



UNIVERSIDAD DE GUADALAJARA
Sistema de Universidad Virtual

Los usuarios podrán en cualquier momento, obtener una reproducción para uso personal, ya sea cargando a su computadora o de manera impresa, este material bibliográfico proporcionado por UDG Virtual, siempre y cuando sea para fines educativos y de investigación. No se permite la reproducción y distribución para la comercialización directa e indirecta del mismo.

Este material se considera un producto intelectual a favor de su autor; por tanto, la titularidad de sus derechos se encuentra protegida por la Ley Federal de Derechos de Autor. La violación a dichos derechos constituye un delito que será responsabilidad del usuario.

Referencia bibliográfica

Huidobro, José; Blanco, Antonio; Calero, Jordán. (2006). Arquitecturas de comunicaciones. En *Administración de sistemas informáticos. Redes de Área Local* (2^a ed). España: Thompson Editores. Pp. 69-100.



www.udgvirtual.udg.mx

Av. De la Paz 2453, Col. Arcos Sur, Guadalajara, Jal., México. C.P. 44140
Larga distancia nacional (01-33), internacional (+52-33)
3134-2208 / 3134-2222 / 3134-2200 / Ext. 8801

Av. Juárez 976 Edif. Cultural y Administrativo Piso 5, Col. Centro, Guadalajara, Jal., México. C.P. 44100. Larga distancia nacional (01-33), internacional (+52-33)
3134-2208 / 3134-2222 / 3134-2200 / Ext. 8802

ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS

Redes de Área Local

2^a EDICIÓN

José M. Huidobro Moya
Antonio Blanco Solsona
J. Jordán Calero

ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS

Redes de Área Local

**José M. Huidobro Moya
Antonio Blanco Solsona
J. Jordán Calero**

2^a EDICIÓN

THOMSON
★
PARANINFO



Redes de área local

© José Manuel Huidobro, Antonio Blanco y Julia Jordán

Gerente Editorial Área Técnico-Vocacional:
M^a José López Raso

Editoras de Producción:
Clara M^a de la Fuente Rojo
Consuelo García Asensio
Olga M^a Vicente Crespo

COPYRIGHT © 2006 International Thomson Editores Spain
Paraninfo, S.A.
Magallanes, 25; 28015 Madrid
ESPAÑA
Teléfono: 91 4463350
Fax: 91 4456218
clientes@paraninfo.es
www.paraninfo.es

Impreso en España
Printed in Spain

ISBN: 84-9732-489-7
Depósito Legal: M-52.386-2005

(012/77/68)

Reservados los derechos para todos los países de lengua española. De conformidad con lo dispuesto en el artículo 270 del Código Penal vigente, podrán ser castigados con penas de multa y privación de libertad quienes reprodujeren o plagiaren, en todo o en parte, una obra literaria, artística o científica fijada en cualquier tipo de soporte sin la preceptiva autorización. Ninguna parte de esta publicación, incluido el diseño de la cubierta, puede ser reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sea éste electrónico, químico, mecánico, electro-óptico, grabación, fotocopia o cualquier otro, sin la previa autorización escrita por parte de la Editorial.

Diseño de cubierta:



Preimpresión:



Impresión:

Clossas Orcoyen, S.L.
Polígono Igarsa
nave 21, 22, 23 y 24
Paracuellos de Jarama
(Madrid)

Méjico y Centroamérica
Tel. (525) 281-29-06
Fax (525) 281-26-56
clientes@mail.internet.com.mx
clientes@thomsonlearning.com.mx
Méjico, D.F.

Puerto Rico
Tel. (787) 758-75-80 y 81
Fax (787) 758-75-73
thomson@coqui.net
Hato Rey

Chile
Tel. (562) 531-26-47
Fax (562) 524-46-88
devoregr@netexpress.cl
Santiago

Costa Rica
EDISA
Tel./Fax (506) 235-89-55
edisacr@sol.racsa.co.cr
San José

Colombia
Tel. (571) 340-94-70
Fax (571) 340-94-75
clithomson@andinet.com
Bogotá

Cono Sur
Pasaje Santa Rosa, 5141
C.P. 141 - Ciudad de Buenos Aires
Tel. 4833-3883 / 4831-0764
thomson@thomsonlearning.com.ar
Buenos aires (Argentina)

República Dominicana
Caribbean Marketing Services
Tel. (809) 533-26-27
Fax (809) 533-18-82
cms@codetel.net.do

Bolivia
Librerías Asociadas, S.R.L.
Tel./Fax (591) 2244-53-09
libras@datacom-bo.net
La Paz

Venezuela
Ediciones Ramvile
Tel. (582) 793-20-92 y 782-29-21
Fax (582) 793-65-66
tclibros@attglobal.net
Caracas

El Salvador
The Bookshop, S.A. de C.V.
Tel. (503) 243-70-17
Fax (503) 243-12-90
amorales@sal.gbm.net
San Salvador

Guatemala
Textos, S.A.
Tel. (502) 368-01-48
Fax (502) 368-15-70
textos@infovia.com.gt
Guatemala

Índice

Introducción XIII

1. Los sistemas de telecomunicaciones 1

1.1. Evolución histórica de los sistemas de comunicaciones	2
1.1.1. Tecnologías asociadas	3
1.1.2. Las redes del futuro	4
1.1.3. La Telemática	5
1.2. Organismos de normalización	6
1.2.1. El proceso de normalización	7
1.2.2. Organismos que establecen estándares	7
1.3. Redes de comunicación de datos	11
1.4. Clasificación de las redes	11
1.4.1. LAN, MAN y WAN	11
1.5. Redes públicas, privadas y RPV	13
1.5.1. Red pública	14
1.5.2. Red privada	14
1.5.3. Red privada virtual	15
1.6. Elementos de una red	16
1.6.1. Estructura de una red de telecomunicaciones	17
1.6.2. Redes de conmutación y difusión	18
1.7. Direcciones útiles de Internet	21
Ejercicios propuestos	24

2. Aspectos físicos de la transmisión de datos 25

2.1. La transmisión de información	26
2.1.1. Transmisión serie y paralelo	26
2.1.2. Métodos de explotación	27
2.1.3. Transmisión analógica y digital	27

2.2. Transmisión asíncrona y síncrona	28
2.2.1. Transmisión asíncrona	28
2.2.2. Transmisión síncrona	29
2.3. Métodos de detección y corrección de errores	30
2.3.1. Control de paridad	31
2.3.2. Códigos CRC	32
2.4. Medios de transmisión	33
2.4.1. Cables de pares	33
2.4.2. Cables coaxiales	34
2.4.3. La fibra óptica	35
2.4.4. Enlace de microondas	36
2.5. La interfaz de comunicaciones V.24 (RS-232)	37
2.5.1. Características	37
2.5.2. Descripción funcional	38
2.6. Ancho de banda, velocidad de transmisión y de modulación	39
2.6.1. Ancho de banda	39
2.6.2. Velocidad de transmisión	40
2.6.3. Velocidad de modulación	41
2.7. Transmisión digital. El módem	42
2.7.1. Normalización según la UIT-T (CCITT)	43
2.7.2. Técnicas de modulación	44
2.7.3. Técnica de modulación PCM	45
2.7.4. Tasa de error	45
2.7.5. Software de control. Comandos HAYES	46
2.8. Detección y corrección de errores	48
2.8.1. Protocolos MNP	48
2.8.2. Normas V.42/V.42bis	49
2.8.3. Respuesta y marcación automática. V.25bis	50
2.9. Compartición de líneas	51
2.9.1. Multiplicadores de interfaz	51
2.9.2. Multiplexores FDM y TDM	52
2.9.3. Concentradores/Hubs	54
2.9.4. Comutadores/Switches	57
2.10. Los puertos de comunicaciones	58
2.11. El bus USB	59
2.11.1. Conexión de dispositivos	60
2.11.2. Funcionamiento del USB	61
2.11.3. Componentes del USB	62
2.11.4. USB comparado con FireWire (IEEE 1394)	64
2.12. Los conectores	64
2.12.1. Conectores de bus de datos	64
2.12.2. Conector DIN	66
2.12.3. Conectores RJ-45	66
2.12.4. Conectores USB	67
Ejercicios propuestos	68
3. Arquitecturas de comunicaciones	69
3.1. Arquitectura estructurada	70
3.1.1. Estructura en Niveles. El modelo OSI	70
3.1.2. Ventajas que aporta el modelo OSI	71

3.2. Terminología empleada en OSI	72
3.2.1. Tipos de servicio	73
3.3. Funciones de cada nivel OSI	73
3.3.1. Niveles OSI orientados a la red	74
3.3.2. Niveles OSI orientados a la aplicación	76
3.4. La arquitectura SNA	76
3.4.1. Niveles de SNA	77
3.4.2. Componentes básicos de una red SNA	78
3.4.3. Unidades direccionables de la red	78
3.5. Introducción a la comunicación en red local	79
3.5.1. Topologías de LAN	81
3.5.2. Técnicas de compartición	81
3.5.3. El nivel físico	84
3.6. Nivel de enlace y métodos de acceso	86
3.6.1. El subnivel MAC	87
3.6.2. El método CSMA/CD	88
3.6.3. El método Paso de Testigo	90
3.6.4. Control del enlace lógico (LLC)	91
3.7. WLAN	92
3.7.1. Redes locales inalámbricas 802.11	94
3.7.2. Normalización IEEE	95
3.7.3. WEP. Compatibilidad y seguridad	98
3.8. Protocolos de las LAN	99
Ejercicios propuestos	100
4. Protocolos de nivel de enlace	101
4.1. Introducción a los protocolos	102
4.2. Códigos de comunicaciones	102
4.2.1. El código ASCII	103
4.3. Protocolos para transmisión de datos	105
4.3.1. Protocolos elementales de enlace	106
4.3.2. El control de flujo	106
4.4. El protocolo XMODEM	107
4.5. Protocolos orientados a carácter (BSC)	109
4.6. Protocolos orientados a bit (HDLC/SDLC)	110
4.6.1. Modo de funcionamiento	111
4.6.2. Estructura de la trama HDLC	111
4.6.3. SDLC (Synchronous Data Link Control)	113
Ejercicios propuestos	114
5. Protocolos de red y transporte	115
5.1. Familia de protocolos TCP/IP	116
5.2. Protocolo de red	117
5.2.1. Estructura de los datagramas IP	117
5.2.2. Direccionamiento IP	118
5.2.3. Funcionamiento de IP	121
5.2.4. El protocolo IPv6	122

5.3. Protocolos de transporte	123
5.3.1. Protocolo UDP	124
5.3.2. Protocolo TCP	125
5.3.3. Formato del segmento TCP	125
5.3.4. Funcionamiento de TCP	127
5.4. Conexiones	128
5.4.1. Establecimiento de una conexión	129
5.5. El concepto de puerto	130
5.5.1. Puertos	131
Ejercicios propuestos	135
6. Introducción a las redes de área local	137
6.1. Concepto y características de las redes	138
6.2. Tecnologías de las redes de área local	138
6.2.1. Topologías: bus, anillo, estrella, árbol	140
6.2.2. Protocolos de control de acceso al medio	146
6.3. Estándares del IEEE: normalización en redes de área local	147
6.3.1. Norma 802.1	148
6.3.2. Norma 802.2	148
6.3.3. Norma 802.3	148
6.3.4. Norma 802.4	148
6.3.5. Norma 802.5	148
6.3.6. Norma 802.6	148
6.3.7. Norma 802.7	148
6.3.8. Norma 802.8	148
6.3.9. Norma 802.9	149
6.3.10. Norma 802.10	149
6.3.11. Norma 802.11	149
6.3.12. Norma 802.12	149
6.3.13. Norma 802.16	149
6.4. Redes locales de alta velocidad	149
6.5. FDDI (Fiber Distributed Data Interfaz)	151
Ejercicios propuestos	153
7. Implementación de una red de área local	155
7.1. Consideraciones previas	156
7.2. Diseño inicial	156
7.2.1. Topología	156
7.2.2. Componentes hardware de la LAN	157
7.2.3. Componentes software de la LAN	159
7.3. Componentes hardware	159
7.3.1. Medios de transmisión	159
7.3.2. Tarjetas de conexión	162
7.3.3. Estaciones de trabajo	171
7.3.4. Servidores de red	172
7.3.5. Periféricos	173
7.4. Componentes software	173
7.4.1. Sistemas operativos de red	173
7.4.2. Funciones del sistema operativo de red	176

7.5. Proceso de instalación de una LAN	181
7.6. Mantenimiento de la red	182
7.6.1. Topología en bus	182
7.6.2. Topología en estrella	185
7.6.3. Adaptadores	186
7.6.4. Concentradores	186
7.6.5. Problemas con los servidores	186
7.7. Redes inalámbricas	187
7.8. Configuraciones inalámbricas	189
7.8.1. Punto de acceso Belkin	189
7.8.2. Punto de acceso Linksys	193
7.8.3. Adaptadores inalámbricos	194
Ejercicios propuestos	198

8. Administración y gestión de una red de área local

.....	199
8.1. Organización de una red	200
8.1.1. Servidor de impresoras	200
8.1.2. Servidor de unidades de disco	201
8.1.3. Servidor de aplicaciones	202
8.2. Administrador del sistema	202
8.3. Configuración y control del sistema de red	205
8.4. Utilidades del supervisor	208
8.5. Control del sistema de red	208
8.6. Correo electrónico	211
8.7. Servidor Web	212
8.8. Cortafuegos físico	214
8.9. Administración y gestión de redes inalámbricas	217
Ejercicios propuestos	217

9. Seguridad en redes de área local

.....	219
9.1. Conceptos generales	220
9.2. Análisis de riesgos y planificación de sistemas de seguridad	221
9.3. Seguridad hardware	221
9.4. Accesos y seguridad de volúmenes, directorios y ficheros	222
9.5. Deshabilitación de cuentas	225
9.6. Protección de accesos vía conexión telefónica	226
9.7. Seguridad en redes inalámbricas	226
9.8. Seguridad contra sobretensiones y descargas atmosféricas	228
Ejercicios propuestos	228

10. Redes de área extensa

.....	229
10.1. Las técnicas de conmutación	230
10.1.1. Conmutación de circuitos	230
10.1.2. Conmutación de mensajes	231
10.1.3. Conmutación de paquetes	231
10.2. Redes de conmutación de paquetes	231
10.2.1. Los nodos de la red	233
10.3. El protocolo X.25	233

10.3.1. El nivel físico	234
10.3.2. El nivel de enlace	234
10.3.3. El nivel de red	234
10.3.4. Facilidades que ofrece X.25	235
10.3.5. Conexiones utilizando un PAD	236
10.4. El servicio Iberpac	237
10.4.1. Servicio Básico	237
10.4.2. Servicio Plus y Uno	237
10.5. La red digital de servicios integrados	237
10.5.1. Evolución de la red telefónica	238
10.6. Integración de servicios en la RDSI	239
10.6.1. El bus pasivo S0	240
10.7. Modelo de referencia de la RDSI	241
10.7.1. Agrupaciones funcionales	241
10.7.2. Puntos de referencia	244
10.7.3. Señalización en la RDSI	244
10.8. Utilización de la RDSI	244
10.8.1. Los servicios que aporta la RDSI	245
Ejercicios propuestos	247
 11. Interconexión de redes de área local	249
11.1. Necesidad de la interconexión	250
11.2. Dispositivos para la interconexión de redes	250
11.2.1. Repetidores	251
11.2.2. Puentes	252
11.2.3. Switches	253
11.2.4. Routers	256
11.2.5. Firewalls	257
11.3. Interconexión de WAN	258
11.3.1. Pasarelas	258
11.3.2. Protocolos SLIP y PPP	259
11.4. Protocolos de transporte y encaminamiento	261
11.4.1. Tablas de direccionamiento	262
11.5. El servicio Frame Relay	263
11.6. El servicio ATM	264
Ejercicios propuestos	266
 12. Internet	267
12.1. Los orígenes de Internet	268
12.2. Protocolos y direccionamiento en Internet	270
12.2.1. El protocolo TCP/IP	270
12.2.2. Internet Protocol o Protocolo para interredes	271
12.2.3. Clases de direcciones Internet (IP)	271
12.3. El modelo cliente-servidor. Navegadores	273
12.4. Servicios básicos en Internet	276
12.4.1. Correo electrónico	277
12.4.2. Transferencia de ficheros	278

12.4.3. Archie	278
12.4.4. Telnet	278
12.4.5. Gopher	279
12.4.6. Grupos de Noticias (News)	279
12.4.7. Búsqueda de usuarios (Finger y Whois)	279
12.4.8. Conversación multiusuario (IRC)	279
12.4.9. World Wide Web	280
12.4.10. Creación de páginas Web	280
12.5. Nombres por dominios	281
12.5.1. La gestión de dominios de Internet	282
12.5.2. Asignación de dominios	283
12.6. Navegadores, portales y buscadores	283
12.6.1. Portales	285
12.6.2. Motores de búsqueda	286
12.7. El correo electrónico	287
12.7.1. Características comunes del correo electrónico	287
12.8. La seguridad de Internet	289
12.8.1. Firewalls. Seguridad entre redes	290
12.8.2. Cifrado de datos	291
12.8.3. Seguridad en el correo y comercio electrónicos	292
Ejercicios propuestos	294
13. Configuración de una red con Linux	295
13.1. Introducción	296
13.2. Conceptos básicos	297
13.2.1. Inicio de sesión	297
13.2.2. Comandos básicos	297
13.3. Sistemas de archivos	298
13.4. Gestión de permisos	299
13.5. Archivos de configuración de red	300
13.6. Configuración de la tarjeta de red	300
13.7. Servicios básicos de red	310
13.7.1 Telnet	311
13.7.2. DNS	312
13.7.3. NFS	313
13.7.4. FTP	316
13.8. Cortafuegos o Firewall	317
Ejercicios propuestos	319
Glosario de términos	321
Bibliografía	331

3

Arquitecturas de comunicaciones

Introducción

La estandarización tiene consecuencias positivas y puede tenerlas negativas, pero en cualquier caso se hace necesaria en un entorno con diversidad de redes, fabricantes de equipos y operadores de telecomunicaciones. La arquitectura de red en capa propuesta por ISO ha supuesto un hito en el estudio y desarrollo de las telecomunicaciones, estableciendo los fundamentos para la comunicación entre elementos de la red y las aplicaciones.

El modelo de red utilizado en las redes de área local no sigue exactamente el modelo OSI, aunque sí se pueden encontrar algunos parecidos con él. En función de la topología de la red y del método de acceso se tiene diferentes estándares, algunos de ellos ampliamente instalados en el mundo empresarial.

Contenido

- 3.1. Arquitectura estructurada. El modelo OSI
- 3.2. Terminología empleada en OSI
- 3.3. Funciones de cada nivel OSI
- 3.4. La arquitectura SNA
- 3.5. Introducción a la comunicación en red local
- 3.6. Nivel de enlace y métodos de acceso
- 3.7. WLAN
- 3.8. Protocolos de las LAN

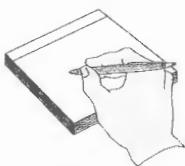
Objetivos

- Introducir el modelo de Interconexión de Sistemas Abiertos, propuesto por ISO, que supone una arquitectura de red en capas o niveles que intercambian información entre ellos.
- Profundizar en los niveles, funciones y servicios de una arquitectura estructurada, a la vez que se efectúa una introducción a las redes de área local.
- Estudiar el nivel de enlace y los métodos de acceso comunes en las redes de área local.

3.1 Arquitectura estructurada

En el capítulo primero se ha descrito de una forma muy básica la necesidad de las redes telemáticas y los requisitos elementales que debe ofrecer a los usuarios. En éste se profundiza en los niveles, funciones y servicios de una arquitectura estructurada, a la vez que se efectúa una introducción a las arquitecturas de redes de área local. El estudio de las redes, al ser un conjunto particularmente complejo, necesita una estructuración que permita descomponer el sistema en sus elementos directamente realizables. Introducimos así el modelo de referencia para la **Interconexión de Sistemas Abiertos (OSI/Open Systems Interconnection)**.

Ejercicio Resuelto 3.1



Realícese una comprobación del funcionamiento del método CSMA/CD mediante un simulador.

SOLUCIÓN

En primer lugar se buscará el programa adecuado mediante una búsqueda en Internet. Por ejemplo, buscando “simulador+CSMA/CD” se puede localizar la versión de evaluación del “Network Simulator”. Se puede encontrar en la dirección:

<http://www.adventnet.com/products/simulator/index.html>

Una vez obtenida dicha versión de evaluación, se instalará y se realizará el estudio por simulación.

3.1.1. Estructura en Niveles. El modelo OSI

El modelo OSI de ISO (*International Organization for Standardization*) surge, en el año 1984, ante la necesidad imperante de interconectar sistemas de procedencia diversa –diversos fabricantes–, cada uno de los cuales empleaba sus propios protocolos para el intercambio de señales. El término *abierto* se seleccionó con la idea de realzar la facilidad básica del modelo que da origen al mismo, frente a otros modelos *propietarios* y, por tanto, cerrados.

El modelo OSI está compuesto por una pila de 7 niveles o capas, cada uno de ellos con una funcionalidad específica, para permitir la interconexión e interoperatividad de sistemas heterogéneos. La utilidad radica en la separación que en él se hace de las distintas tareas que son necesarias para comunicar datos entre dos sistemas independientes.

Es importante señalar que este modelo no es una arquitectura de red en sí mismo, dado que no se especifica, en forma exacta, los servicios y protocolos que se utilizarán en cada nivel, sino que solamente indica la funcionalidad de cada uno de ellos. Sin embargo, ISO también ha generado normas para la mayoría de los niveles, aunque éstas no forman parte del modelo OSI, habiéndose publicado todas ellas como normas independientes.

Los siete niveles del modelo OSI (véase la figura 3.1) son los siguientes:

Nivel	Función
7. Aplicación	Datos normalizados
6. Presentación	Interpretación de los datos
5. Sesión	Diálogos de control
4. Transporte	Integridad de los mensajes
3. Red	Encaminamiento
2. Enlace de datos	Detección de errores
1. Físico	Conexión de equipos

Figura 3.1. Niveles y funciones del modelo de referencia OSI de ISO.

Los tres niveles inferiores están orientados al acceso del usuario –comunicaciones de datos–; el cuarto nivel al transporte extremo a extremo de la información, y los tres superiores a la aplicación.

3.1.2. Ventajas que aporta el modelo OSI

El concepto OSI o ISA está descrito en las normas ISO 7498-1 y UIT-T X.200. Debido a que las dos organizaciones (ISO y UIT) están implicadas en el proceso de estandarización OSI, muchas de las especificaciones referentes a este modelo han sido publicadas por los estándares ISO y por las recomendaciones UIT-T. En estos casos, ambas versiones son equivalentes, o una versión es un subconjunto de la otra.

Los estándares OSI describen las reglas que deben seguir los equipos de comunicaciones para que el intercambio de datos sea posible dentro de una infraestructura que esté compuesta de una gran variedad de productos de diferentes suministradores.

A partir de este modelo se han desarrollado una gran familia de protocolos para que diferentes tipos de ordenadores puedan trabajar y comunicarse conjuntamente sobre diversos tipos de redes.

Con el objetivo de definir un estándar flexible y con posibilidad de ampliarse, los organismos de normalización pensaron que una buena idea para conseguirlo era separar en varios módulos la enorme complejidad de un proceso de comunicación entre dos aplicaciones. Cada módulo se ocupa de unas tareas específicas por lo que resulta mucho más fácil realizar cambios en una parte sin que se tenga que alterar el resto de las especificaciones. Así, el modelo consta de siete módulos o niveles: aplicación, presentación, sesión, transporte, red, enlace y físico.

Las ventajas teóricas más importantes que resultan de la utilización del estándar OSI son:

- Conectividad en todo el mundo sin tener que instalar pasarelas.
- Fácil integración de productos en la red.
- Un punto de vista único a la hora de configurar la seguridad.
- Amplio margen en la elección de suministradores lo que permite una mayor competencia entre éstos y, consecuentemente, precios más bajos.
- Las mejores posibilidades de sobrevivir a las nuevas generaciones tecnológicas sin elevados costes de conversión.

Pese a las ventajas citadas anteriormente, los protocolos OSI no están siendo utilizados fuera de aquellas comunidades en donde su uso está forzado por convenio. Otros protocolos, como por ejemplo TCP/IP, están mucho más extendidos en las empresas que los estándares oficiales. Las razones más ampliamente admitidas del porqué de esta situación son las siguientes:

- Los protocolos OSI no han sido probados ampliamente antes de haber sido estandarizados y no están basados en la práctica en una red de ordenadores a gran escala. Por el contrario, TCP/IP se ha utilizado con profusión desde hace 30 años.
- Los estándares OSI son, comparados a los estándares Internet y los RFC (*Ready for Comment*), muy caros y difíciles de obtener.
- El modelo de referencia OSI es demasiado complejo y con muchos niveles.
- Las nuevas tecnologías de red, como sucede con ATM, no se ajustan del todo al modelo OSI.
- Al definirse dos protocolos alternativos e incompatibles en el nivel de red de OSI (X.25 que es orientado a conexión e IP que es no orientado a conexión), no ayuda a construirse, mantener y utilizar una red totalmente interconectada.
- Existe un amplio acuerdo en que la configuración del nivel de red sin conexión (datagrama) como la existente en Internet (utilizando el protocolo TCP/IP) es técnicamente superior a X.25 (orientado a conexión).

El modelo OSI facilita el estudio de las redes y comprender su funcionamiento.

El modelo TCP/IP no se ajusta al modelo OSI, pero tiene ciertas similitudes con él.

3.2 Terminología empleada en OSI

Para entender la filosofía OSI, es preciso definir una serie de términos básicos del modelo, que son:

Modelo

Marco o entorno de actuación en el cual se definen una estructura y unas funciones aplicables al proceso lógico de un sistema de telecomunicaciones. En consecuencia, el modelo no implica solución tecnológica alguna –no condiciona el entorno de aplicación–, sino que aporta procedimientos para el intercambio de información normalizada.

En el modelo OSI las tareas de cooperación se dividen en siete partes, módulos, niveles o capas, con las siguientes premisas:

1. Cada nivel realiza tareas únicas y específicas, y debe ser creado cuando se necesite un grado diferente de abstracción.
2. Todo nivel tiene conocimiento de los niveles inmediatamente adyacentes y sólo de éstos.
3. Todo nivel se sirve de los servicios del nivel anterior, a la vez que los presta al superior.
4. Los servicios de un nivel determinado son independientes de su implantación práctica.
5. Los límites de cada nivel se deben seleccionar teniendo en cuenta que minimicen el flujo de información a través de las interfaces establecidas.

Sistema

Conjunto de uno o más ordenadores, periféricos, software, etc., que conforman un todo capaz de realizar el procesamiento y/o la transferencia de información.

Nivel

Todo nivel está constituido por una entidad que agrupa un conjunto de funciones que proporcionan servicios específicos que facilitan la comunicación. Cada nivel (N) recibe servicios del nivel inferior ($N-1$) y los proporciona al nivel superior ($N+1$); las interacciones entre los niveles adyacentes se denominan “**primitivas**”, bajo la forma de: peticiones (*Request*), indicaciones (*Indication*), respuestas (*Response*) y confirmaciones (*Confirm*).

Función

Es una entidad lógica que acepta entradas (argumentos) y produce salidas (valor) determinadas por la naturaleza de la función.

Proceso

Elemento dentro de un sistema abierto que efectúa el procesamiento de información para una aplicación determinada. Pueden representar: procesos manuales, físicos o informáticos. OSI se encuentra relacionado con el intercambio de información entre sistemas abiertos y no con el funcionamiento interno de cada sistema.

Además de estos términos (figura 3.2), tenemos otros, como son:

- **Entidades.** Son los elementos activos que se encuentran en cada una de las capas.
- **Puntos de Acceso al Servicio (SAP).** Puntos en los que cada capa encuentra los servicios de la capa inmediatamente inferior.
- **Unidad de Datos de la Interfaz (IDU).** Es el bloque de información que una capa pasa a la entidad correspondiente de la capa inferior.

- **Unidad de Datos del Servicio (SDU).** Cada Unidad de Datos de la interfaz se compone de un campo con información para el control de la interfaz (ICI) y otro con la información que se pasa a través de la red a la entidad homóloga (SDU). La SDU de nivel n es la PDU de nivel n+1: $n+1\text{-PDU} = n\text{-SDU}$.
- **Unidad de Datos del Protocolo (PDU).** Son los paquetes de información que resultan de fraccionar la información que se transfiere (ya que muchas veces no se puede enviar directamente a través de la red), y a la que se le añaden las cabeceras con información de control. La PDU es lo que se intercambian entre pares (niveles homólogos), incluyendo la cabecera.

UNIDADES DE DATOS DE OSI

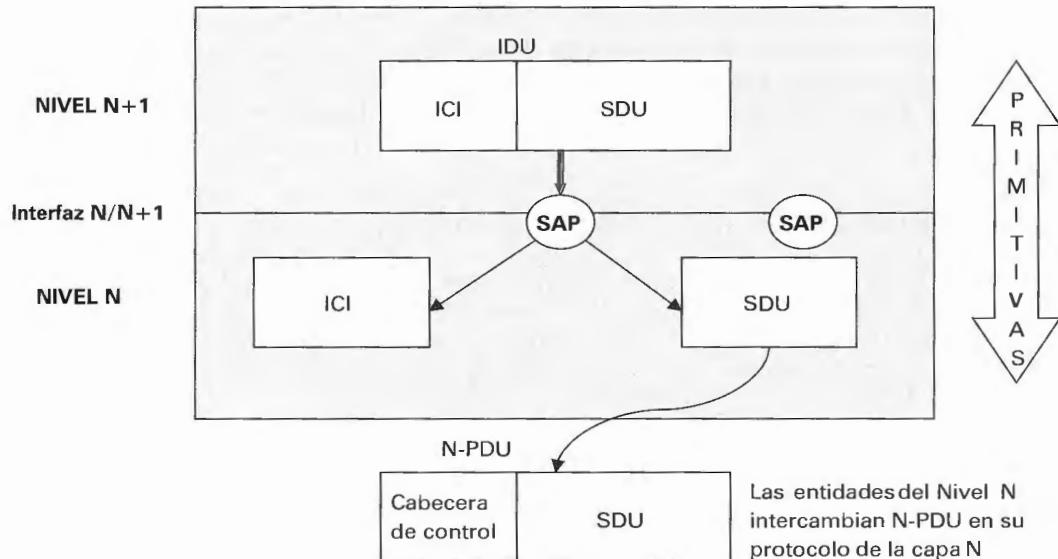


Figura 3.2. Unidades de Datos definidas en el modelo OSI.

Las entidades que abarcan los niveles correspondientes en diferentes máquinas se llaman “iguales” (*peers*).

3.2.1. Tipos de servicio

Existen dos tipos de servicio, que son:

- **Orientado a conexión:** donde el usuario establece inicialmente la conexión, intercambia la información y, finalmente, cuando termina, libera el circuito. Un ejemplo típico de este tipo de servicio se da en la red telefónica y en la comunicación de datos a través de la RTC.
- **Sin conexión:** donde no es necesario establecer, previamente al envío de la información, ningún circuito. Cada mensaje lleva información de la dirección de destino y sigue la ruta más apropiada en cada caso, por lo que pueden llegar en distinto orden y se hace necesario su reordenación.

Un servicio se especifica formalmente como un conjunto de “primitivas” disponibles a un proceso de usuario para que acceda al servicio.

3.3 Funciones de cada nivel OSI

El modelo OSI consta de siete niveles y define cada uno de ellos, pero no normaliza ningún protocolo; los protocolos utilizados son posteriores. Cada nivel agrupa una serie de funciones requeridas para comunicar sistemas y se estructuran en una forma jerárquica, en donde cada capa se apoya en la anterior, realiza su función y ofrece un servicio a la capa superior.

Cada nivel no define un único protocolo, define una función de comunicaciones de datos que puede ser realizada por varios protocolos. Es más, cada nivel puede contener varios protocolos, cada uno de los cuales aporta para culminar la función del nivel correspondiente.

Cada protocolo comunica con su homólogo (*peer*), entendiendo por *peer* una implementación del mismo protocolo en el nivel equivalente sobre un sistema remoto. Así, el protocolo de transferencia de ficheros es el *peer* de un protocolo de transferencia de ficheros remoto. En definitiva, a cada protocolo sólo le concierne la comunicación con su *peer*, siendo ajeno a todo aquello que ocurra con los niveles inferior y superior.

Sin embargo, debe haber un acuerdo sobre cómo pasar los datos entre los diferentes niveles, ya que todos los niveles intervienen en el envío de datos desde una aplicación local hasta una remota, equivalente. Por ello, los niveles superiores confían en los inferiores para enviar los datos a través de la red. Los datos son pasados de un nivel a otro en sentido descendente, hasta llegar al nivel más bajo, el “nivel físico”, que es el encargado de transmitirlos por la red. Al llegar al otro extremo, el proceso se invierte, pasando, en sentido ascendente, desde el nivel más bajo hasta el más alto.

Cada nivel no necesita saber cómo funcionan los niveles adyacentes, sino sólo cómo pasarle los datos. Este tipo de arquitectura permite que se puedan añadir nuevas aplicaciones sin necesidad de modificar la red física, y viceversa, puede modificarse el hardware de red sin que este hecho obligue a modificar la aplicaciones (software).

3.3.1. Niveles OSI orientados a la red

Los niveles más bajos del modelo OSI están orientados a la red, mientras que los más altos se orientan hacia el usuario. Así, los tres primeros tocan aspectos relacionados con el medio físico de transmisión, los procedimientos de enlace para establecer la comunicación y los propios aspectos de envío de información a través de la red.

Nivel 1 — Físico

El nivel físico, el más bajo y más antiguo, proporciona los medios mecánicos, electrónicos, funcionales y de procedimiento para mantener y desactivar las conexiones físicas para la transmisión de bits entre entidades de enlace de datos.

La misión básica de este nivel consiste en transmitir bits por un canal de comunicación, de manera tal que cuando envíe el receptor llegue sin alteración al receptor.

Algunas de las normas dentro de este nivel son:

- X.24** Definiciones relativas a los circuitos de unión establecidos entre dos equipos sobre redes públicas de datos.
- V.10** Características eléctricas de los circuitos de intercambio de doble corriente asimétrica para uso general en teleinformática.
- V.11** Como V.10 pero para corriente simétrica.
- V.24/V.28** Características funcionales/eléctricas para los circuitos de enlace entre dos equipos.
- V.35** Recomendación CCITT para transmisión de datos a 48 kbit/s por medio de circuitos en grupo primario de 60 a 108 kHz.
- ISO 2110** Características mecánicas para el conector de V.24.
- EIA-232** Estándares a nivel físico, eléctrico y funcional de EIA.

Nivel 2 — Enlace de datos

El objetivo de este nivel es facilitar los medios funcionales y de procedimiento para establecer, mantener y liberar conexiones de enlace de datos entre entidades de red y para transferir unidades de datos del servicio de enlace de datos.

Las funciones básicas que realiza este nivel están orientadas a resolver los problemas planteados por la falta de fiabilidad de los circuitos de datos, agrupándose los datos recogidos del nivel de red para su transmisión, formando tramas, que incluyen además bits de redundancia y control para corregir los errores de transmisión; además, regula el flujo de las tramas, para sincronizar su emisión y recepción.

Pertenecen a este nivel:

- HDLC** (*High-level Data Link control*): Protocolo de alto nivel, orientado al bit (especificado por ISO 3309), para el control del enlace de datos, en modo síncrono.
- LAP-B** (*Link Access Procedure-Balanced*): Subconjunto del protocolo HDLC, definido por OSI, para acceso al enlace a redes X.25.
- IEEE 802** Para LAN.

Nivel 3 — Red

El nivel de red proporciona los medios para establecer, mantener y liberar la conexión, a través de una red donde existe una malla compuesta de enlaces y nodos, entre sistemas abiertos que contienen entidades de aplicación en comunicación, así como los medios funcionales y de procedimiento para el intercambio de unidades de datos del servicio de red entre entidades de transporte por conexiones de red.

Es el responsable de las funciones de commutación y encaminamiento de la información; proporciona los procedimientos precisos y necesarios para el intercambio de datos entre el origen y el destino por lo que es necesario que conozca la topología de la red, con objeto de determinar la ruta más adecuada.

Pertenecen a este nivel:

- X.25** Interconexión sobre redes públicas de equipos ETD y ECD para terminales con funcionamiento en modo paquete, conectados a una red pública de transmisión de datos, con línea dedicada.
- X.32** Interfaz entre un ETD y un ECD para terminales que transmiten en modo paquete y acceden a la red pública X.25 a través de la red telefónica conmutada.
- X.3** Servicio complementario de ensamblado y desensamblado de paquetes en una red pública de datos.
- X.28** Interconexión entre ETD/ECD para el acceso de un ETD asíncrono al servicio de ensamblado y desensamblado de paquetes (DEP), en una red pública de datos.
- X.29** Procedimientos de intercambio de información de control y de datos de usuario entre un DEP y un ETD modo paquete u otro DEP.
- ISO 9542** Protocolo de encaminamiento para LAN.

Nivel 4 -- Transporte

El nivel de transporte efectúa la transferencia de datos entre entidades de sesión y las libera de toda otra función relativa a conseguir una transferencia de datos segura y económica.

Su misión básica es la de optimizar los servicios del nivel de red y corregir las posibles deficiencias en la calidad del servicio, con el auxilio de mecanismos de recuperación para condiciones anormales en los niveles inferiores. Proporciona los procedimientos de transporte precisos, con independencia de la red o soporte físico empleado.

Este nivel está muy relacionado con la calidad del servicio ofrecido por la red, ya que si no es suficiente, será este nivel el encargado de establecer el puente entre las carencias de la red y las necesidades del usuario.

Se encuadran dentro de este nivel:

- X.214 (ISO 8072)** Servicio de Transporte
- X.224 (ISO 8073)** Especificación del protocolo de Transporte

3.3.2. Niveles OSI orientados a la aplicación

Son los tres últimos. El nivel 4 (Transporte) es el encargado de garantizar el transporte de datos extremo-a-extremo y que, en función de las aplicaciones que estén corriendo en los equipos, se encarga de solicitar los servicios que sean necesarios de los niveles inferiores.

Nivel 5 — Sesión

El nivel de sesión proporciona el medio necesario para que las entidades de presentación en cooperación organicen y sincronicen su diálogo y procedan al intercambio de datos.

Su función básica consiste en realizar el mapeo de la dirección de sesión hacia el usuario con las direcciones de transporte orientadas a la red y gestionar y sincronizar los datos intercambiados entre los usuarios de una sesión.

En el nivel de sesión tenemos las siguientes recomendaciones:

X.215 (ISO 8326)	Servicio de Sesión
X.225 (ISO 8327)	Especificación del Protocolo de Sesión

Nivel 6 — Presentación

Éste permite la representación de la información que las entidades de aplicación comunican o mencionan en su comunicación. Es el responsable de que la información se entregue al proceso de aplicación de manera que pueda ser entendida y utilizada.

Es responsable de la obtención y liberación de la conexión de sesión cuando existan varias alternativas disponibles, y de establecer el contexto sintáctico del diálogo. A través de él, los procesos de aplicación adquieren independencia de la representación de los datos, incluyendo en su entorno las posibles transformaciones de códigos y la selección de sintaxis.

A este nivel corresponden:

Normas para Videotex, Telefax y Teletex
X.225 del CCITT

Nivel 7 — Aplicación

Al ser el nivel más alto del modelo de referencia, el nivel de aplicación es el medio por el cual los procesos de aplicación acceden al entorno OSI. Por ello. Este nivel no interactúa con uno superior a él.

Su función es proporcionar los procedimientos precisos que permitan a los usuarios ejecutar los comandos relativos a sus propias aplicaciones. Los procesos de las aplicaciones se comunican entre sí por medio de las entidades de aplicación asociadas, controladas por protocolos de aplicación y utilizando los servicios del nivel de presentación. La transferencia de ficheros es una de las aplicaciones más comunes de este nivel.

Pertenecen a este nivel, entre otras:

X.400	Describe el modelo básico del sistema de tratamiento de mensajes en la aplicación de <i>Correo Electrónico</i> .
X.500	Servicio de <i>Directorio</i> en la aplicación de correo electrónico.

3.4 La arquitectura SNA

El modelo OSI es un modelo teórico que, aunque presenta numerosas ventajas, no es seguido por muchos fabricantes, al menos en su totalidad, que han preferido implantar los suyos propios, con gran éxito, como es el caso de IBM con SNA o lo fue en su

momento Digital (DEC) con DNA. Estas redes, aunque no son OSI, presentan algunas similitudes con ese modelo, sobre todo en lo que se refiere a una estructura en capas o niveles que intercambian información entre sí y están especializadas en realizar una serie de funciones específicas. Por el interés que presenta y por su importancia comercial estudiaremos brevemente la arquitectura SNA de IBM.

SNA (Systems Network Architecture) es la arquitectura de redes de ordenadores desarrollada por IBM, que define niveles de protocolos para comunicaciones entre terminales y sistemas y entre programas, así como toda una familia de productos hardware basados en esta arquitectura.

En el momento de su lanzamiento en el año 1974, las comunicaciones estaban basadas en una relación jerárquica **maestro/esclavo** entre un ordenador central y un cierto grupo de terminales, bastante distinto a lo que sucede hoy, en lo que predomina son entornos distribuidos, cercanos al modelo **cliente/servidor**, con una relación de igual-a-igual (*peer-to-peer*) entre sistemas.

Nace ante la necesidad de compatibilizar en un único entorno de comunicaciones de datos todos los diversos equipos, integrándolos en un solo sistema, definiendo el NCP (*Network Control Program*) y el VTAM (*Virtual Telecommunication Access Method*) entre sus características más significativas. El NCP y el VTAM constituyen el software básico para la definición e implantación de una red SNA. El primero reside en los controladores de comunicaciones y el segundo en el HOST, corriendo como una aplicación del sistema operativo; sobre este último, corren como aplicaciones los diferentes subsistemas de software como son CICS, IMS, JES, TSO, etc. El software de gestión de red en el HOST se denomina **NetView**.

La arquitectura SNA ha sido ampliamente utilizada por IBM para dar servicio a grandes empresas e instituciones.

3.4.1. Niveles de SNA

SNA es una especificación que describe la arquitectura para un entorno de red distribuida, definiendo las reglas y protocolos de comunicación entre sus diversos componentes, basada en el concepto de dominios. El modelo de arquitectura de red SNA, definiendo con anterioridad al estándar OSI, sigue también una estructura en niveles, que tiene una cierta correspondencia con él, como se aprecia en la figura 3.3.

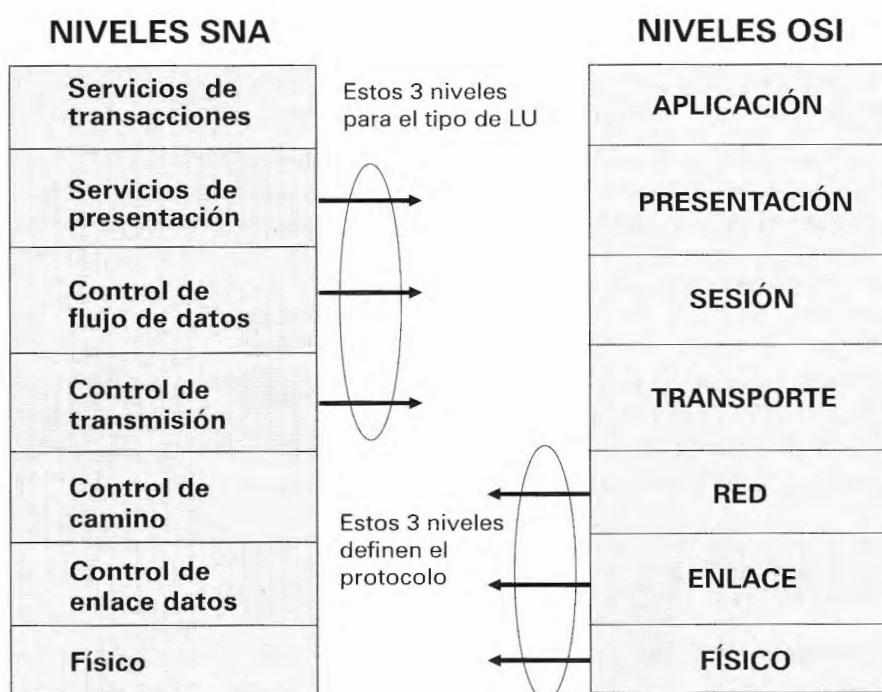


Figura 3.3. Correspondencia entre los niveles SNA y el modelo OSI.

- **Físico**

Define las características físicas y eléctricas de la interfaz entre el terminal y la red, estando disponibles la RS-232 y X.21.

- **Control de enlace de datos**

Este nivel es el encargado de inicializar, desconectar y transferir datos entre dos nodos adyacentes sin errores. El protocolo empleado es el SDLC: *Synchronous Data Link Control*, orientado al bit y basado en el HDLC.

- **Control de camino**

Se ocupa de la posible segmentación o no del mensaje que le llega del nivel 4, del control de flujo y selecciona la ruta para el establecimiento de las sesiones.

- **Control de transmisión**

Atiende a la activación y desactivación de las sesiones, así como a la sincronización y el control de flujo extremo a extremo, entre usuarios finales. Criptografía de mensajes.

- **Control de flujo de datos**

Controla el flujo de datos entre usuarios y correlación durante las sesiones.

- **Servicios de presentación**

Define los protocolos para la comunicación programa a programa y gestiona la comunicación entre programas transaccionales (Sesión). Presentación de la información.

- **Servicios de transacciones**

Ofrece un lenguaje común de comandos para hacer uso de los servicios de la red SNA, interviniendo en el intercambio de datos entre LUs. Interfaz lógica con los usuarios.

3.4.2. Componentes básicos de una red SNA

Las funciones y capacidades de una red SNA se ejecutan en un conjunto de componentes hardware y software que incluyen procesadores de comunicaciones, controladores de periféricos, estaciones de trabajo, métodos de acceso de telecomunicaciones, subsistemas de telecomunicación y programas de control de red y de aplicaciones, respectivamente.

- **Dominios**

La red SNA se basa en el concepto de “dominio”, siendo éste el conjunto de nodos y recursos controlados por un único nodo central. Los usuarios finales de la red (programas de aplicaciones o individuos) no se consideran parte de la red, y es por ello por lo que debe existir una unidad lógica (LU), con una dirección de red asociada, que actúe como punto de acceso a la misma.

- **Nodos**

SNA define un nodo como el punto de la red que contiene componentes hardware y software SNA y que ejecuta las funciones de los niveles de la arquitectura SNA. Cada uno de éstos debe contener una unidad física (PU) que lo represente, a él y a sus recursos, ante la red y frente al SSCP.

3.4.3. Unidades direccionables de la red

SNA presenta un conjunto de unidades direccionables de la red (NAUs), componentes lógicos de la misma, que ofrecen a los usuarios finales puertas de acceso a ella para enviar datos e interactúan con los operadores de la red para desarrollar funciones de gestión y control. Cada NAU tiene una dirección lógica que la identifica frente a las

otras, existiendo tres tipos diferentes: **LU (Logical Unit)**, **PU (Physical Unit)** y **SSCP (System Services Control Point)**.

• Unidades lógicas

La LU (*Logical Unit*) está formada por aquellas partes del programa de aplicación y del software de comunicaciones que pasa y transfiere los datos que proceden de la red hacia la aplicación. El número de usuarios que pueden acceder a la red por medio de una sola LU depende del diseño de la misma, pero cada uno está representado siempre por una LU. La conexión de varias LUs para que sus usuarios puedan comunicarse entre sí es lo que se denomina establecimiento de sesión.

• Unidades físicas

Las PU (*Physical Unit*) son un conjunto de componentes SNA –no dispositivos físicos– que gestionan los enlaces entre un nodo y sus adyacentes (sirven de puntos de entrada entre la red y una o más LUs). Las PUs administran los recursos de la red y facilitan una serie de servicios, tales como IPL (*Initial Program Loading*), activación y desactivación, reportando resultados de rendimiento al SSCP o realizando tests de diagnóstico.

• Punto de control del servicio

El SSCP (*System Services Control Point*) controla todas las situaciones que implican un cambio en el estado de los elementos de la red (PUs y LUs) a él asignados. Contiene las tablas de direcciones de red, las de traducción de los nombres de red a direcciones, tablas de encaminamiento, establece las conexiones entre los nodos y controla el flujo de información a través de la red.

3.5 Introducción a la comunicación en red local

Una red de área local (**LAN/Local Area Network**) es un sistema de comunicaciones constituido por un hardware (cableado, terminales, servidores, etc.), y un software (acceso al medio, gestión de recursos, intercomunicación, etc.) que se distribuyen por una extensión limitada (planta, edificio, grupo de edificios) en el que existen una serie de recursos compatibles (discos, impresoras, bases de datos, etc.), a los que tienen acceso los usuarios para compartir información de trabajo (figura 3.4). La interconexión entre ellas (LAN/LAN) o entre LAN y WAN, se realiza por medio de repetidores (*repeaters*), puentes (*bridges*), encaminadores (*routers*) y pasarelas (*gateways*), empezando ahora, al bajar su precio, a utilizarse conmutadores (*switches*) con un retardo muy bajo para enlazar segmentos de una red, en cuyo caso se dispone de todo el ancho de banda entre los dos elementos puestos en comunicación en cada momento.

Las redes de área local permiten conectar a muchos usuarios entre sí, a gran velocidad, en entornos reducidos.

REDES DE ÁREA LOCAL

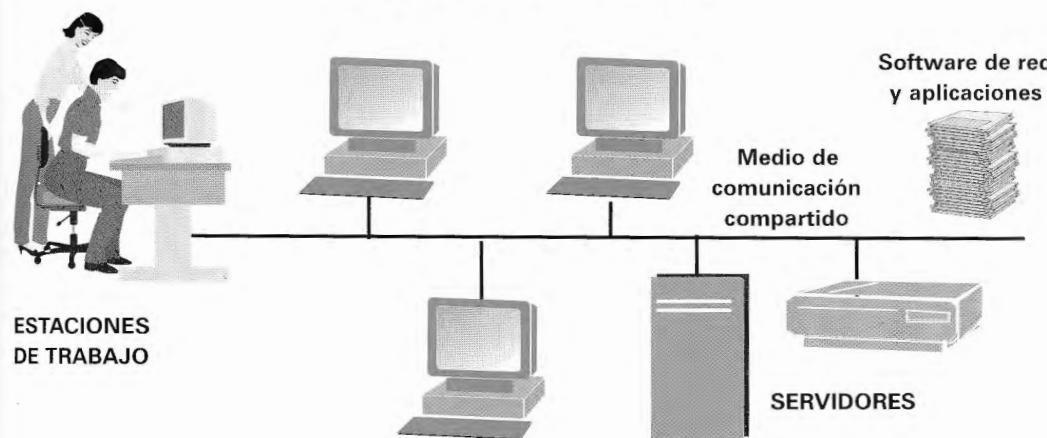
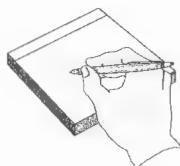


Figura 3.4. Estructura típica de una red de área local en bus.

Según el Comité IEEE 802, una LAN se distingue de otros tipos de redes de datos en que las comunicaciones se restringen a un área geográfica limitada, y en que pueden depender de un canal físico de comunicaciones con una velocidad binaria alta y que presenta una reducida tasa de errores.

En todas las redes de área local nos encontraremos siempre un **modo de transmisión/modulación** (banda base o banda ancha), un **protocolo de acceso** (TDMA, CSMA/CD, Token Passing, FDDI), un **soporte físico** (cables de pares trenzados con o sin pantalla, coaxiales o fibra óptica) y una **topología** (bus, anillo, estrella y malla). A lo largo de los siguientes apartados se expondrán cada uno de estos conceptos, explicando sus características más importantes.

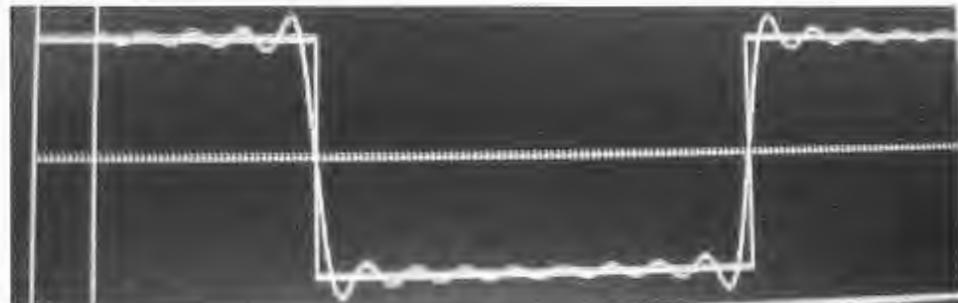
Ejercicio Resuelto 3.2



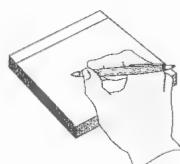
Realícese un estudio según el desarrollo de Fourier y compruébese la forma de onda a la salida de una línea de transmisión telefónica de ancho de banda 3.100 Hz para una entrada de onda cuadrada de 170 Hz, que representa una secuencia de bits. La duración del impulso es de 0,5 T y el desfase de los armónicos es cero.

SOLUCIÓN

Se realiza el desarrollo de Fourier para dicha señal y, teniendo en cuenta el ancho de banda del medio, se obtiene a la salida:



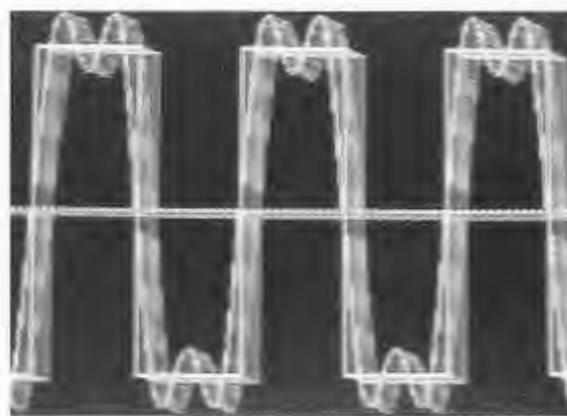
Ejercicio Resuelto 3.3



Realícese un estudio según el desarrollo de Fourier y compruébese la forma de onda a la salida de una línea de transmisión telefónica de ancho de banda 3.100 Hz para una entrada de onda cuadrada de 1.000 Hz, que representa una secuencia de bits. La duración del impulso es de 0,5 T y el desfase de los armónicos es cero.

SOLUCIÓN

Se realiza el desarrollo de Fourier para dicha señal y teniendo en cuenta el ancho de banda del medio se obtiene a la salida:



3.5.1. Topologías de LAN

Para constituir una LAN se utiliza como elemento básico un sistema físico consistente en un cableado que distribuye las señales entre todos los equipos conectados a la misma. Este cableado presenta una serie de características, propias del cable utilizado –coaxial, cable de pares, fibra óptica– como es el ancho de banda, facilidad de conexión, etc. que determinan, entre otras cosas, la velocidad a la que puede circular la información, el número de estaciones de trabajo que pueden conectarse y la distancia máxima a las que éstas pueden estar.

Existen, básicamente, cuatro topologías diferentes para la construcción de una red de área local: Bus, Anillo, Estrella y Malla.

- **Bus**

Es la forma más simple, en la que un único tendido, mediante derivaciones, da servicio a todos y cada uno de los terminales, por lo que en caso de fallo del mismo una parte de la red queda sin servicio. Suele emplearse para ella cable coaxial, y el ejemplo más típico de la misma lo constituyen las redes Ethernet. Se puede complicar, añadiendo diversas ramificaciones, hasta llegar a formar un árbol.

- **Anillo**

Es una variante de la de bus, en la que éste se cierra sobre sí mismo, por lo que en caso de su rotura se puede acceder a las estaciones aisladas por el otro semianillo. En la práctica, la mayoría de las topologías en anillo (lógica) acaban siendo una estrella física. Pueden emplearse cables de pares, coaxiales o fibra óptica, encontrando su ejemplo más significativo de utilización en las redes Token Ring.

- **Estrella**

Es en la que un elemento central (hub) sirve de puente entre todos los terminales de la LAN, proporcionando la conmutación entre ellos. Aísla unos elementos del fallo de otros, pero presenta como un punto crítico el nodo central, que en caso de fallo deja la red sin servicio. El coste del cableado es elevado al requerir conexiones punto a punto para todos los elementos, aunque éste se minimiza al emplear cable UTP.

- **Malla**

Es la topología que presenta un nivel de seguridad mayor que las demás. Los nodos de la red se unen entre sí formando una estructura en la que al menos existen dos rutas posibles por cada nodo; así, si hay un fallo en una de ellas, la información se puede hacer circular por la otra. Esta topología resulta muy adecuada para cubrir, por ejemplo, un país completo y así, es la que utiliza Telefónica para su red Iberpac, pero también es la topología del *backbone* de Internet, a nivel mundial. Puede resultar, inicialmente, más cara que las otras pero si se ha cuidado el diseño y se ha ajustado la capacidad de los enlaces, este incremento se compensará con creces.

Las topologías en bus y estrella son las más comunes en las LAN. Una topología física en estrella puede ser una topología lógica en bus.

3.5.2. Técnicas de compartición

En las redes locales, las técnicas de compartición suelen ser siempre de acceso directo; cada usuario está conectado directamente al medio de comunicación y no a través de un concentrador y la capacidad del canal suele ser del orden de la velocidad de transmisión de los usuarios. Las técnicas de concentración suelen utilizarse con mayor profusión en grandes redes de ordenadores con enlaces de alta capacidad y terminales con velocidades muy dispares.

Existen tres procedimientos básicos de compartir un recurso cuando la conexión de los usuarios es directa (figura 3.5): **selección, reserva y contienda**. Los dos primeros pueden efectuarse con control de acceso centralizado o distribuido. La técnica de contienda, también denominada de acceso aleatorio, es específica para redes con control de acceso distribuido.

MÉTODO DE ACCESO AL MEDIO (LAN)



Figura 3.5. Distintos métodos de acceso a una red de área local, un medio compartido.

• Selección

El usuario es avisado al llegar su turno, y toma control hasta que finaliza la transmisión de los mensajes que tiene pendientes en cola de espera. La asignación de turnos no es en el tiempo. Con frecuencia existe un módulo destinado a esta función (control de acceso centralizado) y cada vez que el recurso queda libre, selecciona a un usuario entre los posibles. En cualquier caso, los usuarios son seleccionados por turno y desconocen cuándo van a serlo nuevamente.

Las técnicas de selección centralizadas pueden ser de tres tipos básicos: sondeo (*polling*), *daisy chaining* y peticiones independientes. Como todos los sistemas centralizados, son muy sensibles a fallos en el controlador.

En las técnicas de sondeo, se selecciona un usuario enviándole su dirección que es recibida también por todos los demás. Cuando un usuario reconoce su dirección toma control del canal avisando al controlador una vez finalizado el envío de sus mensajes, o devuelve control inmediatamente si no tiene ningún mensaje en cola de espera.

El sondeo suele efectuarse por uno de estos tres procedimientos: lista, hub-polling y paso de testigo (*token passing*). En el sondeo por lista, el controlador dispone de una lista completa de direcciones de usuarios. Una vez finalizada vuelve a empezarla por el principio. La dirección de un usuario puede estar más de una vez en la lista, estableciéndose así prioridades entre ellos.

En las técnicas *hub-polling*, el controlador tiene una menor actividad. Únicamente arranca y reinicia el proceso de sondeo una vez finalizado. Cada usuario posee la dirección del siguiente y finaliza su transmisión seleccionándolo directamente en lugar de avisar al controlador para que sea él quien lo haga. El último avisa al controlador. Una vez iniciado el proceso de selección, el controlador no vuelve a intervenir hasta que se finalice el ciclo o detecte algún error que lo haya interrumpido y sea necesaria una reinicialización.

Las técnicas de paso de testigo se han utilizado principalmente en estructuras de conexión en anillo (*token ring*). Son técnicas de selección muy similares a las de *hub-polling*, especialmente cuando se aplican a una estructura de conexión en bus (*token bus*) formando un anillo lógico.

De las tres técnicas básicas descritas para control centralizado, existen versiones con control distribuido. En este caso uno de los usuarios asume las tareas de arranque del proceso de selección y de reinicialización en caso de bloqueo. En la selección por sondeo, únicamente las técnicas de *hub-polling* y paso de testigo admiten un control descentralizado.

• Contienda

Cuando un usuario necesita el canal de comunicación intenta tomarlo, estableciéndose una contienda o disputa con otros usuarios que también desean utilizarlo. En estas técnicas suelen producirse colisiones por tomar el recurso estando ocupado, o porque dos o más usuarios han intentado tomarlo al mismo tiempo. Estas técnicas suelen también denominarse de acceso aleatorio, ya que no está definido el momento de enlace.

Las técnicas de acceso aleatorio al medio pueden clasificarse en técnicas con o sin escucha (transmisión sorda) según tengan información o no de cuándo el canal está libre. Normalmente esta escucha se efectúa por detección de presencia de señal, aunque por haberse utilizado inicialmente en redes de radio (Red ALOHA) de la Universidad de Hawái tomaron el nombre de acceso múltiple con detección de portadora (CSMA).

La transmisión sorda fue la técnica original usada en la red ALOHA y es conocida también como ALOHA-Pura. Cuando un usuario tiene un paquete que transmitir lo envía por el canal. Si ningún otro estaba transmitiendo o lo hace mientras dure el envío, el paquete llegará intacto; en caso contrario, habrá colisión que al detectarse provocará una retransmisión.

En las técnicas con troceado de paquete, el tiempo se divide en intervalos iguales de un tamaño correspondiente a la duración de un paquete. Los mensajes se dividen en paquetes de tamaño prefijado, lo que resulta adecuado en sistemas en los que de existir conmutación, es de paquetes. Todos los usuarios deben estar sincronizados con un reloj maestro que marca los intervalos. Cuando un usuario tiene un paquete para transmitir espera al principio del próximo intervalo y si actúa sin escucha (sordo), procede a su transmisión.

La técnica ALOHA-Ranurada (*Slotted ALOHA*) es un ejemplo de este último caso y fue propuesta como una mejora del ALOHA-Pura. Reduce la posibilidad de colisión al inicio de cada intervalo, permitiendo que una transmisión ya iniciada se finalice correctamente. La inclusión de troceado permite en este caso doblar el caudal teórico máximo.

Las técnicas de troceado dividen el tiempo en intervalos (*time-slots*) cuya duración es igual al retardo máximo de propagación en el canal (propagación de extremo a extremo). También aquí existe un reloj maestro que marca los intervalos. La duración de estos intervalos puede ser importante respecto de la longitud de un paquete si la velocidad de transmisión es elevada. Para un cable de 1 km el retardo es de 6,6 microsegundos, lo que representa 66 bits a 10 Mbit/s.

El troceado de retardo se utiliza en técnicas con escucha, donde este retardo incide en la decisión a tomar de si el canal está o no libre. Naturalmente, estas técnicas no son utilizables en enlaces vía satélite en los que el retardo es del orden de 125 milisegundos. A diferencia de lo que ocurre en el troceado por paquete, en estos casos y en los no troceados, la longitud de los mensajes enviados puede ser variable.

Las técnicas con escucha (CSMA) obtienen ventaja de su capacidad de escucha de la actividad reciente del canal. Esta ventaja en eficiencia en el uso del canal solamente existe si el tiempo de retardo de propagación es mucho menor que el de transmisión en un paquete. Éste suele ser el caso de las redes locales, aunque para velocidades de transmisión de Mbit/s obligue a paquetes de varios centenares de bits. La escucha permite evitar las colisiones cuando el canal se halla ocupado con bastante antelación.

• Reserva

Finalmente, en las técnicas de reserva, a diferencia de lo que ocurre en las de selección, el usuario conoce con adelanto cuándo va a poder utilizar el recurso. O dispone de una reserva permanente o, en su caso, antes de tomar el recurso solicita que se le haga y confirme una determinada reserva. Naturalmente en el intervalo con reserva no se producirán colisiones, aunque sí puede haberlas en el proceso de su solicitud.

Generalmente, existe un controlador que centraliza el despacho de reserva aunque no es imprescindible. Esta técnica no es apenas utilizada en los sistemas comerciales.

Las técnicas ALOHA: pura y ranurada difieren en si se divide o no el tiempo en ranuras discretas en las que deben caber todas las tramas. En ALOHA-Pura no se requiere sincronización global en el tiempo, mientras que en ALOHA-Ranurado sí.

3.5.3. El nivel físico

El nivel físico en una red local define las características lógicas, eléctricas, temporales y mecánicas de la interconexión con el medio físico de comunicación y establece la interfaz con el nivel de enlace. Este nivel tiene una gran influencia en la caracterización de las redes locales, puesto que además de la definición de los parámetros físicos de la comunicación, puede incorporar diversos mecanismos relacionados con el acceso al medio de comunicación, que condicionan de alguna manera las prestaciones de la red.

• Funciones del nivel físico

Las funciones del nivel físico, básicamente, son: *la definición del formato (eléctrico, lógico, temporal) de la unidad de información y asegurar la independencia del nivel de enlace de la tecnología del medio*.

A nivel físico la unidad de información es el bit. El formato debe establecerse de manera que se pueda transferir información (bits) entre los niveles físicos de dos terminales de la red (DTE) con la suficiente fiabilidad. La definición lógica encierra la codificación de la información binaria en el formato con el que se aplicará al medio físico de comunicación. La razón de esta codificación puede venir dada por determinadas necesidades de la transmisión (como la transparencia de información, la codificación en un único símbolo del bit de dato y del reloj de sincronización, entre otros) o del medio físico (como el aprovechamiento del ancho de banda del mismo o la necesidad de un valor medio de potencia nulo para evitar la magnetización de los posibles acoplos inductivos, entre otros).

El formato eléctrico establece los niveles eléctricos de la señal a transmitir y el formato temporal la duración de estos niveles para transferir los datos a una velocidad determinada.

El nivel físico incorpora toda la dependencia tecnológica del dispositivo lógico terminal (DTE) con el medio, de manera que la comunicación entre el nivel de enlace y el nivel físico es independiente de la tecnología utilizada y generalmente compatible con tecnologías diferentes. La definición mecánica de la interconexión al medio físico de comunicación es también una función propia del nivel físico.

Una diferencia entre el nivel físico de una red local y los niveles físicos de las redes de área extensa estriba en el hecho de que las primeras pueden tener, y de hecho la mayoría de las redes locales modernas las utilizan, determinadas funciones de control cuya existencia es fundamental para su utilización por el nivel de enlace, caracterizando el nivel físico de la red. Estas funciones de control se generan aplicando al medio físico de comunicación niveles eléctricos o secuencias lógicas especiales (de valor o secuencia diferentes a los correspondientes a la transferencia de información). Estos niveles son diferentes a los establecidos para el formato de bit y la secuencia puede venir dada por un grupo de bits de secuencia prohibida en el formato de bit o por codificaciones especiales.

De esta manera determinadas funciones de control, generadas por el nivel de enlace, se imprimen por el nivel físico en el medio físico con los mencionados formatos especiales de control, lo que establece un servicio de control ya a nivel físico. Como funciones de control que el nivel de enlace o superiores pueden aplicar al nivel físico se encuentran:

- Indicación de presencia o actividad potencial indicando el estado del “driver” activo o preparado para transmitir, esta indicación puede establecerse con codificaciones especiales de señal de sincronización (reloj) sin dato (ni 1 ni 0) o con la transmisión de portadoras sin modulación alguna.
- Indicación de un preámbulo de sincronización, cuando el medio físico de comunicación ha permanecido inactivo por algún tiempo (o al conectarse inicialmente) puede ser necesario establecer una secuencia de control (preámbulo) a partir de la cual se garantiza una sincronización en la transmisión.
- Indicación de inicio o fin de mensajes. Estos controles pueden servir como banderas (*flags*) delimitadoras de un mensaje, indicando el inicio y el fin del mismo (utilizado para conseguir la transparencia de la información).

- Indicación de aborto del mensaje en curso, utilizado para finalizar la transmisión, por alguna razón, cuando un mensaje está aún en curso de servicio.
- Indicación de violación de código, debido a problemas en la transmisión o a colisión entre dos emisores activos simultáneamente.

El nivel físico puede, pues, imprimir o detectar estas indicaciones de control procedentes o dirigidas del nivel de enlace, independizando a éste de las características del medio.

• Estructura del nivel físico

El nivel físico puede estructurarse en dos bloques, de proceso y de adaptación al medio físico de comunicación. El primer bloque, que se encuentra en relación con el nivel de enlace, soporta las funciones de codificación y decodificación de la información y control. El segundo bloque, que se aplica directamente sobre el medio físico de comunicación, soporta la función de la presentación de las codificaciones al medio físico de comunicación. Este segundo bloque está íntimamente ligado al medio físico de comunicación y es totalmente dependiente de la tecnología del mismo.

En las redes locales es recomendable la subdivisión del nivel físico en dos subniveles: el de acople al medio y el de señales físicas. De esta manera se consigue que un cambio de medio de comunicación, por ejemplo, de cable coaxial banda base a coaxial banda ancha no afecte al subnivel de señales físicas.

Desde el punto de vista de la caracterización del medio según su capacidad de comunicación de dispositivos lógicos terminales, un medio puede ser de tal manera que un mensaje transmitido por una estación llegue a todos los receptores de la red (medio *broadcast*) o sólo a un subconjunto. La topología de bus permite realizar transmisiones de un elemento a todos (transmisión *broadcast*) siendo la topología típica (tanto si el medio es cable como radio) para difusión. Si el subconjunto de receptores de red a los que llega el mensaje es unitario, se dice que el medio físico es secuencial. Para que sea posible la interconexión de todos los elementos, estos medios secuenciales siguen formas cerradas en las que se engloban todos los dispositivos (topología de anillo). En esta topología el nivel físico repite al siguiente dispositivo lo que se encuentra presente en su entrada (transmitido por el dispositivo anterior), a excepción de cuando se elimina un mensaje (propio o dirigido a él).

• Codificación - Decodificación

Las funciones de este bloque estructural son:

- La codificación/decodificación de los bits de información transmitidos/recibidos (es decir, el paso de la forma binaria a la forma codificada o viceversa).
- La generación/detección de codificaciones especiales de control correspondientes a la generación/detección de secuencias de sincronización, delimitadores, absorciones por parte del nivel de enlace lógico.

Como codificación/decodificación se utilizan técnicas como las NRZ y NRZI para la transmisión de datos aislados y técnicas como Bifase y Manchester Diferencial para la codificación de datos autosincronizados. La codificación Manchester Diferencial es muy utilizada en las redes locales, ya que ofrece una alta inmunidad frente al ruido, permitiendo la colocación de la información directamente sobre el medio (*baseband*).

La codificación Manchester Diferencial permite una codificación que reúne los bits de información y el reloj de sincronización en un único símbolo. Cada símbolo consta de dos mitades, donde el nivel de una mitad es siempre el complemento al de la otra. Un bit (0) se representa como un cambio de polaridad al inicio del símbolo. Un bit (1) se representa como un símbolo sin cambio inicial de polaridad. De esta manera para cada bit de información se garantiza una transición de la señal (a la mitad del tiempo de bit) por lo que la señal incorpora el reloj de sincronización.

En las transmisiones con código Manchester Diferencial la media de la forma de onda (potencia) es nula, debido a la transición obligatoria a la mitad del símbolo (figura 3.6):

Ninguna de las versiones de Ethernet utiliza codificación directa con 0 voltios para un bit 0 y +5 voltios para un bit 1, pues ello conduce a ambigüedades.

este hecho permite utilizar esta codificación en medios con acoplamientos inductivos, eliminándose la magnetización de los mismos.

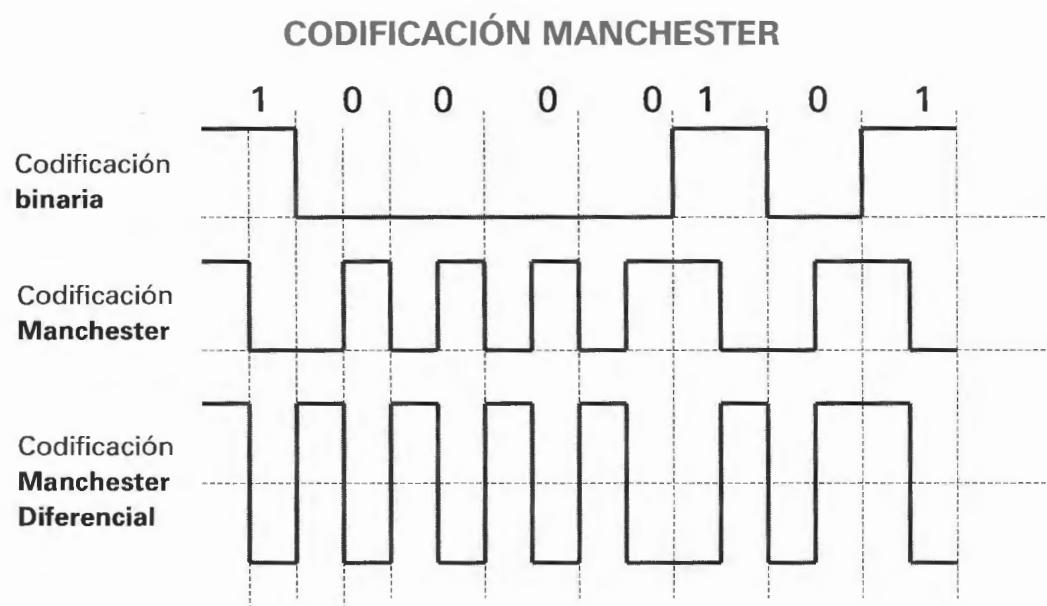


Figura 3.6. Ejemplo de codificación Manchester.

Tras la codificación de la información, ésta puede ser introducida directamente en el medio físico (**baseband**) o modulando una señal portadora en frecuencia (FM), amplitud (AM) o fase (PSK). Esta última técnica permite, sobre un mismo medio, aplicar varias señales de información (**broadband**), cada una de ellas sobre bandas de frecuencia de portadora diferentes, utilizando filtros adecuados en los receptores. La técnica banda base permite únicamente la transmisión de una señal en cada momento, por lo que se utiliza en medios especializados en un canal o en medios multiplexados por división en el tiempo (TDM).

3.6 Nivel de enlace y métodos de acceso

El nivel de enlace, según el modelo OSI, realiza el servicio de enlace de datos, facilitando un canal lógico, independiente del medio físico, para la transmisión de mensajes. De esta manera, corresponde al nivel de enlace el formateado del mensaje (delimitadores, campos de control y direccionamiento, bits de redundancia, campo de información) y la determinación de las acciones a realizar en caso de recepción de un mensaje erróneo.

En el nivel de enlace de las redes de área local, normalmente se añaden dos responsabilidades, no consideradas en las redes de área extensa: el control de acceso al medio y la capacidad de direccionamiento. En las LAN el medio es utilizado por varias comunicaciones, de manera simultánea o por multiplexión por división en el tiempo (TDM), siendo un recurso compartido por los diversos dispositivos lógicos (DTE); así, pues, al decidir el momento de inicio de la transmisión de un mensaje, el nivel de enlace debe seguir una política de acceso al medio. Esto es lo que hace que en las redes de área local el nivel de enlace se subdivida en dos subniveles, el subnivel de control de acceso al medio (MAC) (soportado por el nivel físico) y el subnivel (superior al anterior) de control de enlace lógico propiamente dicho (LLC).

El nivel de enlace (Nivel 2 del modelo OSI) en las redes locales se ha subdividido en dos subniveles:

- **MAC (Media Acces Control) o control del acceso al medio**
- **LLC (Logical Link Control) o control de enlace lógico**

Los objetivos que subyacen, esta decisión de la comisión del IEEE 802 son conseguir que el primer nivel extremo a extremo (LLC) sea independiente de la topología usada en la red local, del medio físico y del método para acceder al mismo. De esta forma, los posibles cambios de red local y de tecnología del medio no implicarán modificaciones en el protocolo de control de enlace.

La principal función de la subcapa MAC, como se ha mencionado, consiste en determinar quién tiene derecho a acceder al canal de comunicación, que ha de ser compartido por todos los usuarios conectados a la red de área local. La función de la subcapa LLC es la agrupación de los bits en tramas, direccionamiento y determinación de si las tramas recibidas son correctas. Ambas subcapas se relacionan con la capa 2 –Enlace– del modelo OSI (figura 3.7).

OSI Y LOS ESTÁNDARES DEL IEEE PARA REDES LOCALES

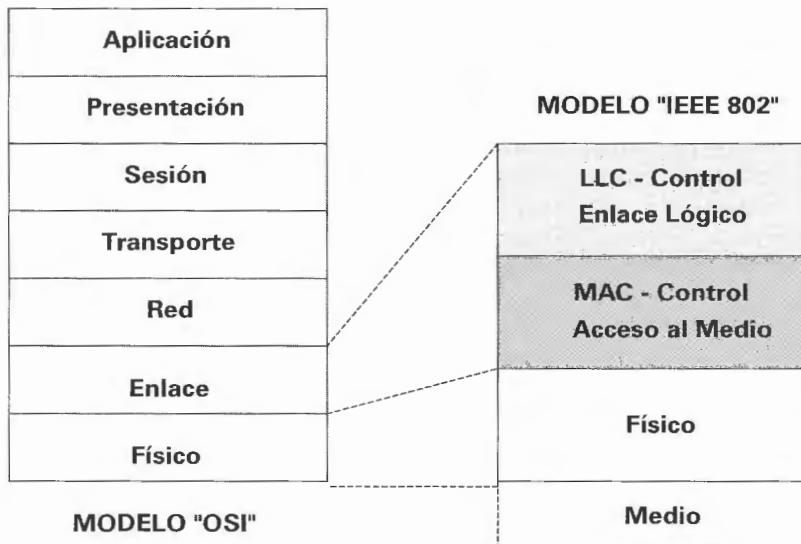


Figura 3.7. Relación de la capa de Enlace de OSI con las subcapas MAC y LLC.

3.6.1. El subnivel MAC

El subnivel de control de acceso al medio (MAC) es el responsable de ejercer la política que en virtud del estado de la red permite o no acceder al medio. De esta manera, el subnivel MAC facilita al subnivel de control de enlace lógico (LLC) un medio de comunicación “aparentemente” propio. El subnivel MAC es dependiente de la topología del medio, puesto que ésta influye en la política de acceso, facilitando al LLC y superiores un servicio independiente totalmente del medio (tanto topológica como tecnológicamente).

El subnivel MAC participa además en el formato del mensaje de dos maneras:

- Inserta los delimitadores (de inicio, DI y de fin, DF) del mensaje.
- Añade campos orientados al control del acceso (CA).

De esta manera, se consigue que el servicio ofrecido al subnivel LLC sea independiente del medio y del tipo de política de acceso.

Se denomina unidad de datos de protocolo (PDU) de un nivel, como vimos al principio al hablar de la terminología empleada en OSI, al conjunto de datos que dicho nivel transfiere al nivel análogo del dispositivo terminal (DTE) destino. Así, la unidad de datos de protocolo transferida por el nivel físico (NF) está formada por los delimitadores, un campo (opcional) de control al acceso y la unidad de datos de servicio del subnivel de control de acceso al medio (MAC).

$\text{<PDU-NF>} = \text{<delimitador>} \text{ <AC>} \text{ <SDU-MAC>} \text{ <delimitador>}$

Los métodos de acceso al medio (MAC) más utilizados en las redes de área local son dos, el método de acceso múltiple con detección de actividad y colisión (CSMA/CD/

*Carrier Sense Multiple Access/Collision Detect) y el método de acceso por paso de testigo (*token passing*), que vamos a estudiar seguidamente.*

3.6.2. El método CSMA/CD

- **CSMA/CD (*Carrier Sense Multiple Access/Collision Detection o Acceso múltiple con escucha de portadora y detección de colisión*).** Es el protocolo de acceso al medio que utilizan las redes Ethernet (las más implantadas en el mundo empresarial, con casi el 100% del mercado) que dispone de una topología lógica de bus (figura 3.8). Esto significa que la red puede estar físicamente dispuesta en bus o en estrella pero su configuración a nivel funcional es el de un medio físico compartido por todos los terminales.

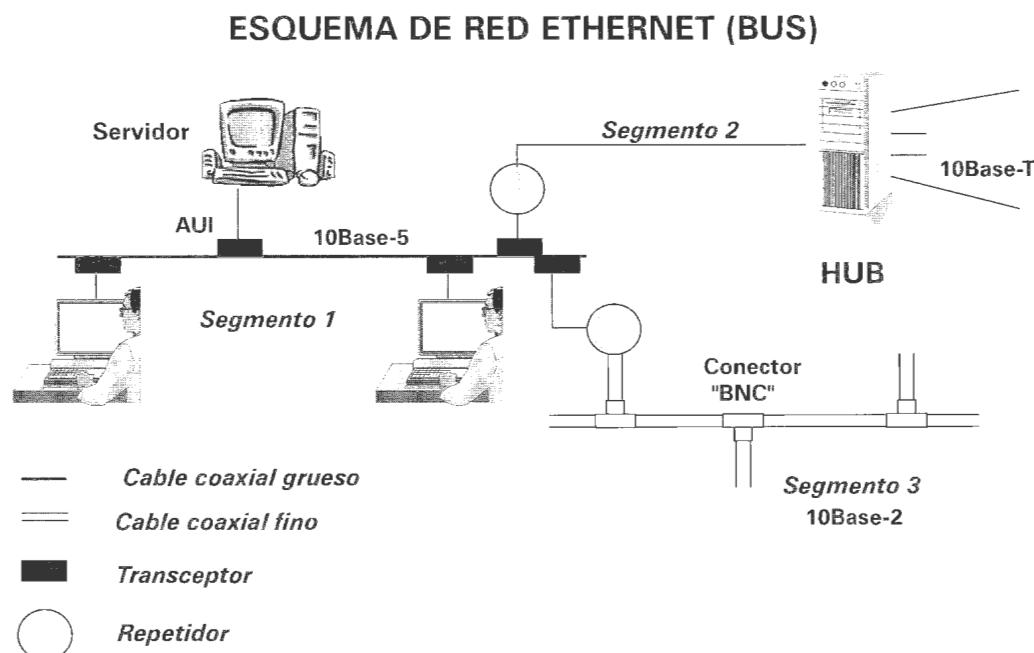


Figura 3.8. Red local Ethernet con topología en bus.

Este método (contienda) es aplicable en medios *broadcast* y destacan, como principales características, su elevada eficacia (sobre todo en utilizaciones medias y bajas), la flexibilidad de conexionado y facilidad de añadir o quitar estaciones en la red, bajo retardo (aunque no acotable determinísticamente) y la ausencia de establecimientos físicos o lógicos al conectarse en red una estación. Los medios y adaptadores al medio deben tener capacidad de detectar actividad (CS) y colisiones (CD).

El método CSMA/CD es el que se emplea en las redes Ethernet, las más ampliamente utilizadas, según el estándar IEEE802.3.

Su funcionamiento es simple: antes de transmitir un ordenador, éste “escucha” el medio de transmisión que comparten todos los terminales conectados para comprobar si existe una comunicación. Esta precaución se toma para que la posible transmisión que se esté realizando en ese momento no sea interferida por otra que quiera transmitir a continuación (figura 3.9). Si no detecta ninguna comunicación, se pondrá a transmitir y en caso contrario esperará un tiempo aleatorio antes de comenzar de nuevo el proceso. En el caso de que dos o más ordenadores transmitan al mismo tiempo se produce una *colisión*, es decir, las señales se interfieren mutuamente quedando inservibles para su correcta recepción por sus respectivos destinatarios. Al estar escuchando una señal ininteligible, los terminales implicados en la colisión cortan la transmisión que están realizando para, a continuación, transmitir una secuencia especial de bits, llamada señal de atasco, cuya misión es garantizar que la colisión dure lo suficiente para que la detecten el resto de terminales de la red. Esta señal tiene más de 32 bit pero menos de 48 bits con el objeto de que los ordenadores conectados a la red puedan interpretar que es un fragmento resultante de una colisión. Las estaciones descartarán cualquier trama que contenga menos de 64 octetos (bytes).

PROCESO DE COLISIÓN EN CSMA/CD

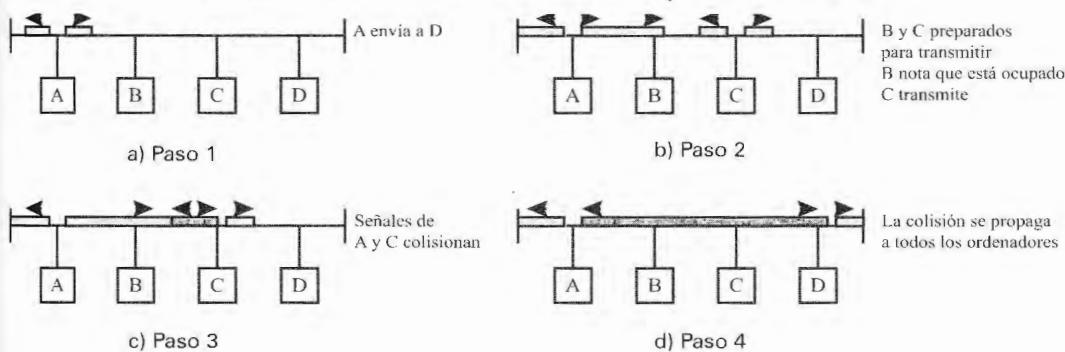


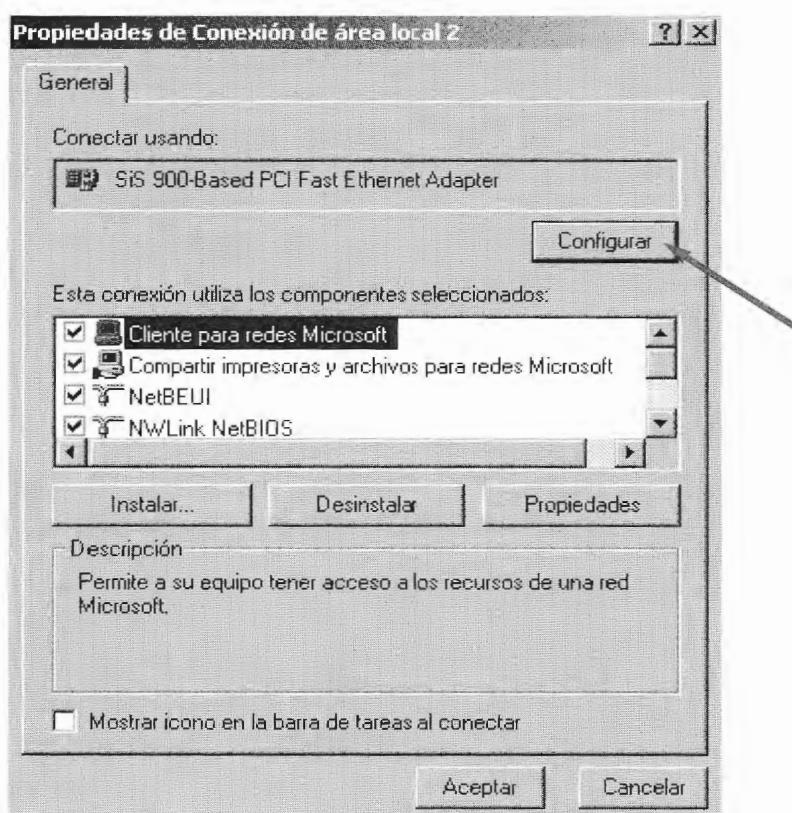
Figura 3.9. Proceso de una colisión en una red en bus.

Este método de acceso al canal es adecuado para redes que soporten aplicaciones que generan un bajo tráfico en la red (como es el caso de las aplicaciones ofimáticas) debido a que si el tráfico generado por cada estación es elevado, la probabilidad de que existan colisiones es elevada. En estas condiciones, una estación puede estar esperando a transmitir un tiempo indeterminado (no garantiza tiempos de espera máximos) por lo que la técnica CSMA/CD no resulta adecuada para soportar aplicaciones de proceso en tiempo real (control de procesos industriales, transmisión de voz y vídeo, etc.).

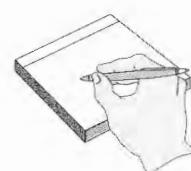
Compruébese la configuración del adaptador de red y selecciónese una velocidad de transmisión automática.

SOLUCIÓN

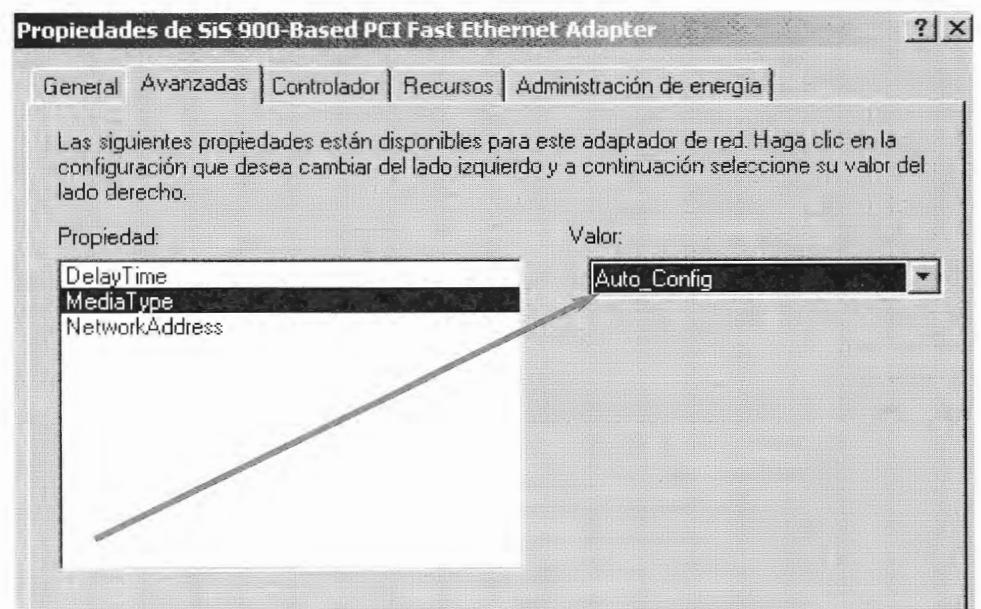
En la opción de propiedades de “Mis sitios de red”, se seleccionan las propiedades del adaptador:



Ejercicio Resuelto 3.4



A continuación se comprueba la velocidad y se selecciona la configuración automática:



3.6.3. El método Paso de Testigo

- **Token Passing (Paso de testigo).** Este método de acceso se utiliza en diferentes redes (con pequeñas variantes) que disponen de un anillo lógico: Token Ring, Token Bus y FDDI. Al contrario que el método anterior, éste se comporta de manera determinística, es decir, que un terminal de la red puede transmitir en un intervalo de tiempo fijado.

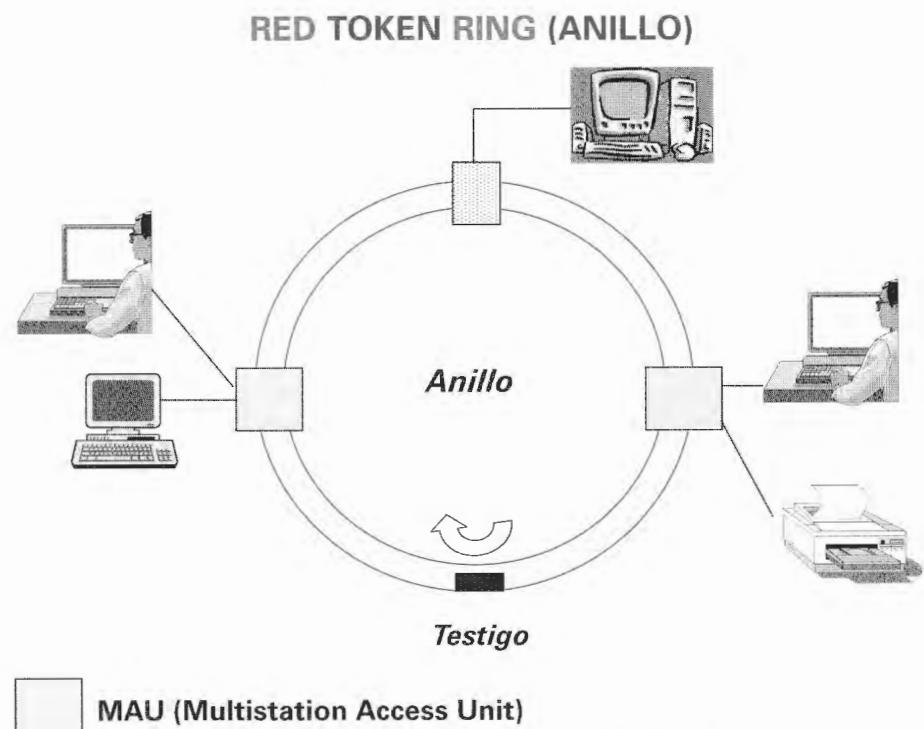


Figura 3.10. Red local en anillo con acceso controlado (Token Ring).

Con este método (selección), únicamente tiene derecho a utilizar el medio momentáneamente la estación –en cada momento sólo una– que dispone del testigo (con frecuencia el testigo suele ser un byte formado por ejemplo por 8 unos –11111111–, y se utilizan técnicas de relleno de bit para evitar que esta secuencia aparezca en un mensaje), resolviéndose de esta manera el problema de la congestión del acceso; dentro de la política se establece que el testigo vaya pasando de manera secuencial de una estación a otra, controlando a su vez el tiempo máximo de pertenencia, dando de esta manera posibilidad a todas las estaciones de hacer uso del medio (formando un anillo lógico).

El método de paso de testigo se vale de una trama especial o *testigo (token)*, que va a ser monitorizado por cada ordenador, para dar a éstos permiso o no de transmisión. En definitiva, los ordenadores conectados al anillo lógico no pueden transmitir los datos hasta que no obtienen el permiso de hacerlo.

Si el testigo está libre (no existe ninguna estación que esté transmitiendo), cualquier ordenador que tenga necesidad de transmitir pasará el testigo al estado de ocupado e iniciará la comunicación insertando los datos detrás del testigo. En este momento el propietario del testigo es la estación que está transmitiendo, siendo esta la que dispone del control absoluto del anillo. La trama resultante pasará por cada terminal, regenerándose, en el camino hacia el terminal destinatario de los datos.

Una vez la trama ha llegado al ordenador destino, se copia en la memoria de éste pasando a retransmitir la trama sobre la red cambiando una serie de bits de forma que el ordenador que envió la información comprueba que el terminal destino la recibió correctamente. De ser éste el caso, el terminal se encarga de liberar el testigo, de manera que otros ordenadores puedan realizar sus comunicaciones. En el caso de que el terminal destino no hubiera recibido correctamente la trama, el terminal origen de la comunicación la volvería a transmitir.

Este tipo de método de acceso es adecuado para las empresas que necesiten tener aplicaciones que exijan un volumen de tráfico elevado y uniforme en la red (multimedia, CAD, autoedición, etc.).

En resumen, sus principales características, son:

- Es un método aplicable tanto en medios *broadcast* como secuencial, aunque entre las políticas en ambos medios hay algunas diferencias.
- Durante el periodo de pertenencia del testigo no se prescribe que un subconjunto de estaciones no pueda hacer uso de otras técnicas (*polling*, CSMA/CD entre otras) de acceso al medio.
- Responde igualmente bien tanto en situaciones de carga elevada como en situaciones de baja utilización.
- Proporciona un reparto equitativo de la capacidad del medio.
- El retardo máximo en el acceso puede ser acotado determinísticamente (el tiempo máximo de pertenencia del testigo (*token*) multiplicado por el número de estaciones).
- El costo de los nodos (adaptadores al medio) a utilizar es bajo debido a la sencillez de los mismos.

3.6.4. Control del enlace lógico (LLC)

Esta subcapa, en colaboración con la otra (MAC), se encarga de garantizar la comunicación, entre emisor y receptor, sin errores de las tramas construidas con la información recibida del nivel de red. Proporciona tres tipos de servicios:

- Servicio sin conexión y sin confirmación.
- Servicio sin conexión y con confirmación.
- Servicio con conexión.

En los dos primeros servicios se envían las tramas sin haber establecido una conexión previa entre emisor y receptor, lo que se llama “servicio no orientado a conexión”. En



uno y otro caso si se produce algún error son las capas superiores o mediante retransmisión como se corrige. Estos servicios son adecuados para redes locales con una tasa de errores muy baja.

- **Servicio no orientado a conexión (CLS/Connection Less Service).** La forma en que entidades de la red pueden intercambiar unidades de datos de servicio de enlace sin necesidad de establecer previamente una conexión de enlace de datos.

En el tercer servicio, se establece, previamente al envío de las tramas, una conexión entre emisor y receptor (servicio orientado a conexión).

- **Servicio orientado a conexión (COS/Connection Oriented Service).** Conjunto de servicios por los cuales las entidades de la red, establecen, usan y finalizan conexiones de datos de enlace. En este servicio sólo son posibles conexiones punto a punto.

Funcionalidad

La funcionalidad del subnivel de enlace lógico de una red de área local es similar a la funcionalidad del nivel lógico de las redes de área extensa a excepción de la capacidad de direccionamiento del mensaje, que en las LAN recae en este nivel.

La responsabilidad del subnivel LLC es, pues, transferir la unidad de servicio de datos correspondiente al subnivel (o subniveles) de enlace lógico del DTE destino (o destinos) sin errores. Para ello formatea la unidad de servicio de datos (SDU) con:

- Un campo de dirección (CDIR), para determinar el destino o destinos del mensaje.
- Un campo de control (CC), para indicar el tipo de mensaje o realizar un control de flujo.
- Y finalmente un campo de bits de redundancia cíclica (CRC) para detección de errores de transmisión, del mensaje de nivel de enlace lógico. El formato de un mensaje del nivel de enlace lógico es:

`<CDIR> <CC> <SDU_LLC> <CRC>`

En caso de recepción errónea del mensaje en destino, se corrige el error con una retransmisión. Los mensajes del subnivel LLC incorporan un conjunto de bits redundantes (código cíclico, normalmente de 32 bits) que permite con una elevada fiabilidad detectar errores en la transmisión. Obsérvese que ni los delimitadores ni el campo de control de acceso quedan cubiertos por este código cíclico que sólo afecta a los campos `<CDIR> <CC> <SDU_LLC>`. Cuando se detecta un error de transmisión se puede recuperar mediante una petición de retransmisión (ARQ), como se realiza normalmente en los protocolos de nivel de enlace.

Con el subnivel LLC son posibles tres tipos de direccionamiento:

- **Individual**, en donde el destinatario es único.
- **Grupo**, en donde el destinatario es un subconjunto de las estaciones de la red.
- **Broadcast**, en donde todas las estaciones de la red son destino.

3.7 WLAN

Una WLAN (*Wireless LAN*) es un sistema de comunicaciones de datos que transmite y recibe datos utilizando ondas electromagnéticas, en lugar del par trenzado, coaxial o fibra óptica utilizados en las LAN convencionales, y que proporciona conectividad inalámbrica dentro de un edificio, de una pequeña área residencial/urbana o de un campus universitario. En EEUU proliferan estas redes para acceso a Internet, en donde hay más de 4.000 zonas de acceso, y en Europa es previsible que pronto se extiendan.

Las WLAN se encuadran dentro de los estándares desarrollados por el IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) para redes locales inalámbricas. Otras tecnologías como HyperLAN apoyada por el ETSI, y el nuevo estándar HomeRF para el

hogar, también pretenden acercarnos a un mundo sin cables y, en algunos casos, son capaces de operar en conjunción y sin interferirse entre sí. Otro aspecto a destacar es la integración de las WLAN en entornos de redes móviles de 3G (UMTS) para cubrir las zonas de alta concentración de usuarios (los denominados *hot spots*), como solución de acceso público a la red de comunicaciones móviles.

Como todos los estándares 802 para redes locales del IEEE, en el caso de las WLAN, también se centran en los dos niveles inferiores del modelo OSI, el físico y el de enlace, por lo que es posible correr por encima cualquier protocolo (TCP/IP o cualquier otro) o aplicación, soportando los sistemas operativos de red habituales, lo que supone una gran ventaja para los usuarios que pueden seguir utilizando sus aplicaciones habituales, con independencia del medio empleado, sea por red de cable o por radio.

Otra tecnología de acceso inalámbrico en áreas de pequeña extensión (*WPAN/WLAN Personal Area Network*) es la denominada Bluetooth, que aunque pueda parecer competencia directa de las WLAN, es más bien complementaria a ella. Bluetooth pretende la eliminación de cables, como por ejemplo todos los que se utilizan para conectar el PC con sus periféricos, o proporcionar un medio de enlace entre dispositivos situados a muy pocos metros, sirviendo también como mando a distancia.

Las WLAN tienen su campo de aplicación específico, igual que Bluetooth, y ambas tecnologías pueden coexistir en un mismo entorno sin interferirse gracias a los métodos de salto de frecuencia que emplean. Sus aplicaciones van en aumento y, conforme su precio se vaya reduciendo, serán más y más los usuarios que las utilicen, por las innegables ventajas que supone su rápida implantación y la libertad de movimientos que permiten.

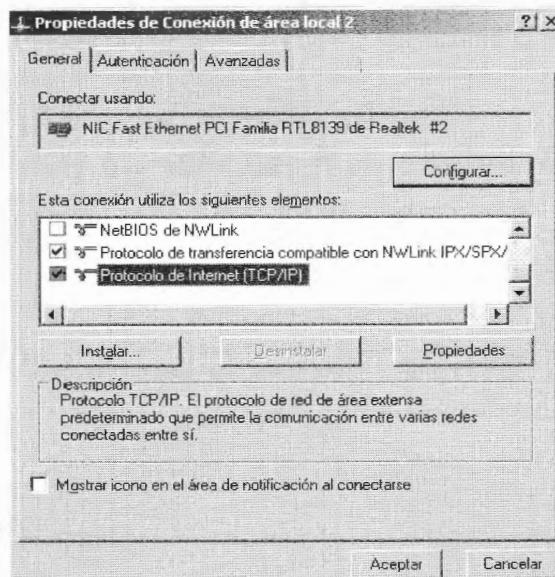
Los WLAN pueden ser de corto alcance, como las 802.11 (Wi-Fi) o de largo como las 802.16 (WiMAX).

Compruébese el protocolo de comunicaciones de una conexión mediante red local a Internet.

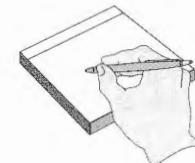
SOLUCIÓN

Las comunicaciones por Internet están basadas en el protocolo TCP/IP. Existen varias formas de comprobarlo. Por ejemplo, ejecutando la aplicación *ipconfig* o *ipconfig/all*.

También se puede comprobar analizando las propiedades de la red, desde el mismo escritorio o desde el panel de control:



Ejercicio Resuelto 3.5



Se comprueba la dirección IP. Puede ser automática, generada por un servidor DHCP o indicada por el propio usuario. De igual manera se tiene en la configuración de la puerta de enlace y de la configuración de los servidores DNS.

3.7.1. Redes locales inalámbricas 802.11

El origen de las LAN inalámbricas (WLAN) se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados por el IEEE, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

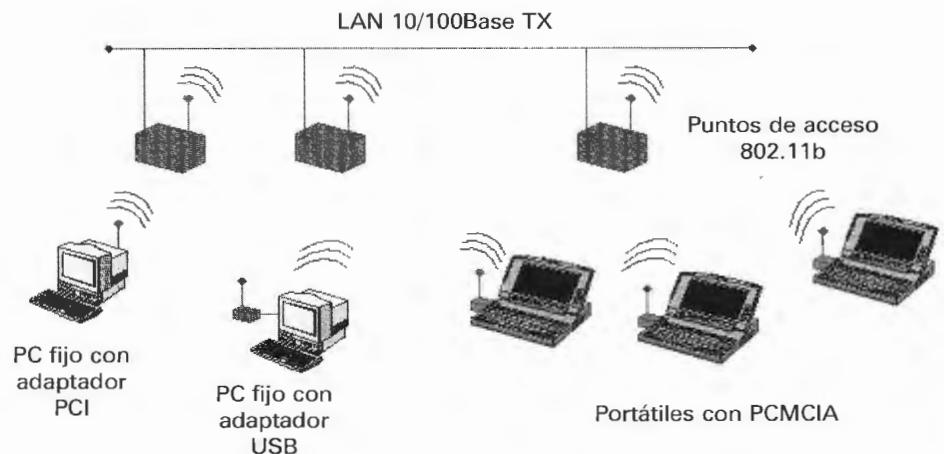


Figura 3.11. Esquema de una Wireless LAN.

Las bandas de frecuencias y servicios asociados se recogen en el CNAF (Cuadro Nacional de Asignación de Frecuencias) que edita la SETSI (Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información) del MITyC.

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas, donde se utilizaba el esquema de espectro expandido (*spread spectrum*). En mayo de 1985, y tras cuatro años de estudios, la FCC (*Federal Communications Commission*), la agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas ISM (*Industrial, Scientific and Medical*) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz para uso en las redes inalámbricas basadas en *Spread Spectrum* (SS), con las opciones DS (*Direct Sequence*) y FH (*Frequency Hopping*). En Europa, la banda de 5 GHz que reutiliza, según el CNAF (Cuadro Nacional de Asignación de Frecuencias) es distinta, y abarca desde 5,150 GHz hasta 5,725 GHz. En la figura 3.12 se pueden apreciar las bandas que contempla ISM.

La técnica de espectro ensanchado es una técnica de modulación que resulta ideal para las comunicaciones de datos, ya que es muy poco susceptible al ruido y crea muy pocas interferencias. La asignación de esta banda de frecuencias propició una mayor actividad en el seno de la industria y ese respaldo hizo que las WLAN empezaran a dejar ya el entorno del laboratorio para iniciar el camino hacia el mercado.

ISM. Bandas de Frecuencia sin Licencia

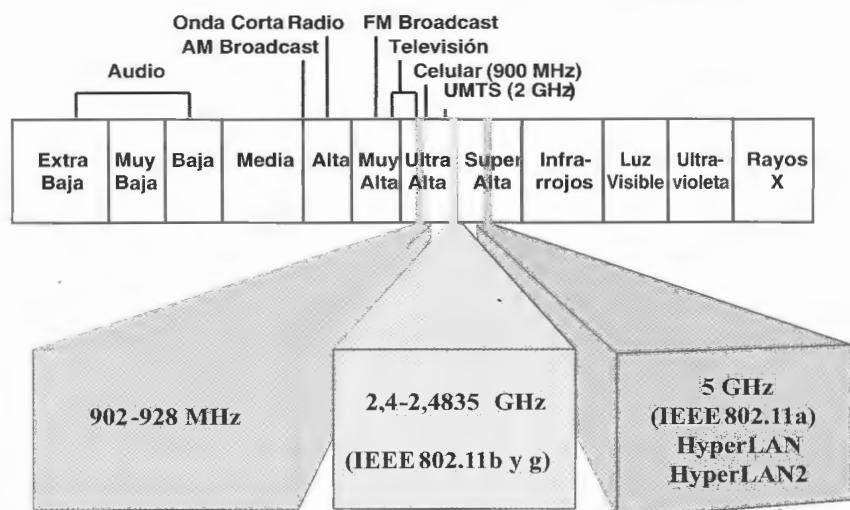


Figura 3.12. Bandas de frecuencia (ISM) que no requieren licencia (de uso común).

Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbit/s, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN, con aplicación empresarial.

Las redes WLAN se componen fundamentalmente de dos tipos de elementos, los puntos de acceso y los dispositivos de cliente. Los puntos de acceso actúan como un concentrador o hub que reciben y envían información vía radio a los dispositivos de clientes, que pueden ser de cualquier tipo, habitualmente, un PC o PDA con una tarjeta de red inalámbrica, con o sin antena, que se instala en uno de los slots libres o bien se enlazan a los puertos USB de los equipos.

La principal ventaja de este tipo de redes (WLAN), que no necesitan licencia para su instalación, es la libertad de movimientos que permite a sus usuarios, ya que la posibilidad de conexión sin hilos entre diferentes dispositivos elimina la necesidad de compartir un espacio físico común y soluciona las necesidades de los usuarios que requieren tener disponible la información en todos los lugares por donde puedan estar trabajando. Además, a esto se añade la ventaja de que son mucho más sencillas de instalar que las redes de cable y permiten la fácil reubicación de los terminales en caso necesario.

También presentan alguna desventaja, o más bien inconveniente, que es el hecho de la "baja" velocidad que alcanzan, por lo que su éxito comercial es más bien escaso y, hasta que los nuevos estándares no permitan un incremento significativo, no es de prever su uso masivo, ya que por ahora no pueden competir con las LAN basadas en cable.

El uso más popular de las WLAN implica la utilización de tarjetas de red inalámbricas, cuya función es permitir al usuario conectarse a la LAN empresarial sin la necesidad de una interfaz física.

3.7.2. Normalización IEEE

La historia de las WLAN es bastante reciente, de poco más de una década. En 1989, en el seno de IEEE 802, se forma el comité IEEE 802.11, que empieza a trabajar para tratar de generar una norma para las WLAN, pero no es hasta 1994 cuando aparece el primer borrador, y habría que esperar hasta el año 1999 para dar por finalizada la norma.



Figura 3.13. Estándares del IEEE para WLAN.

En 1992 se crea Winforum, consorcio liderado por Apple y formado por empresas del sector de las telecomunicaciones y de la informática para conseguir bandas de frecuencia para los sistemas PCS (*Personal Communications Systems*). En 1993 también se constituye la IrDA (*Infrared Data Association*) para promover el desarrollo de las WLAN basadas en enlaces por infrarrojos. En 1996, finalmente, un grupo de empresas del sector de informática móvil (*mobile computing*) y de servicios forman el *Wireless LAN Interoperability Forum* (WLI Forum) para potenciar este mercado mediante la creación de un amplio abanico de productos y servicios interoperativos. Por otra parte, WLANA (*Wireless LAN Association*) es una asociación de industrias y empresas cuya misión es ayudar y fomentar el crecimiento de la industria WLAN a través de la educación y promoción.

Actualmente son cuatro los estándares reconocidos dentro de esta familia; en concreto, la especificación 802.11 original; 802.11a (evolución a 802.11 e/h), que define una conexión de alta velocidad; 802.11b, el que goza de una más amplia aceptación y que aumenta la tasa de transmisión de datos propia de 802.11 original, y 802.11g, compatible con él, pero que proporciona aún mayores velocidades.

• WLAN 802.11

En junio de 1997 el IEEE ratificó el estándar para WLAN IEEE 802.11, que alcanzaba una velocidad de 2 Mbit/s, con una modulación de señal de espectro expandido por secuencia directa (DSSS), aunque también contempla la opción de espectro expandido por salto de frecuencia, FHSS en la banda de 2,4 GHz, y se definió el funcionamiento y la interoperabilidad entre redes inalámbricas.

El 802.11 es una red local inalámbrica que usa la transmisión por radio en la banda de 2,4 GHz, o infrarroja, con regímenes binarios de 1 a 2 Mbit/s. El método de acceso al medio **MAC** (*Medium Access Mechanism*) es mediante escucha pero sin detección de colisión, **CSMA/CA** (*Carrier Sense Multiple Access with Collision Avoidance*).

La dificultad en detectar la portadora en el acceso WLAN consiste básicamente en que la tecnología utilizada es *Spread-Spectrum* y con acceso por división de código (CDMA), lo que conlleva a que el medio radioeléctrico es compartido, ya sea por secuencia directa DSSS o por saltos de frecuencia en FHSS. El acceso por código CDMA implica que pueden coexistir dos señales en el mismo espectro utilizando códigos diferentes, y eso para un receptor de radio implicaría que detectaría la portadora inclusive con señales distintas de las de la propia red WLAN. Hay que mencionar que la banda de 2,4 GHz está reglamentada como banda de acceso pública y en ella funcionan gran cantidad de sistemas, entre los que se incluyen los teléfonos inalámbricos Bluetooth.

• WLAN 802.11b (Wi-Fi)

Los estándares 802.11 se identifican con Wi-Fi.

En el año 1999 se aprobó el estándar 802.11b, una extensión del 802.11 para WLAN empresariales, con una velocidad de 11 Mbit/s (otras velocidades normalizadas a nivel físico son: 5,5 - 2 y 1 Mbit/s) y un alcance que puede llegar a superar los 100 metros con una potencia de emisión de 100 mW (la potencia máxima, PIRE, admitida en interiores es de 200 mW), que al igual que Bluetooth y Home RF, también emplea la banda de ISM de 2,4 GHz, pero en lugar de una simple modulación de radio digital y salto de frecuencia (FH/*Frequency Hopping*), utiliza una modulación lineal compleja (DSSS). Permite mayor velocidad, pero presenta una menor seguridad, y el alcance puede llegar a los 100 metros, suficientes para un entorno de oficina o residencial.

La potencia PIRE (Potencia Isotrópica Radiada Equivalente) es la suma de la potencia del equipo transmisor (en dBm), más la ganancia de la antena (dBi), menos las pérdidas del cable (en dB), así que conviene que éste sea lo más corto posible, para radiar con la máxima potencia posible y así tener mayor alcance o velocidad.

Por ejemplo, un transmisor de 20 dBm utilizando un cable de 15 metros (pérdidas de 3,3 dB y una antena de 21 dBi, da una PIRE de 37,7 dBm (20-3,3+21).

Cobertura vs Velocidad (100 mW)

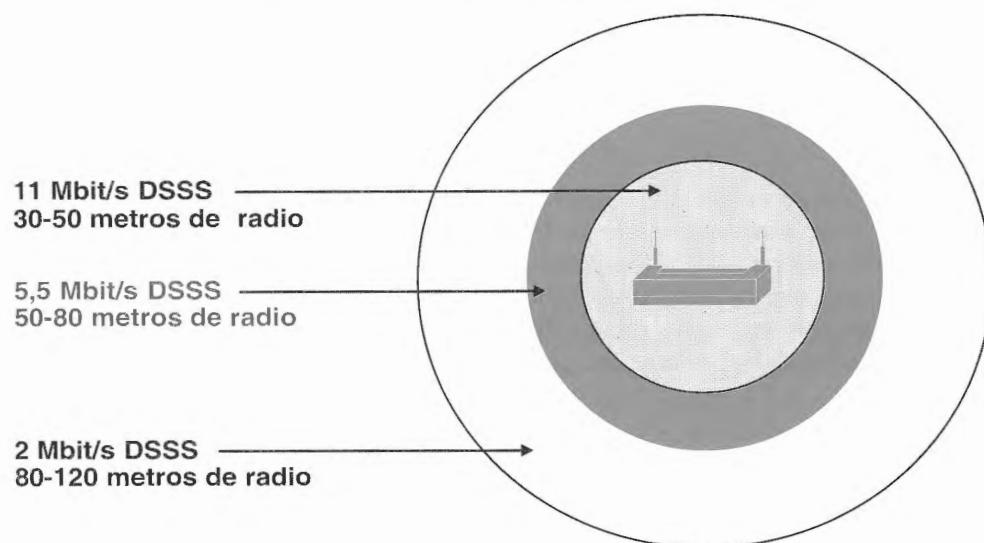


Figura 3.14. En las WLAN existe un compromiso entre alcance y velocidad.

PIRE. Potencia Isotrópica Radiada Equivalente

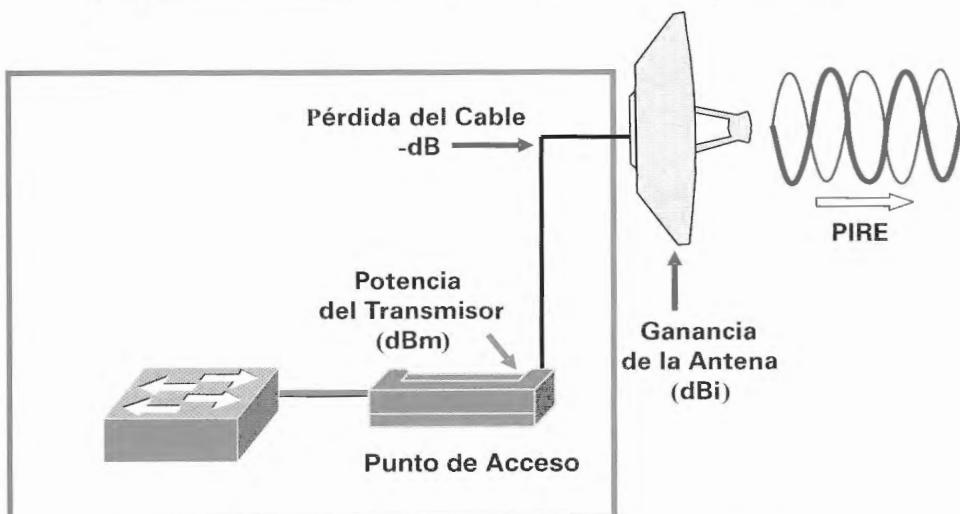


Figura 3.15. En un sistema WLAN la potencia depende del conjunto de elementos.

En la tabla de la figura 3.16 se puede ver la relación (aproximada) entre dBm y mW.

(dBm)	mW	(dBm)	mW	(dBm)	mW
0	1	11	12.5	21	128
1	1,25	12	16	22	160
2	1,56	13	20	23	200
3	2	14	25	24	256
4	2,5	15	32	25	320
5	3,12	16	40	26	400
6	4	17	50	27	512
7	5	18	64	28	640
8	6,25	19	80	29	800
9	8	20	100	30	1.000
10	10				

Figura 3.16. Equivalencia aproximada entre dBm y mW.

Para garantizar las prestaciones de los equipos y no producir interferencias en otros, no se deben modificar las características que indica el fabricante ni hacerlos funcionar "fuera de márgenes".

Nota. Un incremento o reducción de 3 dB significa aumentar la potencia al doble o reducirla a la mitad, mientras que añadir o quitar 10 dB significa multiplicarla o dividirla por 10, respectivamente.

» WLAN 802.11g

El IEEE aprobó en el año 2003 en el estándar 802.11g, compatible con el 802.11b ya que ambos utilizan la misma banda de frecuencias, capaz de alcanzar una velocidad de 54 Mbit/s, para competir con los otros estándares que prometen velocidades mucho más elevadas pero que no son compatibles con los equipos 802.11b ya instalados, aunque pueden coexistir en el mismo entorno debido a que las bandas de frecuencias que emplean son distintas. Por extensión, también se le llama Wi-Fi.

» WLAN 802.11a

El IEEE ratificó en julio de 1999 el estándar en 802.11a, que con una modulación QAM-64 y la codificación OFDM (*Orthogonal Frequency Division Multiplexing*) alcanza una velocidad de hasta 54 Mbit/s en la banda de 5 GHz, menos congestionada y, por ahora, con menos interferencias, pero con un alcance limitado a 50 metros, lo que implica tener que montar más puntos de acceso (*Access Points*) que si se utilizase 802.11b para cubrir el mismo área, con el coste adicional que ello supone.

En las frecuencias autorizadas para uso común la potencia de emisión (PIRE) en interiores no debe sobrepasar los 200 mW, mientras que en exteriores puede llegar hasta 1 wattio.

3.7.3. WEP. Compatibilidad y seguridad

A finales de la década de los 90, los líderes de la industria inalámbrica (3Com, Aironet, Lucent, Nokia, etc.) crearon la WECA (*Wireless Ethernet Compatibility Alliance*), una alianza para la Compatibilidad Ethernet Inalámbrica, cuya misión es la de certificar la interfuncionalidad y compatibilidad de los productos de redes inalámbricas 802.11b y promover este estándar para la empresa y el hogar. Para indicar la compatibilidad entre dispositivos inalámbricos, tarjetas de red o puntos de acceso de cualquier fabricante, se les incorpora el logo "Wi-Fi" (estándar de Fidelidad Inalámbrica), y así los equipos con esta marca, soportada por más de 150 empresas, se pueden incorporar en las redes sin ningún problema, siendo incluso posible la incorporación de terminales telefónicos Wi-Fi a estas redes para establecer llamadas de voz.

Las redes inalámbricas son inseguras aunque sólo sea porque el medio de transporte que emplean es el aire; por tanto, un elemento esencial a tener en cuenta en este tipo de redes al utilizarse la radio, es la encriptación. En general se utiliza WEP (*Wired Equivalent Privacy*), que es un mecanismo de encriptación y autenticación especificado en el estándar IEEE 802.11 para garantizar la seguridad de las comunicaciones entre los usuarios y los puntos de acceso. La clave de acceso estándar es de 40 bits, pero existe otra opcional de 128 bits, y se asigna de forma estática o manual (no dinámica), tanto para los clientes, que comparten todos el mismo conjunto de cuatro claves predeterminadas, como para los puntos de acceso a la red, lo que genera algunas dudas sobre su eficacia. WEP utiliza un esquema de cifrado simétrico en el que la misma clave y algoritmo se utilizan tanto para el cifrado de los datos como para su descifrado.

Antes de la aprobación, a mediados del año 2004 del nuevo estándar 802.11i, con el fin de resolver el tema de la seguridad se lanzó la certificación WPA, aunque algunos expertos consideran que ésta es sólo una solución momentánea que puede llevar a error ya que puede crear en el usuario una sensación de seguridad que este estándar no ofrece.

Otro mecanismo de seguridad definido en el estándar IEE 802.11 es el conocido como SSID (*Service Set Identifiers*) o identificadores del conjunto de servicios, que es como un gestor de asignación de nombres, que proporciona un control de acceso muy rudimentario, razón por la que apenas se utiliza en las implementaciones comerciales.

Con el nuevo estándar, el 802.11i, recientemente aprobado, la seguridad se ve muy mejorada, al introducir claves dinámicas y aumentar su tamaño. Sin embargo, otros usuarios prefieren adquirir soluciones *wireless* convencionales y potenciar la seguridad con tecnología de otros fabricantes especializados en seguridad móvil en lugar de soluciones que incluyan la certificación WPA.

3.8 Protocolos de las LAN

Tomando como referencia el modelo OSI, los protocolos situados por encima del nivel de enlace que se disponen en una LAN no están normalizados por el IEEE ni por ningún otro organismo. De esta forma, los fabricantes han diseñado sus propios protocolos. Por ejemplo, Novell ha creado los protocolos siguientes: IPX para el nivel de red, SPX para el nivel de transporte y NCP implementa los niveles de sesión, presentación y aplicación.

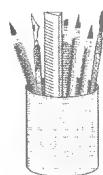
La función de este tipo de protocolos es equivalente a la que ofrecen los protocolos del modelo OSI. Dentro de los protocolos más extendidos en las empresas se destacan los mencionados de Novell para sus redes NetWare y los creados por el Departamento de Defensa de Estados Unidos para su red ARPANET, la precursora de la actual Internet: TCP/IP, que se ha convertido en el estándar de facto para todo tipo de aplicaciones.

La mayor diferencia entre estos dos estándares “de facto” es que en un entorno NetWare los servidores y los clientes son dedicados (de ficheros, de aplicaciones, de impresión, etc.). Los servidores de Novell NetWare no funcionan como clientes y los clientes no funcionan como servidores. En un entorno TCP/IP, los ordenadores pueden ser servidores, clientes o clientes y servidores a la vez. Existen, además, otras diferencias entre estas dos arquitecturas de comunicaciones ya que fueron desarrolladas para dos entornos muy diferentes.

Según el protocolo, se empleará una u otra técnica (contienda o selección) de acceso al medio, ya que la red de área local es un recurso compartido. Las técnicas basadas en una estrategia de contienda, aunque mucho más adecuadas para demandas a ráfagas, resultan con frecuencia más complejas de controlar ya que la asignación de recursos varía con el tiempo, por actuar bajo criterios de demanda. Son técnicas de asignación dinámicas a diferencia de las de selección que son fijas o estáticas.

El problema de acceso a un recurso informático en un sistema de procesamiento distribuido, o el de comunicación entre sistemas distintos conectados a través de una LAN, es básicamente un problema de acceso y utilización de un recurso de comunicaciones. Ya que el tráfico a que se destinan las redes locales suele ser un tráfico a ráfagas, las técnicas más eficientes suelen ser las de contienda. Para un número de usuarios reducido, puede no estar justificado el mayor rendimiento que se obtiene en el uso del recurso con las técnicas de contienda frente a la mayor sencillez de las técnicas de selección.

Debe considerarse, además, que en las técnicas de selección, aunque puedan producirse grandes retardos en obtener todo el servicio solicitado, el acceso al recurso es determinístico y el tiempo de espera máximo está acotado y es conocido. En las de contienda el acceso es aleatorio. El tiempo de espera depende de la carga del sistema y puede llegar a ser muy grande al no estar acotado. Sin embargo, la probabilidad de que esto ocurra en un sistema adecuadamente dimensionado es muy pequeña.



Ejercicios propuestos

- 3.1** Explicar el modelo de referencia OSI de ISO, describiendo la función de cada uno de sus niveles y la relación entre ellos.
- 3.2** Describir las distintas Unidades de Datos que se manejan en el modelo OSI.
- 3.3** Dibujar un diagrama explicativo de los conceptos: capa, interfaz, protocolo, primitiva y servicio en la arquitectura de red, según el modelo OSI.
- 3.4** Clasificar los niveles OSI en función de que estén orientados a red o a la aplicación.
- 3.5** Establecer una comparativa entre los niveles del modelo OSI y de SNA.
- 3.6** Describir los componentes básicos de una red SNA.
- 3.7** Explicar las distintas configuraciones topológicas propias de las redes locales, indicando las características diferenciales y de aplicación de cada una de ellas.
- 3.8** Describir la estructura física de una red local de ordenadores, enumerando las tipologías de equipos, de medios físicos, de modos de conexión y estándares empleados.
- 3.9** Enumerar y describir las principales técnicas de compartición utilizadas en las redes de área local.
- 3.10** Citar las funciones y estructura del nivel físico en una LAN.
- 3.11** Dentro del nivel de enlace, en una LAN, explicar el papel de los dos subniveles en que se divide: MAC y LLC.
- 3.12** Comparar, destacando, las principales ventajas de los dos principales métodos de acceso (CSMA/CD y Paso de Testigo) a una red de área local.
- 3.13** Realizar una tabla comparativa entre los distintos estándares del IEEE 802.11.
- 3.14** Utilizando una red Ethernet y un Access Point, realizar la configuración del mismo, apoyándose en su manual, para poder conectar varios PC. Comprobar el alcance máximo, en función de la velocidad.
- 3.15** Verificar el alcance, con diferentes longitudes del cable entre el Access Point y la antena y con antenas de diferente ganancia.
- 3.16** Verificar los distintos niveles de seguridad que se pueden implementar en una WLAN.