importante pérdida de rendimiento.
El tamaño máximo en *bytes* de la unidad de datos que un protocolo puede procesar se conoce como **MTU** (*Maximum Transfer Unit*). El tamaño máximo del datagrama IP suele adaptarse a la MTU del nivel de enlace. Así, en redes Ethernet donde el tamaño máximo de la trama es de 1.518 *bytes* se establece el tamaño máximo del datagrama IP en 1.500 *bytes*.

- **Identificación**. Este campo se utiliza para enumerar los datagramas fragmentados. La fragmentación de un datagrama IP se produce cuando la MTU de una red es menor que la de la red en la que originó el datagrama. Por las características propias de IP, los datagramas fragmentados pueden llegar con un orden diferente con el que se enviaron por lo que esta numeración es necesaria.
- **Indicadores**. Campo formado por tres bits:
  - El primer bit es de uso reservado y debe ser 0.
  - El segundo bit se llama **DF** (*Don't Fragment*) y se activa a valor 1 para indicar que el datagrama no puede fragmentarse. En caso contrario su valor será 0.
  - El último bit se llama **MF** (*More Fragments*) y su valor debe ser 1 para indicar que el datagrama está fragmentado y aún faltan más fragmentos por enviarse. Cuando su valor es 0 indica que es el último fragmento. En el caso de que sea un datagrama sin fragmentación su valor es también 0.
- **Desplazamiento del fragmento**. Este campo se utiliza para indicar el desplazamiento de los datos incluidos en el datagrama fragmentado respecto al datagrama original.
- **TTL** (*Time To Live*, Tiempo de vida). Este campo es un número que indica el número de saltos que el datagrama puede realizar antes de ser descartado. Cuando se crea el datagrama se asigna a este campo un valor inicial (normalmente 127). Un salto se produce cuando el datagrama cambia de red, esto lo lleva a cabo un *router*. El *router* es el que decrementa el valor de este campo en una unidad. Si el valor del campo llega a cero, el datagrama se descarta. Este funcionamiento se utiliza para evitar que los datagramas permanezcan de forma indefinida en la red.
- **Protocolo**. Este campo es un identificador del protocolo de nivel superior utilizado. Los valores más comunes son: TCP (6), UDP (17) o ICMP (1).
- **Cheksum o suma de comprobación**. Este campo se utiliza para la detección de errores en la cabecera. Para su cálculo no se tiene en cuenta los datos. Los errores de los datos deben ser detectados por los niveles superiores.

El código *checksum* se calcula de forma más sencilla que el CRC. Simplemente se efectúa la suma aritmética de los datos ajustando el resultado para representarlo con 16 bits.

- **Dirección lógica de origen**. Este campo identifica el dispositivo de red del que parte el datagrama. El formato de la dirección lógica utilizado en IP se especifica en el siguiente apartado.
- **Dirección lógica de destino**. Este campo identifica el dispositivo de red al que va dirigido el datagrama.
- **Opciones**. Este campo se puede utilizar para enviar información adicional en la cabecera del datagrama aunque se utiliza con poca frecuencia.

10.3.2 DIRECCIONAMIENTO IPV4

Una de las principales funciones del nivel de red es el llamado direccionamiento lógico. Este direccionamiento lógico se utiliza para definir un identificador para cada dispositivo de la red pero teniendo en cuenta la jerarquía necesaria en la arquitectura de las redes.

Por lo tanto, en el protocolo IP, cada dispositivo debe tener asignada una dirección lógica conocida también como **dirección de red** o **dirección IP**. Dicha dirección IP está formada por 32 bits (4 *bytes*) y consta de tres campos de longitud variable dependiendo del tipo de red a la que pertenezca la dirección. Estos campos son la clase, el identificador de red y el identificador de *host*.

Debido a la incomodidad que supone trabajar con direcciones IP en formato binario utilizando 32 bits, se ha definido una notación más práctica para representar dichas direcciones y que se conoce como **notación punto-decimal**. La representación en dicha notación simplemente consiste en agrupar los bits en grupos de ocho y representar cada grupo en notación decimal en lugar de binaria. Se utiliza el punto (.) para separar cada grupo.

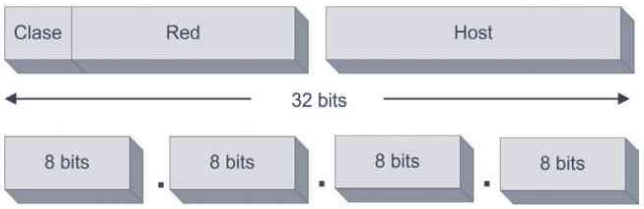


***Figura 10.4**. Dirección IP jerárquica y notación punto-decimal*

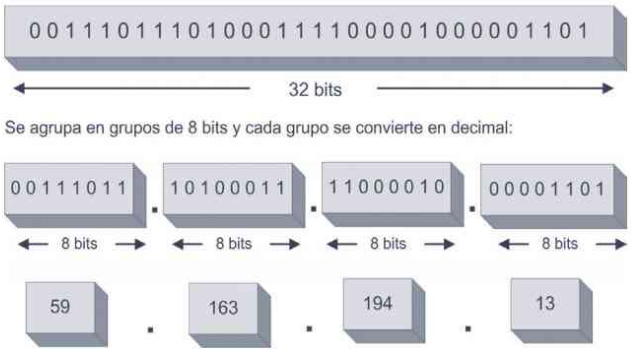


***Figura 10.5**. Ejemplo de dirección IP en formato punto-decimal*

Como se observa, cada número decimal de una dirección IP realmente representa un número binario de 8 bits, por lo tanto, el rango válido de números que pueden aparecer en una dirección IP es del 0 al 255. A cada uno de estos números decimales que forman una dirección de red le denominaremos **octeto**.

La principal diferencia del direccionamiento lógico respecto al direccionamiento físico es que el primero es un direccionamiento jerárquico, donde una parte de la numeración se utiliza para identificar la red y otra parte para identificar el *host* dentro de la red.

Además de la jerarquía utilizada en las direcciones IP para identificar la red y los *host* dentro de cada red, fue necesario definir otro concepto conocido como *clase*. Las **clases** se definieron en el protocolo IP para optimizar el uso

del enrutamiento de los datagramas, ya que no usar clases hubiera supuesto que los *routers* deberían almacenar una gran cantidad de información en sus tablas de encaminamiento, lo cual hubiera sido negativo para el funcionamiento de las redes. Se establecieron varios tipos de redes, es decir, de clases, para cubrir las necesidades de los diferentes tipos de organizaciones, ya que cada clase permite un máximo de direcciones IP en cada red que pertenezca a dicha clase.

Las clases que se definieron en el protocolo IP son:

- **Clase A**. En esta clase, el bit más significativo de la dirección IP vale siempre 0. Se utilizan 7 bits para identificar la red y el resto de bits, es decir, 24, se utilizan para identificar un *host* dentro de la red.
- **Clase B**. En este caso, el valor de los dos primeros bits de la dirección es siempre 10. Se utilizan 14 bits para identificar la red y 16 bits para identificar un *host* dentro de la red.
- **Clase C**. En este caso, el valor que se utiliza en los tres primeros bits para asignar la clase C es el 110. Se utilizan 21 bits para identificar la red y 8 bits para identificar un *host* dentro de la red.
- **Clase D**. Esta clase se identifica por contener en los cuatro primeros bits el valor 1110 y se utiliza para establecer direcciones de multienvío.
- **Clase E**. Identificada por sus primeros 4 bits tiene el valor 1111. Estas direcciones están reservadas inicialmente para usos futuros aunque en la práctica nunca se ha llegado a definir ningún uso para estas direcciones.

El resumen del direccionamiento se puede ver en la siguiente figura:

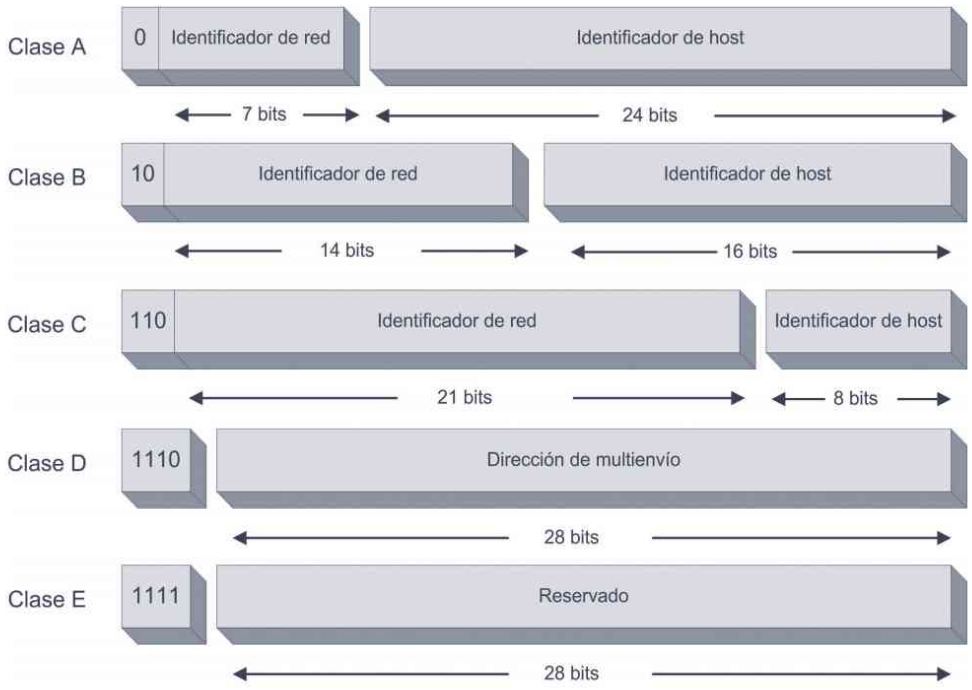


***Figura 10.6**. Las clases en el direccionamiento IP*

Según la definición de las clases, un *host* dentro de una red tendrá asignada una dirección IP que pertenecerá alguna de las tres primeras clases, es decir, las clases A, B y C. Es decir, para llevar a cabo la asignación de direcciones IP en una red, dicha red debe pertenecer a alguna de estas tres clases.

La figura anterior muestra de qué manera se identifica cada una de las clases basándose en el formato binario pero, en la práctica, las direcciones IP se representan utilizando la notación punto-decimal. Por ejemplo, a continuación se indican tres direcciones IP representadas, lógicamente, en notación punto-decimal:

64.54.126.45 188.12.3.4 215.63.10.15

Con la información que tenemos sobre las clases no podemos deducir de forma inmediata a qué clase pertenece cada una de estas direcciones. Habría que pasar al menos el primer octeto a formato binario para conocer el valor de los primeros bits. Sin embargo, es mucho más práctico conocer los valores de ese primer octeto en notación decimal para cada una de las clases.

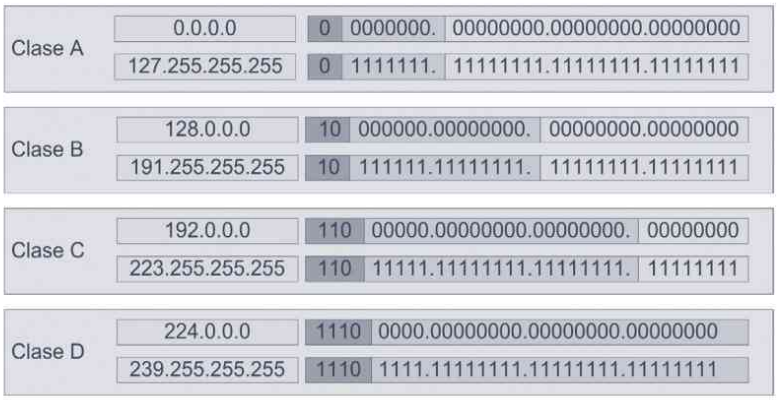


***Figura 10.7**. Los rangos de las clases*

En definitiva, para identificar a qué clase pertenece una dirección IP solo es necesario fijarse en el primer octeto de la dirección IP. Con la tabla anterior ya sí es inmediato identificar a qué clase pertenece cada una de las direcciones anteriores. La primera pertenece a una red de clase A ya que el primer octeto es el 64. La segunda es de clase B, ya que su primer octeto es el 188. Y la tercera pertenece a una red de clase C, ya que el primer octeto de la dirección es el 215.

También es conveniente conocer las capacidades teóricas de cada una de las clases:

- Puede haber un máximo de 128 (2^7) redes de clase A. Cada red de clase A puede contener un máximo de 16.777.216 (2^{24}) *hosts*.
- Puede haber un máximo de 16.384 (2^{14}) redes de clase B. Cada red de clase B puede contener un máximo de 65.536 (2^{16}) *hosts*.
- Puede haber un máximo de 2.097.152 (2^{21}) redes de clase C. Cada red de clase C puede contener un máximo de 256 (2^8) *hosts*.

Lógicamente, los diseñadores del protocolo IP nunca esperaron el espectacular desarrollo de su tecnología y, aunque en el momento de su desarrollo este esquema de direccionamiento parecía más que suficiente para proporcionar direcciones lógicas a todos los dispositivos, cuando empezó el crecimiento de Internet pronto se dieron cuenta que dicho esquema de direccionamiento era poco eficiente.

Por último, es importante destacar que el protocolo define una serie de **direcciones IP reservadas** para otras funciones y que no se pueden utilizar como direcciones para *hosts*. La siguiente tabla muestra dichas direcciones:

X. 0. 0. 0	Dirección de red de una red de clase A.
X. X. 0. 0	Dirección de red de una red de clase B.
X. X. X. 0	Dirección de red de una red de clase C.
X.255.255.255	Dirección de difusión de una red de clase A.
X. X.255.255	Dirección de difusión de una red de clase B.
X. X. X.255	Dirección de difusión de una red de clase C.
0. 0. 0. 0	Dirección utilizada para referirse al propio equipo en las tablas de encaminamiento internas de los equipos.
127. 0. 0. 1	Dirección de loopback o de bucle local. Utilizada habitualmente para hacer pruebas de protocolos superiores.

En la especificación de la dirección en la tabla anterior, el símbolo X representa un valor cualquiera entre 0 y 255, que es el rango válido en la notación punto-decimal.

Las **direcciones de difusión**, también llamadas de **broadcast**, se utilizan para llevar a cabo envíos simultáneos a todos los dispositivos de una red. Las direcciones de difusión solo se pueden utilizar como direcciones destino en un datagrama IP.

La dirección de red se utiliza especialmente en los *routers* para identificar una red. Se podría decir que esa dirección reservada sirve para nombrar la red. Por ejemplo, la dirección IP 188.12.3.4 estaría asignada a un *host* que pertenece a la red 188.12.0.0, que es una red de clase B.

RECUERDA

Cuando en una dirección IP todos los bits reservados para identificar los equipos de una red están a cero, esa dirección no se refiere a ningún equipo, sino que es la **dirección de la red**. Y cuando están a uno, esa dirección es la **dirección de broadcast** o de difusión de la red.

10.3.3 SUBREDES

Como hemos visto, las direcciones IP incluyen dos niveles jerárquicos, por lo que cada dirección de red utiliza una parte para identificar la red y otra parte para identificar un equipo o *host* dentro de la red.

El protocolo IP permite, además, la utilización de un tercer nivel de jerarquía entre los dos niveles jerárquicos definidos por defecto; es el **nivel de subred**. Esta característica se utiliza cuando una organización, que tiene asignado un rango de direcciones IP (públicas o privadas), necesita organizar de forma interna el uso de dichas direcciones.

***Figura 10.8**. Jerarquía de una dirección IP con subredes*

Para ello, se aplica una técnica llamada **enmascaramiento**, que es el proceso por el cual se puede obtener la dirección de red o de subred de una dirección IP dada. El enmascaramiento se puede aplicar tanto en redes que utilicen subredes como en redes que no las utilicen. De hecho, actualmente, y para ofrecer un método homogéneo del tratamiento de las direcciones de red, se aplica siempre el enmascaramiento.

Para utilizar esta técnica se define un parámetro llamado **máscara de subred**, o simplemente **máscara**. La máscara es un número de 32 bits que define qué bits de una dirección IP se utilizan para identificar la red o subred y qué bits se utilizan para identificar el *host*. Lógicamente, el valor de la máscara estará condicionado por la clase a la que pertenezca la dirección de red. Los bits que identifican la red o subred toman el valor 1 en la máscara. Los bits que identifican el equipo toman el valor 0 en la máscara.

Las máscaras utilizadas para redes que no utilizan subredes están acordes con las características de las clases utilizadas.

Clase	Máscara	Máscara en binario
Clase A	255.0.0.0	11111111.00000000.00000000.00000000
Clase B	255.255.0.0	11111111.11111111.00000000.00000000
Clase C	255.255.255.0	11111111.11111111.11111111.00000000

Cuando se utilizan subredes, la máscara especifica cuántos bits de la dirección IP se utilizan para la red y la subred.

EJEMPLO 10.1

CÁLCULO DE SUBREDES

Una empresa tiene reservada para su uso la dirección de clase B 180.30.0.0. Esto le permite utilizar hasta 65.534 direcciones de *hosts* diferentes. Al ser un número elevado de direcciones, y por razones de organización, puede crear subredes. El número máximo de subredes que se pueden crear depende de la máscara elegida y debe ser potencia de dos, es decir, 2, 4, 8, 16, 32...

Se decide utilizar una máscara que permita crear hasta ocho subredes. Se debe, por tanto, añadir tres "*unos*" a la máscara original sin subredes para clase B. Para la clase B, la máscara es 255.255.0.0. Para llevar a cabo este proceso es más sencillo utilizar la notación binaria:

Máscara para una red de clase B: 11111111.11111111.00000000.00000000

Para el uso de ocho subredes se añaden tres "*unos*" a la máscara y se pasa de nuevo a notación punto-decimal.

Máscara en formato binario: 11111111.11111111.**111**00000.00000000

Máscara en notación punto-decimal: 255.255.224.0

Las direcciones de las subredes definidas en el ejemplo serían:

Dirección de subred	Dirección de red	Subred	Hosts
180.30.0.0	10110100.00011110.	000	00000.00000000
180.30.32.0	10110100.00011110.	001	00000.00000000
180.30.64.0	10110100.00011110.	010	00000.00000000
180.30.96.0	10110100.00011110.	011	00000.00000000
180.30.128.0	10110100.00011110.	100	00000.00000000
180.30.160.0	10110100.00011110.	101	00000.00000000
180.30.192.0	10110100.00011110.	110	00000.00000000
180.30.224.0	10110100.00011110.	111	00000.00000000

Para obtener la dirección de subred a partir de una dirección de red y una máscara se sigue el siguiente procedimiento:

- Los *bytes* de la dirección IP que se correspondan con el número 255 en la máscara se repiten en la dirección de la subred.
- Los *bytes* de la dirección IP que se correspondan con 0 en la máscara se cambian por un 0 en la dirección de la subred.
- Para números diferentes a 0 y 255 se aplica el operador AND entre el *byte* de la dirección IP y el *byte* de la máscara.

EJEMPLO 10.2

OBTENER LA DIRECCIÓN DE SUBRED DE UNA DIRECCIÓN IP

En los siguientes ejemplos se obtienen las direcciones de subred y de red de una dirección IP y su máscara:

Ejemplo 1

Dirección IP: 79.199.217.111
Máscara de subred: 255.255. 0. 0

La dirección IP pertenece a una red de clase A con subredes

Dirección de subred: 79.199.0.0

Dirección de red: 79.0.0.0

Se pueden definir hasta 256 subredes con 65534 host cada subred

Ejemplo 2

Dirección IP: 133.210. 51. 8
Máscara de subred: 255.255.255. 0

La dirección IP pertenece a una red de clase B con subredes

Dirección de subred: 133.210.51.0

Dirección de red: 133.210.0.0

Se pueden definir hasta 256 subredes con 254 host cada subred

Ejemplo 3

Dirección IP: 200. 45. 67. 77
Máscara de subred: 255.255.255.192

La dirección IP pertenece a una red de clase C con subredes

Cálculo del cuarto octeto de la dirección de subred
77 01001101
192 11000000 AND
64 01000000

Dirección de subred: 200.45.67.64

Dirección de red: 200.45.67.0

Se pueden definir hasta 4 subredes con 62 host cada subred

10.3.4 ARQUITECTURA IP

El direccionamiento IP permite disponer de rangos de direcciones asignados a diferentes redes interconectadas entre sí. Para poder interconectar dos o más redes es necesario el uso de un dispositivo de interconexión llamado *router* o encaminador.

Un **router** es un dispositivo capaz de transferir datagramas IP de una red a otra con el objetivo de encaminar dichos datagramas a la red final donde está conectado el dispositivo receptor de los datos. La arquitectura de la interconexión de redes está basada fundamentalmente en el uso de estos dispositivos. Los *routers* están conectados a dos o más redes lógicas diferentes, por tanto, un *router* debe tener una interfaz de red por cada red a la que está conectado y cada una de las interfaces de red del *router* deberá tener asignada una dirección IP válida en cada una de las redes.

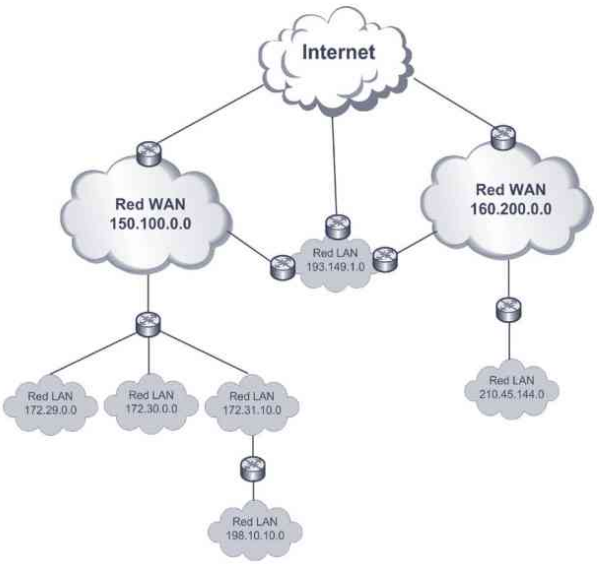


***Figura 10.9**. Interconexión de redes IP mediante routers*

En la figura anterior se pueden observar la interconexión de redes IP utilizando *routers* y formando con ello una estructura jerárquica de redes que, en última instancia, es lo que forma Internet. En la figura se observa que uno de los *routers* está conectado a cuatro redes distintas, por lo que deberá tener asignada una dirección IP por cada red. El caso más sencillo es la interconexión de dos redes. En este caso el *router* posibilita el intercambio de tráfico entre las redes a las que está conectado.

10.3.5 ÁMBITOS EN EL USO DE DIRECCIONES IP: PÚBLICAS Y PRIVADAS

Durante los primeros años de funcionamiento del protocolo IP todos los dispositivos conectados en las redes que formaban Internet utilizaban direcciones IP dentro del espacio de direcciones conocido como **direcciones públicas**. Cuando una empresa o institución quería conectar su red a Internet solicitaba un bloque de direcciones. Esta asignación se hacía mediante las clases, es decir, cuando alguna entidad solicitaba direcciones públicas, se le asignaba un rango completo de una de las clases (A, B ó C). Un organismo llamado **IANA** (*Internet Assigned Numbers Authority*) se encargaba de la asignación de las mismas.

Sin embargo, el rápido crecimiento de Internet hizo que esa política de asignación de direcciones IP no fuese viable. Fue necesario poner en marcha mecanismos para optimizar el uso de las cada vez más escasas direcciones IP públicas. Uno de esos mecanismos fue el uso de **direcciones privadas**, dichas direcciones son válidas en una red privada y no se pueden utilizar para la conexión a otras redes. En la siguiente tabla se muestran todos los rangos de direcciones IP que se pueden utilizar como direcciones privadas.

Rangos de direcciones IP privadas		Total rangos	Descripción
Primer rango	Último rango		
10.0.0.0		1	Dirección de red privada de clase A.
172.16.0.0	172.31.0.0	16	Rangos de direcciones privadas de clase B.
192.168.0.0	192.168.255.0	256	Rangos de direcciones privadas de clase C.

Los mecanismos de enrutamiento desarrollados sobre el protocolo IP no permiten encaminar fuera de las redes privadas datagramas que utilicen este tipo de direccionamiento, por ello también reciben el nombre de **direcciones no enrutables**.

Para poder proporcionar conectividad en Internet a redes que utilizasen direcciones privadas se utilizó una variante de una técnica llamada **NAT** (*Network Address Traslation*). Dicha variante, conocida como **NAPT** (*Network Address Port Traslation*), permite compartir una sola dirección IP pública entre varios dispositivos dentro de la misma red. En la actualidad, lo más frecuente es encontrar redes locales que utilizan direccionamiento privado dentro de la propia red y solo los *routers* tienen direccionamiento público. Para ello, es necesario que los *routers* implementen NAT. Este es el escenario más habitual en muchos tipos de redes, incluyendo las redes residenciales.

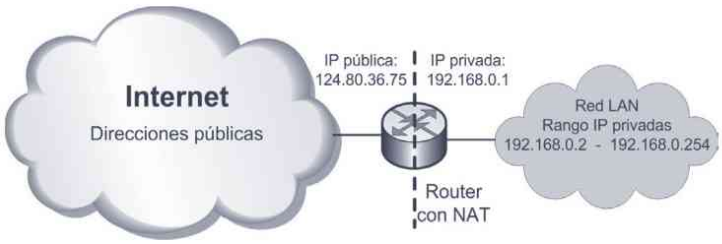


***Figura 10.10**. Conexión de redes privadas con Internet mediante un router con NAT*

En base a lo expuesto, podemos distinguir, por tanto, dos tipos de direcciones IP, las direcciones IP públicas y las direcciones IP privadas. En los dos próximos apartados se expondrá de qué modo se lleva a cabo la asignación de cada tipo.

Aunque la técnica utilizada en la mayor parte de las redes privadas para acceder a Internet es NAPT, se suele emplear el término genérico de NAT para referirse a dicha técnica de traducción de direcciones

10.3.6 ASIGNACIÓN DE DIRECCIONES IP PRIVADAS

Las direcciones IP privadas se suelen utilizar en las redes locales, de forma que todos los dispositivos conectados en una red local necesitan una dirección IP para intercambiar datos con el resto de dispositivos. Sin embargo, para que un equipo funcione correctamente en una red local necesita estar configurado para disponer tanto de conectividad física como lógica.

- **Conectividad física**. Hablaremos de conectividad física entre dispositivos cuando exista una infraestructura física que haga posible la comunicación de dichos dispositivos, por ejemplo, una red local. Todos los dispositivos conectados a dicha infraestructura tendrán conectividad física, es decir, existirá un camino físico por el que los dispositivos podrán intercambiar datos
- **Conectividad lógica**. Por otra parte, hablaremos de conectividad lógica entre dispositivos cuando los parámetros de configuración del nivel de red (y superiores), permitan el intercambio de información entre dichos dispositivos. Lógicamente, para que haya un intercambio real de información entre los dispositivos debe haber tanto conectividad física como lógica.

Por lo tanto, para que un equipo conectado en una red local se pueda conectar con otros equipos, además de estar conectado físicamente a la red (ya sea por Ethernet o por Wi-Fi) se deberá tener correctamente configurado su direccionamiento IP, es decir, su dirección IP y su máscara de subred. Lo más habitual es utilizar alguno de los rangos privados disponibles y su correspondiente máscara.

Primer rango	Último rango	Máscara de subred
10.0.0.0		255.0.0.0
172.16.0.0	172.31.0.0	255.255.0.0
192.168.0.0	192.168.255.0	255.255.255.0

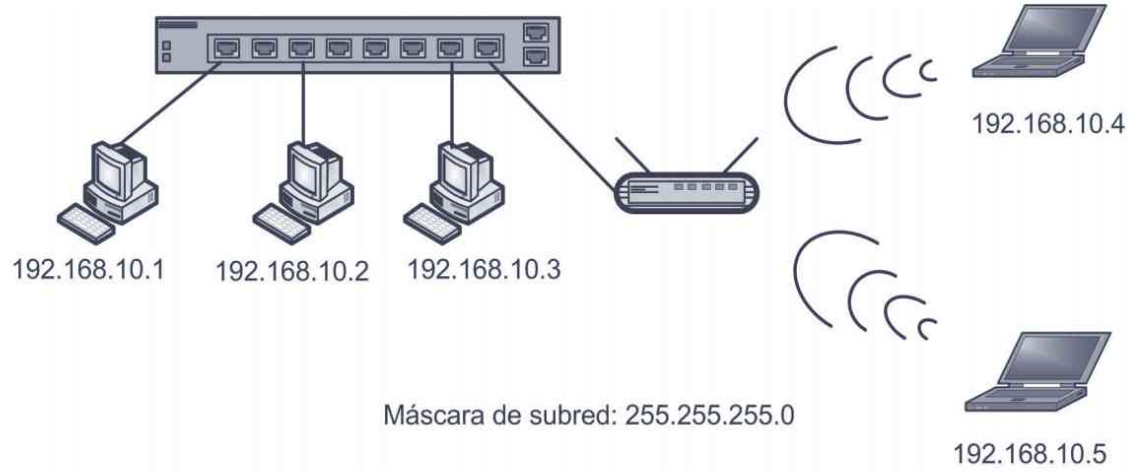


***Figura 10.11**. Configuración de direcciones IP en una red privada*

En algunos casos, además, se podrá organizar el direccionamiento de la red en subredes. El uso de subredes se conoce con el término *subnetting*. El **subnetting** se utiliza principalmente para separar el tráfico de red generado en diferentes áreas de la organización donde está implementada la red.

Si se configuran diferentes subredes en una red local no habrá "visibilidad" entre los equipos de diferentes subredes aunque sí haya conectividad física entre ellos. Para proporcionar conectividad lógica entre dispositivos de diferentes subredes será necesario el uso de *routers*.

10.4 OTROS PROTOCOLOS DE TCP/IP: ARP E ICMP

10.4.1 PROTOCOLO ARP

ARP (*Adress Resolution Protocol*, Protoloco de resolución de direcciones) es un protocolo utilizado en las redes locales para obtener la dirección física (dirección MAC) de un equipo a través de su dirección IP.

Cuando un equipo quiere enviar datos a otro dentro de una red local que utilice la arquitectura TCP/IP, el equipo emisor debe generar uno (o más) datagramas y estos deben ser pasados al nivel inferior (nivel de enlace) y encapsulados en una (o más) tramas Ethernet. En esta situación, la referencia al equipo destino suele ser su dirección IP, pero para poder generar las tramas Ethernet también es necesario conocer la dirección MAC.

Este problema se resuelve mediante dos soluciones. La primera es almacenar en cada equipo una tabla que contenga las direcciones IP de cada equipo y sus correspondientes direcciones MAC. De esa forma, cuando se quiera enviar un datagrama a un equipo cuya dirección IP es conocida, se puede consultar en dicha tabla cuál es la dirección MAC y generar de esta manera la trama Ethernet.

Esta primera solución sería poco práctica si hubiera que mantener de forma manual el contenido de esta tabla. Para ello se utiliza la segunda solución: el protocolo ARP se encarga de obtener la dirección MAC del equipo de destino a partir de su dirección IP y de almacenarlo en la tabla. Es decir, ARP hace el trabajo de mantenimiento de la tabla de direcciones MAC; esta tabla se conoce como **tabla ARP**.

Si la dirección MAC del equipo destino no se encuentra en la tabla ARP, se envía una trama conocida como **Petición ARP** (*ARP Request*). Esta petición contiene la dirección IP del destinatario del que queremos averiguar su dirección MAC. La petición ARP debe llegar a todos los equipos de la red y aquel que tenga la dirección IP del equipo del que se pretende obtener su dirección MAC deberá responder a esta petición con otra trama conocida como **Respuesta ARP** (*ARP Reply*) que contendrá, precisamente, su dirección MAC. Para conseguir que la *Petición ARP* llegue a todos los equipos de la red, se utiliza como dirección MAC de destino la *dirección de broadcast* (FF:FF:FF:FF:FF:FF).

10.4.2 PROTOCOLO ICMP

El protocolo **ICMP** (*Internet Control Message Protocol*, Protocolo de mensajes de control de Internet) es utilizado dentro de la arquitectura TCP/IP para el envío de notificaciones de datagramas IP que no han alcanzado su destino o para el envío de mensajes de control de estado. Conviene recordar que IP no realiza ninguna comprobación de que un datagrama llega al destino, por lo que si un dispositivo de red (típicamente un *router*) tiene problemas al enrutar un datagrama tiene la opción de nofificar al emisor mediante un mensaje ICMP.

ICMP es considerado un protocolo del nivel de red, sin embargo, los mensajes ICMP van encapsulados en datagramas IP.

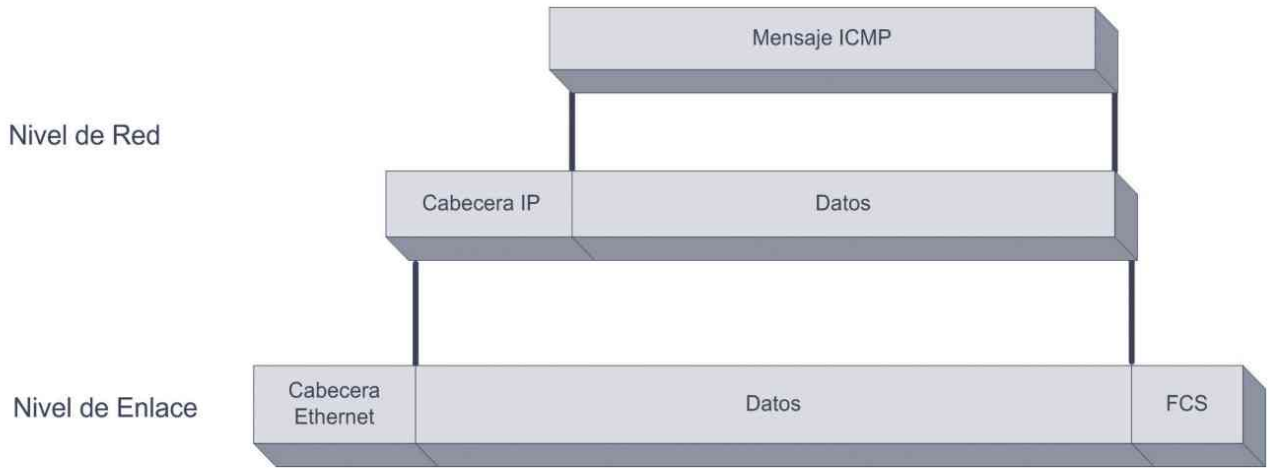


***Figura 10.12**. Encapsulado de un mensaje ICMP en un datagrama IP*

El formato de un mensaje ICMP es el siguiente:

***Figura 10.13**. Formato general de los mensajes ICMP*

Los campos de los que consta un mensaje ICMP son:

- **Tipo**: identifica el tipo de mensaje ICMP.
- **Código**: especifica un código de operación dentro de tipo de mensaje ICMP.
- **Checksum**: código de comprobación de errores.

Pueden aparecer otros campos opcionales que dependen del tipo de mensaje ICMP. Algunos de los mensajes ICMP más comunes se muestran en la siguiente tabla:

Tipo	Código	Descripción original	Descripción
8	0	*Echo*	Petición de eco
0	0	*Echo reply*	Respuesta de eco
3	0	*Net unreachable*	Red inalcanzable
3	1	*Host unreachable*	Host inalcanzable
11	0	*Time Exceeded*	Tiempo de datagrama excedido

Uno de los mensajes ICMP más populares son los de **Echo** (Eco). Son mensajes de control de estado que se utilizan para comprobar que existe conectividad con un host por medio del protocolo IP. Los mensajes ICMP de *Eco* son utilizados por el comando **ping**, implementado en todos los sistemas operativos actuales. Este comando envía el mensaje ICMP *Eco* (Tipo 8) a la dirección IP especificada como parámetro. Si el mensaje ICMP llega al destino, éste responde con el mensaje ICMP de *Respuesta de Eco* (Tipo 0).

Cuando un *router* no puede enviar un datagrama IP envía un mensaje ICMP de tipo 3 (*Destination unreachable*) al emisor de dicho datagrama. El código indica el motivo del error. Los más frecuentes son el código 0 (*Net unreachable*) y el código 1 (*Host unreachable*).

En definitiva, el protocolo ICMP permite el control de ciertas condiciones de error producidas en el nivel de red, sin embargo, su función es simplemente informar de dichos problemas pero no corregirlos. De hecho, el protocolo tampoco se asegura de la llegada de los mensajes ICMP. Por lo tanto, a pesar del uso de mensajes ICMP, el protocolo IP sigue siendo un protocolo no fiable.

10.5 PROTOCOLOS DE TRANSPORTE: TCP Y UDP

El nivel de transporte está implementado en la arquitectura TCP/IP por dos protocolos, TCP y UDP. El protocolo TCP lleva a cabo las principales funciones del nivel de transporte del modelo OSI que se vieron en el Capítulo 7, es decir, proporciona la entrega fiable de mensajes completos desde un origen a un destino. UDP es un protocolo más sencillo que proporciona la entrega de mensaje de origen a destino pero no ofrece la fiabilidad de TCP, por lo que cuando se usa UDP deben ser los protocolos del nivel de aplicación los que se encarguen del control de errores.

Una de las funciones importantes implementadas en el nivel de transporte es la definición de **los puertos del protocolo**, llamados simplemente **puertos**, que ofrecen un mecanismo para identificar la comunicación de un proceso individual dentro de un *host*. En la arquitectura TCP/IP los puertos son números de 16 bits, es decir, el rango de puertos válidos es de 0 a 65.535.

10.5.1 PROTOCOLO UDP

El protocolo **UDP** (*User Datagram Protocol*, Protocolo de datagramas de usuario) es un protocolo del nivel de transporte en la arquitectura TCP/IP no orientado a conexión, que proporciona las funciones básicas necesarias para la entrega de datos de un origen a un destino. No se lleva a cabo control de flujo ni de errores, además UDP no proporciona funciones de secuenciamiento ni de reordenación de paquetes. No puede especificar el paquete dañado cuando se produce un error ni detecta paquetes perdidos.

Como se puede ver, las funciones de UDP son muy limitadas. Realmente, la principal función de UDP es proporcionar el direccionamiento de los puntos de acceso a los diferentes protocolos del nivel de aplicación, es decir, los puertos. Por lo tanto, los protocolos del nivel de aplicación que utilicen UDP deben implementar mecanismos de control de flujo y de errores para llevar a cabo una comunicación fiable.

10.5.2 PROTOCOLO TCP

El protocolo **TCP** (*Transmission Control Protocol*, Protocolo de control de transmisión) proporciona todas las funciones de un protocolo de nivel de transporte, es decir, es un protocolo orientado a conexión que permite la comunicación fiable de datos de un origen a un destino. Implementa funciones de control de flujo y control de errores.

Las unidades de datos en el protocolo TCP se conocen como segmentos. La estructura de un segmento TCP es la siguiente:

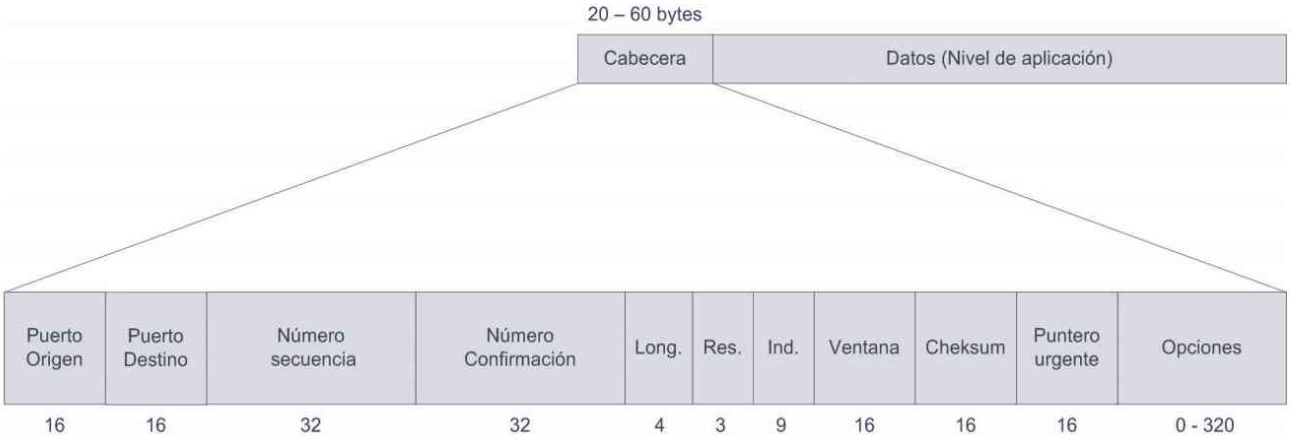


***Figura 10.14**. Formato del paquete TCP*

- **Puerto origen**. Dirección del puerto en el proceso origen.
- **Puerto destino**. Dirección del puerto en el proceso destino.
- **Número de secuencia**. Cada uno de los segmentos en los que se dividen los datos en una comunicación por medio de TCP se numera. En este campo se envía el número asignado a cada paquete TCP.
- **Número confirmación**. Si el indicador ACK está activo, este campo confirma la recepción correcta y sin errores de todos los segmentos con un número de secuencia menor o igual al indicado en este campo y que estuvieran pendientes de confirmación.
- **Longitud**. Este campo contiene el tamaño de la cabecera del segmento TCP expresado en grupos de 4 *bytes*, es decir, para un valor de 5 en este campo, la longitud de la cabecera sería 20 *bytes*.
- **Reservado**. Campo reservado de 3 bits.
- **Indicadores**. Este campo contiene los siguientes flags o indicadores:
  - **NS** (*Nonce Sum*). Indicador utilizado para llevar a cabo funciones de control de la congestión.
  - **CWR** (*Congestion Window Reduced*). Indicador utilizado para llevar a cabo funciones de control de la congestión.
  - **ECE** (*ECN-Echo*). Indicador que se activa para indicar la existencia de información sobre congestión en el campo ECN del datagrama IP.

- **URG**, indica que hay datos urgentes. El campo *Puntero urgente* indica la cantidad de datos urgentes en el segmento.
- **ACK**, bit utilizado para validar segmentos recibidos.
- **PSH**, indica al receptor que entregue al nivel superior todos los datos que tenga disponibles en el *buffer* de recepción.
- **RST**, indica que se necesita reiniciar la comunicación.
- **SYN**, bit utilizado para sincronizar los números de secuencia
- **FIN**, bit utilizado para indicar el fin de la comunicación.

- **Tamaño de ventana**. Parámetro que tiene relación con la función del control de flujo. Se utiliza una técnica conocida como *ventana deslizante* y este campo indica el tamaño de dicha ventana. El tamaño de la ventana está relacionado con el número de paquetes consecutivos que pueden enviarse sin recibir una confirmación de que han llegado. Dicho tamaño depende de las condiciones de transmisión. Si las condiciones de transmisión son buenas se puede aumentar el tamaño de la ventana y sin son malas se debe disminuir.
- **Checksum**. Campo utilizado para la comprobación de errores en la información tanto de la cabecera como de los datos del paquete TCP.
- **Puntero urgente**. Este campo contiene un puntero al final de los datos urgentes por lo que a partir de la posición indicada en este campo, comienza los datos con prioridad normal.
- **Opciones**. Es un campo opcional utilizado para enviar diferentes tipos de información adicional. Su longitud es variable se obtiene del campo *Longitud* de la propia cabecera TCP.

Uno de los usos del campo *Opciones* es el envío de un parámetro llamado **MSS** (*Maximun Segment Size*, Tamaño máximo del segmento) es usarlo para definir cuál es el tamaño del segmento más grande que se puede enviar. Lo más óptimo es que este tamaño sea el adecuado para evitar la fragmentación de datagramas IP. Este parámetro se suele enviar en el proceso de establecimiento de la conexión TCP.

Como hemos visto, TCP es un protocolo orientado a conexión y, por tanto, implementa mecanismos para establecer y finalizar conexiones. Además, para llevar a cabo el control de flujo de los datos se emplea la técnica de ventana deslizante.

El procedimiento para establecer una conexión se lleva a cabo en tres pasos. El origen de la conexión (normalmente un cliente de un servicio de red) envía un segmento TCP con un número de secuencia inicial N y el indicador SYN activo. El destinatario de la conexión (normalmente un servidor de un servicio de red) responde con un segmento TCP con otro número de secuencia M, el indicador SYN activo y el ACK activo con un número de confirmación N+1. En el último paso, el origen de la conexión envía otro segmento TCP con el número de secuencia N+1 y con el indicador de ACK activo y el número de confirmación M+1. La siguiente figura resume el proceso de establecimiento de una conexión TCP.

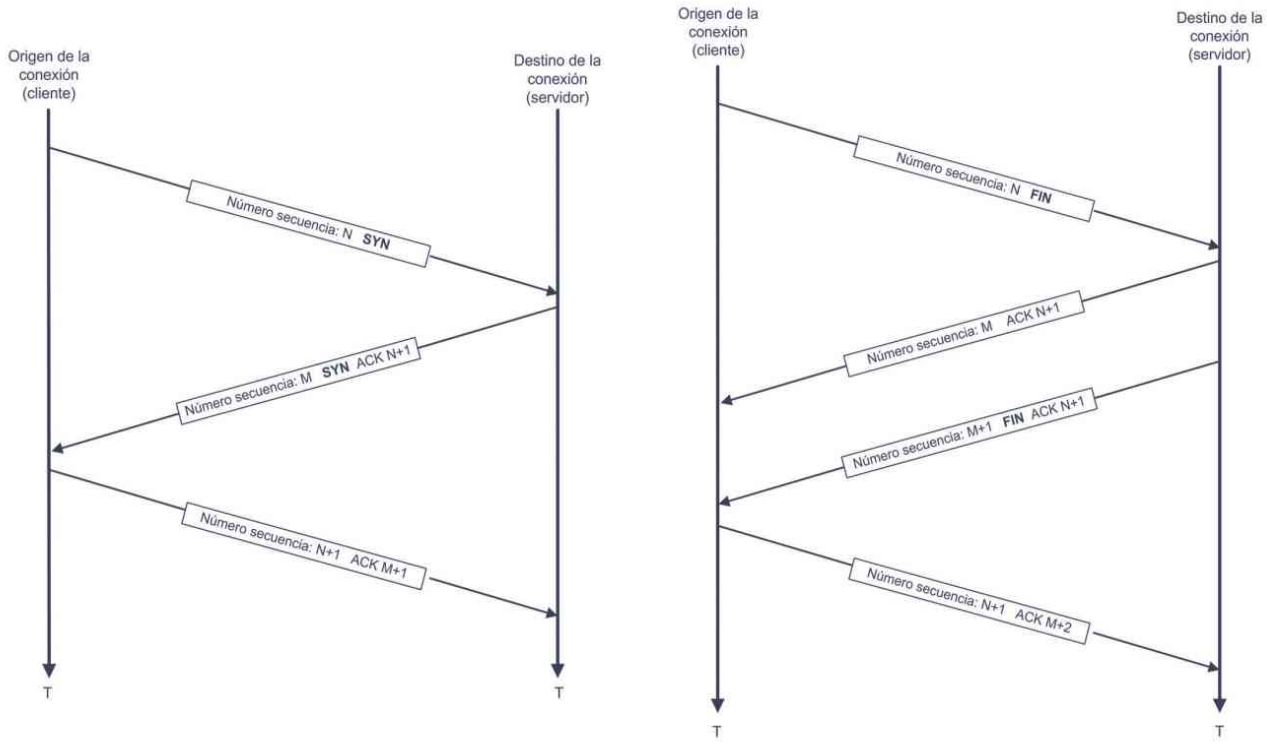


***Figura 10.15**. Establecimiento y finalización de una conexión TCP*

Para finalizar, una conexión TCP se establece un mecanismo de cuatro pasos. El proceso que desea finalizar la conexión envía un segmento TCP con el indicador FIN activo y un número de secuencia inicial N. El proceso en el otro extremo de la conexión envía entonces un segmento TCP con un número de secuencia inicial M y el indicador ACK activo, con el número de confirmación N+1. A continuación, este último proceso envía otro segmento TCP, esta vez con el indicador FIN activo y número de secuencia M+1. El primer proceso, cuando recibe los segmentos anteriores, genera un segmento TCP con número de secuencia N+1 y el indicador ACK activo con el número de confirmación M+2.

Las conexiones TCP pueden encontrarse en varios estados que definen su comportamiento inmediato. Estos estados se muestran en la siguiente tabla:

Estado	Descripción
CLOSED	No hay conexión.
LISTEN	Un proceso servidor espera las peticiones de procesos clientes.
SYN-SENT	Se ha enviado una petición de conexión. En espera del reconocimiento.
SYN-RCVD	Se ha recibido una petición de conexión.
ESTABLISHED	Conexión establecida.
FIN-WAIT-1	Se ha solicitado el cierre de la conexión.
FIN-WAIT-2	El equipo remoto ha aceptado el cierre de la conexión.
TIME-WAIT	Esperando la retransmisión de segmentos.
CLOSE-WAIT	Un proceso servidor espera el cierre del proceso cliente.
LAST-ACK	El proceso servidor espera el último reconocimiento.

10.6 CONFIGURACIÓN DE PARÁMETROS DE RED

En los próximos apartados se mostrarán los mecanismos de configuración de los parámetros de red en los principales sistemas operativos utilizados en la actualidad como son Windows® XP, Windows® 7 y Ubuntu.

Los elementos de configuración relacionados con TCP/IP que se tendrán que configurar son los siguientes:

- **Dirección IP**. Dirección IP asignada al equipo.
- **Máscara de subred**. Máscara de subred asignada al equipo.
- **Puerta de enlace**. Este parámetro se utiliza para indicar la dirección IP del *router*, donde el equipo deberá dirigir los datagramas que deban enviarse fuera de la red (por ejemplo, a Internet).
- **Servidores DNS**. Este parámetro se utiliza para indicar las direcciones IP de los servidores DNS, que se encargan de proporcionar las direcciones IP a partir de los nombres de dominio utilizados en la mayor parte de los servicios de Internet. En el apartado correspondiente se explica con más detalle.

Actualmente existen dos métodos para establecer los parámetros de red en un equipo:

- **Configuración manual**. Si se utiliza esta opción el usuario del equipo o un técnico de administración debe especificar manualmente el valor de dichos parámetros. Esto requiere tener conocimientos sobre el direccionamiento utilizado en la red local para saber qué dirección IP se puede utilizar, si existen subredes en dicha red para establecer el valor adecuado de máscara de subred y cuál es la puerta de enlace del *router* de la red.

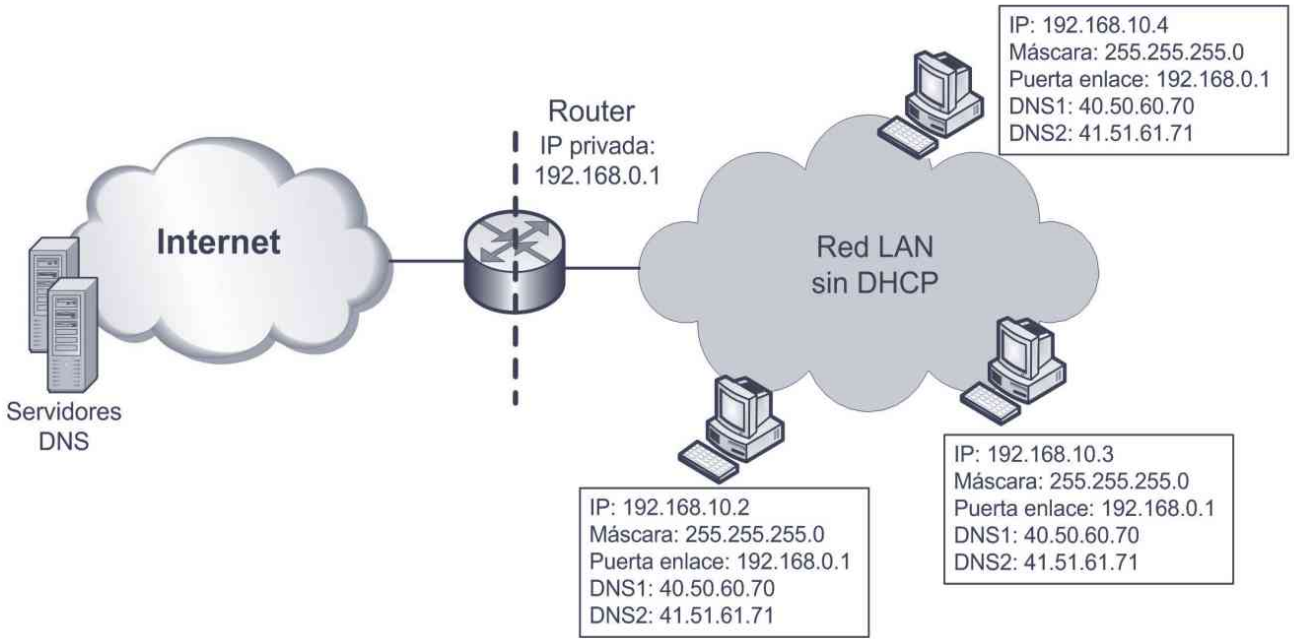


***Figura 10.16**. Configuración manual de los parámetros de red*

- **Configuración automática**. Este método es el que está configurado por defecto en la mayor parte de los equipos. En este caso no es necesario configurar ningún parámetro de red en el equipo ya que se utiliza un procedimiento para obtener los parámetros de red de forma automática. Para ello se utiliza un protocolo llamado DHCP y es imprescindible que en la red exista lo que se conoce como un servidor DHCP que sea el que proporciona al resto de equipos los parámetros de configuración adecuados.

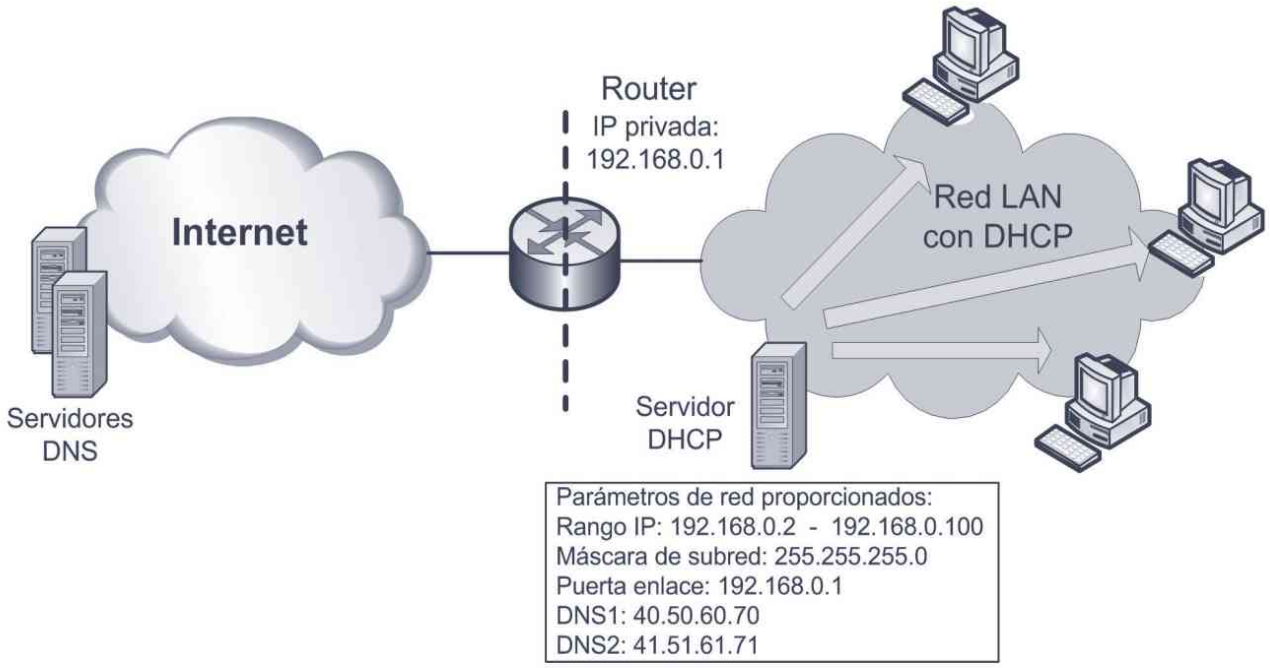


***Figura 10.17**. Configuración Automática proporcionada por un servidor DHCP*

Actualmente el uso de servidores DHCP está muy extendido. La mayoría de los ISP utilizan un servidor DHCP para asignar las direcciones públicas a sus clientes. Y la mayor parte de los *routers* actuales también implementan un servidor DHCP para la asignación de direcciones privadas en una red de área local. Los sistemas operativos de tipo servidor como Windows® 2003/2008 Server o Linux incluyen también servidores DHCP. También es habitual que los puntos de acceso inalámbrico incluyan el servicio DHCP.

10.6.1 ASIGNACIÓN AUTOMÁTICA DE PARÁMETROS IP: SERVICIO DHCP

DHCP (*Dynamic Host Configuration Protocol*, Protocolo de configuración dinámica de estación) es un protocolo cliente-servidor utilizado en redes TCP/IP para proporcionar la configuración de los parámetros de red a un equipo, es decir, una dirección IP, una máscara de red, la dirección IP de la puerta de enlace y la dirección IP de un servidor DNS.

Para utilizar este servicio debe existir un equipo que funcione como servidor DHCP y en el que se configuran los parámetros de red, que se proporcionarán a todos los equipos que lo soliciten, que se consideran clientes del servcio.

DHCP utiliza el protocolo UDP en el nivel de transporte. El servidor lleva a cabo sus comunicaciones por el puerto 67 y los clientes utilizan el puerto 68. Para solicitar una configuración de red a un servidor DHCP se envía una solicitud utilizando la dirección IP de broadcast genérica 255.255.255.255 o la dirección de *broadcast* de la subred.

La asignación de los parámetros de red es dinámica. Esto implica que las asignaciones son temporales, es decir, se asigna un tiempo de validez y transcurrido el mismo se deben renegociar los parámetros de red.

RECUERDA

En la mayor parte de las ocasiones no se utiliza un equipo exclusivamente como servidor DCHP. En redes profesionales suele ser un equipo que proporciona servicios de red entre los que se encuentra el servicio DHCP. En pequeñas redes se suele utilizar el servidor DHCP incluido en la mayor parte de los *routers* proporcionados por el proveedor de conexión a Internet. La mayor parte de los puntos de acceso inalámbricos también implementan un servidor DHCP.

10.6.2 OBTENCIÓN DE DIRECCIONES IP DE DOMINIOS: SERVICIO DNS

DNS (*Domain Name System*, Sistema de nombres de dominio) es el protocolo utilizado para poder asociar a una dirección IP un nombre. DNS utiliza el modelo cliente-servidor. Dichos nombres, conocidos como **nombres de dominio** se almacenan, junto con sus direcciones IP, en una base de datos jerárquica y distribuida.

La asignación de un nombre de dominio es el método utilizado para asociar un nombre a un recurso dentro de Internet. Un nombre de dominio está formado por una sucesión de nombres (dominios) separados por puntos y siguiendo una determinada jerarquía. El dominio de nivel superior (también conocido como **TLD** (*Top Level Domain*) es el que aparece en última posición. Por ejemplo, para el nombre *www.redestelematicas.es*, el dominio de nivel superior es "es".

Los dominios de nivel superior más frecuentes son "com", "org", "edu", "net" o los nombres de dominios asignados por países, como "es" para España, "ar" para Argentina, "br" para Brasil, "de" para Alemania, "nl" para Holanda...

Muchos servicios del nivel de aplicación utilizan nombres para referirse a equipos, sin embargo, para llevar a cabo una comunicación con ese equipo es necesario conocer su dirección IP. Para ello se genera una petición DNS que se envía a un servidor DNS. La información que se mantiene en el sistema DNS es distribuida y si dicho servidor no es capaz de resolver la petición puede redirigirla a otro servidor. Los servidores que gestionan los dominios de nivel superior o TLD se conocen como **root servers**, que se pueden considerar como los nodos primarios del sistema DNS. Actualmente hay 13 *root servers* operativos en Internet.

El envío de la información DNS, tanto de las peticiones como de las respuestas, se lleva a través del puerto 53 y se utiliza tanto UDP como TCP.

10.6.3 CONFIGURACIÓN DE PARÁMETROS IP EN WINDOWS®

Para el caso de la configuración de un equipo en red que utilice Windows® como sistema operativo vamos a presentar dos posibilidades: Windows® XP y Windows® 7.

El acceso a la configuración de los parámetros de red en Windows® XP se puede hacer desde diferentes opciones. Por ejemplo, accediendo al **Panel de Control** de Windows® y seleccionando la opción **Conexiones de red**. En esta ventana aparecerán todas las interfaces de red existentes en el equipo. Cada una de ellas tendrá su propia configuración de red.

Para acceder a la configuración de red se selecciona la opción **Propiedades** del menú contextual.

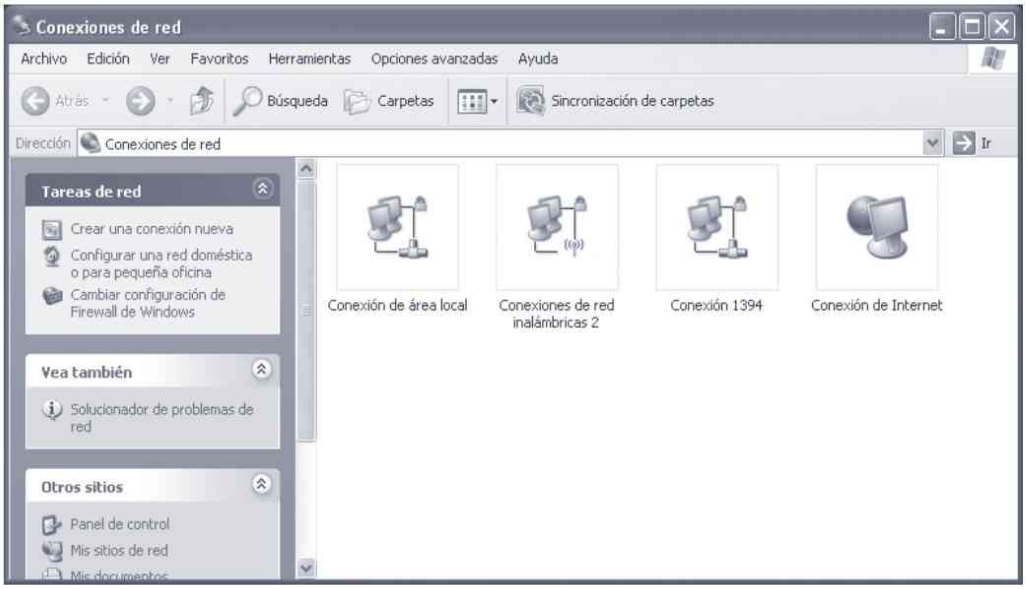


***Figura 10.18**. Ventana de Conexiones de red en Windows® XP*

En la ventana de propiedades aparece una lista de protocolos y servicios de red asociados a esa interfaz y uno de ellos será **Protocolo Internet** (**TCP/IP**). Seleccionar esa opción haciendo doble clic o pulsando el botón **Propiedades**.

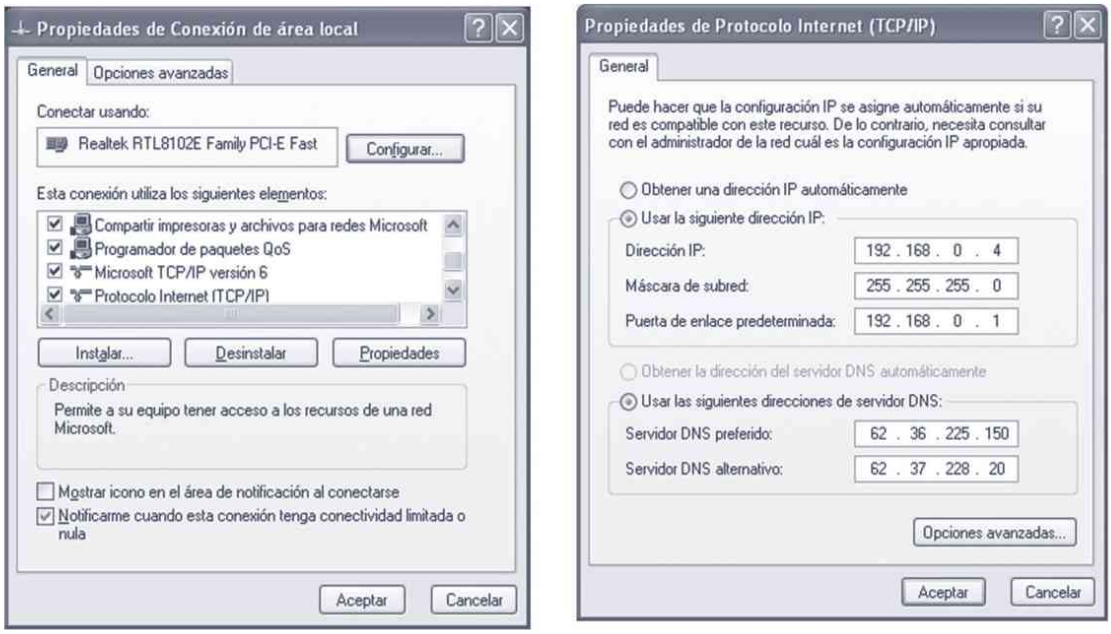


***Figura 10.19**. Ventanas de configuración de red en Windows® XP*

En la ventana de configuración de la figura se puede seleccionar la opción **Obtener una dirección IP automáticamente** y **Obtener la dirección del servidor DNS automáticamente** para seleccionar el modo automático. O seleccionar las opciones **Usar la siguiente dirección IP** y **Usar las siguientes de direcciones de servidor DNS** para seleccionar el modo manual. En este último caso hablamos de introducir los valores adecuados en los campos *Dirección IP*, *Máscara de subred*, *Puerta de enlace predeterminada*, *Servidor DNS preferido* y *Servidor DNS alternativo*.

Puede aparecer una interfaz de red llamada **Conexión 1394**. Esta interfaz de red se utiliza para proporcionar conectividad IP a dispositivos que utilicen el estándar IEEE 1394 (también conocido como **Firewire**). Este estándar se utiliza en dispositivos digitales tales como cámaras de vídeo. La aparición de esta interfaz en la ventana de conexión de red depende de la implementación del *bus* IEEE 1394 en la placa base del equipo.

La configuración de los parámetros de red en equipos con Windows® 7 se lleva a cabo desde la ventana de **Centro de redes y recursos compartidos**, a la que se puede acceder desde el menú de **Propiedades** en la opción de **Red** del menú principal de Windows® 7, o bien desde el **Panel de control** seleccionando la opción **Redes e Internet**.

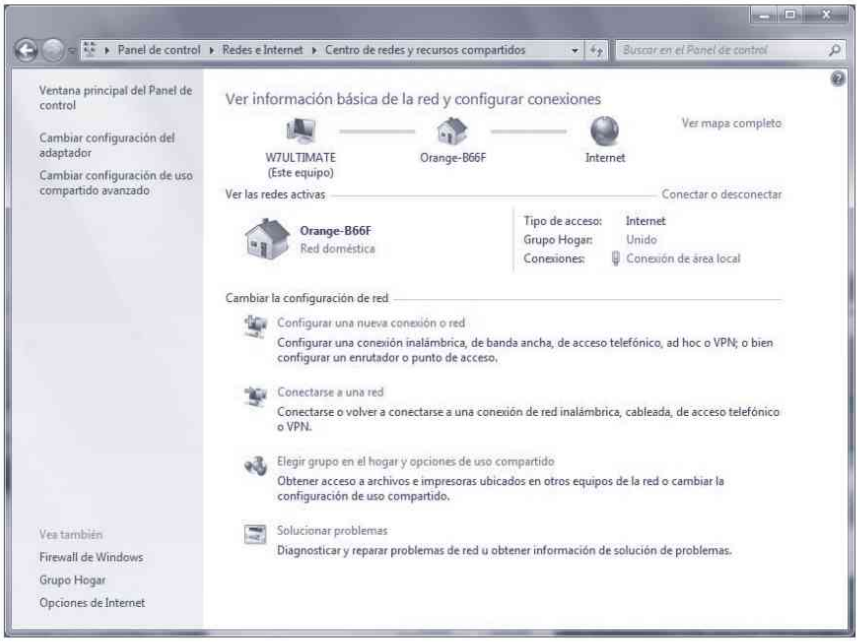


***Figura 10.20**. Ventana Centro de redes y recursos compartidos de Windows® 7*

Desde aquí se puede seleccionar la opción de **Conexión de área local** y con el botón **Propiedades** se puede acceder a la ventana de configuración de los parámetros de red.

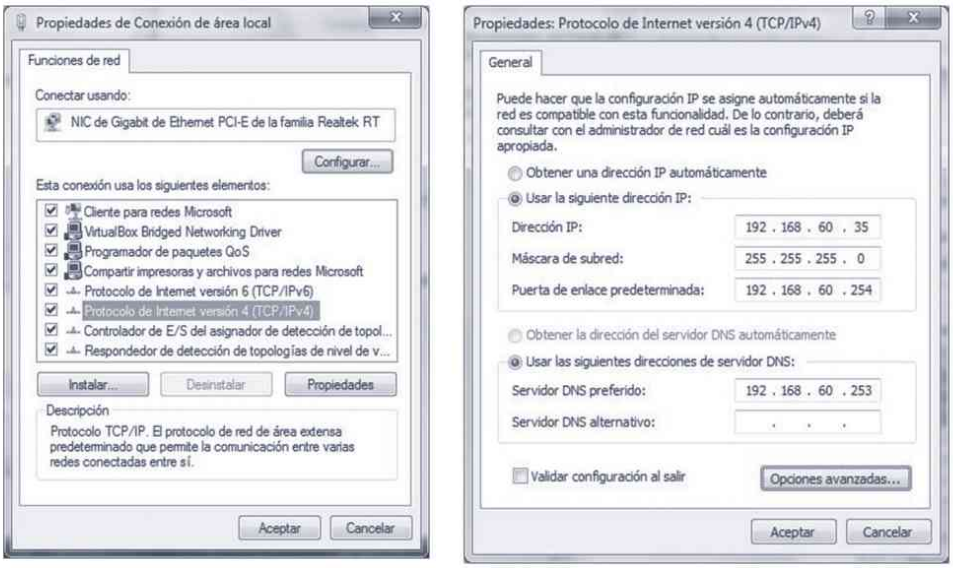


***Figura 10.21**. Ventanas para la configuración de red en Windows® 7*

RECUERDA

Para que el modo de configuración automática funcione, debe haber en la red local un servidor DHCP en funcionamiento.
Los *routers* proporcionados por los provedores de conexión a Internet incluyen un servidor DHCP integrado en el propio *router* y que suele estar activado por defecto. Por ello, en este tipo de redes funciona por defecto el modo de configuración automática.
Podemos encontrar servidores DHCP en sistemas Windows® 2003/2008 Server, en sistemas servidores bajo Linux, en *routers* y en puntos de acceso inalámbricos.

10.6.4 CONFIGURACIÓN DE PARÁMETROS IP EN UBUNTU

Ubuntu es sin duda una de las distribuciones de Linux más utilizadas en la actualidad. Por ello, se utilizará como distribución de referencia. La configuración de red utilizando la versión 11.10 de Ubuntu se puede realizar directamente desde la barra superior, desplegando el icono de red.

Desde este menú se puede activar o desactivar la red y se puede acceder a los parámetros de configuración desde la opción **Editar conexiones**.

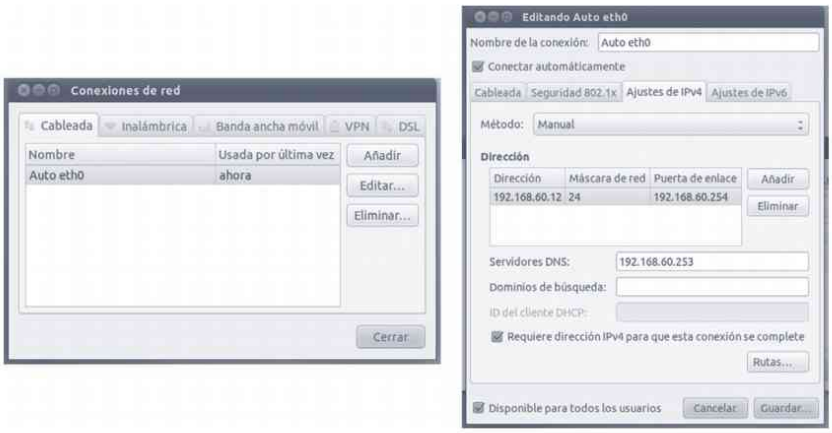


***Figura 10.22**. Ventanas de configuración de red en Ubuntu*

Tradicionalmente Linux, y por extensión, Ubuntu, ha permitido la configuración de los parámetros de red editando los archivos de configuración correspondientes. Sin embargo, en las últimas versiones de Ubuntu Desktop se aconseja la configuración de red siempre desde el modo gráfico. La versión Ubuntu Server sí mantiene la posibilidad de configurar la red editando directamente los archivos de configuración.

10.6.5 FIREWALL

El concepto de **firewall** o **cortafuegos** apareció en el ámbito de las redes de datos para describir los diferentes mecanismos de seguridad destinados a bloquear la transferencia de datos que no cumplan unos criterios de seguridad determinados. Está considerado en la actualidad como un mecanismo de seguridad necesario pero no suficiente para proteger las redes y los equipos conectados a las mismas. Se puede aplicar en dos ámbitos:

- **Firewall de red**. Este ámbito se aplica a dispositivos de interconexión, es decir, *routers*. Un *firewall* de red proporciona los mecanismos de control en los datos intercambiados entre las redes a las que se conecta el *router* o cualquier dispositivo que haga funciones de enrutamiento.

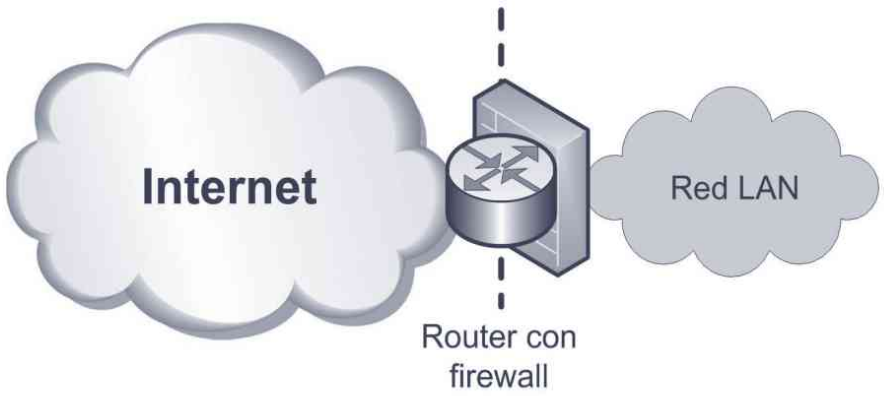


***Figura 10.23**. Firewall de red implementado en un router*

- **Firewall de equipo**. Este ámbito está referido a la función de *firewall* implementada en un ordenador y que tiene como finalidad aplicar los mecanismos de control en los datos intercambiados entre el equipo y la red.

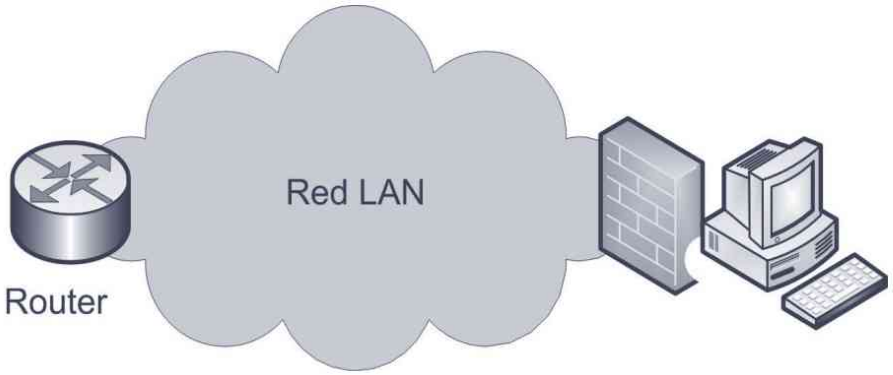


***Figura 10.24**. Firewall de equipo*

Las funciones básicas de un *firewall* consisten en inspeccionar todo el tráfico intercambiado entre dos entidades (entre dos redes o entre un equipo y una red) y comprobar que cumplen ciertas reglas de seguridad permitiendo o denegando dicho tráfico en función que se cumplan o no dichas reglas. El tipo más habitual de reglas se basa en criterio de selección de puertos. De esta manera se establecen una serie de reglas para permitir el paso de datos dirigidos a una serie de puertos determinados, denegando el acceso al resto de los puertos.

En este apartado se tratarán aspectos de configuración del segundo tipo de *firewall* en equipos con Windows® XP, Windows® 7 y Ubuntu. Para acceder a las funciones del *firewall* en sistemas que utilicen Windows® XP se accede al **Panel de Control** y se selecciona la herramienta **Centro de seguridad**.

***Figura 10.25**. Ventana Centro de seguridad desde donde se puede acceder al firewall de Windows® XP*

También es posible acceder al *firewall* desde la ventana de **Conexiones de red** de la Figura 10.18. En ambos casos la ventana principal de configuración permite activarlo o desactivarlo, lo cual no está recomendado.

***Figura 10.26**. Ventana de configuración del firewall de Windows® XP*

Con el *firewall* activo no se permitirá el tráfico entrante de red a ningún puerto, salvo los especificados en la pestaña **Excepciones**.

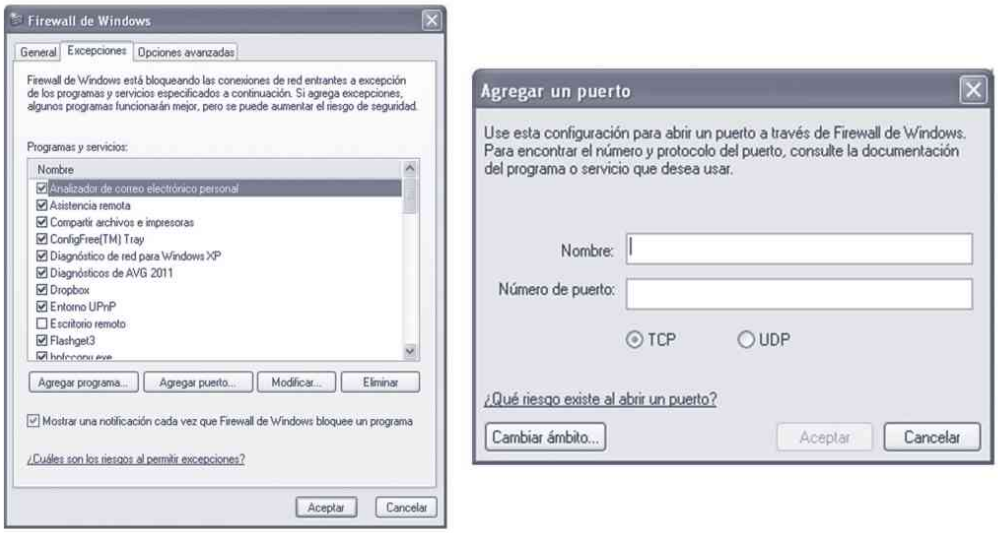


***Figura 10.27**. Ventana de excepciones del firewall y para agregar un puerto a las excepciones*

En Windows® 7 se puede acceder a las características y configuración del *firewall* desde la ventana **Centro de redes y recursos compartidos**.

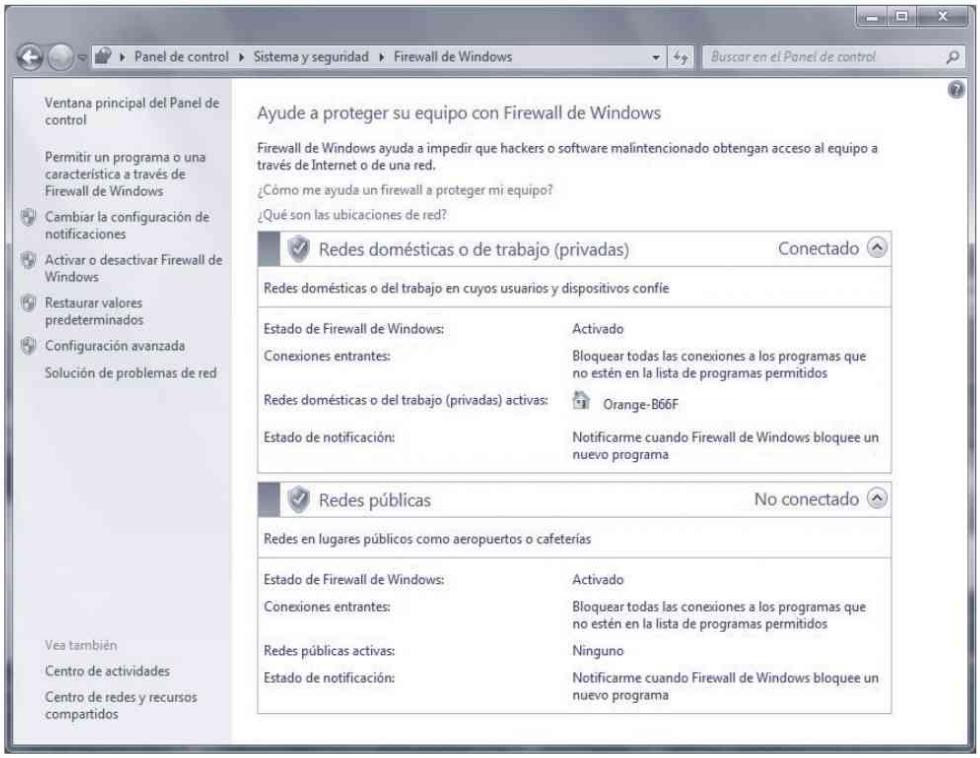


Figura 10.28. *Ventana principal de configuración del firewall de Windows® 7*

10.7 PROTOCOLOS DEL NIVEL DE APLICACIÓN

El nivel de aplicación es el nivel más alto del modelo TCP/IP y su funcionalidad está asociada generalmente a cubrir las necesidades del usuario final. La implementación de las funcionalidades del nivel de aplicación se lleva a cabo, como en el resto de niveles, a través de protocolos. La mayor parte de los protocolos del nivel de aplicación en TCP/IP siguen un modelo cliente-servidor. Uno de los extremos de la comunicación será el que solicita datos (cliente) y el otro extremo de la comunicación se encarga de proporcionar dichos datos (servidor).

En este contexto, la funcionalidad aportada por una aplicación que utiliza alguno de los protocolos del nivel de aplicación se conoce como **servicio**. De esta forma, una aplicación cliente se ejecuta en un equipo para solicitar un servicio (envío de datos) a una aplicación servidor que estará en ejecución en otro equipo atendiendo cualquier petición de servicio que reciba.

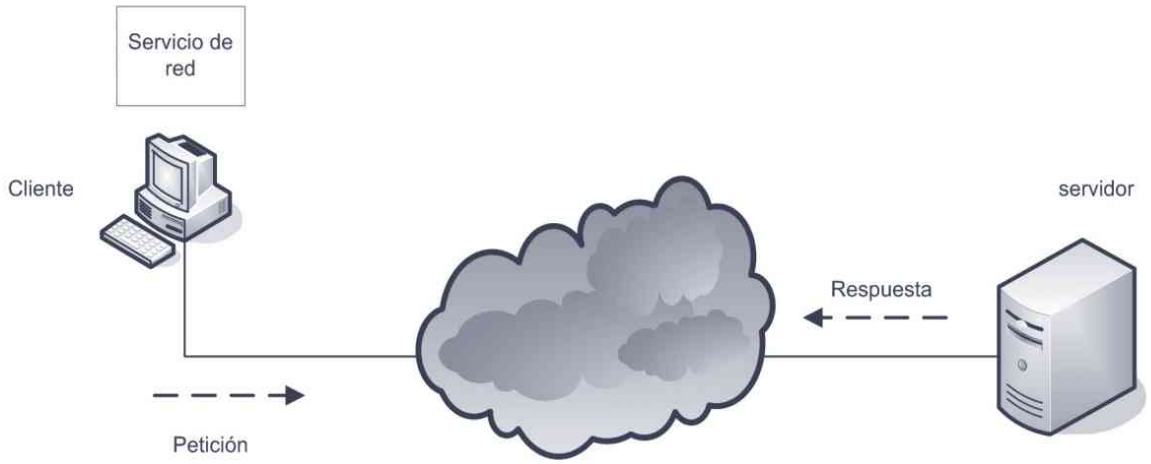


***Figura 10.29**. Modelo cliente-servidor en los servicios de red*

En los próximos apartados se describirán brevemente los principales protocolos utilizados en TCP/IP en el nivel de aplicación.

10.7.1 SERVICIO DE ACCESO A PÁGINAS WEB

El acceso al sistema **World Wide Web** o simplemente **web** es sin duda el servicio más utilizado en Internet en la actualidad. Para acceder a este servicio se utiliza el protocolo **HTTP** (*Hypertext Transfer Protocol*, Protocolo de transferencia de hipertexto). Este protocolo permite la transferencia tanto de texto sin formato, como de texto con formato, hipertexto (permite saltos rápidos entre documentos), imágenes, sonido y vídeo. La comunicación a través del protocolo HTTP se lleva por defecto por el puerto 80.

Es un protocolo cliente-servidor en el cual, el cliente HTTP (normalmente un navegador web) envía mensajes, llamados peticiones, a un servidor HTTP. El servidor responde enviando una respuesta al cliente, esta respuesta contiene normalmente la página web solicitada por el cliente en la petición. Dicha página web en realidad es un archivo.

Para el acceso a los recursos proporcionados por el servicio web se utiliza un parámetro conocido como Localizador uniforme de recursos ó **URL** (*Uniform Resource Locator*). Dicho parámetro sigue un formato estándar para nombrar y localizar cualquier tipo de información en Internet. Un URL está formado por cuatro elementos:

- **Método**: protocolo utilizado para obtener el recurso. Es opcional y si no se especifica se utiliza el valor *http*.
- **Servidor**: equipo donde se encuentra la información a la que se quiere acceder. El servidor se puede especificar mediante su dirección IP o (más habitual) por su nombre de dominio.
- **Puerto**: es opcional y contiene el número de puerto del servidor. Por defecto se utiliza el puerto 80.
- **Ruta**: camino para llegar al recurso al que se quiere acceder. Se utiliza el carácter **/** para separar los nombres de los directorios.

El formato general de un URL es el siguiente:

Método://Servidor:puerto/ruta

Algunos ejemplos:

- *http://www.google.es*
- *http://www.uc3m.es/depar/operativos/index.html*
- *http://www.servidor.com:3500/ejemplo/graficos.html*

En base a lo anterior se podría decir que *World Wide Web* (*www*) o simplemente *web* es un servicio cliente-servidor distribuido que utiliza principalmente el protocolo HTTP para su funcionamiento. La web es un repositorio de información mundial y enlazada entre sí. Los documentos contenidos en la web pueden ser de tres tipos:

- **Páginas web estáticas**: son páginas de contenido fijo que se crean y se almacenan en un servidor. El cliente obtiene bajo petición una copia de las mismas para visualizarlas en el navegador web. El lenguaje estándar utilizado para crear páginas web estáticas es **HTML**. Este lenguaje permite especificar etiquetas para dar formato al texto. Estas etiquetas son leídas e interpretadas por los navegadores web para establecer el formato de visualización de la página.
- **Páginas web dinámicas**: una página dinámica se crea en el servidor cuando un cliente lo solicita. Cuando llega la petición, el servidor web ejecuta un programa que crea el documento y le envía el resultado al cliente. El contenido del documento dinámico puede variar de una petición a otra.

  CGI es la tecnología utilizada para crear y gestionar páginas dinámicas. CGI no es un lenguaje, es un conjunto de estándares que definen cómo escribir una página dinámica, cómo proporcionar la entrada al programa y cómo se debería utilizar el resultado de salida. Un programa CGI puede estar escrito en cualquier lenguaje de programación.
- **Páginas web activas**: las páginas activas son realmente programas que necesitan ejecutarse en el cliente. Cuando un navegador solicita una página activa, el servidor envía una copia de la página en formato binario y ésta es ejecutada en el cliente.

  El lenguaje de programación más utilizado para crear páginas activas es **Java**. Los programas escritos en Java y ejecutados a través de un navegador web se conocen como **applets**.

10.7.2 SERVICIO DE TRANSFERENCIA DE CORREO ELECTRÓNICO: SMTP

SMTP (*Simple Mail Transfer Protocol*, Protocolo simple de transferencia de correo) es un protocolo cliente-servidor que sirve para el envío de mensajes de correo electrónico de un usuario a otro o de un usuario a un servidor SMTP. El envío de correo entre un cliente y un servidor se lleva a cabo a través del puerto 25 de una conexión TCP.

Para el envío de correo se utiliza un sistema de direccionamiento con el siguiente formato:

Parte local @ nombre de dominio

SMTP solo se puede utilizar para enviar texto ASCII. Debido a esta limitación se desarrolló **MIME** (*Multipurpose Internet Mail Extensions*) como una extensión a SMTP para permitir el envío de datos no ASCII.

Otro protocolo asociado al servicio de correo electrónico es **POP3** (*Post Office Protocol*, protocolo de oficina de correos versión 3) que es un protocolo cliente-servidor utilizado para descargar mensajes de correo electrónico desde un servidor (normalmente SMTP). POP3 lleva a cabo la comunicación mediante conexiones TCP utilizando el puerto 110.

En el modelo OSI existía otro protocolo que implementaba el servicio de correo electrónico llamado X.400, pero actualmente apenas se utiliza debido a la gran aceptación de SMTP.

10.7.3 SERVICIO DE TRANSFERENCIA DE ARCHIVOS: FTP

FTP (*File Transfer Protocol*, Protocolo de transferencia de ficheros) es uno de los primeros protocolos del nivel de aplicación desarrollados en redes TCP/IP. Es un protocolo cliente-servidor utilizado para el intercambio de ficheros, que es una de las tareas más habituales realizadas en un entorno de red. Se utilizan dos conexiones TCP para realizar las transferencias, una para los datos que utiliza el puerto 20 y otra para información de control que utiliza el puerto 21.

El servicio de transferencia de ficheros es proporcionado por un servidor FTP, que es un proceso ejecutándose en un equipo y que escucha las peticiones recibidas a través del puerto 21. Este protocolo utiliza la validación de la conexión mediante la introducción de un nombre de usuario y una contraseña aunque la mayor parte de los servidores FTP admiten la posibilidad de activar lo que se conoce como **usuario anónimo** (*anonymous*) para permitir el acceso anónimo a un servidor FTP, normalmente con acceso restringido.

Las primeras implementaciones de clientes FTP se usaban sobre líneas de comandos. Este tipo de clientes todavía están disponible en los sistemas Windows® o en Linux, a través del **comando ftp**. Actualmente existen clientes FTP que se ejecutan en los avanzados entornos gráficos y que son mucho más sencillos de utilizar. Incluso los navegadores web implementan la funcionalidad del protocolo FTP.

Una de las principales carencias del protocolo FTP es que todos los datos intercambiados, incluidos los datos de validación (nombre de usuario y contraseña), se transfieren sin ningún tipo de encriptación. Actualmente se han desarrollado otros protocolos de transferencia de ficheros en modo seguro, con encriptación de los datos, como FTP sobre SSH (conocido como **Secure FTP**), **FTPS** (FTP/SSL) o **SCP** (*Secure Copy Protocol*).

10.7.4 SERVICIO DE TERMINAL REMOTO: TELNET Y SSH

Telnet (*Terminal Network*, Terminal de red) es un protocolo cliente-servidor que permite la conexión a un equipo remoto a través de un terminal desde el cual se pueden ejecutar comandos y aplicaciones como si se ejecutasen de forma local. El protocolo Telnet envía los caracteres tecleados en el equipo local (cliente) al equipo remoto (servidor), el cual los interpreta como si se hubiesen tecleado en un terminal de comandos local. La salida producida en el equipo remoto se envía al equipo local, donde se visualiza. Telnet utiliza el puerto 23.

Es uno de los primeros protocolos implementados en redes TCP/IP. En los sistemas Unix ha sido ampliamente utilizado para llevar a cabo la administración de equipos de forma remota.

Al igual que el protocolo FTP, uno de sus principales problemas es la seguridad, ya que ni siquiera el nombre de usuario y la contraseña de validación se envían encriptados. Por ello, se ha desarrollado el protocolo **SSH** (*Secure Shell*) con la misma funcionalidad que Telnet, pero llevando a cabo la encriptación de todos los datos que se transmite. SSH utiliza el puerto 23 y se utiliza ampliamente en los sistemas Linux.

10.7.5 SERVICIO DE GESTIÓN DE RED: SNMP

SNMP (*Simple Network Management Protocol*, Protocolo simple de gestión de red) es un protocolo para gestionar dispositivos de red a través del protocolo TCP/IP. Está basado en el concepto de gestor y agente. Un gestor es normalmente un equipo que controla y monitoriza un conjunto de agentes, normalmente *routers*. Como este protocolo está definido en el nivel de aplicación, puede gestionar redes con características y tecnologías diferentes.

Los equipos gestores ejecutan un cliente SNMP. Los dispositivos gestionados o agentes ejecutan un servidor SNMP. El protocolo SNMP proporciona un mecanismo útil y eficaz para monitorizar redes. Sin embargo, el intercambio de información entre gestores y agentes hace que el tráfico de red aumente.

La transferencia de los datos del protocolo SNMP se lleva a cabo mediante UDP a través de los puertos 161 (agente) y 162 (gestor).

10.8 DIRECCIONAMIENTO EN EL NUEVO PROTOCOLO IPV6

El principal objetivo por el que se desarrolló la versión 6 de IP fue la ampliación del espacio de direcciones, que se había quedado corto con IPv4 después del gran desarrollo que experimentó Internet. Una dirección IPv4 es un número de 32 bits representados en formato punto decimal, es decir, agrupando los bits de ocho en ocho y pasando cada cifra a decimal. El nuevo protocolo IPv6 utiliza direcciones de 128 bits, es decir, cuatro veces más bits que una dirección IPv4. Con ello, el espacio de direcciones en IPv6 es de 2^{128}, un número enorme y prácticamente inagotable.

Además de ampliarse el número de bits de las direcciones IPv6, también se ha cambiado la forma de representar dichas direcciones. Se utiliza la numeración hexadecimal y se forman grupos de 16 bits, es decir, de 4 digitos hexadecimales. Por lo tanto, una dirección IPv6 estará formada por 8 grupos de 4 dígitos hexadecimales. El carácter separador de cada grupo son los dos puntos (**:**). La siguiente dirección es un ejemplo de dirección IPv6:

2001:0bd8:0000:0000:0012:ac43:0000:65d3

La escritura de las direcciones IPv6 admite además varias simplificaciones:

- Dentro de cada bloque de 4 dígitos hexadecimales se pueden quitar los ceros a la izquierda. Aplicando esta regla, la dirección anterior quedaría:

  2001:**bd8**:0000:0000:**12**:ac43:0000:65d3

- Un bloque donde todos los dígitos sean cero se puede representar con un solo cero. Siguiendo con el ejemplo anterior:

  2001:bd8:**0**:**0**:12:ac43:**0**:65d3

- Se pueden sustituir varios bloques consecutivos con el valor cero por la abreviatura "**::**". Esto solo se puede aplicar una vez. Aplicando esta regla en el ejemplo:

  2001:bd8**::**12:ac43:0:65d3

En el siguiente ejemplo se muestra otra dirección donde existen bloques consecutivos a cero en dos partes de la dirección. Solo se aplica la regla anterior en la primera aparición:

- ✓ Dirección sin simplificaciones: 2001:006b**:0000**:**0000:**cd41:**0000**:**0000**:923a
- ✓ Dirección con simplificaciones: 2001:6b**::**cd41:**0:0**:923a

10.8.1 TIPOS DE DIRECCIONES IPV6

Se han definido tres tipos de direcciones IPv6:

- **Unicast**. Dirección utilizada para identificar una interfaz de red única. Es equivalente a las direcciones IPv4 actuales. Hay varios tipos de direcciones Unicast que se pueden asignar a una interfaz de red. Las más comunes son las siguientes:
  - **Direcciones unicast globales**. Utilizadas como direcciones públicas. Actualmente el rango que se está utilizando para la asignación de direcciones *unicast* globales es **2000::/3**
  - **Direcciones unicast de enlace local** (*local-link*). Son direcciones utilizadas con propósitos de autoconfiguración y como dirección IP en redes donde no hay *router* que asigne una dirección *unicast global*, por tanto, este direccionamiento se aplica en el ámbito de redes locales. Son direcciones IP que no se pueden enrutar a otras redes. Se utiliza el rango **fe80:: / 10**

- **Anycast**. Dirección utilizada para identificar un grupo de interfaces, normalmente asociadas a diferentes dispositivos. Un datagrama enviado a una dirección *anycast* se entrega solo a uno de los dispositivos del grupo de dispositivos asociados a la dirección *anycast*. Dicho dispositivo será el más cercano en términos de la distancia al nodo origen determinada por el algoritmo de encaminamiento que se esté utilizando. Este tipo de direcciones son útiles para poder implementar varios servidores de un mismo servicio distribuidos geográficamente. Se utiliza una única dirección IP *anycast* y los dispositivos cliente que soliciten el servicio serán atendidos por el servidor "más cercano". Las direcciones *anycast* utilizan los mismos rango que las direcciones *unicast* globales.
- **Multicast**. Dirección utilizada para identificar un grupo de interfaces, normalmente associadas a diferentes dispositivos. A diferencia de una dirección anycast, un datagrama enviado a una dirección multicast se entrega a todos los dispositivos del grupo. Este tipo de direcciones se utiliza para aplicaciones de difusión, donde se desea que una sola transmisión llegue a varios dispositivos. El rango utilizado para direcciones *multicast* es **ff00:: /8**. En IPv6 no hay direcciones de *broadcast*, en su lugar se utilizan las direcciones *multicast*.

Existen un par de direcciones IPv6 reservadas que son las siguientes:

- **Dirección no especificada**. Utilizada en tablas de enrutamiento y otros mecanismos de configuración para indicar que no existe una dirección IPv6 específica.

  Dirección completa 0:0:0:0:0:0:0:0 Dirección abreviada **::**

- **Dirección de bucle local** (*loopback*). Tiene el mismo significado que en IPv4. Es la dirección IP de una interfaz lógica de bucle utilizada para hacer pruebas internas de servicios de red.

  Dirección completa: 0:0:0:0:0:0:0:1 Dirección abreviada **::1**

Cada interfaz de red tendrá al menos una dirección *unicast* de enlace local. Dicha dirección se establece de forma automática en la interfaz de red. Para ello se utiliza el prefijo de red para direcciones de enlace local fe80:: / 64 y para establecer los últimos 64 bits de la dirección se utiliza el denominado Identificador global de 64 bits (EUI-64) que se forma utilizando la dirección MAC de la interfaz de red, como se muestra en el ejemplo.

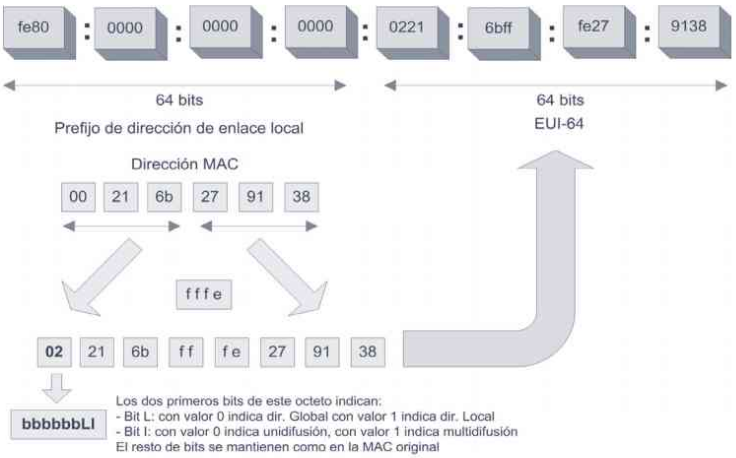


***Figura 10.30**. Establecimiento de la dirección de enlace local*

EJEMPLO 10.3

SEGUIMIENTO DE RUTAS IP

El objetivo de este ejercicio práctico es estudiar la ruta que siguen los datagramas IP en la comunicación con algunos servidores públicos. Para ello se utilizarán dos herramientas:

- **Comando tracert** (en sistemas Linux se llama *traceroute*). Este comando utiliza mensajes ICMP para obtener información de los *routers* por los que va pasando un datagrama IP hasta llegar al destino especificado como parámetro.
- **Base de datos WHOIS**. Contiene información sobre la asignación de los recursos de Internet. WHOIS realmente es un protocolo que opera en el nivel de aplicación. Inicialmente existía un cliente WHOIS desarrollado para entornos Unix y que accedía a los servidores WHOIS para obtener la información solicitada. En la actualidad existen páginas web que ofrecen este servicio, por lo que no es necesario utilizar un cliente WHOIS. Para la práctica se utilizará la siguiente página web para acceder a la información proporcionada por WHOIS:

  whois.domaintools.com

Con estas dos herramientas obtener información sobre la ruta que siguen los datagramas IP para alcanzar los siguientes servidores web:

1. *www.facebook.com*
2. *www.ubuntu.com*
3. *www.fta.org.au*

Otra fuente de información para obtener datos interesantes es el propio nombre de los *routers*, aunque no todos los operadores asignan un nombre público a sus equipos. En el caso de que sí lo proporcionen, dicho nombre aparece en la información del comando *tracert*.

EJEMPLO 10.4

ANÁLISIS DE PUERTOS

Otro ejemplo de análisis que se puede hacer con herramientas básicas de redes es el seguimiento de los puertos abiertos en un equipo. Para ello se utilizarán dos herramientas existentes en sistemas Windows®:

- **Comando netstat**. Se utiliza para obtener información sobre diferentes aspectos relacionados con la pila de protocolos TCP/IP.
- **Comando tasklist**. Este comando específico de sistemas Windows® se utiliza para ver información sobre los procesos activos en memoria.

Los pasos a seguir son los siguientes:

Paso1. Ejecutar el comando *netstat –aon*.

El significado de los modificadores se puede consultar con la ayuda del comando: *netstat /?*

Al ejecutar el comando anterior se puede ver una lista de todas las conexiones y puertos de escucha. La última columna es el PID o identificador del proceso responsable de la conexión o escucha.

Paso 2. Elegir de la lista anterior todas las conexiones que puedas suponer algún tipo de amenaza. Se puede elegir como criterio aquellas conexiones cuya Dirección remota sea una dirección IP externa a la red.

Paso 3. Ejecute el comando *tasklist* para obtener la lista de todos los procesos en memoria y su correspondiente PID.

Paso 4. A partir del PID, obtener el nombre de los procesos de los que se está haciendo el seguimiento.

Paso 5. Analizar si el proceso origen de la conexión o el puerto en escucha es legítimo o podría tratarse de un proceso dañino para el sistema. Consultar en Internet la información que se crea oportuna.

RESUMEN DEL CAPÍTULO

La familia de protocolos TCP/IP son los que cubren las funciones de los niveles de red, de transporte y de aplicación en las redes de todo el mundo. En este capítulo se hace un repaso a dichos protocolos.

El protocolo IP es el principal protocolo del nivel de red, que cubre una de las funciones más importantes como es el direccionamiento lógico. Además, se estudia el método para establecer subredes junto con el uso de los dos ámbitos de direccionamiento, el direccionamiento público y el privado.

Se incluyen también los protocolos ARP e ICMP como protocolos auxiliares del nivel de red, así como los protocolos TCP y UDP utilizados en el nivel de transporte. Se hace un repaso de los principales protocolos utilizados en el nivel de aplicación.

Por último, se añade un apartado para hablar del nuevo protocolo IPv6, la próxima versión diseñada para sustituir al actual protocolo IP, conocido también como IPv4.

EJERCICIOS PROPUESTOS

1. Indicar la clase y la dirección de red de las siguientes direcciones IP:

- 203.56.125.12
- 238.56.112.78
- 109.235.1.90
- 129.157.221.2
- 191.1.23.44

2. ¿Cuál es el máximo número de subredes en una red de clase A utilizando las siguientes máscaras?

- 255.192.0.0
- 255.255.128.0
- 255.255.255.0
- 255.255.248.0

3. ¿Cuál es el máximo número de subredes en una red de clase B utilizando las siguientes máscaras?

- 255.255.255.0
- 255.255.252.0
- 255.255.255.128
- 255.255.192.0

4. ¿Cuál es el máximo número de subredes en una red de clase C utilizando las siguientes máscaras?

- 255.255.255.248
- 255.255.255.192
- 255.255.255.252
- 255.255.255.224

5. Indicar la dirección de subred de cada una de las siguientes direcciones IP:

- IP: 121.63.120.56 Máscara: 255.255.0.0
- IP: 98.231.126.198 Máscara: 255.255.128.0
- IP: 168.50.121.5 Máscara: 255.255.224.0
- IP: 180.4.30.101 Máscara: 255.255.192.0
- IP: 205.78.44.153 Máscara: 255.255.255.240

6. Establecer el direccionamiento para obtener seis subredes a partir del rango 193.105.10.0/24:

Dir. Subred	Rango de direcciones	Máscara	Dir. Broadcast

7. A partir del esquema de la figura se desea configurar tres subredes. La subred 1 formada por los equipos PC01, PC02 y PC03. La subred 2 formada por los equipos PC04 y PC06. La subred 3 formada por los equipos PC05 y PC07. La capacidad máxima de cada subred debe ser de 60 equipos.

- Dirección de red: 204.34.56.0/24

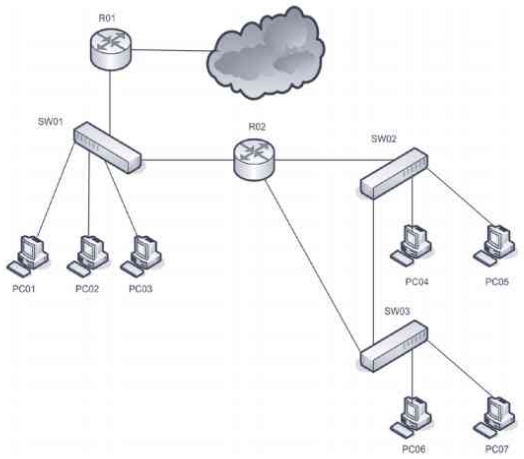


***Figura 10.31**. Esquema de red del ejercicio 7*

8. Especificar la configuración de red (dirección IP, máscara y puerta de enlace) de todos los PC, así como las direcciones IP y máscaras de las interfaces de red de los *routers*.

- ¿Los datagramas enviados de PC06 a PC07 serán procesados por el *router* R02? Justificar la respuesta.
- ¿Los datagramas enviados de PC04 a PC06 serán procesados por el *router* R02? Justificar la respuesta.
- Para pasar el equipo PC03 a la subred 2, ¿sería necesario algún cambio en la configuración física de la red? Justificar la respuesta.
- Para pasar el equipo 5 a la subred 2, ¿sería necesario algún cambio en la configuración física de la red? Justificar la respuesta.

TEST DE CONOCIMIENTOS

1 El modelo de niveles de la arquitectura TCP/IP:
- a) Es prácticamente igual al modelo OSI.
- b) Solo están definidos los niveles de red y de transporte.
- c) No se hace distinción entre el nivel físico y el de enlace.
- d) Las funcionalidades del nivel de sesión se incluyen en el nivel de red.

2 IP es un protocolo:
- a) Orientado a conexión.
- b) Basado en datagramas.
- c) Del nivel de transporte.
- d) Todas las respuestas anteriores son correctas.

3 Una de las principales funciones de IP:
- a) Llevar a cabo el control de flujo de la comunicación.
- b) Evitar las congestiones en las redes.
- c) Identificar errores en la transmisión.
- d) Proporcionar un direccionamiento lógico.

4 Una dirección de difusión (*broadcast*) en IP:
- a) Tiene todos los bits a 1.
- b) Tiene a 1 todos los bits que identifican la red.
- c) Tiene a 1 todos los bits que identifican los equipos en una red.
- d) No existe la dirección de difusión en IP solo en Ethernet.

5 Una petición ARP (*ARP Request*) se envía:
- a) Cada vez que se solicita el envío de un datagrama IP.
- b) Si la dirección IP no se encuentra en la tabla ARP.
- c) Si la dirección IP está fuera de la red.
- d) Si lo solicita el usuario con un comando *ping*.

6 De las cinco clases de direcciones IP definidas se utilizan para asignación a redes:
- a) Todas las clases.
- b) Solo las clases A, B y C.
- c) Solo las clases A, B, C y D.
- d) Solo las clases A y B. La clase C es solo para subredes.

7 El enmascaramiento se utiliza:
- a) Solo en redes que utilicen subredes.
- b) Solo en redes de clase C.
- c) Tanto en redes con subredes como en redes sin subredes.
- d) Solo en los *routers*.

8 Los paquetes de respuesta ARP (*ARP Reply*):
- a) Se envían siempre a la dirección MAC de la puerta de enlace.
- b) Se envían a la dirección de *broadcast*.
- c) Se envían encapsulados en un datagrama IP.
- d) Se envían encapsulados en una trama Ethernet.

9 Cuando un datagrama IP llega a un *router*:
- a) El *router* decrementa el campo TTL una unidad.
- b) El *router* cambia la dirección de destino.
- c) El *router* cambia la dirección origen.
- d) El *router* rennvía el datagrama a todas sus interfaces.

10 La nueva versión IPv6:
- a) Mantiene el formato del datagrama respecto a IPv4.
- b) Mantiene el formato de dirección lógica respecto a IPv4.
- c) Sustituye las direcciones de *broadcast* por las de *multicast*.
- d) Elimina la dirección de bucle local o *loopback*.

11 Para que un equipo obtenga los parámetros de configuración de red de forma automática es necesario que en la red haya:
- a) Un servidor HTTP.
- b) Un servidor DHCP.
- c) Un servidor DNS.
- d) Un servidor SNMP.

12 El localizador uniforme de recursos o URL se suele utilizar para acceder a recursos del servicio:
- a) SMTP.
- b) SSH.
- c) Web.
- d) DHCP.

11 Redes LAN Inalámbricas

OBJETIVOS DEL CAPÍTULO

- ✓ Entender el significado de los términos WLAN, IEEE 802.11 y Wi-Fi.
- ✓ Conocer las diferentes configuraciones y modos de funcionamiento de las redes inalámbricas.
- ✓ Entender las principales características relacionadas con redes inalámbricas como son el alcance, la potencia de transmisión y recepción, los canales y el acceso al medio de transmisión.
- ✓ Conocer los diferentes mecanismos de seguridad que se pueden usar en redes Wi-Fi.
- ✓ Conocer los diferentes dispositivos existentes en la actualidad que proporcionan conectividad en redes Wi-Fi.

11.1 INTRODUCCIÓN

Las redes LAN inalámbricas, también conocidas como **WLAN** (*Wireless LAN*), son redes de área local que utilizan ondas electromagnéticas para la transmisión de los datos. En los últimos años, este tipo de redes locales han alcanzado gran popularidad tanto en entornos domésticos como en empresas, ya que permiten la conexión de un equipo a una red sin apenas infraestructura. Además, la proliferación de dispositivos móviles con grandes capacidades de conectividad ha aumentado todavía más la demanda de este tipo de redes. Al igual que ocurre con Ethernet en las redes locales cableadas, existe un estándar que domina la implantación de redes locales inalámbricas y que se conoce como **Wi-Fi**.

11.2 EL ESTÁNDAR IEEE 802.11 Y LA CERTIFICACIÓN WI-FI

El estándar **IEEE 802.11**, al igual que el resto de estándares de redes LAN, cubre las funciones del nivel físico y del subnivel MAC del nivel de enlace. La primera versión del estándar se desarrolló en 1997. En esta primera especificación se incluía como medios de transmisión tanto los infrarrojos como las ondas radioeléctricas en la banda de 2,4 GHz. La velocidad de transmisión máxima alcanzada estaba entre 1 y 2 Mbps. El uso de infrarrojos como medio de transmisión, aunque se llegó a especificar en el estándar, nunca ha llegado a utilizarse debido a las limitaciones de este tipo de comunicaciones.

La banda de frecuencias utilizada en esta primera versión del IEEE 802.11 se situa en 2,4 GHz y comprende el rango de frecuencias desde 2,4 GHz hasta 2,4835 GHz, es decir, ocupa 83,5 MHz. Esta banda forma parte de un grupo de bandas conocidas como **ISM** (*Industrial, Scientific and Medical*), cuya principal característica es que no requieren licencia de uso. El uso de dicha banda ISM beneficia la utilización de dispositivos inalámbricos, pero tiene el inconveniente de que es utilizada por otros dispositivos como hornos microondas, teléfonos inalámbricos o dispositivos *Bluetooth* con los que podría tener interferencias.

En el año 1999 se publican dos nuevas ampliaciones del estándar conocidas como **IEEE 802.11a** y **IEEE 802.11b**. La principal diferencia entre estas versiones era la banda de frecuencia utilizada. Mientras que la versión IEEE 802.11b seguía utilizando la banda de 2,4 GHz (aunque aumentaba la velocidad máxima a 11 Mbps), la IEEE 802.11a utilizaba una banda en 5 GHz consiguiendo una velocidad de 54 Mbps.

Esta banda de frecuencia en 5 GHz, al contrario que la banda de 2,4 GHZ, no estaba disposible en todos los países, ya que la regulación del espectro de radiofrecuencia no es común, sino que cada país aplica su propia legislación al respecto. Por ejemplo, tanto en Estados Unidos como Japón se podía utilizar la banda de 5 GHz pero en Europa dicha banda estaba reservada para la tecnología HiperLAN.

Paralelamente al desarrollo de los estándares IEEE, en el año 1999 algunos de los más importantes fabricantes de soluciones inalámbricas crearon una organización llamada **WECA** (*Wireless Ethernet Compatibility Alliance*) con el objetivo de fomentar la compatibilidad de los dispositivos inalámbricos desarrollados bajo dichos estándares. Unos años más tarde, esta organización cambia su nombre a **Wi-Fi Alliance**. Los dispositivos que cumplen los estándares IEEE 802.11 son comercializados con la denominación **Wi-Fi** (*Wireless Fidelity*) lo que asegura su compatibilidad con el resto de dispositivos Wi-Fi del mercado.

Se puede obtener la lista de dispositivos Wi-Fi certificados por la Wi-Fi Alliance en:
www.wi-fi.org/search_products.php

Por lo tanto, hay que diferenciar el nombre del estándar, que es IEEE 802.11, del nombre comercial asignado para garantizar que un dispositivo cumple con el estándar IEEE 802.11 y que es Wi-Fi. Este distintivo es asignado a los dispositivos certificados por la Wi-Fi Alliance.

***Figura 11.1**. Logos de Wi-Fi y de un producto certificado Wi-Fi*

En el año 2003 se publica la versión **IEEE 802.11g**. Su principal característica es el aumento de la velocidad hasta los 54 Mbps utilizando la banda de 2,4 GHz. Los dispositivos comercializados que soportan esta versión ofrecen compatibilidad con el estándar anterior IEEE 802.11b. Hasta la fecha posiblemente sea el estándar inalámbrico más extendido, especialmente en Europa.

La última versión del estándar se publica en 2009 y recibe la denominación **IEEE 802.11n**. Esta nueva versión incluye como principal característica un nuevo aumento de velocidad hasta unos teóricos 600 Mbps, aunque actualmente la velocidad máxima de los productos que cumplen este estándar está entre 150 y 300 Mpbs. Dicho aumento de velocidad se basa en dos características:

- El uso de las dos bandas de frecuencia, la de 2,4 GHz y la de 5 GHz. Se aprovecha así la liberación de la banda de 5 GHz en algunas áreas importantes como en Europa.
- El empleo de la tecnología **MIMO** (*Multiple Inpunt Multiple Output*). Esta tecnología está basada en el uso de varias antenas, tanto en el emisor como en el receptor, consiguiendo con ello un incremento de la tasa de transmisión respecto al uso de una única antena. MIMO utiliza una técnica llamada **SDM** (*Spatial Division Multiplexing*, Multiplexación por división espacial) para conseguir varios flujos de información sobre el mismo rango de frecuencias. Esto se consigue aprovechando las llamadas multi-rutas de las señales radioeléctricas debido a las reflexiones, que sin el uso de esta técnica se podrían considerar interferencias pero que gracias a SDM se pueden aprovechar para el envío de más información. Lo interesante además, es que este incremento de la tasa de transmisión se consigue sin aumentar el ancho de banda o la potencia de transmisión.

11.3 ARQUITECTURA DE UNA RED INALÁMBRICA

El estándar IEEE 802.11 contempla dos posibles configuraciones con las que se pueden interconectar los dispositivos en una red inalámbrica. La configuración básica llamada **BSS** admite a su vez dos modos de operación y se utiliza para establecer redes inalámbricas simples con un área de cobertura y número de equipos limitados. Por el contrario, la configuración **ESS** se utiliza cuando se requieren mayores alcances en la red inalámbrica. En los siguientes apartados se explica el funcionamiento de cada configuración.

11.3.1 BSS (BASIC SERVICE SET)

Es el nombre que recibe la configuración básica de una red en la que dos o más dispositivos se conectan de forma inalámbrica. Esta configuración admite dos modos de operación conocidos como ad-hoc e infraestructura.

- **Ad-hoc**. También conocido como configuración **IBSS** (*Independent Basic Service Set*). Consiste en establecer una red inalámbrica básica formada por dos o más equipos.

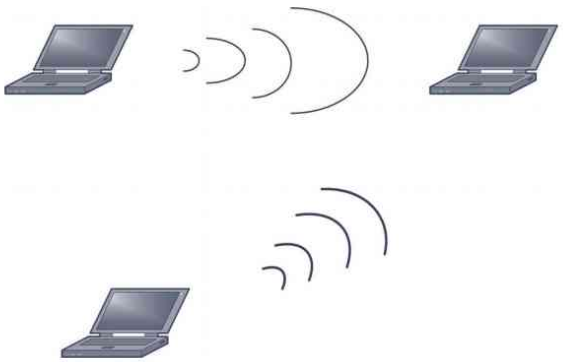


***Figura 11.2**. Red inalámbrica ad-hoc*

  - Este modo de operación se utiliza para la conexión inalámbrica de unos pocos dispositivos sin grandes exigencias de cobertura y prestaciones. Habitualmente esta configuración se utiliza para conectar dos equipos de forma temporal. La conexión de más de dos dispositivos en esta configuración degrada sustancialmente las prestaciones por lo que apenas se utiliza.

- **Infraestructura**. Este modo de configuración presenta varias mejoras respecto al anterior, y su funcionamiento se basa en la utilización de un dispositivo llamado **punto de acceso inalámbrico** (**AP**, *Access Point*).

  Un punto de acceso proporciona algunas características importantes a la red inalámbrica:

  - Permite la conexión de la red inalámbrica a una red cableada.
  - Permite la conexión de un número mayor de dispositivos sin que las prestaciones de la red se degraden, ya que el punto de acceso centraliza las transmisiones entre dispositivos gestionando más eficazmente el medio de transmisión.
  - Cubre una mayor área de cobertura que el modo ad-hoc.

El modo infraestructura es el más habitual en redes domésticas que disponen de un *router* de banda ancha con funciones de punto de acceso.

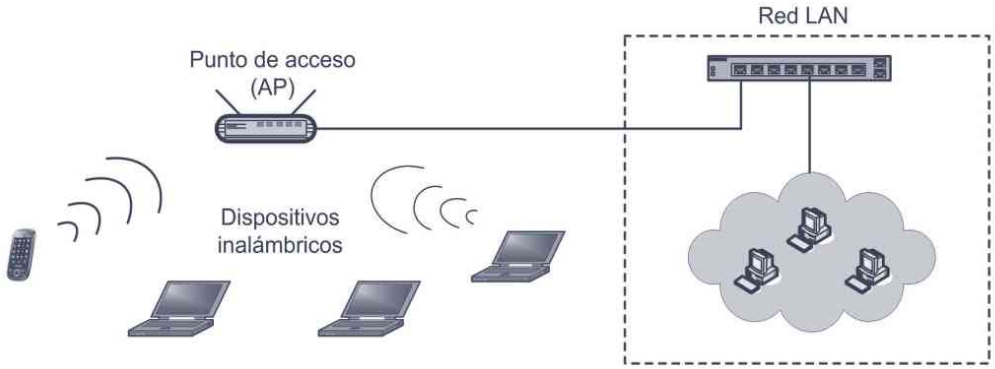


***Figura 11.3**. Red inalámbrica en modo infraestructura*

El ancho de banda del canal utilizado en una red inalámbrica está compartido entre todos los dispostivos conectados a esa red (un punto de acceso sería algo así como un hub inalámbrico). Debido a esta característica, el número máximo de dispositivos conectados simultáneamente sin sufrir una alta degradación de las prestaciones está entre 25 y 30.

11.3.2 ESS (EXTENDED SERVICE SET)

La configuración BSS permite la creación de redes inalámbricas sencillas incluyendo el uso de un punto de acceso para proporcionar conexión a una red cableada, pero en muchas ocasiones el alcance o las prestaciones de un solo punto de acceso no son suficientes. En este caso, el estándar define el uso de la configuración **ESS** cuya principal función es la ampliación de la cobertura de una red inalámbrica mediante el uso de varios puntos de acceso.

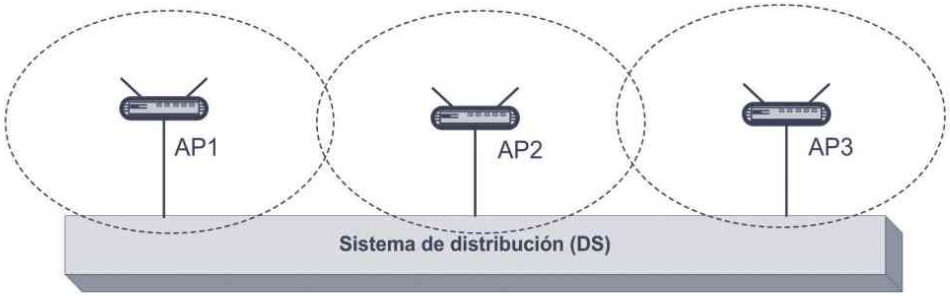


***Figura 11.4**. Configuración ESS con varios puntos de acceso*

El estándar IEEE 802.11 define la existencia de la configuración ESS y define los servicios necesarios para implementar esta configuración pero no los desarrolla. Debido a ello, y para evitar problemas de compatibilidad, es aconsejable utilizar puntos de acceso del mismo fabricante para la puesta en servicio de una configuración ESS.

Como se observa en la figura anterior, el uso de varios puntos de acceso amplía el área de cobertura de la red inalámbrica ampliando además el número de dispositivos que pueden estar conectados simultáneamente.

La comunicación entre los puntos de acceso para realizar operaciones de gestión de la red inalámbrica se lleva a cabo mediante lo que el estándar denomina **Sistema de Distribución** (DS, *Distribution System*). Este sistema de distribución debe permitir la comunicación entre los diferentes puntos de acceso que forman la red inalámbrica. Existen dos posibilidades:

- **DS cableado**. En este caso, la infraestructura que comunica los puntos de acceso es una red local Ethernet.

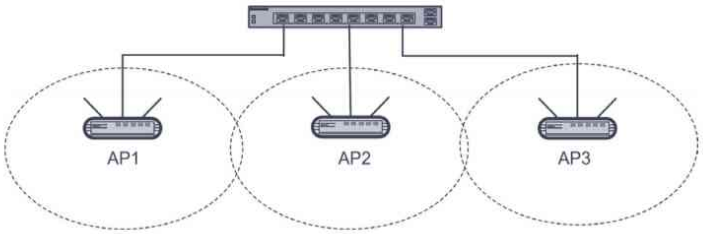


***Figura 11.5**. Configuración ESS con DS cableado*

- **DS inalámbrico**, también conocido como **WDS** (*Wireless Distribution System*). En este caso, los puntos de acceso se comunican mediante un enlace inalámbrico.

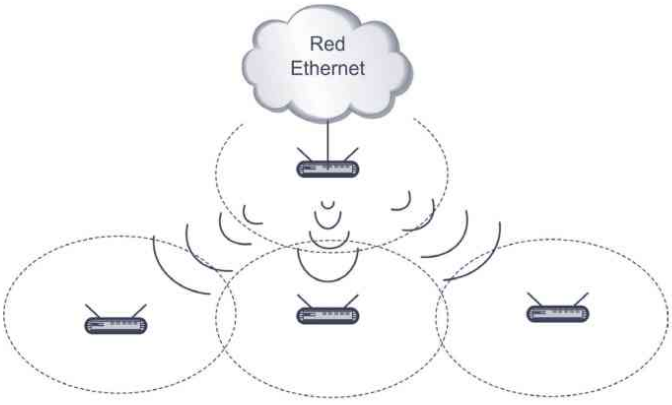


***Figura 11.6**. Configuración ESS con DS inalámbrico (WDS)*

11.3.3 MODO BRIDGE (PUENTE)

Algunos puntos de acceso ofrecen el llamado modo *bridge* o modo puente que permite la conexión de dos redes locales cableadas mediante un enlace inalámbrico. Este modo de funcionamiento no forma parte del estándar por lo que es muy recomendable utilizar dispositivos del mismo fabricante para establecer un puente inalámbrico. Existen dos modos de operación en este caso:

- **Punto a punto** (*Point-to-point bridge*). Los puntos de acceso configurados en modo punto a punto establecer un enlace inalámbrico entre dos puntos de acceso por lo que no permiten la conexión de dispositivos, ya que no constituyen una red inalámbrica.

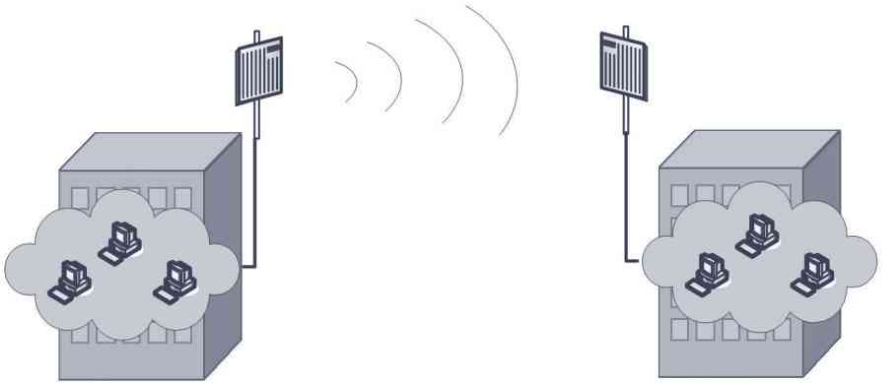


***Figura 11.7**. Enlace inalámbrico con dos puntos de acceso configurados en modo bridge*

- **Punto a multipunto** (*Point-to-multipoint bridge*). Un punto de acceso que admita este modo de funcionamiento podrá establecer varios enlaces inalámbricos con otros puntos de acceso. Igual que en modo punto a punto no es posible la conexión de dispositivos para establecer una red inalámbrica.

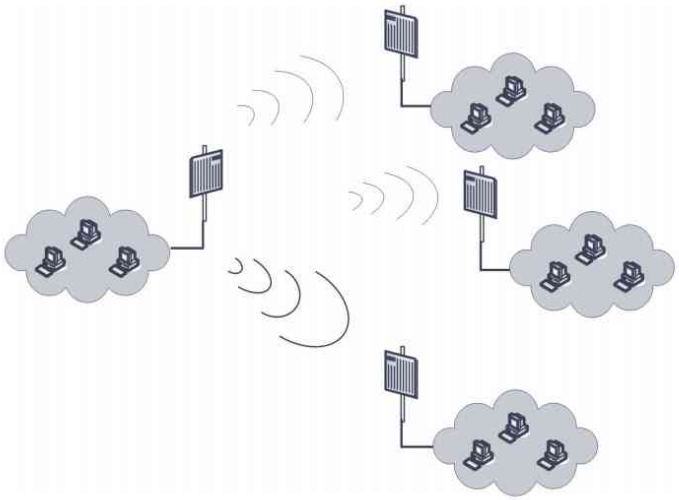


***Figura 11.8**. Enlaces inalámbricos en modo punto a multipunto*

11.3.4 IDENTIFICADOR DE UNA RED INALÁMBRICA: SSID

El método utilizado en el estándar IEEE 802.11 para identificar una red inalámbrica es mediante un identificador conocido como **SSID** (*Service Set Identifier*). El estándar establece realmente dos niveles de identificadores:

- **BSSID** (*Basic Service Set Identifier*)
  Se utiliza para identificar una red BSS. Este identificador es un valor numérico de 48 bits representado con un formato similar al de una dirección MAC. Para el modo ad-hoc el identificador se establece como un valor aleatorio. En el modo infraestructura este valor está asignado por el punto de acceso con un valor establecido de fábrica (similar a las direcciones MAC).
- **ESSID** (*Extended Service Set Identifier*)
  El identificador utilizado para configuraciones ESS es un valor alfanumérico de 32 *bytes* (distingue entre mayúsculas y minúsculas) y es configurado por el administrador de la red en el punto de acceso.

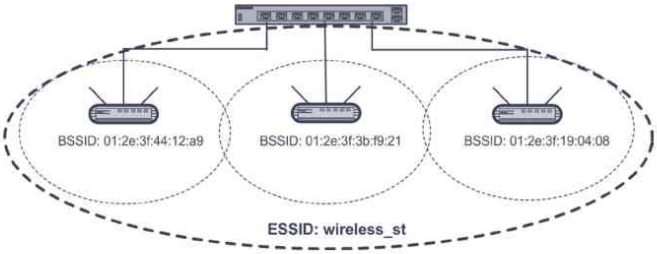


***Figura 11.9**. Configuración ESS con todos sus identificadores*

Actualmente, el identificador ESSID es el valor utilizado para identificar todas las redes inalámbricas Wi-Fi aunque operen con un solo punto de acceso (es decir, en modo infraestructura).

11.4 CANALES

En las diferentes versiones del estándar IEEE 802.11 se han utilizado dos bandas de frecuencia, la banda situada en 2,4 GHz y la de 5 GHz. En ambos casos, la banda se divide en canales por los que se lleva a cabo la transmisión. Cada red Wi-Fi utiliza un solo canal en alguna de las bandas.

En el caso de la banda de 2,4 GHz, su principal característica es que dichos canales están solapados, como se puede apreciar en la Figura 11.10, por lo que si hay dos redes Wi-Fi en funcionamiento con un área de cobertura común, dichas redes producirán interferencias entre sí si utilizan canales cercanos. De hecho, la distancia entre canales para que no haya solapamiento y, por tanto, interferencias, es de 5 canales.

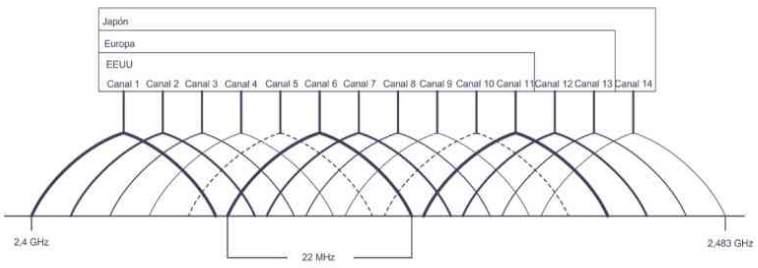


***Figura 11.10**. Asignación de canales en la banda de 2,4 GHz*

Otra característica a tener en cuenta es que, debido a las restricciones de los organismos de regulación del espectro radioeléctrico, no todos los canales tienen permitido su uso en los diferentes países. Así, por ejemplo, en Europa se permite el uso de los canales del 1 al 13. Sin embargo, en EE.UU. solo se permite utilizar los canales del 1 al 11. En Japón se añade un canal adicional, el canal 14.

En definitiva, dos redes Wi-Fi funcionando en un área de cobertura común deberían utilizar canales diferentes con una separación de 5 canales, por ejemplo, 3 y el 8. Esta distribución de los canales permitiría un máximo de tres redes Wi-Fi operando en la misma área de cobertura sin producir interferencias entre ellas, utilizando los canales 1, 6 y 11. Para Europa, además, se podría utilizar una asignación de canales que permitiría hasta cuatro canales en la misma área de cobertura con un solapamiento mínimo. Los canales utilizados serían el 1, 5, 9 y 13.

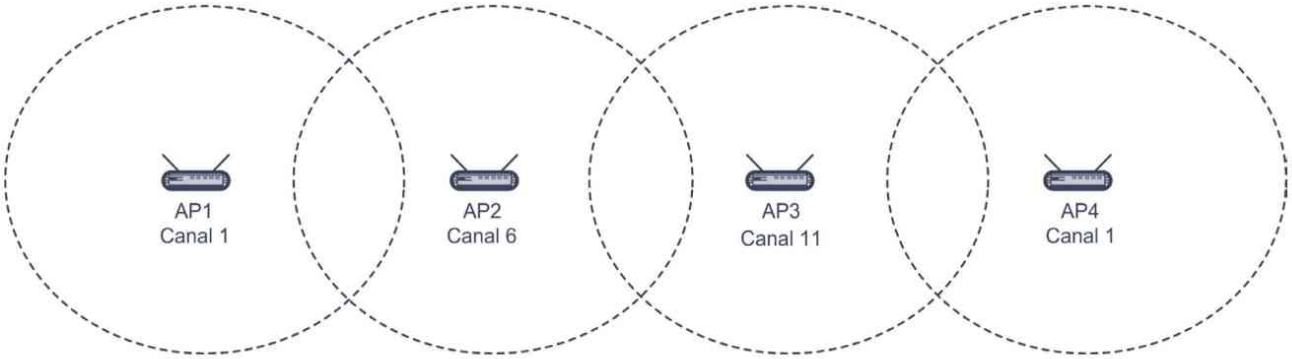


***Figura 11.11**. Estrategia típica de reutilización de canales en una red ESS*

En el estándar IEEE 802.11n además, se pueden utilizar canales de 40 MHz en la banda de 2,4 GHz. Gracias a ello se duplica la velocidad de transmisión pero reduce el uso de canales simultáneos a solo 2. El uso de canales de 40 MHz está recomendado en redes Wi-Fi a la que solo se conecten dispositivos que usen el estándar IEEE 802.11n.

Una de las principales novedades del estándar IEEE 802.11n es que también puede utilizar la banda de 5 GHz. El uso de la misma tiene dos grandes ventajas. La primera es que es una banda en general menos usada por otro tipo de dispositivos, por lo que no habrá tantos problemas de interferencias. La segunda es que hay más canales disponibles que en la banda de 2,4 GHz y, además, los canales no están solapados, por lo que no hay que preocuparse por el uso de los mismos. Normalmente, se puede dejar al punto de acceso que busque un canal libre de forma automática.

RECUERDA

En el caso de solapamiento de las áreas de cobertura de redes Wi-Fi trabajando en la banda de 2,4 GHz lo ideal es que haya una separación de 5 canales. Las opciones más utilizadas son:

- Canales 1, 6 y 11.
- Canales 1, 7 y 13.
- Canales 1, 5, 9 y 13.

En la banda de 5 GHz no hay problema de solapamiento.

11.5 ALCANCE Y NIVELES DE POTENCIA

Uno de los factores importantes a tener en cuando cuando se establece una red inalámbrica es el alcance de dicha red. Este alcance depende de varios factores:

- **Potencia de emisión del punto de acceso**. No está definido en el estándar ya que depende de los organismos de regulación de cada país. Habitualmente, los puntos de acceso utilizan valores máximos entorno a los 20 dBm que son unos 100 mW. El objetivo es cubrir una distancia de 100 metros libres de obstáculos.
- **Sensibilidad de los dispositivos inalámbricos**. Este parámetro se refiere a la potencia de señal mínima necesaria en el receptor para la recepción de los datos. Este parámetro se expresa en dBm.
- **Obstáculos en el área de cobertura**. Las frecuencias utilizadas en Wi-Fi son sensibles a los obstáculos que haya en el recorrido entre el emisor y el receptor, por tanto, el alcance de la comunicación será sensiblemente inferior cuando existen obstáculos. Hay que considerar también el tipo de material del obstáculo ya que el índice de absorción de las ondas no es el mismo en cada material. Así, por ejemplo, el hormigón genera muchas más pérdidas en las ondas utilizadas en Wi-Fi que la madera, el plástico o el vidrio.

Para mejorar el alcance y cobertura de una red Wi-Fi existen en el mercado antenas que proporcionan características mejoradas respecto a las que incluyen los dispositivos por defecto. El uso de antenas externas solo es posible en dispositivos Wi-Fi que incluyan el conector adecuado.

***Figura 11.12**. Antena Wi-Fi con el detalle del conector coaxial*

Habitualmente los parámetros de potencia se especifican en una unidad llamada **dBm**, que es una unidad logarítmica que utiliza como referencia 1 mW. La relación entre valores en dBm y en mW es la siguiente:

$$P\,(dBm) = 10 \cdot \log P\,(mW)$$

$$P\,(mW) = 10^{\frac{P\,(dBm)}{10}}$$

11.6 DIRECCIONAMIENTO

Al igual que ocurre con Ethernet en redes cableadas, en redes inalámbricas también es necesario asignar una dirección física que identifique a cada dispositivo en el nivel de enlace. Por compatibilidad con Ethernet, en el estándar IEEE 802.11 se utiliza el mismo formato de dirección física, es decir, es un número de 48 bits donde los 24 primeros bits representan el fabricante.

Al igual que en Ethernet, la dirección física de los dispositivos inalámbricos se establece en la fabricación, no se puede modificar y habitualmente se representa en formato hexadecimal.

11.7 ACCESO AL MEDIO COMPARTIDO: CSMA/CA

Dentro de una red inalámbrica todas las transmisiones se hacen utilizando la misma banda de frecuencias, por lo que se puede considerar que el medio de transmisión está compartido (igual que los *hubs* en redes cableadas) y, por tanto, es necesario establecer algún mecanismo de acceso a dicho medio compartido.

RECUERDA

Lógicamente el uso de un medio de transmisión compartido (en este caso un canal de radiofrecuencia) hace que las transmisiones en redes inalámbricas se consideren transmisiones **half-dúplex**.

CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) es la técnica para llevar a cabo el control de acceso al medio en las redes inalámbricas. Su funcionamiento básico es el siguiente:

- Un dispositivo que quiere transmitir primero escucha el medio.
- Si el medio está ocupado, espera un tiempo aleatorio.
- Cuando transcurre ese tiempo, el dispositivo escucha de nuevo el medio. Si está libre transmite.

Con este funcionamiento básico se evitan las colisiones de tramas cuando todos los dispositivos de la red están dentro del área de cobertura del resto de dispositivos. Pero el uso de puntos de acceso produce una situación conocida como **problema del nodo oculto**, que ocurre cuando un dispositivo no detecta que otro está transmitiendo porque está fuera de su alcance (nodo oculto) aunque sí esté en el área de cobertura del punto de acceso. Para solucionarlo se añade al método básico descrito anteriormente el uso de tramas de control llamadas RTS y CTS. El funcionamiento es el siguiente:

- Cuando un dispositivo quiere transmitir (y el medio está libre) transmite la trama de control **RTS** (*Request To Send*, Petición para enviar) indicando además el tiempo que necesita para enviar su trama de datos.
- El punto de acceso envía una trama **CTS** (*Clear To Send*, Preparado para enviar) a todos los dispositivos de la red aceptando la solicitud de envío e informando al resto que no está permitido enviar nada en el tiempo especificado en la trama RTS.
- Si un dispositivo envía una trama RTS y no obtiene respuesta después de un tiempo, retransmite la trama RTS de nuevo (si el medio está libre). Esto puede ocurrir cuando dos dispositivos envían su trama RTS a la vez. En ese caso se produciría una colisión y se perderían las tramas. Es el único caso de colisión que se puede producir.

11.8 SEGURIDAD

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 porque, 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. El mecanismo estándar de seguridad en Wi-Fi incluye tanto la autenticación de la conexión como el cifrado de los datos. Actualmente, los dispositivos Wi-Fi se pueden configurar con varios mecanismos de seguridad.

11.8.1 WEP

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, por lo que actualmente no se aconseja su uso. Se basa en la utilización de claves simétricas con las que se lleva a cabo la encriptación de los datos basándose en un algoritmo llamado **RC4**.

Para utilizar WEP es necesario configurar, tanto en el punto de acceso como en los dispositivos de la red, una clave de auntenticación común para todos ellos. Esta clave admite dos formatos:

- **Formato corto**: pueden ser 10 caracteres hexadecimales ó 5 caracteres alfanuméricos. El valor obtenido será de 40 bits en ambos casos.
- **Formato largo**: pueden ser 26 caracteres hexadecimales ó 13 caracteres alfanuméricos. El valor obtenido será de 104 bits.

La clave o contraseña de validación se utiliza junto con un vector de inicialización de 24 bits para generar la clave de encriptación, que será de 64 ó 128 bits.

11.8.2 WPA

Debido a las debilidades de WEP, el IEEE comenzó a desarrollar un nuevo estándar de seguridad más robusto que WEP al que se le asignó la numeración oficial IEEE 802.11i. Sin embargo, la Wi-Fi Alliance decide no esperar a la finalización del estándar del IEEE y basándose en los desarrollos preliminares desarrolla una nueva especificacón de seguridad para los dispositivos Wi-Fi conocida como **WPA** (*Wi-Fi Protected Access*, Acceso protegido Wi-Fi). Esta especificación utiliza un nuevo protocolo de seguridad llamado **TKIP** (*Temporal Key Integrity Protocol*), que es el mismo que se utiliza en el estándar IEEE 802.11i. Una ventaja proporcionada por esta especificación es que se puede emplear el mismo hardware que WEP, es decir, no es necesario cambiar los dispositivos inalámbricos, 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. Corrige fallos de seguridad y 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.

El nuevo estándar además incluye un robusto 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 autenticación:

- **WPA-Enterprise**. El proceso de autenticación se lleva a cabo a través de un servidor de autenticación (normalmente un servidor RADIUS) y se utiliza habitualmente en entornos profesionales.

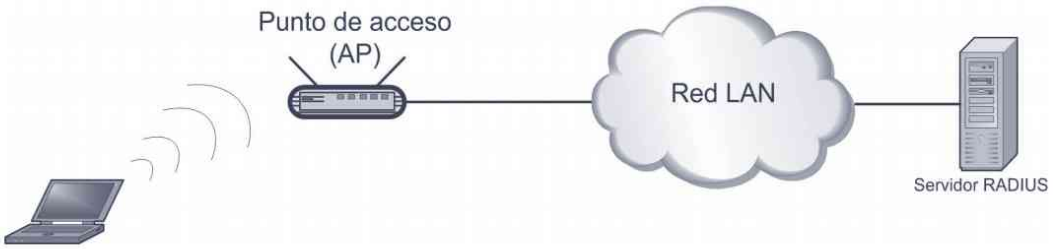


Figura 11.13. *Arquitectura de autenticación con servidor RADIUS*

- **WPA Personal** o **WPA-PSK** (WPA *Pre-Shared Key*). Se lleva a cabo través de una clave precompartida y se utiliza en entornos menos restrictivos y entornos domésticos. Dicha clave es un valor de 256 bits, que suele ser solicitada en formato alfanumérico como una cadena de 8 a 63 caracteres (se utiliza formato ASCII de 7 bits por carácter).

11.8.3 WPA2

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. En la siguiente tabla se muestra un resumen de las características de los tres estándares de seguridad Wi-Fi:

Estándar	Protocolo de seguridad	Encriptación	Autenticación
IEEE 802.11	WEP	RC4	No hay
WPA(Wi-Fi Alliance)	TKIP	RC4	IEEE 802.1x (EAP)
WPA2 (IEEE 802.11i)	TKIP	AES	IEEE 802.1x (EAP)

11.8.4 MECANISMOS DE SEGURIDAD COMPLEMENTARIOS

Además de los mecanismos de seguridad descritos en el apartado anterior, la mayor parte de los puntos de acceso inalámbrico proporcionan dos mecanismos de seguridad complementarios:

- **SSID (identificador de red) oculto**

  Este mecanismo de seguridad consiste en la no emisión de tramas baliza (*Beacon frames*) por parte del punto de acceso. De esta forma, la red no está "anunciada" y no aparecerá en la lista de redes disponibles en los dispositivos con capacidades inalámbricas.

  Para acceder a una red con el SSID oculto es necesario conocer dicho SSID y especificarlo en las opciones de configuración del dispositivo inalámbrico que desea acceso a dicha red. Aunque esta característica puede ayudar a evitar accesos no deseados, no se considera un método de seguridad efectivo y solo deberá ser usado como complemento a los mecanismos de seguridad del estándar IEEE 802.11.

La activación de esta característica depende del modelo de punto de acceso. En la Figura 11.14 se utiliza un parámetro llamado *Broadcast Essid* (difusión de ESSID) que permite dos valores *Enable* (Habilitar) y *Disable* (Deshabilitar). Para activar la característica de SSID oculto hay que elegir la opción *Disable*.

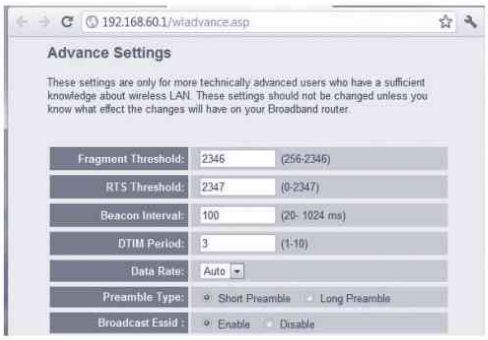


***Figura 11.14**. Uso de SSID oculto seleccionando la opción Disable del parámetro Broadcast Essid*

Filtrado de direcciones MAC

Los puntos de acceso que proporcionan este mecanismo de seguridad ofrecen una opción de configuración que permite especificar una lista de las direcciones MAC de los dispositivos inalámbricos que tienen permiso de acceso a la red inalámbrica, de forma que un dispositivo inalámbrico cuya MAC no esté en la lista no tendrá acceso a dicha red.

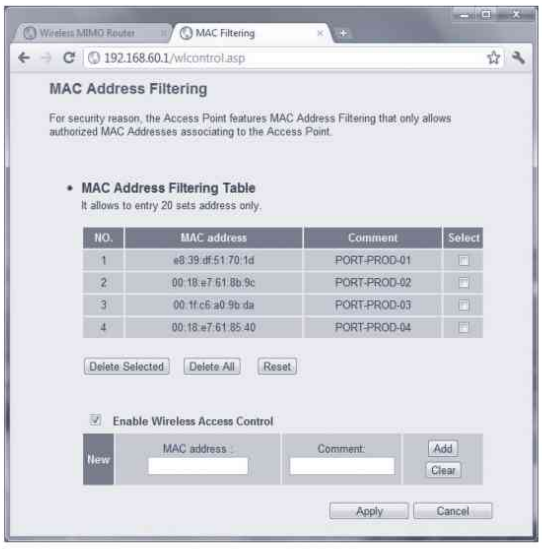


***Figura 11.15**. Ejemplo de configuración de filtrado de direcciones MAC*

Al igual que el mecanismo de SSID oculto, éste tampoco se consiera un método fiable y de igual modo, solo se utilizará junto con algún sistema de seguridad como WPA o WPA2. El filtrado de direcciones MAC no es factible en sistemas Wi-Fi donde los usuarios conectados al sistema no son fijos, como en hoteles, puntos de acceso públicos, etc.

11.9 DISPOSITIVOS INALÁMBRICOS

Después de hacer un repaso a todas las principales características de las redes inalámbricas, en este apartado se expondrán los principales tipos de dispositivos que existen en el mercado para su uso en redes inalámbricas.

11.9.1 TARJETAS DE RED INALÁMBRICAS

Los elementos básicos de cualquier red inalámbrica son las tarjetas de red inalámbricas y los puntos de acceso inalámbricos. Cualquier equipo o dispositivo que necesite conectarse a una red inalámbrica debe incluir las funciones de la tarjeta de red inalámbrica. En muchas ocasiones estas funciones no están localizadas en una tarjeta o módulo independiente, sino que están incluídas dentro del propio hardware del dispositivo. Esto ocurre por ejemplo en los ordenadores portátiles. Igualmente, los teléfonos de última generación o *smartphones* también incluyen las funciones de las tarjetas inalámbricas.

***Figura 11.16**. El segundo icono por la izquierda es el indicador de conexión inalámbrica en un portátil*

***Figura 11.17**. Símbolo de conectividad Wi-Fi utilizado en dispositivos electrónicos como smartphones*

Para los equipos de sobremesa que no incluyen las funciones inalámbricas por defecto, se pueden incorporar tarjetas conectadas a un puerto PCI, o se puede optar por utilizar una tarjeta inalámbrica conectada a un puerto USB. Esta última suele ser la opción más cómoda y flexible.

***Figura 11.18**. NIC inalámbrica por USB conocida como USB Wi-Fi y NIC inalámbrica por puerto PCI*

***Figura 11.19**. NIC inalámbrica IEEE 802.11n que utiliza la funcionalidad MIMO*

La popularidad y flexibilidad de Wi-Fi ha propiciado la aparición de cada vez más dispositvos que utilizan esta tecnología para el acceso a una red de datos. Por ello, existen otros dispositivos que incluyen este tipo de conectividad como cámaras IP, impresoras o dispositivos multimedia.

11.9.2 PUNTOS DE ACCESO (AP)

Los puntos de acceso son los dispositivos utilizados para constituir una red inalámbrica, tanto en la configuración BSS en modo Infraestructura como en la configuración ESS utilizando varios puntos de acceso para ampliar el alcance de una red inalámbrica. Todos los puntos de acceso proporcionan un puerto Ethernet para su conexión con la red cableada.

La principal característica de un punto de acceso es el soporte de los diferentes estándares. En la actualidad pueden ofrecer hasta el IEEE 802.11n aunque ofrecen compatibilidad con versiones anteriores. Además, habrá que tener en cuenta otras características como es el soporte PoE (*Power over Ethernet*) o el modo WDS (*Wireless Distribution System*), también conocido como modo repetidor (*repeater*).

***Figura 11.20**. Puntos de acceso inalámbrico*

Todos los puntos de acceso requieren la configuración de varias características y para ello proporcionan acceso a su configuración mediante un servicio web interno accesible mediante un equipo con un navegador web.

11.9.3 PUENTES INALÁMBRICOS

Los puentes (*bridge*) inalámbricos ofrecen las funcionalidades de un punto de acceso incluyendo la configuración en modo puente punto a punto y punto a multipunto. Se utilizan para conectar redes locales en ubicaciones diferentes pero con buena línea de visión directa. Su característica más destacada es que están preparados para ser instalados en el exterior, por lo que están montados en una carcasa protectora y reciben alimentación a través del cable Ethernet mediante PoE (*Power over Ethernet*).

***Figura 11.21**. Puente inalámbrico para montaje en el exterior*

11.9.4 ROUTER BANDA ANCHA CON CAPACIDADES INALÁMBRICAS

El uso de Wi-Fi a nivel doméstico se ha hecho muy popular debido a que en la actualidad todos los provedores de conexión a Internet (ISP) proporcionan un *router* para dicha conexión que incluye la funcionalidad de un punto de acceso.

Habitualmente, estos *routers* funcionan en modo infraestructura. Utilizan como identificador de red un ESSID y suelen dar servicio a unos pocos dispositivos inalámbricos.

***Figura 11.22**. Router de banda ancha que incluye funciones de punto de acceso*

RECUERDA

La mezcla de los términos Wi-Fi e Internet

La mayor parte de los usuarios domésticos utilizan el *router* proporcionado por su provedor de acceso a Internet (ISP) exclusivamente para la conexión a Internet. Esto lleva a creer que Wi-Fi es una tecnología de acceso a Internet y esto no es cierto. Wi-Fi es una tecnología de redes locales inalámbricas que permite el acceso inalámbrico al *router*, y es el *router* el que nos proporciona acceso a Internet. Recuerde que dicho *router*, además de proporcionar acceso a Internet, nos permite establecer una red local con cuatro dispositvos conectados por Ethernet y varios más mediante conexión inalámbrica Wi-Fi.

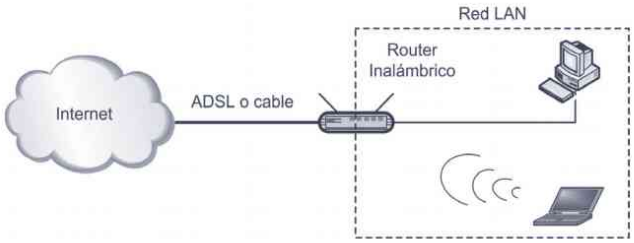


***Figura 11.23**. Uso de Wi-Fi en una red doméstica*

11.10 CONFIGURACIÓN DE REDES INALÁMBRICAS

11.10.1 CONFIGURACIÓN DE UN PUNTO DE ACCESO

El método más habitual para configurar un punto de acceso es la utilización de un servicio web interno al propio punto de acceso que permite visualizar y modificar los diferentes parámetros de configuración. Para habilitar este servicio hay que establecer la configuración de red para dicho punto de acceso, esto es, habrá que configurar una dirección de red y una máscara de subred. Esta dirección IP tiene una función exclusiva de configuración, por lo que no se puede considerar un punto de acceso como un dispositivo de nivel 3, sino de nivel 2, igual que un *switch*.

Por lo tanto, para acceder a la configuración de un punto de acceso basta utilizar un navegador web (Explorer, Firefox, Chrome…) en cualquier equipo que esté conectado a la misma red que el punto de acceso, escribiendo en la barra de direcciones del navegador la dirección IP del punto de acceso.

IMPORTANTE

En pequeñas redes privadas, lo más habitual es utilizar direcciones IP con el formato **192.168.A.B** donde A es un número entre 0 y 255 que identifica una red y B es un número entre 1 y 254 que identifica un equipo dentro de la red. Ejemplos:

- 192.168.0.1 y 192.168.0.2 serían las direcciones IP de dos equipos dentro de la misma red ya que el tercer número de cada dirección es el mismo (el 0).
- 192.168.0.1 y 192.168.10.2 serían las direcciones IP de dos equipos situados en diferentes redes, ya que el tercer número de cada dirección es diferente (el 0 y el 10).
- En cuanto a la máscara de subred, para direcciones de red con el formato 192.168.A.B y donde no existen subredes se utiliza la máscara **255.255.255.0**.

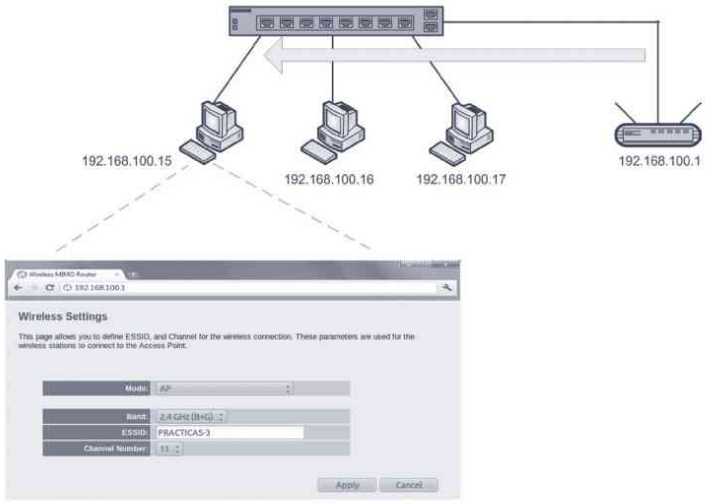


Figura 11.24. *Acceso a la configuración de un punto de acceso*

Las pantallas de configuración pueden variar entre diferentes modelos de puntos de acceso y las prestaciones que ofrezcan. En muchos casos, los fabricantes no ofrecen soporte multilingüe y solo proporcionan la información en inglés.

Las opciones más comunes que se pueden configurar en un punto de acceso son:

- **Nombre de la red** (SSID). Este valor será un nombre de hasta 32 caracteres.
- **Modo de operación**.
- **Canal de transmisión**. Algunos puntos de acceso proporcionan una opción de selección automática del canal.
- **Tipo de seguridad**. Habitualmente estarán disposibles los tres tipos: WEP, WPA y WPA2. Si se utiliza el modo Enterprise de WPA/WPA2, además se deberá configurar la dirección IP del servidor RADIUS, que hará la validación de usuarios.

***Figura 11.25**. Pantalla de configuración de la seguridad en un punto de acceso*

- **Dirección IP y máscara de subred**. Son parámetros del nivel de red utilizados solo para el acceso a la configuración del dispositivo. Típicamente se utilizan direcciones IP privadas en el rango 192.168.A.B con la máscara de subred 255.255.255.0.
- **Intervalo de transmisión de las tramas baliza** (*beacon frames*) **para anunciar la red**. Por defecto suele ser 100 ms.
- **Nivel de potencia de transmisión**.

Para llevar a cabo la configuración inicial lo habitual es conectar el PC al puerto Ethernet del punto de acceso y utilizar la dirección IP configurada por defecto, que el fabricante suele facilitar en el manual.

11.10.2 CONFIGURACIÓN DE UN DISPOSITIVO EQUIPADO CON CONECTIVIDAD INALÁMBRICA

Cada vez son más numerosos los tipos de dispositivos electrónicos que proporcionan conectividad inalámbrica mediante el estándar IEEE 802.11. Además de los PC y ordenadores portátiles, hay que añadir los *smartphones*, *netbooks*, *tablets*, PC, impresoras, cámaras y, en general, cualquier dispositivo que se pueda conectar a una red local.

Debido a esta gran variedad, también existe una gran variedad de procedimientos de configuración aunque lo más habitual es que el propio dispositivo proporcione una función de búsqueda de redes inalámbricas, que mostrará la lista de redes disponibles en el área de cobertura del dispositivo. Bastará con seleccionar el nombre (SSID) de la red inalámbrica a la que queramos conectarnos e introducir la contraseña del método de seguridad utilizado en dicha red.

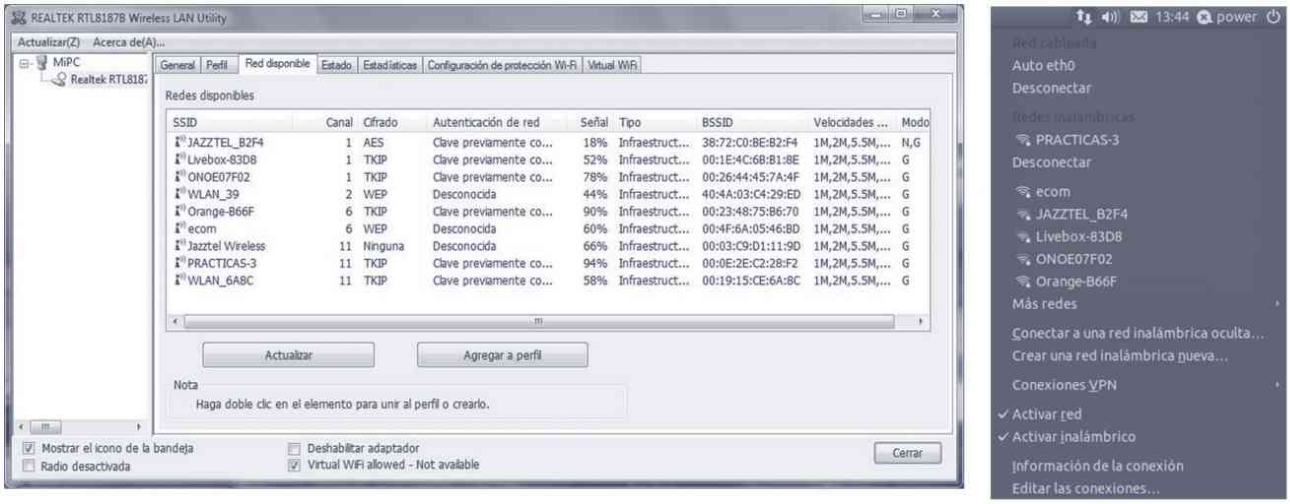


***Figura 11.26**. Ventana para visualizar las redes disponibles en Windows® 7 y en Ubuntu*

Los dispositivos también ofrecen la posibilidad de configurar manualmente la conexión a una red inalámbrica. En este caso, los parámetros necesarios son el nombre de la red (SSID), el tipo de seguridad y la contraseña.

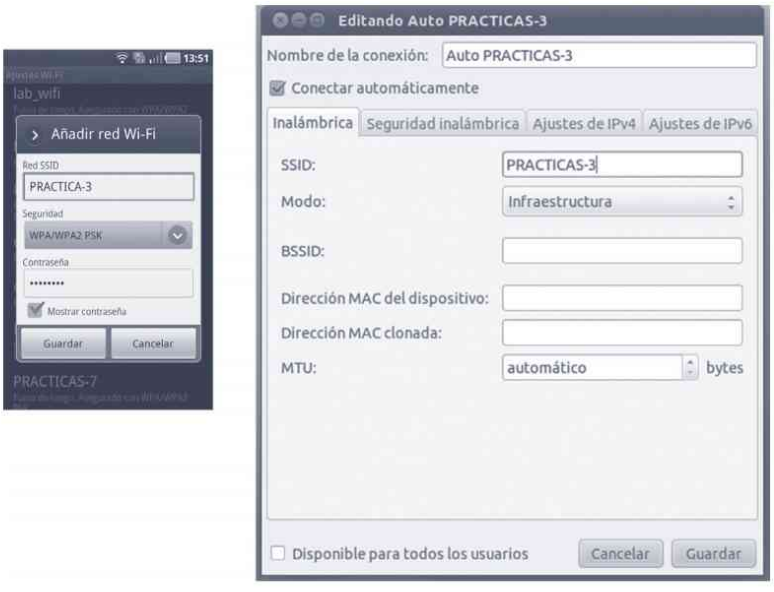


***Figura 11.27**. Configuración de una red Wi-Fi en un Smartphone y en Ubuntu*

Para el caso de ordenadores, antes de poder utilizar las funciones inalámbricas es necesario instalar los correspondientes controladores para que el sistema operativo reconozca el hardware que lleva a cabo las funciones de conectividad inalámbrica. Para el caso de ordenadores portátiles, el fabricante suele incluir dichos controladores preinstalados.

En el caso de instalar tarjetas Wi-Fi externas al equipo, como una tarjeta PCI o una tarjeta USB Wi-Fi, el fabricante proporcionará los controladores apropiados para el sistema operativo utilizado. Habitualmente se proporcionarán los controladores para sistemas Windows®.

En el caso de Linux, no todos los fabricantes proporcionan controladores. Será necesario consultar foros en Internet para encontrar el procedimiento de instalación del controlador adecuado. El comando utilizado en Linux para configurar los parámetros de la red inalámbrica es *iwconfig*. Ejecutado sin parámetros muestra información sobre la configuración actual.

RESUMEN DEL CAPÍTULO

Sin duda, una de las tecnologías que ha experimentado un mayor auge es la utilizada para implementar redes LAN inalámbricas. Dicha tecnología es un estándar publicado como IEEE 802.11, aunque se conoce más por el término Wi-Fi.

En este capítulo se muestran las principales características del estándar Wi-Fi, especialmente los relacionados con los diferentes modos de funcionamiento, como pueden ser el modo Ad-hoc, el modo Infraestructura, la configuración ESS, incluyendo WDS y el modo *Bridge*.

Además, se incluyen los diferentes mecanismos de seguridad para redes inalámbricas Wi-Fi y se hace un repaso de los diferentes dispositivos que implementan esta tecnología.

EJERCICIOS PROPUESTOS

1. Buscar en Internet información sobre las características de varios modelos de puntos de acceso y de tarjetas de red inalámbricas.

2. Probar las funciones de la herramienta de planificación de una red inalámbrica proporcionada en la página web *www.airtightnetworks.com*.

- Acceder a la opción *RF Planning* y seleccionar *802.11n WLAN Coverage Estimator* (esta página está en inglés).

3. Estudiar el funcionamiento de la técnica CSMA/CA mediante la animación disponible en la página web:

- *media.pearsoncmg.com/aw/aw_kurose_network_2/applets/csma-ca/withouthidden.html*

4. La página mostrada a continuación contiene un simulador de la configuración de un punto de acceso inalámbrico. Acceder a dicha página y comprobar todas las funcionalidades que ofrece.

- *ui.linksys.com/files/WAG120N/1.00.11/setup.cgi@next_file=Setup.htm*

TEST DE CONOCIMIENTOS

1 La principal diferencia entre IEEE 802.11b y IEEE 802.11g es:
- a) IEEE 802.11b no es un estándar abierto y IEEE 802.11g sí lo es.
- b) IEEE 802.11b no incluye mecanismos de seguridad y IEEE 802.11g sí los incluye.
- c) IEEE 802.11b alcanza 11 Mbps y IEEE 802.11g alcanza hasta 54 Mbps.
- d) IEEE 802.11b opera en la banda de 2.4 GHz y IEEE 802.11g en la banda de 5 GHz.

2 Las tecnologías de redes LAN inalámbricas implementan las funciones OSI:
- a) De todos los niveles excepto el de aplicación.
- b) De los niveles físico y de enlace.
- c) De los niveles físico, de enlace y de red.
- d) Depende del tipo de red.

3 El sistema de seguridad Wi-Fi conocido como WPA:
- a) Fue el primer sistema de seguridad implementado y el más inseguro.
- b) Fue desarrollado por la Wi-Fi Alliance como una mejora de WEP.
- c) No se utiliza actualmente por ser demasiado complejo.
- d) Es incompatible a nivel hardware con WEP.

4 El direccionamiento físico utilizado en IEEE 802.11:
- a) Utiliza el mismo formato que Ethernet.
- b) Utiliza el mismo formato que IP.
- c) Utiliza un formato propio de direcciones de 128 bits.
- d) En IEEE no es necesario direccionamiento físico, solo lógico.

5 El estándar IEEE 802.11n:
- a) Utiliza solo la banda de 5 GHz.
- b) Utiliza solo la banda de 2,4 GHz.
- c) Utiliza las bandas de 2,4 y 5 GHz.
- d) Este estándar aún no está desarrollado.

6 En la configuración ESS de una red inalámbrica:
- a) Se utiliza un identificador numérico llamado BSSID común para todos los puntos de acceso.
- b) Se utiliza un identificador alfanumérico llamado ESSID para cada punto de acceso.
- c) Cada punto de acceso tiene su propio identificador numérico (BSSID) y su propio identificador alfanumérico (ESSID).
- d) Se utiliza un identificador alfanumérico llamado ESSID común a todos los puntos de acceso.

7 El modo de operación conocido como Infraestructura:
- a) Permite la conexión de la red inalámbrica a una red cableada.
- b) Permite la conexión de un número mayor de dispositivos que el modo Ad-hoc.
- c) Proporciona mayor área de cobertura que el modo Ad-hoc.
- d) Todas las respuestas anteriores son correctas.

8 La tecnología MIMO que aprovecha las multirutas de las señales radioeléctricas se utiliza en el estándar:
- a) IEEE 802.11a.
- b) IEEE 802.11n.
- c) IEEE 802.11g.
- d) IEEE 802.11b.

9 Para utilizar el modo infraestructura en una red inalámbrica:
- a) Hay que emplear un punto de acceso.
- b) Hay que emplear varios puntos de acceso.
- c) Hay que emplear al menos una tarjeta de red inalámbrica que lo soporte.
- d) Hay que emplear el estándar IEEE 802.11g o superior.

10 Para unir dos redes cableadas con un enlace inalámbrico se emplea:
- a) El modo Infraestructura.
- b) El modo Ad-hoc.
- c) El modo *Bridge*.
- d) El modo ESS.

11 La transmisión de datos en una red inalámbrica es *half-dúplex*:
- a) En el modo Ad-hoc.
- b) En el modo Infraestructura.
- c) En el modo ESS.
- d) En todos los casos.

12 Un dispositivo Wi-Fi tiene acceso a Internet:
- a) Siempre.
- b) Si se conecta a un *router* de banda ancha (ADSL o cable) con funciones inalámbricas.
- c) Solo si se contrata una conexión Wi-Fi a un operador (ISP).
- d) Solo si el dispositivo dispone además de conectividad 3G.

12 Mantenimiento y puesta en servicio de sistemas informáticos

OBJETIVOS DEL CAPÍTULO

- ✓ Aprenderá a diagnosticar problemas en equipos microinformáticos y resolverlos.
- ✓ Conocerá las operaciones de mantenimiento más frecuentes en equipos informáticos.
- ✓ Aprenderá a prevenir problemas y averías que se puedan producir en un equipo informático.
- ✓ Aprenderá a realizar operaciones de mantenimiento sencillas en portátiles y otros equipos.
- ✓ Conocerá los problemas más comunes que se puedan presentar en equipos portátiles y de sobremesa.
- ✓ Aprenderá a utilizar herramientas para la clonación y particionado de equipos.
- ✓ Aprenderá a respaldar la información de los sistemas informáticos y a recuperarla.

12.1 AVERÍAS EN SISTEMAS INFORMÁTICOS

PELIGRO

Los dos sitios más peligrosos a la hora de la manipulación son el interior de la fuente de alimentación y el interior del monitor. No deberían abrirse salvo que sea un técnico especialista en este tipo de aparatos.

La detección de averías es en algunos casos un enigma. Dependiendo de la experiencia del técnico los misterios se van despejando en mayor o menor medida. La experiencia ayuda mucho a la resolución de problemas.

IMPORTANTE

Recuerda que para abrir un equipo informático debe estar **apagado y sin batería** (en el caso de que sea un portátil). Siempre que se abra y se manipule un equipo informático hay que hacerlo con **herramientas adecuadas**, teniendo en cuenta **no dañar los componentes internos** del mismo (cuidado con la electrostática).

Hay que distinguir entre averías software y hardware. Normalmente, las averías software pueden resistirse más que las averías hardware.

Entre los fallos hardware hay que distinguir entre los fallos del montaje y los fallos que puedan ocurrir una vez que el equipo ya ha funcionado correctamente.

Para la detección de una avería es necesario conocer bien los síntomas, dependiendo de los síntomas que se aprecien en el equipo se optará por una opción u otra.

12.2 MANTENIMIENTO EN SISTEMAS INFORMÁTICOS

Definiríamos el mantenimiento de sistemas informáticos como aquellas operaciones necesarias para que los equipos se mantengan en perfecto estado de uso y sigan cumpliendo las funciones en base a las que fueron ensamblados. Dada la definición anterior se deduce que algunas funciones del mantenimiento será la subsanación de averías o prevención de las mismas, adaptación de los equipos a las nuevas necesidades o añadir nuevas funcionalidades y mejoras.

Dentro del mantenimiento de los sistemas informáticos se consideraría tanto el mantenimiento físico (reparación de averías, actualización de equipos, instalación de tarjetas y componentes) como del mantenimiento lógico (actualización

o instalación de *drivers*, clonaciones, *backup*, modificación de parámetros en sistemas operativos, instalación de periféricos, etc).

Existen varios tipos de mantenimiento. A continuación se detallan cada uno de ellos:

- **Mantenimiento correctivo**. Este mantenimiento se encarga de detectar fallos, analizarlos y solventarlos. Existen muchos tipos de fallos, algunos de ellos son debidos a un mal funcionamiento del software (errores en los *drivers*, sistema operativo, mala configuración del sistema, etc.), otros fallos son fallos pueden ser debidos al hardware (averia en un disco duro, placa base, etc).

- **Mantenimiento preventivo o planificado**. Este tipo de mantenimiento se realiza antes que ocurra cualquier fallo o avería del sistema informático, bajo condiciones controladas, en momentos en los que los equipos no están siendo utilizados. Generalmente, este tipo de mantenimientos están totalmente planificados, las actividades a realizar están bastante detalladas y se tiene una estimación más o menos fiable de cuándo comienza y cuándo termina dicho plan de mantenimiento.

  Generalmente no se suelen hacer mantenimientos preventivos sobre el hardware de un equipo (por ejemplo, el cambiar una memoria o disco duro en previsión de que falle), lo que sí se suele hacer es realizar clonaciones o *backups* de equipos en previsión de que si falla el sistema informático se pueda recuperar. La razón de no hacer mantenimientos preventivos es por el coste. El cambiar piezas que no se han estropeado aumenta mucho el coste de un equipo informático en funcionamiento. Generalmente, lo que se hace es esperar a que el componente se estropee para repararlo.

- **Mantenimiento de emergencia**. Este tipo de mantenimiento se realiza en ocasiones cuando el mantenimiento preventivo no es posible. En estas ocasiones se realizan funciones o procedimientos para mantener el sistema informático operativo. En muchos casos, las reparaciones se quedan a la espera de una corrección de los fallos más planificada en otro momento. Por ejemplo, se estropea un portátil de un comercial de nuestra empresa y esta persona lo necesita con urgencia para trabajar. Una solución es arreglar el equipo e instalar los programas y datos básicos. En otro momento con más tiempo se le instalarán los demás programas y se copiarán los datos del equipo que le hagan falta.

- **Mantenimiento adaptativo**. Tiene por objetivo la modificación del sistema para ampliar sus funciones o adaptarse a las nuevas necesidades del proceso productivo. Muchas de estas transformaciones suelen tener origen en los cambios tecnológicos (adaptaciones tecnológicas). Por ejemplo, el instalar un lector de *blu-ray* para la lectura de discos con este formato para poder leer información de dichos soportes.

- **Mantenimiento perfectivo**. Consiste en la realización de mejoras, ampliando algunas de las limitaciones que tenían los equipos o adaptándolo de una manera más acorde a las necesidades. Generalmente, este tipo de mantenimiento busca la mejora del rendimiento o cambios en el mismo para que las futuras acciones de mantenimiento tengan un menor coste. Por ejemplo, el instalar un nuevo *driver* para una impresora que mejora ciertas prestaciones o el instalar alguna actualización de un programa ofimático que permite salvar documentos en PDF podrían ser acciones de un mantenimiento adaptativo.

  El mantenimiento adaptativo y perfectivo son muy parecidos. En el primero se adapta el sistema a nuevas necesidades y en el segundo se mejoran las características del sistema existente. Del mismo modo, el mantenimiento correctivo y de emergencia son también similares. El mantenimiento de emergencia se puede considerar como correctivo, lo único que lo diferencia es la urgencia del mismo. En el mantenimiento de urgencia el sistema informático debe dejarse en funcionamiento en seguida porque su utilización es fundamental.

12.3 NIVELES DE MANTENIMIENTO

En toda empresa se podrían establecer tres niveles de mantenimiento. Dado que el mantenimiento son todas las acciones necesarias para que los sistemas informáticos funcionen y estén operativos, los actores o personas responsables del mantenimiento serán muchas. A continuación detallaremos tres niveles de mantenimiento.

- **Nivel 1**. En este nivel es el propio usuario el que se encarga del mantenimiento de parte del sistema. Dependiendo del nivel de conocimiento del usuario, éste realizará más o menos acciones de mantenimiento. Por ejemplo, el realizar una copia de seguridad de ciertos datos del equipo en un disco compacto (DVD o CD) es una operación que puede ser realizada sin dificultad por un usuario con cierto nivel de conocimiento. Sin embargo, reemplazar un disco duro del equipo por otro de mayor capacidad, seguramente no podrá realizarla el usuario y será una operación a realizar por personal que se encargue del segundo nivel de mantenimiento.
- **Nivel 2**. En este nivel, el mantenimiento se realiza por personal informático o personal del servicio de mantenimiento de una empresa. Dependiendo del conocimiento informático de los empleados de la empresa dependerá que el personal dedicado al mantenimiento realice más o menos operaciones. Citaremos a continuación algunas operaciones que se realizan en este nivel de mantenimiento:
  - Operaciones de diagnóstico de problemas en sistemas informáticos.
  - Defragmentación y comprobación de soportes de información.
  - Mantenimiento de los soportes de información.
  - Almacenamiento y etiquetado de soportes de información.
  - Replicación de particiones y discos duros.
  - Instalación y particionado de soportes de información.
  - Tratamiento de residuos informáticos.
  - Mantenimiento de periféricos.
  - Instalación de *drivers* y nuevos periféricos.
- **Nivel 3**. En este nivel se realizan operaciones que no son posibles realizarlas por el personal de mantenimiento debido a que el producto está en garantía, las operaciones sobre el equipo son muy específicas, no se dispone de los medios o el tiempo necesario u otra razón. Una operación de este nivel sería, por ejemplo, la reparación de un monitor, de un *router* o de una impresora. Muchas veces, el personal de mantenimiento no tiene medios para diagnósticar el problema o incluso no posee el conocimiento para repararla.

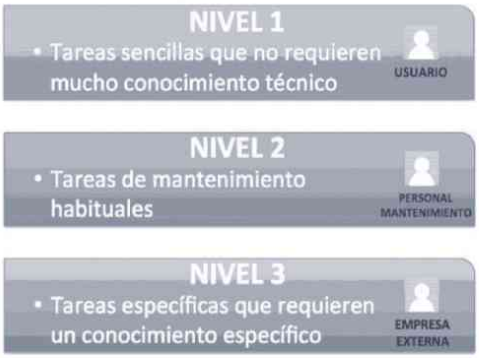


***Figura 12.1**. Niveles de mantenimiento.*

12.3.1 FACTORES QUE PUEDEN AFECTAR AL RENDIMIENTO O DURABILIDAD DE LOS COMPONENTES DE UN EQUIPO INFORMÁTICO

La temperatura

La temperatura es uno de los principales factores de avería y degradación de los dispositivos electrónicos. En realidad muchas veces son los propios dispositivos electrónicos los que se destruyen a sí mismos dado que gran parte de la energía que reciben la transforman en calor.

Los microprocesadores son los elementos que más se calientan en un equipo informático. Eso es debido a que están formados por millones de transistores. Cada transistor tiene varios estados y cuando cambia de un estado a otro necesita energía (este consumo de energía hace que se caliente el microprocesador).

En electrónica existen unas reglas y una serie de soluciones a las mismas que actualmente se están aplicando:

- **Regla 1**

  A más velocidad → Más calor.

- **Regla 2**

  A más consumo de energía (mas voltaje) → Más calor.

- **Solución a la regla 1**

  Aumentar el número de núcleos. Se reduce la velocidad pero se aumenta el rendimiento.

- **Solución a la regla 2**

  Reducir la tecnología de fabricación para así poder reducir el voltaje. Por ejemplo, pasar de 45 nanómetros a 32 nanómetros.

RECUERDA

El calor no solo destruye los chips y microprocesadores, también otros elementos como los discos duros mecánicos sufren debido al exceso de temperatura.

La solución más barata contra el calor es la disipación del calor de los microprocesadores a base de disipadores y ventiladores.

IMPORTANTE

Cuando instale ventiladores extra en la caja de un equipo informático colóquelos de tal forma que el aire recircule dentro de la caja. Elija ventiladores cuanto más grandes mejor pues seguramente sean menos ruidosos.

¿Qué pasa si se avería el ventilador?

Si el ventilador falla (porque esté averiado o porque la suciedad no permita que funcione correctamente) los componentes se pueden dañar de forma muy rápida pues en poco tiempo alcanzan grandes temperaturas. El corazón del micro está compuesto de cristal de silicio y éste puede llegar a romperse a temperaturas extremas. No obstante, por regla general, los microprocesadores dejan de funcionar cuando la temperatura del microprocesador supera un umbral determinado.

RECUERDA

El cobre es un metal mucho más conductivo (conduce mejor el calor) que el aluminio, por tanto, es mejor elegir disipadores de cobre. Si el disipador es más grande, mejor. A más superficie hay más contacto con el aire y disipa más calor.

RECUERDA

Cuando ponga pasta o silicona térmica procure no poner demasiada. La silicona es mucho menos conductiva que el cobre y, por tanto, si pone mucha el microprocesador se calentará mucho más.

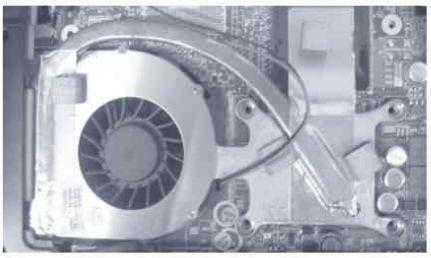


***Figura 12.2**. Sistema de refrigeración de un portátil*

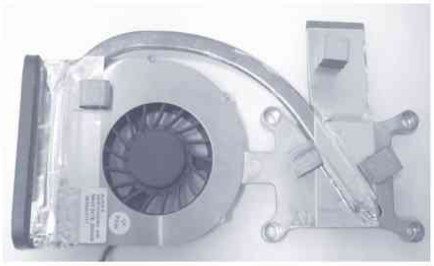


***Figura 12.3**. Sistema de refrigeración de un portátil (detalle)*

Acciones que se deberían realizar para disminuir la temperatura de los equipos:

- Colocar un ventilador trasero en la caja que evacue el aire caliente y, si es posible, uno delantero que introduzca aire a la caja (de esa manera hay corriente de aire dentro de la caja).
- Las cajas deben estar ventiladas. No meterlas en armarios o cajones que hacen que el aire no circule desde dentro hacia fuera de la caja.
- Escoger gráficas que estén bien ventiladas.
- Poner sistemas de ventilación en los discos duros (muy recomendable cuando hay más de uno).
- Normalmente, las cajas de calidad están mejor ventiladas. No elegir una caja solo por el precio, hay otros factores que también son muy importantes.
- Los filtros antipolvo suelen funcionar bastante bien, sobre todo cuando los equipos están colocados en el suelo.
- Evitar la exposición directa de los equipos a la luz solar.
- El tener un termómetro interno no reduce la temperatura pero puede indicarnos la misma y se pueden tomar acciones al respecto.

Temperaturas máximas aceptables de los componentes

Supuestamente, los componentes descritos anteriormente deberían de funcionar en temperaturas inferiores a las citadas. Es cierto que estos componentes pueden trabajar a temperaturas superiores (por ejemplo, microprocesadores trabajando regularmente a 90º), pero ello lo único que provoca es una vida del componente más corta.

La temperatura se puede medir vía software o hardware mediante sensores.

Tabla 12.1 Temperatura máxima aceptable en los componentes de un equipo informático

Componentes	Temperatura máxima ideal
Procesador	65º
Disco duro	55º
Caja	45º
Fuente de alimentación	99º

Polvo y partículas

El polvo está en todas partes suspendido en el aire y se va depositando sobre las superficies de los objetos.

El problema con respecto a los dispositivos electrónicos es que el polvo depositado hace que disminuya la refrigeración de los componentes al obstruir las ranuras de ventilación, los ventiladores…

Para evitar el polvo en los equipos se pueden utilizar rejillas antipartículas, limpiar la parte exterior de la caja con un trapo húmedo con algún producto antipolvo y periódicamente hacer una limpieza interior del equipo (cada 6 meses-1 año) desplazando el polvo con algún espray antipolvo. Estos esprays llevan aire a presión y por su composición no dañan los componentes electrónicos. Evitar rociar con otro tipo de esprays porque se pueden dañar los componentes.

RECUERDA

A la hora de pasarle un espray antipolvo hacerlo lejos de otros equipos pues el polvo que sacamos de un equipo puede ir a parar a los otros.

Humedad y corrosión

Normalmente, los equipos están diseñados para trabajar con un grado alto de humedad. La humedad hace que se produzca corrosión sobre los componentes de los equipos. No obstante, si se prevé que el equipo va a funcionar en algún sitio con una humedad muy alta (superior al 80%) bastaría con utilizar un deshumidificador.

Los líquidos son otro peligro. En caso de que caiga algún líquido sobre algún componente electrónico lo primero que hay que hacer es apagarlo. Una vez apagado se recomienda desensamblarlo lo mejor posible, secarlo bien pieza a pieza y volver a ensamblarlo. En el caso de que el líquido no sea agua hay que retirar el líquido utilizando la mínima agua posible y secarlo bien antes de ensamblarlo. Es necesario que las piezas estén bien secas antes de poner el dispositivo en funcionamiento.

Impactos y Vibraciones

***Figura 12.4**. Equipo golpeado durante el transporte*

Normalmente, el elemento que sufre más los impactos es el disco duro. No es lo mismo un impacto cuando el equipo está apagado que cuando está encendido. En este último caso resulta mucho peor.

Las vibraciones pueden estropear el disco duro y en ocasiones pueden hacer que los componentes se suelten de sus conectores o zócalos. Para evitar que las vibraciones afecten al equipo hay que fijar adecuadamente los componentes. También una buena caja reduce en gran parte las vibraciones.

Energía electrostática (descargas electrostáticas)

La energía estática se acumula en el cuerpo humano. A veces es inevitable. Puede ocurrir caminando sobre una alfombra, desempaquetando y quitando el plástico de algún producto…

Cuando una persona esta cargada estáticamente y toca algún componente entonces se descarga. Estas descargas muchas veces no son visibles al ojo humano pero son letales para los componentes electrónicos.

Consejos para evitar descargas electrostáticas son evitar trabajar sobre alfombras, moquetas o suelos plásticos como vinilos, evitar utilizar prendas de lana o materiales sintéticos, mantener los componentes en su bolsa antiestática hasta que se monten o utilizar pulseras antiestáticas a la hora del montaje.

12.3.2 MANTENIMIENTO PREVENTIVO EN EQUIPOS PORTÁTILES

A la hora de utilizar un portátil hay varias reglas que hay que seguir para prevenir posibles fallos o averías. Se podrían llamar normas de buena conducta.

- **Software**. Realizar *backups* periódicos tanto de los datos como de todo el sistema.
- **Líquidos y demás productos**. Evitar que caigan líquidos, migas, polvo… al equipo. Normalmente, caen al teclado y de éste al interior del equipo. En el caso de que caiga algún líquido hay que apagar el portátil, retirarlo y secarlo durante mucho tiempo (48 horas al menos) en un lugar seco y ventilado para que seque del todo. No volver a encender el equipo hasta que no este completamente seco.

- **Transporte**. Hay que transportar el portátil en las mejores condiciones. Utilizar para ello un maletín o mochila en la que se pueda fijar correctamente el equipo (y los accesorios). La bolsa de transporte tiene que ser dura y estar correctamente acolchada para evitar posibles daños si se golpea.
- **Funcionamiento**. Colocar el portátil en una superficie lisa y dura para trabajar. Si se coloca en una superficie blanda las entradas y salidas de aire se taponan y el portátil terminará recalentándose en exceso.
- **Modo de utilización**. Cuando no va a ser utilizado durante tiempo, el portátil hay que apagarlo. Utilizar el *standby* o hibernación solo cuando sea necesario, no hay que abusar de esta funcionalidad (se ahorra energía y se alarga la vida del portátil).
- **Batería**. Trabajar siempre con la batería. Cuando la batería tenga poca carga se pondrá a cargar el portátil (el propio equipo avisa cuando hay que cargar la batería). Si el equipo se va a utilizar durante mucho tiempo se puede desconectar la batería y enchufarlo a la corriente si se desea. No obstante, hay que tener en cuenta que siempre con el uso las baterías van perdiendo capacidad de carga.

CONSEJO

No hace falta que la batería del portátil se descargue completamente, algunas baterías de ion-litio pueden estropearse si se quedan durante mucho tiempo sin carga (igual se recomienda para PDA y móviles).

12.4 HERRAMIENTAS DE ANÁLISIS DEL SISTEMA

12.4.1 MONITORIZACIÓN DE LA PLACA BASE

Prácticamente en la mayoría de las placas base la BIOS ofrece funciones de monitorización del procesador, placa base y otros dispositivos. Normalmente se encuentra en un menú que se llama *Health Status*, *Hardware Monitoring*, o algo equivalente.

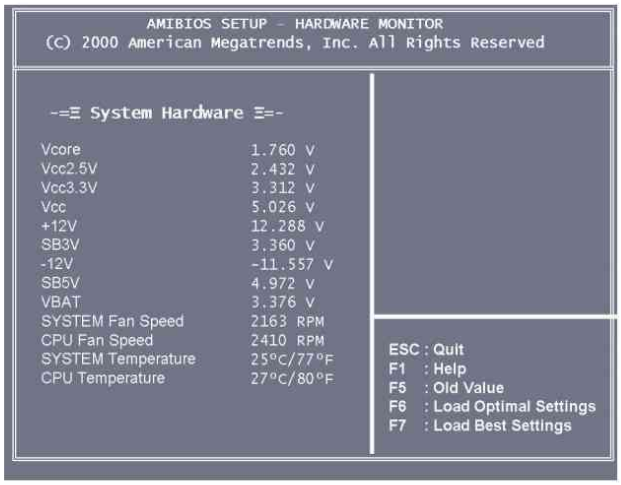


***Figura 12.5**. Monitorización del hardware a través de la BIOS*

Mediante esta herramienta se pueden monitorizar los voltajes del equipo, las revoluciones por minuto (RPM) de los ventiladores del equipo y del procesador, la temperatura de la placa base (se puede tomar como temperatura de la caja) y del micro, entre otros.

Todos estos valores pueden ser accesibles en remoto (desde otro equipo de la red) o bien mediante programas específicos.

PRÁCTICA 12.1

Monitorización de la temperatura de discos con HWInfo para Windows

- Existen muchos programas de monitorización de temperaturas en un equipo. Para este ejercicio se ha elegido un programa portable. Los programas portables tienen la ventaja de no tener que estar instalados en el equipo que se va a ejecutar. Otra ventaja es que un técnico en mantenimiento y reparación de equipos puede tener un *pendrive* con una serie de utilidades portables que puede utilizar en el desempeño de sus actividades y realizar todos los chequeos pertinentes en las máquinas con las que este trabajando sin tener que hacer ninguna instalación.

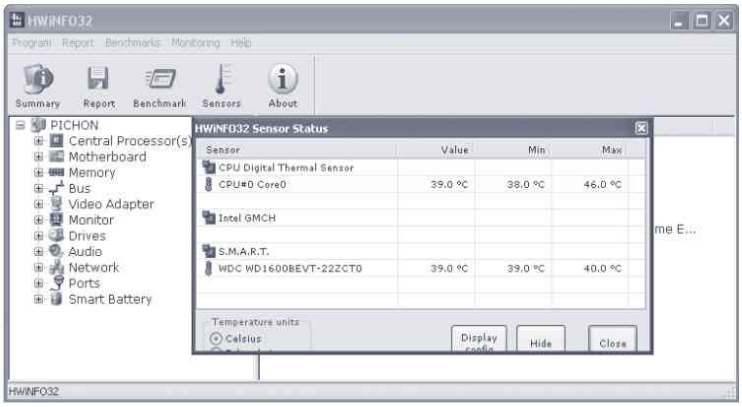


***Figura 12.6**. HWiNFO32. Valores de los sensores*

- Para obtener los valores de temperatura del equipo hay que acceder a la opción **Sensors** y en esta opción se pueden ver los valores actuales, mínimo y máximo de temperatura tanto de la CPU como de los discos.

12.5 PUESTA EN SERVICIO, ANÁLISIS, DIAGNÓSTICO Y LOCALIZACIÓN DE AVERÍAS

Entre los fallos hardware hay que distinguir entre los fallos del montaje y los fallos que puedan ocurrir una vez que el equipo ya ha funcionado correctamente. La forma de proceder frente a estas dos situaciones es completamente diferente. Obviamente, los problemas que se producen cuando se está montando un equipo son de configuración mientras que el problema que podemos encontrar en un equipo que ya ha estado funcionando suelen ser debido al software, desconfiguración o fallo en algún componente.

12.5.1 PUESTA EN SERVICIO DE LA COMPUTADORA UNA VEZ MONTADA

***Figura 12.7**. Arranque del equipo por primera vez. El sistema operativo no está instalado*

RECUERDA

La primera comprobación del equipo deberá hacerla con la caja abierta.

Si una vez montado el equipo, enchufado el monitor, ratón y teclado y se procede a encenderlo, se escucha un solo pitido y aparece un mensaje como el siguiente:

"Reboot and Select proper Boot device or Insert Boot Media in selected Boot device and press a key".

Eso puede ser un buen síntoma. Seguramente quiere decir que el sistema está correctamente instalado.

Compruebe también que todos los led están funcionando y que todos los ventiladores están funcionando correctamente. En el caso de que un led no esté funcionando correctamente puede ser bien fallo del led o que el dispositivo no esté correctamente conectado. En ese caso lo primero que habría que hacer es verificar la polaridad de la conexión del led.

12.5.2 TRAS EL MONTAJE DE UN EQUIPO TENEMOS PROBLEMAS

En esta sección se dan una serie de pistas para poder resolver los problemas que se tengan con la instalación. Las comprobaciones que se resumen aquí no van a resolver todos los tipos de problemas que existen, por supuesto, pero pueden servir de guía y ayuda.

RECUERDA

Un solo pitido corto normalmente indica que el equipo funciona correctamente.

El equipo no responde

Si el equipo no hace nada de nada compruebe:

- Los cables de los conectores de encendido del ordenador.
- Si el cable de alimentación ATX está conectado a la placa y está conectado correctamente.
- Puede que la fuente de alimentación funcione pero no llegue corriente a la placa. Mire si existe un led en la placa que evidencie que le está llegando corriente y está encendido.
- La memoria está conectada correctamente (antes de insertarla en el zócalo comprobamos que era compatible con todos nuestros componentes).
- El microprocesador está correctamente instalado (antes de instalar el micro nos aseguramos que era compatible con la placa base).

El equipo enciende pero no se ve nada en el monitor

Si parece que el ordenador enciende (da un pitido y parece arrancar) pero no se ve nada en el monitor compruebe:

- El monitor funciona en otros equipos.
- La tarjeta de vídeo está perfectamente instalada.
- El cable VGA del monitor esta correctamente conectado.
- La RAM está correctamente ensamblada.

El equipo no pita, no se escucha nada pero parece que enciende

- ¿Es posible que se haya conectado el cable del *speaker* correctamente?
- Puede ser que falle el *speaker*.

IMPORTANTE

Utilice siempre la última versión de los *drivers* para su equipo. Hay algunos errores que se solucionan instalando la última versión del *driver* del componente (en las últimas versiones tienen corregidos los errores detectados hasta la fecha). Antes de instalar el *driver* proporcionado en el CD del producto mire en la página web del fabricante por si existiese alguna versión más reciente.

El equipo emite un pitido continuo

- Puede ser que la fuente de alimentación esté averiada (compruébelo).
- La corriente no está llegando al equipo correctamente.

RECUERDA

Siempre que quite un micro y lo vuelva a colocar en su zócalo deberá retirar la pasta térmica antigua y colocar nuevamente más pasta.

Cuando el equipo pita más de una vez: mensajes de la BIOS

Cuando arranca el equipo, la BIOS examina los componentes críticos del sistema y determina si están funcionando correctamente o no. En el caso de haya algún componente o error en el sistema nos avisa con una serie de pitidos. Dependiendo de la marca de la BIOS, el mensaje es uno u otro.

CONSEJO

Cuando un ordenador falla o no arranca, la mejor solución es dejar el equipo con las mínimos componentes para que funcione (quitar las tarjetas de expansión, quitar los lectores ópticos, los discos duros, si tiene varios módulos de memoria dejar solo uno...). De esa manera podemos descartar que el error esté en alguno de esos componentes o bien al conectarlos todos juntos.

12.5.3 FALLOS COMUNES POR COMPONENTES

Fuente de alimentación

Las fuentes de alimentación pueden averiarse como cualquier otro componente electrónico. En muchas ocasiones la fuente de alimentación no hace nada (en ese caso se suele decir que la fuente está muerta). Otras veces, la fuente de alimentación tiene un comportamiento anormal, llegando en ocasiones a afectar a los componentes del equipo.

En ocasiones, si la fuente de alimentación tiene poca potencia para el funcionamiento del equipo se pueden producir apagados y reseteos.

Existen aparatos de medición de fuentes de alimentación. Se conecta el conector ATX, miden voltajes y avisan en el caso de que la fuente tenga algún error. Otra forma de medir una fuente de alimentación es mediante el polímetro (más lento pero igual de efectivo).

Fallos en la caja

La caja la verdad es que tiene pocos componentes que puedan estropearse (botones de encendido y *reset*, leds, ventiladores, conectores USB y de audio).

Cuando no funcionan los **botones** tanto de encendido como los de *reset*, lo que se puede hacer es probarlos con un polímetro. Cuando están sin pulsarse la resistencia de estos será muy alta y muy pequeña cuando están pulsados.

Los **led** tienen polaridad, esto quiere decir que funcionan solo cuando se colocan en la posición correcta (conector + y -), por tanto, si se ha manipulado el equipo y no funcionan éste puede ser el fallo.

Los **ventiladores** pueden dejar de funcionar porque falle el motor interno o porque tengan mucha suciedad. Para la suciedad hay que utilizar un espray limpiapolvo y limpiarlos en un sitio abierto. Si se limpian en la misma sala lo que puede pasar es que el polvo vuelva al equipo. Cuando la caja no está muy refrigerada el equipo se calienta en exceso. Esto puede medirse con algún termómetro (algunas cajas ya lo incorporan) y si se ve que la temperatura es alta se puede colocar un ventilador adicional o cambiar el existente por uno más potente. En ocasiones el único problema es simplemente que el aire no recircula correctamente por la caja.

Los **puertos USB frontales** que son los que más fallan se pueden probar conectando el cable a otros conectores USB de la placa para ver dónde puede estar el problema.

Microprocesador

Uno de los problemas que suele tener el microprocesador es el sobrecalentamiento. El sobrecalentamiento se puede medir con alguna utilidad desde el sistema operativo o mediante la BIOS.

Los microprocesadores tienen sistemas de protección frente a sobrecalentamientos, que hacen parar el micro antes de que tome una temperatura excesiva.

Los síntomas cuando el microprocesador está roto es que el equipo no hace nada de nada, no ejecuta ni el POST, aunque estos síntomas también pueden deberse a un fallo en la placa base o en la fuente de alimentación, entre otros.

Otros problemas que pueden afectar al microprocesador son los referentes a su refrigeración. Si el ventilador no gira o lo hace lentamente, el micro se verá afectado. Igualmente, si el disipador no está correctamente pegado al micro también puede haber problemas.

Placa base

El problema que existe con las placas base es que cada vez ejecutan más funciones y tienen integrados más chips (red, sonido, vídeo, controladoras de discos…). Esto provoca que fallen mucho más.

En ocasiones un fallo que parece de otro componente en realidad es un fallo de la placa base (por ejemplo, un disco, su fallo puede deberse a la controladora de discos). También algún mal funcionamiento de la BIOS puede hacernos pensar que la placa está averiada (los valores, por defecto, y las actualizaciones de la BIOS nos ayudarán en este punto).

RECUERDA

Un tornillo suelto en contacto con la placa base puede ocasionar problemas.

Memoria

El POST puede detectar errores en la memoria. Cuando el POST encuentra algún error avisará con una serie de pitidos. No obstante, puede haber problemas que deben de ser chequeados con algún programa específico el cual comprobará todas las celdas de la memoria de una manera más exhaustiva.

Tarjetas de expansión

Algunos de los problemas que pueden tener las tarjetas de expansión pueden ser debidos al *driver*, por tanto, antes de dar por estropeada una tarjeta de expansión hay que actualizar el driver a la última versión. Normalmente, la detección de los problemas en las tarjetas de expansión no es complicada pues deja de funcionar el dispositivo en cuestión (tarjeta de red, tarjeta gráfica, tarjeta wireless, tarjeta expansora de puertos, tarjeta sintonizadora de TV…).

RECUERDA

Una tarjeta de red con un funcionamiento incorrecto en una red de área local puede hacer que la red no funcione correctamente.

Discos duros

Los discos duros cuentan con una utilidad de nombre SMART, que permiten predecir si un disco va a fallar o si ya está dando síntomas de un mal funcionamiento. Para utilizar SMART en un disco duro hay que habilitarlo en la BIOS y utilizar un programa que reciba e interprete esos valores que dará el disco duro (tipo Smartmontools para Linux, HDTune para Windows® o similar). También se pueden usar utilidades que escaneen la superficie del disco en busca de errores. Generalmente, este tipo de utilidades escriben y leen la superficie del disco como método de análisis.

CONSEJO

Un ruido anormal en el disco duro generalmente es síntoma de que el disco va a fallar en un futuro.

La temperatura excesiva en discos evidencia que el disco puede tener problemas en un futuro (mas de 50º empieza a ser un mal síntoma). Para medir la temperatura del disco se pueden utilizar utilidades SMART.

Los cables de conexión y la configuración maestro/esclavo en los discos PATA también son elementos que hay que tener en cuenta a la hora de evaluar si un disco funciona o no.

Unidades ópticas

Las unidades ópticas también pueden dar problemas, sobre todo las unidades ópticas de los portátiles. La mejor comprobación es la sustitución por otra unidad óptica. En el caso de los equipos de sobremesa una sustitución de un dispositivo óptico es sencilla y más complicado es cambiarla en un portátil.

Cables de datos

Es raro que un cable se estropee salvo que se desconecte tirando de él. Los cables PATA sí suelen dar problemas pero los demás no, salvo que el conector esté dañado.

PRÁCTICA 12.2

Realización de un *benchmark* a un equipo con *HWINFO32*

Una buena práctica tras montar un equipo informático o hacer una reparación del mismo puede ser pasarle un *benchmark* o una serie de *benchmark* para cerciorarse de que todo funciona correctamente. El *benchmark* que se le va a pasar al equipo en este caso práctico es muy sencillito y rápido pero podemos optar por hacerle pruebas más exhaustivas.

En los casos en que los errores son aleatorios o que ocurren cuando el usuario ya lleva trabajando con el equipo y que tras haber descartado que el software sea el causante del mismo o la temperatura, lo mejor es pasarle una serie de pruebas exhaustivas por si la memoria tuviese celdas estropeadas, la placa base tuviese algún componente averiado o el micro no estuviese funcionando como debiera. Podemos optar por realizar un test de tortura u otro tipo de *benchmark* o pruebas más especificas. En estos casos siempre es mejor realizar una configuración mínima con los componentes imprescindibles y testearlos a fondo para luego ir añadiendo componentes y seguir testeando.

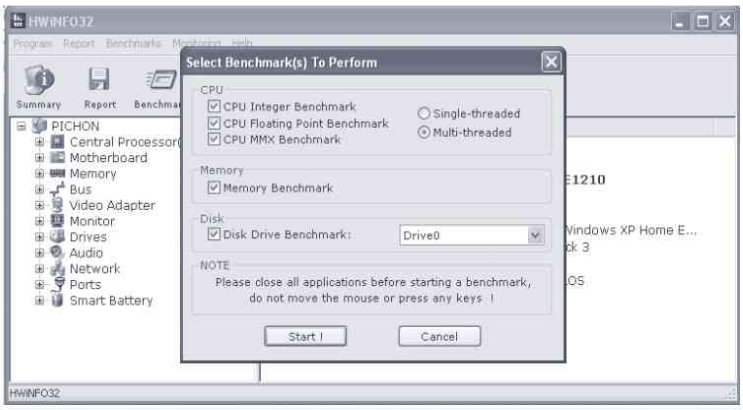


***Figura 12.8**. Benchmark con HWiNFO32*

- Para realizar el *benchmark* al equipo elegimos la opción **Benchmark** del menú principal y pulsamos **Start** con todas las opciones activadas.

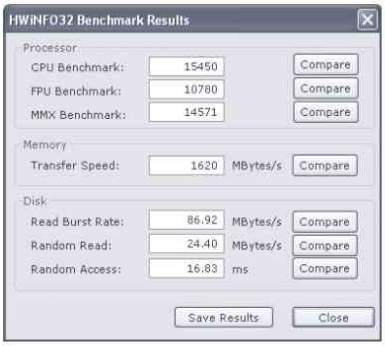


***Figura 12.9**. Resultado del benchmark de HWiNFO32*

- Este *benchmark* es rápido y realiza las operaciones necesarias para recopilar los valores que luego presentará, pero al menos ha hecho una mínima comprobación de la memoria, el procesador y el disco duro que son los componentes básicos del equipo.

12.6 REPARACIONES DE EQUIPOS INFORMÁTICOS

Las reparaciones de equipos informáticos de telecomunicaciones suelen consistir en la mayoría de las ocasiones en una sustitución del componente que está fallando. Una vez reparado el equipo se debería hacer una revisión en profundidad verificando primeramente que el componente reparado funciona ahora correctamente y, posteriormente, que los demás componentes del equipo funcionan como debieran. Como se ha dicho anteriormente, la experiencia hace que la detección, reparación y puesta en funcionamiento de los equipos sea mucho más ágil. En este apartado del capítulo nos vamos a centrar algo más en los equipos portátiles dada su proliferación actualmente.

12.6.1 REPARACIONES EN EQUIPOS PORTÁTILES

Las averías en los portátiles, por regla general, suelen ser más caras que las averías en un PC de sobremesa. En muchas ocasiones hay que recurrir al servicio técnico especializado y eso significa un desembolso mayor que la mayoría de tiendas de confianza.

Los portátiles tienen una desventaja y es que en el mismo aparato está el monitor, teclado, pila, placa base, memoria, disco duro, tarjeta de red… Es decir, que las posibilidades de que el equipo falle son mucho mayores al tener los componentes agrupados.

IMPORTANTE

Antes de abrir o manipular cualquier portátil hay que desconectar el cable de alimentación y la batería (no olvidar nunca la batería).

Fallos en la alimentación

- **La batería se agota en seguida**. Las baterías no duran eternamente, como las baterías de los móviles tienen una vida determinada y al llegar un cierto tiempo dejan de funcionar correctamente. Dependiendo del trato y del uso que se le dé pueden llegar a durar más o menos. El reemplazo de la batería se puede hacer por una de la misma marca o bien alguna compatible con un coste inferior. La duración de la garantía de las baterías suele ser de poco tiempo (3 meses la mayoría de las marcas).

RECUERDA

Para alargar la vida de la batería del portátil es mejor dejarla agotarse por completo antes de conectar el transformador a la corriente para que se cargue.

- **El transformador no funciona**. En ese caso por experiencia lo más rentable es comprar un transformador universal. Normalmente, los transformadores tienen una luz testigo que indican si está funcionando el transformador o no.

RECUERDA

A la hora de utilizar un cargador de portátil universal configure correctamente los voltios y los amperios de salida. Tienen que ser los mismos que los de su transformador original.

CONSEJO

Para proteger el sistema eléctrico del portátil trabaja siempre con la batería puesta. De esta forma evitará picos, sobretensiones...

- **Falla la conexión con el transformador**. En ocasiones lo que falla es la conexión con el transformador en el propio portátil. En ese caso hay que reparar esa conexión.

  ¿Cómo sabemos que puede ser el conector?

  - El portátil funciona con la batería pero ésta no carga.
  - El transformador da corriente (lo podemos comprobar con el polímetro).

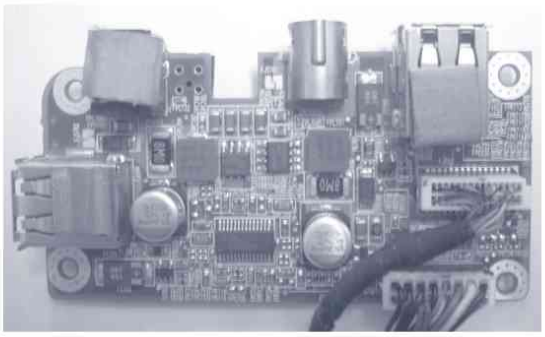


***Figura 12.10**. Placa con conector hembra de corriente y demás conexiones de alimentación así como puertos USB*

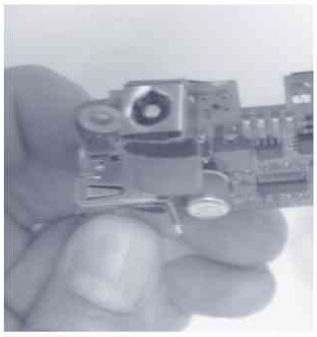


***Figura 12.11**. Detalle del conector hembra de corriente*

En la figura anterior podemos ver una placa interna de un portátil (vista desde arriba) que es la que tiene el conector hembra de corriente, también se pueden observar los puertos USB y los conectores de corriente que alimentarán a los demás componentes del equipo. En la figura de la derecha se puede apreciar mejor el conector hembra de corriente.

La conexión puede fallar porque un punto de soldadura del conector se haya soltado (solución: se aplicará ese punto de soldadura). Si el problema es el macho o la hembra de los conectores habrá que cambiar el que está averiado (si encontramos uno igual) o bien cambiar ambos. Estos conectores son baratos y no es muy difícil encontrarlos. Es muy frecuente que debido al uso estos conectores se estropeen.

CONSEJO

En ocasiones el transformador falla porque el cable está machacado o retorcido. Cuando sospeche que puede ser el transformador haga una revisión de todo el cableado del transformador, ahí podría estar el problema.

Fallos en el teclado

El teclado de los portátiles es más frágil que un teclado normal. Además, tiene la característica de que debajo están los componentes más sensibles del equipo (placa base, memoria, tarjetas….). Como se ha dicho en el mantenimiento preventivo de los equipos portátiles hay que evitar que le caigan líquidos, migas u otro producto al teclado para alargar la vida del mismo y del propio equipo.

Si se avería el teclado puede sustituirse por otro compatible o bien utilizar un teclado externo, lo cual no suele ser muy práctico.

PRÁCTICA 12.3

Sustitución del teclado en un portátil

- El principal escollo a la hora de la sustitución del teclado en un portátil es el acceso al mismo. Además de los problemas que pueda tener el teclado por caída de líquidos o suciedad, las teclas de un teclado son muy sensibles y si en algún momento se liberan o se estropean podemos encontrarnos con problemas. En algunos casos puede ser necesario hasta cambiar el teclado.
- Otra razón por la cual cambiar el teclado es por la compra de un equipo en otro país y la necesidad de su utilización en España. La distribución del teclado no es la misma. En el sistema operativo es fácil cambiar la distribución del teclado a español pero las teclas seguirán siendo diferentes. La solución en este caso es el cambio del teclado. Se sustituirá por uno idéntico o alguno compatible con el anterior.

a. El primer paso es el acceso al teclado. Dependiendo del modelo será fácil o muy difícil teniendo en ocasiones que desmontar gran parte del portátil.

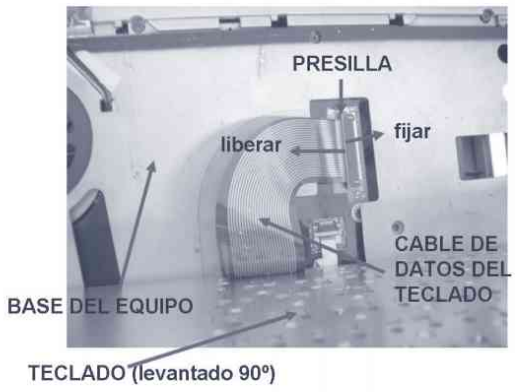


***Figura 12.12**. Conexión del teclado de un portátil*

b. Una vez accedido al mismo se procede a liberar el viejo teclado y sustituirlo por el nuevo. El sistema de fijación que se muestra en la figura anterior es de tipo presa pero puede cambiar dependiendo del modelo. La faja o cable de datos está sujeto al equipo mediante una presilla o pestaña. Sacando la pestaña hacia fuera se liberará el cable de datos y ajustándola se fijará el cable de datos.

c. El último paso consistirá en volver a montar el equipo y comprobar el funcionamiento del nuevo teclado.

CONSEJO

Cuando compremos un nuevo teclado para un portátil, deberemos asegurarnos que este es compatible 100% con el equipo.

Los *touchpad* también se averían pero suele ser menos frecuente, normalmente son muy robustos (siempre tendremos la solución del ratón, para portátiles los hay de todo tipo y de todos los tamaños).

Memoria

Los problemas con la memoria son exactamente los mismos que para un equipo de sobremesa. El acceso a la memoria suele ser bastante fácil salvo en los equipos ultraportátiles o demasiado compactos, en los que hay que desmontar bastante el equipo para acceder a ella.

Unidades ópticas

Las unidades ópticas suelen ser más delicadas que una unidad óptica normal de 5 ¼, dado que son más delgadas y se llevan muchos más golpes. Muchas veces los errores son fallos de lectura o simplemente que no lee el disco. En ese caso la solución es sustituir el lector dañado por otro compatible con nuestro equipo.

PRÁCTICA 12.4

Reemplazo de una unidad óptica estropeada

Tenemos un equipo con una tarjeta lector óptico estropeado. Ya se han realizado las operaciones pertinentes descartando otros posibles fallos y se ha llegado a la conclusión de que con toda probabilidad el lector está averiado.

Los pasos a seguir son los siguientes:

Paso 1. Retirar los tornillos de sujeción del lector al equipo.

***Figura 12.13**. Retirando los tornillos de fijación*

Paso 2. Extraer el lector y reemplazarlo por el nuevo lector.

***Figura 12.14**. Sustitución del lector*

Paso 3. Volver a fijar el lector al equipo y comprobar su funcionamiento.

Disco duro

Los discos duros salvo unidades SSD suelen dar más problemas que un disco duro de un ordenador de sobremesa debido a que el ordenador se mueve, sufre golpes, está menos ventilado…

CONSEJO

Si escucha un pequeño ruido anormal cuando el disco está funcionando puede ser síntoma de que el disco duro no está bien.

Aquí podemos utilizar las mismas técnicas que con un disco duro convencional. La sustitución de un disco duro es bastante sencilla y frecuente en la mayoría de los portátiles. Además, en el mercado hay cientos de utilidades que chequean discos duros y podemos examinarlos para ver si tienen sectores dañados. Es muy frecuente que un disco comience por algunos sectores dañados y termine por estropearse del todo.

CONSEJO

No mueva el equipo cuando está funcionando o durante el apagado. Es muy común apagar el portátil y mientras éste está realizando la función de apagado lo cogemos y lo guardamos. Esto acorta la vida del disco duro del equipo.

Placa base

Un fallo en placa base equivale muchas veces a decir adiós al portátil si éste no está en garantía. Si el equipo ni enciende o no arranca y descartamos que sea un problema de alimentación, entonces hay muchas probabilidades de que la placa base este estropeada. Antes de señalar como culpable a la placa base hay que cerciorarse que el disco duro funciona correctamente conectándolo a un dispositivo USB. A la conclusión de que la avería está en la placa base se llega normalmente cuando se descarta que los demás componentes funcionan correctamente (alimentación, HD, memoria, micro…).

La placa base de un portátil se puede cambiar pero la pieza puede salir algo cara. En muchas ocasiones puede ser más barato sustituir el equipo por otro dado que los equipos bajan de precio y aumentan sus prestaciones y ya no resulta rentable reparar el antiguo.

Fallos en la pantalla

La pantalla en un portátil es un elemento muy sensible. Las pantallas de los portátiles son más delicadas que un monitor LCD normal, el sistema de retroalimentación es más delicado y además la pantalla hace de tapa del portátil con lo cual se suele llevar muchos más golpes que un monitor de sobremesa. Además las pantallas de un portátil suelen dar más problemas que una pantalla LCD normal.

Figura 12.15. *Posibles fallos de una pantalla cuando no se ve nada en ella*

Cuando esta rota la pantalla puede ser debido a tres causas. La primera es que este rota la misma pantalla (el TFT), también puede tener estropeado el inversor o inverter (es una placa que suele estar en la parte posterior de la pantalla y se encarga de suministrar corriente eléctrica al sistema de emisión de luz de la pantalla). El inversor es menos costoso que una pantalla y generalmente suele averiarse con más frecuencia que la pantalla.

***Figura 12.16**. Inverter de una pantalla LCD*

CONSEJO

Si la pantalla se ve oscura o simplemente no se ve y cuando conectamos un monitor externo éste se ve perfectamente, el problema estará seguramente en el *inverter* o inversor. En otras ocasiones, por culpa del inversor, la pantalla parpadea y por momentos se deja de ver.

La tercera opción es que la tarjeta gráfica esté estropeada. Normalmente, si conectamos un monitor externo y no se ve nada o se sigue viendo la imagen distorsionada es muy probable que la tarjeta gráfica este dañada. Muchas veces la tarjeta gráfica está integrada en la placa base y la reparación de la misma pasa por cambiar la placa base completa, lo cual es costoso y en muchas ocasiones no es rentable.

CONSEJO

En el caso de que la pantalla esté rota, generalmente la reparación consiste en comprar otra pantalla totalmente nueva. Es el propio fabricante el que suministra la pantalla (también se puede buscar alguna pantalla compatible de coste inferior) y el precio dependerá del modelo. Generalmente, este tipo de reparación no es rentable.

También la pantalla tiene bisagras, cables de conexión entre pantalla y placa y estos se pueden estropear pero es menos frecuente. Normalmente, cuando la pantalla se ve mal pero al moverla o girarla se ve bien, esto suele ser debido a que la conexión entre la placa y pantalla está fallando. Esta avería no suele repararse porque la solución más drástica pasa por cambiar la pantalla y suele resultar muy caro.

PRÁCTICA 12.5

Reemplazo de una tarjeta WIFI defectuosa

Tenemos un equipo con una tarjeta Wi-Fi estropeada. Ya se han realizado las operaciones pertinentes descartando otros posibles fallos y se ha llegado a la conclusión de que la tarjeta Wi-Fi ha dejado de funcionar porque está averiada.

Los pasos a seguir son los siguientes:

Paso 1. Retirar la portezuela de acceso a la tarjeta Wi-Fi.

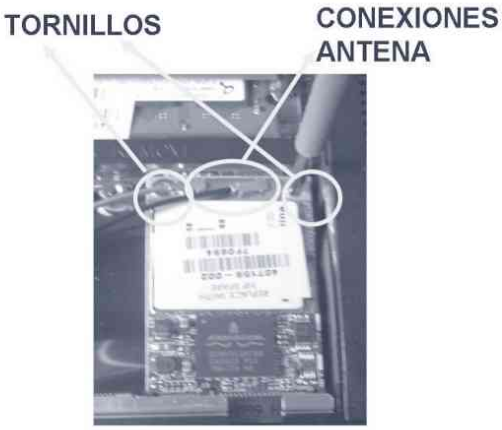


***Figura 12.17**. Tarjeta WIFI de un equipo portátil*

Paso 2. Extraer la tarjeta Wi-Fi defectuosa y reemplazar por una tarjeta idéntica. La tarjeta generalmente viene atornillada y sujeta a la antena mediante dos conexiones. La antena recorre partes del ordenador para recoger mejor la señal. Habrá que retirar las conexiones que van fijas por presión y los tornillos de fijación.

***Figura 12.18**. Detalle tarjeta Wi-Fi*

Paso 3. Volver a instalar la nueva tarjeta tal y como venía instalada la anterior y comprobar su funcionamiento.

12.7 CLONACIONES

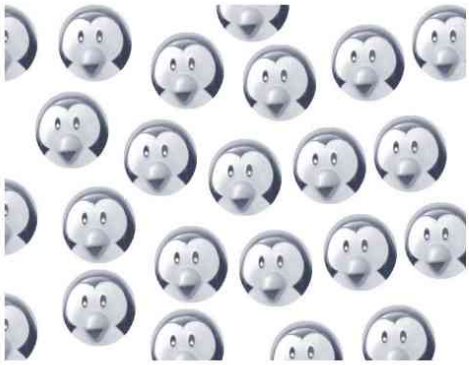


***Figura 12.19**. Las clonaciones. Fuente Saquayo*

Para la clonación de discos se va a utilizar un *live* CD con una distribución Linux llamada **Parted Magic**.

IMPORTANTE

¿Cómo conseguir Parted Magic?

- Primero hay que descargar la ISO del CDRom desde *www.partedmagic.com* o utilizar la versión del Material de recursos (ésta puede no ser la última versión).
- Una vez descargada habrá que descomprimirla si está comprimida.
- El último paso es grabar la imagen ISO a un CD (un CD basta, pues son menos de 100 MB).

Su CD grabado estará disponible para arrancar desde él en un equipo.

***Figura 12.20**. Parted magic*

IMPORTANTE

Ejecutar Parted Magic

Para ejecutar Parted Magic asegúrese que su equipo arranca desde la unidad óptica antes que desde el disco duro (quizás tenga que cambiar la secuencia de arranque en la BIOS).
Una vez verificado este punto, introduzca el CD en el lector y encienda el equipo.
La mejor opción de arranque de Parted Magic es la opción por defecto en la que se carga el sistema en RAM.

***Figura 12.21**. Mount gtk*

Con Parted Magic tenemos múltiples herramientas como:

- **G4L**. *Ghost for linux*. Herramienta de clonación de discos. Es un clon de Norton Ghost® para Windows®.
- **Gparted**: herramienta para realizar particionamiento (crear, borrar y cambiar el tamaño de particiones).
- **Partition Image**: herramienta para clonar particiones.
- **Make Parted Magic USB**: herramienta para hacer que funcione Parted Magic desde un dispositivo USB.
- **Hardinfo**: el Everest de Linux. Proporciona todo tipo de información sobre el sistema.
- **GSmartControl**: proporciona información SMART sobre nuestros discos.
- **XArchiver**: herramienta para realizar copias de seguridad.
- **Mount-gtk**: monta y desmonta dispositivos en el sistema.
- Etc.

Todas estas herramientas se pueden encontrar en System Tools del menú principal.

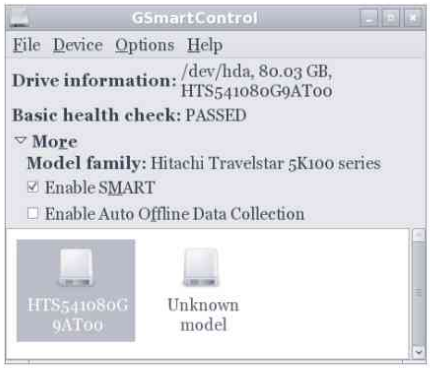


***Figura 12.22**. GSmartControl*

12.7.1 CLONACIÓN DE PARTICIONES Y DE DISCOS

IMPORTANTE

¿Qué es una clonación?

Una clonación es una copia exacta de algo. En nuestro caso será una copia exacta de un disco o una partición.

Cuando se tiene un disco que no contiene ningún sistema operativo desde el cual arrancar, basta con clonar las particiones y recuperarlas en otro disco y el disco contendrá los mismos datos.

¿SABÍAS QUE...?

Aparte de parted magic, existen otras alternativas con muy buenas prestaciones como pueden ser Norton Ghost o Acronis Truimage.

Si lo que se quiere hacer es un clon de un disco con el cual arranque el equipo se deberá clonar todo el disco. De esa manera se clonará el sector de arranque y se estará seguro de que si se sustituyen los discos el sistema funcionará perfectamente.

IMPORTANTE

Clonación de equipos

Para clonar un equipo deberá hacer una réplica del disco/s y tendrá que asegurarse de que el hardware es el mismo.

Las clonaciones funcionan creando un archivo de imagen (al igual que una imagen ISO de un CD/DVD) que es una réplica del disco o la partición.

Cuando se quiera volver el disco o partición a su estado anterior bastaría con restaurar el disco con la imagen creada.

12.7.2 CLONACIÓN DE PARTICIONES

Para la clonación de particiones se va a utilizar Partition Image. Con este programa es muy sencillo crear y recuperar una partición.

Es posible realizar (y por cierto bastante útil) la opción de crear imágenes y almacenarlas en un equipo externo conectado al nuestro mediante la red. De esta manera no hace falta almacenar la imagen en otro dispositivo como un disco USB.

EJERCICIO 12.1

CREACIÓN/RECUPERACIÓN DE UNA PARTICIÓN CON PARTITION IMAGE

Creación de la imagen

El primer paso a dar es la elección de la partición a clonar.

***Figura 12.23**. Partition Image. Partición a clonar*

Se selecciona la acción a realizar que en este caso será salvar la partición en un fichero imagen y se tecleará (incluida la ruta) el nombre del fichero a crear.

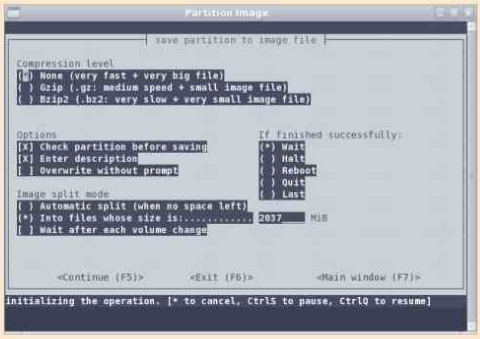


***Figura 12.24**. Partition Image. Ruta del fichero destino*

El siguiente paso es seleccionar las opciones del proceso (compresión o no, partir la imagen en ficheros de 2 GB por si se almacenan en discos con sistemas de archivos FAT…).

En nuestro caso no se ha comprimido el fichero dado que existe espacio en el disco duro externo que se va a emplear para alojar la imagen y se pretende que el proceso vaya más rápido al no tener que comprimirse los archivos. También se ha fraccionado la imagen en ficheros de 2.037 MB porque el disco externo USB que se va a emplear está formateado como FAT y no permite ficheros más grandes de 2 GB.

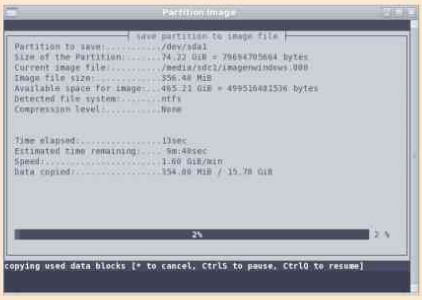


***Figura 12.25**. Partition Image. Proceso de clonación*

En todo momento se puede ver el progreso del proceso y el tiempo estimado que falta por completarse.

***Figura 12.26**. Partition Image. Finalización del proceso de clonación*

Cuando se llegue al paso de la imagen anterior el proceso estará completado. Ya solo quedaría recuperar la partición.

Restauración de la imagen

El proceso de recuperación de la imagen es análogo al anterior. Es el paso opuesto.

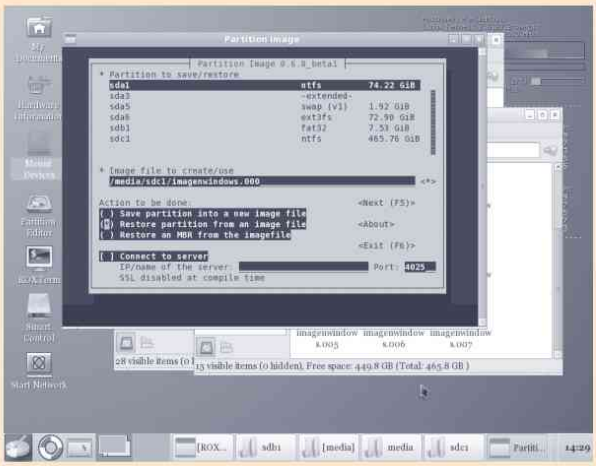


***Figura 12.27**. Partition Image. Restauración de la imagen*

En este caso se elige la opción de restaurar la partición desde un fichero de imagen.

***Figura 12.28**. Partition Image. Opciones de la restauración*

En este caso se dejan las opciones por defecto y ejecutaremos el proceso.

***Figura 12.29**. Partition Image. Finalización del proceso de restauración*

El proceso finalizará mostrando un resumen de los datos copiados, velocidad y tiempo empleado.

Ya solamente queda probar el sistema para corroborar que el proceso se ha realizado correctamente.

12.7.3 CLONACIÓN DE DISCOS

Para la clonación de un disco se va a utilizar la herramienta **G4L** (*Ghost for Linux*). Como su nombre dice es un clon del Norton Ghost pero gratuito.

Con él se pueden hacer copias de seguridad o clones de los discos y particiones en modo local y remoto.

EJERCICIO 12.2

CREACIÓN O CLONACIÓN/RECUPERACIÓN DE UN DISCO CON G4L

La primera ventana que nos encontramos al ejecutar G4L es la siguiente:

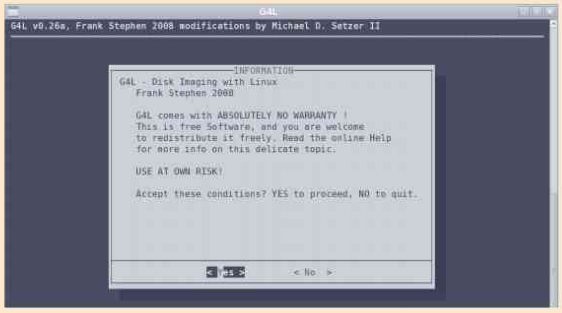


***Figura 12.30**. G4L. Ghost for Linux*

No hay que tener pánico. Obviamente, como es un software gratuito, es lógico que el creador no se quiera hacer responsable de cualquier problema que pueda ocurrir puesto que no se está pagando por su utilización.

CREACIÓN DE LA IMAGEN

***Figura 12.31**. G4L. Creación de la imagen*

Para la réplica de un disco se utilizará el modo RAW para copiar toda la información (todos los bits del disco).

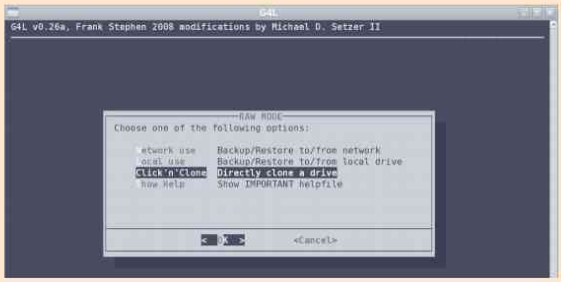


***Figura 12.32**. G4L. Opción click and clone*

Dado que se va a hacer un clon del disco en un disco USB externo se elegirá la opción **Click'n'Clone**. Se podría crear una imagen del disco solamente y en ese caso se podría elegir alguna de las dos primeras opciones.

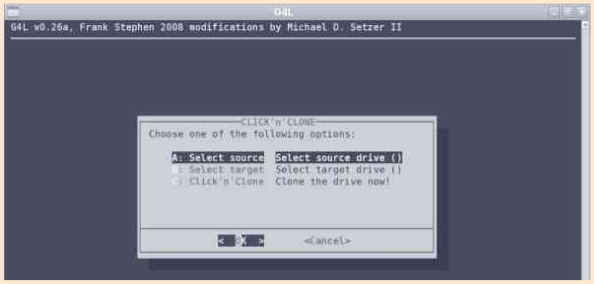


***Figura 12.33**. G4L. Selección del disco a clonar*

Se selecciona la primera opción (A) para elegir el disco origen. En nuestro caso se elegirá el disco *hda* que es el disco IDE del sistema (*hda1*, *hda2* y *hda3* son las particiones del disco *hda*).

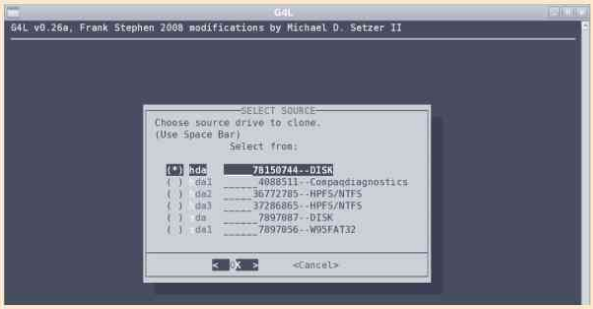


***Figura 12.34**. G4L. Selección del disco destino*

Una vez elegido el disco a clonar se debe elegir el disco destino (opción B). El disco destino deberá tener como mínimo la misma capacidad del disco origen.

Para ejecutar el proceso se elige la opción C.

El resultado de este proceso es una réplica del disco que se quería clonar.

Se aconseja para la clonación discos de la misma capacidad.

RECUPERACIÓN DE UN DISCO/RESTAURACIÓN DE LA IMAGEN

El proceso de restauración del disco es análogo al anterior.

En este caso se seleccionan los discos origen y destino y se haría la copia.

Ya solamente queda probar el sistema para corroborar que el proceso se ha realizado correctamente tras la restauración.

12.8 COPIAS DE SEGURIDAD

El respaldo de sistemas se basa fundamentalmente en las copias de seguridad o *backup*. No obstante, existen algunas otras alternativas como pueden ser la clonación o los puntos de restauración de Windows®.

12.8.1 QUE ES UNA COPIA DE SEGURIDAD O BACKUP

Una copia de seguridad es hacer una duplicación de todo o parte del sistema.

En caso de un fallo en el sistema (borrado accidental, rotura de un disco, fallo del sistema operativo o alguna aplicación, etc.) se procederá a ejecutar el proceso de restauración del mismo. Este proceso permite dejar el sistema en el estado del mismo momento en el que se hizo el *backup*.

Las copias de seguridad no deberían de estar muy espaciadas en el tiempo. Cuanto más tiempo exista entre copia y copia mayor será el volumen de información que se pueda perder.

RECUERDA

Cuando hay un fallo en el sistema se pierde la información existente entre el último *backup* y el momento del fallo. Esa información es posible que no se pueda recuperar.

12.8.2 TIPOS DE COPIAS DE SEGURIDAD

Básicamente existen 3 tipos de copias de seguridad o *backup*:

- **Total o completa**: es aquella que copia toda la información almacenada en el sistema. Desactiva el atributo de modificado a todos los archivos.
- **Incremental**: copia solo los archivos que tienen el atributo de modificado activado. Una vez realizada la copia de seguridad ese atributo se desactiva.
- **Diferencial**: es igual que la incremental, lo único que el atributo modificado no se desactiva (este atributo se desactivará cuando se haga una copia de seguridad incremental o completa).

Cuando se trabaja con archivos y estos sufren alguna modificación el atributo de modificado se activa.

En la figura siguiente se puede ver cómo funcionan los *backup* totales, incrementales y diferenciales. El aspa indica que el fichero ha cambiado de contenido y la estrella marca los ficheros que se han incluido en el *backup*.

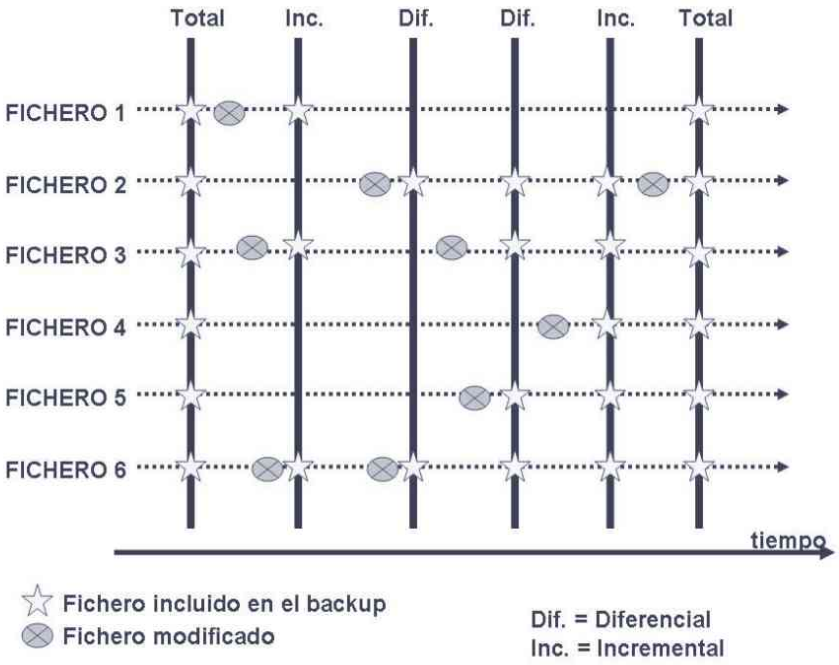


***Figura 12.35**. Diagrama de backups*

RECUERDA

El *backup* diferencial nunca desactiva el atributo modificado.

El proceso de restauración

El proceso de restauración (*restore*) consistirá en:

1. Restablecer la última copia de seguridad total.
2. Posteriormente, se restauran desde la más antigua hasta la más moderna aquellas copias de seguridad incrementales desde la última exportación total.
3. Por último, se restablece la última copia de seguridad diferencial realizada siempre y cuando sea ésta la última copia realizada (no existe ninguna copia incremental ni total posterior).

12.8.3 LOS 10 CONSEJOS DE LAS COPIAS DE SEGURIDAD

1. Realizar copias de seguridad de cuanto se pueda, como mínimo de los ficheros de datos.
2. Los *backups* deben ser **comprobados** para saber si funcionan. Deberán también estar correctamente etiquetados (fecha, equipo, tipo de *backup*, contenido…) y ordenados.
3. Mantener los *backups* en **sitios diferentes** a los que se encuentran los datos.
4. Realizar *backups* incrementales o diferenciales si no es posible realizar siempre *backup* total.
5. **No demorar** en el tiempo los *backups*.
6. **Automatizar** los *backups*.
7. **No fiarse** de hacer copia de seguridad sólo en otro PC.
8. **Comprobar** que el soporte en el que se hacen las copias de seguridad está en uso y no está obsoleto y proteger las copias de seguridad de su posible deterioro.
9. Hacer un **simulacro** de pérdida de información.
10. Las copias de seguridad tienen que estar **protegidas**.

RECUERDA

Los CD o DVD hay que manejarlos por los bordes y conservarlos en un lugar fresco y seco.

RECUERDA

Es prácticamente imposible garantizar la seguridad de un sistema al 100%. De todas formas, si no se sigue una adecuada política de copias de seguridad la probabilidad de que algo ocurra al sistema se incrementa exponencialmente.

12.8.4 UTILIDADES PARA HACER COPIAS DE SEGURIDAD EN LINUX

Linux tar

El comando tar (*Tape ARchiver*) se utilizó para crear copias de seguridad en cinta, de ahí su nombre. Ahora sigue siendo útil a pesar de que se utilizan las cintas cada vez menos. El comando *tar* tiene múltiples parámetros. Actualmente, este comando es útil en la instalación de programas. En este apartado se van a ver ejemplos sencillos de cómo funciona este comando.

CONSEJO

Ejecute el comando *man tar* en un terminal y observe la sintaxis del comando.

Ejemplo de utilización

Empaquetar un directorio:

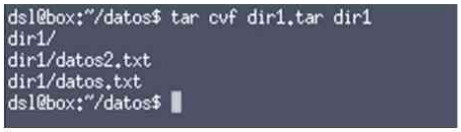


***Figura 12.36**. tar. Empaquetar un directorio*

```
$ tar cvf dir1.tar dir1
```

Este comando creará un fichero *dir1.tar* que contendrá el directorio *dir1* (con todos sus ficheros y subdirectorios si existen).

Linux Sbackup

Sbackup es un programa con el cual poder realizar de una forma sencilla copias de seguridad en forma local o incluso de forma remota.

El funcionamiento es sencillo y aunque se diseñó esta aplicación para trabajar con Ubuntu, funciona para cualquier distribución derivada de Debian.

EJERCICIO 12.3

MANEJO DE SBACKUP EN UBUNTU LINUX

Para la instalación de esta herramienta en Ubuntu, basta con ejecutar el siguiente comando:

```
$ sudo apt-get install sbackup
```

Una vez ejecutado este comando nos aparecerá en **Sistema** → **Administración** el acceso a la configuración de las copias de respaldo y la restauración de las copias de respaldo.

El aspecto del programa se muestra en la siguiente figura:

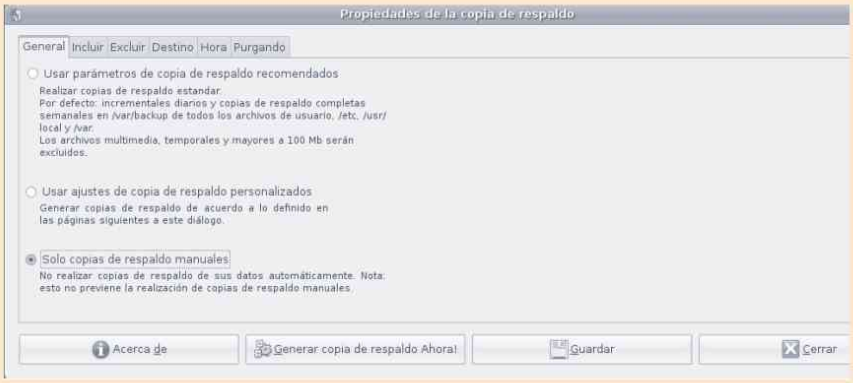


***Figura 12.37**. SBackup*

Se elegirá utilizar copias de respaldo recomendadas, personalizadas o manuales y en la siguiente pestaña se incluirán los ficheros de los que se quiere hacer copias de respaldo o respetar los ficheros que propone el sistema:

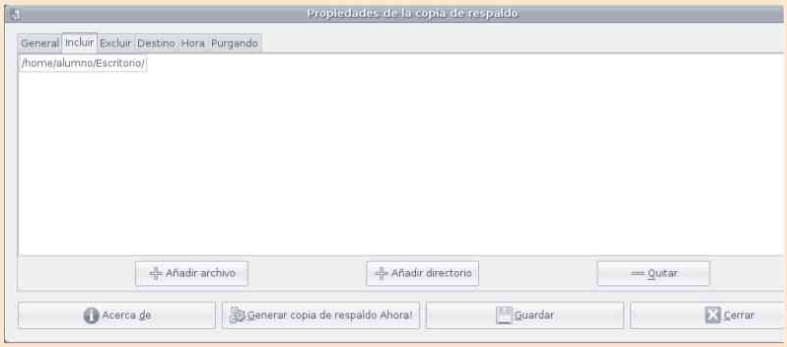


***Figura 12.38**. SBackup. Incluir ficheros y directorios*

Una vez se pulsa **Generar copia de respaldo ahora** se comienza a ejecutar el *backup* automáticamente.

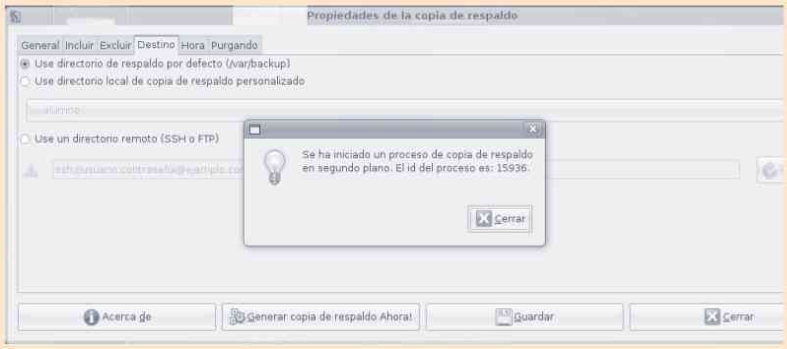


***Figura 12.39**. SBackup. Ejecución de un backup*

El directorio destino es configurable. El directorio que utiliza el programa por defecto es */var/backup*.

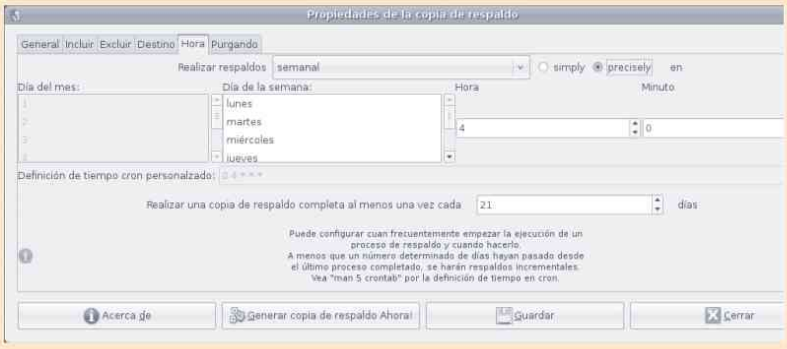


***Figura 12.40**. SBackup. Programación de un backup*

También es posible programar las copias de seguridad. Esta herramienta lo que hace es automatizar la copia mediante la herramienta cron del sistema pero de una manera más fácil e intuitiva para el usuario.

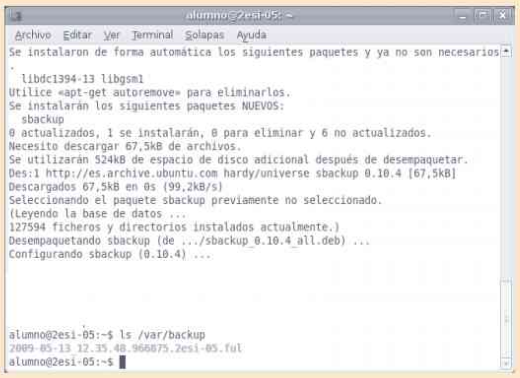


***Figura 12.41**. SBackup. Confirmación del backup realizado*

Siempre que se hace una copia de seguridad hay que verificar dos cosas:

1. La copia de seguridad se ha generado. En nuestro caso se verifica que la copia se ha generado correctamente en el directorio */var/backup* con un simple *ls*.
2. Probar que la copia de seguridad contiene los ficheros que se quería salvaguardar. Para ello, una opción es recuperar los datos en otro dispositivo o en otro directorio.

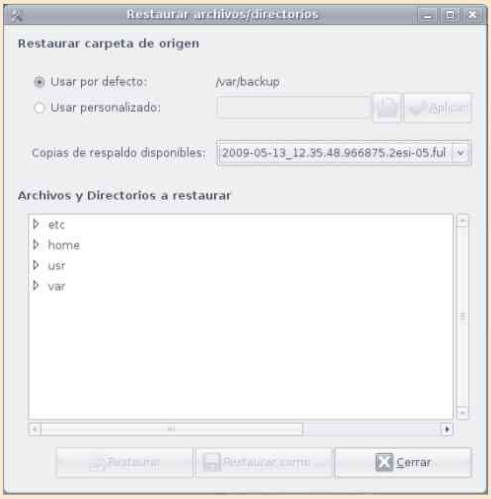


***Figura 12.42**. SBackup. Restauración de un backup*

La restauración se hará mediante la aplicación restaurar copias de seguridad del menú **Sistema → Administración**.

ACTIVIDADES 12.1

Como actividad se propone que el alumno realice lo siguiente:

a. Instalar Sbackup en el equipo.

b. Crear un directorio en el escritorio incluyendo en el algún fichero de texto editando su contenido.

c. Crear un *backup* de dicho directorio mediante la herramienta Sbackup.

d. Borrar el directorio y los ficheros que contiene.

e. Restaurar la copia de seguridad.

f. Verificar la existencia del directorio restaurado y el contenido de los ficheros restaurados.

12.9 PLANES DE PUESTA EN SERVICIO DE SISTEMAS INFORMÁTICOS

El objetivo de un plan de puesta en servicio o puesta en marcha es describir qué pasos se van a dar, cuándo (fechas) y en qué orden para poner en marcha un sistema informático. Un sistema informático no solo es el equipo informático, sino que comprende también el software, las personas y la información.

Generalmente, estos planes de puesta en marcha se suelen realizar para grupos de equipos informáticos o equipos informáticos de gran potencia como servidores o similares. Para ello se tendrán que poner de acuerdo los miembros de la organización y estar todos coordinados.

Antes de la puesta en marcha de un equipo o conjunto de equipos el entorno técnico e infraestructura deberá estar definido y en muchas ocasiones implantado. Cuestiones como las aplicaciones que va a utilizar el equipo, tipo de arquitectura, sistema operativo, etc., deberán de estar perfectamente definidos.

Se pueden plantear dos formas de puesta en marcha, una gradual u otra completa o integral. Lo más comun es establecer la puesta en marcha en varias fases y que en cada fase intervenga un tipo determinado de personas. Hay que darse cuenta que al poner en marcha un equipo informático se deberá crear la infraestructura física, instalar los sistemas base, instalar aplicaciones y demás software, cargar los datos de las nuevas aplicaciones, etc.

La parte que suele ser más importante y laboriosa en la implantación y puesta en marcha de un sistema informático es la instalación, configuración de las aplicaciones y por qué no decir, la introducción de datos en el nuevo sistema.

12.10 RENDIMIENTO Y MONITORIZACIÓN DE SISTEMAS INFORMÁTICOS

12.10.1 RENDIMIENTO DEL SISTEMA: BENCHMARKING

Un *benchmark* es una técnica utilizada para medir el rendimiento de un sistema o alguna parte del mismo. Generalmente, los resultados del *benchmark* se comparan con otros equipos o dispositivos similares para establecer una comparativa.

IMPORTANTE

Benchmarking del almacenamiento con HDTune

HDTune es un *benchmark* que permite realizar pruebas e informes del estado de los discos duros de un equipo informático.

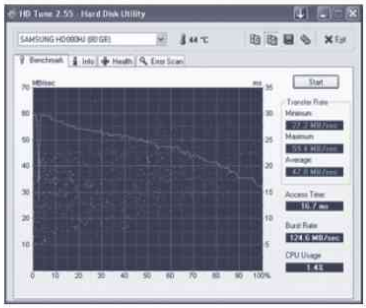


***Figura 12.43**. HD Tune. Utilidad Benchmark*

El programa además de indicar la temperatura del disco en la botonera superior, tiene 4 pestañas principales:

- *Benchmark*
- *Info*
- *Health*
- *Error scan*

Pestaña benchmark

En esta pestaña se puede someter al disco a una serie de pruebas para obtener los siguientes parámetros:

- **Tasa de transferencia** (*transfer rate*). Es la cantidad de información por unidad de tiempo (segundo) que el disco transfiere una vez que la aguja está en la pista y sector determinado.
  - Mínima.
  - Máxima.
  - Media.
- **Tiempo de acceso**. Es el tiempo que tarda la aguja en colocarse en la pista y sector deseado.
- **Burst rate**. Es la máxima velocidad (en megabytes por segundo) a la cual los datos pueden ser transferidos desde el interface del disco (IDE, SATA, SCSI…) al sistema operativo.
- **Uso de CPU**. Es el porcentaje de CPU que necesita el sistema al leer datos desde el disco duro.

12.10.2 HERRAMIENTAS DE MONITORIZACIÓN Y MEDICIÓN DE PARÁMETROS DEL SISTEMA

Muchas herramientas de monitorización y medición vienen con el propio sistema operativo. Por ejemplo, el monitor de actividad puede ser una herramienta de suma utilidad. Existen monitores de actividad en todos los sistemas operativos (Windows®, Linux, Macintosh® y otros).

Algunas operaciones que se pueden realizar con este tipo de sistemas es analizar la memoria y el % de CPU que consumen ciertos recursos y de esa manera conocer si hay alguna aplicación que está sobrecargando el sistema apropiándose de los recursos.

***Figura 12.44**. Monitor de actividad. CPU. Mac OS X*

En este tipo de herramientas se puede conocer el tiempo de CPU que el sistema dedica al usuario, al sistema o en espera de trabajo (*idle*).

***Figura 12.45**. Monitorización de la memoria. Mac OS X.*

Otra opción interesante es conocer cómo está siendo utilizada la memoria. Por ejemplo, en la figura anterior se puede observar que el equipo tiene 2 GB de memoria de los cuales 1,69 GB están siendo usados y 315,3 MB están libres.

IMPORTANTE

La memoria libre

El disponer de memoria libre en el sistema es muy importante. Si el sistema se queda sin memoria libre o con muy poca, se ralentiza y deja de funcionar de forma aceptable.

También se puede observar que de los 1,69 GB utilizados 260,7 MB son memoria *wired*, lo que implica que necesitan almacenarse en memoria RAM de forma obligatoria, 1,06 GB están activos (utilizándose de forma activa) y 385,4 MB pertenecen a la memoria inactiva (memoria que ha dejado de utilizarse).

IMPORTANTE

Detectando programas que no funcionan correctamente

En ocasiones los programas empiezan a trabajar de forma incorrecta y empiezan a consumir mucha CPU o mucha memoria sin causa justificada. Con el monitor de actividad se pueden detectar fácilmente estos procesos. Ordena los procesos por la columna % de CPU consumido ó % de memoria consumida y aparecerán los primeros. Utilice la opción del sistema operativo para eliminarlo de los programas en ejecución.

RESUMEN DEL CAPÍTULO

Una de las funciones más necesarias en todo sistema informático es el mantenimiento del mismo. El mantenimiento, entre otras funciones, se encarga de minimizar o anular el impacto que pueda tener un fallo o suceso negativo, prevenir frente a imprevistos (virus, fallos hardware, borrados accidentales, fallos software…), mantener el sistema operativo y proporcionar funcionalidad, así como recuperar los sistemas en caso de averías.

Los técnicos en su trabajo diario se encontrarán con que tienen que montar sistemas desde cero pero en muchas más ocasiones quizás deberán de mantener sistemas ya existentes.

En este capítulo se explica la clonación tanto de particiones como de discos. Esta práctica es sencilla y muy útil. Cualquier técnico en sistemas informáticos debe conocer y utilizar en su día a día las clonaciones y las copias de seguridad. El *backup* o copia de seguridad como se ha explicado será una opción complementaria a la clonación, dado que no siempre es posible ni operativo hacer una clonación.

EJERCICIOS PROPUESTOS

En los siguientes ejercicios se van a hacer una serie de manipulaciones a los equipos. Lo ideal es que se realicen este tipo de pruebas a equipos de prácticas y que el alumno no trabaje con el equipo de trabajo.

1. Copias de seguridad.

Coloque la estrella al igual que en la figura del Apartado 12.8.2 del capítulo en los siguientes supuestos:

Supuesto 1

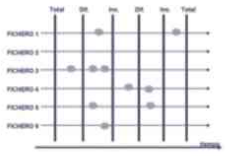


***Figura 12.46**. Backup Supuesto 1*

Supuesto 2

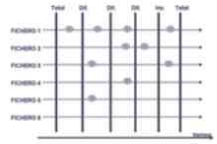


***Figura 12.47**. Backup Supuesto 2*

Supuesto 3

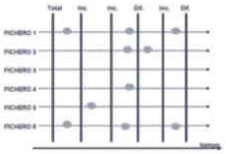


***Figura 12.48**. Backup Supuesto 3*

2. Copia de seguridad en Windows®.

- Utilice Uranium *backup* free para realizar una copia de seguridad de tu sistema. Deje la copia preparada para que se ejecute todos los días de la semana (salvo sábados y domingos) a una hora determinada (elija 5 minutos después de la hora actual y así podrás ver el resultado). La copia de seguridad deberá estar comprimida y cifrada. Una vez realizado el *backup*, copie algunos de los ficheros incluidos en el *backup* en un dispositivo como *pendrive* o similar y pruebe a restaurarlos en su ubicación original desde el *backup*. Uranium *backup free* se encuentra en su CD de recursos. También puede bajarse una versión más actualizada de *www.uraniumbackup.com*.

3. Clonación de discos.

- Realice una clonación de un disco tal y como se explica al comienzo del capítulo utilizando para ello los siguientes dispositivos:
  - Disco duro USB.
  - Instalando otro disco duro en el equipo.
  - A través de la red.

4. Clonezilla.

- Clonezilla es una herramienta de clonación Opensource muy parecida a las utilizadas en este tema y parecida también a Norton Ghost®. Para una mayor rapidez solo salva y restaura los bloques utilizados de un disco o partición. El ejercicio que se propone al alumno es que cree un *pendrive* o disco USB con la versión *live* de clonezilla, la cual se puede descargar en la siguiente dirección:
  http://clonezilla.org
- Una vez descargado el ZIP (la ISO se utilizaría para quemar un CD/DVD) se procederá a generar un *pendrive* o disco USB *bootable*. La información de cómo se genera se puede encontrar en la página web anterior.
- El disco deberá estar formateado FAT32.
- Una vez descomprimido el fichero ZIP en el dipositivo USB se procederá a hacerlo *bootable* ejecutando el *script makeboot.sh* situado en el directorio **utils/linux** del dispositivo USB.
- El objetivo del ejercicio además de crear el dispositivo USB es hacer una clonación/restauración de un equipo utilizando otro disco (externo o interno) y una ubicación de red.
- Recuerde cambiar la secuencia de arranque en la BIOS para arrancar desde el dispositivo USB.

5. Ejercicio de profundización: FOG.
FOG es una herramienta de clonación a alto nivel. Gracias a su interfaz web el manejo de FOG es sencillo, intuitivo e independiente del sistema operativo.
- El objetivo del ejercicio es que en grupos de 2, 3 ó 4 personas se monte un entorno FOG con un servidor y clientes que generen sus imágenes y las recuperen después.
- Como primera documentación el alumno puede utilizar la siguiente:
  - Linux+ número 2/2010. Clonación automática de equipos con FOG de Andrés Rosique. Esta revista y otras están descargables en *http://lpmagazine.org/es/*
  - *http://www.fogproject.org/*

6. Con el equipo desconectado de la corriente ábralo y desconecte el cable SATA o IDE del disco de sistema del equipo. Una vez desconectado este cable, cierre el equipo y enciéndalo. ¿Qué mensajes de error o síntomas presenta?
Una vez comprobado este punto restaure el equipo a su configuración original.

7. Con el equipo desconectado de la corriente ábralo y retire los módulos de RAM que haya instalados en el equipo. Una vez desconectado este cable, cierre el equipo y enciéndalo. ¿Qué mensajes de error o síntomas presenta?
Una vez comprobado este punto restaure el equipo a su configuración original.

8. Con el equipo desconectado de la corriente ábralo y retire el conector ATX 12V de la placa base que alimenta el procesador. Una vez desconectado este cable, cierre el equipo y enciéndalo. ¿Qué mensajes de error o síntomas presenta?
Una vez comprobado este punto restaure el equipo a su configuración original.

9. Con el equipo desconectado de la corriente ábralo y retire el procesador. Una vez retirado cierre el equipo y enciéndalo. ¿Qué mensajes de error o síntomas presenta?
Una vez comprobado este punto restaure el equipo a su configuración original.

10. Con el equipo desconectado de la corriente ábralo y deje solo un módulo de memoria en su equipo. Pruebe a arrancar el equipo con el módulo de memoria en cada uno de los bancos que tenga la placa base. ¿Funciona la memoria en todos los bancos? Busque en Internet si da igual colocar la memoria en el banco que se quiera para todas las placas.

Una vez comprobado este punto restaure el equipo a su configuración original.

11. Empareje cada error con su posible causa.

Tabla 12.2 Empareja cada error con su posible causa

Error	Causa
Mensaje por pantalla al iniciar el equipo: *"Parity Error"*.	La fuente tiene poca capacidad.
Tenemos una BIOS AMI y escuchamos al encender el ordenador 2 pitidos.	El cable del monitor a el ordenador no está bien conectado.
El equipo tras funcionar durante un rato se apaga. Si se vuelve a encender se apaga pero dura encendido menos tiempo.	Falló la tarjeta gráfica integrada.
El equipo no enciende.	Problema en la Memoria.
Mensaje por pantalla al iniciar el equipo: *"No video card found o No monitor connected o No monitor connected"*.	Problema en el refresco de la memoria RAM.
Tras instalar un nuevo disco duro, la fuente tiene un comportamiento anormal. En ocasiones se producen apagados y reseteos.	El valor en la BIOS para parada por sobrecalentamiento es muy bajo.
Mensaje por pantalla al iniciar el equipo: *"RAM Refresh Failure"*.	Este error puede ser debido a una mala configuración de la BIOS al no soportar paridad de memoria. Se deshabilita en la BIOS y se vuelve a arrancar el equipo.
El equipo se apaga de repente.	Problema de sobrecalentamiento.
El equipo enciende pero el monitor no muestra nada en pantalla.	Fuente de alimentación averiada.

12. El microprocesador de un equipo se calienta demasiado. Con un software de medición de temperaturas se ha comprobado que funciona normalmente por encima de los 80°-90°. ¿Qué soluciones se pueden adoptar?

13. ¿Qué es la energía electrostática?

14. Se desea cambiar el disipador y el ventilador de mi microprocesador porque se ha averiado. Un día dejo de funcionar y se ha comprobado que el ventilador no funciona. En la tienda de informática hay en venta 2 disipadores, uno de aluminio y otro de cobre, con las mismas características, dimensiones y al mismo precio. ¿Cuál aconseja el alumno y por qué?

15. Mi amigo Miguel, que monta ordenadores en sus ratos libres, me ha dicho que cuanta más pasta térmica se le ponga a un micro será mejor, pues estará mucho más ventilado. ¿Debo creerle? Si el alumno no está de acuerdo que lo explique razonando la respuesta.

16. El disco duro de un equipo hace unos ruidos que antes no hacía. ¿Qué puede estar pasando? Razonar respuesta.

17. En la oficina de Raúl, que es fumador, siempre hay mucho polvo porque hay reformas en el edificio. ¿Qué consejos le puede dar para que los equipos se conserven lo mejor posible?

18. María es nueva en el mundo de la informática y se ha comprado un portátil. ¿Puede darle uno o más consejos con respecto a la batería del equipo? Le dice que no sabe si tiene que tenerla siempre enchufada o desconectada. También explique las características que tienen las baterías de los portátiles y aconséjele cuál sería la mejor opción, dado que ella es representante y trabaja fuera de casa.

19. Acabo de montar un equipo. Dígame 7 cosas que debería de verificar antes de poner el equipo en marcha.

20. El equipo no arranca. ¿Cómo puedo verificar si lo que está estropeado es la fuente de alimentación?

21. Mi equipo al arrancar da 2 pitidos largos y 1 corto antes de arrancar. ¿Qué puede estarle pasando?

22. ¿Qué es más seguro frente a golpes, una unidad SSD o un disco duro?

23. Quiero ampliar la memoria y la capacidad del disco duro de mi equipo pero no se nada de informática. ¿Qué posibilidades hay si quiero conservar el disco y memoria que ya tiene?

24. El equipo con el que trabajo está en un mueble. El equipo cabe justo en el hueco del mueble que está también pegado a la pared. El equipo se apaga muchas veces y mi vecino, que ha estudiado un ciclo de formación profesional, me ha dicho que puede ser por la falta de ventilación de la caja ¿Es eso cierto o puede deberse a otros factores? ¿Cómo puedo comprobar si esto es cierto?

TEST DE CONOCIMIENTOS

1 Elija la respuesta incorrecta:

a) Solo los microprocesadores de calidad tienen sistemas de protección frente a sobrecalentamientos.
b) La energía estática se acumula en el cuerpo humano.
c) El cobre es un metal mucho más conductivo que el aluminio.
d) *Sbackup* es un programa con el cual poder realizar de una forma sencilla copias de seguridad de forma remota.

2 Elija la respuesta incorrecta:

a) Los puertos USB frontales fallan más que los traseros integrados en la placa base.
b) Las descargas electrostáticas muchas veces no son visibles al ojo humano.
c) La electromigración es uno de los principales factores de avería y degradación de los dispositivos electrónicos.
d) A pesar de las copias de seguridad, es prácticamente imposible garantizar la seguridad de un sistema al 100%.

3 Elija la respuesta correcta:
- a) Solo los microprocesadores de calidad tienen sistemas de protección frente a sobrecalentamientos.
- b) La energía estática se acumula en el interior de los materiales aislantes.
- c) El *backup* diferencial nunca desactiva el atributo modificado.
- d) Los síntomas cuando el microprocesador está roto es que el equipo ejecuta el POST pero no pasa de ahí.

4 Elija la respuesta correcta:
- a) Si el *speaker* del equipo está desconectado, el equipo avisará con una serie de pitidos este problema.
- b) El mantenimiento correctivo se anticipa a los fallos que puedan ocurrir en el hardware.
- c) Es seguro manipular el interior de una fuente de alimentación una vez desenchufada.
- d) Cuando hay un fallo en el sistema se pierde la información existente entre el último *backup* y el momento del fallo.

5 Elija la respuesta correcta:
- a) El mantenimiento predictivo espera a que el componente falle para luego sustituirlo.
- b) Las baterías de los portátiles hay que dejarlas descargarse completamente, de lo contrario se producirá electromigración y la vida de la batería se acortará.
- c) A pesar de las copias de seguridad, es prácticamente imposible garantizar la seguridad de un sistema al 100%.
- d) Un *live* CD no puede considerarse una herramienta informática.

6 Elija la frase correcta:
- a) Es posible monitorizar los voltajes del equipo mediante la BIOS.
- b) Antes de manipular un portátil hay que descargar la batería. Una forma de hacer esto es dejar el aparato encendido hasta su descarga.
- c) Normalmente, los equipos no están diseñados para trabajar con un grado alto de humedad.
- d) Reducir la tecnología de fabricación permite aumentar el voltaje a los microprocesadores y de esta manera aumentar el rendimiento de los mismos.

7 Elija la respuesta correcta:
- a) Las baterías de los portátiles hay que dejarlas descargarse completamente, de lo contrario se producirá electromigración.
- b) Cuando el POST encuentra algún error avisará con una serie de pitidos esté el *speaker* conectado o no.
- c) El mantenimiento predictivo espera a que el componente falle para luego sustituirlo.
- d) Si la pantalla se ve oscura o simplemente no se ve y cuando conectamos un monitor externo este se ve perfectamente, el problema estará seguramente en el *inverter* o inversor.

8 Elija la frase incorrecta:
- a) Antes de manipular un portátil hay que descargar la batería. Una forma de hacer esto es dejar el aparato encendido hasta su descarga.
- b) La temperatura es uno de los principales factores de avería y degradación de los dispositivos electrónicos.
- c) Muchos errores se pueden detectar desde el POST y la BIOS.
- d) Al aumentar el número de núcleos se reduce la velocidad de los microprocesadores.

9 Elija la respuesta correcta:
- a) El *inverter* es una placa que suele estar en la parte posterior de la pantalla y se encarga de suministrar corriente eléctrica al sistema de emisión de luz de la pantalla.
- b) El mantenimiento correctivo se anticipa a los fallos que puedan ocurrir en el hardware.
- c) Los síntomas cuando el microprocesador está roto es que el equipo ejecuta el POST pero no pasa de ahí.
- d) Es seguro manipular el interior de una fuente de alimentación una vez desenchufada.

10 Elija la frase incorrecta:
- a) Muchos errores se pueden detectar desde el POST y la BIOS.
- b) Contra la energía electrostática los mejores aliados son las pulseras de cuero y el calzado con suela de goma o material aislante.
- c) A más velocidad de un micro se produce más calor.
- d) Al aumentar el número de núcleos se reduce la velocidad de los microprocesadores.

11 Elija la respuesta incorrecta:

a) Los puertos USB frontales fallan más que los traseros.

b) Cuando hay un fallo en el sistema se pierde la información existente entre el último *backup* y el momento del fallo.

c) Si el *speaker* del equipo está desconectado, el equipo avisará con una serie de pitidos este problema.

d) Las descargas electrostáticas muchas veces no son visibles al ojo humano.

12 Elija la frase correcta:

a) Un ruido anormal en el disco duro generalmente es síntoma de que el disco va a fallar en un futuro.

b) Reducir la tecnología de fabricación permite aumentar el voltaje a los microprocesadores y, de esta manera, aumentar el rendimiento de los mismos.

c) Un *live* CD no puede considerarse una herramienta informática.

d) Normalmente, los equipos no están diseñados para trabajar con un grado alto de humedad.

13 Elija la frase incorrecta:

a) Hay muchos componentes o modelos de equipos que presentan los mismos fallos.

b) Un disipador de plata sería mucho más efectivo que uno de cobre o aluminio.

c) Para alargar la vida de la batería del portátil es mejor dejarla agotarse antes de recargarla.

d) Los puertos USB frontales fallan más que los traseros debido a que el *driver* no es el mismo.

14 Elija la frase correcta:

a) Antes de abrir o manipular cualquier portátil hay que desconectar el cable de alimentación y la batería.

b) El *inverter* es una placa que suele estar integrada en la placa base y se encarga de suministrar corriente eléctrica al sistema de emisión de luz de la pantalla.

c) Con el comando *tar cvf dir1.tar dir1* se creará un fichero *tar* comprimido *dir1.tar* que contendrá el directorio *dir1* con todos sus ficheros y subdirectorios si existen.

d) Los discos duros cuentan con una utilidad de nombre *SMART*, que permiten saber si un disco no va a fallar o si ya está dando síntomas de un mal funcionamiento.

15 Elija la frase incorrecta:

a) Los dos sitios más peligrosos a la hora de la manipulación son el interior de la fuente de alimentación y el interior del monitor.

b) En el mantenimiento preventivo lo que se pretende es preservar y prevenir que ocurran averías en el equipo informático.

c) Cuando un ordenador falla o no arranca, la mejor solución es dejar el equipo con los mínimos componentes para que funcione.

d) Para proteger el sistema eléctrico del portátil es mejor no trabajar siempre con la batería puesta.

16 Elija la frase correcta:

a) Al aumentar el número de núcleos se aumenta el rendimiento de los microprocesadores.

b) Si la pantalla se ve oscura o simplemente no se ve y cuando conectamos un monitor externo éste se ve perfectamente, el problema estará seguramente en la tarjeta gráfica.

c) Normalmente si conectamos un monitor externo y no se ve nada o se sigue viendo la imagen distorsionada es muy probable que el inversor esté estropeado.

d) GSmartControl es una utilidad de Windows® que proporciona información *SMART* sobre los discos del equipo.

17 Elija la frase correcta:

a) En caso de que caiga algún líquido sobre algún componente electrónico lo primero que hay que hacer es apagarlo.

b) Si la pantalla se ve oscura o simplemente no se ve y cuando conectamos un monitor externo éste se ve perfectamente, el problema estará seguramente en la tarjeta gráfica.

c) Normalmente si conectamos un monitor externo y no se ve nada o se sigue viendo la imagen distorsionada es muy probable que el inversor esté estropeado.

d) GSmartControl es una utilidad de Windows® que proporciona información SMART sobre los discos del equipo.

13 Mantenimiento y puesta en servicio de redes locales

OBJETIVOS DEL CAPÍTULO

- ✓ Conocer los procedimientos necesarios para la puesta en servicio de redes de área local.
- ✓ Entender los mecanismos para el diagnóstico y la localización de averías relaccionando los síntomas de las mismas con las posibles soluciones.
- ✓ Entender el funcionamiento de diferentes herramientas para la monitorización de las redes locales.

Las dos principales tareas que un técnico de redes va a llevar a cabo habitualmente son la puesta en servicio de redes y el mantenimiento de dichas redes. Este mantenimiento incluye, además, las labores de localización y reparación de averías. Este capítulo aborda estas dos tareas. En la primera parte se exponen los principales aspectos relacionados con la puesta en servicio o instalación de redes de área local. La fase de planificación tiene una gran importancia tanto en el uso de los recursos de red como en el adecuado dimensionamiento de la misma. Para llevar a cabo la planificación se tendrá muy en cuenta la normativa sobre cableado estructurado que se mostró en el Capítulo 8.

13.1 DIMENSIONADO DE LA RED

Uno de los pasos que se deberá llevar a cabo en la planificación de la red es el adecuado dimensionado del sistema de cableado estructurado. A continuación se exponen algunos criterios generales para llevar a cabo el dimensionado de los diferentes elementos que formarán parte de dicho sistema de cableado estructurado:

- **Dimensionado de las tomas de usuario**. Se deben instalar dos tomas de datos en cada puesto de trabajo más un número de tomas extra para dispositivos de uso compartido como impresoras, fotocopiadoras, puntos de acceso inalámbricos, etc.
- **Dimensionado del cableado horizontal**. Se deberá calcular el cableado necesario para conectar todas las tomas de usuario con el repartidor de cableado horizontal añadiendo un porcentaje extra de cableado para posibles ampliaciones. Un valor típico puede ser del 5%. Además, habrá que añadir tanto los latiguillos del puesto de trabajo para conectar la roseta al equipo del usuario, como los latiguillos de parcheo utilizados en el armario de comunicaciones.
- **Dimensionado del cableado vertical**. Se debe decidir el tipo de cableado y el número de pares utilizados. Habitualmente se utiliza cable de fibra óptica multimodo si la longitud del tendido no supera los 500 metros y cable de fibra óptica monomodo si el tendido supera dicha longitud. El número de fibras utilizadas dependerá de cada instalación. También serán necesarios latiguillos de fibra óptica.
- **Dimensionado del cableado troncal de campus**. Se suele utilizar cableado de fibra óptica monomodo que conecta cada uno de los distribuidores de edificio con el distribuidor de campus. Tanto en el cableado vertical como de campus de deberá sobredimensionar el número de fibras utilizadas para tener en cuenta futuras ampliaciones.
- **Dimensionado de las canalizaciones**. Las canalizaciones interiores deberán ser dimensionadas para prever futuras ampliaciones. De esta forma, las canalizaciones principales deberán dejar una capacidad libre de hasta el 50% de su capacidad total.

De igual forma, con la información del número de tomas de usuario por planta y la estimación de futuras ampliaciones se deberá hacer un cálculo del número de *switches* necesarios, así como sus principales características, para dar servicio a la red de datos.

13.2 PLANOS Y ESQUEMAS

Se deberá disponer de los planos de todas las plantas donde se va a realizar la instalación de la red. Estos planos deberán ser suministrados por el cliente preferentemente en algún formato electrónico estándar, como puede ser el formato **AutoCad** (archivos de tipo DWG). En dichos planos se detallará la ubicación de todos los elementos que forman parte de la red de área local debidamente etiquetados.

Existen alternativas de software gratuito para poder visualizar y editar archivos de AutoCAD. Uno de los más interesantes es **DraftSight** disponible en Windows®, Linux y Mac:
www.3ds.com/es/products/draftsight/overview

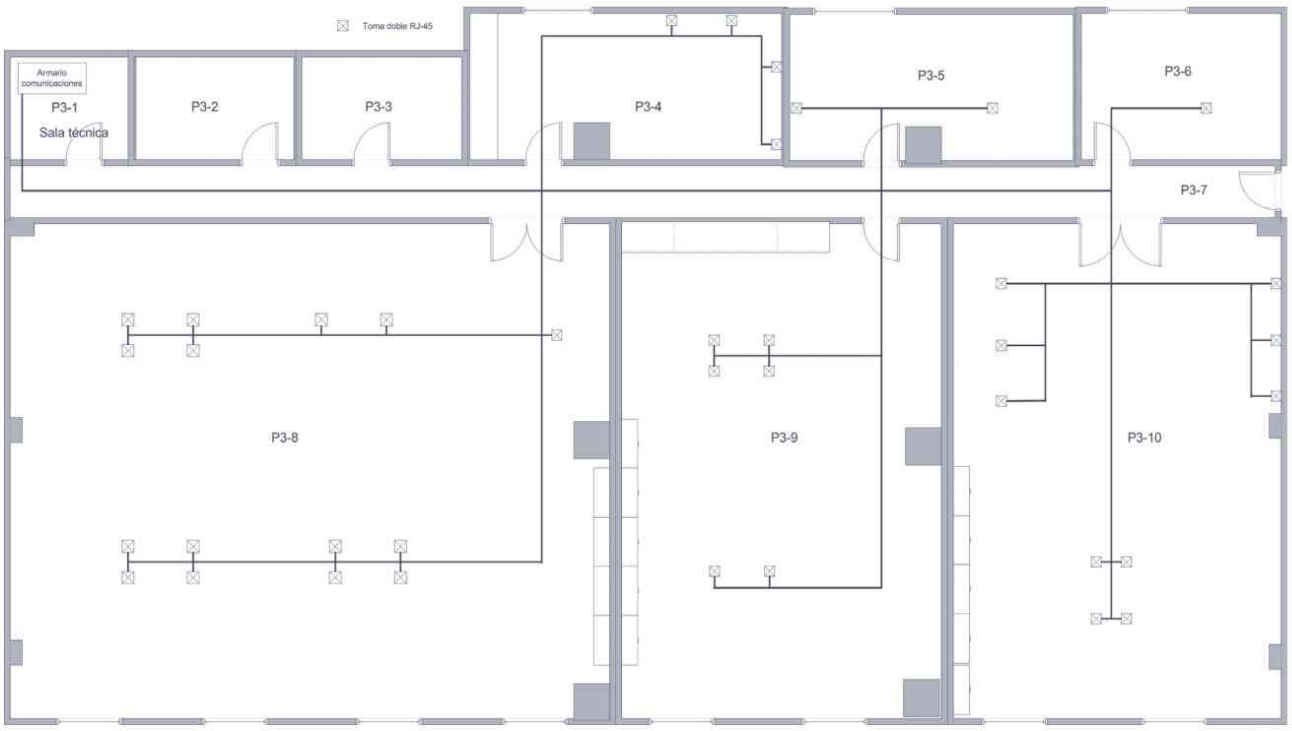


***Figura 13.1**. Plano de una planta donde se han ubicado los puntos de red*

Además de los planos de todas las plantas en las que se realizará la instalación de la red se debe incluir:

- Esquema de interconexión global de todos los elementos que componen la infraestructura.
- Esquemas de todos los armarios instalados donde se indique todo el equipamiento que incluyen.
- Esquema unifilar de todo el sistema eléctrico de uso exclusivo de las infraestructuras de la red.

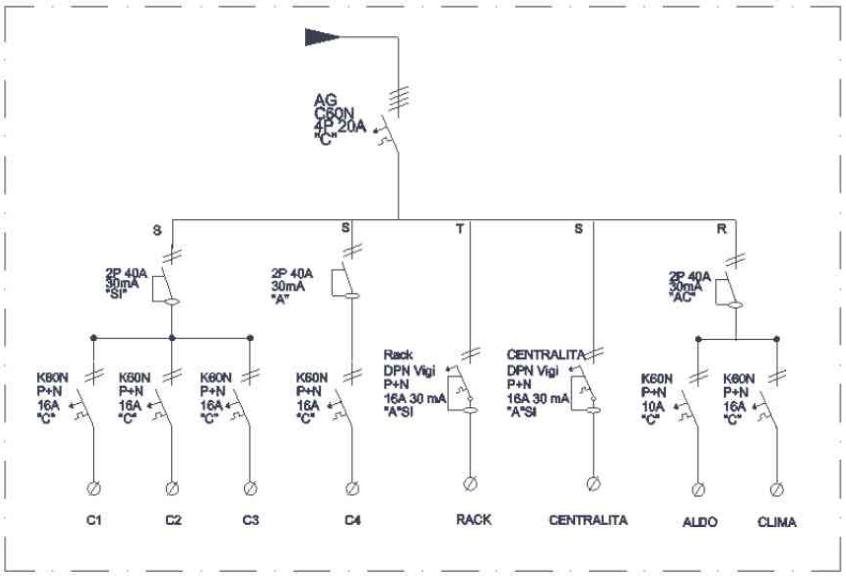


***Figura 13.2**. Esquema unifilar de una red de voz y datos*

13.3 ETIQUETADO

No existe una referencia exacta sobre los criterios de etiquetado de los diferentes elementos del sistema de cableado estructurado aunque sí es muy aconsejable que exista un procedimiento de etiquetado lo más claro posible. A continuación se ofrecen unas pautas generales para llevar a cabo dicho etiquetado:

- **Distribuidores de planta**. Se puede utilizar un código que corresponda a la planta y otro código que identifique el número de armario, si hubiera más de un armario de comunicaciones dentro del distribuidor de planta. En algunos casos se utiliza una letra para identificar el armario. Ejemplo:

  1A Distribuidor primera planta, armario A
  1B Distribuidor primera planta, armario B
  S1.1 Distribuidor sótano 1, armario 1

- **Cableado de subsistema vertical**. Se suele asignar un código a cada manguera de cableado vertical para identificar el tipo de cableado, el identificador de armario de distribución de planta al que se conecta y un número asociado al último par de la manguera. Ejemplos:

  VD-1A-100 Identifica un enlace vertical de datos (VD) que conecta con el distribuidor de planta 1A (armario A de la primera planta) y que incluye hasta el par número 100.

  VF-8.1-12 Identifica un enlace vertical de fibra óptica (VF) que conecta con el distribuidor de planta 8.1 (primer armario de la planta 8) hasta la fibra número 12.

- **Tomas de usuario**. La identificación de las tomas de usuario se suele hacer indicando el código del distribuidor de planta al que está conectado y se añade un código único identificativo. La asignación del número de identificación de la toma de usuario dentro de cada distribuidor de planta se suele hacer siguiendo unos determinados criterios.

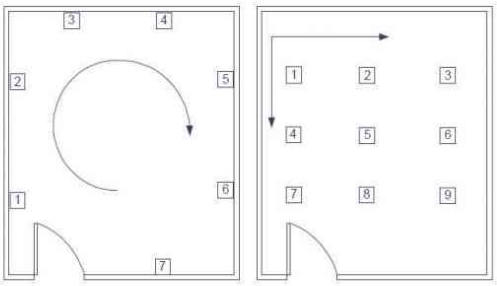


***Figura 13.3**. Criterios de numeración de tomas de usuario*

Ejemplos de identificadores de tomas de usuario:

1A-15 y 1A-16	Identifica las tomas 15 y 16 situadas en la primera planta y conectadas al armario A.
3.2-23	Identifica la toma 23 de la tercera planta y que está conectada al armario 2.
S1.1-10	Identifica la toma 10, situada en el sótano 1 y conectada al armario 1.

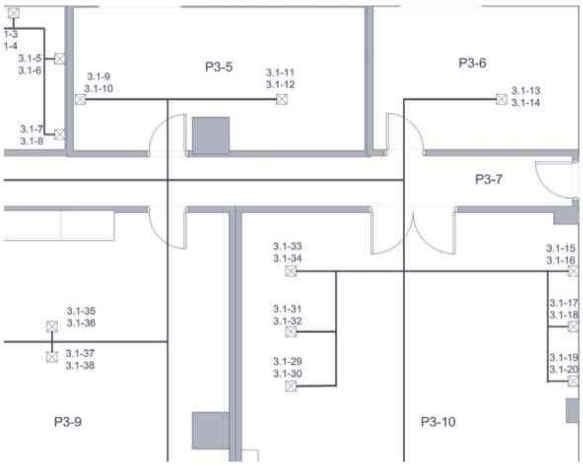


***Figura 13.4**. Etiquetado en plano de las tomas de usuario*

- **Cableado horizontal**. El etiquetado del cableado horizontal puede seguir los mismos criterios que el de las tomas de usuario y de hecho, se puede utilizar el mismo código asignado a la toma de usuario. Por ejemplo, un cable horizontal etiquetado como 3.2-23 identifica el par que conecta la toma 23 con el armario 2 de la primera planta.
- **Paneles de parcheo**. Para el etiquetado de los puertos de los paneles de parcheo se sigue igualmente una numeración correlativa. En muchas ocasiones el número de identificación de los puertos del panel de parcheo se corresponde con el identificador de la toma de usuario para facilitar las labores de mantenimiento.

13.4 MATERIALES Y EQUIPAMIENTO

Otro de los aspectos a considerar en la planificación de la puesta en servicio de una red son las especificaciones técnicas de los materiales utilizados así como las condiciones de instalación. En muchos casos, estas especificaciones técnicas vienen impuestas por las diferentes normativas que se deben cumplir. Por ejemplo, todos los materiales utilizados deben cumplir las normativas antiincendios. En cuanto al cableado y los elementos de conexión, estos deben cumplir habitualmente la normativa UNE-EN 50173.

13.4.1 CABLEADO HORIZONTAL

A continuación se indican algunos ejemplos de especificaciones técnicas referidas al cableado horizontal:

- El cableado horizontal se realizará de una sola tirada entre la roseta de usuario y el panel de conectores del armario repartidor de planta, estando terminantemente prohibidos los puntos de transición, empalmes o inserción de otros dispositivos.
- Como mínimo se instalarán dos cables balanceados de categoría 6 y constituirán enlaces permanentes y canales de Clase E, según las especificaciones de la norma EN 50173.
- En caso de instalarse fibra óptica será multimodo de índice gradual 62.5/125 µm.
- La distancia máxima entre la roseta de usuario y conector ubicado en el armario distribuidor de planta será de 90 metros (longitud mecánica). Se entregará una gráfica con la distribución estadística de los enlaces del SH dependientes de cada DP.

13.4.2 TOMAS DE USUARIO

Se indican algunos ejemplos representativos de especificaciones técnicas referidas a los materiales utilizados en las tomas de usuario.

- Las tomas de telecomunicaciones se instalarán preferentemente en cajas modulares de superficie, que serán de diferentes medidas:
  - Caja para 4 tomas RJ45 hembra.
  - Caja para 8 tomas RJ45 hembra.
  - Caja para 12 tomas RJ45 hembra.
- Las tomas de usuario en las que terminará el extremo del cable horizontal UTP serán de tipo RJ45 hembra y categoría 6, según especificación EN 60603-7-4.
- En caso de utilizar cableado horizontal de tipo STP, éste terminará en tomas RJ49 hembra y categoría 6, según especificación EN 60603-7-5.
- En ambos casos, la parte trasera del conector en la que se inserta el cable será de tipo IDC 110 y estará rotulada al menos con el código de colores normalizado según N 60603-7 opción B (equivalente al código EIA/TIA 568-B).
- Los latiguillos de usuario estarán compuestos por cable de cobre de 4 pares trenzados balanceados de tipo UTP, terminados en conectores RJ45 machos y categoría 6, debiendo cumplir la especificación EN 50288-6-2. Las medidas estándar de los latiguillos a emplear serán de 1 m, 2 m, 3m y 5m.

13.4.3 CABLEADO VERTICAL

Se indican en este apartado algunos ejemplos de especificaciones técnicas de los materiales utilizados en el cableado vertical:

- El cableado vertical se realizará de una sola tirada entre los dos distribuidores a unir, estando terminantemente prohibido el uso de empalmes o inserciones de otros dispositivos intermedios.
- Para la vertical de datos se utilizarán mangueras de 12 fibras ópticas multimodo de índice gradual 62,5/125 µm, según especificación EN 60793-2-10:2002-A1b, y deberá cumplir al menos la Categoría OM1.
- Adicionalmente, deberá cumplir las condiciones mecánicas y ambientales, según especificaciones EN 60794-1, IEC 60794-2 y EN 60794-3.
- La manguera de 12 fibras ópticas multimodo se conectará a un panel de 12 fibras de 1 U de altura, dotado de casete organizador y distribuidor de fibras. El panel se terminará en conectores de tipo ST.

13.4.4 CABLEADO DE CAMPUS

Se exponen a continuación algunos ejemplos de especificaciones técnicas relacionadas con elementos utilizados en el cableado de campus.

- El cableado de campus se realizará, salvo casos concretos y muy justificados, de una sola tirada entre los dos distribuidores a unir, estando terminantemente prohibido el uso de empalmes o inserciones de otros dispositivos intermedios.
- Se utilizarán mangueras de 12 fibras ópticas monomodo de salto de índice de 9/125 µm, según especificación EN 60793-2-50:2002-B1, y deberá cumplir la Categoría OS1.
- Adicionalmente, deberá cumplir las condiciones mecánicas y ambientales, según especificaciones EN 60794-1, IEC 60794-2 y EN 60794-3.
- La manguera de 12 fibras ópticas monomodo llevará una cubierta de protección de tipo PKP antihumedad y antiroedores y se conectará a un panel de 12 fibras de 1 U de altura, dotado de casete organizador y distribuidor de fibras. El panel se terminará en conectores de tipo SC simple.

13.4.5 ARMARIOS DE COMUNICACIONES

Se exponen algunos ejemplos de especificaciones técnicas referentes a los armarios de comunicaciones:

- Armarios tipo Rack de 19", anchura de 800 mm y profundidad de 800mm.
- Techo, parte trasera y laterales en chapa de acero, desmontables y con rejillas de ventilación.
- Ruedas dobles giratorias con banda de rodadura de goma.
- Tendrán una altura mínima de 42U, y máxima de 47U
- Puerta frontal transparente, provista de juntas de goma y cerradura con llave.

En los armarios de comunicaciones se podrán configurar los siguientes módulos:

- VF. Paneles para las tomas verticales de datos (fibra óptica).
- VD. Paneles para las tomas verticales de datos (enlaces de cobre).
- HD. Paneles para las tomas horizontales de datos.
- EL. Hueco para la electrónica.

13.4.6 ALIMENTACIÓN

Se indican en este apartado algunos ejemplos de especificaciones técnicas de los materiales utilizados en la alimentación utilizada para los armarios de comunicaciones:

- Se instalarán regletas de tomas de corriente tipo *schuko* de 16A con toma de tierra. Todas las regletas contarán con protección magnetotérmica integrada, o bien serán cableadas hasta las bornas del magnetotérmico instalado en el armario.
- Las regletas serán de montaje en unidades de 19" y se instalarán en horizontal en el perfil posterior del *rack*, mirando hacia la parte frontal. Se colocará un pasahilos para gestionar los cables de alimentación de los equipos conectados a la regleta.
- El número de tomas tipo *schuko* será:
  - Un mínimo de 8 en los armarios DP que puedan contener algún tipo de electrónica de red.
  - Un mínimo de 12 en los armarios DE que puedan contener algún tipo de electrónica de red.
- La ubicación de los armarios garantizará una separación mínima de 3 metros respecto de las principales fuentes de señales parásitas (transformadores, onduladores, ascensores, etc.).
- Los armarios contarán con un kit de puesta a tierra que conectará al SPAT dedicado todas sus partes metálicas y las de los elementos que contenga.
- En caso de que el edificio posea un sistema de alimentación ininterrumpida (SAI) con la suficiente capacidad, se deberá conectar el armario distribuidor a dicho sistema, realizando todo lo necesario para ello.

13.4.7 ELEMENTOS DE DISTRIBUCIÓN

Se indican en este apartado algunos ejemplos de especificaciones técnicas de los materiales utilizados en la canalización del sistema:

- **Bandeja de rejilla de acero galvanizado**. Bandeja de rejilla con varillas de acero de 4,5 y 5 mm, de alta resistencia electrosoldadas, ajustada a las normas UNE 37-552-73 (ensayo sobre recubrimientos) y EN 50.085 (prenorma europea de ensayo de cargas para una deformación máxima f £ L/200 siendo L la distancia entre apoyos en mm). La distancia entre apoyos debe ser inferior o igual a 1 metro. Medidas: ancho de 60, 100, 200, 300, 450 y 600 mm; alto de 33, 62 y 100 mm; largo de 3.000 mm.
- **Tubo PVC**. Tubo flexible por espiral de PVC + PVC rígido, de grado de protección IP 67 y auto extinguible (según VL 94), resistente al impacto grado 4 según prenorma europea 50.086-1. Temperatura de operación entre -5 °C y 65 °C. Ajustado a la norma UNE 20.324/78 o DIN 40.050 (para los grados de protección).
- **Tubo Flexible de Poliamida**. Protección IP 67 ajustado a la norma UNE 20.324/78 o DIN 40.050, resistente al impacto grado 4 según prenorma europea 50.086-1. Temperatura de operación entre -30 °C y 100 °C. Resistente a fuel y aceites, no emisor de halógenos.
- **Tubo Flexible de PVC**. PVC liso interior y exterior, auto extinguible de grado de protección IP 67 ajustado a norma UNE 20.324/78 o DIN 40.050. Temperatura de operación entre -5 °C y 65 °C.
- **Tubo metálico**. Fleje de acero laminado en frío (según DIN 1624) galvanizado por ambos lados + PVC exterior, flexible, auto extinguible con grado de protección IP 67 ajustado a norma UNE 20.324/78 y resistente al impacto grado 3 según prenorma europea 50.086-1. Temperatura de operación entre -20 °C y 80 °C.
- **Bandeja de PVC con tapa**. Temperatura de servicio entre –20 °C a 60 °C. Rigidez dieléctrica según UNE 21.316. Auto extinguible a 960 °C (sin goteo del material inflamado o de partículas incandescentes) en el ensayo del hilo incandescente y no propagador de la llama en el ensayo de resistencia a la llama de plásticos autoportantes, según norma UNE 55.315. Difícilmente inflamable clasificada UL 94-VO. Coeficiente de dilatación lineal inferior a 0,07 mm/°C m. Protección contra daños mecánicos y contra penetración de cuerpos sólidos según norma UNE 20.324

13.5 DOCUMENTACIÓN

Los proyectos de puesta en servicio de redes locales, como cualquier otro tipo de proyectos, requieren la generación de una serie de documentos. Los documentos más comunes que será necesario redactar son los siguientes:

- **Memoria Técnica del Proyecto**. Es el documento de diseño base sobre el que se realizarán posteriormente los trabajos de ejecución de la puesta en servicio de la red local.
- **Informe del plan de ejecución**. Documento que incluye la temporización de los trabajos para llevar a cabo la puesta en servicio de la red local. También se suele incluir en este informe una relación del personal técnico que participará así como su función y cualificación.Todo lo relativo al desarrollo de los aspectos técnicos del proyecto se puede englobar en el llamado *plan de implantación*.
- **Plan de mantenimiento y formación**. Documento que normalmente exige el cliente donde se deben indicar los procedimientos de mantenimiento requeridos por la red así como los conocimientos sobre la misma que deben adquirir los técnicos que vayan a mantener dicha red.
- **Informe de certificación de calidad**. En muchas ocasiones el cliente exige diferentes certificaciones relacionadas con la implantación en los procesos de prestación del servicio de planes de calidad. El certificado más importante en este ámbito es el relacioando con las normas ISO 9000.
- **Informe de certificación EN-50173**. Como se ha visto anteriormente existen métodos estándarizados para comprobar las características del cableado. Los dispositivos conocidos como certificadores emiten dichos informes que en muchos casos son también exigidos por los clientes como garantía de la correcta instalación del cableado.
- **Presupuestos**. Un elemento importante dentro de la documentación es información relativa a los costes necesarios para llevar a cabo el proyecto. En los presupuestos habrá que desglosar todos los gastos indicando tanto el coste de los materiales como el coste por la mano de obra de los técnicos.
- **Planos de la instalación**. Es habitual entregar al cliente diferentes planos de las instalaciones indicando la ubicación de los diferentes elementos que forman parte de la red.

La documentación técnica final, que normalmente es necesario entregar al cliente, deberá incluir la siguiente información:

- ✓ Esquema general de las infraestructuras de comunicación.
- ✓ Número y tipo de tomas de usuario.
- ✓ Grado de ampliación de las infraestructuras existentes (cuando corresponda).
- ✓ Descripción completa y diagrama de cada uno de los armarios de comunicaciones.
- ✓ Descripción detallada y cálculos de dimensionamiento del sistema eléctrico.
- ✓ Canalizaciones empleadas, indicando dimensiones, accesorios necesarios y material de fabricación. Se detallarán los procedimientos de instalación de cada tipo de canalización en cada zona concreta del edificio.
- ✓ Tipo de cables y nº de conductores. Tipo de conectores y rosetas. Se detallarán los materiales de fabricación y las características exigibles.
- ✓ Dispositivos de red utilizados, normalmente *switches* y puntos de acceso, aunque también pueden incluirse otros como *routers*, *firewalls*, balanceadores de carga, inyectores de potencia PoE, convertidores de medios, etc. Se deberá indicar marca, modelo y sus principales características.

- ✓ Procedimientos detallados de instalación de todos los elementos que aseguren la calidad del sistema.
- ✓ Descripción completa de la obra civil asociada.
- ✓ Etiquetado y documentación de todo el sistema.
- ✓ Plan de implantación, incluyendo fases de ejecución y estimación del tiempo empleado en completar cada fase. En el caso en que se necesite un plan de migración del servicio de voz y datos, se incluirá en detalle.

13.6 CERTIFICACIÓN DE LA INSTALACIÓN

En muchas ocasiones y para asegurar la calidad de la instalación se debe llevar a cabo la certificación del cableado. Todos los enlaces instalados de cableado horizontal deben ser certificados de acuerdo a los procedimientos descritos en la norma EN 50346: 2002 con el aparato de medida homologado y calibrado al efecto, debiéndose presentar el modelo de equipo y su fecha de última calibración.

La certificación medirá para cada enlace los valores de todos los parámetros especificados por la norma EN 50173 para la clase correspondiente. La información de certificación normalmente se puede entregar en formato electrónico.

La aceptación de la infraestructura estará condicionada por tanto al cumplimiento de la clase correspondiente por parte de todos los enlaces. Adicionalmente, se deberán realizar todas las pruebas, comprobaciones y depuraciones necesarias de funcionamiento de la infraestructura de cableado en su totalidad, antes de la puesta en servicio a nivel de usuario.

PROYECTO
ID. Cable: S 1H-083
LUGAR:
Fecha / Hora: 11/03/2011 11:35:37am
OPERADOR:
Versión de Software: 2.3600
NVP: 68.2% Fecha de calibración: 25/08/2010

Sumario de Pruebas:PASA
Paso Libre: 5.1 dB (NEXT del Remoto 12-36)
Límite de Prueba: IS011801 Channel Class E
Tipo de Cable: Cat 6A UTP
DTX-1800 N/S: 8662005 DTX-CHA001
DTX-1800E N/S: 8662006 DTX-CHA001
Version de Límites: 1.5000

Mapa de Cableado: PASA (T568B) Result. TERM. RJ45: 1 2 3 4 5 6 7 8 / 1 2 3 4 5 6 7 8

Par	Longitud (m)	Lim.	Tiempo de Prop. ns	Lim.	Diferenc. Retardo ns	Lim.	Resistencia ohm.	Lim.	Impedancia ohm.	Lim.	Pérdida inserción Result. (dB)	Frec. MHz	Lim. (dB)
12	112.0		546	555	27	50	15.1	25.0			5.1	248.5	35.8
36	107.1		524	555	3	50	14.6	25.0			5.3	249.0	35.9
45	106.5		521	555	0	50	14.6	25.0			6.0	250.0	35.9
78	112.9		552	555	31	50	15.4	25.0			5.2	246.5	35.7

Resultados Principales — Resultados del Remoto

Par	Peor Margen Margen (dB)	Frec. MHz	Lim. (dB)	Peor Valor Margen (dB)	Frec. MHz	Lim. (dB)	Peor Margen Margen (dB)	Frec. MHz	Lim. (dB)	Peor Valor Margen (dB)	Frec. MHz	Lim. (dB)
RL												
12	10.0	215.5	8.7	10.0	215.5	8.7	9.0	3.0	19.0	14.4	155.5	10.1
36	9.3	53.3	14.7	12.9	216.5	8.6	6.5	67.0	13.7	8.4	247.0	8.2
45	8.8	69.5	13.6	11.2	236.0	8.3	6.8	5.9	19.0	7.7	191.0	9.2
78	9.3	102.5	11.9	10.2	146.0	10.4	9.2	3.0	19.0	10.9	182.0	9.4
PS NEXT												
12	7.5	7.5	56.1	19.4	192.0	32.2	7.4	79.5	38.8	11.4	228.0	30.9
36	7.7	30.9	45.8	9.7	224.0	31.0	6.9	79.5	38.8	10.6	238.5	30.5
45	9.1	30.8	45.8	10.8	224.0	31.0	8.4	7.5	56.1	10.6	224.0	31.0
78	8.3	7.6	55.9	12.2	192.0	32.2	8.9	5.0	59.0	12.5	246.5	30.3
PS ACR-N												
12	8.2	7.5	50.4	17.1	236.0	-4.2	7.3	3.1	58.0	18.4	248.0	-5.6
36	8.9	9.6	47.8	14.6	224.0	-2.8	8.0	4.1	56.1	15.8	238.5	-4.5
45	10.7	7.5	50.4	16.3	224.0	-3.6	8.5	4.3	55.6	17.2	245.5	-5.3
78	8.0	3.3	58.0	19.4	234.0	-4.0	8.1	3.9	56.6	17.7	246.5	-5.4
NEXT												
12-36	7.5	4.9	61.7	11.1	222.5	34.0	5.1	79.3	41.6	9.9	226.5	33.6
12-45	12.4	217.0	33.5	12.4	237.0	33.5	11.7	5.8	60.5	13.3	247.5	33.2
12-78	5.8	7.6	58.5	10.1	192.0	35.1	6.2	66.8	42.9	11.4	157.0	36.6
36-45	6.6	30.8	48.5	9.0	224.0	33.9	6.2	22.8	50.7	9.9	224.0	33.9
36-78	8.8	122.0	36.5	9.0	122.0	36.5	8.6	5.0	61.5	13.8	246.5	33.2
45-78	13.4	9.4	57.0	14.6	188.5	35.2	11.7	83.5	41.3	12.8	247.5	33.2
ACR-N												
12-36	7.6	4.8	57.3	16.1	222.5	0.3	7.7	79.3	22.5	15.6	236.5	-1.5
12-45	14.7	4.3	58.3	18.3	237.0	-1.4	12.4	5.8	55.5	19.3	248.0	-2.4
12-78	6.0	3.3	60.5	16.9	234.0	-1.0	7.1	3.3	60.5	21.9	248.5	-2.7
36-45	8.2	30.8	36.8	14.5	224.0	0.1	7.1	7.5	52.9	18.4	224.0	0.1
36-78	11.1	9.8	50.3	21.0	246.0	-2.4	9.2	5.0	56.6	16.9	246.5	-2.4
45-78	14.1	9.4	50.7	24.4	244.5	-2.2	9.9	4.1	58.6	18.2	245.5	-2.3
ACR-F												
12-36	17.5	126.0	21.2	17.9	204.5	17.0	16.7	210.0	16.8	16.7	210.0	16.8
12-45	18.0	249.0	15.3	18.0	249.0	15.3	16.6	245.0	15.5	16.6	245.0	15.5
12-78	12.6	4.6	50.0	12.8	242.0	15.6	11.7	249.0	15.3	11.7	249.0	15.3
36-12	16.6	212.0	16.7	16.6	212.0	16.7	17.5	126.0	21.2	18.1	204.5	17.0
36-45	11.4	236.5	15.6	11.5	243.0	15.5	12.5	159.0	19.2	12.9	241.0	15.6
36-78	14.9	179.5	18.2	14.9	179.5	18.2	16.4	182.0	18.1	17.6	223.5	16.3
45-12	18.4	243.0	15.5	18.4	243.0	15.5	17.1	248.5	15.4	17.1	248.5	15.4

***Figura 13.5**. Informe de la certificación de una instalación de red*

13.7 DIAGNÓSTICO Y LOCALIZACIÓN DE AVERÍAS

Como en cualquier otro ámbito tecnológico, las redes de datos son susceptibles de presentar problemas y averías en su funcionamiento. Debido a gran cantidad de posibles configuraciones y los diferentes niveles de complejidad que podemos encontrar no es posible dar pautas concretas y precisas para el diagnóstico y la localización de averías en las redes de datos. Sin embargo, se ofrecerán unas pautas generales que podrían ser válidas para cualquier tipo de red.

La primera labor que hay que llevar a cabo cuando se presenta un funcionamiento anómalo en una red es determinar con la mayor precisión posible los síntomas del problema. Para ello hay que entrevistarse con las personas afectadas para que nos proporcionen información sobre dichos síntomas

Después de obtener la información sobre los síntomas detectados por los usuarios será necesario llevar a cabo las comprobaciones sobre los diferentes elementos de la red. Para ello se emplearán tanto herramientas hardware (por ejemplo comprobadores de red) como herramientas software (aplicaciones y utilidades de diagnóstico). Una de las finalidades de las comprobaciones es aislar el problema, es decir, las comprobaciones, deberían servirnos para saber si el problema afecta a toda la red o solo una parte, y si es un problema software o hardware.

Para facilitar la tarea de diagnóstico de las averías es importante contar con información detallada sobre la red, como la topología, ubicación de los elementos de la red, ubicación del cableado, modelos de los diferentes dispositivos, servicios proporcionados por la red, direcciones de red y cualquier otra información que sea relevante para conocer el funcionamiento de la red. En definitiva, el primer paso que se debe dar en la resolución de un problema es determinar su ámbito. Para ello:

- Determinar si el problema afecta a un solo usuario de la red, a un grupo reducido o a toda la red.
- Determinar si el problema afecta a algún servicio de red concreto o afecta a todos los servicios. Algunos ejemplos de problemas en servicios concretos podrían ser el acceso al servidor web de la empresa, el acceso a Internet, el acceso a algún servidor de archivos, el acceso al correo. O por el contrario podría ser un problema de conectividad, por lo que afectaría a todos los servicios.

En muchas ocasiones, para llevar a cabo las primeras pruebas para determinar el ámbito del problema, se empieza por utilizar el comando *ping*.

Otra práctica interesante, que puede ayudar en algunos casos, es mantener un registro de los problemas ocurridos con anterioridad en la red con información sobre los síntomas detectados y la solución adoptada.

13.7.1 EL COMANDO PING COMO HERRAMIENTA DE DIAGNÓSTICO

Posiblemente, una de las herramientas más utilizadas por los técnicos de redes para verificar el funcionamiento de la red sea el comando *ping*, presente en todos los sistemas operativos actuales. Recordemos que el comando *ping* envía mensajes ICMP de tipo *Echo* al equipo que le indiquemos como parámetro. Si dicho equipo recibe los mensajes

ICMP, responde con mensajes ICMP de tipo *Echo Request*. De esta forma podemos comprobar si existe conectividad física y lógica entre dos equipos.

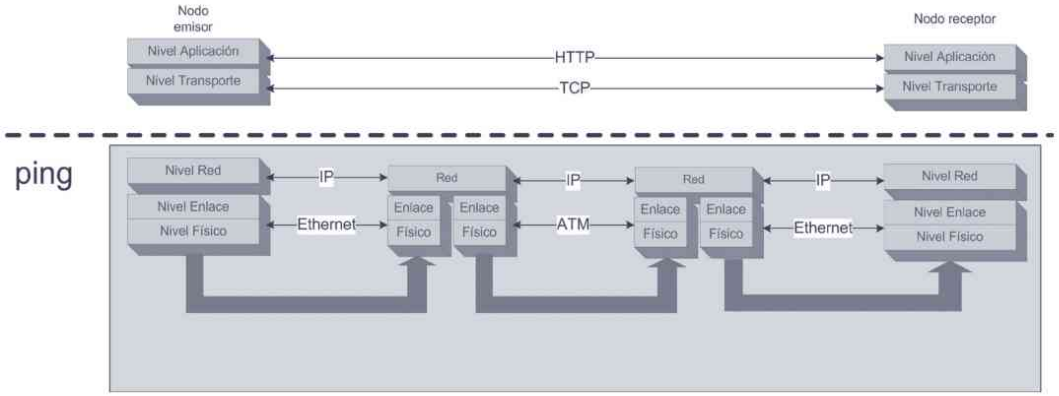


***Figura 13.6**. Alcance del comando ping en el modelo en niveles*

En la figura anterior se puede observar el alcance del comando *ping* dentro del modelo en niveles. Con la simple ejecución del comando *ping* podemos obtener las siguientes conclusiones:

- **Si recibo respuesta es que existe conectividad lógica entre los equipos**. Si estamos utilizando *ping* por algún problema en la red, sabremos que el problema está o en el nivel de transporte o en el nivel de aplicación.

```
Haciendo ping a 192.168.100.26 con 32 bytes de datos:
Respuesta desde 192.168.100.26: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.100.26: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.100.26: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.100.26: bytes=32 tiempo=1ms TTL=64
Estadísticas de ping para 192.168.100.26:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 1ms, Media = 1ms
```

- **Si no recibo respuesta es que el problema está en alguno de los tres primeros niveles**. El físico, el de enlace o el de red.

```
Haciendo ping a 192.168.100.254 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Estadísticas de ping para 192.168.100.254:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),
```

Puede ocurrir también que al ejecutar el comando ping algunos mensajes obtengan respuesta y otros no. En este caso habitualmente el problema suele estar en el nivel físico o en el de enlace.

Filtrado de los mensajes icmp del comando ping

Existe una excepción a la interpretación del comando *ping*. Algunos equipos tienen habilitada la función de cortafuegos y puede ocurrir que dicho cortafuegos no permita el paso de los mensajes ICMP. En este caso, aunque exista conectividad lógica y física entre los equipos no obtendríamos respuesta al comando *ping*. Filtrar los mensajes ICMP es una medida de seguridad ya que algunos ataques de denegación de servicio (DOS) pueden utilizar esta vía de acceso, aunque bien es cierto que el fitrado de los mensajes ICMP del comando *ping* entorpece las labores de mantenimiento de las redes.

Para comprobar esta característica en equipos con Windows® XP, se debe acceder al la configuración del *firewall* desde el **Panel de control → Centro de seguridad → Firewall de Windows®** y se elige la pestaña de **Opciones avanzadas**. En esta ventana podemos ver el apartado **ICMP** y pulsando el botón **Configuración** se accede a la ventana donde activar o desactivar el filtrado de mensajes ICMP *Echo*. La opción se llama **Permitir solicitud de eco entrante**.

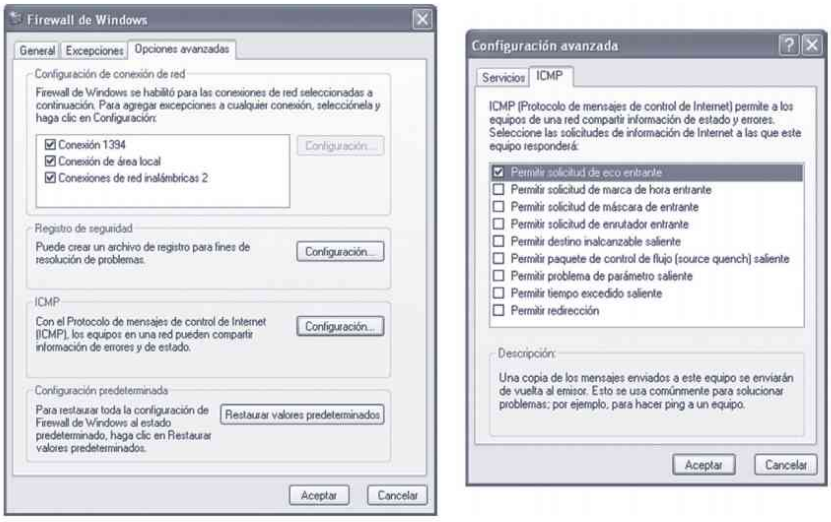


***Figura 13.7**. Configuración del firewall de Windows® XP para el filtrado de mensajes ICMP*

Para comprobar el filtrado de los mensajes ICMP en el *firewall* de Windows® 7 se debe acceder a la ventana principal de configuración del *firewall* desde el **Panel de Control**.

***Figura 13.8**. Ventana principal de configuración del firewall en Windows® 7*

Desde la ventana principal se debe seleccionar la opción **Configuración avanzada**. En la ventana que aparece se debe buscar en las reglas de entrada la opción **Archivos e impresoras compartidos** (**petición eco: ICMPv4 de entrada**).

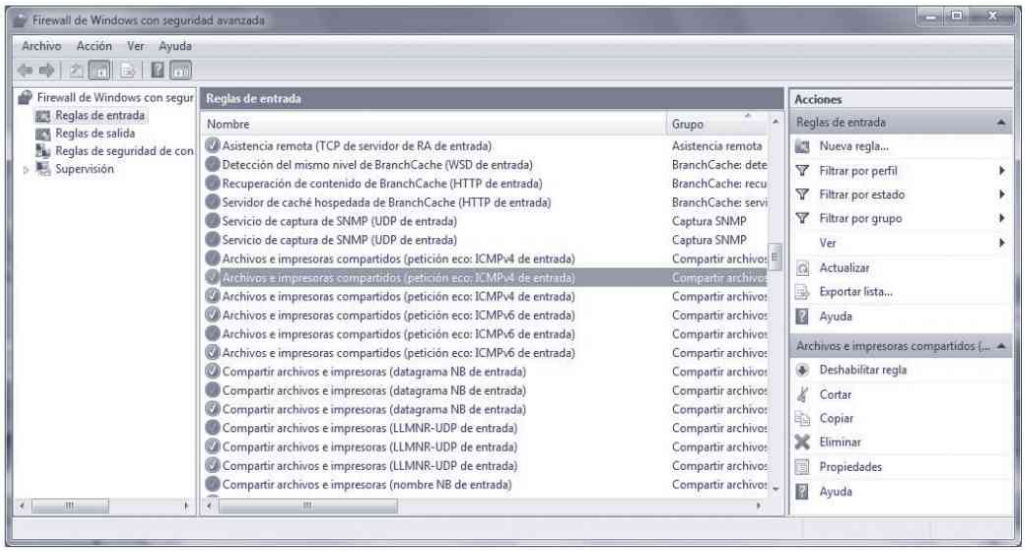


***Figura 13.9**. Ventana de configuración avanzada del firewall en Windows® 7*

Las distribuciones basadas en Linux normalmente suelen permitir la entrada de los mensajes ICMP *Echo* por defecto. Muchas de ellas utilizan un software llamado **iptables** para llevar a cabo las funciones de *firewall* en el equipo. Lo cierto es que *iptables* ofrece muchas posibilidades de configuración. Se ofrece un ejemplo sencillo suponiendo que no hay establecida ninguna regla de filtrado en *iptables*.

Se puede ver el estado del filtrado con *iptables* con el comando:

```
iptables -L
```

Si por alguna razón se desea bloquear los mensajes ICMP se pueden utilizar el siguiente comando:

```
iptables -A INPUT -p icmp -icmp-type echo-request -j DROP
```

Si se desea volver a habilitar la entrada de mensajes ICMP habría que borrar la regla anterior de *iptables* con el comando:

```
iptables -D INPUT número
```

El valor de *número* sería el orden de la regla dentro de la tabla INPUT. Por ejemplo, cuando solo exista esa regla de filtrado, para borrarla se utilizaría el comando:

```
iptables -D INPUT 1
```

13.7.2 VERIFICACIÓN DE LA CONECTIVIDAD LÓGICA

Se entiende por verificar la conectividad lógica de un equipo a comprobar que dicho equipo tiene correctamente configurados sus parámetros de red para acceder a otros equipos de la red o incluso a otros equipos fuera de la red.

Cuando un equipo no tiene conectividad a ningún elemento de la red la primera tarea es verificar la correcta configuración del mismo y para ello habrá que fijarse en los parámetros de red del equipo que, recordemos, son los siguientes:

- ✓ Dirección IP.
- ✓ Máscara de subred.
- ✓ Puerta de enlace.
- ✓ Servidores DNS.

Para asegurarnos que los parámetros establecidos en el equipo son los adecuados hay que tener información sobre la estructura lógica de la red. Además, habrá que tener en cuenta si en la red existe un servidor DHCP y el equipo está configurado para obtener los parámetros de red de forma automática.

- Para un equipo con los parámetros de red configurados manualmente:
  - **Para la red local**: asegurarse que están bien configuradas la dirección IP y la máscara de subred. Esta puede ser una fuente importante de problemas. Simplemente un número cambiado en alguno de los octetos que definen la dirección IP y el equipo no tendrá conexión.
  - **Para Internet**: así mismo, asegurarse que están correctamente configurados tanto la puerta de enlace como los servidores DNS. Una configuración incorrecta de alguno de estos dos parámetros ocasionaría que el equipo no se conecte a Internet, aunque sí tendría conexión a la red local.
- Para un equipo con los parámetros de red configurados automáticamente. En este caso, lo que habrá que comprobar es que exista un servidor DHCP en funcionamiento en la red. En alguna ocasión los equipos no consiguen comunicarse con el servidor DHCP y se quedan sin los parámetros de configuración de red. Generalmente cuando ocurre esto basta con reiniciar el equipo (o la interfaz de red) para que se soliciten de nuevo.

Cómo usar ping

En un entorno real, cuando un usuario de la red notifica que algún servicio de red no está funcionando, la primera comprobación que se suele hacer es verificar la conectividad del equipo en la red utilizando el comando *ping*. Para ello se ejecuta dicho comando especificando como destino la dirección IP de otro equipo de la red. Una práctica muy habitual es utilizar la dirección IP del *router* de salida de la red, que estará configurado como puerta de enlace (o *gateway*), pero se podría utilizar cualquier dirección IP que sepamos con certeza que está operativa en la red.

Si el comando *ping* no recibe respuesta tenemos un indicador de que el problema está en algún elemento del nivel físico o del nivel de enlace, como el latiguillo de red, la tarjeta de red, etc., o bien en la configuración de red del equipo.

Si el comando *ping* obtiene respuesta es que el equipo está funcionando correctamente dentro de la red y habrá que buscar el origen del problema en otra parte de la red o en los niveles superiores. Supongamos que tenemos un equipo en una red local con los siguientes parámetros de configuración de red:

- ✓ Dirección IP: 192.168.100.25
- ✓ Máscara de subred: 255.255.255.0
- ✓ Puerta de enlace: 192.168.100.254
- ✓ DNS1: 80.56.23.4
- ✓ DNS2: 80.45.12.2

Si dicho equipo presenta problemas de conectividad, por ejemplo, no funciona la conexión a Internet, las comprobaciones más típicas que se harán con el comando *ping* para estimar el ámbito del problema son:

Comprobación de la conectividad con algún equipo de la red que esté operativo.

```
ping 192.168.100.20
```

Comprobar la conectividad con la puerta de enlace:

```
ping 192.168.100.254
```

Comprobar la conectividad con los servidores DNS:

```
ping 80.56.23.4
```

Comprobar la conectividad con algún servidor web de Internet. Si los servidores DNS están correctamente configurados se puede utilizar un nombre en lugar de la dirección IP.

```
ping www.google.es
```

El resultado de estas comprobaciones nos dará información para determinar el ámbito del problema.

En los sistemas Linux, por defecto, el comando *ping* envía mensajes ICMP *Echo* indefinidamente hasta que interrumpamos la ejecución del comando con las teclas [**Ctrl**] + [**C**]. En los sistemas Windows®, sin embargo, el comando *ping*, por defecto, envía cuatro mensajes ICMP *Echo* y finaliza su ejecución. Para que envíe indefinidamente mensajes ICMP, como en Linux, hay que utilizar el modificador *–t*:
ping –t 10.20.30.40

13.7.3 VERIFICACIÓN DE LA CONECTIVIDAD FÍSICA

Después de verificar que los parámetros de red están correctamente configurados habrá comprobar los diferentes elementos físicos que permiten establecer la conexión en el equipo:

- **Cableado**. Si la red sigue las reglas del cableado estructurado, en enlace entre el equipo y el *switch* está dividido en varias partes.

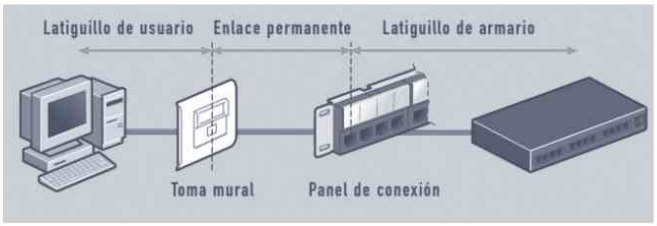


***Figura 13.10**. Tramos del cableado horizontal*

- **Latiguillo del área de trabajo**. Algún tirón fuerte al latiguillo del área de trabajo puede producir un mal funcionamiento del mismo. La comprobación más rápida es sustituir dicho latiguillo por uno de pruebas y comprobar si el problema de conectividad continúa.
- **Cableado horizontal**. Con un buen sistema de cableado estructurado esta es la parte donde es menos probable que esté el problema. Quizás la parte más susceptible en la que se puede producir algún problema es en la roseta, ya que al estar situada en el área de trabajo algún tirón al latiguillo o un golpe con algún objeto contundente podría llegar a dañarla.

  Para comprobar si el problema está en este tramo se puede utilizar un *tester* de red conectando uno de los módulos en la roseta y el otro módulo en el repartidor (*patch panel*).

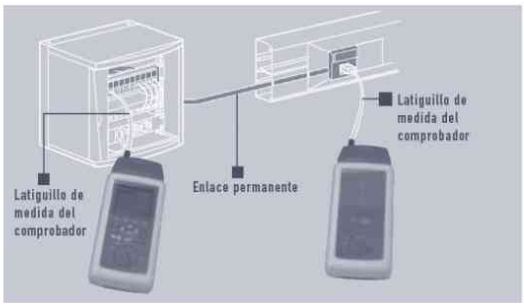


***Figura 13.11**. Verificación del cableado horizontal*

- **Cableado en repartidor**. Normalmente este cableado no suele presentar ningún problema aunque conviene asegurarse que las conexiones del repartidos al *switch* son las correctas.

- **Switch**. Puede ocurrir que el puerto del *switch* donde está conectado el equipo tenga algún problema. Para verificarlo se puede cambiar el puerto utilizado y comprobar si el problema persiste.
- **Controlador de la tarjeta de red**. En algunos casos, la instalación de alguna actualización del sistema operativo o algún otro componente software de bajo nivel puede ocasionar que el controlador de la tarjeta de red falle. En estos casos, lo único que se puede hacer es dirigirse a la página web del fabricante para obtener la versión más actualizada de dicho controlador. En muchas ocasiones la actualización del controlador puede solucionar los problemas con la tarjeta de red.
- **Tarjeta de red**. Esta es la última comprobación que se hace ya que es poco frecuente que se estropeen las tarjetas de red y su comprobación supone el cambio de la misma, lo que implica abrir el equipo y sustituir dicha tarjeta de red. Si la tarjeta de red está incluida en la placa base bastaría con instalar una nueva tarjeta de red en un *slot* libre y conectar el cable de red a la misma.

IMPORTANTE

Algunos indicadores visuales de que existe algún problema de conectividad física en un equipo son:

- **Luces indicadores de conexión**. Tanto en las tarjetas de red como el los puertos de los *switches* existe un indicador luminoso (normalmente de color verde) que nos indica que hay conectividad física.
- **Indicador software**. El propio sistema operativo puede indicar también la ausencia de conexión física con un icono en la barra de estado.

13.7.4 LA AVERÍA MÁS COMÚN: FALLO EN LA CONEXIÓN A INTERNET

Lo cierto es que en la actualidad uno de los usos más comunes de los equipos conectados en una red es el acceso a Internet, por ello, una de las frases más utilizadas por los usuarios ante algún fallo en la red es "*no me funciona Internet*", "*no tengo conexión a Internet*" y frases similares. Habitualmente se llega a esa conclusión porque el navegador web falla en el intento de acceder a alguna página web.

***Figura 13.12**. Mensajes de error en el navegador web*

Ante este síntoma la primera acción es determinar si el fallo en la conexión a Internet se produce solo en un equipo o en todos.

- **Fallo de conexión en todos los equipos de la red**. En este caso hay que determinar si el problema está dentro de la red LAN o fuera. Para ello basta comprobar la conectividad con la puerta de enlace (el *router* que proporciona acceso a Internet). Si no hay conectividad con la puerta de enlace posiblemente el problema esté en la red local. En este caso, habrá que comprobar tanto el *router* como el *switch* (o *switches* si hubiera varios). Si hay conectividad con la puerta de enlace se puede comprobar la conectividad con los servidores DNS o con algún servidor web externo ya que es posible que el problema esté ocasionado por el proveedor de servicios de Internet.
- **Fallo de conexión en un solo equipo**. Si el fallo de conexión se produce en un solo equipo habrá que seguir los pasos especificados en los anteriores apartados para la comprobación de la conectividad lógica y la conectividad física. En caso de que tanto la conectividad física como la lógica sean correctas, el problema habrá que buscarlo en los niveles superiores, es decir, comprobar el filtrado del *firewall* del equipo y comprobar la correcta configuración y funcionamiento del navegador web utilizado.

El supuesto presentado se refiere a redes en las que solo hay un *router*, que es el que proporciona conexión con Internet. En redes más complejas, con subredes y *routers* intermedios, el procedimiento de verificación dependerá de la estructura de la red.

13.8 MONITORIZACIÓN

Debido al uso cada vez más intensivo de las redes de datos, así como la continua evolución a las que son sometidas, tanto en el número y distribución de usuarios, como el tipo de servicios utilizados, la monitorización cobra cada vez mayor importancia y forma parte de las tareas de mantenimiento de las mismas. Esta función de supervisión también tiene una relación directa con la detección precoz de problemas de malfuncionamiento de alguno de sus componentes.

Los procedimientos y estrategias de monitorización están basados casi todos en componentes software. Existen herramientas de monitorización comerciales, algunas de ellas proporcionadas por fabricantes de dispositivos hardware de red y utilizadas para monitorizar sus equipos. En los próximos apartados, sin embargo, se expondrán algunas de las herramientas de monitorización de uso libre.

13.8.1 CAPTURADORES DE TRÁFICO

Los capturadores de tráfico se conocen también por su término en inglés, **sniffers** (husmeadores) y son herramientas software que se utilizan para capturar el tráfico que pasa por una interfaz de red del equipo donde está instalada dicha herramienta, con la finalidad de analizarlo posteriormente. Un capturador de tráfico de red será capaz de capturar todo el tráfico que pase por la interfaz de red seleccionada, tanto entrante como saliente.

Hay que tener en cuenta que por la naturaleza de las redes locales actuales, un *host* recibirá por su interfaz de red solo el tráfico dirigido a él, o el tráfico de *broadcast*. Por lo tanto, desde un equipo conectado en la red solo se puede monitorizar dicho tráfico. Sin embargo, hay ocasiones en las que interesa capturar el tráfico de otros equipos de la red o incluso de un segmento de red completo. Para ello, la solución más común es utilizar un *switch* que permita la configuración de un puerto de monitorización (*port mirroring*).

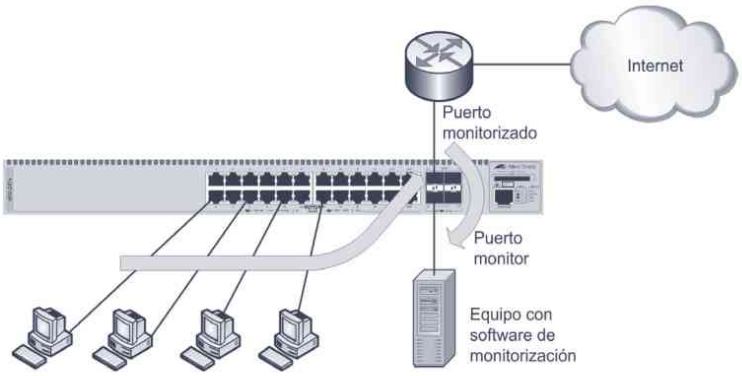


***Figura 13.13**. Monitorización mediante un switch que admite un Monitor Port*

En la figura anterior se utiliza un *switch* configurable que admite la monitorización de puertos. En este caso se desea monitorizar el tráfico dirigido hacia el *router* que conecta la red con Internet. El puerto donde está conectado el *router* se configura como puerto monitorizado y el puerto donde se conecta el equipo que va a llevar a cabo la función de monitorización se configura como puerto monitor. Por lo tanto, todo el tráfico que se dirija al *router* también será redirigido al equipo de monitorización.

Si no se dispone de un *switch* que permita la configuración de puertos monitor se puede utilizar la configuración que aparece en la siguiente figura.

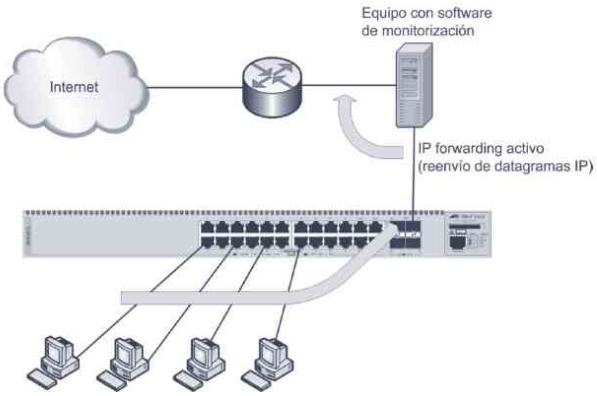


***Figura 13.14**. Monitorización con switch sin Monitor Port*

En este caso, el equipo de monitorización se ubica entre el *switch* y el *router*, para que pase por él todo el tráfico dirigido al *router*. Como se observa, este equipo debe tener dos interfaces de red para conectarse al *switch* y al *router*, y tener activada la opción de **reenvío de tráfico IP** (conocido como *IP forwarding*). Por otra parte, se requiere hacer los cambios adecuados en la configuración de las direcciones IP tanto del equipo monitor como del *router*.

En cuanto a las herramientas para la captura de tráfico de red, sin duda la más popular es la aplicación **Wireshark**. Esta aplicación multiplataforma se distribuye bajo licencia GPL de libre distribución y permite capturar y almacenar el tráfico que se envía y recibe en alguna de las interfaces de red del equipo donde esté instalado. *Wireshark* no solo permite capturar tráfico, sino que además ofrece funcionalidades muy avanzadas para el análisis de dicho tráfico, por tanto, *Wireshark* se utiliza tanto para labores de monitorización como de detección y análisis de problemas en la red.

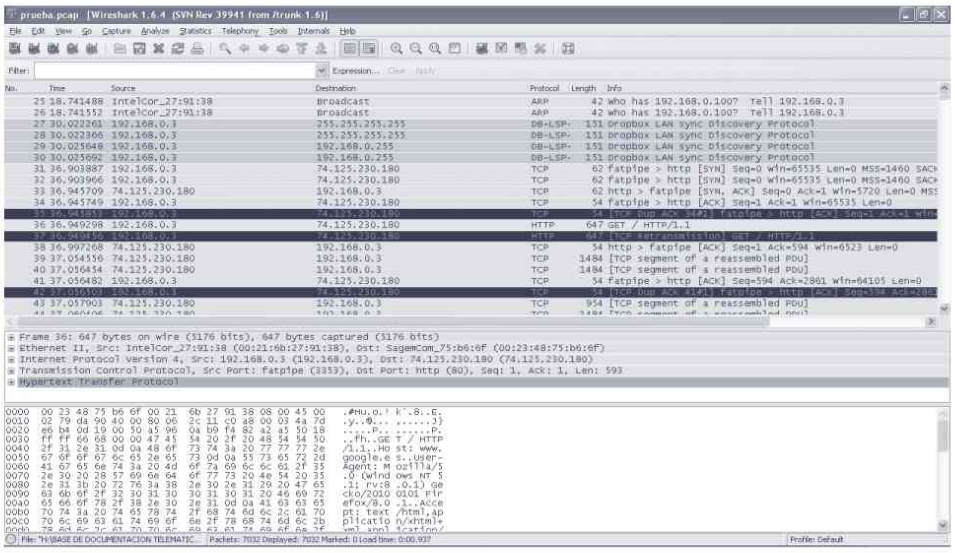


***Figura 13.15**. Aplicación Wireshark para capturar tramas*

RECUERDA

Si ejecuta cualquier aplicación de captura de tráfico en un equipo de la red donde se utilicen *switches* (la gran mayoría en la actualidad) solo capturará el tráfico dirigido o enviado desde este equipo y el tráfico de *broadcast*.
Para capturar tráfico de otros equipos lo más común es utilizar un *switch* que soporte monitorización de puertos.

13.8.2 ESCANEADORES DE PUERTOS

Los programas conocidos como escaneadores de puertos se utilizan para monitorizar el uso de los puertos en los dispositivos de la red. Habitualmente el uso inadecuado de puertos está asociado a algún problema relacionado con virus o *malware* en general, por ello, muchos administradores de red escanean los puertos de los dispositivos de la red en busca de indicios de la existencia de este tipo de software.

Uno de los programas de escaneo de puertos más conocido, muy ligado a entornos Unix es **nmap**. Este software permite multiples posibilidades de escaneo y requiere de ciertos conocimientos técnicos. Puede ser utilizado desde cualquier equipo de la red, ya que el programa permite especificar el rango de direcciones IP para el que se desea llevar a cabo el escaneo.

Existe una versión de *nmap* para sistemas Windows® que utiliza una interfaz gráfica y permite un uso más sencillo.

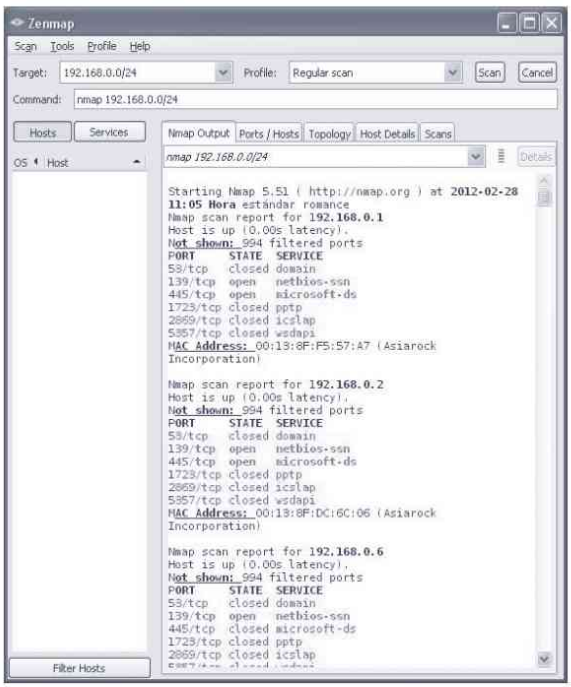


***Figura 13.16**. Interfaz gráfica en Windows® para la aplicación nmap*

13.8.3 SUPERVISIÓN DEL TRÁFICO DE RED: NTOP

Otra de las herramientas que se pueden utilizar para la monitorización de redes locales es **ntop**. Esta aplicación se utiliza especialmente en entornos Unix y se distribuye bajo licencia GPL. Su instalación y uso en sistemas Linux es muy sencillo. El programa *ntop* utiliza una interfaz web para visualizar la información de monitorización por lo que en el equipo donde se utilice *ntop* se deberá tener instalado un servidor web, típicamente *apache*.

Al igual que los programas de captura de tráfico, la ubicación del equipo donde se instale *ntop* es fundamental para obtener la información adecuada. Si se instala *ntop* en un equipo de la red solo se verá información sobre el tráfico de ese equipo. Por lo tanto, los escenarios de ejecución de *ntop* son similares a los mostrados en el apartado 13.8.1.

Por ejemplo para equipos con alguna distribución Debian, Ubuntu o derivadas se puede instalar con el comando:

```
sudo apt-get install ntop
```

El proceso de instalación nos pedirá la contraseña de administración. Para parar y arrancar el servicio se utilizan los comandos:

```
sudo /etc/init.d/ntop stop
sudo /etc/init.d/ntop start
```

Con *ntop* funcionando en el equipo, este recogerá datos del uso de la interfaz de red especificada. Con un servidor web instalado y funcionando, para visualizar la información que proporciona *ntop* se debe especificar como URL en un navegador web el nombre **localhost**, que es el nombre del propio equipo, y el puerto 3000, que es el que utiliza *ntop*. Dicho nombre se traduce siempre por la dirección IP de bucle local, 127.0.0.1. Se puede acceder de forma remota simplemente utilizado en la URL la dirección IP del equipo donde está instalado *ntop* en lugar de utilizar *localhost*.

***Figura 13.17**. Acceso a la información de ntop mediante navegador web*

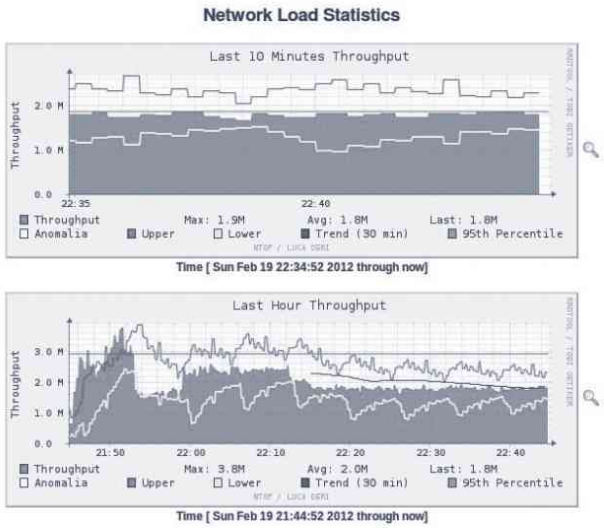


***Figura 13.18**. Gráficos generados por la aplicación ntop*

Para cambiar la interfaz de red que se desea monitorizar se debe editar el archivo */var/lib/ntop/init.cfg* y modificar la línea donde esté especificada la interfaz original, por defecto *eth0*. Se puede utilizar el editor *gedit* para editar el archivo. Después de guardar los cambios hay que reiniciar el servicio *ntop*:

```
sudo gedit /var/lib/ntop/init.cfg
sudo /etc/init.d/ntop restart
```

La aplicación *ntop* utiliza licencia GNU GPL por lo que el código fuente está disponible para su compilación en cualquier plataforma. Sin embargo, la versión binaria ya compilada para sistemas Windows® se ofrece con una limitación en el número de paquetes monitorizados.

13.8.4 PROTOCOLO SNMP

El **protocolo SNMP** forma parte de los protocolos del nivel de aplicación de la arquitectura TCP/IP (fue descrito en el Capítulo 10) y sigue el modelo cliente-servidor para proporcionar funciones de monitorización de red. Este protocolo se utiliza para supervisar dispositivos de red como *switches* o *routers*, aunque también se puede utilizar para monitorizar servidores o equipos de escritorio. La información que se puede monitorizar son parámetros estandarizados para todos los fabricantes que implementen este protocolo en sus productos, por lo que permite monitorizar redes formadas por equipos de diferentes fabricantes.

Para llevar cabo su funcionamiento en el protocolo SNMP existen dos entidades: los **NMS** (*Network Management Station*) son los equipos utilizados para llevar a cabo la supervisión, y los **Agentes**, que son el componente software instalado en los equipos que se desea monitorizar y son los que proporcionan la información a los NMS. Para su funcionamiento, tanto el agente como el NMS utilizan una estructura de datos normalizada conocida como **MIB** (*Management Information Base*) y un pequeño conjunto de comandos para intercambiar la información. Dicho intercambio de información se lleva a cabo utilizando el protocolo UDP en el nivel de transporte mediante los puertos 161 y 162.

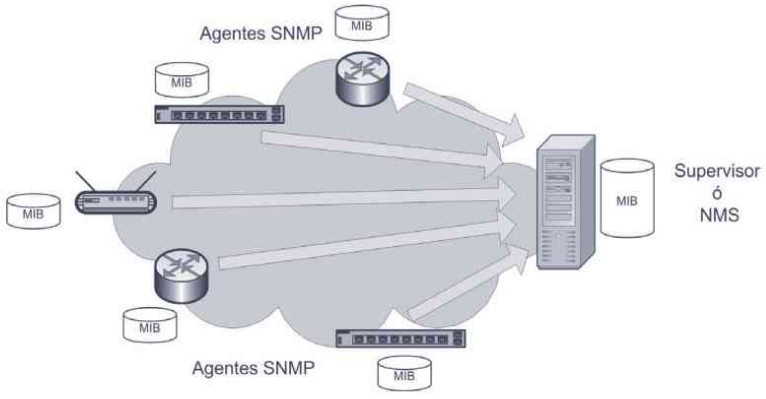


***Figura 13.19**. Arquitectura de monitorización con un sistema SNMP*

La mayor parte de los dispositivos de red como *switches* configurables, *routers* y puntos de acceso inalámbrico incluyen en sus características la activación de la función de agente SNMP.

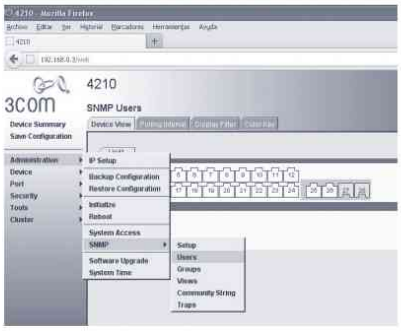


***Figura 13.20**. Configuración SNMP en un switch*

Para habilitar la función de Agente SNMP en un equipo con Linux se utiliza la aplicación **snmpd** disponible en los repositorios de la mayor parte de las distribuciones.

El equipo utilizado en la red como supervisor o NMS requiere la instalación del software específico de monitorización mediante SNMP. Existen en el mercado múltiples aplicaciones que cumplen esta función, algunas de ellas son de libre distribución.

***Figura 13.21**. Herramienta de monitorización SNMP*

Los datos proporcionados por los agentes SNMP pueden ser utilizados por herramientas de monitorización. Un ejemplo de ello es la aplicación **MRTG** (*Multi Router Traffic Grapher*) que se utiliza para supervisar la carga de tráfico de interfaces de red. La diferencia de *MRTG* respecto a *ntop* es que con *ntop* se puede supervisar la carga de cualquier interface de red de la máquina donde está instalado *ntop*. Sin embargo, con MRTG se puede supervisar la carga de cualquier interfaz de red de la red siempre que tenga un agente SNMP proporcionando la información.

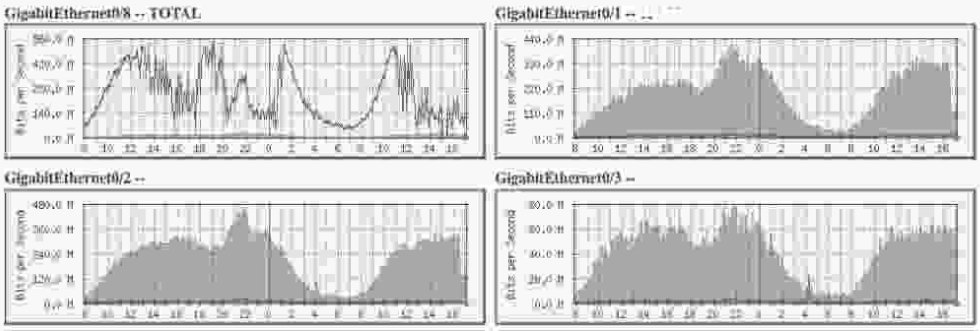


Figura 13.22. *Gráficos de tráfico de red generados por la herramienta MRTG*

Otros protocolos de monitorización:

- **RMON** (*Remote Network Monitoring*). Protocolo desarrollado por el IETF para monitorizar redes LAN. Utiliza como base el protocolo SNMP pero añadiendo más características a través de una MIB propia. Hay varias versiones: RMON1, RMON2 y SMON.
- **NetFlow**. Protocolo desarrollado por Cisco para recolectar datos sobre el tráfico de una red. Sigue el diseño cliente-servidor de SNMP. En este caso existen las llamadas *sondas Netflow* que son los dispositivos monitorizados que generan información que recogen los llamados *recolectores NetFlow*.
- **sFlow**. Protocolo para la recolección de datos de supervisión de la red. Este protocolo es altamente escalable, ya que permite la monitorización de cientos e incluso miles de puertos por lo que es muy usado en redes con gran volumen de tráfico a monitorizar.

13.8.5 SUPERVISIÓN DE REDES INALÁMBRICAS

Tanto para el mantenimiento como para la implantación de redes inalámbricas, cada vez es más necesario el uso de herramientas que proporcionen información de las redes inalámbricas en funcionamiento en nuestra área de cobertura. También son útiles estas herramientas para la puesta en servicio de redes inalámbricas en modo infraestructura que utilicen más de un punto de acceso.

Recordar que las redes inalámbricas que utilizan la banda de 2,4 GHz necesitan una separación de 5 canales para que no se produzcan interferencias. La tecnología Wi-Fi está preparada para trabajar con interferencias, es decir, con otras transmisiones en esa misma banda. Sin embargo, el uso simultáneo de bandas solapadas produce un descenso del rendimiento de la transmisión. Por ello, el principal uso de las herramientas de supervisión de redes inalámbricas es la supervisión de las bandas de frecuencia activas en nuestra zona de cobertura para poder buscar el canal "más limpio". Otro parámetro que deberá tenerse en cuenta es la potencia con la que llega la señal, ya que una señal con una potencia muy baja apenas producirá interferencias.

Respecto a la potencia, las unidades más utilizadas son los dBm. Los puntos de acceso suelen emitir en un rango en torno a los -20 dBm. La potencia óptima de recepción estará entre 40 y 70 dBm y la sensibilidad de los receptores suele estar entre -80 y -90 dBm. De forma que señales que estén en este último rango se pueden considerar señales débiles, por lo que apenas tendrán influencia en una zona de cobertura con señales Wi-Fi más altas.

Para disponer de toda esta información existen varias aplicaciones. Una de las más interesantes para entornos Windows® es **inSSIDer** cuyo aspecto se puede observar en la figura siguiente. Para poder instalar esta herramienta es necesario tener instalado en el equipo el componente de desarrollo conocido como *Microsoft .NET Framework 2.0*.

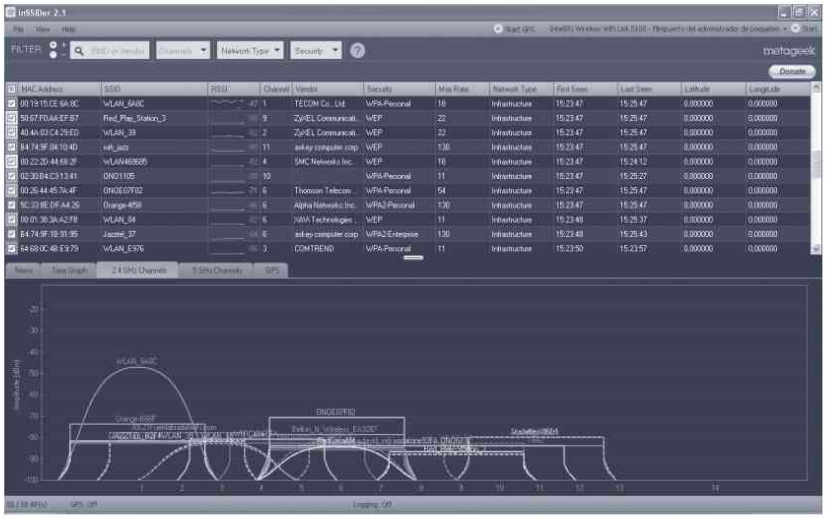


***Figura 13.23**. Aplicación inSSIDer*

Otra de las aplicaciones de supervisión de redes Wi-Fi de libre distribución más populares es **Netstumbler**, pero lo cierto es que el proyecto que mantiene dicha aplicación lleva varios años parado.

Gracias a la proliferación de dispositivos móviles, como *smartphones* con conectividad Wi-Fi, existen también en el mercado herramientas de supervisión de redes inalámbricas que se ejecutan en dichos dispositivos. En la siguiente figura se puede observar la aplicación **Wifi Analyzer** disponible para sistemas *Android*. Gracias a la movilidad que permiten estos dispositivos, estas herramientas nos permiten establecer las áreas de cobertura de los puntos de acceso de una red en infraestructura de forma sencilla.

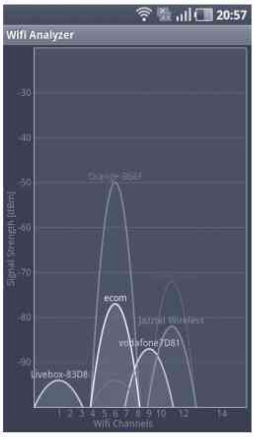


***Figura 13.24**. Aplicación Wifi Analylez para dispositivos con Android*

RESUMEN DEL CAPÍTULO

En este capítulo se presentan dos actividades relacionadas con las redes locales. La primera es la puesta en servicio de las redes, es decir, se establecen los criterios generales para la implementación de una red local como pueden ser el dimensionamiento, el etiquetado, condiciones técnicas de los materiales y el equipamiento.

En la segunda parte se proporciona información sobre el diagnóstico y localización de averías en las redes locales, utilizando herramientas básicas como el comando *ping*. Además, se proporcionan pautas para la localización de las averías, diferenciando en los ámbitos de conectividad física y lógica.

Por último, se incluyen algunas herramientas para llevar a cabo la monitorización de las redes locales como pueden ser capturadores de tráfico, escaneadores de puertos, herramientas de supervisión del tráfico de red y el uso del protocolo SNMP para la monitorización de dispositivos de red.

EJERCICIOS PROPUESTOS

- **1.** Comprobar la existencia de los elementos del subsistema horizontal del aula como, por ejemplo, las rosetas, canaletas, el etiquetado de los diferentes elementos, etc. Elaborar un pequeño documento con toda la información obtenida.
- **2.** Activar el filtrado de mensajes ICMP de tipo Eco en un equipo y comprobar que dicho equipo no responde al comando *ping*.
- **3.** Instalar la aplicación Wireshark en un equipo y comprobar sus principales características.
- **4.** Otra aplicación de libre distribución que se puede utilizar para la monitorización del tráfico es NetworkMiner. Instalarla y estudiar sus funcionalidades, comparando sus características con las de Wireshark.
- **5.** Si se dispone de un equipo con conexión inalámbrica, instalar la aplicación InSSIDer y comprobar sus principales características.

TEST DE CONOCIMIENTOS

1 En la documentación de la puesta en servicio de una red local se debe incluir:
- a) Memoria técnica del proyecto.
- b) Presupuestos.
- c) Planos.
- d) Todos los anteriores.

2 En el cableado horizontal, la distancia máxima que puede existir entre la roseta de usuario y el conector ubicado en el armario de distribución de planta es de:
- a) 200 metros.
- b) 100 metros.
- c) 90 metros.
- d) 50 metros.

3 Los armarios de comunicaciones habitualmente son del tipo:
- a) Rack de 19".
- b) Rack de 25".
- c) Rack de 29".
- d) Rack de 10".

4 Si aparece un mensaje de error de conexión en el navegador web, una posible causa podría ser:
- a) Los puertos cerrados en el equipo.
- b) El *firewall* de red.
- c) Un problema con los servidores DNS.
- d) Un problema de versión del navegador.

5 El comando *ping* se utiliza para:
- a) Comprobar los parámetros de configuración de red.
- b) Comprobar si funciona el servicio DNS.
- c) Comprobar si funciona el servicio web.
- d) Comprobar si existe conectividad lógica con otro equipo.

6 El funcionamiento del comando *ping* está basado en el uso de mensajes:
- a) ARP.
- b) ICMP.
- c) TCP.
- d) UDP.

7 En caso de fallo de conectividad la posible fuente del problema puede estar en:
- a) La roseta.
- b) El latiguillo del área de trabajo.
- c) El puerto del *switch*.
- d) Todas las respuestas anteriores son correctas.

8 La característica de Monitor Port presente en algunos *switches* se utiliza para:
- a) Abrir y cerrar puertos en la red.
- b) Gestionar el volumen de tráfico de los puertos.
- c) Monitorizar tráfico.
- d) Ninguna respuesta anterior es correcta.

9 Uno de los programas más utilizados para la captura y análisis de tramas es:
- a) *Ntop*.
- b) MRTG.
- c) *Wireshark*.
- d) *Nmap*.

10 Para utilizar el protocolo SNMP en monitorización de una red:
- a) Debe existir un solo equipo configurado como Agente SNMP.
- b) Cada equipo a ser monitorizado debe tener un Agente SNMP.
- c) Debe haber instalado un Agente SNMP en el *router* principal.
- d) Debe instalarse un servidor web.

Índice Alfabético

Símbolos

10BASE-T, 232
10-Gigabit Ethernet, 240
100BASE-FX, 235
100BASE-T4, 236
100BASE-TX, 235
1000BASE-T, 238
1000BASE-X, 239

A

Administrador, 124
AES, 313
Agente SNMP, 393
AGP, 37, 104
Alan Turing, 156
Alicates, 80
Almacenamiento y reenvío, 251
Android, 118
Antialiasing, 37
Aplicación portable, 163
Armario de comunicaciones, 377
ARP, 275
Arquitectura cliente-servidor, 132, 160
Arquitectura de tres niveles, 160
Arquitectura monolítica, 160
ATX, 22, 25, 49, 88
Auto MDI/MDI-X, 242, 248
Averías, 326
AWG, 195

B

B2G, 120
Backup, 332, 356
Bada, 120
Barebone, 23
Batería, 28, 333, 341
Benchmark, 339, 363
BIOS, 122, 136
BlackBerry OS, 118
Boot Manager, 136
BoottoGecko, 120
Brazos, 41
Brida, 80
BSS, 304
BSSID, 308
Buffer, 250
Bus, 20

C

Cabecera, 179
Cabezas, 41
Cableado de campus, 377
Cableado estructurado, 208
Cableado horizontal, 210, 211, 376
Cableado vertical, 210, 377
Cable coaxial, 194, 201
Cable de par trenzado, 190
Cable STP, 193, 201
Cable UTP, 191, 201, 241
Cable UTP cruzado, 242
Caché, 43
Caché L1, 29
Caché L2, 27, 29
Caja, 337
Capturador de tráfico de red, 389
Categorías de cableado, 192
Certificadores de cableado, 215
Charles Babbage, 156
Chasis, 21, 107
Chipset, 27, 33
Ciclo de vida del software, 157
Cifrado, 181
Cinta, 39
Circuito impreso, 26

Clases IP, 265
Cleaners, 166
Clonación, 348, 350
Codificación, 202
Codificación Manchester, 203
Codificación NRZ-I, 203
Colisión, 231
Compresión, 181
Conector ATX, 88
Conector BNC, 194
Conectores SATA, 48
Conectores USB, 107
Conector RJ-45, 191
Conector SC, 199
Conector ST, 198
Conexión a tierra, 193
Conexión multipunto, 204
Conexión punto a punto, 204
Configuración, 165
Controlador, 28, 227
Control de acceso al medio, 183
Control de errores, 181, 183
Control de flujo, 181, 183
Copias de seguridad, 356, 358
Copyleft, 67
Core, 28
Corrosión, 331
CPU, 364
CRC, 232
Crimpadora, 214
CSMA/CA, 311
CSMA/CD, 231

D

Datagrama, 263
DDR, 31
DDR2, 31
DDR3, 31, 32
Desinstalación, 165
Desinstalador, 165
DHCP, 282
DIMM, 27, 31
Direccionamiento, 181
Direccionamiento físico, 183, 227
Direccionamiento IP, 265
Direccionamiento lógico, 182
Dirección de broadcast, 228, 268
Dirección MAC, 228
Disco, 96
Disco duro, 39, 40, 78, 345
Disco flexible, 39
Disipador, 81, 92
DNS, 283
Documentación, 17
Dual Fan, 48
Dual memory, channel, 31

E

EATX, 22
Energía electrostática, 332
Energía estática, 76
Energía eléctrica, 76
Energy Star, 23
Enrutamiento, 182
Entorno operativo, 60
Entornos ide, 70
Escaneador de puertos, 391
Espectro electromagnético, 200
ESS, 305
ESSID, 308
Estanqueidad, 77
Ethernet, 220
Expresscard, 37

F

Fallos comunes, 337
Fast Ethernet, 235
Fibra monomodo, 197
Fibra multimodo, 197
Fibra óptica, 195, 201
Firewall, 287
Frecuencia de reloj, 29
Freeware, 65
Front Side Bus (FSB), 29
FTP, 293
Fuente de alimentación, 48, 77, 87, 337

G

G4L, 349, 353
GBIC, 249
GDDR, 32
Gestionar grupos y usuarios, 147
Gestor de arranque, 124
Gestor de paquetes, 162
Gigabit Ethernet, 238
Gigaherzio (GHz), 29
Gparted, 349
GPL, 66
GPU, 37
GRUB, 60, 137
Grupos de usuarios, 146
GSmartControl, 349

H

Hardinfo, 349
Hardware, 17
Heatpipes, 29
Herramienta de impacto, 214
Herramientas, 79
Herzio (Hz), 29
Hipertransport, 29
HTTP, 291
Hub, 234, 243
Hub Link., 27
Humedad, 331

I

ICMP, 275
IEEE 802.3, 221
IEEE 802.11, 302
Impactos, 332
Ingeniería del Software, 157
Instalación de software, 160
Instalador, 161
Inteligencia artificial, 72
Interfaz, 114
Interfaz del disco duro, 41
Interfaz SATA, 42
Internet, 171
Intervalo de bit, 202
Intranet, 172
IP, 262
iPhone OS, 118
IPv6, 294
ISM, 302
ISP, 175

J

Jumper, 96, 103

K

Kernel, 137
KiloHerzio (KHz), 29

L

LAN, 174, 220
Latiguillo de red, 211, 223, 254
Led, 337
LGPL, 67
Licencia bsd, 67
Licencia de software, 65
LILO, 137
Linus Torvalds, 116
Linux, 116
Livecd, 116
LPC, 27

M

MAC, 55
Mac OS, 117
Mainboard, 25
Mainframes, 132
MAN, 176
Mantenimiento, 326
Mantenimiento adaptativo, 327
Mantenimiento correctivo, 327
Mantenimiento de emergencia, 327
Mantenimiento perfectivo, 327
Mantenimiento preventivo, 327, 332
Master, 97
Medios guiados, 170, 190
Medios no guiados, 190
Megahertzio (MHz), 29
Memoria, 78, 338, 344
Memoria auxiliar o secundaria, 20

Memoria caché, 29
Memoria de video, 32
Memoria principal, 19
MIB, 393
Micro-ATX, 22
Micro-DIMM., 32
Microondas, 200
Microprocesador, 28, 77, 338
MIMO, 303
Mini-ATX, 25
Mini-GBIC, 249
Modelo OSI, 179
Modo Ad-hoc, 304
Modo Bridge, 307
Modo infraestructura, 304
Modos de transmisión, 184, 204
Molex, 102
Monitorización, 333
Montaje, 86
Motherboard, 25
Mount-gtk, 349
Mozilla, 120
Máscara de subred, 269
MTU, 263
Módem, 55
Módulo de memoria, 31
Módulos de RAM, 94
Multímetro, 82
Multitarea, 114
Multiusuario, 114

N

Nano-ITX, 25
Nanómetro, 30
NAT, 273
NetFlow, 395
NIC, 106, 226
Nivel de aplicación, 180
Nivel de enlace, 182
Nivel de presentación, 180
Nivel de red, 182
Nivel de sesión, 181
Nivel de transporte, 181
Niveles homónimos, 179
Nivel físico, 184
NMS, 393
NorthBridge, 27, 33
NTLDR, 137

O

Oblea, 30
OCR, 70
Ondas de radio, 200
Ondas infrarrojas, 200
Oracle, 118
OUI, 228
Overclocker, 24
Overclocking, 30

P

P2P, 71, 135
Palm OS, 117
Panel del sistema, 107
Pantalla, 345
Paquete integrado o suite, 64
Parted Magic, 348
Particionamiento, 123
Particiones, 44, 350
Partición activa, 45
Partition Image, 349, 351
Pasta térmica, 81
PATA, 96, 103
Patch Panel, 212
PCB, 26
PCI, 35, 37, 104
PCI Express, 27, 35, 37, 104
PCMCIA, 37
Peer-to-peer, 135
Periféricos, 53
Permisos, 149
PFC, 48
Pico-ITX, 22, 25
Pila de protocolos, 179
Placa base, 78, 86, 338, 345
Placas peltier, 24
Plan de puesta en servicio, 362
Platos, 41
Plugin, 125

Polímetro, 80, 82
Polvo, 331
POP3, 292
Portátil, 84, 341
Power Over Ethernet, 252
Programa, 20
Protocolo, 179
Protocolo IPv6, 262
Puente, 243
Puente inalámbrico, 317
PuenteNorte, 27, 33
PuenteSur, 27, 33
Puertos USB, 337
Punto de acceso inalámbrico, 304
Punto de demarcación, 210
Punto de memoria, 19
Puntos de acceso inalámbrico, 316

R

RAM, 31, 94
Red de datos, 170
Red de área extensa, 175
Red de área local, 174
Redes de área metropolitana, 176
Reenvío directo, 250
Refrigeración líquida, 24, 77
Refrigeración por aire, 24
Repositorios, 162
Restauración, 357
Richard Stallman, 116
RIMM, 31
RMON, 395
Root, 146
Root servers, 283
Roseta, 212, 223
Router, 55, 272
rpm, 163

S

Sbackup, 359
Sector de arranque, 45
Sector translation, 41
Secuencia de arranque, 121, 136
Servicio, 138
Servicios de red, 180
Servicio web, 291
sFlow, 395
SFP, 249
Shareware, 65
SIMM, 27, 31
Single fan, 48
Single memory channel, 31
Sistema, 16
Sistema de comunicación, 16
Sistema informático, 16
Slave, 97
SMTP, 292
Sniffer, 389
SNMP, 293, 393
Socket, 26
Socket LGA, 26
Socket PGA, 26
Socket ZIF, 26
SO-DIMM, 32
Software, 17, 156, 332
Software de aplicación, 158
Software de programación, 158
Software de sistema, 158
Software de tiempo real, 72
Software empotrado, 72
Software libre, 65
Solid State Drive, 46
SouthBridge, 27, 33, 34
Spanning tree, 251
Speaker, 107
SSD, 46
SSH, 293
SSID, 308
Subnetting, 275
Subnivel LLC, 222
Subredes, 269
Switch, 55, 225, 236, 244
Symbian, 118

T

TAR, 358
Tarjeta de expansión USB, 105
Tarjeta de red, 224, 226

Tarjeta de vídeo, 104
Tarjeta gráfica, 37
Tarjetas de expansión, 37, 338
Tasa de bits, 202
TCP, 278
TCP/IP, 185
Teclado, 342
Tecnología flash, 36
Tecnología magnética, 36
Tecnología magneto-óptica, 36
Tecnología óptica, 36
Teléfono ip, 55
Telnet, 293
Temperatura, 329, 334
Tensiones, 51
Téster de red, 214
TFT, 346
TKIP, 312
TLD, 283
Toma de tierra, 76
Tomas de usuario, 376
Topología, 184
Topologías de red, 205
Trama Ethernet II, 230
Trama IEEE 802.3, 229
Transformador, 84, 341

U

UCP, 18
UDP, 277
UML, 159
Unidad aritmético-lógica, 19
Unidad de control, 19
Unidad de entrada-salida, 20
Unidad óptica, 103 344
URL, 291

V

Velocidad de acceso, 31
Velocidad de reloj, 31
Velocidad de rotación, 42
Velocidad de transmisión, 202
Ventiladores, 337
Vibraciones, 332
Virtualización, 151
VLAN, 251
Voltaje, 31
Voltios, 76
Von Neumann, 17, 18, 19

W

WAN, 175
Watercooling, 24
WDS, 306
Webmin, 143
WEP, 312
Wi-Fi, 302 347
Wi-Fi Alliance, 302
Windows, 115
Windows® Mobile, 117
WLAN, 302
WPA, 312
WPA2, 313

X

XArchiver, 349

Z

Zócalo, 90

La presente obra está dirigida a los estudiantes del Ciclo Formativo **Sistemas de Telecomunicación e Informáticos**, en concreto para el módulo profesional **Sistemas Informáticos y Redes Locales**.

Los contenidos incluidos en este libro abarcan conceptos como los equipos informáticos de telecomunicaciones, su configuración, la integración con redes de datos, haciendo hincapié en las redes inalámbricas, su puesta en servicio y mantenimiento, tanto del sistema informático como de las redes locales, etc.

Los capítulos incluyen actividades y ejemplos con el propósito de facilitar la asimilación de los conocimientos tratados.

Así mismo, se incorporan test de conocimientos y ejercicios propuestos con la finalidad de comprobar que los objetivos de cada capítulo se han asimilado correctamente.

Además, reúne los recursos necesarios para incrementar la didáctica del libro, tales como un glosario con los términos informáticos, bibliografía y documentos para ampliación de los conocimientos.

En la página web de **Ra-Ma** (**www.ra-ma.es**) se encuentra disponible el material de apoyo y complementario.