Introducción

La presente obra se ha concebido para cubrir el temario del Módulo *Sistemas Telemáticos* del Ciclo Formativo de grado superior *Sistemas de Telecomunicación e Informáticos*. La evolución de la Telemática ha sido importante en los últimos años de manera que se ha tratado de cubrir todos los contenidos del currículo oficial pero actualizados convenientemente.

El primer capítulo sirve para presentar algunos conceptos generales sobre la materia. En el segundo capítulo se estudian las bases de la transmisión de datos, empezando por un repaso de los principales conceptos sobre las señales eléctricas y los medios de transmisión, se continúa presentando las principales técnicas de transmisión como la modulación, codificación, conmutación y multiplexación, y se acaba con una de las técnicas de transmisión de datos más extendidas como es la tecnología ADSL.

El modelo OSI, a pesar de no haberse implementado, es una buena referencia para conocer de qué manera se afronta el complejo desarrollo de los sistemas telemáticos, que es utilizando un modelo por capas o niveles. El modelo OSI se estudia en el capítulo 3.

El capítulo 4 incluye un repaso a las principales interfaces serie utilizadas en los sistemas telemáticos, incluyendo además la popular interfaz paralela Centronic y las nuevas interfaces como USB o Bluetooth. En el capítulo 5 se estudian en detalle las técnicas utilizadas en el nivel de enlace, además de los principales protocolos utilizados, especialmente el protocolo HDLC. En el capítulo 6 se presenta uno de los dispositivos más populares para las transmisión de datos, el módem.

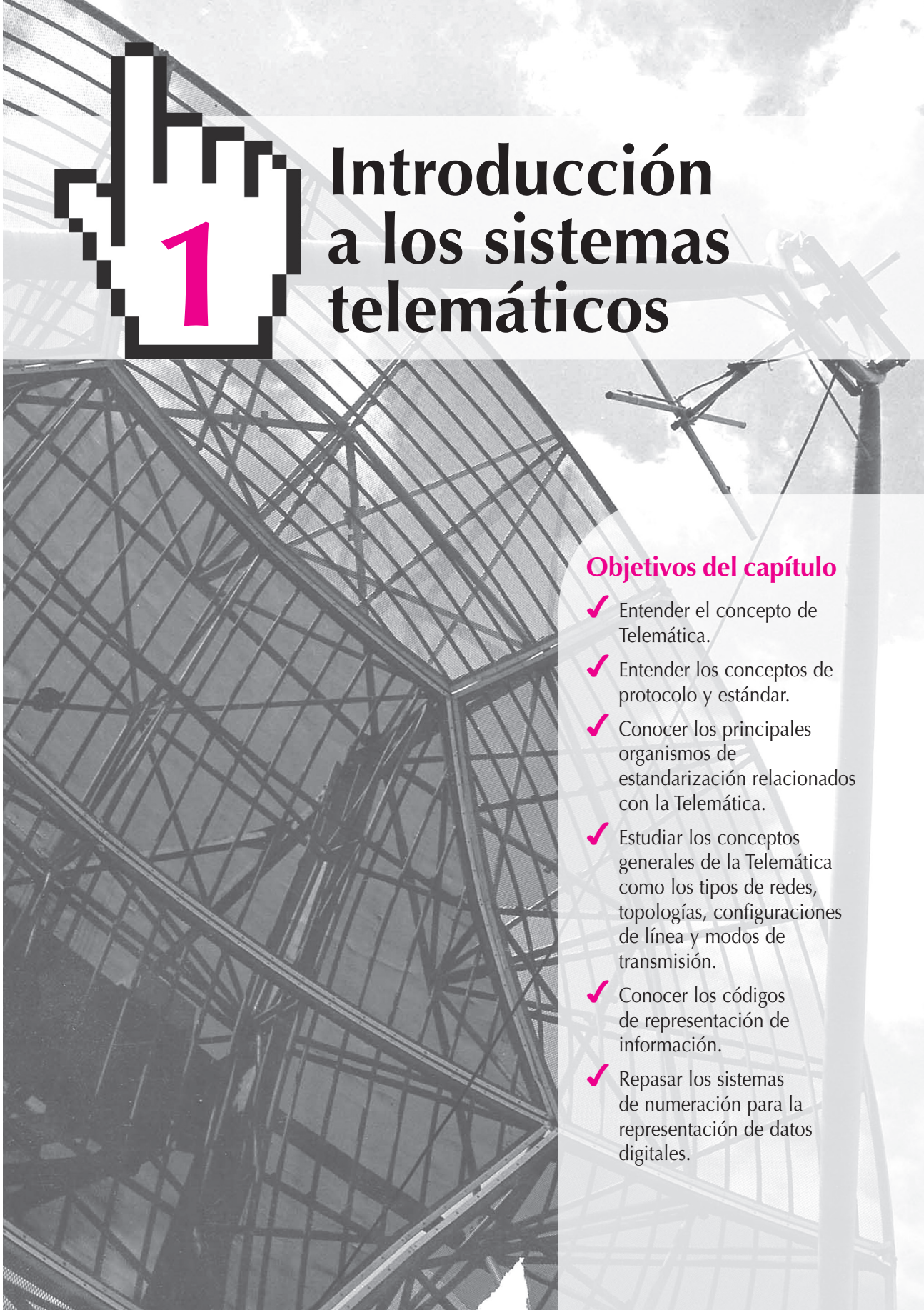
Sin ninguna duda las tecnologías relacionadas con las redes de área local son uno de los principales aspectos de los sistemas telemáticos que más se han desarrollado. En el capítulo 7 se estudian en detalle. Dichas tecnologías cubren los niveles físico y de enlace.

Para los niveles superiores, los protocolos que se han impuesto en la actualidad tanto en redes de área local como en redes de área extensa han sido los protocolos TCP/IP, que se estudian en profundidad en el capítulo 8. Las principales tecnologías utilizadas para el acceso a redes de área extensa como PPP, X.25, Frame Relay o ATM se estudian en el capítulo 9.

Por último, en el capítulo 10 se ofrece una visión global de los servicios telemáticos más populares actualmente. Básicamente los servicios relacionados con Internet y los servicios de conectividad proporcionados por los principales operadores.

Para contactar con el autor se puede utilizar la siguiente dirección de correo electrónico: **manuel.sg63@gmail.com**.

Se puede encontrar material adicional para esta obra en el CD-ROM que la acompaña y en la página web de Ra-Ma: **www.ra-ma.es/cf**.



1 Introducción a los sistemas telemáticos

Objetivos del capítulo

- ✓ Entender el concepto de Telemática.
- ✓ Entender los conceptos de protocolo y estándar.
- ✓ Conocer los principales organismos de estandarización relacionados con la Telemática.
- ✓ Estudiar los conceptos generales de la Telemática como los tipos de redes, topologías, configuraciones de línea y modos de transmisión.
- ✓ Conocer los códigos de representación de información.
- ✓ Repasar los sistemas de numeración para la representación de datos digitales.

1.1 TELEMÁTICA

1.1.1 DEFINICIÓN

La Telemática se encarga de la transmisión de datos entre sistemas de información basados en computadoras. Se puede decir que en la telemática hay aspectos relacionados con las Telecomunicaciones y aspectos relacionados con la Informática. Se podría, por tanto, establecer la siguiente regla:

Telemática = Telecomunicación + Informática

Los procesos básicos de transmisión de datos que se llevan a cabo en los sistemas telemáticos están directamente relacionados con las Telecomunicaciones. Estos aspectos serán tratados en el capítulo 2 de este libro. Sin embargo la aplicación de estos conceptos no es suficiente para la implementación de los sistemas telemáticos, es necesario definir muchas otras funciones que proporcionen un intercambio eficiente de la información. Muchas de estas funciones están muy relacionadas con los sistemas informáticos donde se implementan, es por ello que la Telemática se puede considerar que tiene un importante componente informático.

La complejidad en el diseño de los sistemas telemáticos requiere su abstracción en capas o niveles. Este aspecto será tratado en el capítulo 3 utilizando como referencia el modelo OSI o modelo de interconexión de sistemas abiertos.

Otro elemento clave en los sistemas telemáticos es el uso de información digital y su convergencia con los servicios de telecomunicación clásicos. Desde sus inicios, los datos intercambiados por los sistemas telemáticos han sido de naturaleza digital. El avance de las tecnologías de procesamiento digital ha propiciado que servicios tradicionales de telecomunicaciones, que han sido tratados de forma analógica como la telefonía, televisión, radio estén evolucionando hacia el tratamiento digital. Es por ello que actualmente se está produciendo una convergencia entre la Telemática tradicional (transmisión de datos, normalmente digitales) y las Telecomunicaciones (transmisión de audio, video, normalmente analógico).

Como uno de los ejemplos más claros está la evolución que se está produciendo en el servicio telefónico, donde se prevé que en un futuro cercano una gran parte de las comunicaciones de voz se procesen a través de las redes de datos y no a través del sistema telefónico tradicional (voIP).

A pesar de esta convergencia, en este libro se tratarán los sistemas telemáticos desde el punto de vista tradicional, obviando por ello las nuevas comunicaciones digitales como son los servicios de telefonía móvil, televisión y radio digital, Voz IP. Sobre todo para adaptar la obra el temario oficial del Módulo profesional de *Sistemas Telemáticos*. Quizás en una próxima edición la realidad imponga un cambio de planteamiento.

1.1.2 OBJETIVOS DE LOS SISTEMAS TELEMÁTICOS

Los objetivos de la Telemática se podrían resumir en los siguientes puntos generales:

- ✓ Compartir información, como ficheros, bases de datos, backups…
- ✓ Compartir recursos, como impresoras, dispositivos de almacenamiento de gran capacidad, módem…
- ✓ Mejora de la comunicación, a través del correo electrónico, envío de documentos, convocatoria de reuniones, fax…

1.1.3 COMPONENTES DE UN SISTEMA DE TRANSMISIÓN DE DATOS

Los componentes generales de cualquier sistema de transmisión de datos son los que aparecen en la siguiente figura:

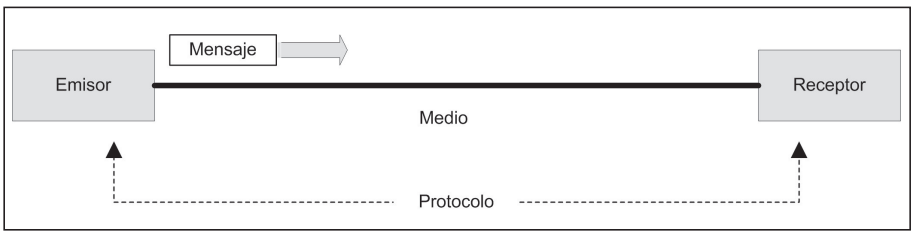


Figura 1.1. *Esquema general de un sistema telemático.*

- **Mensaje,** contiene la información que se quiere transmitir.
- **Emisor,** dispositivo que genera el mensaje.
- **Receptor,** dispositivo destino del mensaje.
- **Medio,** referido al medio físico utilizado para llevar a cabo la transferencia de la información. Pueden ser medios guiados como el cable de cobre, cable coaxial y la fibra óptica, y medios no guiados como el aire.
- **Protocolo,** es el conjunto de reglas que gobiernan la transmisión de datos.

1.2 PROTOCOLOS Y ESTÁNDARES

Uno de los elementos más importantes en los sistemas de transmisión de datos es el protocolo. Como se ha visto en el apartado anterior, un **protocolo** es un conjunto de reglas que gobiernan todos los aspectos de la comunicación de datos. Un protocolo define qué se comunica, cómo se comunica y cuando se produce la comunicación. Los elementos clave de un protocolo son:

- ✓ **Sintaxis,** estructura del formato de los datos.
- ✓ **Semántica,** significado de cada sección.
- ✓ **Temporización,** cuándo y con qué rapidez se deberían enviar los datos.

Un **estándar** proporciona un modelo de desarrollo abierto que hace que un producto funcione adecuadamente con otros, sin tener en cuenta el fabricante. Los estándares son esenciales para crear y mantener un mercado abierto y competitivo. Los estándares son normalmente desarrollados por organismos oficiales de estandarización.

Existen los llamados estándares de facto que son desarrollados inicialmente por una organización u organismo no oficial y se convierten en estándares debido a la extensión de su uso. Puede haber dos tipos de estándares:

- ✓ **Estándares propietarios o cerrados,** cuando son implementados por empresas privadas y los detalles de su desarrollo no son accesibles a nadie.
- ✓ **Estándares no propietarios o abiertos,** cuando los detalles de su desarrollo son públicos y accesibles a cualquier empresa que quiera implementarlos.

Ejemplos de estándares: HTML, formato PDF, TCP/IP...

Existen a nivel mundial varias organizaciones encargadas de proponer y desarrollar los estándares utilizados en los sistemas telemáticos:

- **ISO es la Organización Internacional de estandarización.** Creada en 1947 y formada actualmente por 157 países. Una de las principales aportaciones de esta organización es el Modelo OSI que será estudiado en el capítulo3.

  www.iso.org

- **ITU (International Telecommunicatios Union, Unión Internacional de Telecomunicaciones).** Es un organismo internacional dependiente de las Naciones Unidas encargado de coordinar los servicios y las redes globales de telecomunicación. Está dividido en tres sectores: ITU-R coordina los servicios radioeléctricos, ITU-T se encarga del desarrollo de estándares e ITU-D encargado del desarrollo en concreto de proyectos e iniciativas dentro del sector.

  www.itu.int

- **ETSI (European Telecommunications Standards Institute, Instituto europeo de estándares de telecomunicaciones).** Es una organización constituida para el desarrollo de estándares especialmente de ámbito europeo. Está formado por 655 miembros de 59 países diferentes tanto de Europa como de fuera de Europa.

  www.etsi.org

- **ANSI (American National Standars Institute, Instituto nacional Americano de estándares).** Es el equivalente americano del ETSI. Su dilatada historia

(nació en 1919) ha hecho que muchos de los estándares publicados por ANSI se hayan adoptado a nivel mundial.

www.ansi.org

- **IEEE (Institute of Electrical and Electronics Engineers).** Organismo formado por profesionales de las nuevas tecnologías, electricidad, electrónica y comunicaciones. Una de sus principales labores es la de la estandarización. Uno de sus más destacados trabajos está desarrollado por un comité conocido como Proyecto 802 dedicado a estandarizar sistemas de red.

  www.ieee.org

- **EIA (Electronics Industries Alliance).** Otro organismo de estandarización norteamericano formado principalmente por empresas del sector tecnológico y enfocado a proporcionar estándares para el mercado americano, como por ejemplo el famoso interfaz serie EIA-232, antes conocido como RS-232. La EIA también se ha encargado de desarrollar las normas de cableado estructurado que luego se han aplicado a nivel mundial.

  www.eia.org

1.3 CONCEPTOS BÁSICOS

1.3.1 REDES TELEMÁTICAS

El término de red telemática se refiere al conjunto de dispositivos (también denominados nodos) conectados entre sí a través de uno o varios enlaces implementados sobre un determinado medio físico. Los nodos pueden ser ordenadores, impresoras o cualquier dispositivo capaz de enviar o recibir datos de otros nodos.

En función de la definición anterior existen tres tipos de redes:

LAN

El término **LAN (Local Area Network) o red de área local** se aplica a una red telemática cuando los dispositivos unidos en dicha red se encuentran ubicados en un área geográfica limitada. Las distancias entre dispositivos conectados a una red de área local pueden variar entre unos pocos metros hasta varios cientos de metros o incluso kilómetros. En este caso, lo importante es que los equipos conectados pertenezcan a una misma unidad organizativa, por ejemplo, una empresa, centro educativo, organismo público...

Se han desarrollado tecnologías específicas para realizar esta función, por ello, otro criterio de identificación de una red LAN es el uso de una tecnología específica para redes LAN. Se tratará en profundidad las tecnologías de redes LAN en el capítulo 7.

MAN

En este caso, el término **MAN (Metropolitan Area Network) o red de área metropolitana** se aplica a aquellas redes con un ámbito y alcance mayor que las redes LAN. Normalmente se utiliza este término cuando se trata de redes que unen redes LAN o dispositivos dispersos en varias ubicaciones dentro de un núcleo de población o de varios núcleos cercanos entre sí. Por lo general, estas diferentes ubicaciones pertenecen, igual que en el caso anterior, a la misma unidad organizativa. Las distancias cubiertas por las redes MAN son, lógicamente, mayores que en las redes LAN y se suelen utilizar las infraestructuras de operadores de telecomunicaciones que dan servicio en la zona de cobertura de la red MAN.

Existen también tecnologías propias específicamente diseñadas para redes MAN.

WAN

Por último, el término **WAN (Wide Area Network) o redes de área extensa** se aplica a aquellas redes telemáticas que unen redes o dispositivos dispersos en diferentes zonas geográficas sin límite de distancia. En este caso es obligatorio el uso de las infraestructuras proporcionadas por los operadores de telecomunicación cuyo ámbito de actuación está dentro de las zonas que cubren este tipo de redes.

Al igual que en los casos anteriores, también se han desarrollado tecnologías específicas para la implementación de redes WAN. Las más importantes de estas tecnologías serán tratadas en el capítulo 9.

1.3.2 TOPOLOGÍAS DE RED

En el contexto de los sistemas telemáticos, la topología se refiere a la forma en que está diseñada la red, bien físicamente o bien lógicamente. Dos o más dispositivos se conectan a un enlace. Dos o más enlaces forman una topología. Por tanto, en función de cómo estén conectados los diferentes dispositivos que forman una red existen varias topologías:

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

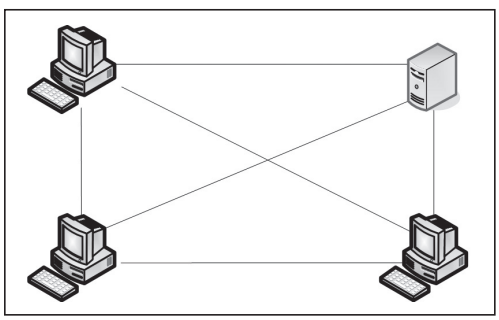


Figura 1.2. *Topología en malla.*

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

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

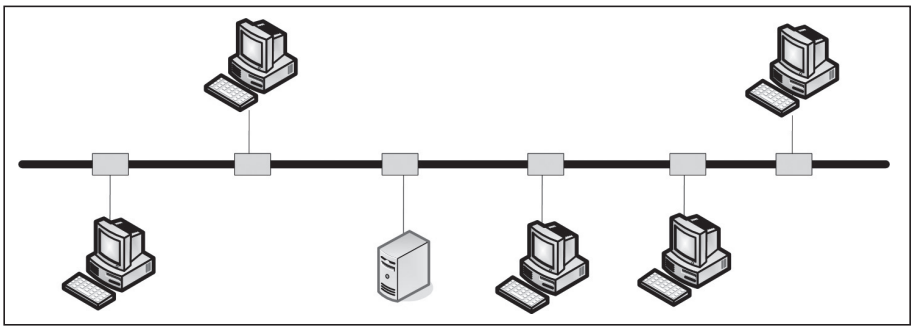


Figura 1.3. *Topología en bus.*

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

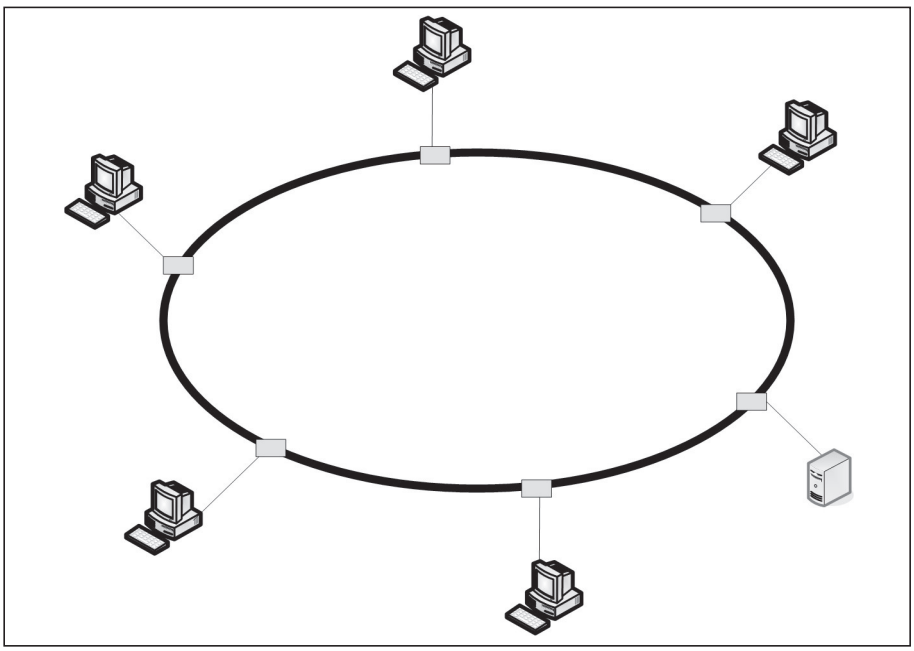


Figura 1.4. *Topología en anillo.*

- **Estrella.** En este caso, cada dispositivo solamente tiene un enlace dedicado con el controlador central, llamado concentrador.

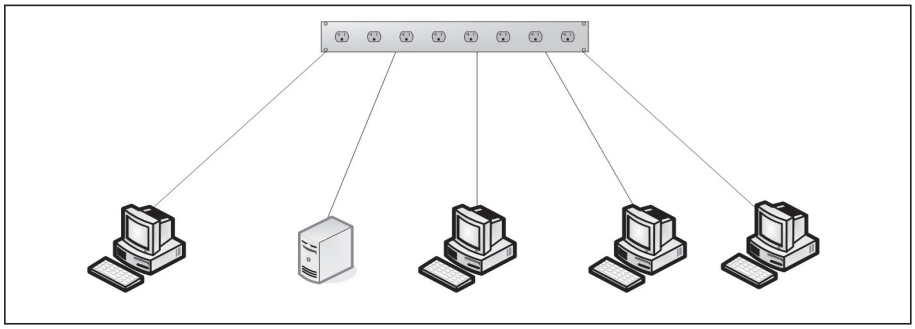


Figura 1.5. *Topología en estrella.*

- **Árbol.** Esta topología es una variante de la topología en estrella.

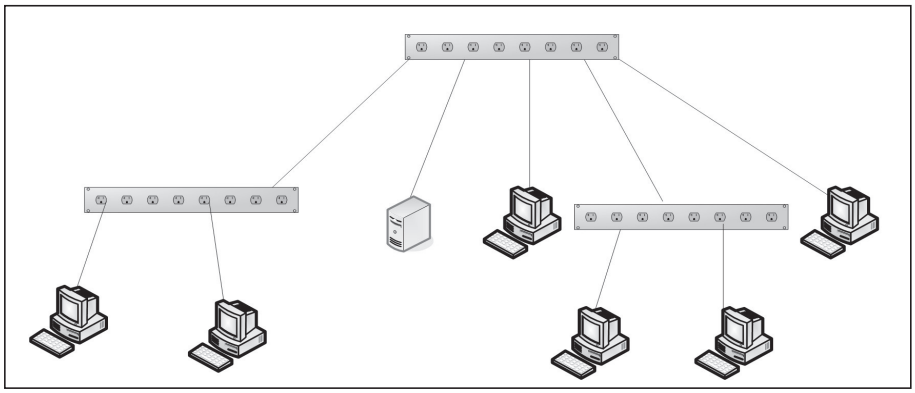


Figura 1.6. *Topología en árbol.*

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

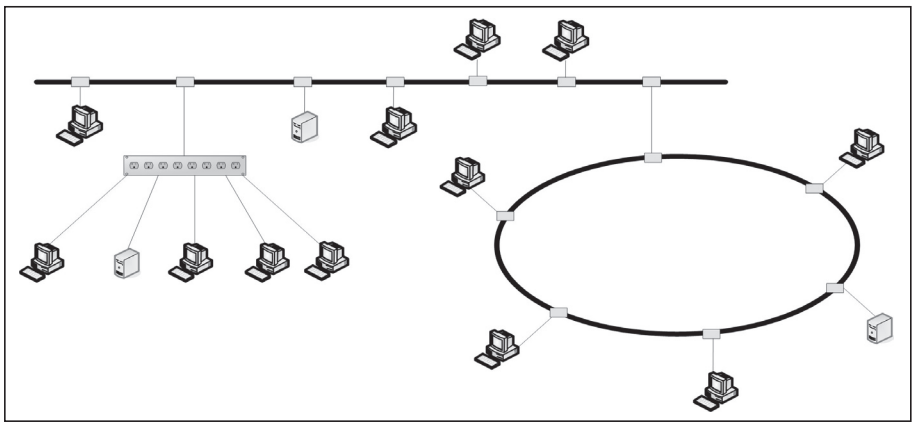


Figura 1.7. *Topología híbrida.*

1.3.3 CONFIGURACIÓN DE LA LÍNEA

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

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

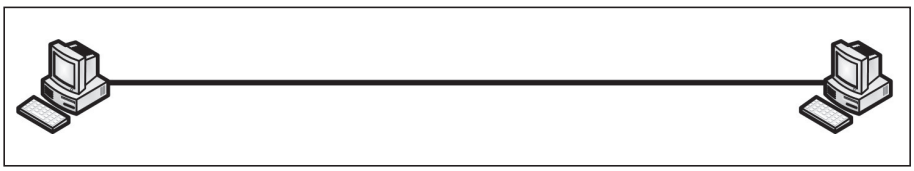


Figura 1.8. *Configuración punto a punto.*

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

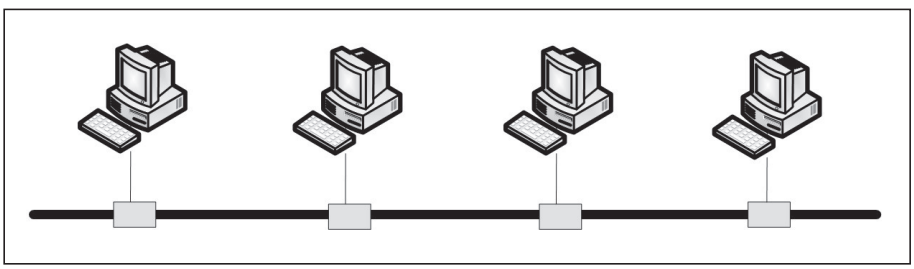


Figura 1.9. *Configuración multipunto.*

1.3.4 MODO DE TRANSMISIÓN

El modo de transmisión se establece en función de la dirección del flujo de las señales entre dos dispositivos enlazados. Hay tres tipos:

- **Símplex,** cuando se establece una comunicación unidireccional entre dos dispositivos. Una estación sólo recibe y la otra sólo envía.
- **Half-dúplex o semidúplex,** cada estación puede enviar y recibir datos pero no al mismo tiempo. Cuando un dispositivo envía, el otro sólo puede recibir y viceversa.
- **Full-dúplex o dúplex,** cuando las dos estaciones que llevan a cabo la comunicación pueden enviar y recibir de forma simultánea. Para ello debe haber dos caminos físicos diferentes o se tiene que dividir la capacidad del canal.

1.4 PRINCIPALES HITOS HISTÓRICOS DE LA TELEMÁTICA

El desarrollo de la Telemática está muy asociado con la evolución de la tecnología en general, especialmente con el desarrollo y la evolución de las Telecomunicaciones. A continuación se presenta un resumen de los principales hitos en el desarrollo de la telemática:

Tabla 1.1

Año	Hito histórico
1790	Invención del Telégrafo óptico, desarrollado por Claude Chappe
1794	Se envía el primer telegrama de la historia utilizando el telégrafo óptico de Lille a París (232 Km) con 22 torres
1800	Se envía el primer telegrama en España de Madrid a Aranjuez
1833	Desarrollo del Telégrafo eléctrico
1837	Desarrollo del Sistema Morse
1844	Se envía el primer mensaje telegráfico utilizando el código Morse
1851	Se pone en funcionamiento el primer cable telegráfico submarino entre Dover (Inglaterra) y Calais (Francia)
1857	Wheatstone patenta un sistema telegráfico que utiliza el código Morse y es capaz de transmitir 70 palabras por minuto
1865	Maxwell desarrolla las leyes del electromagnetismo fundamentales para la radiotransmisión
1876	Alexander G. Bell inventa el teléfono
1897	Se llevan a cabo las primeras transmisiones radioeléctricas realizadas por Marconi
1901	Se realiza la primera transmisión radioeléctrica que cruza el Atlántico (Marconi)
1915	Se realizan las primeras pruebas radiotelefónicas
1927	Se establece el primer enlace radio trasatlántico para comunicaciones telefónicas
1960	Se realizan las primeras conexiones entre ordenadores
1962	Se ponen en funcionamiento los primeros satélites repetidores
1969	Se desarrolla la red ARPANET, precursora de Internet, por encargo del Departamento de Defensa de EEUU
1973	Se desarrolla en Xerox la primera versión de Ethernet
1977	Se realiza la primera transmisión telefónica a través de fibra óptica
1981	Se alcanza la cifra de 213 ordenadores conectados a la red ARPANET pertenecientes a universidades y centros de investigación
1983	El Departamento de Defensa de EEUU se desliga de ARPANET
1984	Comienza a utilizarse una nueva red para conectar redes conocida como NSFNET utilizando los protocolos TCP/IP
1989	Tim Berners-Lee desarrolla el servicio WWW (World Wide Web), utilizando el lenguaje de marcación de hipertexto HTML y el protocolo HTTP
1990	Desaparece ARPANET y queda completamente sustituida por NSFNET
1993	Se extiende el uso del WWW con la aparición del navegador Mosaic
1995	Se desmantela la red NSFNET y comienza la descentralización del backbone de Internet adoptando la estructura que se mantiene en la actualidad

1.5 CÓDIGOS DE REPRESENTACIÓN DE LA INFORMACIÓN

En los primeros sistemas telemáticos, la mayor parte de los datos intercambiados era de tipo textual y como la información debía ser transmitida en formato binario surgió la necesidad de crear códigos binarios que se puedan utilizar para representar información textual.

Los primeros códigos utilizados en Telemática se pueden considerar los códigos utilizados en telegrafía, que fueron principalmente el código Morse y el Baudot. Actualmente estos códigos están en desuso.

Posteriormente, se desarrollaron otros códigos para representar la información que se quería transmitir en formato digital. Estos códigos podían servir para representar información numérica o alfabética:

- **Códigos numéricos.** Los más utilizados son el binario natural y el código BCD.
- **Códigos alfabéticos.** Un código alfabético es aquél utilizado para representar letras y signos de puntuación. El más utilizado de forma histórica es el código **ASCII (American Standard Code for Information Interchange)** que en su primera versión estaba formado por 7 bits, lo que permitía hasta 128 posibles códigos. Posteriormente se desarrolló el llamado código ASCII extendido, utilizando 8 bits y por lo tanto extendiendo el número de posibles códigos a 256. Esta codificación está normalizada por la ISO como ISO 8859. En sistemas IBM ha sido ampliamente utilizado el código EBCDIC formado por 8 bits.

En la tabla 1.2 se presentan los códigos ASCII con sus caracteres correspondientes. Los primeros 32 códigos (del 0 al 31) y el último (el 127) no son caracteres imprimibles sino que tienen otras funciones, algunas de ellas relacionadas con la transmisión de datos como se verá en el capítulo 5.

En la actualidad, aunque el código ASCII se sigue empleando extensamente, han surgido necesidades de codificación para codificar los posibles caracteres de otras lenguas diferentes al inglés, que es el idioma utilizado como base para el código ASCII. El resultado es el llamado estándar **Unicode**.

El desarrollo del sistema Unicode no está relacionado directamente con los sistemas telemáticos. Es un sistema de codificación de caracteres dentro del ámbito informático. Su principal objetivo es dar soporte a todos los caracteres existentes a nivel mundial, mejorando así la principal limitación de los sistemas de codificación anteriores como ASCII. El estándar Unicode está desarrollado por el llamado **Unicode Consortium**, organismo creado para esta finalidad y que cuenta entre sus miembros a los principales fabricantes de hardware y software. La primera versión, la 1.0, se publicó en 1991 con la colaboración de la organización ISO,

que lo publicó con la numeración ISO/IEC 10646. La última versión, Unicode 5.0, se ha publicado en 2006.

El estándar Unicode define la asignación de un código a cada carácter conocido de cualquier tipo de representación a nivel mundial. Sin embargo, no se define explícitamente en el estándar de qué forma se almacena cada código y de qué forma se representa.

Tabla 1.2 Caracteres no imprimibles

Binario	Dec.	Hex.	Abreviatura	Función
00000000	0	00	NUL	Carácter Nulo
00000001	1	01	SOH	Inicio de cabecera
00000010	2	02	STX	Inicio de Texto
00000011	3	03	ETX	Fin de Texto
00000100	4	04	EOT	Fin de Transmisión
00000101	5	05	ENQ	Solicitud
00000110	6	06	ACK	Asentimiento
00000111	7	07	BEL	Timbre
00001000	8	08	BS	Retroceso
00001001	9	09	HT	Tabulación horizontal
00001010	10	0A	LF	Salto de línea
00001011	11	0B	VT	Tabulación Vertical
00001100	12	0C	FF	Form feed
00001101	13	0D	CR	Retorno de carro
00001110	14	0E	SO	Shift Out
00001111	15	0F	SI	Shift In
00010000	16	10	DLE	Data Link Escape
00010001	17	11	DC1	Device Control 1
00010010	18	12	DC2	Device Control 2
00010011	19	13	DC3	Device Control 3
00010100	20	14	DC4	Device Control 4
00010101	21	15	NAK	Asentimiento negativo
00010110	22	16	SYN	Carácter de sincronismo
00010111	23	17	ETB	Fin de bloque
00011000	24	18	CAN	Cancelación
00011001	25	19	EM	
00011010	26	1A	SUB	Substitución
00011011	27	1B	ESC	Escape
00011100	28	1C	FS	File Separator
00011101	29	1D	GS	Group Separator
00011110	30	1E	RS	Record Separator
00011111	31	1F	US	Unit Separator
01111111	127	7F	DEL	Borrar

Tabla 1.3 Caracteres imprimibles

Binario	Dec.	Hex.	Carácter
00100000	32	20	Espacio
00100001	33	21	!
00100010	34	22	"
00100011	35	23	#
00100100	36	24	$
00100101	37	25	%
00100110	38	26	&
00100111	39	27	'
00101000	40	28	(
00101001	41	29	)
00101010	42	2A	*
00101011	43	2B	+
00101100	44	2C	,
00101101	45	2D	-
00101110	46	2E	.
00101111	47	2F	/
00110000	48	30	0
00110001	49	31	1
00110010	50	32	2
00110011	51	33	3
00110100	52	34	4
00110101	53	35	5
00110110	54	36	6
00110111	55	37	7
00111000	56	38	8
00111001	57	39	9
00111010	58	3A	:
00111011	59	3B	;
00111100	60	3C	<
00111101	61	3D	=
00111110	62	3E	>
00111111	63	3F	?
01000000	64	40	@
01000001	65	41	A
01000010	66	42	B
01000011	67	43	C
01000100	68	44	D
01000101	69	45	E
01000110	70	46	F
01000111	71	47	G
01001000	72	48	H

Binario	Dec.	Hex.	Carácter
01001001	73	49	I
01001010	74	4A	J
01001011	75	4B	K
01001100	76	4C	L
01001101	77	4D	M
01001110	78	4E	N
01001111	79	4F	O
01010000	80	50	P
01010001	81	51	Q
01010010	82	52	R
01010011	83	53	S
01010100	84	54	T
01010101	85	55	U
01010110	86	56	V
01010111	87	57	W
01011000	88	58	X
01011001	89	59	Y
01011010	90	5A	Z
01011011	91	5B	[
01011100	92	5C	\
01011101	93	5D	]
01011110	94	5E	^
01011111	95	5F	_
01100000	96	60	`
01100001	97	61	a
01100010	98	62	b
01100011	99	63	c
01100100	100	64	d
01100101	101	65	e
01100110	102	66	f
01100111	103	67	g
01101000	104	68	h
01101001	105	69	i
01101010	106	6A	j
01101011	107	6B	k
01101100	108	6C	l
01101101	109	6D	m
01101110	110	6E	n
01101111	111	6F	o
01110000	112	70	p
01110001	113	71	q

Tabla 1.3 Caracteres imprimibles *(cont.)*

Binario	Dec.	Hex.	Carácter
01110010	114	72	r
01110011	115	73	s
01110100	116	74	t
01110101	117	75	u
01110110	118	76	v
01110111	119	77	w
01111000	120	78	x
01111001	121	79	y
01111010	122	7A	z
01111011	123	7B	{
01111100	124	7C	|
01111101	125	7D	}
01111110	126	7E	~

En la siguiente tabla aparecen los caracteres del código ASCII extendido, es decir, desde el código 128 al 255:

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
128	80	Ç	160	A0	á	192	C0	└	224	E0	α
129	81	ü	161	A1	í	193	C1	┴	225	E1	ß
130	82	é	162	A2	ó	194	C2	┬	226	E2	Γ
131	83	â	163	A3	ú	195	C3	├	227	E3	π
132	84	ä	164	A4	ñ	196	C4	─	228	E4	∑
133	85	à	165	A5	Ñ	197	C5	┼	229	E5	σ
134	86	å	166	A6	ª	198	C6	╞	230	E6	µ
135	87	ç	167	A7	º	199	C7	╟	231	E7	τ
136	88	ê	168	A8	¿	200	C8	╚	232	E8	Φ
137	89	ë	169	A9	⌐	201	C9	╔	233	E9	Θ
138	8A	è	170	AA	¬	202	CA	╩	234	EA	Ω
139	8B	ï	171	AB	½	203	CB	╦	235	EB	δ
140	8C	î	172	AC	¼	204	CC	╠	236	EC	∞
141	8D	ì	173	AD	¡	205	CD	═	237	ED	ø
142	8E	Ä	174	AE	«	206	CE	╬	238	EE	ε
143	8F	Å	175	AF	»	207	CF	╧	239	EF	∩
144	90	É	176	B0	░	208	D0	╨	240	F0	≡
145	91	æ	177	B1	▒	209	D1	╤	241	F1	±
146	92	Æ	178	B2	▓	210	D2	╥	242	F2	≥
147	93	ô	179	B3	│	211	D3	╙	243	F3	≤
148	94	ö	180	B4	┤	212	D4	╘	244	F4	⌠
149	95	ò	181	B5	╡	213	D5	╒	245	F5	⌡
150	96	û	182	B6	╢	214	D6	╓	246	F6	÷
151	97	ù	183	B7	╖	215	D7	╫	247	F7	≈
152	98	ÿ	184	B8	╕	216	D8	╪	248	F8	°
153	99	Ö	185	B9	╣	217	D9	┘	249	F9	∙
154	9A	Ü	186	BA	║	218	DA	┌	250	FA	·
155	9B	¢	187	BB	╗	219	DB	█	251	FB	√
156	9C	£	188	BC	╝	220	DC	▄	252	FC	ⁿ
157	9D	¥	189	BD	╜	221	DD	▌	253	FD	²
158	9E	₧	190	BE	╛	222	DE	▐	254	FE	■
159	9F	ƒ	191	BF	┐	223	DF	▀	255	FF	□

Figura 1.10. *Representación de los caracteres de la codificación ASCII extendida.*

El problema está en que la mayor parte de los sistemas de procesamiento de información utiliza un byte (8 bits) para almacenar códigos de caracteres. Con esto sólo es posible trabajar con 256 códigos diferentes, al igual que el ASCII de 8 bits. Sin embargo en Unicode se ha definido la codificación de más de 90.000 caracteres.

Para resolver este problema se han definido varios métodos de mapeo de los caracteres Unicode en función de las características del sistema donde se utilice. Los más utilizados son:

- ✓ **UTF-8,** codificación de 8 bits de longitud variable
- ✓ **UTF-16,** codificación de 16 bits de longitud variable
- ✓ **UTF-32,** codificación de 32 bits de longitud fija

El más utilizado de estos mapeos del estándar Unicode es el **UTF-8 (8-bit Unicode Transformation Format)**, soportado para la codificación de texto en todos los protocolos de Internet actualmente e implementado en la mayor parte de los navegadores web. De hecho el organismo IETF, responsable de los procesos de estandarización de las tecnologías utilizadas en Internet, lo tiene contemplado en el documento RFC 3629.

UTF-8 codifica los caracteres Unicode utilizando entre 1 y 4 bytes. Los primeros 128 caracteres se codifican con 8 bits utilizando los mismos códigos que ASCII. De esta forma, los códigos ASCII de 7 bits son compatibles con UTF-8 y se representan con un solo byte. Para códigos diferentes al estándar ASCII, se puede utilizar 2, 3 o hasta 4 bytes para su representación. Los caracteres de las principales lenguas latinas se representan con un código de 2 bytes. En la siguiente tabla se muestra el mapeo llevado a cabo en UTF-8:

Tabla 1.4

Carácter Unicote (Hex.)	Codificación en UTF-8 (binario)
0000 0000 0000 007F	0xxxxxxx
0000 0080 0000 07FF	110xxxxx 10xxxxxx
0000 0800 0000 FFFF	1110xxxx 10xxxxxx 10xxxxxx
0001 0000 0010 FFFF	11110xxx 10xxxxxx 10xxxxxx 10xxxxxx

Como se observa, para distinguir del resto la codificación utilizando un solo byte, se utiliza el bit más significativo a cero. Para el resto de codificaciones extendidas, el número de unos en el primer byte indica el número de bytes utilizados para la codificación del carácter.

1.6 SISTEMAS DE NUMERACIÓN

Un sistema de numeración es una forma de representar cualquier cantidad numérica. Casi todos los sistemas de numeración utilizados en la actualidad son de tipo polinomial. Todo sistema polinomial cumple las siguientes características:

- ✓ Todo número es una expresión formada por un conjunto de símbolos, llamados dígitos, cada uno con un valor fijo y diferente a los demás.
- ✓ El número de símbolos distintos que se pueden usar en un determinado sistema de numeración constituye su "base", es decir, en base 10 los números que podemos representar son {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}, en base 2 son {0, 1}, en base 8 son {0, 1, 2, 3, 4, 5, 6, 7} y en base 16 {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F}.
- ✓ El valor numérico que expresa una determinada combinación de dígitos en una base de numeración dada depende de dos factores: del valor de los dígitos y de la posición de cada uno de ellos en el polinomio.
- ✓ Cada posición del dígito tiene un valor intrínseco que aumenta de derecha a izquierda según potencias sucesivas de la base del sistema de numeración empleado. El dígito que aparece en el extremo izquierdo es el de más valor o más peso y el colocado en el extremo derecho es el de menos valor o menor peso.

De forma general, en un sistema de numeración de **base b** (b entero y mayor que la unidad), un número **N** cualquiera (representado como $\mathbf{N_b}$) se puede expresar mediante un polinomio de potencias de la base, multiplicadas por un símbolo perteneciente al sistema de numeración. Así, un número **N** cuya base sea **b** viene dado por el siguiente polinomio (no hay que olvidar que las operaciones deben hacerse en base **b**).

$$\mathbf{N_b} = a_n * b^n + a_{n-1} * b^{n-1} + a_{n-2} * b^{n-2} + \ldots + a_2 * b^2 + a_1 * b^1 + a_0 * b^0$$

1.6.1 SISTEMAS BINARIO, OCTAL Y HEXADECIMAL

Nosotros utilizamos el sistema decimal (base 10), es decir, un sistema de numeración polinomial que utiliza 10 dígitos. Los sistemas digitales, entre los que podemos incluir la mayor parte de los sistemas telemáticos, utilizan el sistema de numeración binario (base 2). Este sistema es también polinomial pero utiliza sólo dos dígitos, 0 y 1.

Al igual que en el sistema decimal, en el sistema binario el valor de cada posición de un dígito binario aumenta de izquierda a derecha en potencias de su base. Como en el sistema binario su base es 2, el peso de cada posición es una potencia de 2 según se muestra a continuación:

2^{10}	2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1024	512	256	128	64	32	16	8	4	2	1

Sin embargo, a pesar de ser el sistema binario el utilizado en los sistemas telemáticos, en muchas ocasiones resulta incómodo trabajar con datos utilizando el sistema binario ya que para representar números relativamente pequeños hacen falta muchos dígitos binarios.

Un ejemplo de ello es la dirección física de una tarjeta de red, que es un número binario de 48 bits, esto es algo así:

00110101 01110010 11001010 11001101 11010101 10101000

Para poder trabajar con números que requieran menos dígitos para su representación y que sea fácil su conversión a binario y viceversa se ha hecho frecuente el uso de otros sistemas de numeración alternativos. Éstos son el sistema octal y el hexadecimal. El sistema octal, al igual que el decimal y el binario, es de tipo polinomial pero utiliza ocho dígitos para representar números. El sistema hexadecimal también es polinomial y utiliza 16 dígitos, los números del 0 al 9 y añade las letras A, B, C, D, E y F para completar los dígitos utilizados.

La principal característica de los sistemas octal y hexadecimal es que sus bases son potencias de 2 por lo que la conversión entre ellos y el sistema binario es muy sencilla. A continuación se muestra una tabla con la representación de los primeros 16 dígitos en los cuatro sistemas:

Tabla 1.5

Decimal	Hexadecimal	Octal	Binario
0	0	0	0000
1	1	1	0001
2	2	2	0010
3	3	3	0011
4	4	4	0100
5	5	5	0101
6	6	6	0110
7	7	7	0111
8	8	10	1000
9	9	11	1001
10	A	12	1010
11	B	13	1011
12	C	14	1100
13	D	15	1101
14	E	16	1110
15	F	17	1111

Como se observa, en la tabla anterior, tres dígitos binarios se pueden representar por un solo dígito octal. Y cuatro dígitos binarios se representan por un solo dígito hexadecimal. Por ejemplo, la dirección física de la tarjeta de red del ejemplo anterior se podría representar de forma más compacta en hexadecimal:

35 72 CA CD D5 A8

Debe quedar claro que los sistemas digitales operan siempre con el sistema binario. Los sistemas octal y hexadecimal se utilizan como una forma más cómoda para los seres humanos de trabajar con valores binarios, ya que la conversión entre el sistema binario y el decimal no es tan sencilla.

1.6.2 CONVERSIÓN ENTRE BASES

Para trabajar con los distintos sistemas de numeración es necesario conocer los métodos utilizados para pasar de un sistema a otro. En la tabla resumen que se muestra a continuación aparecen todas las conversiones entre los sistemas decimal, binario y hexadecimal. El sistema octal se trata de forma similar al hexadecimal.

Tabla 1.6

De	A	Método de conversión
Binario	Decimal	Descomposición en su forma polinomial
Hexadecimal	Decimal	Descomposición en su forma polinomial
Binario	Hexadecimal	Cada cuatro dígitos binarios se convierte en un dígito hexadecimal
Hexadecimal	Binario	Cada dígito hexadecimal se descompone en cuatro dígitos binarios
Decimal	Binario	Método de divisiones sucesivas
Decimal	Hexadecimal	Método de divisiones sucesivas

El método de descomposición polinomial consiste en representar el número como un polinomio y llevar a cabo la suma de sus elementos.

Ejemplo: convertir a decimal el número binario 10010111.

$$10010111 = 1 * 2^7 + 0 * 2^6 + 0 * 2^5 + 1 * 2^4 + 0 * 2^3 + 1 * 2^2 + 1 * 2^1 + 1 * 2^0 = 2^7 + 2^4 + 2^2 + 2^1 + 2^0 = 128 + 16 + 4 + 2 + 1 = 151$$

Para convertir de hexadecimal se utiliza el mismo procedimiento. Por ejemplo, convertir el número 2B9.

$$2B9 = 2 * 16^2 + B * 16^1 + 9 * 16^0 = 2*256 + 11*16 + 9 = 512 + 176 + 9 = 697$$

La conversión de binario a hexadecimal se lleva a cabo agrupando los dígitos binarios de cuatro en cuatro empezando por la izquierda. Después de formar los grupos, cada grupo se convierte al sistema hexadecimal según la tabla de correspondencia binario-hexadecimal:

Tabla 1.7

Hex.	Binario
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010
B	1011
C	1100
D	1101
E	1110
F	1111

Por ejemplo, para pasar el número 1100100100110101 11, se hacen grupos empezando por la izquierda:

0011	0010	0100	1101	0111

Como se aprecia, se han añadido dos ceros por la derecha para completar el último grupo. A continuación se convierte cada grupo en un dígito hexadecimal:

0011	0010	0100	1101	0111
3	2	4	E	7

El número hexadecimal resultante es: 324E7.

La conversión inversa, es decir, de hexadecimal a binario se lleva a cabo aplicando el mismo método pero en sentido inverso, es decir, cada dígito hexadecimal se descompone en cuatro dígitos binarios. Por ejemplo, para convertir a binario el número hexadecimal AB519D:

A	B	5	1	9	D
1010	1011	0101	0001	1001	1101

Por lo tanto, el número resultante es:

1010 1011 0101 0001 1001 1101

Por último, el método para convertir números hexadecimales o binarios a decimales se conoce como divisiones sucesivas. Para ello se divide el número decimal que se desea convertir entre la base del sistema destino. Se anota el cociente y el resto de la división y se vuelve a dividir el cociente resultante entre la base. De nuevo se anota el cociente resultante y el resto. Esta operación se repite hasta que el cociente resultante no pueda ser dividido entre la base. El número resultante será el formado por el último cociente, que será el dígito de mayor peso, y los restos de las divisiones sucesivas. A continuación se muestra como ejemplo la conversión del número decimal 517 a binario:

Tabla 1.8

División	Cociente	Resto (coeficiente)
517: 2	258	a0 = 1
258 : 2	129	a1 = 0
129 : 2	64	a2 = 1
64 : 2	32	a3 = 0
32 : 2	16	a4 = 0
16 : 2	8	a5 = 0
8 : 2	4	a6 = 0
4 : 2	2	a7 = 0
2 : 2	1	a8 = 0
		a9 = 1

El término a_9 representa el dígito de mayor peso por lo tanto el número binario resultante es:

1 0 0 0 0 0 0 1 0 1

Para la conversión de decimal a hexadecimal se aplica el mismo método pero llevando a cabo las divisiones entre 16. Como las divisiones utilizando como divisor el 16 pueden entrañar alguna dificultad, se puede llevar a cabo la conversión de decimal a hexadecimal, pasando de decimal a binario (más fácil dividir entre 2) y luego convertir el número binario resultante a hexadecimal convirtiendo cada grupo de cuatro dígitos binarios en un dígito hexadecimal.

RESUMEN DEL CAPÍTULO

En este primer capítulo se ha dado una visión general de la Telemática como una disciplina que engloba tanto aspectos de Telecomunicaciones como de Informática. En definitiva, la Telemática se encarga de la transmisión de datos de forma eficiente.

Uno de los aspectos básicos en la Telemática es la utilización de protocolos que definen los procesos de comunicación y los estándares que permiten que diferentes equipos sean capaces de comunicarse entre sí utilizando protocolos comunes.

Se repasan algunos conceptos básicos relacionados con la telemática como son la clasificación de las redes telemáticas, las topologías de red, la configuración de línea de los dispositivos y su modo de transmisión.

Después de apuntar los principales hitos históricos relacionados en mayor o menor medida con la Telemática y que han influido decisivamente en su evolución, se repasan los códigos de representación de la información más utilizados, especialmente ASCII y Unicode.

Para terminar esta visión general e introductoria se ha dado un repaso a los sistemas de numeración utilizados cuando se estudian los sistemas telemáticos: binario, octal y hexadecimal.

EJERCICIOS PROPUESTOS

- **1.** Codificar, utilizando la codificación ASCII, la cadena de caracteres "Sistemas Telemáticos".

- **2.** Obtener, haciendo uso de los medios disponibles (libros, revistas, Internet...), la codificación en UFT-8 de los diferentes caracteres no incluidos en el estándar ASCII que se utilizan en el idioma español. Por ejemplo: ñ, á, é, í, ó, ú...

- **3.** Elaborar una lista de los estándares que conozcas relacionados con la Telemática o la Informática y averiguar si son estándares abiertos o cerrados. En el caso de estándares abiertos, obtener el organismo encargado de su desarrollo. Para los estándares cerrados, averiguar qué empresa u organismo lo ha desarrollado.

- **4.** Llevar a cabo las siguientes conversiones de números binarios o hexadecimales a decimales:
  a) Binario: 1010001101
  b) Hexadecimal: 8BC
  c) Binario: 10000011
  d) Hexadecimal: 101

- **5.** Llevar a cabo las conversiones de los siguientes números a hexadecimal:
  a) Decimal: 1000
  b) Decimal: 65302
  c) Binario: 10101010111
  d) Binario: 11100011010110011

- **6.** Llevar a cabo las conversiones de los siguientes números a binario:
  a) Decimal: 345
  b) Decimal: 88
  c) Hexadecimal: ABCD
  d) Hexadecimal: 987

TEST DE CONOCIMIENTOS

1 La Telemática se encarga principalmente del estudio de:
  a) El sistema telefónico.
  b) La transmisión de señales de audio y video.
  c) La transmisión de datos.
  d) Todas las respuestas anteriores son válidas.

2 Los estándares son normalmente desarrollados:
  a) Por organismos de estandarización.
  b) Por empresas del sector privado representativas del sector.
  c) Por los principales gobiernos.
  d) Cualquiera puede desarrollar un estándar siempre que lo registre.

1 La Telemática se encarga principalmente del estudio de:
- **a)** El sistema telefónico.
- **b)** La transmisión de señales de audio y video.
- **c)** La transmisión de datos.
- **d)** Todas las respuestas anteriores son válidas.

2 Los estándares son normalmente desarrollados:
- **a)** Por organismos de estandarización.
- **b)** Por empresas del sector privado representativas del sector.
- **c)** Por los principales gobiernos.
- **d)** Cualquiera puede desarrollar un estándar siempre que lo registre.

3 El organismo de estandarización que depende de Naciones Unidas es:
- **a)** ISO.
- **b)** ITU.
- **c)** IEEE.
- **d)** ETSI.

4 La diferencia entre los organismos de estandarización ETSI y ANSI es que:
- **a)** El ETSI se encarga de estándares abiertos y el ANSI de estándares cerrados.
- **b)** El ETSI es un organismo europeo y el ANSI es americano.
- **c)** El ETSI propone los estándares y el ANSI los desarrolla.
- **d)** Realmente no hay ninguna diferencia.

5 ¿Qué topología utiliza un elemento central llamado concentrador?
- **a)** Bus.
- **b)** Anillo.
- **c)** Estrella.
- **d)** Malla.

6 La principal diferencia entre los diferentes tipos de redes telemáticas es:
- **a)** La velocidad de transmisión siendo la más elevada en las redes LAN y la más baja en las WAN.
- **b)** El número de dispositivos conectados. Las redes LAN y MAN tienen limitaciones de varios cientos de dispositivos mientras que las WAN no tienen limitación.
- **c)** La distancia cubierta. Las redes LAN y MAN tienen limitación geográfica y las WAN no.
- **d)** El tipo de medio de transmisión utilizado. Cable de cobre y coaxial en redes LAN y MAN, y fibra óptica en redes WAN.

7 La configuración de línea se refiere:
- **a)** A la definición de los parámetros de la conexión, como la velocidad.
- **b)** A la forma de los conectores y la función de cada pin.
- **c)** A la dirección del flujo de la información transmitida.
- **d)** A la forma en la que los dispositivos se conectan a un enlace.

8 La diferencia entre la codificación ASCII y la Unicode es:
- **a)** ASCII puede representar números y letras, Unicode sólo letras.
- **b)** ASCII es un estándar de la ISO y Unicode no.
- **c)** ASCII no permite compresión y Unicode sí.
- **d)** ASCII no permite representar los caracteres de cualquier idioma y Unicode sí.

9 ¿Hasta cuántos bytes se pueden utilizar en UTF-8 para codificar un carácter?

2 Transmisión de datos

Objetivos del capítulo

- ✓ Comprender la diferencia entre señales analógicas y digitales.
- ✓ Entender las principales características de las señales, en el dominio del tiempo y de la frecuencia.
- ✓ Conocer el principal método de transmisión de señales digitales en banda base: la codificación.
- ✓ Estudiar y analizar las principales técnicas utilizadas en la transmisión de datos como son la modulación de señales digitales, la conmutación y la multiplexación.
- ✓ Conocer una de las tecnologías de transmisión de datos más extendidas actualmente: ADSL.

2.1 INTRODUCCIÓN

Sin ninguna duda, la esencia de los sistemas telemáticos es la transmisión de los datos. En este contexto y como norma general, los sistemas que intercambian datos son sistemas digitales y, por lo tanto, los datos intercambiados son datos binarios.

Estos datos, en última instancia y para ser transmitidos, deben representarse en forma de señales eléctricas (o señales ópticas para el caso de utilizar como medio de transmisión la fibra óptica). En este capítulo veremos algunos conceptos elementales sobre las señales eléctricas, también se incluye un repaso a los principales medios de transmisión utilizados en los sistemas telemáticos, para, por último, repasar algunas de las principales técnicas que se usan en la transmisión de datos.

Sin embargo, hay que tener en cuenta que la transmisión de datos es sólo la base sobre la que están diseñados los sistemas telemáticos. Como se verá en el próximo capítulo, la complejidad de estos sistemas requiere la abstracción de su diseño en niveles o capas, donde la transmisión de datos resuelve funciones del primer nivel, el más elemental.

2.2 SEÑALES

La transmisión de datos se basa en el envío de señales eléctricas o electromagnéticas a través de un medio de transmisión. Los datos que se van a transmitir, sea cual sea su naturaleza (texto, sonidos, imágenes…), son transformados en última instancia en señales electromagnéticas.

Normalmente la información que se quiere transmitir estará en formato digital pero no siempre será posible utilizar señales digitales para llevar a cabo la transmisión. Las características que deben cumplir las señales utilizadas en los sistemas telemáticos dependen en gran medida del medio de transmisión utilizado.

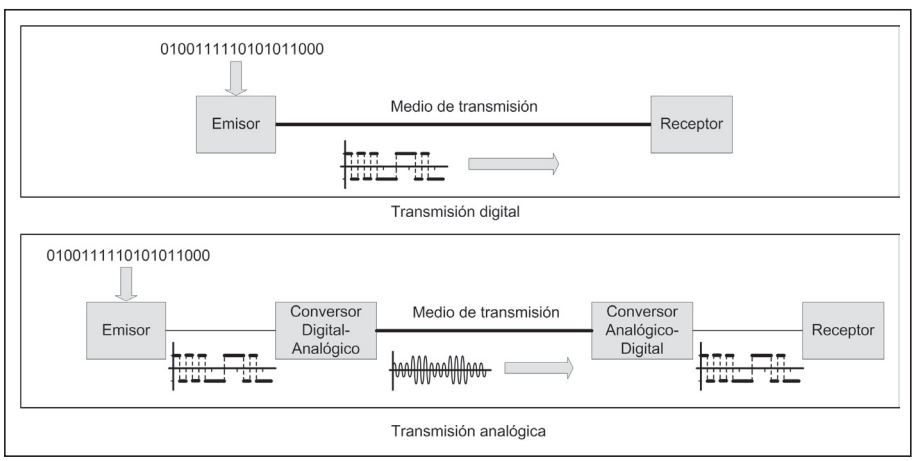


Figura 2.1. *Esquema básico de transmisión con señales analógicas y digitales.*

2.2.1 SEÑALES ANALÓGICAS Y DIGITALES

Las señales de naturaleza eléctrica pueden ser de dos tipos: analógicas o digitales.

En general, cuando se habla de una magnitud analógica, hablamos de una magnitud cuya variación es continua, es decir, entre un valor mínimo y uno máximo, la magnitud puede tomar todos los infinitos posibles valores entre ellos. Todas las magnitudes físicas son de naturaleza analógica, por ejemplo, la velocidad, temperatura, presión atmosférica... De igual manera, se habla de un señal eléctrica o electromagnética analógica (o simplemente señal analógica) cuando la magnitud física, normalmente la tensión eléctrica o la corriente eléctrica, puede tomar cualquier valor dentro de un posible rango. Su variación, es decir, el paso de un valor a otro, se hace de forma continua, pasando por todos los valores intermedios.

Podemos representar la variación de una magnitud analógica de forma gráfica con dos ejes de coordenadas donde el eje X representa el tiempo y el eje Y representa la magnitud. En la siguiente figura se observa la variación de velocidad (magnitud analógica) de un vehículo en función del tiempo:

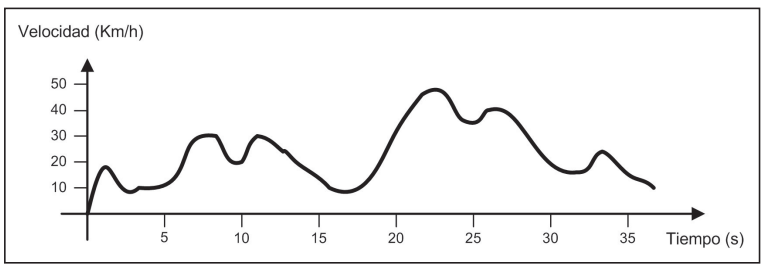


Figura 2.2. *Representación de la variación de la velocidad de un vehículo como ejemplo de una magnitud analógica.*

En el gráfico anterior se aprecia perfectamente el carácter continuo de la magnitud analógica. Igualmente se puede representar una señal analógica. En este caso, la magnitud eléctrica que varía es la tensión o voltaje eléctrico:

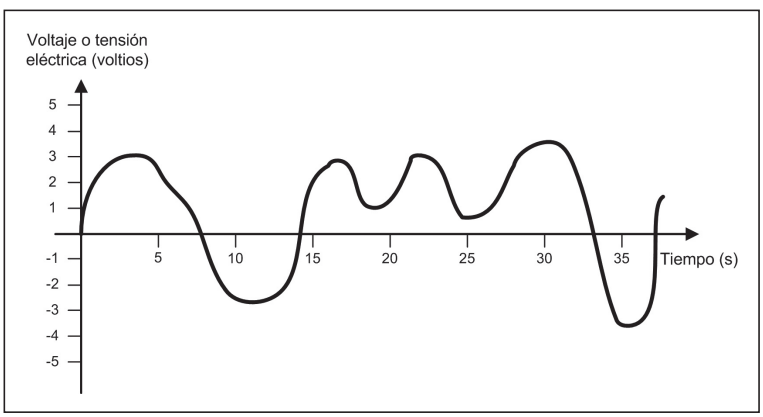


Figura 2.3. *Representación de una señal analógica.*

En contrapartida, una magnitud digital tiene una variación discreta, es decir, entre dos puntos, la magnitud sólo puede tomar un número limitado y concreto de valores. Por tanto, el paso de un posible valor de la magnitud al siguiente se hace de forma discontinua. No existen en la naturaleza magnitudes físicas digitales pero sí existen representaciones digitales de las mismas, por ejemplo, un velocímetro digital con una resolución de 10 Km/h entre 0 y 200 Km/h sólo podrá representar 20 velocidades diferentes. Es decir, un número discreto de variaciones. Mientras que la velocidad es una magnitud analógica, la medición de la misma es digital. El velocímetro pasará de 10 a 20 Km/h, pero la velocidad realmente aumentará de forma continua, pasando por todas las posibles velocidades entre 10 y 20.

En el siguiente gráfico se representa la indicación de velocidad de un velocímetro digital con una resolución de 10 Km/h:

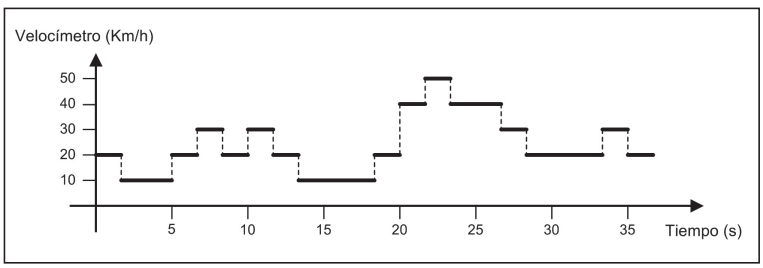


Figura 2.4. *Representación de una magnitud digital.*

Las señales digitales cumplen esta misma característica, es decir, la magnitud eléctrica sólo puede tomar un número concreto de valores entre un límite inferior y otro superior. En la siguiente figura se representa un ejemplo de señal digital. En este caso, la magnitud que varía es una tensión o voltaje eléctrico:

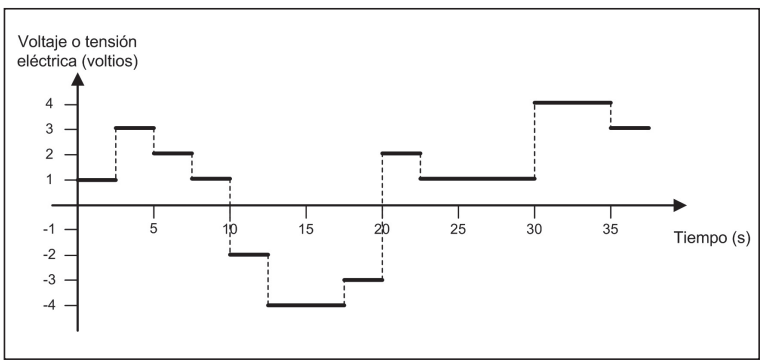


Figura 2.5. *Representación de una señal digital.*

La señal de la figura anterior puede tomar hasta ocho valores diferentes en el rango de entre -4 v y +4 v. Sin embargo, uno de los tipos de señales digitales más

comunes son aquéllas que sólo pueden tomar dos valores. A estas señales se les denomina señales digitales binarias. En la siguiente figura se representa una señal digital binaria que puede tomar sólo dos valores, +5 v y -5 v.

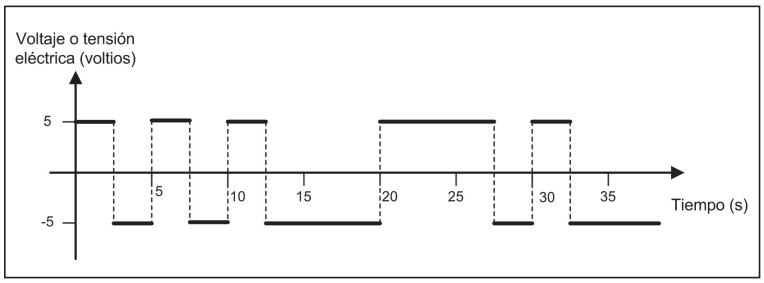


Figura 2.6. *Ejemplo de la representación de una señal digital binaria.*

NOTA 2.1

RECORDAR:
Señal analógica = variación continua de su valor
Señal digital = variación discreta de su valor. Se producen saltos o discontinuidades

2.2.2 SEÑALES PERIÓDICAS Y APERIÓDICAS

Las señales, además de poder clasificarse en función de la variación de la magnitud eléctrica, en señales analógicas o digitales, pueden clasificarse en función de la existencia o no de un patrón de repetición de la variación. Esta clasificación se puede aplicar tanto a señales analógicas como digitales.

Las señales periódicas son aquéllas en las que se establece un patrón que se repite consecutivamente a lo largo del tiempo. El patrón de repetición se conoce como ciclo y el tiempo que tarda en completarse un ciclo es el período. Lógicamente, el período se mide en unidades de tiempo, por ejemplo, segundos. En la siguiente figura se representan dos ejemplos típicos de señales periódicas, una analógica y otra digital.

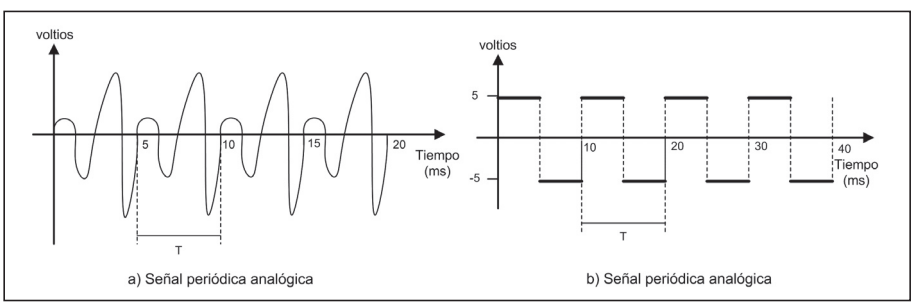


Figura 2.7. *Ejemplos de señales periódicas.*

La unidad para representar un período es el segundo, aunque con mucha frecuencia se utilizan los submúltiplos del segundo:

Milisegundo (ms)	10^{-3} s	0'001 s
Microsegundo (μs)	10^{-6} s	0'000001 s
Nanosegundo (ns)	10^{-9} s	0'000000001 s
Picosegundo (ps)	10^{-12} s	0'000000000001 s

Las señales aperiódicas son aquéllas que no presentan ningún patrón de repetición en el tiempo. Las figuras 2.3 y 2.5 del apartado anterior son ejemplos de señales aperiódicas, la primera analógica y la segunda digital.

2.2.3 SEÑALES ANALÓGICAS SIMPLES

Una señal analógica simple o fundamental es la señal analógica periódica más sencilla que se puede obtener. La representación gráfica de una señal simple se conoce como onda sinusoidal y se corresponde con la representación gráfica de la función trigonométrica seno:

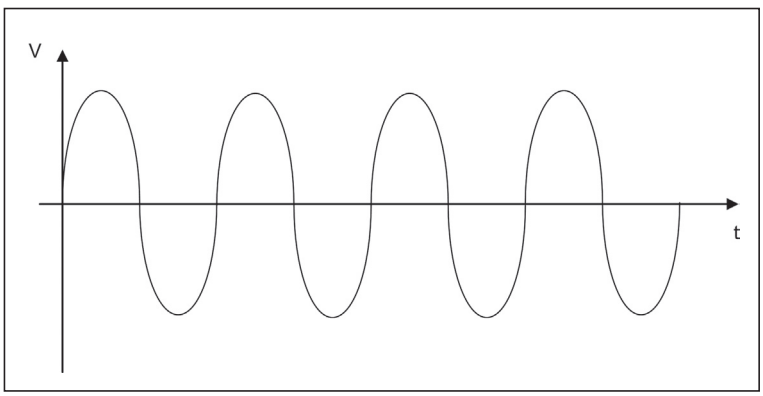


Figura 2.8. *Señal sinusoidal.*

La expresión matemática que define la función seno es:

$$V(t) = A_0 \operatorname{sen}(wt + \phi)$$

Las señales analógicas simples se describen mediante tres características: amplitud, frecuencia y fase.

La amplitud de una señal es el valor de la magnitud eléctrica de la señal en un instante dado. La amplitud máxima o amplitud de pico es el valor más alto que puede alcanzar. En la expresión matemática anterior este valor se corresponde con A_0. Los valores de amplitud se miden en las unidades de la magnitud eléctrica considerada, por ejemplo, voltios, amperios...

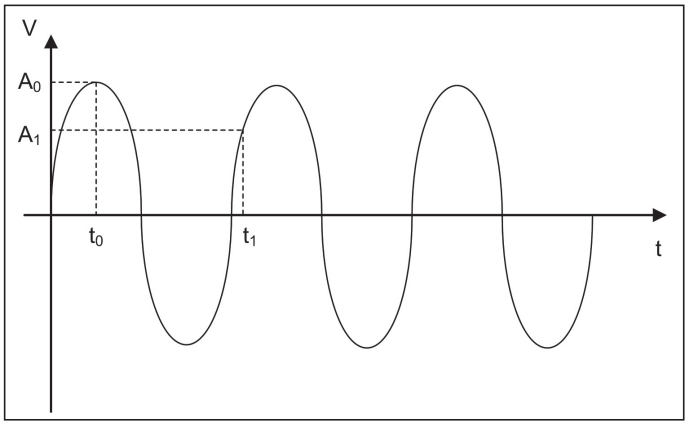


Figura 2.9. *La amplitud en las señales sinusoidales.*

La frecuencia es el número de veces que se presenta el patrón de repetición (ciclo) de la señal en un segundo, o dicho de otra forma, es el número de períodos que se producen en un segundo. La frecuencia se mide en ciclos por segundo, unidad conocida como Hertzio (Hz) aunque también es muy común utilizar múltiplos de esta unidad:

Kiloherzio (KHz)	10^3 Hz
Megahertzio (MHz)	10^6 Hz
Gigahertzio (GHz)	10^9 Hz
Terahertzio (THz)	10^{12} Hz

Como se observa en la figura, se cumple que la frecuencia es la inversa del período y viceversa. En la expresión matemática de la señal sinusoidal la frecuencia se representa por el factor wt, que se puede representar por $2\pi t/T$.

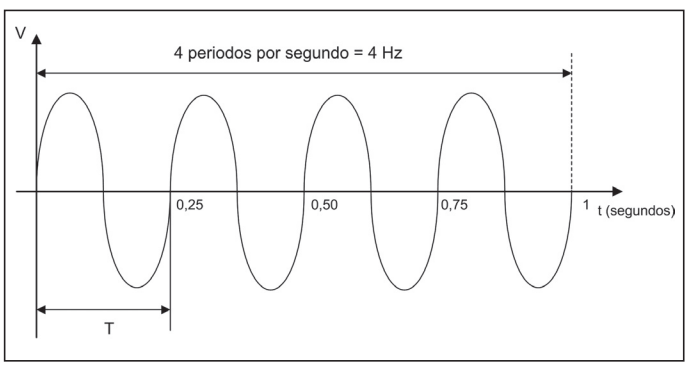


Figura 2.10. *La frecuencia en una señal sinusoidal.*

La frecuencia es la característica de una señal que nos proporciona una medida de lo rápido que cambia la señal. Cuanta más alta sea la frecuencia de una señal más rápido cambia.

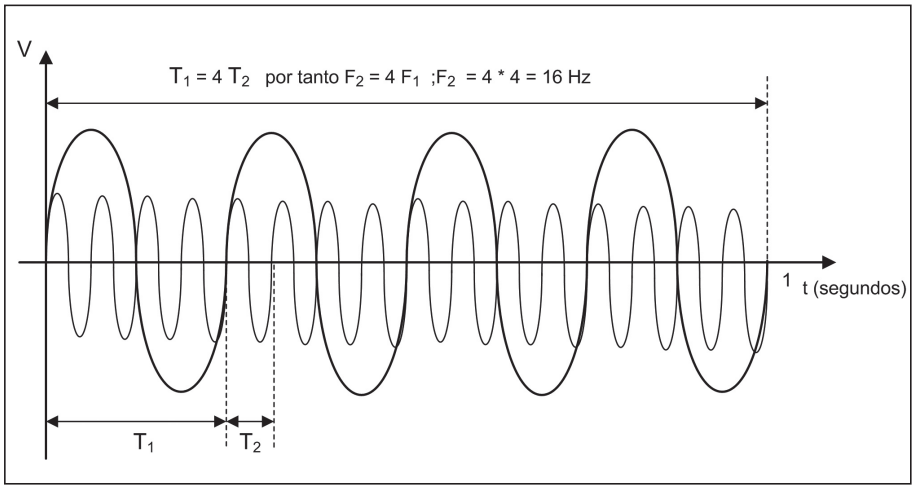


Figura 2.11. *Comparación de dos señales con distinta frecuencia.*

La fase de una señal analógica simple describe la posición de la señal respecto a una posición de referencia. Normalmente esa posición de referencia se toma en el origen de las coordenadas de la gráfica. En la expresión matemática de la onda sinusoidal la fase se representa por el factor ϕ.

La fase se mide en grados o radianes, teniendo en cuenta que la fase puede tener un valor máximo de 360º, que se corresponde a 2π radianes. En la figura siguiente se representan señales con un desplazamiento de fase de 0º, 90º, 180º y 270º.

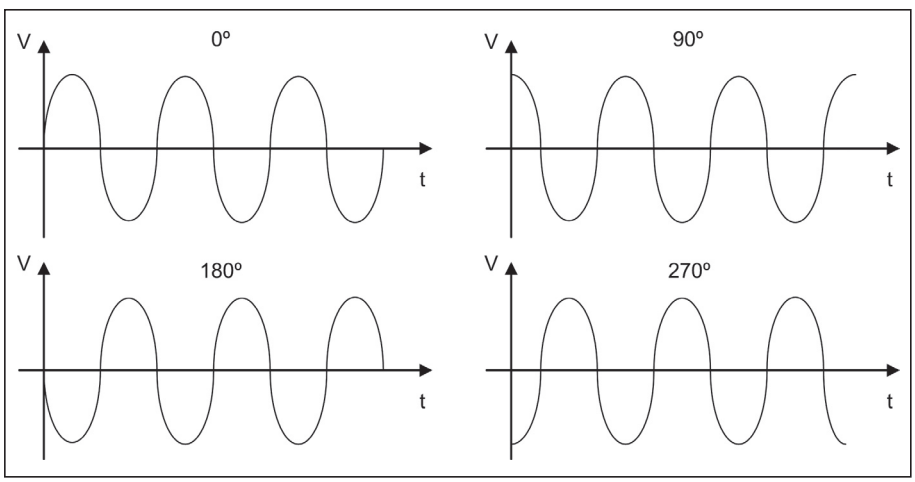


Figura 2.12. *Comparación de señales con diferentes fases.*

En la práctica, la fase de una señal representa la diferencia de posición respecto a otra señal que se toma como referencia.

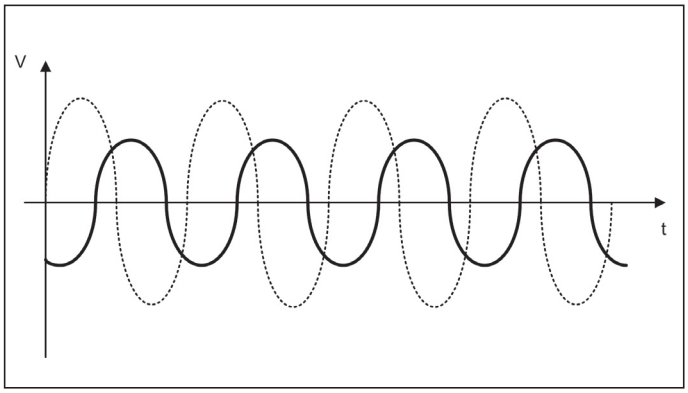


Figura 2.13. *Fase de una señal respecto a otra señal de referencia.*

2.2.4 SEÑALES ANALÓGICAS COMPUESTAS

Las señales analógicas compuestas son señales periódicas cuya variación no sigue la forma onda sinusoidal.

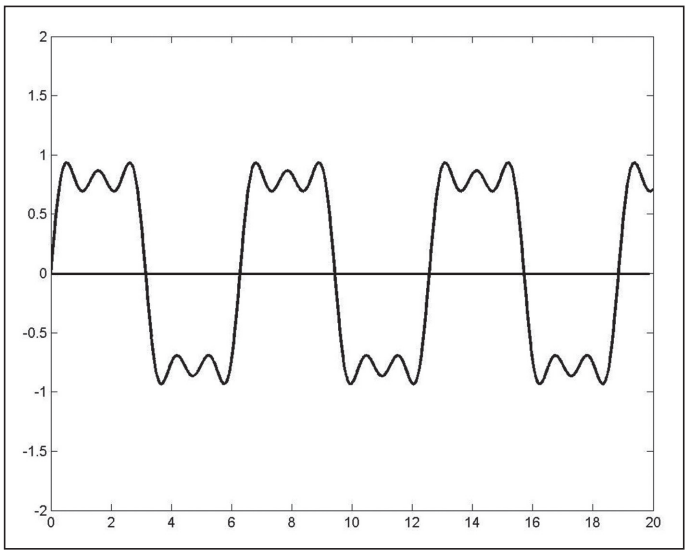


Figura 2.14. *Ejemplo de señal periódica compuesta.*

Se puede demostrar, mediante la teoría matemática conocida como análisis de Fourier, que cualquier señal periódica, sin importar su complejidad, se puede descomponer en una serie de señales simples sinusoidales, cada una de ellas con una amplitud, frecuencia y fase determinadas. Al proceso de descomposición de una señal periódica en la suma de señales simples se le conoce como **Series de Fourier**.

Por tanto, cualquier señal periódica de período T se puede representar mediante la siguiente expresión:

$$V(t) = A_0 + A_1 \text{sen}(wt+\theta_1) + A_2 \text{sen}(2wt+\theta_2) + A_0 \text{sen}(3wt+\theta_3) + \ldots + A_n \text{sen}(nwt+\theta_n)$$

donde $w = 2\pi f$, siendo $f = 1/T$.

Como se observa, el primer componente de tipo sinusoidal de la Serie de Fourier sería una señal sinusoidal con un período igual al período de la señal original. La frecuencia de este primer componente ($f = 1/T$) se conoce como **frecuencia fundamental**. El resto de componentes son señales sinusoidales con frecuencias múltiplos enteros de la frecuencia fundamental conocidos como **armónicos**.

Obviando todo el desarrollo matemático, el proceso de descomposición se puede observar de forma gráfica en la siguiente figura:

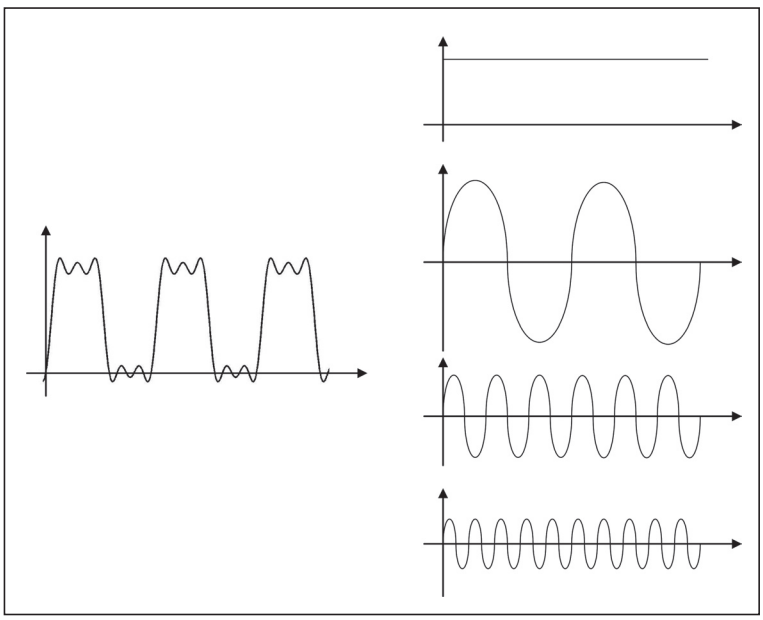


Figura 2.15. *Señal periódica formada por cuatro componentes sinusoidales.*

La aplicación del análisis de Fourier a las Telecomunicaciones es fundamental para estudiar el contenido frecuencial de las señales compuestas.

2.2.5 EL DOMINIO DE LA FRECUENCIA: ESPECTRO Y ANCHO DE BANDA

Hasta ahora, las señales se han representado mediante un gráfico que muestra la variación de la magnitud eléctrica (amplitud de la señal) en función del tiempo.

Este tipo de representación de las señales se denomina representación en el dominio del tiempo.

Existe otro tipo de representación de las señales conocido como dominio de la frecuencia. En este caso, se representa la relación entre la amplitud de la señal y la frecuencia. En el siguiente gráfico se puede ver la representación en el dominio de la frecuencia de una señal sinusoidal. Como se observa, en el dominio de la frecuencia se refleja solamente la amplitud máxima o de pico.

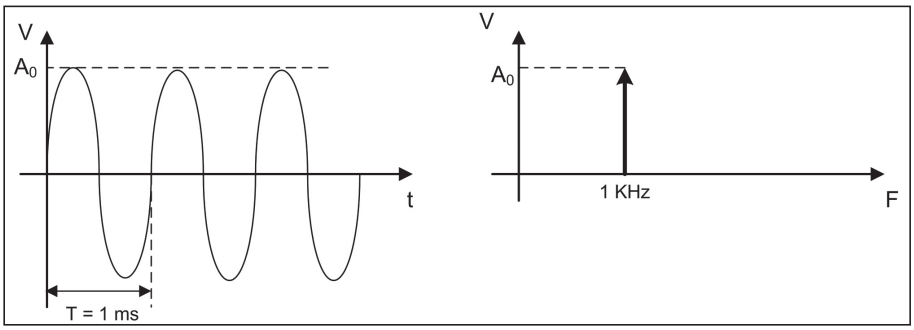


Figura 2.16. *Representación de una señal sinusoidal en el dominio de la frecuencia.*

De la misma forma, una señal periódica compuesta se representa en la frecuencia como una serie de componentes discretas situadas en la frecuencia fundamental y en sus diferentes armónicos.

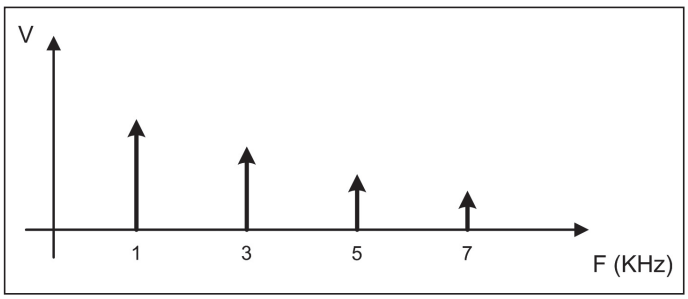


Figura 2.17. *Representación en el dominio de la frecuencia de una señal periódica compuesta.*

La representación de señales en el dominio de la frecuencia añade dos nuevos conceptos:

- **Espectro:** es la representación de una señal en el dominio de la frecuencia.
- **Ancho de banda:** es la anchura del espectro de una señal. O dicho de otra forma, la diferencia entre el componente más alto de frecuencia y el más bajo.

El concepto de ancho de banda se puede apreciar claramente en la siguiente figura:

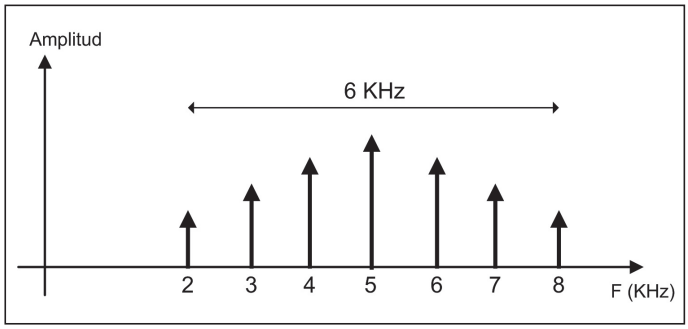


Figura 2.18. *Ancho de banda.*

La descomposición de una señal periódica en señales sinusoidales utilizando las Series de Fourier es fundamental para representar señales periódicas en el dominio de la frecuencia. Para el conocimiento de las componentes de frecuencia de señales aperiódicas se utiliza otra herramienta matemática conocida como **Transformada de Fourier**. En este caso, el espectro de una señal aperiódica es continuo.

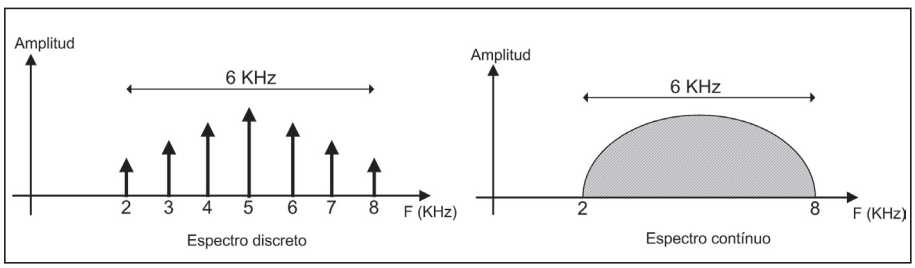


Figura 2.19. *Espectro continuo vs. discreto.*

Hay algunas relaciones interesantes entre el dominio del tiempo y el dominio de la frecuencia que conviene tener en cuenta:

- ✓ Los cambios rápidos de la amplitud de una señal en el dominio del tiempo dan lugar a componentes de frecuencia altos.
- ✓ Los cambios lentos de la amplitud de una señal en el dominio del tiempo dan lugar a componentes de frecuencia bajos.
- ✓ Si la amplitud de una señal no cambia nunca (señal continua), su frecuencia es cero.
- ✓ Si una señal cambia su valor de forma instantánea, su frecuencia es infinito.

Por último, es interesante apuntar que existe una relación entre las Series y la transformada de Fourier: la Transformada de Fourier de una señal aperiódica es la envolvente de las Series de Fourier para esa misma señal convertida en periódi-

ca. Para aclarar esta afirmación se utilizará como ejemplo una señal aperiódica conocida como pulso y su correspondiente señal periódica, conocida como tren de pulsos.

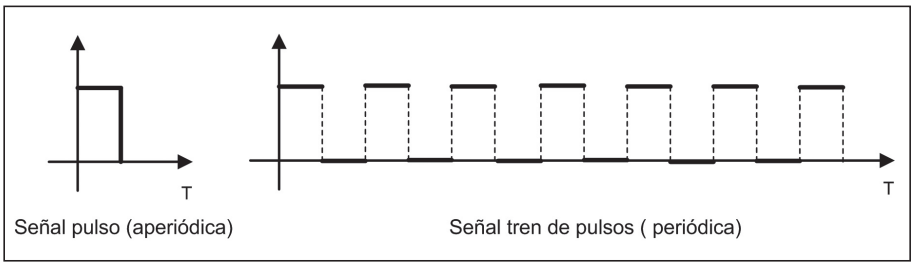


Figura 2.20. *Representación de las señales pulso y tren de pulsos.*

A continuación se puede observar la representación en el dominio de la frecuencia de estas dos señales obtenidas mediante la transformada y Series de Fourier respectivamente.

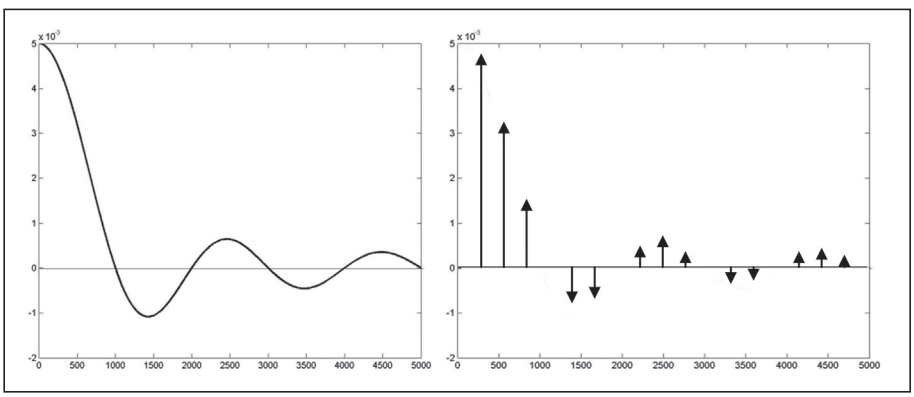


Figura 2.21. *Señales pulso y tren de pulsos en el dominio de la frecuencia.*

Se puede apreciar como el espectro de la señal pulso es la envolvente del espectro de la señal tren de pulsos. Sería como unir todos los puntos del espectro discreto del tren de pulsos para obtener el espectro continuo del pulso.

NOTA 2.2

Si una señal compuesta es periódica, se descompone en una serie de señales con frecuencias discretas (espectro discreto).
Si la señal compuesta es aperiódica, se descompone en una serie de señales con frecuencias continuas (espectro continuo).

2.2.6 SEÑALES DIGITALES

Los parámetros utilizados para describir las señales analógicas simples no son apropiados para las señales digitales. Es más, las señales digitales normalmente son aperiódicas por lo que ni siquiera resulta apropiado hablar de frecuencia. Para las señales digitales utilizadas en la transmisión de datos se utilizan dos nuevas características:

- **Intervalo de bit.** Es el tiempo necesario para transmitir un bit. Equivale al período en las señales periódicas. Se mide en segundos o submúltiplos.
- **Tasa de bits.** Es el número de bits transmitidos en un segundo. Equivale a la frecuencia en señales periódicas. La tasa de bits también se conoce como velocidad de transmisión. Se mide en bits por segundo (bps) o múltiplos como Kbps, Mbps…

NOTA 2.3

Las señales digitales periódicas normalmente son utilizadas cono patrón o reloj para los sistemas digitales síncronos, por lo tanto no contienen información. En este caso sí se utiliza la frecuencia como parámetro característico.

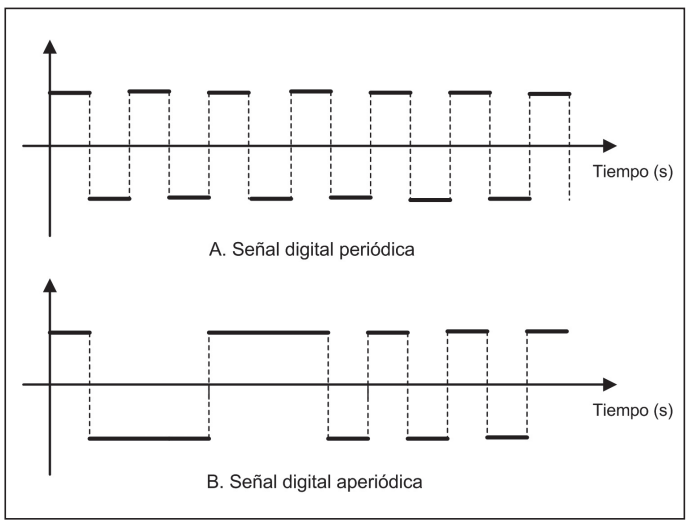


Figura 2.22. *Comparación señal digital periódica y aperiódica con sus parámetros característicos.*

En el apartado anterior se apuntó una idea importante y que afecta directamente a las señales digitales: si una señal cambia su valor de forma instantánea, su frecuencia es infinito. Como se puede observar en la siguiente figura, en cada discontinuidad de la señal se produce precisamente este hecho, su valor cambia

de forma instantánea. Es decir, para transmitir una señal digital de forma exacta sería necesario un ancho de banda infinito. Lógicamente en la práctica esto es imposible, por lo que habrá que establecer qué ancho de banda es necesario para transmitir señales digitales sin que se pierda la información que representa. El siguiente apartado resuelve esta cuestión.

NOTA 2.4

Las señales digitales tienen un ancho de banda infinito.

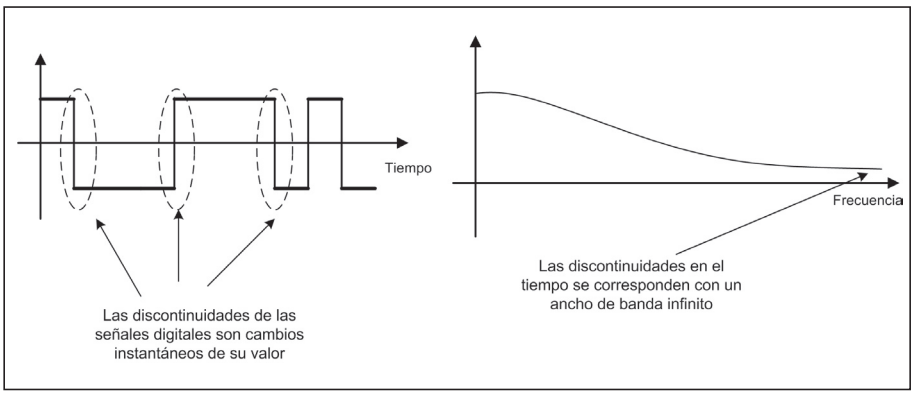


Figura 2.23. *Discontinuidad de las señales digitales.*

2.3 MEDIOS DE TRANSMISIÓN

El medio de transmisión constituye el soporte físico a través del cual emisor y receptor pueden comunicarse en un sistema de transmisión de datos. Distinguimos dos tipos de medios: **guiados** y **no guiados**. En ambos casos, la transmisión se realiza por medio de ondas electromagnéticas. Los medios guiados conducen las ondas a través de un campo físico (cables). Los medios no guiados proporcionan un soporte para que las ondas se transmitan, pero no las dirigen (como es el aire).

La naturaleza del medio, junto con la de la señal que se transmite a través de él, constituye un factor determinante de las características y la calidad de la transmisión. En el caso de medios guiados, es el propio medio el que determina las limitaciones de la transmisión. Las transmisiones a través de medios no guiados, sin embargo, están muy influidas por las condiciones atmosféricas.

En los próximos apartados se repasan las características de los medios de transmisión más comunes.

2.3.1 PAR TRENZADO

El **par trenzado** consiste en dos cables de cobre aislados, normalmente de 1 mm de espesor, enlazados de dos en dos de forma helicoidal. La forma trenzada del cable se utiliza para reducir la interferencia eléctrica con respecto a los pares cercanos y a otras interferencias procedentes del exterior, ya que dos conductores próximos y paralelos constituyen una antena simple y por tanto son capaces de captar señales electromagnéticas cercanas, lo que produce interferencias.

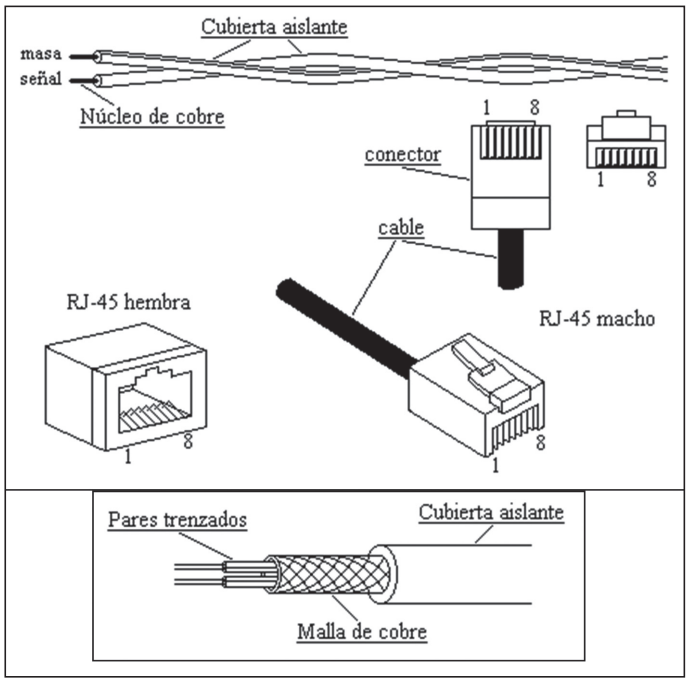


Figura 2.24. *Cable de par trenzado.*

La figura anterior muestra la forma de un par trenzado y los conectores habituales para este tipo de configuración. El clásico uso del cable de cobre de par trenzado ha sido en el sistema telefónico para transportar señales analógicas vocales. Sin embargo, con la llegada de las primeras redes de datos, se han desarrollado cables de cobre con características mejoradas que permiten transferencias de señales digitales. Su bajo coste y fácil instalación hacen que el cable de par trenzado sea actualmente uno de los medios de transmisión más utilizados.

Existen varios tipos de cables de par trenzado:

- **Pares trenzados no apantallados (UTP):** son los más simples y no tienen ningún tipo de pantalla conductora. Su impedancia característica es de 100 Ω y es muy sensible a interferencias. El par trenzado UTP categoría 5 está recubierto de una malla de teflón que no es conductora.

- **Pares trenzados apantallados individualmente (STP):** son iguales que los anteriores, pero en este caso se rodea a cada par de una malla conductora, que se conecta a las diferentes tomas de tierra de los equipos. Son los que poseen una mayor inmunidad al ruido.
- **Pares trenzados apantallados (FTP):** son unos cables de pares que poseen una pantalla conductora global en forma trenzada. Mejora la protección frente a interferencias y su impedancia es de 120 Ω.

Así mismo, dependiendo del número de pares que tenga un cable, el número de vueltas por metro que posee su trenzado y los materiales utilizados, los estándares de cableado estructurado clasifican a los tipos de pares trenzados por categorías: **categoría 1** (cable paralelo), **categoría 2**, **categoría 3**, **categoría 4**, **categoría 5**, **categoría 5e**, **categoría 6** y **categoría 7**.

2.3.2 CABLE COAXIAL

El **cable coaxial** es otro medio típico de transmisión. Este cable tiene mejor blindaje que el par trenzado, por lo que puede alcanzar velocidades de transmisión mayores y los tramos entre repetidores o estaciones pueden ser más largos.

El cable coaxial consta de un alambre de cobre duro en su parte central por donde circula la señal, el cual se encuentra rodeado por un material aislante. Este material está rodeado por un conductor cilíndrico presentado como una malla de cobre trenzado que hace de masa. El conductor externo está cubierto por una capa de plástico protector. Esta construcción le confiere un elevado ancho de banda y excelente inmunidad al ruido.

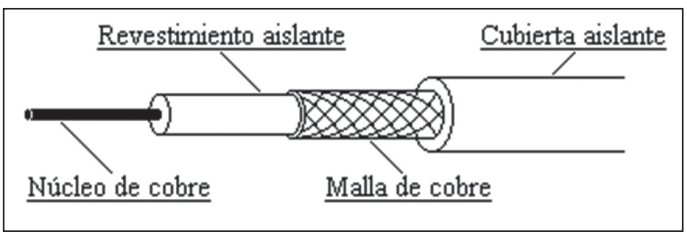


Figura 2.25. *Cable coaxial.*

La figura anterior muestra la estructura de un cable coaxial. La velocidad de transmisión de este cable depende de su longitud y en cables de 1 km es posible entre 1 y 2 Gbps. Los cables coaxiales solían utilizarse en el sistema telefónico, pero ahora se les ha reemplazado por fibra óptica en rutas de largo recorrido y troncales de gran ancho de banda. También se utilizó ampliamente para las primeras implementaciones de redes Ethernet. Actualmente, el cable coaxial todavía se utiliza para la televisión por cable y para los tramos locales de algunos tipos de líneas de datos.

Hay varios tipos de cable coaxial, los más conocidos son:

- **RG-8,** conocido como coaxial grueso, con alrededor de 1 cm de diámetro y 50 Ω de impedancia. Este tipo se ha utilizado ampliamente en las redes de área local aunque actualmente no se usa.
- **RG-58,** conocido como coaxial fino, con un diámetro de 0,5 cm y 50 Ω de impedancia. Al igual que el anterior, se han utilizado para redes de área local aunque actualmente no se usa.
- **RG-59,** este tipo de unos 0,6 cm de diámetro y 75 Ω de impedancia se utiliza actualmente en las redes de transmisión de señales de televisión por cable.

Los conectores que se utilizan para el cableado coaxial se conocen como conector BNC.

2.3.3 FIBRA ÓPTICA

La fibra óptica está basada en la utilización de las ondas de luz para transmitir información binaria. Un sistema de transmisión óptico tiene tres componentes:

La fuente de luz: se encarga de convertir una señal digital eléctrica (ceros y unos) en una señal óptica. Típicamente se utiliza un pulso de luz para representar un "1" y la ausencia de luz para representar un "0", o se modifica su longitud de onda.

- **El medio de transmisión:** se trata de una fibra de vidrio ultradelgada que transporta los pulsos de luz.
- **El detector:** se encarga de generar un pulso eléctrico en el momento en el que la luz incide sobre él.

Al conectar una fuente de luz en un extremo de una fibra óptica y un detector en el otro, tenemos un sistema de transmisión de datos símplex que acepta una señal eléctrica, la convierte y transmite en pulsos de luz y, después, reconvierte la salida a una señal eléctrica en el extremo del receptor.

La fibra óptica está cuidadosamente diseñada para transportar señales de luz. Se trata de un cilindro de pequeña sección flexible, con un diámetro del orden de 2 a 125 μm (como comparación, el grosor del cabello humano es de alrededor de 50 μm) por el que se transmite la luz, recubierto de un medio con un índice de refracción menor que el del núcleo a fin de mantener toda la luz en el interior de él. A continuación viene una cubierta plástica delgada para proteger el revestimiento e impedir que cualquier rayo de luz del exterior penetre en la fibra. Finalmente, varias fibras suelen agruparse en haces protegidos por una funda exterior, como se muestra en la siguiente figura.

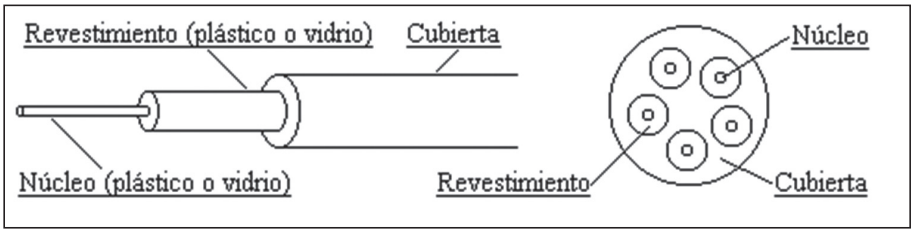


Figura 2.26. *Fibra óptica.*

Los cables de fibra óptica pueden transmitir la luz de tres formas diferentes:

- **Monomodo:** en este caso, la fibra es tan delgada que la luz se transmite en línea recta. El núcleo tiene un radio de 10 μm y la cubierta, de 125 μm.
- **Multimodo:** la luz se transmite por el interior del núcleo incidiendo sobre su superficie interna, como si se tratara de un espejo. Las pérdidas de luz en este caso también son prácticamente nulas. El núcleo tiene un diámetro de 100 μm y la cubierta, de 140 μm.
- **Multimodo de índice gradual:** la luz se propaga por el núcleo mediante una refracción gradual. Esto es debido a que el núcleo se construye con un inci-de de refracción que va en aumento desde el centro a los extremos. Suele tener el mismo diámetro que las fibras multimodo.

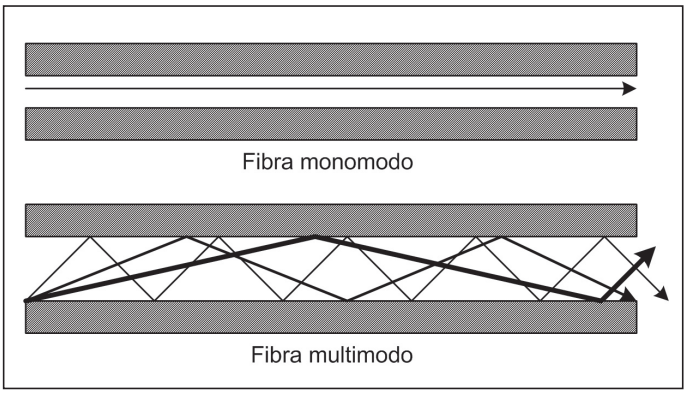


Figura 2.27. *Modos de transmisión en fibra óptica.*

Los conectores utilizados en fibra óptica exigen una alta precisión ya que cualquier mínima desviación puede producir pérdidas apreciables en la potencia de la señal transmitida. Existen varios modelos de conectores de fibra en el mercado como son los conectores FC, LC, FDDI, SC, SC dúplex o ST.

Las principales ventajas de la fibra óptica como medio de transmisión son:

- **Ancho de banda muy alto,** que permite la transmisión de las señales con velocidades elevadas del orden de varios GHz.

- **Inmunidad frente al ruido.** Las señales ópticas no se ven afectadas por ningún tipo de perturbación electromagnética.
- **Atenuación baja.** Lo que permite alcanzar distancias altas sin necesidad de utilizar repetidores o regeneradores de señal.

Las principales desventajas son:

- **Coste.** Es el medio de transmisión más caro debido a que el proceso de fabricación es complejo.
- **Instalación y mantenimiento especializado.** La manipulación de cable de fibra deber hacerse con más cuidados ya que es un cable más frágil. Por otra parte, los conectores exigen también una alta precisión.

2.3.4 MEDIOS INALÁMBRICOS

La comunicación inalámbrica (que no necesita de ningún tendido de cable entre el emisor y el receptor) resulta indispensable para aquellos usuarios móviles que necesitan estar continuamente "en línea". También es de mucha utilidad cuando resulta muy costoso tender hilos de comunicación en zonas geográficas de difícil acceso.

Las comunicaciones inalámbricas consisten en el envío y recepción de electrones (o fotones) que circulan por el espacio libre (el aire). Estos electrones viajan en forma de ondas electromagnéticas que se propagan del mismo modo que las ondas del agua en un estanque. La distancia que separa dos "picos" o máximos consecutivos de esas ondas se llama **longitud de onda** y se designa universalmente con la letra griega λ (lambda). Hay que decir que para las ondas electromagnéticas que circulan por el aire no se utiliza la medida del período de la señal. La relación entre la frecuencia (*f*) y la longitud de onda (λ) de la señal viene expresada por la siguiente ecuación:

$$c = \lambda \cdot f$$

Dependiendo de la frecuencia de la señal (y, por extensión, de su longitud de onda), existen diferentes tipos de enlaces inalámbricos, exhibiendo diferentes propiedades. Éstos se explican en los apartados siguientes.

Ondas de radio

Las **ondas de radio** son fáciles de generar, pueden viajar largas distancias, penetran en los edificios sin problemas y viajan en todas direcciones desde la fuente emisora. Sin embargo, por la capacidad que tienen de viajar a largas distancias, es necesario realizar un control estricto por parte de los gobiernos para que las diferentes transmisiones no se interfieran entre sí.

Existen dos tipos de ondas de radio:

- ✓ **Ondas de radio de baja frecuencia:** se caracterizan porque en su recorrido siguen la curvatura de la Tierra y pueden atravesar con facilidad los edificios. Sin embargo, su ancho de banda sólo permite velocidades de transmisión bajas.
- ✓ **Ondas de radio de alta frecuencia:** estas ondas tienden a ser absorbidas por la Tierra, por lo que deben ser enviadas a la ionosfera donde son reflejadas y devueltas de nuevo, con lo que se consigue transmitir a largas distancias.

Microondas

Además de su aplicación en hornos, las **microondas** permiten transmisiones tanto terrestres como con satélites. Sus frecuencias están comprendidas entre 1 y 10 Ghz y posibilitan velocidades de transmisión aceptables, del orden de 10 Mbps. Por encima de los 1.000 Hz, las microondas viajan en línea recta y, por tanto, se pueden enfocar en un haz de pequeña anchura. Concentrar toda la energía en un haz pequeño con una antena parabólica produce una relación señal/ruido muy alta (es decir, la amplitud del ruido puede ser muy pequeña), pero las antenas del emisor y el receptor deben estar muy bien alineadas entre sí.

A diferencia de las ondas de radio, las microondas no atraviesan bien los obstáculos, de forma que es necesario situar antenas repetidoras cuando queremos realizar comunicaciones a largas distancias. En el caso de las comunicaciones por satélite, hay que tener en cuenta que siempre existe un pequeño retardo en las transmisiones debido a que la señal tarda aproximadamente 0,3 segundos en llegar y volver. Para algunas aplicaciones de envío y recepción de datos, este tiempo de espera puede resultar inaceptable.

Ondas infrarrojas

Las ondas infrarrojas y milimétricas se utilizan mucho para la comunicación de corto alcance, en controles remotos de televisores, grabadoras de video, estéreos, etc. También es frecuente encontrar un puerto de comunicación infrarroja en los ordenadores portátiles. Estos controles son relativamente direccionales, baratos y fáciles de construir, pero tienen un inconveniente importante: no atraviesan los objetos sólidos. Este inconveniente también resulta a veces una ventaja en el sentido de que ofrecen más seguridad, precisamente porque la comunicación no atraviesa las paredes de un edificio. Además, no es necesario obtener licencia del gobierno para operar con un sistema de transmisión infrarrojo.

Ondas de luz

Es posible comunicar dos edificios mediante un láser montado en cada azotea. La señalización óptica coherente mediante láser es unidireccional, de modo que cada edificio necesita un emisor láser y un receptor. Este esquema ofrece un coste muy bajo, es fácil de instalar y posee una elevada velocidad de transmisión. Por su parte las desventajas de este sistema son:

- ✓ Es difícil colocar correctamente los emisores y los receptores.
- ✓ El rayo láser no puede penetrar la lluvia y la niebla densa.
- ✓ Las corrientes de convección (aire caliente que sube del edificio) interfieren también en el haz de láser.

2.4 TRANSMISIÓN EN BANDA BASE DE SEÑALES DIGITALES

Se denomina banda base al conjunto de señales que son transmitidas en su frecuencia original a la salida de la fuente que las origina, es decir, no sufren ningún proceso de modulación. Como contraposición, si una señal se transmite variando las frecuencias originales, se dice que la señal ha sido modulada. La modulación como técnica de transmisión de datos se estudiará en un próximo apartado.

La transmisión en banda base se utiliza para distancias relativamente cortas y cuando el medio de transmisión lo permita, esto es, cuando el medio actúe como un filtro paso bajo y no como un filtro paso banda. Es decir, el medio de transmisión debe permitir la transmisión de señales con frecuencia baja incluyendo componentes de frecuencia cero, es decir, componentes de señal continua.

En los Sistemas Telemáticos, la información que se maneja es de naturaleza digital y en algunas ocasiones será necesario transmitir la información digital utilizando señales digitales. Es lo que se conoce como transmisión en banda base de señales digitales. Para ello habrá que tener en cuenta dos factores, la capacidad del canal de transmisión y la frecuencia de la propia señal digital, que en teoría es infinito.

Capacidad de un canal

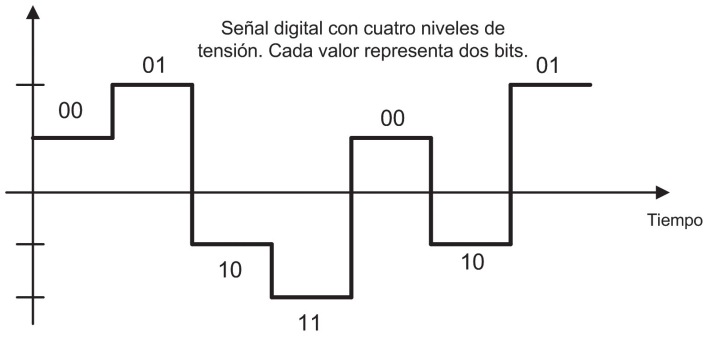
Para la transmisión de señales digitales en banda base, Nyquist determinó que la máxima velocidad alcanzable para un ancho de banda dado es dos veces dicho ancho de banda si no existe ruido.

$$C = 2\ BW$$

C es la velocidad de transmisión (o tasa de bits) y BW (Bandwidth) es el ancho de banda del canal. Si se tienen señales digitales de más de dos niveles, es decir que cada elemento de la señal representa más de un bit, la fórmula de Nyquist resulta:

$$C = 2\ BW \log_2 M$$

donde M es la cantidad de niveles.



Esta fórmula establece la capacidad máxima teórica sin ruido con la que se puede transmitir una señal digital a través de un canal con un ancho de banda dado.

NOTA 2.5

Ejemplo: aplicando la fórmula anterior, un canal de 10 MHz de ancho de banda que no se vea afectado por ruido puede transmitir señales digitales con una velocidad de 20 Mbps.

Ancho de banda efectivo

Como hemos visto, una señal digital es una señal con un ancho de banda infinito. En una transmisión en banda base, el ancho de banda requerido es proporcional a la tasa de bits o velocidad de transmisión, por lo tanto, si se necesita enviar bits más rápidos, se necesita más ancho de banda.

El ancho de banda requerido por tanto para transmitir una señal digital en banda base depende de la precisión deseada. Lo mínimo es transmitir el primer armónico:

$$BW = \text{Tasa de bits} / 2$$

Se pueden transmitir, para mayor precisión, los siguientes armónicos, múltiplos impares del primer armónico.

Por ejemplo, para una señal de 1 Mbps se debe utilizar un ancho de banda de 500 KHz como mínimo, para transmitir el primer armónico. Si se desea transmitir el primero y el tercero se necesita un ancho de banda de 1,5 MHz (3 x 500 KHz).

2.5 CODIFICACIÓN

La codificación es la representación de la información digital mediante una señal digital. Básicamente consiste en traducir los ceros y unos binarios que se desea transmitir a una secuencia de pulsos de voltaje, adecuada para su transmisión. La codificación es la técnica fundamental utilizada en las transmisiones digitales en banda base.

En los siguientes apartados se describirán los principales tipos de codificaciones utilizadas en los sistemas telemáticos.

2.5.1 EJEMPLO BÁSICO: CODIFICACIÓN UNIPOLAR

La codificación unipolar es el tipo de codificación más sencilla y primitiva, y que actualmente se considera obsoleta. Su principal ventaja es su sencillez. Para codificar información digital (ceros y unos) mediante esta técnica, se asigna a cada nivel lógico un nivel de voltaje usando únicamente una polaridad. Por ejemplo, los "unos" se codifican con un valor de voltaje positivo y los "ceros" se codifican con el valor de voltaje cero.

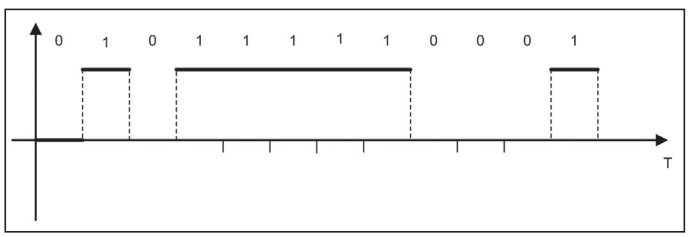


Figura 2.28. *Codificación unipolar.*

Los datos se codifican para solucionar principalmente dos aspectos inherentes a la banda base:

- ✓ Disminuir la componente continua
- ✓ Proveer sincronismo entre transmisor y receptor

No es posible enviar junto con los datos una señal de sincronismo. El receptor se sincroniza por medio de las transiciones de pulsos recibidos. Pero si se tiene una larga secuencia de ceros o de unos, la señal permanece constante durante un tiempo bastante largo en la línea y el receptor no puede identificar el principio y fin de cada bit.

2.5.2 CODIFICACIÓN POLAR

La codificación polar utiliza dos niveles de voltaje, con la misma amplitud pero con polaridades diferentes, es decir, un nivel con polaridad positiva y el otro con

polaridad negativa. Con esta característica se consigue reducir la componente continua. Existen varios tipos de codificaciones polares que se explican a continuación.

■ 2.5.2.1 NRZ-L

En este tipo de codificación polar, cada valor lógico se codifica con uno de los niveles de tensión. Normalmente, un nivel de voltaje positivo representa un 0 y un nivel de voltaje negativo representa un 1. En la siguiente figura se muestra un ejemplo de codificación NRZ-L:

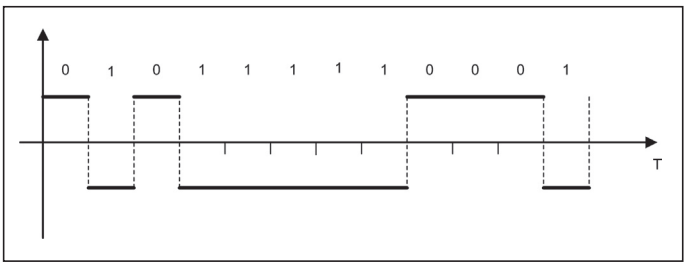


Figura 2.29. *Codificación NRZ-L.*

Aunque con la codificación NRZ-L se consigue reducir el valor de la componente continua, que sería nula si en la transmisión hubiera el mismo porcentaje de ceros y unos, sigue existiendo el problema del sincronismo para secuencias largas de ceros y unos.

■ 2.5.2.2 NRZ-I

En este tipo de codificación, un nivel lógico 1 se representa con una inversión del nivel de voltaje, y un nivel lógico 0 se representa sin ningún cambio de polaridad. En la siguiente figura se muestra un ejemplo de codificación NRZ-I:

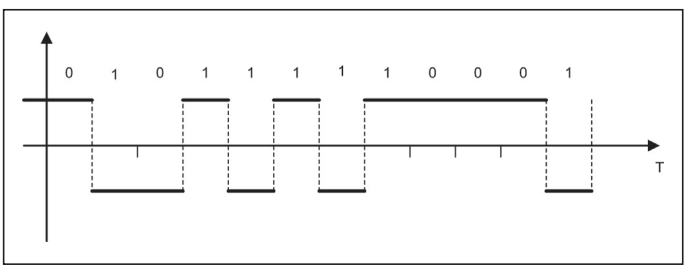


Figura 2.30. *Codificación NRZ-I.*

En este caso, se introduce una mejora respecto a la codificación NRZ-L ya que, además de reducir el valor de la componente continua, característica común en todas las codificaciones polares, se consigue reducir el problema de sincronismo ya que éste sólo afecta a las secuencias largas de ceros.

2.5.2.3 RZ

En la codificación RZ, para solucionar los problemas de sincronismo se utilizan tres niveles de voltaje: positivo, negativo y cero. De esta forma, se produce un cambio de voltaje en cada bit, lo que se utiliza para sincronizar cada bit enviado.

Un bit con valor 1 se representa por la transición de voltaje positivo a cero y un bit con valor 0 se representa por la transición de voltaje negativo a cero. La transición se lleva a cabo en la mitad del intervalo de bit. En la siguiente figura se puede comprobar el funcionamiento de RZ con un ejemplo:

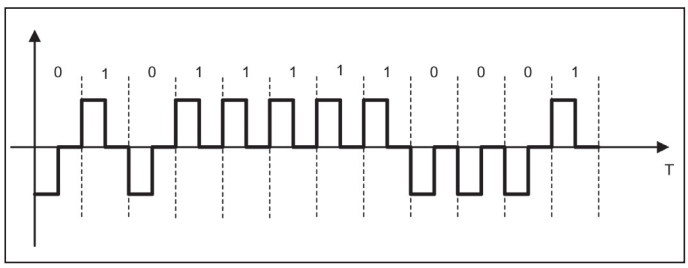


Figura 2.31. *Codificación RZ.*

La única desventaja respecto a los códigos NRZ es que necesita más ancho de banda ya que para cada codificar cada bit se necesitan dos cambios de la señal, es decir, hay más cambios para codificar cada bit por lo tanto la señal tendrá mayor frecuencia.

2.5.2.4 Manchester

En la codificación Manchester, también conocida como codificación bifásica, se usa una inversión de la polaridad de la señal en mitad de cada intervalo de bit. El sentido de la inversión es el que indica el valor del bit codificado. Una transición de negativo a positivo representa un 1 binario y una transición de positivo a negativo representa un 0 binario. En el ejemplo siguiente se puede apreciar este funcionamiento:

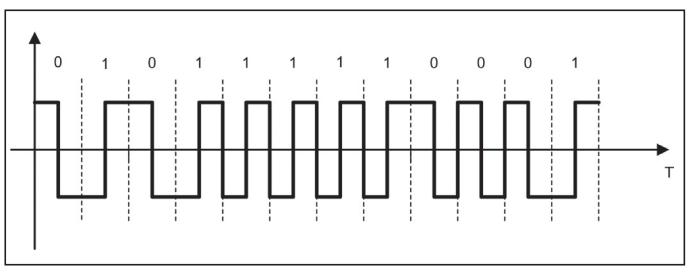


Figura 2.32. *Codificación Manchester.*

La codificación Manchester representa un tipo de codificación bastante eficiente ya que se consigue anular completamente la componente continua y ade-

más proporciona una sincronización en cada bit por lo que no presenta problemas de sincronismo.

2.5.2.5 Manchester diferencial

En la codificación Manchester diferencial se utiliza una transición en la mitad del intervalo de bit para sincronización, igual que en la codificación Manchester, pero la representación de un bit se lleva a cabo por la existencia de inversión o no al principio de cada bit. Una transición al comienzo del intervalo de bit significa un 0 binario y la ausencia de transición significa un 1 binario.

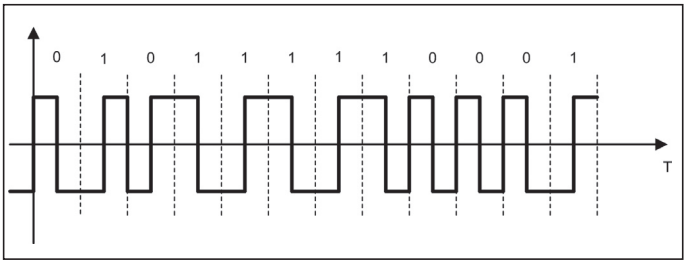


Figura 2.33. *Codificación Manchester diferencial.*

Al igual que en el caso anterior, esta codificación consigue anular la componente continua y solucionar los problemas de sincronismo.

2.5.3 CODIFICACIÓN BIPOLAR

Las codificaciones bipolares utilizan tres niveles de voltaje (positivo, negativo y cero) al igual que en la codificación RZ pero en este caso cada nivel representa un valor lógico. Concretamente, el nivel cero se utiliza para codificar el 0 lógico y el 1 lógico se representa alternando polaridad positiva y negativa. Existen varios tipos de codificaciones bipolares.

2.5.3.1 AMI

La codificación AMI es el tipo de codificación bipolar más sencilla ya que se aplica la regla general mencionada en el párrafo anterior, es decir, el 0 lógico es

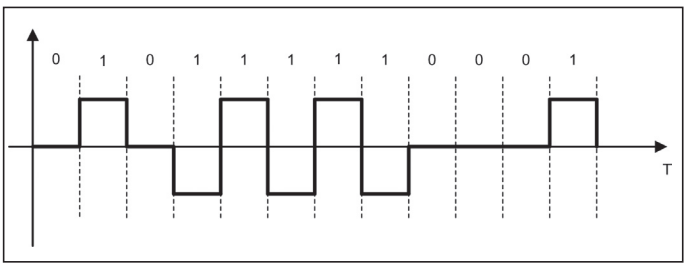


Figura 2.34. *Codificación AMI.*

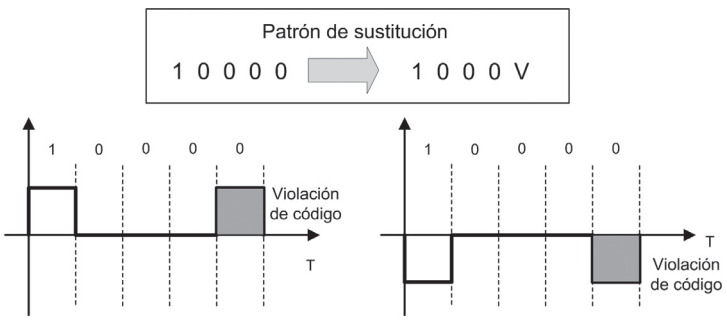
un nivel de tensión cero y el 1 lógico es, alternativamente, voltaje positivo y negativo.

Con este código se elimina prácticamente la componente continua y sólo hay problemas de sincronismo con secuencias largas de ceros.

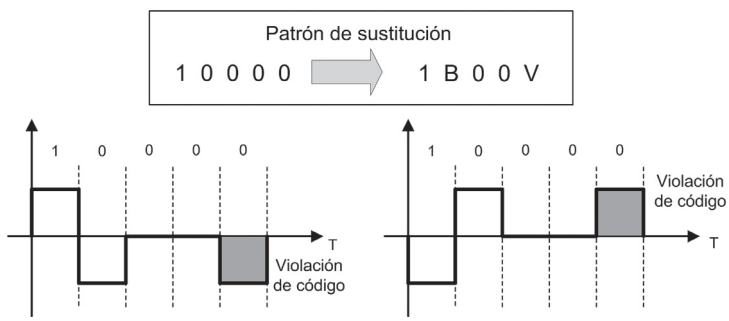
2.5.3.2 HDB3

La codificación HDB3 es la solución de codificación adoptada en Europa (también se utiliza en Japón) para las líneas digitales como las líneas E-1, E-3 y líneas RDSI. Utiliza las mismas reglas que la codificación AMI pero introduce una modificación en este funcionamiento para evitar que las secuencias largas de ceros produzcan problemas de sincronismo. Para ello, cuando se debe codificar una secuencia de cuatro ceros se introduce un patrón determinado llamado patrón de violación, llamado así porque introduce una violación de la regla general de la codificación bipolar precisamente con la finalidad de identificar el patrón claramente. El patrón que se utiliza depende del número de unos codificados desde la última sustitución, es decir, desde la última aplicación del patrón.

Para un número de unos desde la última sustitución impar, la sustitución que se lleva a cabo es:



Para un número de unos desde la última sustitución par, la sustitución que se lleva a cabo es:



En la siguiente figura se representa un ejemplo de codificación HDB3:

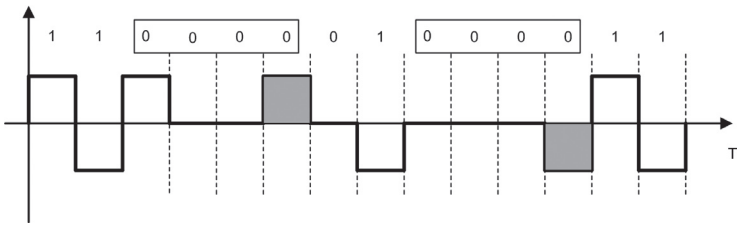


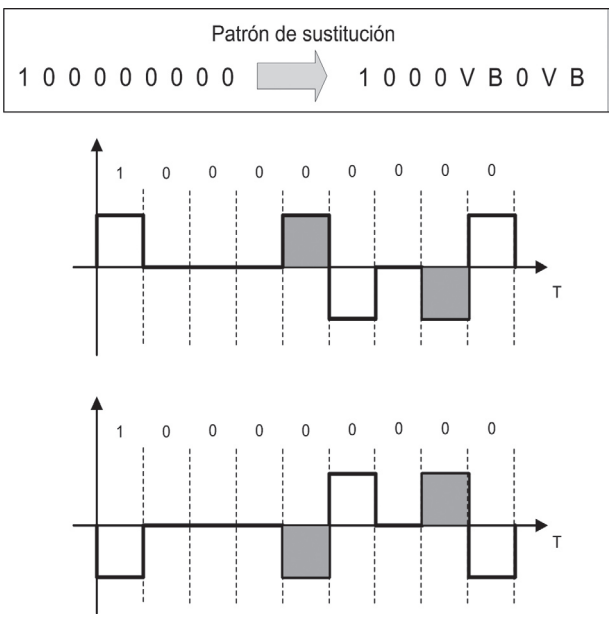
Figura 2.35. *Codificación HDB3.*

Con esta codificación se consigue tanto eliminar la componente continua como evitar los problemas de sincronismo.

■ 2.5.3.3 B8ZS

La codificación B8ZS es la solución de codificación bipolar utilizada en Norteamérica, principalmente para las líneas digitales T-1.

Funciona igual que la codificación AMI pero añade una característica para evitar la pérdida de sincronismo ante secuencias largas de ceros. Cuando aparece en los datos a transmitir una secuencia de ocho ceros consecutivos, éstos son sustituidos por un patrón de violación, igual que en caso de la codificación HDB3. En este caso, el patrón de violación es el siguiente:



En la siguiente figura se puede observar un ejemplo de codificación B8ZS:

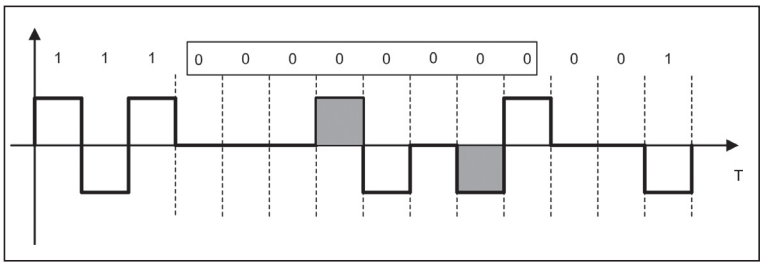


Figura 2.36. *Codificación B8ZS.*

Al igual que HDB3, en la codificación B8ZS se resuelve tanto el problema de la componente continua como el problema de la falta de sincronismo.

NOTA 2.6

Un patrón de violación es una alteración de la codificación original utilizada para evitar secuencias largas de ceros.

2.6 DIGITALIZACIÓN

Actualmente, la mayor parte de la información que transmiten los sistemas telemáticos está representada por datos digitales aunque la información original que se desea transmitir sea analógica. Por ejemplo la voz, música o video son tipos de información que representan magnitudes analógicas y, por tanto, las señales obtenidas son analógicas, sin embargo la tendencia actual es a realizar la transmisión de datos digitales. Para ello y antes de la transmisión en sí, es necesario convertir la señal analógica original a una señal digital. A este proceso se le conoce como digitalización.

Aunque el proceso de digitalización no forma parte de la transmisión de datos propiamente dicha, los parámetros utilizados para llevar a cabo este proceso son una referencia importante en la transmisión de señales de naturaleza analógica. En la siguiente figura se puede observar el proceso que se lleva a cabo para transmitir una señal analógica.

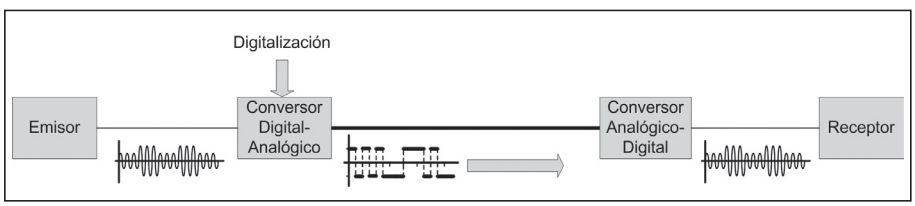


Figura 2.37. *Proceso general de transmisión de señales analógicas.*

El aspecto fundamental de esta conversión es pasar de un conjunto infinito y continuo de valores de una señal analógica a un número discreto de la digital sin perder calidad.

La técnica utilizada se conoce como **Modulación por codificación de pulsos (PCM)** y para llevarla a cabo se utilizan tres pasos:

1. **Muestreo y retención.** Éste es el primer paso que se lleva a cabo. Consiste en tomar muestras de la señal analógica a intervalos regulares de tiempo y mantener el valor muestreado un corto espacio de tiempo para poder llevar a cabo el procesamiento adecuado sobre cada muestra.
2. **Cuantificación.** Éste es el paso crítico de la digitalización. A cada valor muestreado en el paso anterior se le asigna un código binario. Un parámetro de diseño importante es elegir cuántos bits se utilizarán para cuantificar cada muestra. Cuantos más bits se utilicen, más precisión se obtendrá en el proceso de cuantificación.
3. **Codificación.** Por último y después de obtener un código binario de cada muestra, es necesario transformar dichos códigos a señales electromagnéticas. Este proceso se lleva a cabo mediante la codificación, proceso descrito en el apartado anterior.

En la siguiente figura se puede observar todo el proceso de digitalización de forma general.

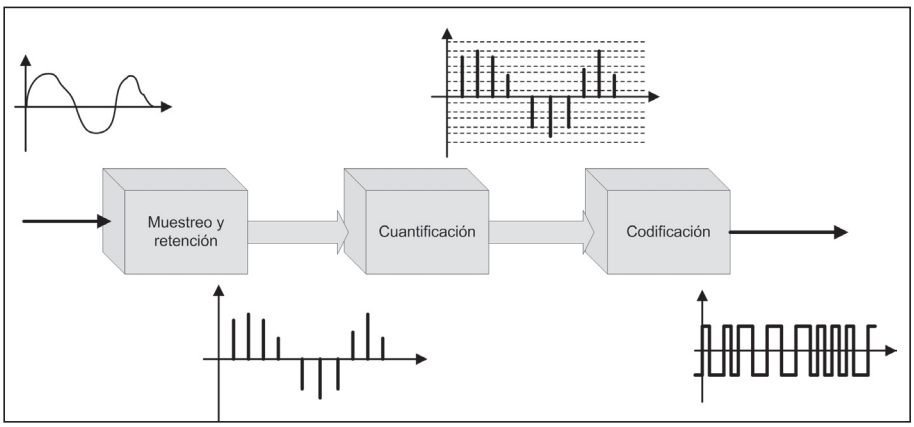


Figura 2.38. *Proceso de digitalización.*

Uno de los principales parámetros que hay que definir cuando se lleva a cabo la digitalización de señales es el número de muestras que se deben de tomar de la señal analógica original. Cabe suponer que para reproducir perfectamente una señal analógica a partir de sus muestras sería necesario un número infinito de muestras. Por tanto, podría suponerse que cuantas más muestras se utilicen más fielmente se reproducirá la señal original.

Sin embargo, y según el **Teorema de Nyquist**, para obtener la reproducción exacta de una señal analógica muestreada, la frecuencia de muestreo debe ser al menos el doble de la frecuencia más alta de la señal muestreada. Se conoce como **frecuencia de muestreo** al número de muestras de la señal tomadas por segundo.

¿Cuántos bits por muestra?

Además de elegir la frecuencia de muestreo apropiada es necesario decidir los bits por muestra utilizados en la cuantificación de la señal. Como ya se ha mencionado, este número dependerá de la precisión que se quiera obtener. Por ejemplo, se desea digitalizar una señal analógica que toma valores entre 0 y 16 V. Si utilizamos 3 bits para codificar el valor muestreado tendremos ocho niveles de cuantificación que estarían asignados, por ejemplo, a los valores: 2, 4, 6, 8, 10, 12, 14 y 16 v.

Al intervalo entre dos valores consecutivos se le llama resolución y se calcula mediante la siguiente fórmula:

$$Res = V_{max} / 2^n$$

El máximo error que se produce al cuantificar será, por tanto, la mitad del intervalo, es decir, E = Res / 2. En este caso el error máximo de cuantificación es de 1 V. Este error de cuantificación nos da una idea de la precisión de la señal digitalizada.

Para conseguir una señal de mejor calidad se aumenta el número de bits. Por ejemplo, para el caso anterior, se aumenta el número de bits a 4, por tanto:

$$Res = 16 / 16 = 1\ V$$

En este caso, los intervalos de cuantificación podrían ser los siguientes: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16.

Y el error máximo de cuantificación es de 0'5 V.

Por último, utilizando el valor típico de 8 bits, se obtiene una resolución:

$$Res = 16 / 256 = 0'0625\ V = 62'5\ mV$$

Y los intervalos de cuantificación son los siguientes: 0'0625, 0'125, 0'1875, 0'25, 0'3125, 0'375...

Por último, el error máximo de cuantificación en el caso de utilizar 8 bits es 0'0625 / 2 = 0'03125 = 31'25 mV

Por tanto, el número de bits por muestra dependerá de la precisión que se quiera obtener en el proceso. Cuantos más bits, más precisión. Este parámetro depende del conversor utilizado (ADC).

A partir de la frecuencia de muestreo y el número de bits por muestra se puede obtener fácilmente la tasa de bits de la señal a transmitir:

Tasa de bits = (Frecuencia de muestreo) x (Número de bits por muestra)

2.7 MODULACIÓN

La modulación es el proceso por el cual se realizan cambios en algún parámetro de una señal, llamada señal portadora, en función de la información de otra señal, llamada señal moduladora. El resultado del proceso es la llamada señal modulada. La finalidad de este proceso es el de adecuar la señal moduladora a las características del medio de transmisión.

Considerando que la señal portadora va a ser una señal analógica, podremos tener dos tipos de modulación en función de que la señal moduladora sea digital o analógica. Sin embargo, en los sistemas telemáticos, la modulación utilizada normalmente es la modulación de una señal digital, llamada **modulación digital a analógica**. Por tanto, será este tipo el que se estudiará. El resto de modulaciones quedan fuera del ámbito de este libro.

Uno de los principales usos de esta técnica es transmitir datos digitales provenientes de un ordenador a través de una línea telefónica, utilizada para transmitir señales analógicas.

Para la modulación digital a analógica se va a utilizar una señal sinusoidal como señal portadora en la cual se varía algún parámetro. Los parámetros fundamentales de una señal sinusoidal son la amplitud, frecuencia y fase. Por tanto, variando cualquiera de estos parámetros podemos llevar a cabo la modulación.

Tasa de bits y tasa de baudios

En la modulación de señales digitales, existen dos parámetros que se definen en la señal modulada:

- **Tasa de baudios.** Viene dada por el número de unidades de señal por segundo. Las unidades de señal contienen los bits que se transmiten. La tasa de baudios determina el ancho de banda de la señal a transmitir. Este parámetro se mide en baudios y también se conoce como **velocidad de modulación**.
- **Tasa de bits.** Es la velocidad de transmisión y se calcula como la tasa de baudios por el número de bits representados para cada unidad de señal. La tasa de bits es siempre mayor o igual a la tasa de baudios.

NOTA 2.7

En los próximos apartados se estudiarán los principales tipos de modulaciones de señales digitales utilizando una portadora analógica.

2.7.1 ASK. MODULACIÓN POR DESPLAZAMIENTO DE AMPLITUD

En la modulación ASK, el parámetro que se altera de la señal portadora es la amplitud. Como la información de la señal moduladora es digital, sólo es necesario definir dos amplitudes que se corresponderán al 0 y 1 binario. En la siguiente figura se representa un ejemplo de señal ASK que contiene la información digital 01010:

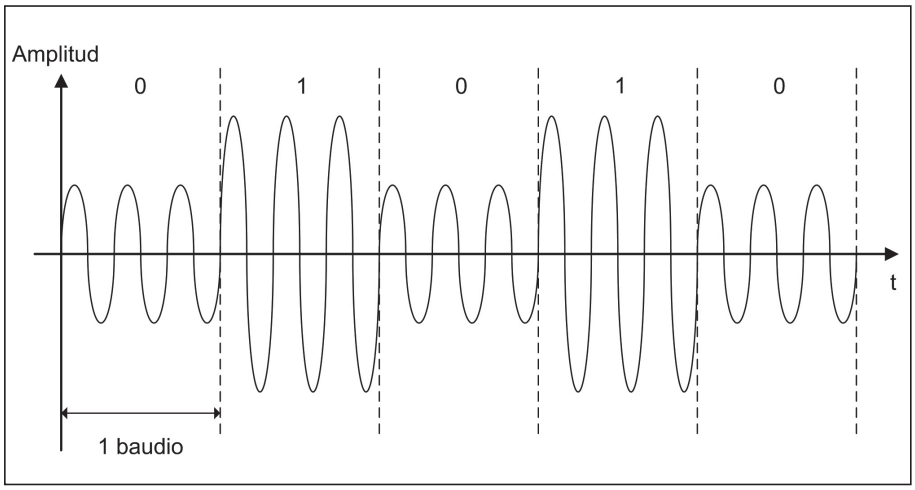


Figura 2.39. *Señal ASK.*

Como se observa, en la unidad de señal (baudio) se transmite un bit, por lo tanto una señal modulada en ASK tiene la misma velocidad de transmisión que de modulación. Si en la figura anterior el tiempo representado fuese de 1 segundo, la velocidad de modulación sería de 5 baudios y la velocidad de transmisión de 5 bps.

El problema de la modulación ASK es que es altamente susceptible al ruido ya que, habitualmente, el ruido afecta a la amplitud de la señal, que es donde está incluida la información digital en ASK.

Otro parámetro importante en una señal ASK es el ancho de banda, que se calcula de forma genérica con la siguiente expresión:

$$BW = (1 + d) * N_{baudios}$$

El factor d es un parámetro que depende de la línea de transmisión, y cuyo valor mínimo es 0. Por tanto el ancho de banda mínimo de una señal digital modulada ASK es igual a la tasa de baudios.

El espectro de una señal modulada en ASK estará centrado en la frecuencia de la señal portadora.

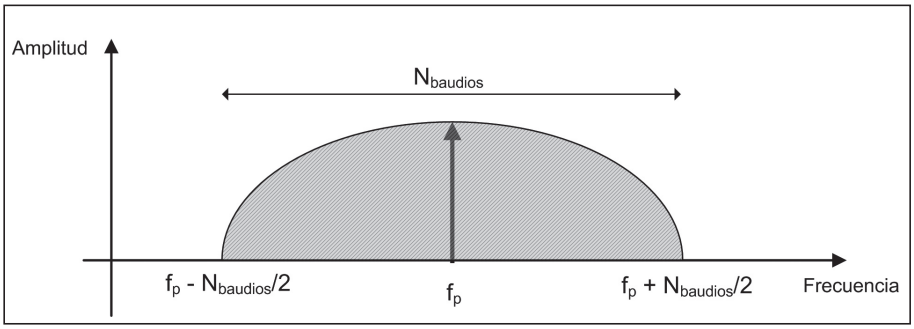


Figura 2.40. *Ancho de banda de una señal ASK .*

2.7.2 FSK. MODULACIÓN POR DESPLAZAMIENTO DE FRECUENCIA

En la modulación FSK, el parámetro que varía en la señal portadora en función de la información digital es la frecuencia. Como en el caso anterior, como hay que representar sólo dos posibles valores, 0 y 1, se asigna a cada uno una frecuencia diferente. La amplitud de la señal se mantiene constante. En la siguiente figura se representa una señal FSK:

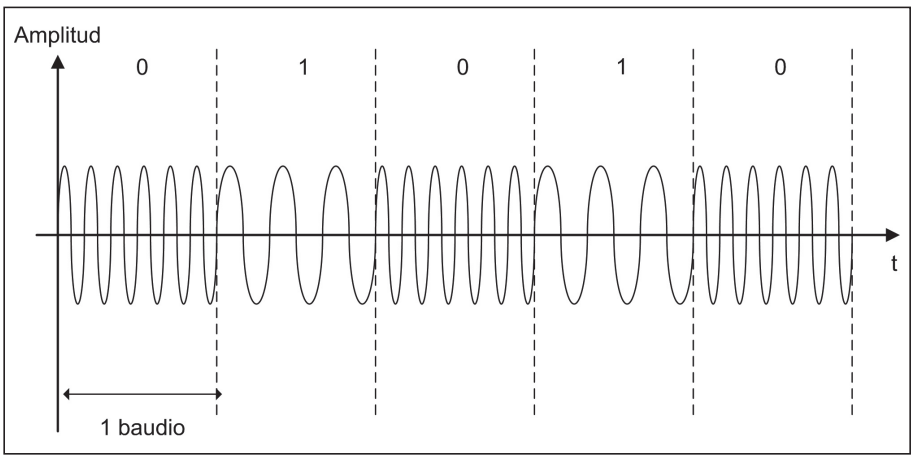


Figura 2.41. *Señal FSK.*

En este caso, el ruido afecta muy poco a las señales FSK ya que no se tienen en cuenta las variaciones de amplitud de la señal ya que la información digital está representada por cambios de frecuencia.

El ancho de banda de una señal FSK es igual a la tasa de baudios de la señal más la diferencia entre las dos frecuencias utilizadas en la modulación.

$$BW = (f_2 - f_1) + N_{baudios}$$

donde f_2 es la frecuencia superior y f_1 es la frecuencia inferior. Por ejemplo, en una señal FSK con una tasa de bits de 5 Kbps y que utiliza las frecuencias portadoras 7 KHz y 10 KHz, el ancho de banda será:

$$BW = (10000 - 7000) + 5000 = 8000 \text{ Hz} = 8 \text{ KHz}$$

Por tanto, el inconveniente de una señal FSK es que utiliza más ancho de banda que una señal ASK con la misma tasa de bits. Además, este ancho de banda depende de la diferencia de las dos frecuencias portadoras. Como se observa, interesa que sea una diferencia pequeña y esta condición en la práctica es difícil de conseguir. En la siguiente figura se puede observar de forma gráfica el ancho de banda de una señal FSK:

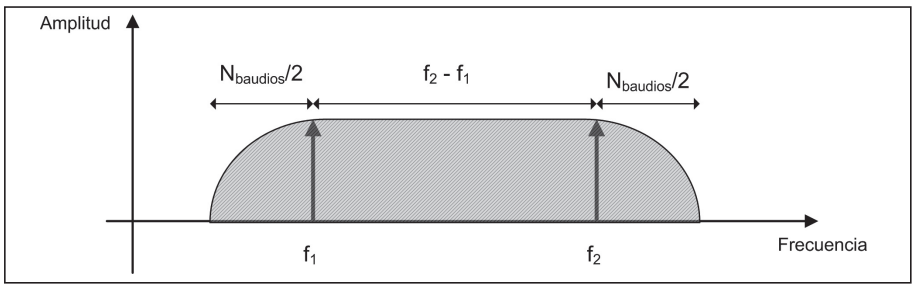


Figura 2.42. *Ancho de banda de una señal FSK.*

2.7.3 PSK. MODULACIÓN POR DESPLAZAMIENTO DE FASE

En la modulación PSK el parámetro que varía en la señal portadora es la fase. En este caso, tanto la amplitud como la frecuencia se mantienen constantes. Para representar los valores 0 y 1 binarios se utilizan dos fases diferentes, por ejemplo 0º y 180º. En la siguiente figura se puede observar una señal PSK.

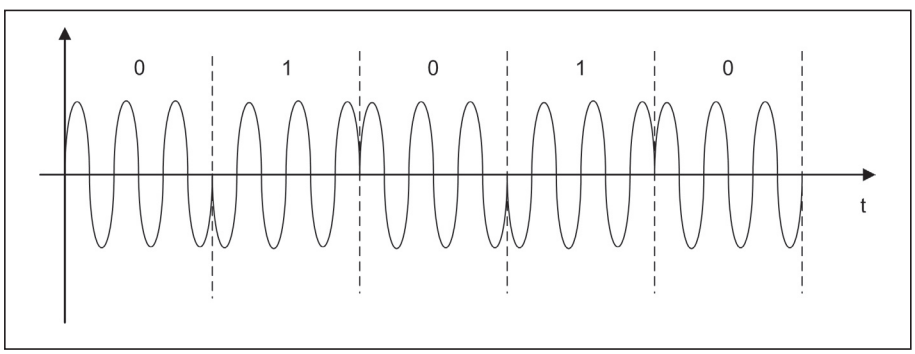


Figura 2.43. *Señal PSK.*

La señal ASK representada en la figura también se conoce como **2-PSK** o **BPSK (Binary PSK)** debido a que se usan dos fases. Al igual que en las modulaciones

anteriores, como cada unidad de señal (baudio) representa un solo bit, la tasa de bits es igual a la tasa de baudios.

En este tipo de modulación de fase permite llevar a cabo pequeñas alteraciones de la fase siendo perfectamente detectables en el receptor. Esto significa que se pueden utilizar más de dos fases con relativa facilidad. De esta forma se obtiene la técnica de modulación llamada **4-PSK**. En este caso se utilizan cuatro fases distintas para representar la información digital. Se pueden utilizar valores de fases arbitrarios siempre que la diferencia de fase entre cada fase utilizada sea de 90º. Al poder utilizar cuatro valores de fase distintos, a cada fase se le pueden asignar dos bits. En la siguiente tabla se muestra una posible asignación:

Fase	**Bits**
0º	00
90º	01
180º	10
270º	11

En la siguiente figura se muestra un ejemplo de señal 4-PSK.

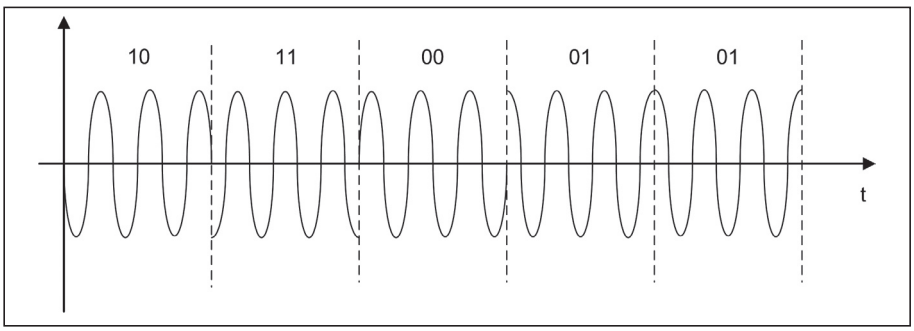


Figura 2.44. *Señal 4-PSK.*

Como se observa en la figura, en este caso cada unidad de señal contiene 2 bits, por lo tanto la tasa de bits es el doble de la tasa de baudios.

Hay un tipo de modulación 4-PSK muy utilizado conocido como **QPSK**. En este caso se utilizan las fases 45º, 135º, 225º y 315º.

De igual forma, existe una modulación PSK que utiliza ocho fases diferentes y que se conoce como 8-PSK. En este caso, las fases utilizadas deben estar separadas entre sí 45º. La utilización de ocho fases diferentes nos permite asignar a cada fase un valor de 3 bits. Y por tanto, la tasa de bits se obtiene multiplicando por tres la tasa de baudios ya que cada baudio (unidad de señal) representa 3 bits.

El ancho de banda mínimo para las señales PSK es el mismo que para las señales ASK, es decir:

$$BW = N_{baudios}$$

2.7.4 QAM. MODULACIÓN DE AMPLITUD EN CUADRATURA

La modulación PSK con más de ocho fases diferentes, a velocidades de modulación elevadas, resulta difícil de demodular. Para mejorar las prestaciones se acude a otros esquemas de modulación.

Una posibilidad es usar conjuntamente modulación en amplitud y fase dando lugar a la modulación QAM o modulación en cuadratura.

Se pueden obtener numerosas combinaciones entre fases y amplitudes. Para representar de forma sencilla la combinación de fases y amplitudes utilizadas en un determinado tipo de modulación QAM, se suele utilizar un gráfico conocido como **constelación**. En él, una determinada combinación de fase y amplitud se representa como un vector donde la longitud del mismo representa la amplitud, y el ángulo de inclinación respecto a los ejes de coordenadas representa la fase. A continuación se muestran algunos ejemplos de constelaciones para modulaciones QAM de 4, 8 y 16 combinaciones de amplitud-fase, conocidas como 4-QAM, 8-QAM y 16-QAM.

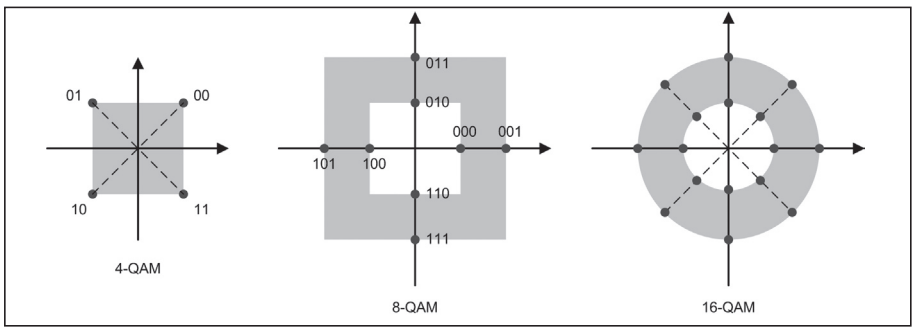


Figura 2.45. *Constelaciones QAM.*

En la siguiente figura se muestra una señal 8-QAM, es decir, que utiliza ocho combinaciones amplitud-fase y que, por tanto, cada posible combinación (unidad de señal) representa 4 bits.

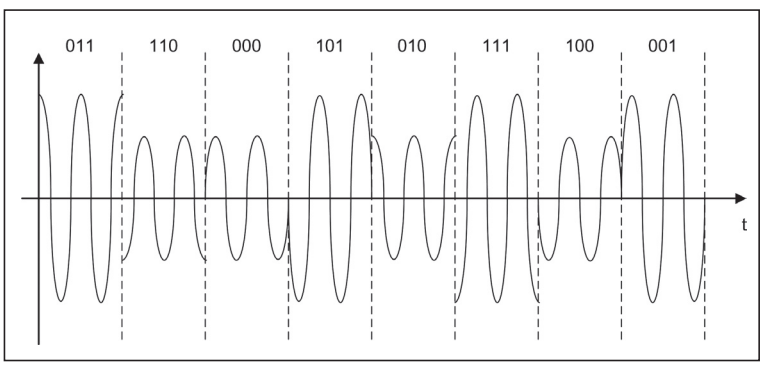


Figura 2.46. *Señal 8-QAM.*

La inmunidad frente a los errores de un determinado esquema de modulación está condicionada por la proximidad entre puntos adyacentes de la constelación. Por ello, en la constelación 16-QAM de la figura 2.45 se usan ocho fases distintas, pero los niveles de amplitud asociados a fases adyacentes son distintos. De esta manera se aumenta la separación entre puntos, restringiendo el número de combinaciones posibles entre amplitudes y fases. Observe que serían posible cuatro niveles de amplitud distintos y ocho fases en cada nivel totalizando 32 símbolos frente a los 16 utilizados.

El aumento de las combinaciones de amplitud-fase utilizadas hace que aumente también la tasa de bits para la misma velocidad de modulación. Así por ejemplo, una señal 16-QAM tendrá una tasa de bits igual a la tasa de baudios multiplicada por 4, ya que cada grupo de 4 bits puede representar 16 posibles variaciones de amplitud-fase (2^4).

El ancho de banda mínimo para una señal QAM es igual al de ASK o PSK, es decir:

$$BW = N_{baudios}$$

El desarrollo tecnológico ha llevado al desarrollo de circuitos electrónicos cada vez más precisos que han permitido aumentar las combinaciones de amplitud-fase en la modulación QAM. Así, se han conseguido modulaciones 32-QAM, 64-QAM, 128-QAM y 256-QAM. La siguiente tabla resume las características de las modulaciones estudiadas:

Tabla 2.1

Modulación	Bits/baudio	Tasa de bits
ASK, FSK, 2-PSK	1	$N_{baudios}$
4-PSK, 4-QAM	2	$2 * N_{baudios}$
8-PSK, 8-QAM	3	$3 * N_{baudios}$
16-QAM	4	$4 * N_{baudios}$
32-QAM	5	$5 * N_{baudios}$
64-QAM	6	$6 * N_{baudios}$
128-QAM	7	$7 * N_{baudios}$
256-QAM	8	$8 * N_{baudios}$

2.8 CONMUTACIÓN

La conmutación es el proceso por el cual se establece una comunicación entre un emisor y un receptor a través de una infraestructura de comunicaciones común formada por una red de nodos de conmutación llamados conmutadores. Estos conmutadores son dispositivos capaces de crear conexiones temporales entre dos o más dispositivos conectados al mismo.

La conmutación es una técnica utilizada ampliamente en los sistemas de transmisión de datos para optimizar los recursos dedicados a la transmisión. De hecho, actualmente todos los sistemas de transmisión aplican, de una u otra forma, las técnicas de conmutación.

2.8.1 CONMUTACIÓN DE CIRCUITOS

En la conmutación de circuitos se establece una conexión física que se mantiene activa mientras se produce la comunicación. Por tanto, la conmutación de circuitos se lleva a cabo en tres fases:

1. Establecimiento de la conexión, es donde se crea la conexión física entre los dos dispositivos.
2. Envío de información.
3. Finalización de la conexión, se liberan los recursos utilizados en la comunicación y la conexión física deja de ser válida.

Un conmutador de circuitos es un dispositivos de *n* entradas y *m* salidas que crea una conexión temporal entre un enlace de entrada y un enlace de salida.

Existen dos técnicas de conmutación de circuitos:

- ✓ Por división en el espacio: a cada comunicación se le asocia un camino físico e independiente de los demás.
- ✓ Por división en el tiempo: cada comunicación está asociada a la ocupación en el tiempo de un circuito físico, es decir, que los circuitos físicos están compartidos en el tiempo. Esto se consigue utilizando multiplexación en el dominio de tiempo (TDM), concepto que se estudiará en el próximo apartado.

La conmutación de circuitos se emplea en el sistema telefónico, es decir, en transmisión de voz.

2.8.2 CONMUTACIÓN DE PAQUETES

Es el tipo de conmutación utilizado para la transmisión de datos. La información se divide en unidades más pequeñas y de longitud más o menos fija, de forma que la conmutación se puede realizar de manera rápida y eficiente. Además de los datos, en cada paquete se envía información de control que es la que el conmutador utiliza para reencaminar los paquetes. Hay dos tipos de conmutación de paquetes:

- **Datagramas:** cada paquete es tratado de forma independiente de los otros. En este caso, los paquetes se denominan datagramas.
- **Circuitos virtuales:** al comienzo de la sesión se elige una ruta por la que luego se transmiten todos los paquetes de una comunicación. Existen dos tipos de circuitos virtuales: conmutados (muy parecidos conceptualmente a la conmutación de circuitos) y permanentes, en los cuales la ruta entre los dispositivos que realizan la conexión es fija.

La conmutación de paquetes se utiliza para datos en lugar de la conmutación de circuitos porque la transmisión de datos tiende a hacerse a ráfagas para lo cual es más eficiente la conmutación de paquetes.

2.8.3 CONMUTACIÓN DE MENSAJES

En este tipo de conmutación, la información se envía en bloques (mensajes) con un origen y un destino. El mensaje se envía del emisor al primer nodo de la red donde se almacena y se espera a que la ruta correspondiente esté libre, entonces se reenvía. Este proceso se repite hasta alcanzar el destino.

Esta técnica requiere que se establezcan buffers en cada nodo de conmutación para almacenar los mensajes hasta su retransmisión, lo que puede ocasionar retardos en la transmisión. No es apropiado para la transmisión de voz, sólo se utiliza para datos.

Su aplicación más extendida fue para el servicio de telegrafía Télex para transmisiones telegráficas. Actualmente está en desuso.

2.9 MULTIPLEXACIÓN

La multiplexación es el conjunto de técnicas que permiten transmitir de forma simultánea varias señales a través de un mismo enlace. Se utiliza cuando la capacidad del medio de transmisión es mayor a las necesidades de un canal de comunicación individual entre el transmisor y el receptor.

Por ejemplo, para llevar a cabo una transmisión analógica full-dúplex utilizando como medio de transmisión el cable de cobre, serían necesarios dos cables, uno para cada sentido de la transmisión ya que, en una comunicación full-dúplex, existen siempre dos canales de comunicación. Utilizando las técnicas de multiplexación se pueden transmitir los dos canales a través del mismo cable, siempre y cuando el ancho de banda del medio (el cable de cobre) sea igual o superior a la suma de los anchos de banda de cada canal.

Actualmente, la multiplexación es una técnica fundamental en las telecomunicaciones, incluida la telemática. Debido al enorme volumen de información que se intercambia, es necesario aprovechar al máximo las altas capacidades de los medios de transmisión actuales como el cable coaxial y la fibra óptica a través de los cuales, y gracias a la multiplexación, pueden viajar simultáneamente cientos e incluso miles de canales de datos.

2.9.1 FDM. MULTIPLEXACIÓN POR DIVISIÓN DE FRECUENCIA

La multiplexación por división de frecuencia o **FDM (Frequency Division Multiplexing)** es una técnica empleada cuando se quieren transmitir varias señales

analógicas a través de un medio de transmisión con un ancho de banda mayor al de las señales a transmitir.

La multiplexación de las señales se lleva a cabo modulando cada una de las señales con una frecuencia portadora distinta. La distancia en frecuencia entre las portadoras debe ser tal que no se produzca solapamiento entre las diferentes señales.

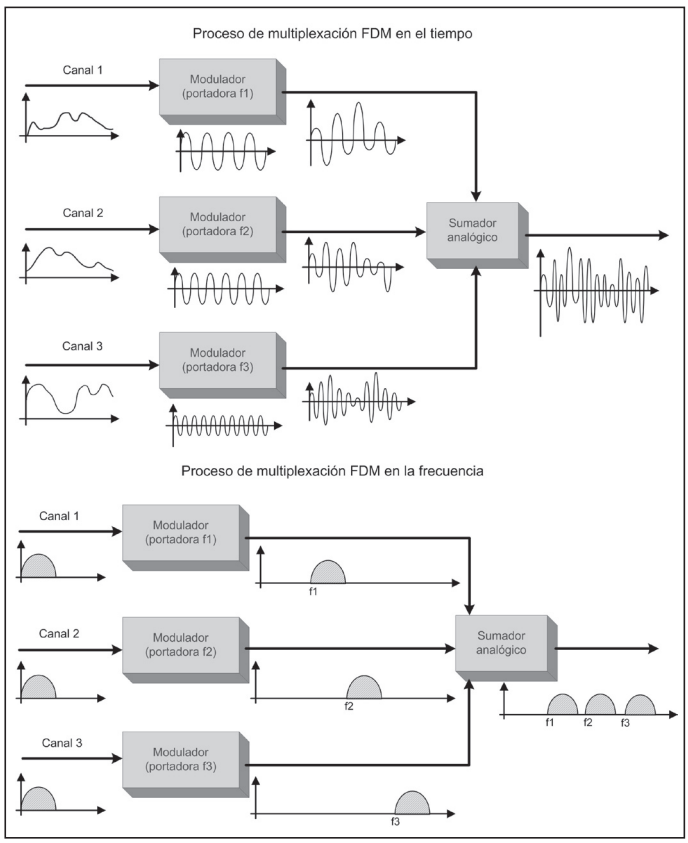


Figura 2.47. *Multiplexación FDM.*

Además, se deben elegir frecuencias portadoras que no existan en las señales que se van a multiplexar. Por ejemplo, si se desea multiplexar una señal que ocupa una banda entre 0 y 100 KHz, no se podrá utilizar una portadora dentro de esa banda de frecuencias.

FDM se aplica para multiplexar señales analógicas por lo que se deberá utilizar cualquier técnica de modulación de señales analógicas, por ejemplo, AM o FM. El problema es que tanto en AM como en FM la señal modulada tiene un ancho de banda mayor que la original. Para conseguir un mejor aprovechamiento del ancho

de banda del medio, se pueden utilizar otras técnicas como **BLU (Banda Lateral Única)** donde el ancho de banda de la señal modulada es el mismo que el de la señal original.

El proceso de demultiplexación, es decir, de extracción de cada una de las señales multiplexadas se basa en la utilización de filtros paso banda en el receptor. Es necesario un filtro por cada señal a demultiplexar. Después del filtrado ya se puede aplicar la demodulación que devolverá cada señal a sus frecuencias originales.

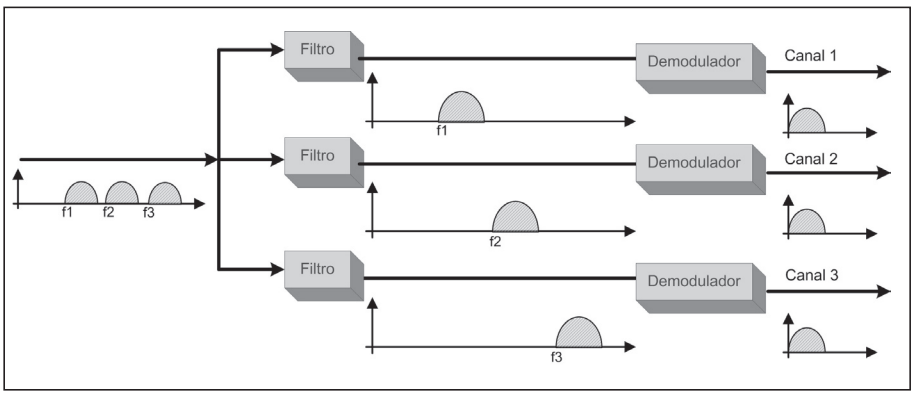


Figura 2.48. *Demultiplexación FDM.*

2.9.2 TDM SÍNCRONA. MULTIPLEXACIÓN POR DIVISIÓN EN EL TIEMPO SÍNCRONA

La multiplexación por división en el tiempo o **TDM (Time Division Multiplexing)** es un proceso que se utiliza para transmitir señales digitales cuando la tasa de bits permitida por el medio de transmisión es mayor a la tasa de bits de los datos a multiplexar.

En este caso, la multiplexación consiste en enviar varias señales digitales por un único enlace dividiendo el tiempo de transmisión entre las señales a multiplexar. El multiplexor TDM consta de varios canales digitales de entrada. La señal digital que llega por cada canal se envía a un canal único de salida durante cierto tiempo, transcurrido este tiempo el multiplexor comunica el siguiente canal de entrada con la salida. Este proceso se repite hasta llegar al último canal después del cual se pasa de nuevo al primer canal. El proceso sería algo así como una puerta giratoria con varias entradas y una única salida.

Existen dos tipos de TDM: síncrona y asíncrona.

El término síncrono no tiene el mismo significado que el que se vio en la transmisión serie de datos. En este caso, síncrono se refiere a que en la multiplexación, a cada canal que se desea transmitir se le asigna exactamente la misma porción de tiempo, independientemente de si en el canal hay datos para transmitir. Digamos

que se asignan turnos de transmisión fijos e iguales a cada canal. Si tenemos cuatro canales, a cada canal se le asigna un turno de transmisión. Si a un canal le toca transmitir y no tiene nada, durante ese turno no se transmitirán datos.

Cada porción de tiempo que un dispositivo transmite datos de forma continua se denomina **time slot** (o ranura de tiempo). Durante ese time slot se transmite siempre el mismo número de bits.

Una **trama** estará formada por un turno completo de porciones de tiempo o time slot. Es decir, si tenemos cuatro canales, una trama estará formada por los cuatro turnos cada uno de ellos con la duración de un time slot.

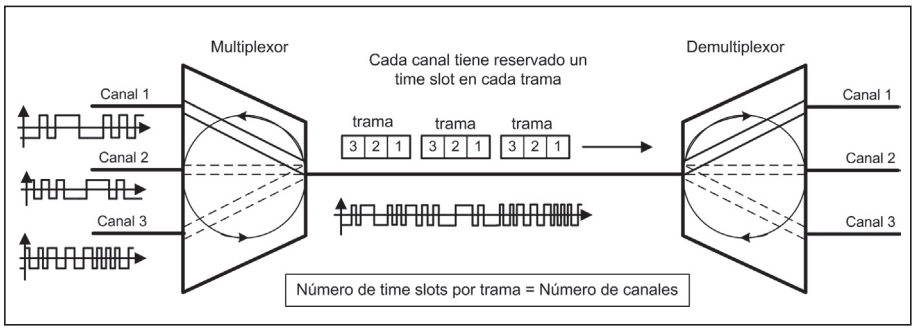


Figura 2.49. *Multiplexación TDM síncrona.*

La velocidad de transmisión de la señal multiplexada será igual a la velocidad de cada canal por el número de canales en el caso de que la tasa de bits de cada canal sea la misma.

Si todos los canales tienen la misma velocidad de transmisión, a cada canal se le asigna un time slot. Si existen dispositivos a mayor velocidad se le asigna más de un time slot con la condición de que las tasas de datos deben ser múltiplo entero unas de otras.

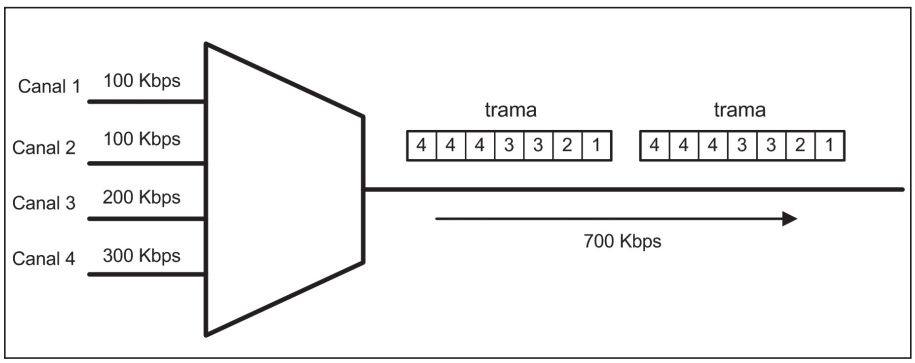


Figura 2.50. *Multiplexación TDM con canales a distintas velocidades.*

En algunas transmisiones TDM síncronas se pueden utilizar bits adicionales por trama para proporcionar un nivel más de sincronismo. Estos bits se denominan **bits de tramado**.

Como cada canal tiene asignado un time slot fijo dentro de la trama, en principio no es necesario enviar bits de control para identificación de los canales.

Para transmitir con tasas de datos que no sean múltiplos enteros, el multiplexor añade bits extra al canal del que se desea ajustar su tasa de bits.

El principal inconveniente de la TDM síncrona es la pérdida de eficiencia de la transmisión cuando haya canales que no transmiten datos. Como cada canal tiene asignado un time slot en cada trama, si un canal no transmite datos en un momento dado, su time slot quedará vacío. Por tanto, la TDM síncrona se utiliza para multiplexar canales con un flujo continuo de información.

2.9.3 TDM ASÍNCRONA O ESTADÍSTICA

Para solucionar el problema del no aprovechamiento de la capacidad del enlace en la TDM síncrona cuando algún canal no transmite datos se utiliza la técnica denominada TDM asíncrona (o estadística).

El proceso de multiplexación se lleva a cabo de la misma forma que en TDM síncrona. La diferencia es que los canales no tienen asignado un time slot fijo en cada trama. Al igual que en TDM síncrono, se establece un turno por cada canal, pero en este caso, si un canal no tiene datos para transmitir, se pasa el turno al siguiente canal de forma que todos los time slot que forman la trama contengan datos aunque no necesariamente de canales consecutivos.

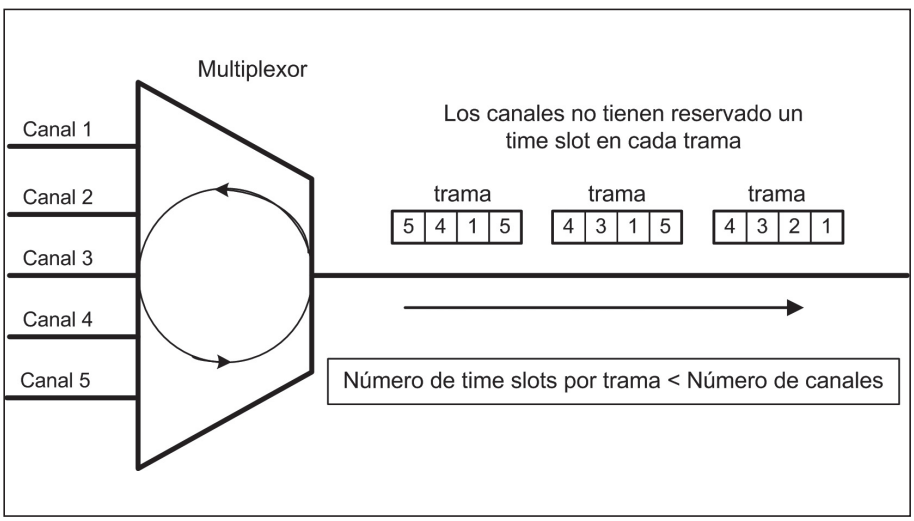


Figura 2.51. *Multiplexación TDM asíncrona.*

Debido a esto, el número de time slots de una trama no tiene que coincidir con el número de canales como ocurría en TDM síncrono. De hecho el número de time slots de la trama interesa que sea igual al promedio del número de canales que transmiten datos. Es decir, si tenemos un sistema TDM con 10 canales y se calcula de forma estadística que hay siempre un promedio de seis canales transmitiendo datos simultáneamente, se elegirá este número como número de time slots por trama y no 10. De esta forma se aprovecha de forma mucho más eficiente la capacidad del enlace ya que apenas habrá time slots vacíos.

La velocidad de transmisión de la señal multiplexada será la tasa de bits de cada canal por el número de time slots. En el ejemplo anterior, la señal multiplexada es equivalente a una multiplexación de seis canales. Será necesario implementar un buffer de memoria ya que cuando haya transmisión simultánea en más de seis canales llegarán datos más rápidamente de lo que se pueden transmitir.

Debido a que los datos de cada canal no ocupan posiciones fijas en la trama es necesario incluir una identificación del canal para cada time slot. Esta situación implica un aumento de datos de control en el enlace lo cual limita la eficacia de TDM asíncrona. Para minimizar el impacto que supone llevar a cabo este direccionamiento es necesario utilizar un tamaño de time slot grande e intentar utilizar el menor número de bits para la identificación del canal.

2.9.4 WDM. MULTIPLEXACIÓN POR DIVISIÓN DE LONGITUD DE ONDA

La multiplexación por división de longitud de onda o **WDM (Wavelength Division Multiplexing)** es una técnica de multiplexación similar a FDM pero utilizando señales ópticas en lugar de señales electromagnéticas. Por tanto, WDM se utiliza para la transmisión de varias señales utilizando fibra óptica como medio de transmisión. En este caso, cada canal que se desea multiplexar se transmite utilizando una longitud de onda diferente.

Para su implementación es necesario utilizar emisores láser que emitan luz a diferentes longitudes de onda. Todas las señales ópticas generadas se combinan y transmiten por un único canal. En el receptor es necesario utilizar filtros ópticos y fotodetectores ajustados a las longitudes de onda adecuadas.

Se conoce como **DWDM (Dense Wavelength Division Multiplexing)** la evolución de WDM en la que se ha conseguido acercar las longitudes de onda portadoras, de forma que el canal de fibra tiene más capacidad. Además, en DWDM existen otras mejoras importantes, como la capacidad de amplificar todas las longitudes de onda sin necesidad de convertirlas a señales eléctricas. También permite transportar señales ópticas de diferentes velocidades y tipos de forma simultánea.

Tanto WDM como DWDM usan fibra óptica monomodo para transportar señales ópticas a diferentes longitudes de onda. No confundir este concepto con el modo de transmisión por fibra multimodo.

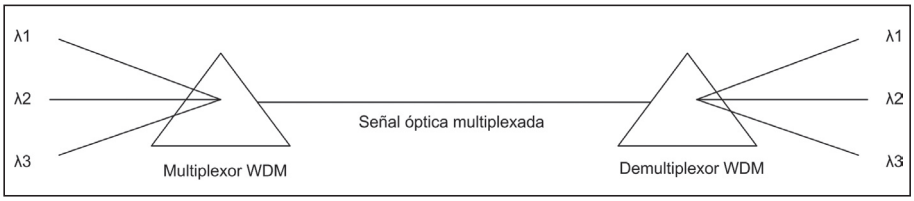


Figura 2.52. *Multiplexación WDM.*

Las técnicas WDM se comenzaron a utilizar para aprovechar el enorme ancho de banda de la fibra óptica. Actualmente, y gracias a esta técnica, se han conseguido velocidades de transmisión de 25 Tbps a través de una única fibra óptica.

2.10 ADSL

Con la aparición de los módem de 56K se llega al límite de velocidad aprovechando la banda de frecuencias de la telefonía tradicional.

Para conseguir un aumento de velocidad de la conexión de un abonado a las redes de datos utilizando el bucle local telefónico se desarrollan las tecnologías **DSL (Digital Subscriber Line)**, entre las cuales aparecen ADSL, HDSL, SDSL y VDSL, todas ellas basadas en el aprovechamiento de todo el ancho de banda del bucle local.

ADSL (Asymetric Digital Subscriber Line) es una tecnología desarrollada en el año 1989 para proporcionar acceso de alta velocidad a redes de datos usando el bucle de abonado de la red telefónica. ADSL es asimétrico ya que se utiliza más ancho de banda para la recepción que para la emisión.

En este capítulo se expondrá ADSL como una técnica de transmisión de datos, en el capítulo 6 se estudiarán los módems ADSL y en el capítulo 10 se verá ADSL como un servicio de datos proporcionado por los operadores de telecomunicaciones.

La tecnología ADSL de transmisión de datos a alta velocidad a través del bucle de abonado telefónico está basada en el aprovechamientote todo el ancho de banda del cable telefónico del bucle local, aproximadamente 1'1 MHz, dividiéndolo en tres bandas:

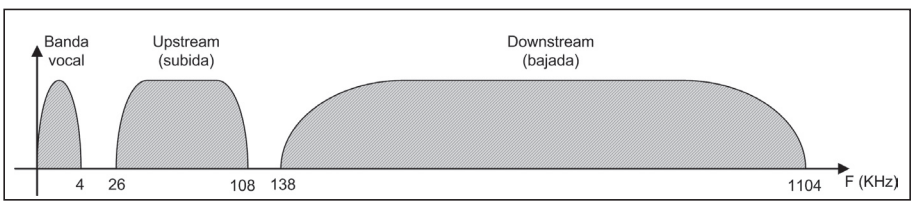


Figura 2.53. *Multiplexación en ADSL.*

Por tanto, como se observa, ADSL utiliza multiplexación FDM para transmitir tres señales a través de un solo canal de comunicación, el cable de par trenzado.

2.10.1 SISTEMA DE MODULACIÓN EN ADSL

Para enviar los canales de datos downstream y uptream en ADSL se utiliza un tipo de modulación conocida como **DMT (Discrete MultiTone, Técnica Multitono Discreta)**. Esta técnica de modulación consiste en dividir la señal digital en canales, cada uno de los cuales se modula con una frecuencia subportadora distinta utilizando modulación QAM.

En el inicio, el módem envía señales de test para determinar la relación señal-ruido (S/R) de cada canal. El reparto del flujo de datos entre subportadoras se hace en función de la estimación de esta relación S/R en la banda asignada a cada una de ellas. Cuanto mayor es la relación S/R, mayor es el caudal que se puede transmitir por la subportadora y mayor es el número de bits asignados al canal. El principal factor que influye en esta relación S/R es la distancia entre el abonado y la central telefónica local. Cuanto mayor sea esta distancia peor es la relación S/R de los canales de forma que para distancias superiores a 5 Km puede ser inviable el uso de esta técnica.

Por tanto, la tasa de bits de cada canal es variable. La tasa máxima ante una buena relación S/R es de 60 Kbps, es decir, una modulación QAM de 15 bits/baudio. La señal modulada resultante de cada canal tiene un ancho de banda de 4 KHz, con una separación entre subportadoras de 4,3125 KHz.

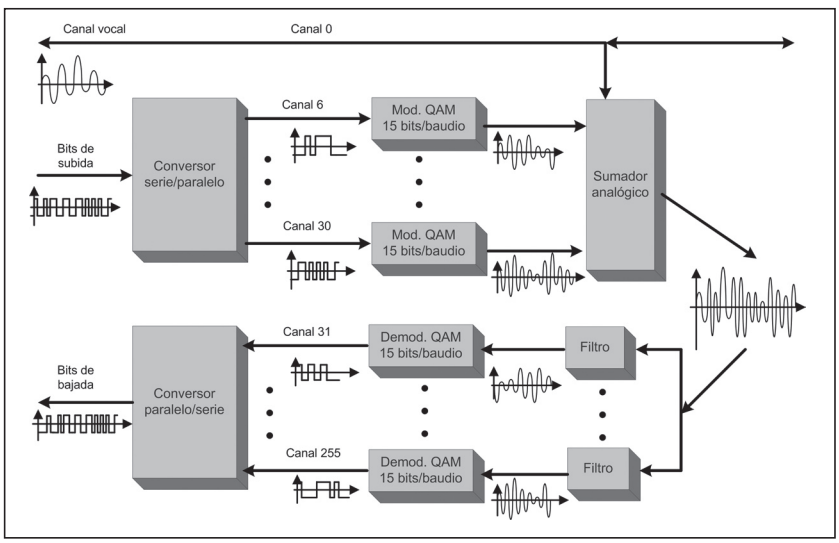


Figura 2.54. *Funcionamiento de la modulación en ADSL.*

Como se observa en el gráfico, se utilizan 25 canales de subida (modulados en el módem/router del usuario) y 224 canales de bajada (modulados en el DSLAM).

Por lo tanto, la tasa máxima teórica de subida de datos (upstream) es de:

25 canales QAM * 60 Kbps = 1'5 Mbps

aunque, debido a las condiciones reales de la línea, el máximo real está por debajo de 1 Mbps.

Para el canal downstream, la tasa máxima teórica de bajada sería de:

200 canales QAM * 60 Kbps = 13'44 Mbps

En la práctica y por las condiciones reales, esta tasa está limitada aproximadamente a unos 8 Mbps a una distancia a la central de 1'5 Km.

NOTA 2.8

DSLAM es una agrupación de módems ubicados en la central local.

2.10.2 ADSL2 Y ADSL2+

ADSL2 y ADSL2+ introduce mejoras importantes con respecto a ADSL:

- ✓ Mayor velocidad en sentido bajada.
- ✓ Menor consumo de energía.
- ✓ Establecimiento rápido de la conexión.
- ✓ Mejor interoperatividad entre chips de diferentes fabricantes.
- ✓ Posibilidad de transportar servicios basados en paquetes (como Ethernet).

Otra de las características es la posibilidad de no utilizar la banda de frecuencia reservada para la transmisión de voz analógica. De esta forma, esta banda se añade a la banda reservada al canal de subida consiguiendo un aumento de 256 Kbps. Esta opción es interesante si la línea donde se utiliza la tecnología ADSL no se va a utilizar para llamadas telefónicas convencionales, sólo para datos.

La ventaja que más salta a la vista es la posibilidad de utilizar la **multiplexación inversa (IMA, Inverse Multiplexing over ATM).** Gracias a esta opción es posible **juntar pares de cobre.** Con ADSL2+ podríamos por ejemplo disponer de 4*24 = 96 Mbps de bajada y 4 * 1 = 4 Mbps de subida a menos de 1.000 metros de la central.

Con ADSL2 se pueden alcanzar tasas de 12 Mbps hasta 1.500 metros de bucle local.

Con ADSL2+ para bucles locales de menos de 2.500 m se dobla el ancho de banda del cable a 2'2 MHz.

2.10.3 OTRAS TECNOLOGÍAS xDSL

Aunque ADSL es la tecnología xDSL más implantada en la actualidad, existen otras tecnologías que utilizan el bucle local de abonado y que están más o menos desarrolladas. Se exponen a continuación algunas de ellas:

SDSL (Symmetric Digital Subscriber Line)

Fue desarrollado para sustituir las líneas T1/E1 por lo tanto proporciona velocidades simétricas de hasta 1'544 Kbps (T1) o 2'048 Kbps (E1).

Utiliza codificación conocida como 2B1Q y se puede utilizar en bucles de abonado con unas distancias máximas de hasta 3 Km.

No existe un estándar oficial de esta tecnología.

HDSL (High bit rate Digital Subscriber Line)

Estándar publicado por la ITU-T en 1998 como G.991.1. Ofrece características similares a SDSL.

Existe una versión mejorada de HDSL conocida como HDSL2 que utiliza otra técnica de codificación conocida como TC-PAM (modulación por amplitud de pulso codificados trellis) y se puede utilizar con bucles de abonado de hasta 4 Km.

SHDSL (Symmetric High-Speed Digital Subscriber Line)

Es el resultado de la estandarización de las tecnologías SDSL, HDSL y HDSL2. Por lo tanto, esta tecnología está definida en el estándar de la ITU-T G.991.2 publicado en el año 2001. Como su nombre indica es una tecnología simétrica de transmisión de datos, es decir, los canales downstream (bajada) y upstream (subida) tienen la misma capacidad.

Utiliza, al igual que HDSL2, la técnica de codificación TC-PAM con alcances teóricos de 6 Km.

Las velocidades de conexión que proporciona son:

192 Kbps – 2'048 Mbps para un solo par

384 Kbps – 4'6 Mbps para dos pares

Utiliza la banda telefónica vocal, por lo tanto, no es posible utilizar el servicio telefónico analógico en este tipo de líneas.

VDSL (Very High Data Rate Digital Subscriber Line)

Evolución de HDSL publicada por la ITU-T como G.993.1. En VDSL se alcanzan velocidades teóricas de 52 Mbps de bajada y 12 Mbps de subida. Se utiliza como técnica de modulación DMT.

En España se prevé que Telefónica comience a ofrecer servicios VDSL a partir de 2007.

VDSL2 es el estándar DSL más reciente, publicado por la ITU-T como G.993.2. Proporciona velocidades muy altas pero con distancias muy cortas a la central. A partir de 1'6 Km la velocidad de VDSL2 se iguala a la de ADSL2+.

RESUMEN DEL CAPÍTULO

En este capítulo se ha hecho un extenso repaso a muchos de los conceptos que deben conocerse sobre la transmisión de datos dentro de los sistemas telemáticos. Estos conceptos se podrían agrupar en tres bloques:

- ✓ Señales
- ✓ Medios de transmisión
- ✓ Técnicas de transmisión

En el apartado de señales se ha hecho un repaso a los principales conceptos sobre señales utilizadas en los sistemas de transmisión de datos. Mientras que en el apartado de medios de transmisión se han visto las principales características de los medios de transmisión más comunes.

El resto del capítulo se ha dedicado a repasar las principales técnicas de transmisión de datos como son la codificación, modulación, conmutación y multiplexación.

El capítulo se complementa con una visión general del proceso de digitalización, muy relacionado con la transmisión de datos. Y para acabar se profundiza en una de las tecnologías más en auge actualmente y que incluye algunos de los conceptos vistos en este capítulo: el ADSL.

EJERCICIOS PROPUESTOS

1. Realizar los siguientes cambios de unidades:
- **a)** 56.500 Hz en KHz.
- **b)** 2.248 KHz en MHz.
- **c)** 36 GHz en KHz.
- **d)** 4.876.246 Hz en MHz.
- **e)** 0,0045 segundos en milisegundos.
- **f)** 0,0619 milisegundos en microsegundos.
- **g)** 0,000000728 segundos en picosegundos.
- **h)** 0,0000854 segundos en nanosegundos.

2. Dibujar la gráfica en el dominio del tiempo (para un milisegundo) de una señal sinusoidal con una amplitud máxima de 5 voltios, una frecuencia de 4 KHz y una fase de 270º.

3. Dibujar dos señales sinusoidales en la misma gráfica de dominio del tiempo (para un milisegundo) con las siguientes características:

- ✓ Señal A: amplitud 20 v, frecuencia 1 KHz, fase 0º.
- ✓ Señal B: amplitud 10 v, frecuencia 10 KHz, fase 90º.

Representar las señales anteriores en el dominio de la frecuencia.

4. Obtener la velocidad de transmisión (tasa de bits) para cada una de las siguientes señales:
- **a)** Una señal en la cual un bit dura 0,005 segundos.
- **b)** Una señal en la cual un bit dura 8 milisegundos.
- **c)** Una señal en la cual 5 bits dura 60 microsegundos.
- **d)** Una señal en la cual 2.000 bits dura 100 picosegundos.

5. ¿Cuál es la duración de un bit para cada una de las señales siguientes?
- **a)** Una señal con una velocidad de transmisión de 500 bps.
- **b)** Una señal con una velocidad de transmisión de 200 Kbps.
- **c)** Una señal con una velocidad de transmisión de 2 Mbps.
- **d)** Una señal con una velocidad de transmisión de 4 Gbps.

6. Codificar la secuencia de bits 0111110100000011 en las siguientes codificaciones:
- **a)** NRZ-L.
- **b)** NRZ-I.
- **c)** Manchester.
- **d)** Manchester diferencial.
- **e)** HDB3.
- **f)** B8ZS.

7. Obtener el flujo de datos a partir de las siguientes codificaciones:
- **a)** Codificación HDB3.

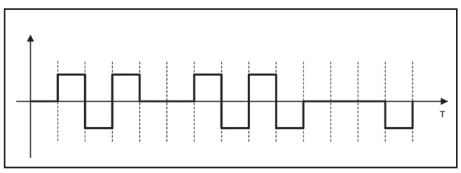


Figura 2.55. *Codificación HDB3 del ejercicio 7.*

- **b)** Codificación B8ZS.

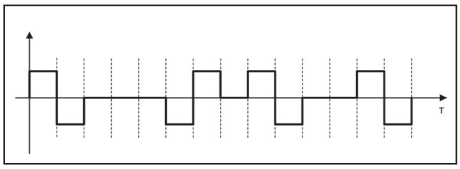


Figura 2.56. *Codificación B8ZS del ejercicio 7.*

■ **8.** Calcular la tasa de baudios para las siguientes tasas de bits y tipos de modulación:
- **a)** 4 Kbps, FSK.
- **b)** 3 Kbps, ASK.
- **c)** 5 Kbps, 2-PSK.
- **d)** 6 Kbps, 4-PSK.
- **e)** 7 Kbps, 8-PSK.
- **f)** 8 Kbps, 4-QAM.
- **g)** 10 Kbps, 16-QAM.
- **h)** 25 Kbps, 64-QAM.

■ **9.** Se dispone de un ancho de banda de 200 KHz para una comunicación full-dúplex que utiliza FDM para la transmisión de los dos sentidos de la comunicación, con una banda de guarda de 20 KHz. Obtener la velocidad de transmisión en cada uno de los apartados siguientes:
- **a)** Utilizando modulación FSK con una separación de frecuencias de 30 KHz.
- **b)** Utilizando modulación QPSK.
- **c)** Utilizando modulación 32-QAM.

■ **10.** Diseñar la configuración apropiada para transmitir, usando un canal de satélite de 5'12 MHz, veinte canales de datos (digitales) multiplexados utilizando FDM. Cada uno de los canales se debe transmitir a 2'048 Mbps.

■ **11.** Se multiplexan en TDM cuatro canales de 1 Kbps. Si en la ranura de tiempo (time slot) del multiplexor se envía 1 bit, hallar:
- **a)** La duración de un bit antes de la multiplexación.
- **b)** Tasa de bits de la transmisión.
- **c)** Duración de una trama.
- **d)** Duración del time slot.

■ **12.** Se desea multiplexar dos canales, uno con una tasa de 100 Kbps y otro de 200 Kbps con un time slot de 1 bit. ¿Cómo se podría realizar? ¿Cuántas tramas por segundo se enviarían? ¿Cuál es la duración de una trama? ¿Cuál es la tasa de bits de la transmisión?

■ **13.** Se desea transmitir 24 canales de voz, utilizando TDM con un time slot de 8 bits y un bit de sincronismo por trama. Para ello cada canal de voz se convierte a digital utilizando PCM y utilizando 8 bits por muestra. La tasa de bits de la señal multiplexada es de 1'544 Mbps. Dibujar la configuración del sistema ¿Cuál es la tasa de bits por canal? ¿Cuál es la tasa de muestreo en los conversores PCM?

■ **14.** Un concentrador telefónico utiliza un sistema TDM para trabajar internamente con señales de audio. Las señales de audio se digitalizan a 8.000 muestras por segundo y se utilizan 8 bit para codificar cada muestra. El sistema TDM utiliza un time slot de 1 byte. Los datos se envían en tramas de 1.024 bytes en las que se utilizan 2 bytes para señalización y sincronismo. Hallar:
- **a)** Tasa de bits de cada canal de audio.
- **b)** ¿Con cuántos canales de audio puede trabajar el sistema?
- **c)** Tasa de bits de la señal multiplexada.
- **d)** Número de tramas por segundo.

TEST DE CONOCIMIENTOS

1 ¿Cuál es el ancho de banda de una señal que tiene componentes de frecuencia de 100 Hz, 500 Hz y 1.000 Hz?
- **a)** 100 Hz.
- **b)** 500 Hz.
- **c)** 900 Hz.
- **d)** 1.000 Hz.

2 Una señal senoidal es un ejemplo de señal:
- **a)** Aperiódica.
- **b)** Digital.
- **c)** Compuesta.
- **d)** Analógica.

3 Una señal con una frecuencia de 10 KHz tiene más ciclos por segundo que otra señal con una frecuencia de:
- **a)** 1 GHz.
- **b)** 100 KHz.
- **c)** 1 KHz.
- **d)** Ninguna de las anteriores es correcta.

4 Al conjunto de todos los componentes de frecuencia de una señal compuesta se le conoce como:
- **a)** Fase.
- **b)** Espectro.
- **c)** Ancho de banda.
- **d)** Amplitud.

5 ¿Qué técnica de codificación usa valores alternativos positivos y negativos para la codificación de los unos?
- **a)** Manchester.
- **b)** RZ.
- **c)** NRZ-I.
- **d)** AMI.

6 En las codificaciones HDB3 y B8ZS una violación se utiliza:
- **a)** Para distinguir entre los códigos HDB3 y B8ZS.
- **b)** Para evitar la pérdida de sincronismo en la transmisión de muchos ceros seguidos.
- **c)** Para detectar códigos erróneos.
- **d)** Para minimizar el efecto de la componente continua en secuencias largas de unos.

7 ¿Cuál de las siguientes técnicas de codificación no proporciona buena sincronización?
- **a)** RZ.
- **b)** NRZ-L.
- **c)** HDB3.
- **d)** B8ZS.

8 ¿En qué tipo de modulación puede ser la tasa de bits tres veces mayor que la tasa de baudios?
- **a)** ASK.
- **b)** FSK.
- **c)** PSK.
- **d)** Ninguna de las anteriores.

9 El ancho de banda mínimo de una señal modulada en ASK:
- **a)** Depende de la frecuencia de la moduladora.
- **b)** Es el mismo que el de la señal original.
- **c)** Es el doble que el de la señal original.
- **d)** Es igual a la tasa de baudios.

10 En una modulación 8-PSK, ¿qué separación hay entre dos códigos consecutivos?
- **a)** 8 º.
- **b)** 45 º.
- **c)** 60 º.
- **d)** Depende de la señal moduladora.

11 En la modulación 32-QAM hay 32:
- **a)** Amplitudes diferentes.
- **b)** Fases diferentes.
- **c)** Combinaciones de amplitud y fase diferentes.
- **d)** Baudios.

12 La tasa de muestreo, expresada en millones de muestras por segundo, necesaria para una señal con componentes en el rango de 10MHz a 100 MHz es de:
- **a)** 10.
- **b)** 90.
- **c)** 100.
- **d)** 200.

13 La calidad de una señal PCM reconstruida depende de:
- **a)** La frecuencia y la tasa de muestreo.
- **b)** El número de bits por muestra y la tasa de muestreo.
- **c)** El ancho de banda y la tasa de muestreo.
- **d)** La tasa de muestreo.

14 En TDM asíncrono, si un canal tiene datos que enviar, los datos van dentro de la trama en:
- **a)** El siguiente time slot disponible.
- **b)** Un time slot preasignado.
- **c)** El primer time slot.
- **d)** Ninguna de las anteriores es correcta.

15 ¿Qué elementos usa un demultiplexor FDM para descomponer la señal multiplexada en sus señales constituyentes?
- **a)** Bandas de guardia.
- **b)** Filtros.
- **c)** Repetidores.
- **d)** Amplificadores.

16 La técnica utilizada en FDM para transportar el espectro de las señales al rango adecuado es:
- **a)** Codificación.
- **b)** Digitalización.
- **c)** Conmutación.
- **d)** Modulación.

17 En TDM asíncrona:
- **a)** Hay menos canales que time slots en una trama.
- **b)** Hay más canales que time slots en una trama.
- **c)** Hay el mismo número de canales que de time slots en una trama.
- **d)** No hay relación entre el número de canales y los time slots por trama.

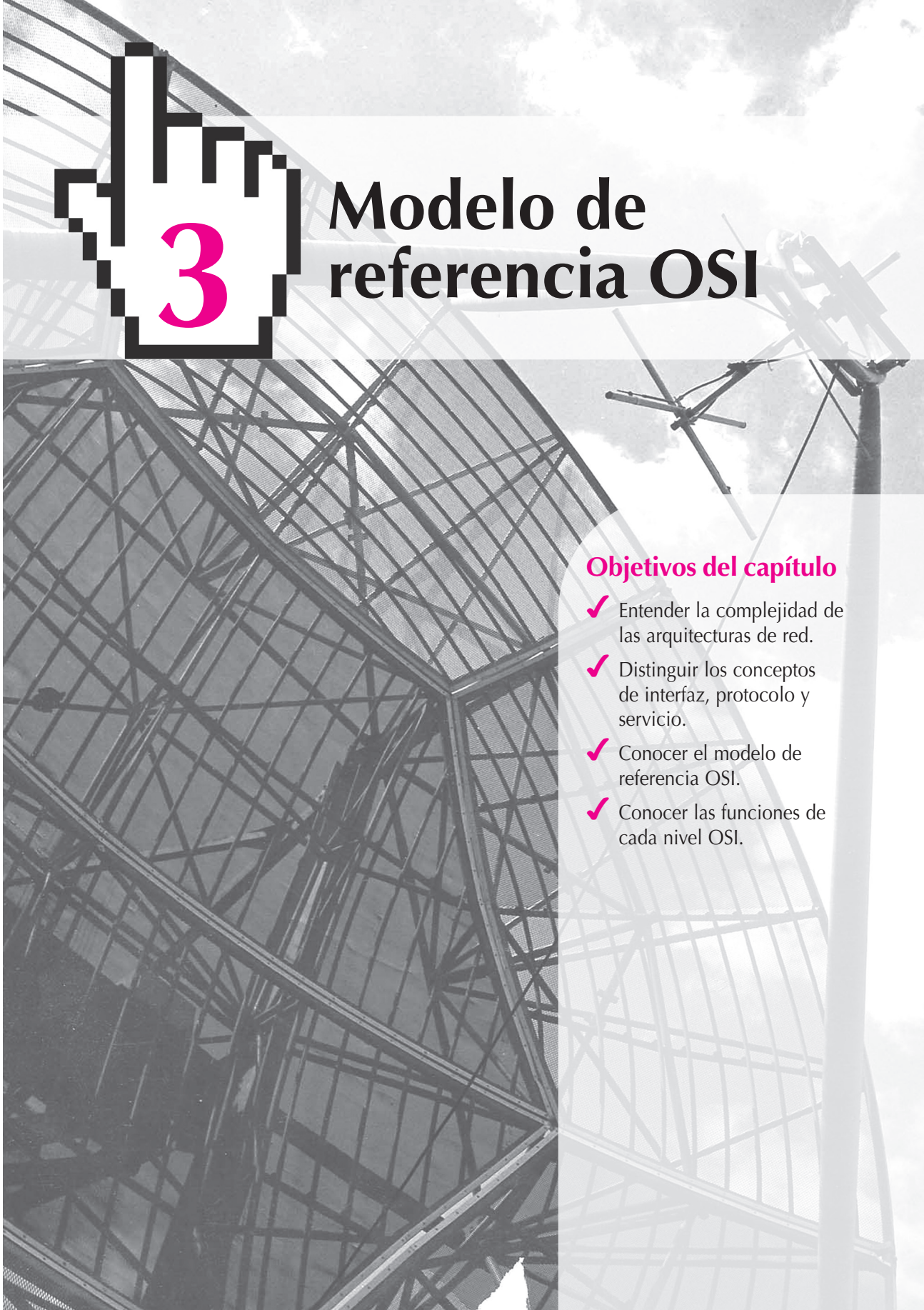
18 El ancho de banda de una señal FDM es:
- **a)** Mayor o igual a la suma de los anchos de banda de las señales multiplexadas.
- **b)** Menor o igual a la suma de los anchos de banda de las señales multiplexadas.
- **c)** Siempre igual a la suma de los anchos de banda de las señales multiplexadas.
- **d)** Depende si los canales son analógicos o digitales.

19 ¿Qué tipo de cable se divide en tres bandas de frecuencia para utilizar ADSL?

a) Coaxial.
b) Fibra óptica.
c) Par trenzado.
d) Cualquiera de las anteriores.

20 En la tecnología ADSL:

a) Se utilizan módems iguales en ambos lados de la transmisión.
b) Se utilizan módems diferentes en ambos lados de la transmisión.
c) Se utiliza un solo módem, en el otro extremo sólo es necesario un filtro.
d) No se utilizan módems para las transmisiones ADSL.



3 Modelo de referencia OSI

Objetivos del capítulo

- ✓ Entender la complejidad de las arquitecturas de red.
- ✓ Distinguir los conceptos de interfaz, protocolo y servicio.
- ✓ Conocer el modelo de referencia OSI.
- ✓ Conocer las funciones de cada nivel OSI.

3.1 JERARQUÍA DE NIVELES

En el capítulo 2 se han estudiado las técnicas fundamentales para la transmisión de datos utilizadas para el intercambio de datos, normalmente bits, entre dos dispositivos. La aplicación de dichas técnicas resuelve algunos de los requisitos elementales de los Sistemas Telemáticos, pero no todos.

Para que dos sistemas intercambien datos, no sólo es necesario que implementen técnicas de transmisión, sino que además lo hagan de forma armonizada, o dicho de otra forma, que se pongan de acuerdo en todos los aspectos que admiten posibles variaciones. Por ejemplo, la utilización del mismo tipo de codificación para los datos, los mismos niveles eléctricos, la misma frecuencia de modulación o la misma velocidad de transmisión…

Todo lo anterior sirve para que dos sistemas intercambien información con más o menos fortuna. Pero en la mayor parte de los sistemas telemáticos esto no es suficiente. Se plantean otras funciones que necesitan ser cubiertas para asegurar una comunicación fiable y eficiente, además de la mera transmisión de los datos.

Por ejemplo, es necesario implementar mecanismos que permitan un control del flujo de la información para evitar que el receptor se sature al no poder procesar todo lo que recibe. También se necesitan mecanismos para comprobar si se han producido errores durante la transmisión, especialmente en comunicaciones a largas distancias o comunicaciones radioeléctricas. Es posible que los datos deban pasar por varios sistemas hasta alcanzar su destino final, para ello es necesario implementar algún mecanismo de direccionamiento. La lista de funciones a implementar puede ser bastante extensa.

La primera conclusión que se puede obtener es que la implementación de un sistema telemático es un problema complejo. Para dar una visión más clara de esta complejidad se propone el siguiente ejercicio. Se trataría de obtener las funciones relacionadas con la comunicación que es necesario implementar en un tipo de comunicación en la que actualmente estamos todos familiarizados: **acceso a una página Web**.

La pregunta es ¿qué procesos relacionados con la comunicación se desencadenan cuando alguien sentado delante de un ordenador abre un navegador Web (Internet Explorer o Mozilla Firefox por poner dos de los más utilizados) e intenta acceder a una página Web? ¿Qué cuestiones se deben resolver para realizar la transferencia de datos que concluya con la visualización en el navegador Web de la página solicitada?

Cuando el usuario hace la petición de una página Web. El navegador transforma esta petición en una secuencia de bits, y esa secuencia de bits es lo que se tendrá que enviar a través posiblemente de varias redes hasta alcanzar el destino final, que será el equipo donde se esté ejecutando el servidor Web de la página solicitada. Cuando el servidor Web reciba la petición, generará una respuesta (la página Web solicitada) que, de nuevo, será transformada en una secuencia de bits,

y que serán transmitidos a través de diferentes sistemas hasta alcanzar el ordenador del usuario que solicitó la página Web.

Algunas de las cuestiones que se podría plantear el lector podrían ser:

Tabla 3.1

Tipo de medio de transmisión	Tanto el ordenador donde un usuario intenta acceder a una página Web como los diferentes sistemas por donde pasará la información podrán utilizar diferentes medios de transmisión como cable de cobre, espectro radioeléctrico, fibra óptica…
Codificación de los datos	Si se utiliza codificación en banda base (como por ejemplo en una red de área local), se deberá utilizar una técnica de codificación de los datos, como NRZ, AMI, HDB3, Manchester… Es más, si los datos pasan por diferentes sistemas (como, posiblemente sea el ejemplo planteado) hay que establecer el tipo de codificación de cada uno dichos sistemas.
Niveles de tensión de la señal eléctrica	La secuencia de bits generada por el navegador Web será transformada en una señal eléctrica con unos niveles de tensión determinados. En nuestro caso, este proceso se lleva a cabo en la tarjeta de red.
Acceso al medio de transmisión	Hay que establecer cuestiones como el tipo de conector, número de pines del mismo, tipo de antena si se utilizan medios inalámbricos…
Velocidad de transmisión	Esta velocidad normalmente es función de las características del medio de comunicación aunque pueden influir muchos otros factores. Se mide en bits por segundo (bps).
Encaminamiento	Es necesario establecer mecanismos para obtener la ruta que debe seguir la secuencia de bits para alcanzar el destino.
Direccionamiento	Si un sistema telemático está formado por varios dispositivos, se debe establecer un mecanismo para identificar de forma única cada uno de los dispositivos. En muchos casos, como en el ejemplo propuesto, este direccionamiento debe ser jerárquico.
Control de flujo	Esta función es necesaria para que un transmisor sólo envíe datos cuando tiene la certeza de que el receptor los puede procesar.
Control de errores	Ningún medio de transmisión está libre de errores por lo que habrá que establecer algún mecanismo para detectarlos y corregirlos.
Tramado	Para llevar un control efectivo de errores, del flujo y en general optimizar el rendimiento de los sistemas es necesario dividir la información que se quiere enviar en fragmentos.
Cifrado	En muchas ocasiones es necesario enviar información importante de forma segura. El mecanismo más efectivo para ello es el cifrado. La información se altera siguiendo un patrón establecido normalmente a través de una clave o contraseña de forma que si alguien intercepta esta información no será capaz de interpretarla.
Compresión	Las técnicas de compresión permiten reducir el número de bits necesarios para enviar la información, de forma que favorecen el rendimiento de las comunicaciones.

En la tabla anterior se han planteado algunas cuestiones básicas que es necesario definir para que la comunicación se lleve a cabo. Aunque no son todas, sí son suficientes para hacerse una idea de la complejidad mencionada.

Para afrontar esta complejidad, el diseño de las redes de comunicación de datos se lleva a cabo utilizando el concepto de **capas o niveles**. La idea fundamental de este tipo de diseño es dividir el proceso de comunicación en niveles. Cada uno de estos niveles deberá implementar una serie de funciones concretas sin tener en cuenta el resto de funciones, que serán resueltas en otros niveles.

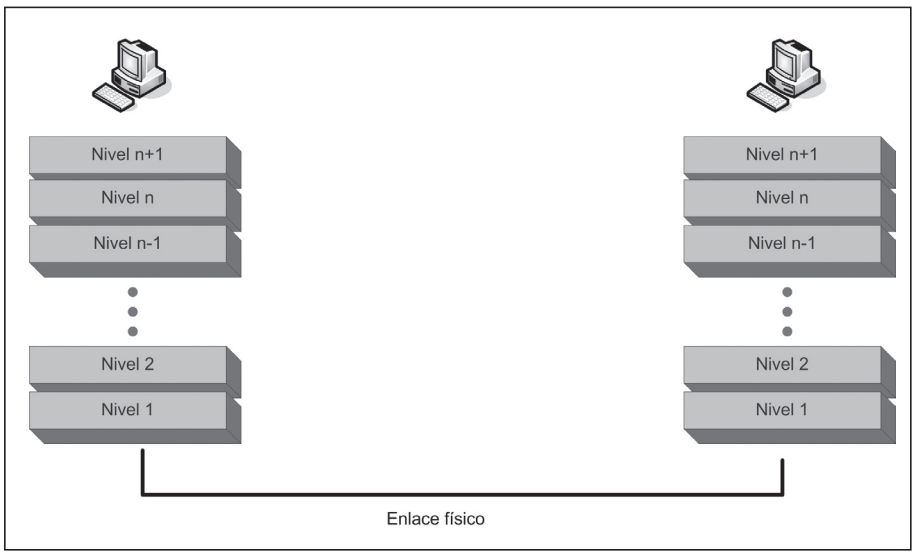


Figura 3.1. *Arquitectura de red por niveles.*

El diseño de una arquitectura en niveles está basado en los siguientes principios:

- ✓ Cada nivel lleva a cabo una serie de funciones de la comunicación. Estas funciones deben estar claramente definidas.
- ✓ El número de niveles y su función puede ser diferente en cada arquitectura de red. El número de niveles debe ser suficiente para separar las funciones de forma eficiente pero un número demasiado alto de niveles complicaría en exceso el diseño.
- ✓ Cada nivel *n* conoce la existencia de los niveles adyacentes, es decir, el nivel superior n+1 y el nivel inferior n-1.
- ✓ La comunicación entre niveles adyacentes se lleva a cabo por medio de **servicios**. Se dice, por tanto, que cada nivel ofrece servicios al nivel superior y utiliza servicios del nivel inferior.

- Una **interfaz** define básicamente qué información y servicios ofrece un nivel determinado al nivel superior. Es muy importante que las interfaces estén muy bien definidas. Cuando esto ocurre, la implementación específica de las funciones de un nivel puede ser modificada o reemplazada sin realizar ningún cambio en los niveles adyacentes, característica que se conoce como **modularidad**. Unas interfaces bien definidas proporcionan modularidad a la arquitectura de red.
- El diseño de las interfaces debe hacerse de forma que se minimice el flujo de información entre los niveles, en definitiva, las interfaces deben ser lo más sencillas posible.

3.2 TRANSFERENCIA DE INFORMACIÓN EN EL MODELO EN NIVELES

La finalidad del modelo de interconexión por niveles es transferir datos de un sistema a otro. Como se observa en la figura 3.2, cuando un nivel tiene que transferir datos, éstos deben pasar obligatoriamente por todos los niveles inferiores hasta alcanzar el destino de la comunicación donde la información transmitida deberá pasar igualmente por los niveles inferiores hasta alcanzar el nivel de destino.

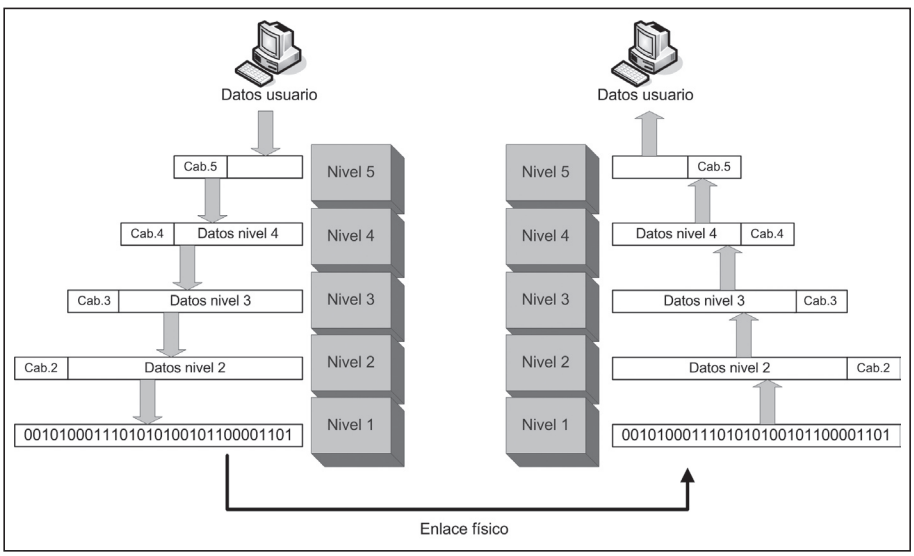


Figura 3.2. *Transferencia de datos en la arquitectura por niveles.*

En la jerarquía de niveles del transmisor, cada nivel añade a los datos que se envían al nivel inferior determinada información de control que será utilizada por el nivel homónimo de la comunicación. Esta información será tratada por el nivel inferior

como datos sin ningún significado especial y sólo el nivel homónimo en el receptor será capaz de interpretarlos. A esta información adicional se le denomina **cabecera o información de control**.

En la jerarquía de niveles del receptor el proceso será el inverso. Los datos llegarán al nivel más bajo, éste utilizará la información de la cabecera para llevar a cabo sus funciones y pasará los datos al nivel superior suprimiendo su cabecera. Este procedimiento se repite hasta alcanzar el nivel más alto que entrega los datos al proceso destino.

El diálogo que se lleva a cabo entre dos sistemas de comunicación en el mismo nivel se denomina **protocolo**. Un protocolo es un conjunto de reglas que se establecen para llevar a cabo una comunicación. Para que la comunicación entre niveles homónimos sea posible es necesario que utilicen el mismo protocolo.

A la lista de protocolos empleados en un sistema, con un protocolo por nivel, se le denomina **pila de protocolos**.

Se podría decir, por tanto, que en un modelo por niveles existen dos comunicaciones. Una real, llevada a cabo entre niveles adyacentes y cuya implementación a través de servicios se denomina interfaz, y otra **virtual**, llevada a cabo entre niveles homónimos a través de los llamados protocolos.

3.3 MODELO OSI

El modelo **OSI (Open System Interconnection, Interconexión de sistemas abiertos)** fue publicado en 1983 por el organismo de estandarización ISO. Este modelo aparece en la ISO como ISO 7498 y también forma parte de las recomendaciones de la ITU-T como recomendación X.200.

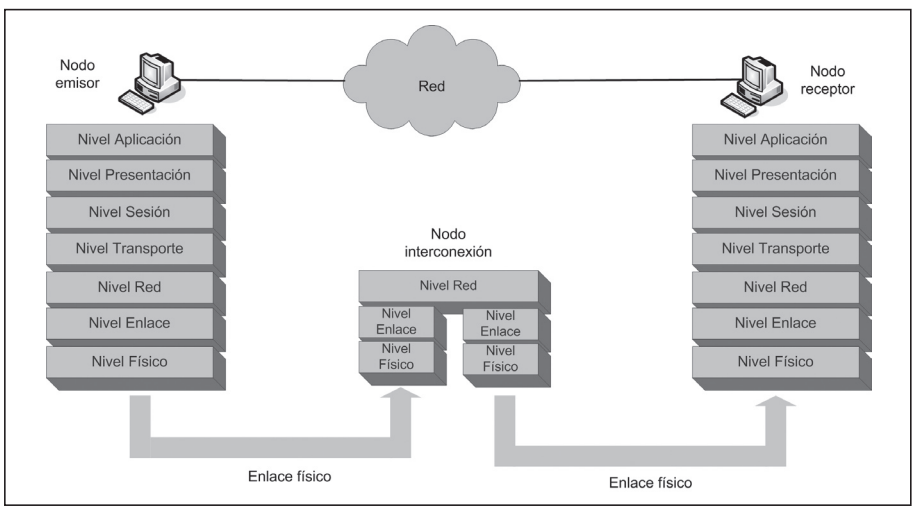


Figura 3.3. *Modelo OSI.*

OSI es una arquitectura basada en niveles para el diseño de sistemas de red. Este modelo además permite la interconexión de sistemas abiertos, o lo que es lo mismo, permite que dos sistemas diferentes se puedan comunicar independientemente de su arquitectura. Es importante resaltar que OSI es un modelo, no un protocolo. Además, el modelo OSI no especifica los servicios ni los protocolos que forman parte de cada nivel.

Los niveles definidos en el modelo OSI son siete: físico, enlace, red, transporte, sesión, presentación, aplicación.

En el modelo OSI, los niveles superiores se implementan por software mientras que los inferiores suelen llevar un alto componente hardware. El nivel físico es principalmente hardware.

En el gráfico anterior se tiene en cuenta la existencia de sistemas intermedios entre el emisor y receptor que pueden requerir la implementación de uno o varios niveles. Los sistemas intermedios más sofisticados podrán tener implementados los tres primeros niveles de la arquitectura, es decir, hasta el nivel de Red.

En los próximos apartados se exponen las funciones que deben ser cubiertas por cada uno de los niveles del modelo OSI.

3.4 FUNCIONES DEL NIVEL FÍSICO

El nivel físico se encarga de la transmisión de la información a través de un medio físico, es decir, el nivel físico debe ser capaz de enviar datos (bits) a través de un canal de comunicaciones (cable, fibra, aire) procurando que esos datos no sufran alteraciones y puedan ser correctamente interpretados en el receptor.

Para lograr este propósito se llevan a cabo las siguientes funciones:

- Definición de las **características físicas de las interfaces** con el medio de transmisión. Por ejemplo, las especificaciones de los conectores (interfaces con el medio de transmisión), tanto eléctricas (nivel de señal, impedancia…) como mecánicas (tipo de conector, dimensiones físicas, distribución del patillaje…) y funcionales (función de cada patilla en el conector…).
- Definición de las **características del medio de transmisión.** En el caso de medios guiados (cable y fibra óptica) será necesario definir las características físicas y mecánicas de dichos medios.
- **Codificación de los datos digitales.** La codificación fue tratada en el tema 2. Como se vio, este proceso consiste en representar los datos digitales, unos y ceros, en señales eléctricas que pueden ser transmitidas por el medio.

- **Configuración de la línea.** Que está referido a la forma en la que se conectan los dispositivos al medio. Puede ser punto a punto o multipunto.
- **Topología física.** Referido a las topologías de red vistas en el tema 1.
- **Modo de transmisión:** símplex, half-dúplex, full-dúplex.
- **Velocidad de transmisión.** Con todas las características anteriores se establece la velocidad a la que se pueden transmitir los datos, es decir, la tasa de bits de la comunicación.

Un ejemplo de implementación del nivel físico estandarizada es la conexión entre un DTE (equipo generador de datos, por ejemplo un ordenador) y un DCE (equipo transmisor de datos, por ejemplo un módem). Los principales organismos dedicados a estandarizar las distintas implementaciones del nivel físico han sido la EIA y la ITU-T.

3.5 FUNCIONES DEL NIVEL DE ENLACE

La transmisión de los datos se lleva a cabo en el nivel físico, aunque dicho nivel no proporciona ningún mecanismo para asegurar que los datos (bits) que se envían llegarán libres de errores al receptor. El objetivo del nivel físico es llevar a cabo la transmisión de los datos con la mayor fiabilidad posible pero sin llevar a cabo ningún control de errores, función de la que se encarga el nivel de enlace.

La principal función del nivel de enlace es, por tanto, la de proporcionar fiabilidad a la comunicación entre dos nodos de una red.

Además, el nivel de enlace lleva a cabo las siguientes funciones:

- **Encapsulación de datos: tramado.** Para llevar a cabo las funciones del nivel de enlace se hace necesario dividir el flujo de datos que llega del nivel superior en bloques de datos llamados tramas, a las cuales se añaden la cabecera con información de control del nivel de enlace. Una de las informaciones de control más importante que se añade es un código de comprobación de errores. Este código no se incluye en la cabecera sino que suele ir al final de la trama.
- **Proporcionar un direccionamiento físico.** Esto es necesario en los enlaces multipunto donde hay varios dispositivos conectados a una red y cualquiera de ellos puede ser el receptor de los datos. En este caso es necesario proporcionar un mecanismo de identificación del receptor. De hecho, tanto la dirección física del emisor como del receptor es una información incluida en la cabecera que se añade a los datos en el nivel de enlace.

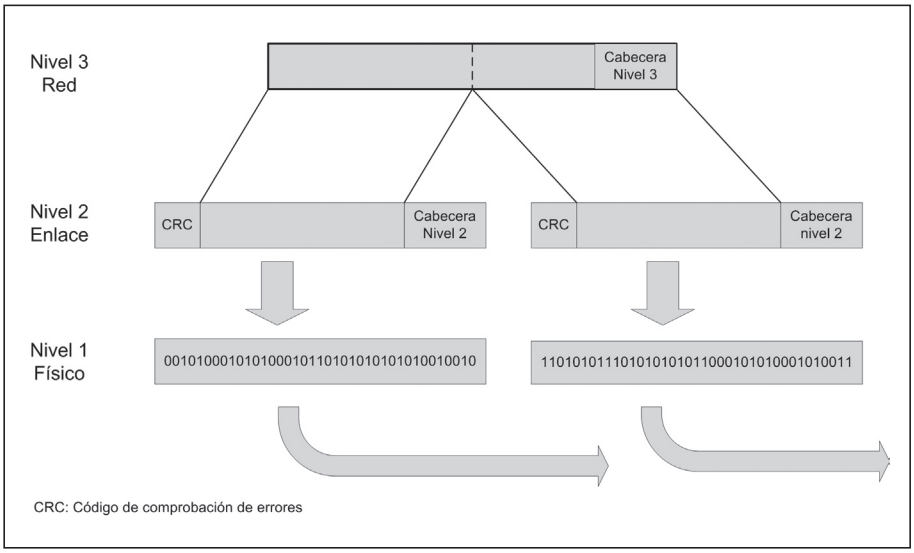


Figura 3.4. *Direccionamiento en el nivel de enlace.*

- **Control de acceso al medio.** Esta función no es siempre necesaria, sólo cuando el enlace es compartido por varios dispositivos. En este caso, es el nivel de enlace el encargado de determinar qué dispositivo puede acceder al medio para transmitir.
- **Control de flujo.** En una transmisión puede ocurrir que el receptor no sea capaz de procesar la información a la velocidad a la que la recibe. Si no se establecen mecanismos de control de flujo el receptor podrían perder datos. De esta forma, el emisor sólo transmite datos cuando el receptor pueda procesarlos.
- **Control de errores.** Como ya se ha apuntado, ésta es la principal función del nivel de enlace. Esta función incluye la capacidad de detectar y retransmitir tramas con error y tramas perdidas, así como detectar tramas duplicadas.

3.6 FUNCIONES DEL NIVEL DE RED

El nivel de red es responsable de la entrega de datos cuando el origen y el destino están situados en redes diferentes. Este nivel recibe un paquete de datos del nivel superior y se encarga de que llegue a su destino siendo necesario llevar a cabo mecanismos de encaminamiento. Cuando no es necesario ningún mecanismo de encaminamiento no sería necesario un nivel de red, bastaría con el nivel de enlace, por ejemplo, en un enlace punto a punto. Las funciones básicas que realiza, por tanto, son:

- **Encaminamiento o enrutamiento de los paquetes.** El nivel de red proporciona los mecanismos para la identificación de la ruta que deben llevar los paquetes de datos hasta alcanzar su destino.
- **Proporcionar un direccionamiento lógico.** El direccionamiento físico proporcionado por el nivel de enlace se utiliza para la identificación de equipos dentro de una red pero cuando es necesario la identificación de equipos distribuidos en redes diferentes es necesario establecer otro mecanismo de direccionamiento normalmente de tipo jerárquico. Por tanto, cada equipo debe identificarse a través de una dirección lógica. Estas direcciones se añaden a la cabecera del nivel de enlace.

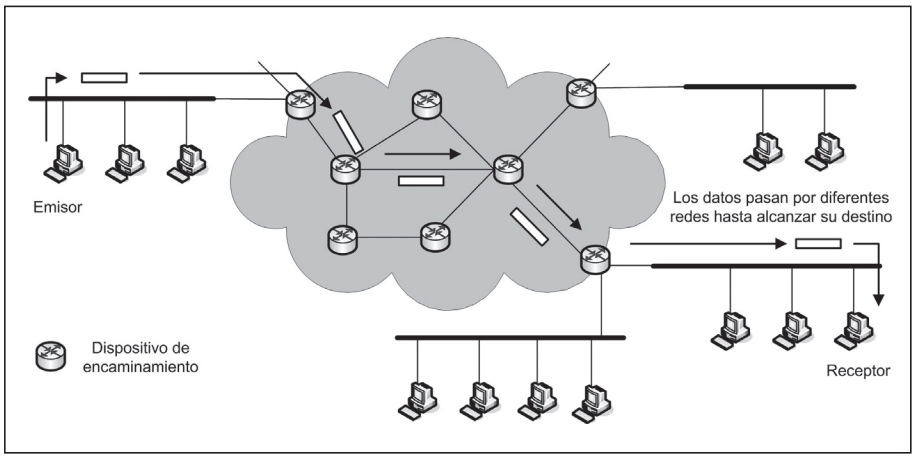


Figura 3.5. *Direccionamiento en el nivel de red.*

- **Control de la congestión.** La congestión se produce en las redes cuando los dispositivos de enrutamiento no son capaces de manejar el volumen de tráfico presente en la red. El control de la congestión podría confundirse con el control de flujo. La diferencia es que el control de la congestión se implementa para asegurar que la red es capaz de transportar el tráfico ofrecido mientras que el control de flujo está referido sólo a la conexión entre dos dispositivos concretos.

  La función principal llevada a cabo por el nivel de red, por tanto, es encaminar los paquetes de la máquina origen a la máquina destino. Los servicios implementados para llevar a cabo esta función pueden ser:

- **Servicios orientados a conexión.** Dichos servicios se implementan mediante lo que se conoce como circuitos virtuales. En estos servicios, para la transmisión de datos entre un origen y un destino se escoge una ruta para la transmisión de paquetes y esa ruta se utilizará para todas sus comunicaciones.

- **Servicios no orientados a conexión.** En este caso se dice que se realiza una conexión por datagramas. La ruta para la transmisión se calcula para cada paquete de forma independiente. Así, puede darse el caso de que dos paquetes con el mismo origen y destino utilicen rutas diferentes

Normalmente, los servicios no orientados a conexión añaden complejidad al siguiente nivel, el de transporte, mientras que los servicios orientados a conexión añaden complejidad al propio nivel de red. Los protocolos implementados en el nivel de red utilizarán un tipo u otro de servicios.

3.7 FUNCIONES DEL NIVEL DE TRANSPORTE

El nivel de transporte se encarga de llevar a cabo la entrega de un mensaje completo desde un origen a un destino. La diferencia con el nivel de red es que éste sólo se encarga del envío de paquetes individuales entre un origen y un destino sin tener en cuenta la relación entre los paquetes, es decir, trata cada paquete de forma individual. El nivel de transporte es responsable de que la información completa que se envía del emisor al receptor llegue correctamente. Las funciones que se desarrollan son:

- **Control de la conexión.** Al igual que en el nivel de red, existen dos formas de implementar las funciones del nivel de transporte, con servicios orientados a conexión y no orientados a conexión, los cuales existen de forma complementaria al nivel de red. Cuando se implementan servicios orientados a conexión, la transmisión del mensaje se lleva a cabo en tres pasos: establecimiento de la conexión, transferencia de datos y finalización de la conexión. Los servicios de un nivel de transporte orientado a conexión le dan fiabilidad a un nivel de red no orientado a conexión. Un ejemplo de protocolo de nivel de transporte orientado a conexión es TCP.
- **Control de flujo.** Esta función es similar a la ofrecida en el nivel de enlace pero en este caso el control del flujo se lleva a cabo sobre paquetes y no sobre bits, es decir, se lleva a cabo de extremo a extremo (donde normalmente estarán involucrados varios dispositivos de interconexión de redes) y no en una conexión entre dos dispositivos.
- **Control de errores.** Este control se lleva a cabo, al igual que el control de flujo, de extremo a extremo y no en la conexión entre dos dispositivos. La finalidad es asegurarse que todos los paquetes llegan sin errores, sin pérdidas y sin duplicados.
- **Direccionamiento.** Un equipo conectado a una red puede tener varios procesos, normalmente en la capa de aplicación, que llevan a cabo comunicación de datos a través de la red. Por ello, es necesario distinguir qué procesos dentro de cada equipo emisor y receptor están intercambiando información. Este direccionamiento se lleva a cabo en el nivel de transporte a través de la llamada **dirección de punto de servicio o dirección de puerto**.

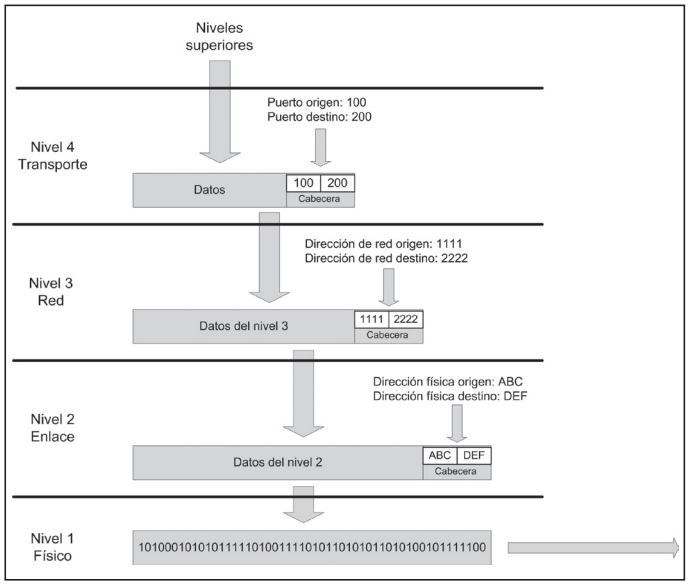


Figura 3.6. *Direccionamiento en el nivel de transporte.*

- **Calidad de servicio (QoS, Quality Of Service).** En el nivel de transporte se pueden proporcionar servicios para la mejora de la calidad del servicio. A continuación se enumeran algunos de los parámetros de calidad de servicio que puede proporcionar el nivel de transporte:
  - Retardo en el establecimiento de la conexión
  - Probabilidad de error en el establecimiento de una conexión
  - Velocidad de transmisión
  - Tasa de mensajes con error
  - Prioridad
  - Retardo en la liberación de la conexión

En la práctica, hay pocas implementaciones del nivel de transporte que tengan en cuenta todos los parámetros de calidad de servicio anteriores.

3.8 FUNCIONES DEL NIVEL DE SESIÓN

El nivel de sesión organiza y sincroniza el intercambio de datos entre procesos de aplicación. Las funciones que se llevan a cabo son:

- **Gestión de sesiones.** Para ello implementa las funciones necesarias para crear, mantener y finalizar sesiones de comunicación.
- **Sincronización.** Funciona con el nivel de aplicación para proporcionar conjuntos de datos sencillos llamados puntos de sincronización, que per-

mitirá a una aplicación conocer cómo está progresando la transmisión y recepción de datos. En caso de pérdida de transmisión o de errores es capaz de resincronizar el flujo de información.

El nivel de sesión asume que los dos extremos de la comunicación tienen la misma categoría, algo que no es muy frecuente en los servicios de red, los cuales son, en su gran mayoría, de tipo cliente-servidor.

3.9 FUNCIONES DEL NIVEL DE PRESENTACIÓN

La principal función del nivel de presentación es aislar las capas inferiores del formato de los datos del nivel de aplicación. Este nivel implementa características que tienen que ver con la sintaxis y la semántica de la información que se intercambia entre un emisor y un receptor. Las funciones que se pueden incluir en este nivel son:

- **Traducción o conversión.** Esta característica se utiliza cuando el emisor y el receptor utilizan sistemas de codificación de los datos diferentes. El nivel de presentación realiza una conversión del formato de datos específico del emisor a un formato común, que es el que utiliza para la transmisión de la información. El nivel de presentación del receptor volverá a realizar la conversión del formato común al formato específico utilizado en el receptor.
- **Cifrado.** Algunos procesos de red necesitan que la información se transmita cifrada para asegurar su privacidad. Los datos son transformados en función de los algoritmos de cifrado y en el receptor se realiza el proceso inverso para recuperar los datos originales.
- **Compresión.** Para aumentar las prestaciones de la transferencia de datos sobre todo para volúmenes altos se puede utilizar compresión.

3.10 FUNCIONES DEL NIVEL DE APLICACIÓN

El nivel de aplicación proporciona la interfaz de usuario para llevar a cabo los procesos de comunicación. Este nivel es el que está en contacto directo con las aplicaciones de usuario y, por tanto, los servicios que ofrece son aquéllos que son útiles a los usuarios de las redes. Como el nivel de aplicación es el nivel más alto en el modelo OSI no se añaden cabeceras a los datos.

Algunos ejemplos de funciones implementadas en el nivel de aplicación son:

- **Servicios de correo electrónico.** Este nivel implementa los mecanismos para el envío, recepción y almacenamiento de mensajes de correo electrónico. Para llevar a cabo esta función, la organización ISO junto con la

ITU-T desarrollaron el protocolo **X.400**. Sin embargo, en la actualidad se ha impuesto el protocolo utilizado en el modelo TCP/IP llamado **SMTP (Simple Mail Transfer Protocol)**.

- **Servicio de transferencia de ficheros.** Este servicio permite enviar o recibir archivos de un equipo remoto. El protocolo desarrollado por la ISO para llevar a cabo esta función es **FTAM (File Transfer Access and Management)** que, al igual que en el servicio de correo, actualmente no se utiliza a favor del protocolo de transferencia de ficheros utilizado en el modelo TCP/IP, llamado **FTP (File Transfer Protocol)**.
- **Servicio World Wide Wide (o www).** Este servicio de acceso a páginas Web es uno de los pilares de Internet y por extensión del modelo TCP/IP aunque se puede considerar un servicio típico del nivel de aplicación también en el modelo OSI. El protocolo mediante el que se implementa este servicio es **HTTP**.
- **Terminal virtual.** Mediante esta función es posible ejecutar comandos en un equipo remoto. El protocolo más conocido de terminal virtual es telnet, desarrollado para el modelo TCP/IP.

3.11 IMPLANTACIÓN DEL MODELO OSI

En el contexto en el que se desarrolló, el modelo OSI parecía una solución a la interconexión de sistemas debido a la existencia de grandes empresas con arquitecturas propietarias e incompatibles, como SNA de IBM y DECnet de Digital.

Sin embargo, la complejidad que supuso el desarrollo de los protocolos que implementaran este modelo y el auge de la arquitectura TCP/IP, que ya tenía sus protocolos desarrollados y estaban suficientemente probados en entornos académicos, supuso el progresivo declive de la implementación del modelo OSI a favor del modelo TCP/IP que ha sido el que se ha impuesto definitivamente propiciado sobre todo por el auge de Internet.

Uno de los principales problemas del modelo OSI es que fue desarrollado sin tener en cuenta los protocolos que luego se deberían utilizar. De esta forma, hay algunos niveles donde apenas se desarrollaron protocolos, como el nivel de sesión, y otros, como el nivel de enlace, en los que fue necesario desarrollar protocolos complejos e incluso dividir sus funciones en subniveles.

La arquitectura TCP/IP propone la existencia de cinco niveles: físico, enlace, red, transporte y aplicación. Como se observa, la diferencia más obvia es que en este modelo no aparecen los niveles de sesión y presentación. Lo que ocurre es que cualquier función por encima del nivel de transporte en TCP/IP se implementa en el nivel de aplicación. Los niveles con más similitudes entre el modelo OSI y el modelo TCP/IP son los de red y de transporte.

La principal aportación del modelo OSI es servir como referencia al desarrollo de arquitecturas de red. En dicho modelo se establecen de forma clara los conceptos de servicio, interfaz y protocolo, cosa que no ocurre en TCP/IP. Por ello, este modelo tiene gran valor pedagógico en el estudio de arquitecturas de red.

Por el contrario, aunque la arquitectura TCP/IP es la que se ha impuesto en la actualidad, su modelo no es un modelo general y sólo sirve para describir su propia arquitectura. Como ejemplo, en el modelo TCP/IP no se hace una distinción entre las capas física y de enlace (por lo que, en realidad el modelo TCP/IP consta de cuatro niveles), cosa que desde el punto de vista del diseño de redes no es muy aceptable. Esto es debido a que primero se desarrollaron los protocolos y el modelo TCP/IP es tan sólo una descripción de dichos protocolos.

Se puede concluir, por tanto, que la referencia en interconexión de sistemas como modelo es el modelo OSI y como protocolos, son los protocolos de la arquitectura TCP/IP.

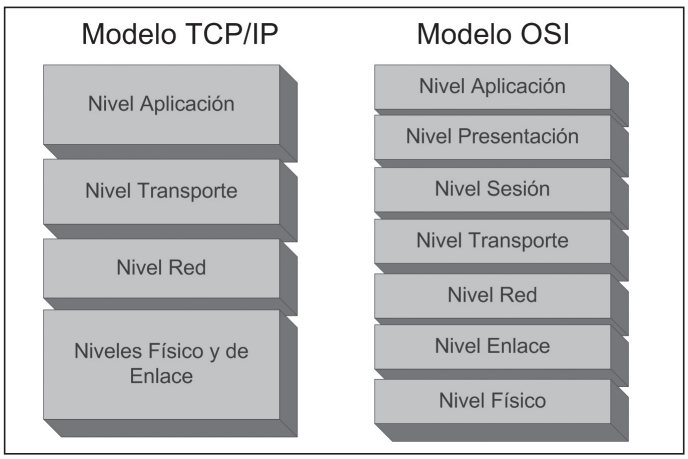


Figura 3.7. *Comparación del modelo OSI y el modelo TCP/IP.*

RESUMEN DEL CAPÍTULO

Después de estudiar las técnicas de transmisión de datos en el capítulo anterior, en este capítulo se plantea la necesidad de resolver la complejidad de las comunicaciones telemáticas mediante el establecimiento de niveles, donde cada uno de los cuales se responsabiliza de una serie de funciones de la comunicación.

Con esta premisa se estudia el modelo OSI propuesto por la ISO. Este modelo, además, está planteado para permitir la interconexión de sistemas abiertos, es decir, que la comunicación entre dos sistemas sea independiente de su arquitectura hardware.

El resto del capítulo se dedica a exponer las funciones que el modelo OSI asigna a cada uno de los siete niveles definidos:

Tabla 3.2

Nivel 1	Físico	Transmisión de bits sobre el medio. Proporcionar especificaciones eléctricas y mecánicas
Nivel 2	Enlace	Organizar los bits en tramas y proporcionar entrega fiable de nodo a nodo de un enlace
Nivel 3	Red	Transportar paquetes entre un origen y un destino, enrutando los paquetes a través de diferentes redes
Nivel 4	Transporte	Proporcionar la entrega fiable de un mensaje completo entre un origen y un destino
Nivel 5	Sesión	Gestión de sesiones y establecimiento de punto de sincronización
Nivel 6	Presentación	Lleva a cabo funciones de traducción, cifrado y compresión de los datos
Nivel 7	Aplicación	Permitir acceso a recursos y servicios de red

Por diferentes razones el modelo OSI nunca fue llevado a la práctica y ninguna arquitectura de red lo implementa, aunque sigue siendo útil para ofrecer una visión clara de los modelos de red. En la práctica, la arquitectura predominante y que no se ajusta al modelo OSI es TCP/IP, que se estudiará en el capítulo 8.

EJERCICIOS PROPUESTOS

1. Aplicar los conceptos que aparecen en la jerarquía por niveles del modelo OSI a una empresa de logística que envía paquetes de todo tipo a cualquier lugar del mundo.

Para ello definir primero las funciones, los niveles y asignar cada función en uno de los niveles definidos. Aplicar en alguno de los niveles definidos el concepto de interfaz y de protocolo.

A continuación se sugieren algunos aspectos que se deben tener en cuenta en la definición de las funciones:

- ✓ Identificación del destinatario: nombre, dirección, localidad…
- ✓ Reglas de tratamiento de los paquetes: frágiles, voluminosos, peligrosos…
- ✓ Tipo de embalaje
- ✓ Métodos de comprobación de los destinatarios
- ✓ Etiquetado de paquetes
- ✓ Prioridades
- ✓ Elaboración de rutas de envío
- ✓ Tipos de medios de transporte: camión, coche, avión, barco…
- ✓ Elementos físicos: carreteras, calles…

2. Con la ayuda de los diferentes materiales de apoyo como libros, revistas e Internet, y el apoyo del profesor, elabora una lista de protocolos utilizados en sistemas telemáticos indicando el nivel OSI correspondiente y la arquitectura de red a la que pertenece.

TEST DE CONOCIMIENTOS

1 En el modelo OSI, los niveles añaden sus propias cabeceras excepto el nivel 1 y el nivel:

a) 2.
b) 5.
c) 7.
d) Ninguna es correcta.

2 Para que haya comunicación entre dos niveles homónimos en el modelo OSI es necesario que utilicen:

a) El mismo protocolo.
b) La misma interfaz.
c) El mismo lenguaje de programación.
d) El mismo sistema operativo.

3 La información contenida en la cabecera la procesa:

a) El nivel superior.
b) El nivel inferior.
c) El nivel homónimo.
d) El nivel más alto.

4 El nivel que asegura la transmisión fiable de datos en un enlace simple es:

a) El nivel físico.
b) El nivel de enlace.
c) El nivel de transporte.
d) El nivel de aplicación.

5 La dirección física de los dispositivos se define:
a) En el nivel físico.
b) En el nivel de enlace.
c) En el nivel de transporte.
d) En el nivel de sesión.

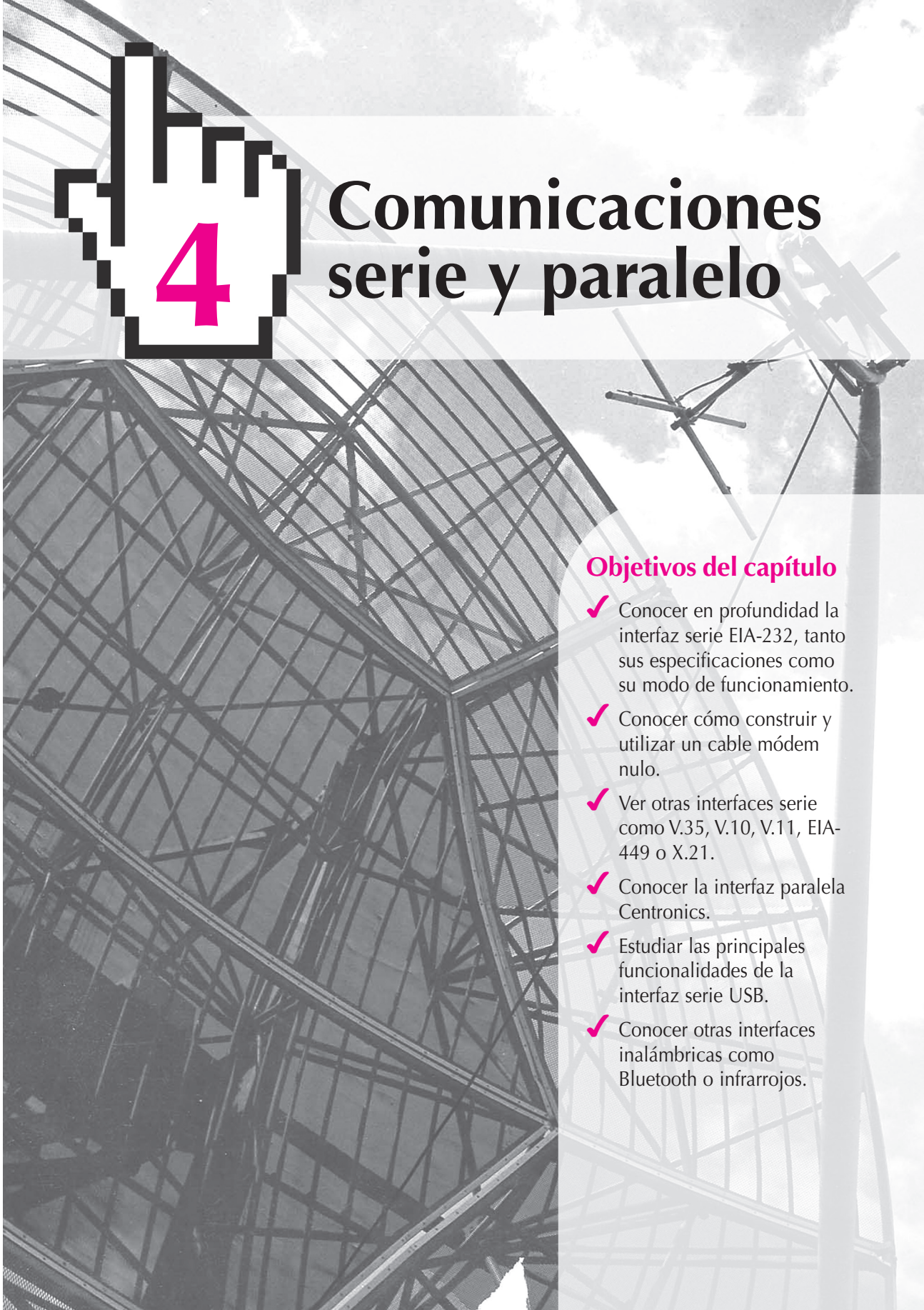
6 El control de la congestión se lleva a cabo en el:
a) Nivel de enlace.
b) Nivel de transporte.
c) Nivel de red.
d) Nivel de aplicación.

7 Las direcciones de puerto se definen en el:
a) Nivel de enlace.
b) Nivel de transporte.
c) Nivel de red.
d) Nivel de aplicación.

8 ¿Cuál de los siguientes niveles no incluye en sus funciones ningún tipo de direccionamiento?
a) Nivel de enlace.
b) Nivel de transporte.
c) Nivel de red.
d) Nivel de aplicación.

9 La transferencia de ficheros es un servicio proporcionado por el:
a) Nivel de enlace.
b) Nivel de transporte.
c) Nivel de red.
d) Nivel de aplicación.

10 Actualmente la mayor parte de las redes:
a) Utilizan arquitecturas basadas en el modelo OSI en redes WAN.
b) Utilizan arquitecturas basadas en el modelo OSI en redes LAN.
c) Utilizan la arquitectura TCP/IP y arquitecturas basadas en el modelo OSI conjuntamente.
d) Utilizan la arquitectura TCP/IP.



4 Comunicaciones serie y paralelo

Objetivos del capítulo

- ✓ Conocer en profundidad la interfaz serie EIA-232, tanto sus especificaciones como su modo de funcionamiento.
- ✓ Conocer cómo construir y utilizar un cable módem nulo.
- ✓ Ver otras interfaces serie como V.35, V.10, V.11, EIA-449 o X.21.
- ✓ Conocer la interfaz paralela Centronics.
- ✓ Estudiar las principales funcionalidades de la interfaz serie USB.
- ✓ Conocer otras interfaces inalámbricas como Bluetooth o infrarrojos.

4.1 INTRODUCCIÓN

En el tema anterior se vio como los sistemas de red se estructuran en niveles, cada uno de los cuales se encarga de llevar a cabo algunas de las funciones de la comunicación.

En este tema se estudiará un ejemplo de la implementación del nivel físico: **las interfaces serie**. Además, como ejemplo de transmisión de datos en paralelo se verá la interfaz Centronics, utilizada para la interconexión de un ordenador con una impresora.

También se estudiará una de las interfaces serie más extendidas hoy en día en el mercado informático de consumo, la interfaz USB. Esta interfaz aunque no forma parte de los sistemas de red, actualmente se utiliza para la conexión de casi cualquier dispositivo a un ordenador.

Una interfaz en el nivel físico tiene como objetivo la interconexión de dos dispositivos de forma que se pueda establecer entre ellos un flujo efectivo de información. Para que esto sea posible, independientemente del fabricante de los dispositivos, es necesario definir perfectamente sus características eléctricas, mecánicas y funcionales, es decir, será necesario definir un estándar. La mayor parte de los aspectos tratados en este capítulo están definidos en sus correspondientes estándares.

NOTA 4.1

Las interfaces serie y paralelo tratan las funciones del nivel 1 o nivel físico del modelo OSI, es decir, especificaciones eléctricas, mecánicas y funcionales, normalmente definidas a través de estándares.

4.2 CONCEPTOS DE TRANSMISIÓN DE DATOS DIGITALES

4.2.1 TRANSMISIÓN PARALELA Y SERIE

La transmisión de datos digitales se puede llevar a cabo de dos formas:

- **Transmisión paralela.** Los datos binarios, formados por unos y ceros se agrupan formando palabras. En la transmisión paralela se envían simultáneamente los *n* bits que forman una palabra. Para ello se emplea un solo cable por cada bit de la palabra. El valor típico de bits para la transmisión en paralelo es de 8 bits.

  Este tipo de transmisión aporta en principio más velocidad, ya que se pueden transmitir varios bits simultáneamente. La principal desventaja es el coste, por tanto, se utiliza sólo para distancias cortas.

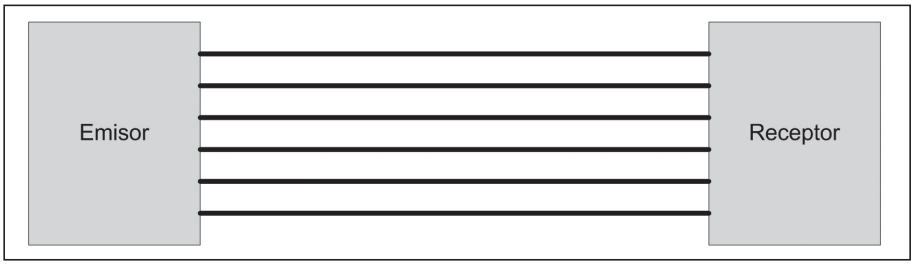


Figura 4.1. *Transmisión paralela.*

- **Transmisión serie.** Los datos binarios se envían bit a bit, uno detrás de otro, por un solo canal de comunicaciones. La ventaja de este tipo de comunicación es su bajo coste respecto a la transmisión paralela. Normalmente, los equipos de emisión y recepción trabajan con la información en paralelo por lo que se necesitarán conversores paralelo-serie y serie-paralelo.

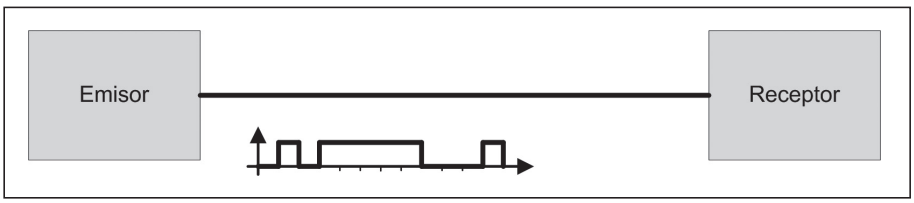


Figura 4.2. *Transmisión serie.*

4.2.2 TRANSMISIÓN ASÍNCRONA Y SÍNCRONA

Las transmisiones serie de datos digitales se pueden realizar de dos formas:

- **Transmisión asíncrona.** Para enviar los datos, los bits se agrupan en bytes, es decir, en 8 bits. Como no hay sincronización entre el emisor y el receptor se envía un bit extra, llamado bit de comienzo (start), al principio de cada byte para indicar la llegada de datos. Se envía también un bit al final de cada byte llamado bit de parada (stop). Estos bits de parada y arranque sirven para la sincronización de los datos.

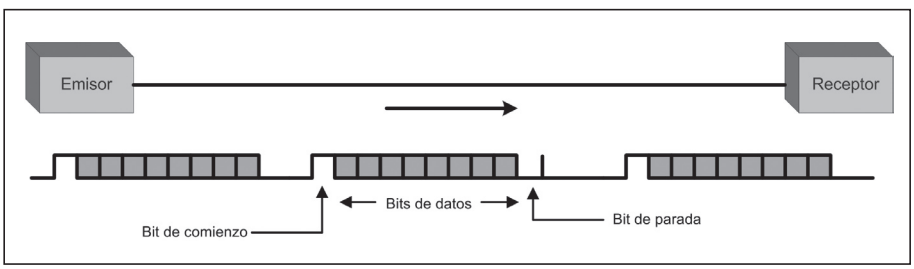


Figura 4.3. *Transmisión asíncrona.*

- **Transmisión síncrona.** Los datos se transmiten como una cadena continua de unos y ceros y el receptor se encarga de extraer los bytes de forma adecuada. Como no existe separación entre los bytes y tampoco existen bits de inicio y parada es muy importante la sincronización entre el emisor y el receptor. Para ello es necesario que la transmisión sea continua. Si no hay datos que transmitir se envían secuencias especiales de ceros que indican un vacío de datos.

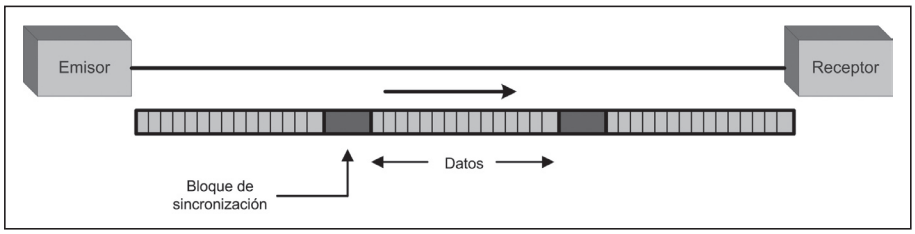


Figura 4.4. *Transmisión síncrona.*

4.2.3 INTERFAZ DTE-DCE

En muchos sistemas de comunicación existe una separación entre el equipo que genera los datos y el equipo que transmite o recibe los datos a través de una red telemática. De forma genérica, estos dos tipos de elementos se conocen como DTE y DCE:

- **DTE (Data Terminal Equipment, Equipo Terminal de Datos)** es cualquier dispositivo que funcione como origen o destino para datos digitales binarios que se van a transmitir. Normalmente suele ser un ordenador o un router.
- **DCE (Data Circuit-Terminating Equipment, Equipo Terminal del Circuito de Datos)** es cualquier dispositivo que lleve a cabo el intercambio de datos a través de una línea de comunicación. Por ejemplo un módem.

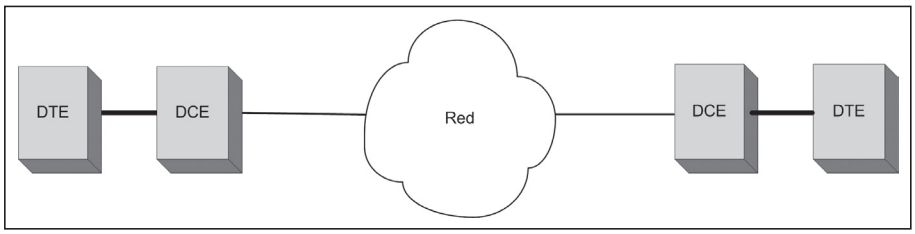


Figura 4.5. *Interfaz DTE-DCE.*

Como se observa en la figura, debe existir un enlace o interfaz entre estos dos elementos. La mayor parte de las especificaciones de interfaces serie precisamente definen la interconexión de un DTE y un DCE.

4.3 INTERFAZ EIA-232 / V.24

Una de las interfaces serie más populares y utilizadas en la transmisión de datos es la conocida como EIA-232, desarrollada originalmente para la interconexión de un DTE con un DCE.

La primera especificación de esta interfaz se publicó en 1962 y desde entonces ha sido revisada varias veces. Una de las revisiones más extendidas fue la EIA-232-C. El primer nombre que recibió esta interfaz fue **RS-232**, nombre que aún hoy se utiliza ampliamente, a pesar de que dicho estándar lo adoptaría la organización de estandarización norteamericana **EIA (Electronic Industries Alliance**, o hasta 1997 **Electronic Industries Association**) cambiando su nombre al actual EIA-232.

Posteriormente la ITU-T desarrolló las correspondientes recomendaciones basadas en la interfaz EIA-232. La recomendación V.24 especifica los aspectos funcionales y operacionales, es decir, se definen qué circuitos o señales tienen que implementarse en la interfaz y la función de cada uno de ellos. Los aspectos eléctricos de la interfaz están definidos en la recomendación V.28.

En los siguientes apartados se expondrán las principales características definidas en las correspondientes recomendaciones V.24 y V.28.

4.3.1 ESPECIFICACIONES MECÁNICAS

- ✓ Se utiliza un cable de 25 conductores, cada uno de ellos con una función específica. En la mayor parte de las aplicaciones no se utilizan todos los conductores.
- ✓ En los extremos del cable se utiliza un conector DB-25 macho en uno de los extremos y un conector DB-25 hembra en el otro. La norma no obliga a la utilización de este conector. De hecho existe una variante que utiliza conectores DB-9.
- ✓ Se utiliza la norma ISO 2110 desarrollada por la ISO donde se incluyen las especificaciones mecánicas y asignación de pines del conector DB-25. Para las especificaciones mecánicas y asignación de pines del conector DB-9 se utiliza la norma ISO 4902.
- ✓ El conector hembra se utiliza para el DTE (ordenador) y el conector macho para el DCE (módem).
- ✓ La longitud del cable no puede exceder de 15 metros.

NOTA 4.2

IMPORTANTE: la mayor parte de los ordenadores actualmente tienen un puerto paralelo que utiliza un conector DB-25 macho. **No confundir con una interfaz serie EIA-232 que requeriría un conector DB-25 hembra.**

4.3.2 ESPECIFICACIONES ELÉCTRICAS

En las especificaciones eléctricas se definen los niveles de voltaje y el tipo de señal a transmitir.

- Se utiliza codificación NRZ-L, es decir, el *cero lógico* se codifica con un pulso positivo y el *uno lógico* se codifica con un pulso negativo, con unos rangos de tensión permitidos de entre 3 y 15 v y de entre -3 y -15 v. La tensión nominal es de 12 v. Y la tensión máxima de 25 v.

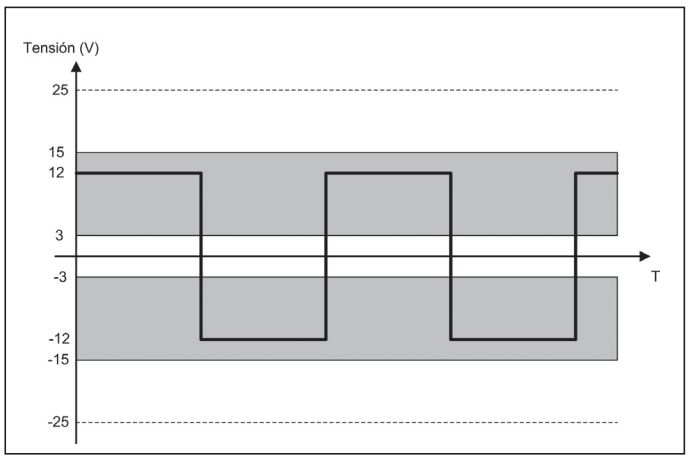


Figura 4.6. *Señal eléctrica en la interfaz V.24.*

- De los 25 conductores sólo cuatro son utilizados para datos. El resto son de control, temporización, tierra y pruebas. La especificación eléctrica para estos circuitos es igual que para los datos, considerando el estado ON equivalente al *cero lógico* y OFF equivalente al *uno lógico*.
- La transmisión de la señal eléctrica se lleva a cabo de forma **no balanceada**. La transmisión de los datos a través de líneas no balanceadas es más sencilla ya que se utiliza un solo conductor por cada señal a transmitir y una señal común de tierra para todas. En las **líneas balanceadas** se utilizan dos conductores por cada señal a transmitir además de una tierra común, por tanto necesita más conductores para transmitir las mismas señales. Sin embargo, la transmisión balanceada se utiliza en algunas interfaces ya que hace más inmune al ruido a la señal y permite alcanzar velocidades más altas.
- La tasa de bits máxima que se recomienda en la norma para la distancia máxima de 15 metros es de 20 Kbps. Esta velocidad se puede aumentar si se disminuye la distancia de conexión. En la recomendación V.28 se especifica que en determinadas condiciones se podría llegar hasta 64 Kbps.

4.3.3 ESPECIFICACIONES FUNCIONALES

Existen dos implementaciones funcionales de la EIA-232 en función del conector y número de conductores utilizado.

4.3.3.1 Implementación DB-25

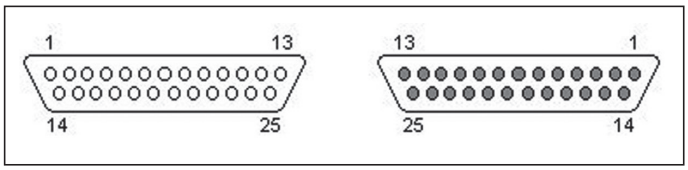


Figura 4.7. *Esquema pines de los conectores DB-25 macho y hembra.*

La definición de las funciones asignadas a cada uno de los pines de un conector DB-25 son las mostradas en la tabla siguiente:

Tabla 4.1 Función de los pines en el conector DB-25

Nº pin	Nombre	Función	Dirección
1		Protección a tierra	-
2	TX	Transmisión de datos	DTE-DCE
3	RX	Recepción de datos	DCE-DTE
4	RTS	Request to send - Petición para enviar	DTE-DCE
5	CTS	Clear To Send - Listo para enviar	DCE-DTE
6	DSR	Data Set Ready - DCE listo	DCE-DTE
7	GND	Tierra	-
8	DCD	Data Carrier Detect - Detección de portadora	DCE-DTE
9		Reservado para test	
10		Reservado para test	
11		Sin asignar	
12	DCD 2	Data Carrier Detect - Detección de portadora del canal secundario	DCE-DTE
13	CTS 2	Clear To Send - Listo para enviar del canal secundario	DCE-DTE
14	TX 2	Transmisión de datos del canal secundario	DTE-DCE
15	TC	Temporización (reloj) de transmisión (modo síncrono)	DCE-DTE
16	RX 2	Recepción de datos del canal secundario	DCE-DTE
17	RC	Temporización (reloj) de recepción (modo síncrono)	DCE-DTE
18		Bucle local	DTE-DCE
19	RTS 2	Request To Send - Petición para enviar del canal secundario	DTE-DCE
20	DTR	Data Terminal Ready - DTE listo	DTE-DCE
21	SQ	Signal Quality - Bucle local y detector de calidad de la señal	DTE-DCE
22	RI	Ring Indicator - Indicador llamada entrante	DCE-DTE
23		Selector de velocidad del DTE	DTE-DCE
24	XTC	Temporización (reloj) de transmisión (modo síncrono)	DTE-DCE
25		Reservado para test	

- El pin 2 se utiliza para transmitir datos en serie desde el DTE al DCE (transmisión) y el pin 3 se utiliza para transmitir datos en serie desde el DCE al DTE (recepción).

  Además existen dos pines más para la transmisión y recepción de datos para un canal secundario opcional. El 14 se utiliza para transmisión y el 16 para recepción del canal secundario.

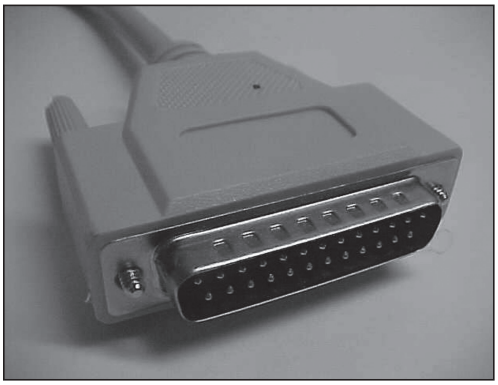


Figura 4.8. *Conector DB-25 macho.*

- Los pines 15, 17 y 24 se utilizan para enviar señales de reloj o sincronismo en el caso de llevar a cabo transmisiones síncronas. Para transmisiones asíncronas estos pines no se utilizan.

Las funciones de los principales pines de control son:

- **Pin 4 – RTS.** Utilizado por el DTE para solicitar el envío de datos al DCE. Es decir, la activación de esta señal informa al DCE que el DTE quiere enviar datos.
- **Pin 5 – CTS.** Utilizado por el DCE para indicar al DTE que está listo para enviar datos y por tanto el DTE puede comenzar a enviar los datos.
- **Pin 6 – DSR.** Utilizado por el DCE para indicar al DTE que está operativo. Cuando el DCE es un módem, esta señal indica que el módem está conectado a una línea telefónica y preparado para establecer una comunicación.
- **Pin 20 – DTR.** Utilizado por el DTE para indicarle al DCE que está operativo y preparado para solicitar el envío de datos.
- **Pin 8 – DCD.** Cuando el DCE es un módem se utiliza para indicar que la línea está descolgada, la conexión se ha establecido y se ha recibido el tono de respuesta del módem remoto.
- **Pin 22 – RI.** Cuando el DCE es un módem se utiliza para indicar que se ha detectado una señal de llamada entrante.

Los pines 9, 10, 18, 21 y 25 están reservados para realización de pruebas de transmisión y detección de la calidad de la señal. No se suelen utilizar.

Como se observa en la tabla anterior existen también pines de control CTS, RTS y DCD para el canal secundario.

■ 4.3.3.2 Implementación DB-9

Debido a que muchos de los circuitos definidos en la implementación DB-25 no se utilizan, se ha desarrollado una versión más sencilla de la norma EIA-232 utilizando un conector DB-9, con 9 pines. Al igual que para el conector DB-25, el conector para el DTE (ordenador) debe ser hembra.

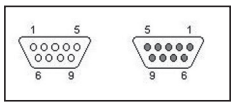


Figura 4.9. *Esquema pines de los conectores DB-9 macho y hembra.*

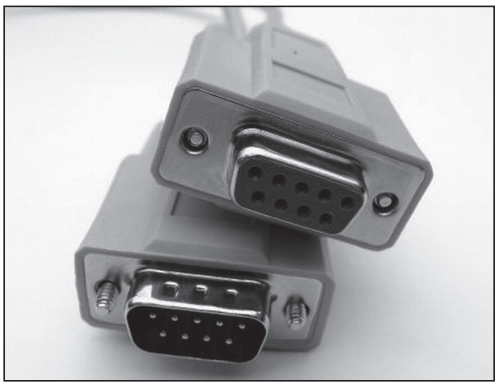


Figura 4.10. *Conectores DB-9 macho y hembra.*

La asignación de pines es la siguiente:

Tabla 4.2 Función de los pines en el conector DB-9

Nº pin	Nombre	Función	Dirección
1	DCD	Data Carrier Detect – Detección de portadora	DCE-DTE
2	RX	Recepción de datos	DCE-DTE
3	TX	Transmisión de datos	DTE-DCE
4	DTR	Data Terminal Ready – DTE listo	DTE-DCE
5	GND	Tierra	-
6	DSR	Data Set Ready – DCE listo	DCE-DTE
7	RTS	Request To Send – Petición para enviar	DTE-DCE
8	CTS	Clear To Send – Petición para enviar	DTE-DCE
9	RI	Ring Indicator – Indicador de llamada entrante	DCE-DTE

También se pueden encontrar interfaces serie EIA-232 que utilizan los dos tipos de conectores. Normalmente suele ser DB-25 macho para la conexión al DCE y DB-9 hembra para la conexión al DTE. Un ejemplo se puede ver en la siguiente figura:

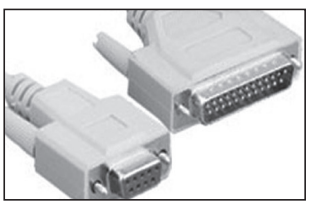


Figura 4.11. *Interfaz EIA-232 con conectores DB-25 y DB-9.*

4.3.4 EJEMPLO DE COMUNICACIÓN ENTRE UN DTE Y UN DCE

A continuación se mostrará una temporización típica utilizada para la comunicación entre un DTE y un DCE cuando el DCE es un módem y se desea transmitir datos al DCE remoto. El proceso se puede dividir en tres fases:

Fase 1:

Conexión DTE-DCE preparada. La primera fase se utiliza para comprobar que los dispositivos DTE y DCE están operativos:

1. El DTE activa la señal DTR (DTE listo).
2. El DCE activa la señal DSR (DCE listo).

Fase 2:

Establecimiento de la conexión DTE-DTE y transferencia de datos:

3. El DTE activa la señal RTS (Petición para enviar) para solicitar el envío de datos al módem.

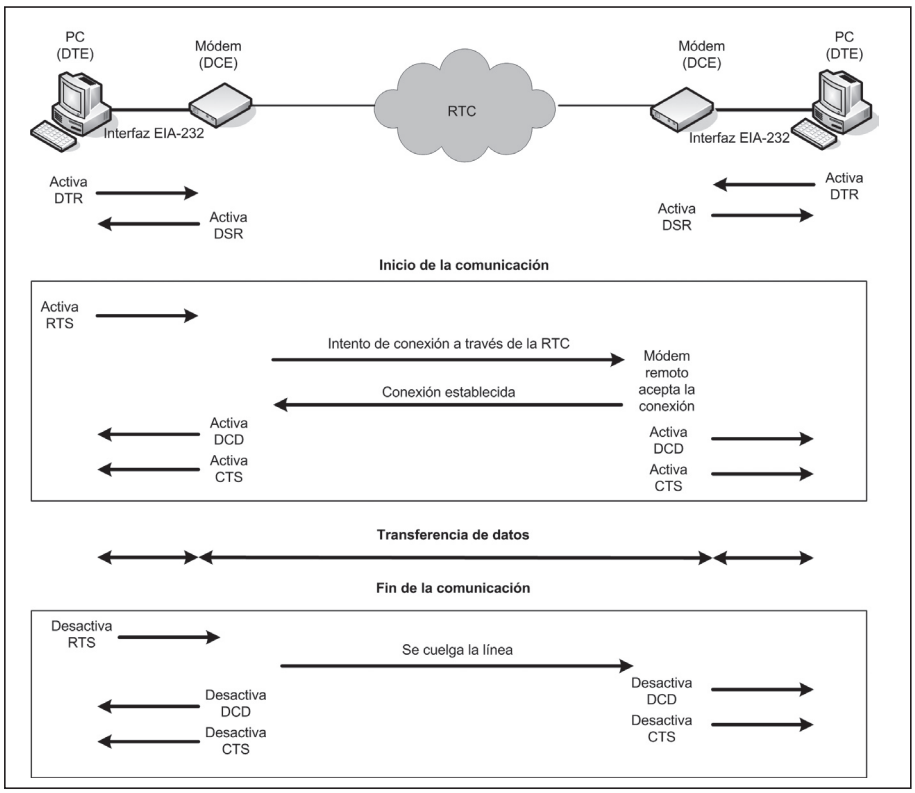


Figura 4.12. *Temporización entre módems remotos.*

4. El módem realiza la conexión con el módem remoto.
5. Cuando el módem remoto acepta la comunicación se activa la señal DCD (Detector de portadora) para indicar que la conexión ha sido establecida.
6. El DCE activa la señal CTS (Listo para enviar) para indicar al DTE que ya está listo para enviar datos.
7. Se lleva a cabo la transferencia de datos por las líneas de transmisión y recepción.

Fase 3:

Finalización de la conexión:

8. El DTE desactiva la señal RTS para indicar que se desea finalizar la conexión.
9. El módem cuelga la línea, desactiva la señal DCD y a continuación desactiva CTS.

4.4 CABLE MÓDEM NULO

Aunque el estándar EIA-232 / V.24 se diseñó para la comunicación entre un DTE y un DCE, también se utiliza para conectar dos DTE directamente sin necesidad de utilizar DCE. Por ejemplo, para conectar dos ordenadores ubicados en la misma sala no sería necesario transmitir los datos a través de la red telefónica por medio de la utilización de módems (DCE), para ello bastaría con unirlos mediante un cable serie.

Este cable serie que sigue las especificaciones de la interfaz EIA-232 se conoce como cable módem nulo. La diferencia entre un cable módem nulo y un cable

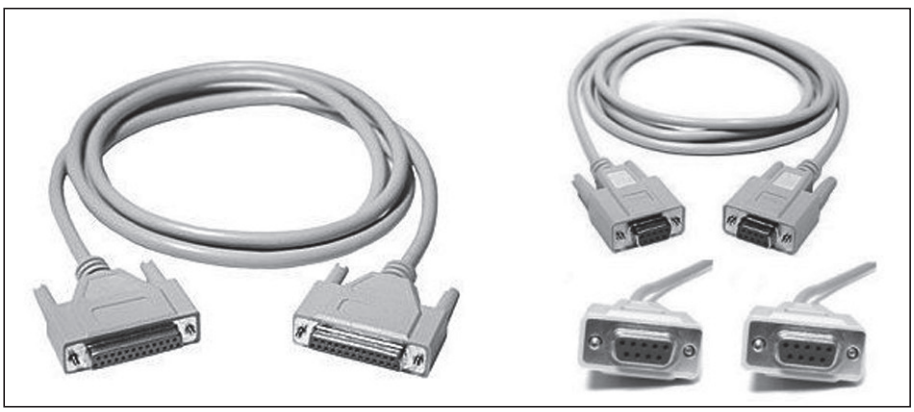


Figura 4.13. *Cable módem nulo con conectores DB-25 y DB-9.*

EIA-232 es que las conexiones de datos y control deben estar cruzadas y los conectores deben ajustarse para que se pueda conectar a dos DTE.

Existen varias combinaciones posibles entre DB-9 y DB-25. Para la conexión de dos ordenadores, la combinación más utilizada es la formada por dos conectores DB-9 hembra ya que la mayor parte de los ordenadores proporcionan un puerto de comunicaciones serie con un conector macho de nueve pines.

Tabla 4.3 Asignación de pines en los conectores de un cable módem nulo

Conector 1			Conector 2		
nº DB-9	nº DB-25	Nombre	nº DB-9	nº DB-25	Nombre
-	1	Protección a tierra	-	1	Protección a tierra
3	2	TD	2	3	TD
2	3	RD	3	2	RD
7	4	RTS	8	5	CTS
8	5	CTS	7	4	RTS
5	7	GND	5	7	GND
6	6	DSR	4	20	DTR
1	8	DCD	4	20	DTR
4	20	DTR	1	8	DCD
4	20	DTR	6	6	DSR

A continuación se presenta la tabla de conexiones de un cable módem nulo teniendo en cuenta los dos tipos de conectores que se pueden utilizar:

En la siguiente tabla se resumen las principales configuraciones de cables serie que se pueden utilizar:

Tabla 4.4 Resumen de las principales configuraciones de cables serie

	Terminal 1		Terminal 2		
Tipo cable	Conector	Equipo	Conector	Equipo	Observaciones
Conexión DTE-DCE	DB-9 hembra	DTE	DB-9 macho	DCE	EIA-232 BD-9
Conexión DTE-DTE	DB-25 hembra	DTE	DB-25 macho	DCE	EIA-232 DB-25
Conexión DTE-DCE	DB-9 hembra	DTE	DB-25 macho	DCE	
Cable módem nulo	DB-25 hembra	DTE	DB-25 hembra	DTE	
Cable módem nulo	DB-9 hembra	DTE	DB-9 hembra	DTE	El más común de cable módem nulo

4.5 OTRAS INTERFACES SERIE

Las interfaces serie presentadas a continuación son utilizadas normalmente para la conexión de módems (DCE) con equipos de interconexión de redes o routers que hacen la función de DTE.

4.5.1 INTERFAZ V.35

La recomendación V.35 define las características eléctricas de una interfaz serie para la conexión de un DTE a un DCE. Las características funcionales para las interfaces V.35 suelen utilizar las de la recomendación V.24 vista anteriormente.

Las características mecánicas están definidas en la norma ISO 2593 en la que se especifica la utilización de un conector de 34 pines conocido como conector Winchester.

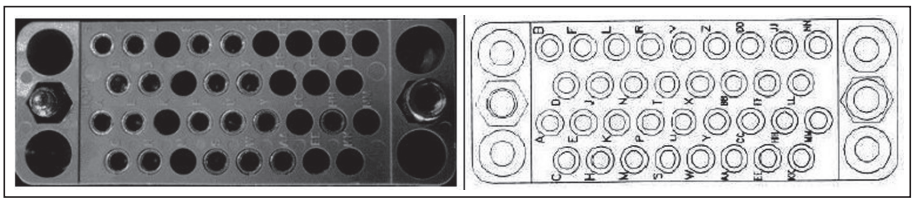


Figura 4.14. *Conector V.35 hembra de 34 pines.*

Esta norma actualmente se considera obsoleta y está sustituida por las recomendaciones V.36 y V.37, sin embargo en la práctica todavía se usa para proporcionar una interfaz a equipos de comunicaciones para conexiones a líneas punto a punto y a redes WAN. Aunque la recomendación inicial especifica velocidades de transmisión de datos de 48 Kbps hasta 64 Kbps, la interfaz V.24/V.35 se utiliza para velocidades de hasta 2 Mbps

Figura 4.15. *Conector V.35.*

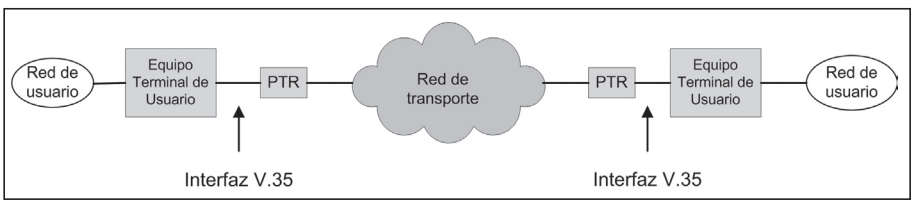


Figura 4.16. *Típico uso de la interfaz V.35 para la conexión a una red WAN.*

4.5.2 INTERFACES V.10 Y V.11

La **recomendación V.10** define las características eléctricas de los circuitos de enlace asimétricos (desbalanceados) para transmisión de datos de hasta 100 Kbps. Se puede aumentar la distancia reduciendo la velocidad de transmisión según la gráfica especificada en la recomendación.

Como se observa, la distancia que se puede alcanzar con este tipo de interfaz es de hasta 50 metros a 20 Kbps o la máxima de 100 Kbps con una distancia de 10 metros.

Las características mecánicas de la interfaz V.10 y la asignación de los pines se incluyen en la norma ISO 4902 donde se utilizan dos conectores DB-37 y DB-9 en cada extremo, de 37 y 9 patillas respectivamente, o la norma ISO 4903 donde se utiliza un conector DB-15.

La recomendación V.10, utilizando la norma ISO 4902 para los conectores, está especificada por la EIA en el mercado norteamericano como RS-423.

La **recomendación V.11** define las características eléctricas de los circuitos de enlace simétricos (balanceados) para transmisión de datos de hasta 10 Mbps. Como se observa, el aumento de la velocidad respecto a la V.10 se debe al uso de líneas balanceadas que proporcionan mayor inmunidad al ruido.

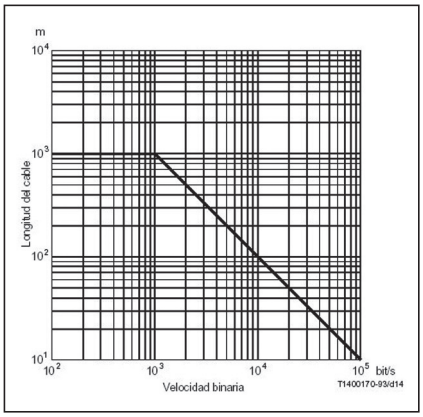


Figura 4.17. *Velocidad de transmisión en función de la distancia para una interfaz V.10.*

Figura 4.18. *Conector de la interfaz V.10 de 37 pines.*

Al igual que en la interfaz V.10, se puede aumentar la distancia disminuyendo la velocidad de conexión. La distancia que se puede alcanzar con este tipo de interfaz es de 1.000 metros con una velocidad de 100 Kbps, 50 metros a 2 Mbps o la velocidad máxima de 10 Mbps con una distancia de 10 metros.

Al igual que la interfaz V.10, las características mecánicas y asignación de pines se especifican en las normas ISO 4902 para el conector de 37 pines o ISO 4903 para el conector de 15 pines.

La recomendación V.11, utilizando la norma ISO 4902 para los conectores, está especificada por la EIA en el mercado norteamericano como RS-422.

4.5.3 INTERFAZ EIA-449

Estándar desarrollado por la EIA como sustituto de la interfaz EIA-232. También se le conoce como interfaz RS-449. En esta interfaz se especifican los aspectos funcionales y mecánicos.

Las características funcionales se corresponden con las recomendaciones de la ITU-T V.36 para velocidades de hasta 72 Kbps y V.37 para velocidades superiores a 72 Kbps.

Las características mecánicas se corresponden con la norma ISO 4902, es decir, se utilizan dos conectores en cada extremo DB-37 y DB-9.

Las características eléctricas se especifican en la norma RS-423 que, como se ha visto, se corresponde a la recomendación V.10 para circuitos no balanceados, y la norma RS-422 que se corresponde con la recomendación V.11 para circuitos balanceados, alcanzando para esta última velocidades de hasta 10 Mbps.

4.5.4 INTERFAZ X.21

Interfaz estándar diseñado por la ITU-T con las siguientes características:

- ✓ Se elimina una gran parte de las líneas de control de las conexiones EIA. La información de control se envía codificada por las líneas de datos.
- ✓ Velocidad de transmisión máxima de 64 Kbps.
- ✓ Se utiliza como nivel físico del estándar X.25 (arquitectura de red de área extensa de conmutación de paquetes).
- ✓ Conector BD-15, donde normalmente se usan sólo ocho de los conductores.

Figura 4.19. *Conector DB-15 para X.21.*

4.6 INTERFAZ CENTRONICS

La interfaz paralela Centronics fue desarrollada inicialmente para la conexión de una impresora a un PC. La primera especificación de esta interfaz paralela fue realizada por la empresa Centronics (nombre con el que también es conocido este puerto).

Es un puerto unidireccional, que trabaja con 8 bits en paralelo. Las velocidades de transferencia que utiliza son de 50 a 500 Kbps.

La interfaz Centronics utiliza un conector de 36 pines llamado Centronics para la impresora y un conector DB-25 igual que el del puerto serie pero hembra (puerto de 25 pines macho en el PC).

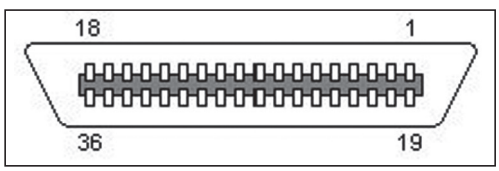


Figura 4.20. *Esquema de pines del conector Centronics .*

Actualmente esta implementación del puerto paralelo se conoce también como **SPP (*Standard Parallel Port*)**. En la tabla siguiente se muestran las funciones de los pines de un conector DB-25 de un puerto paralelo:

Tabla 4.5 Funciones de los pines del conector DB-25 en la interfaz Centronics

Pin	Nombre	Dirección	Descripción
1	/STROBE	Salida	Esta señal se activa cuando se quiere enviar datos a la impresora
2	D0	Salida	Línea de datos
3	D1	Salida	Línea de datos
4	D2	Salida	Línea de datos
5	D3	Salida	Línea de datos
6	D4	Salida	Línea de datos
7	D5	Salida	Línea de datos
8	D6	Salida	Línea de datos
9	D7	Salida	Línea de datos
10	/ACK	Entrada	Esta señal se activa cuando la impresora ha recibido correctamente los datos
11	BUSY	Entrada	Esta señal se activa cuando la impresora está ocupada y no puede aceptar datos
12	PE	Entrada	Indica que la impresora no tiene papel
13	SEL	Entrada	Esta señal indica que la impresora está preparada para imprimir
14	/AUTOFD	Salida	Cuando se activa esta señal, la impresora inserta una línea por cada retorno de carro
15	/ERROR	Entrada	Indica que existe una condición de error
16	/INIT	Salida	Esta señal se activa para reiniciar la impresora
17	/SELIN	Salida	Esta señal se activa para seleccionar la impresora
18	GND		GND de la señal de STROBE
19	GND		GND de las señales D0 y D1
20	GND		GND de las señales D2 y D3
21	GND		GND de las señales D4 y D5
22	GND		GND de las señales D6 y D7
23	GND		GND de la señal de BUSY
24	GND		GND para /ACK, PE y SEL
25	GND		GND para /AUTOFD, /SELIN y /INIT

Aunque la interfaz Centronics ofrecía una solución de conectividad entre ordenadores y periféricos a través de un puerto paralelo, dicha interfaz tenía algunos inconvenientes. No había un estándar que definiese las características eléctricas de la interfaz lo que podía ocasionar incompatibilidades entre equipos. Además el hecho de que fuese una interfaz unidireccional limitaba su uso para otros tipos de dispositivos.

Para superar estas limitaciones, en 1991 un grupo de empresas fabricantes de impresoras y productos de red se asocian en el llamado ***Network Printing Alliance*** y se

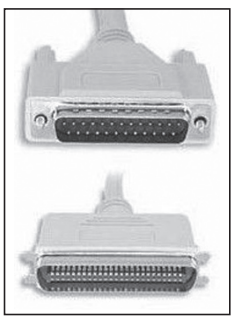


Figura 4.21. *Conectores de la interfaz Centronics.*

desarrolla la especificación **EPP (*Enhanced Parallel Port*)**. En esta especificación, la transferencia de datos puede ser bidireccional y se aumenta la velocidad, aunque se mantiene la compatibilidad con el modo SPP (Centronics). De esta forma se puede emplear el puerto paralelo para conectar otros dispositivos como escáner, discos duros, CD-ROM…

Posteriormente, en 1992, se desarrolló la especificación **ECP (*Extended Capabilities Port*)** que también proporciona comunicación de datos bidireccionales a través del puerto paralelo a alta velocidad; tanto ECP como EPP alcanzan hasta 2 Mbytes/s.

En 1994 las especificaciones ECP y EPP se recogen en el estándar IEEE 1284. Lógicamente las funciones de los pines de las interfaces EPP y ECP son diferentes que en la norma Centronics original.

Por tanto, actualmente existen tres modos de transferencia de datos a través del puerto paralelo de un PC:

- **SPP (*Standard Parallel Port*)** o Centronics. Modo unidireccional a baja velocidad. Utilizado para impresoras antiguas.
- **EPP (*Enhanced Parallel Port*).** Modo bidireccional de alta velocidad utilizado para dispositivos que no son impresoras como lectores de CD-ROM, discos duros…
- **ECP (*Extended Capabilities Port*).** Modo bidireccional de alta velocidad utilizado por impresoras y escáner recientes.

4.7 INTERFAZ USB

USB (*Universal Serial Bus*, Bus Serie Universal) es un estándar para la interconexión de periféricos a un ordenador a través de una interfaz serie. Los principales objetivos perseguidos al diseñar este estándar fueron:

- ✓ Admitir de forma sencilla la conexión de diferentes periféricos.
- ✓ Bajo coste y velocidades altas de transferencia de datos.
- ✓ Protocolos flexibles a los diferentes tipos de comunicación.

La primera especificación, llamada USB 1.0 se publicó en enero de 1996. La siguiente versión importante, USB 1.1, se lanzó en septiembre de 1998 y la última versión desarrollada ha sido la USB 2.0 con fecha de abril de 2000.

En el estándar USB se especifican tanto el nivel físico como el nivel de enlace de la interfaz.

Figura 4.22. *Diferentes logotipos para la interfaz USB.*

4.7.1 CABLES Y CONECTORES

La interfaz USB utiliza cables compuestos por cuatro conductores, dos para datos (llamados D+ y D-) y dos para alimentación (Vcc y GND). Los conductores son apantallados para transmisiones de alta velocidad y no apantallados para baja velocidad. Los conductores de alimentación se utilizan para proporcionar corriente eléctrica de alimentación a los dispositivos USB conectados a un bus. La alimentación máxima es de 500 mA por bus.

La longitud de cable máxima para USB 1.0 es de 3 metros y para las versiones USB 1.1 y USB 2.0 es de 5 metros.

Hay tres tipos de conectores: Tipo A, tipo B y tipo mini-B.

Conectores Tipo A

En las figuras se muestran el conector y el receptáculo Tipo A. El conector se utiliza para conectar el cable proveniente del dispositivo USB al host (ordenador). El receptáculo se corresponde con el puerto USB proporcionado por el host.

Figura 4.23. *Conector y receptáculo de tipo A.*

Conectores Tipo B

En las figuras se muestran el conector y el receptáculo Tipo B. Este conector se utiliza para conectar un cable USB a un dispositivo USB. El receptáculo se corresponde con el puerto USB proporcionado por el dispositivo periférico.

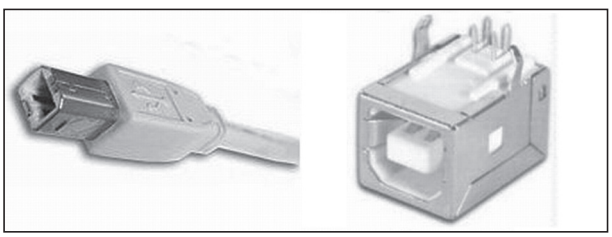


Figura 4.24. *Conector y receptáculo de tipo B.*

Conectores Tipo mini-B

Este tipo de conector se especificó para obtener un ahorro de espacio para periféricos de pequeño tamaño. Al igual que el conector B, el mini-B se utiliza

para conectar un cable USB al periférico. El receptáculo se corresponde con el puerto USB proporcionado por el dispositivo periférico.

La velocidad de transmisión por la interfaz USB depende de la versión utilizada:

- USB 1.0: 1'5 Mbps
- USB 1.1: 12 Mbps
- USB 2.0: 480 Mbps

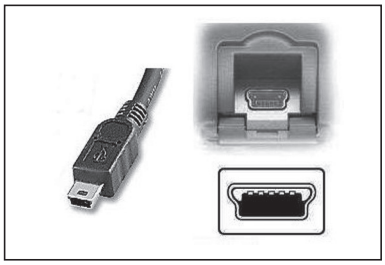


Figura 4.25. *Conector y receptáculo de tipo mini-B.*

Como se observa, la versión 2.0 ha supuesto un importante salto en la velocidad de transmisión. Se ofrece total compatibilidad hacia versiones anteriores de forma que se puede conectar un dispositivo USB 1.0 a un puerto 2.0 sin ningún problema aunque lógicamente la velocidad será la proporcionada por el dispositivo, es decir, 1'5 Mbps.

Se utiliza codificación NRZ-I, donde el *uno lógico* se codifica sin cambio de nivel y el *cero lógico* se codifica con un cambio de nivel.

Algunos ordenadores sólo incorporan puertos USB como interfaz serie aunque en el mercado existen conversores de USB a EIA-232 de nueve pines:

Figura 4.26. *Conversor USB – Puerto serie DB-9.*

4.7.2 ARQUITECTURA

La comunicación a través del bus USB emplea una topología llamada de estrellas apiladas o árbol con las siguientes características:

- ✓ El controlador anfitrión controla todo el tráfico que circula por el bus.
- ✓ Esta topología permite a varios dispositivos conectarse a un único bus lógico.
- ✓ Permite la conexión de hasta 127 dispositivos a un único puerto USB del PC.
- ✓ Es Plug&Play, es decir, permite la conexión de dispositivos "en caliente" sin tener que reiniciar el sistema.

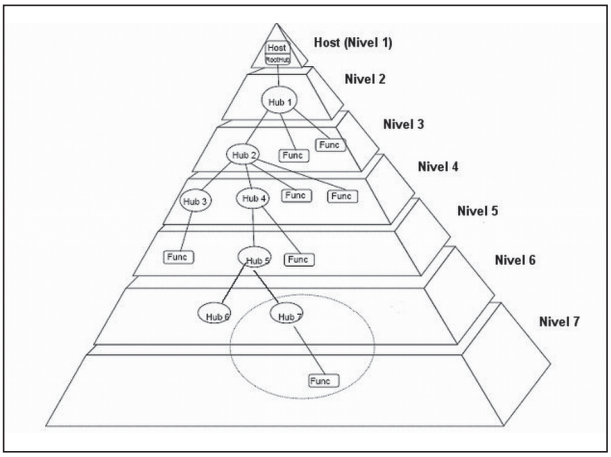


Figura 4.27. *Topología en árbol del bus USB.*

El bus USB implementa un nivel de enlace con las siguientes características:

- ✓ El control de flujo se lleva a cabo por sondeo desde el host.
- ✓ El control de acceso al medio se basa en el paso de testigo o "token".
- ✓ El controlador de bus distribuye el testigo por el bus.
- ✓ El dispositivo cuya dirección coincide con la del testigo responde aceptando o enviando datos al controlador.
- ✓ Los datos se envían divididos en tramas llevándose a cabo un control de errores por trama a través de un código CRC.

Como se ha visto, la interfaz USB no tiene líneas de control como ocurre con las interfaces serie anteriores, por tanto, se utilizan las líneas de datos para enviar tanto datos como información de control lo que complica la lógica de gestión del bus USB.

4.7.3 COMPONENTES DE UN SISTEMA USB

Como se ha visto en el apartado anterior, el bus USB está compuesto por tres tipos de elementos. En primer lugar aparece el controlador, que es el componente raíz de la arquitectura en árbol. En segundo lugar se pueden apreciar los concentradores o hubs, que se utilizan para crear ramificaciones de las estructuras en árbol del sistema USB, y por último están los dispositivos USB. A continuación se describen las principales funciones y características de cada uno de estos elementos:

- Controlador o host
  - Reside dentro del PC.
  - Es el responsable de la comunicación entre los periféricos USB y el PC.

- Detecta las conexiones y desconexiones de los dispositivos.
- Realiza la admisión de los periféricos. Para ello determina su tipo, les asigna recursos del sistema y una dirección lógica.
- Detecta errores y los comunica al PC.

■ Concentradores o hubs
- Son distribuidores inteligentes de datos y alimentación para los dispositivos conectados a ellos.
- Cada bus USB debe tener al menos un concentrador llamado concentrador raíz y que aparece en la figura 4.28 en el nivel 2. Este controlador raíz está implementado en el interior del PC.

Figura 4.28. *Hub USB.*

■ Periféricos
- Pueden ser de baja, media o alta velocidad al igual que las velocidades que admiten las distintas versiones de USB.
- Ejemplos de dispositivos de baja velocidad: teclados, ratones, joysticks...
- Ejemplos de dispositivos de media y alta velocidad: impresoras, módems, escáneres, discos duros...

4.8 INTERFACES INALÁMBRICAS: BLUETOOTH E INFRARROJOS

4.8.1 BLUETOOTH

Bluetooth es la definición de una especificación de interconexión inalámbrica de dispositivos utilizando señales de radiofrecuencia. Actualmente su uso está ampliamente extendido a todo tipo de dispositivos como ordenadores, teléfonos móviles, agendas electrónicas, impresoras, cámaras digitales… La primera especificación de Bluetooth es del año 1994 y fue desarrollada

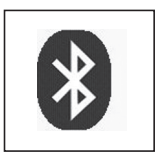


Figura 4.29. *Logotipo de Bluetooth.*

por un grupo de empresas englobadas en el llamado SIG (*Special Interest Group*) entre las cuales se encuentran Intel, Microsoft, IBM, Nokia, Motorola, Toshiba y Ericsson. También se ha incluido como estándar en la organización IEEE con el código IEEE 802.15.1.

Las transmisiones se efectúan utilizando señales de radiofrecuencia en la banda libre de 2'40 a 2'48 GHz. Para evitar interferencia con otras emisiones en esta misma banda de frecuencias, Bluetooth divide la banda en 79 canales, cada uno de ellos de 1 MHz, y realiza las transmisiones realizando saltos entre estos canales. A esta técnica se le conoce como FHSS (Espectro expandido por salto de frecuencia) y pueden llevarse a cabo hasta 1600 saltos de frecuencia por segundo. La velocidad alcanzada para la versión 1 es de 720 Kbps en modo asimétrico con 56,7 Kbps de velocidad en el canal de retorno. Para la versión 2 se alcanzan velocidades de 2 Mbps.

El radio de alcance de un dispositivo Bluetooth depende de la potencia con la que se transmite la señal de radiofrecuencia. Para ello se han definido tres clases de dispositivos:

- ✓ **Clase 1.** Con una potencia máxima de 100 mW y un alcance de hasta 100 metros.
- ✓ **Clase 2.** Con una potencia máxima de 2'5 mW y un alcance de hasta 10 metros.
- ✓ **Clase 3.** Con una potencia máxima de 1 mW y un alcance de hasta 1 metro.

Estas distancias se toman libres de obstáculos, con lo que en la práctica pueden ser sensiblemente inferiores.

Se pueden comunicar hasta ocho dispositivos formando una red. Uno de los dispositivos Bluetooth actúa de master y controla las comunicaciones entre el resto de dispositivos clientes, por tanto, cuando dos dispositivos cliente se quieren comunicar, lo hacen a través del dispositivo master. En las comunicaciones entre dos dispositivos Bluetooth, uno de ellos toma las funciones de master y el otro de cliente.

Figura 4.30. *Interfaz Bluetooth para su conexión a un PC a través de un puerto USB.*

4.8.2 INFRARROJOS

Por último, mencionar otro tipo de comunicación inalámbrica a través de emisiones de luz en la banda de los infrarrojos. El estándar de transferencia de datos por infrarrojos más popular actualmente es el desarrollado por la asociación conocida como **IrDA (*InfraRed Data Association*)** y que está formada por un grupo de empresas entre las que se encuentran HP, IBM y Sharp. Esta tecnología de

infrarrojos es la misma que la utilizada en muchos dispositivos de control remoto como mandos a distancia, pero optimizada para la transmisión de datos.

Al igual que Bluetooth, este tipo de comunicación se puede utilizar por diferentes tipos de dispositivos como ordenadores, teléfonos móviles, agendas electrónicas…

La transferencia de información se basa en la utilización como emisor de un diodo que transmite una señal de luz infrarroja modulada a una frecuencia de 35-40 KHz y un receptor que incluye un sensor fotoeléctrico. Las ventajas que ofrecen las comunicaciones por infrarrojos es que no están reguladas, son de bajo coste e inmunes a las interferencias de los sistemas de radio de alta frecuencia.

Figura 4.31. *Interfaz IrDA para su conexión a un PC a través de un puerto USB.*

Sin embargo, tiene algunos inconvenientes como su corto alcance o que para que la comunicación sea posible es necesario contacto visual con un ángulo entre los dos dispositivos no inferior a 15º.

Este tipo de comunicaciones se utiliza sólo para enlaces punto a punto, es decir, entre dos dispositivos. La distancia entre los dispositivos debe ser inferior a 1 metro y el rango de velocidades admitidas va desde 2'4 Kbps hasta 16 Mbps.

4.9 PRÁCTICA

El objetivo de esta práctica es conocer el funcionamiento de diferentes tipos de interfaces vistos en el capítulo.

4.9.1 MATERIAL NECESARIO POR GRUPO DE TRABAJO

- ✓ 2 PC con Windows 98/2000/XP y con puertos serie DB9, paralelo y USB
- ✓ 2 Conectores DB-9 hembra
- ✓ 1 Cable de pares o cable Ethernet
- ✓ 1 Cable módem nulo DB-9
- ✓ 1 Cable paralelo DB-25 – DB-25 macho
- ✓ 1 Cable USB para conexión PC-PC
- ✓ 1 Programa para generar fichero de prueba (incluido en el CD-ROM)
- ✓ 2 Adaptadores Bluetooth conectados por USB
- ✓ 2 Adaptadores de infrarrojos conectados por USB
- ✓ 1 Software de comunicaciones. Por ejemplo LapLink de Travelling Software

4.9.2 DESARROLLO DE LA PRÁCTICA

1. Construir un cable módem nulo utilizando dos conectores DB-9 hembra y cable de pares o cable Ethernet que incluye cuatro pares.
2. Instalar un software de comunicaciones en los PC, por ejemplo, LapLink de Travelling Software.
3. Conectar dos equipos utilizando el cable módem nulo y el software LapLink. Describir el proceso de configuración. Comprobar y describir las funcionalidades permitidas en este tipo de conexión.

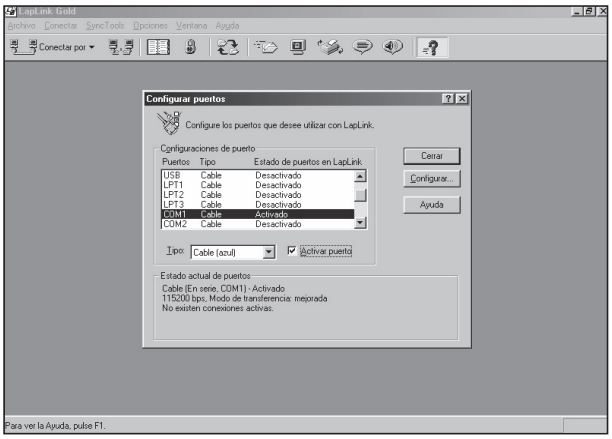


Figura 4.32. *Ventana de configuración de puertos en el software LapLink.*

4. Medir la velocidad de la conexión transfiriendo ficheros con tamaños conocidos y midiendo los tiempos. Generar ficheros de prueba con el tamaño deseado con el programa incluido en el CD-ROM (se ejecuta desde la consola de comandos).

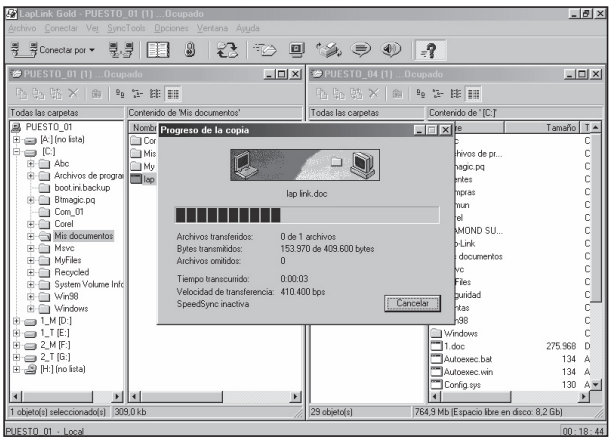


Figura 4.33. *Transferencia de ficheros a través de un cable serie utilizando el software LapLink.*

5 Conectar dos equipos utilizando un cable paralelo y la herramienta de Windows 98 "Conexión directa por cable" o el "Asistente para conexión nueva" de Windows XP. Comprobar y describir las funcionalidades permitidas por esta herramienta.

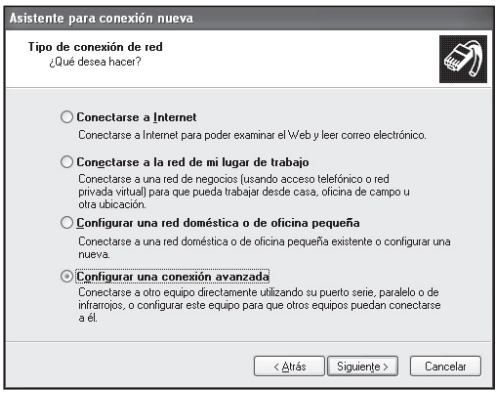


Figura 4.34. *Asistente para conexión nueva de Windows XP.*

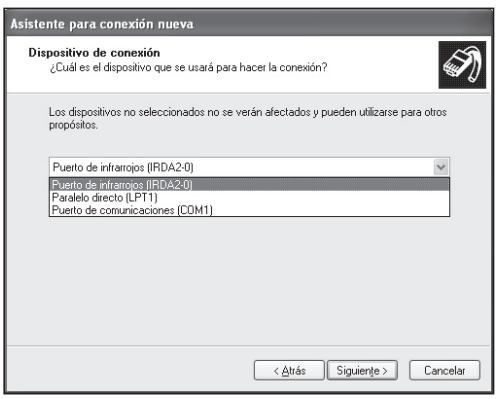


Figura 4.35. *Elección del puerto de comunicaciones desde el asistente de Windows XP.*

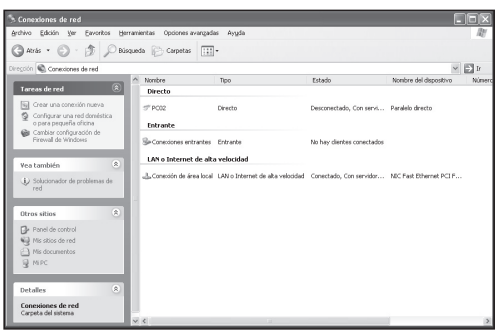


Figura 4.36. *Ventana de conexiones de red en Windows XP con dos conexiones serie configuradas, una como Host y otra como Invitado.*

6 Utilizando el mismo procedimiento que en el apartado 4, medir la velocidad de la conexión del cable paralelo.

7 Repetir el apartado 3 pero utilizando un cable USB para conexión PC-PC. Medir la velocidad de la conexión con el mismo procedimiento que el del apartado 4.

8 Buscar información sobre el puerto de comunicación Firewire, velocidades, dispositivos, patillaje, protocolo utilizado, etc. Incluir en la memoria los URL de las páginas web consultadas.

4.9.3 APARTADOS OPCIONALES

9 Instalar el adaptador Bluetooth en dos PC. Para ello será necesario instalar el software incluido normalmente con el dispositivo. Describir el proceso de configuración. Comprobar y describir las funcionalidades permitidas en este tipo de conexión. Medir la velocidad de la conexión con el mismo procedimiento que el del apartado 4.

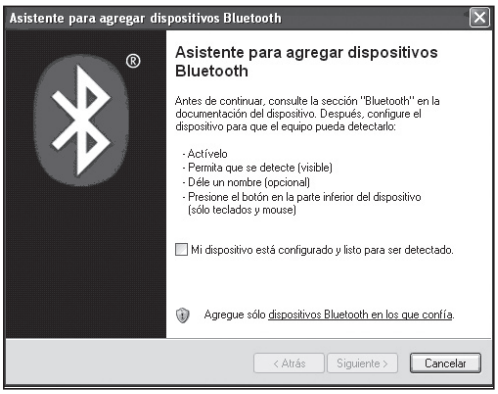


Figura 4.37. *Asistente para configurar una conexión Bluetooth en Windows XP.*

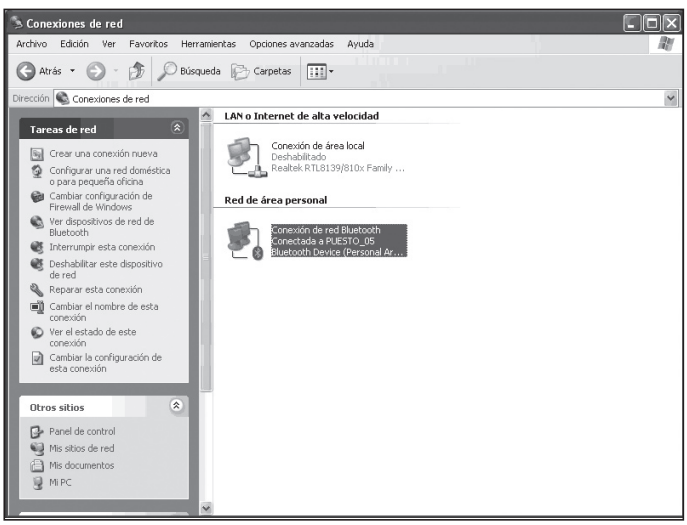


Figura 4.38. *Ventana de conexiones de red en Windows XP con una conexión Bluetooth configurada.*

10 Repetir el apartado anterior pero con el adaptador de infrarrojos.

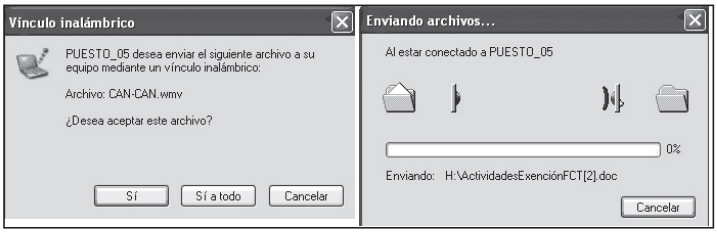


Figura 4.39. *Uso de una conexión de infrarrojos desde Windows XP.*

RESUMEN DEL CAPÍTULO

En este capítulo se presenta uno de los tipos de comunicación más simples dentro de los sistemas telemáticos como es la comunicación directa entre dos dispositivos.

Se establecen primero algunos conceptos fundamentales en la transmisión de datos digitales como las diferencias entre transmisión serie y paralelo. Y dentro de la transmisión serie, sus dos variantes: síncrona y asíncrona. Además se presenta la configuración más genérica donde se utilizan los tipos de comunicación que se estudiarán en este capítulo, la interfaz DTE-DCE.

La primera interfaz que se presenta, la interfaz EIA-232 (o RS-232) ha sido una de las más utilizadas a lo largo de sus más de 40 años de historia. Es una interfaz serie utilizada normalmente para comunicar un DTE con un DCE. Se estudian los aspectos mecánicos, eléctricos y funcionales también definidos a través de las normas de la ITU-T, V.24 y V.28. También se incluye el llamado cable módem nulo, basado en el estándar EIA-232 pero utilizado para unir directamente dos DTE.

Existen otras interfaces serie utilizadas en los sistemas telemáticos y que se presentan también en este capítulo, como son V.35, V10, V.11, EIA-449 y X.21.

Como interfaz paralela se incluye la interfaz Centronics diseñada originalmente para la comunicación entre un PC y un ordenador, aunque más tarde se extendió su uso a otros periféricos. Actualmente tiende a desaparecer siendo sustituida por la interfaz USB.

La interfaz USB se ha convertido en un estándar de conexión de periféricos a un PC y en este capítulo se estudian tanto sus aspectos mecánicos y eléctricos, como la arquitectura en la que se basa.

El capítulo concluye haciendo una breve descripción de las alternativas inalámbricas para la conexión directa de dos dispositivos: Bluetooth e infrarrojos.

EJERCICIOS PROPUESTOS

- **1.** Escribe una tabla con todos los estándares mencionados en el capítulo y el organismo que lo ha desarrollado.

- **2.** Se presenta una lista con dispositivos que pueden comunicarse con alguna de las interfaces vistas en este capítulo. Para cada uno de ellos especifique qué tipo de interfaz pueden utilizar y si su función es de DTE, DCE o no es aplicable.
  - ✓ Ordenador
  - ✓ Impresora
  - ✓ Módem
  - ✓ Router
  - ✓ Escáner
  - ✓ Disco duro externo

- **3.** Dibuje un esquema de las conexiones en un conector DB-9 para implementar un bucle local en un puerto serie de un PC, es decir, todo lo que se envíe a través del puerto se recibirá de nuevo.

- **4.** Dibuje un esquema de las conexiones en un conector DB-25 para implementar un bucle local en un puerto serie de un PC, es decir, todo lo que se envíe a través del puerto se recibirá de nuevo.

- **5.** Aunque en el apartado 4.4 del capítulo se presenta una tabla de conexionado de un cable módem nulo, existen otras alternativas más simples que no tienen en cuenta el control de flujo proporcionado por las señales de control. Dibuje el esquema de conexionado de dichas alternativas.

TEST DE CONOCIMIENTOS

1 Para transmitir grupos de 6 bits, en una transmisión serie son necesarios:
- **a)** Un canal.
- **b)** Seis canales.
- **c)** 12 canales.
- **d)** Depende del tipo de medio físico.

2 Las transmisiones asíncronas se caracterizan por:
- **a)** El envío de uno o varios bits de comienzo.
- **b)** El envío de uno o varios bits de parada.
- **c)** No hay sincronización entre emisor y receptor.
- **d)** Todas las anteriores son correctas.

3 En una comunicación por módem, un ordenador se considera:
- **a)** Un DTE.
- **b)** Un DCE.
- **c)** Depende del sistema.
- **d)** Ninguna de las anteriores es correcta.

4 El nivel de tensión y el tipo de codificación de la interfaz serie EIA-232 forman parte de las especificaciones:
- **a)** Mecánicas.
- **b)** Eléctricas.
- **c)** Funcionales.
- **d)** Ninguna de las anteriores.

5 En la implementación DB-25 de la interfaz EIA-232 la mayoría de los pines se utilizan para:
- **a)** Transmisión de datos.
- **b)** Señales de control y temporización.
- **c)** Señales de prueba.
- **d)** No tienen asignación.

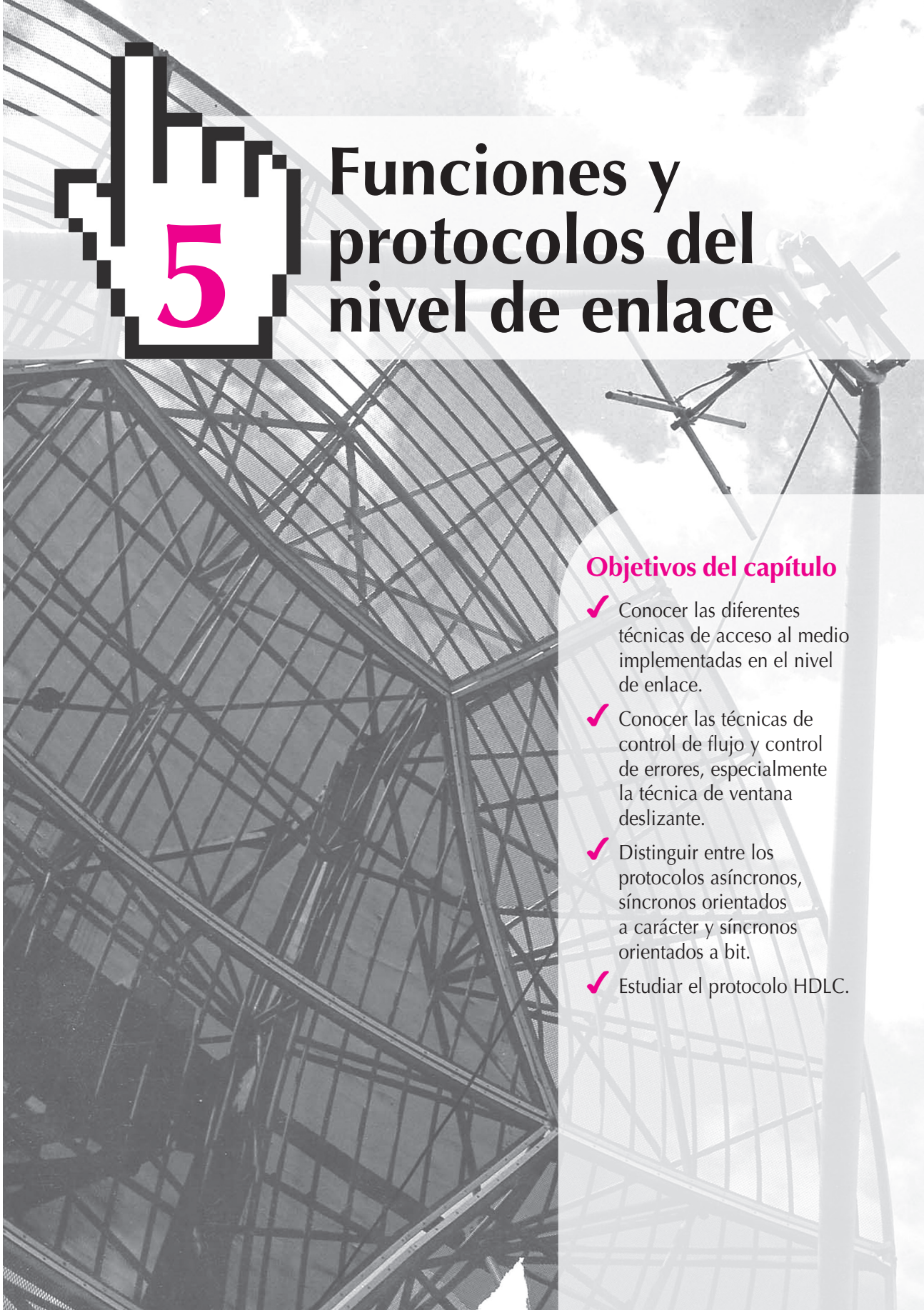
6 Para conectar dos DTE directamente se utiliza una interfaz:
- **a)** EIA-232.
- **b)** V.10.
- **c)** X.21.
- **d)** Cable módem nulo.

7 El conector de 34 pines se corresponde a la interfaz:
- **a)** V.10.
- **b)** V.11.
- **c)** V.34.
- **d)** V.35.

8 La diferencia entre USB 1.1 y 2.0 es:
- **a)** El tipo de conectores utilizados, tipo A para 1.1 y tipo B para 2.0.
- **b)** USB 1.1 no proporciona alimentación a los dispositivos y USB 2.0 sí.
- **c)** La velocidad máxima de transmisión es mayor en 2.0 que en 1.1.
- **d)** Todas las anteriores son correctas.

9 Los controladores USB:
- **a)** Asignan recursos a los dispositivos conectados al bus.
- **b)** Detectan la desconexión de los dispositivos.
- **c)** Detectan errores.
- **d)** Todas las anteriores son correctas.

10 Existen varias clases de dispositivos Bluetooth en función de la potencia de transmisión. Esta característica influye en:
- **a)** La compatibilidad con otras especificaciones, como IrDA.
- **b)** La velocidad de transmisión. A más potencia, más velocidad.
- **c)** En el radio de alcance. A más potencia, más alcance.
- **d)** En la habilitación de características avanzadas.



5 Funciones y protocolos del nivel de enlace

Objetivos del capítulo

- ✓ Conocer las diferentes técnicas de acceso al medio implementadas en el nivel de enlace.
- ✓ Conocer las técnicas de control de flujo y control de errores, especialmente la técnica de ventana deslizante.
- ✓ Distinguir entre los protocolos asíncronos, síncronos orientados a carácter y síncronos orientados a bit.
- ✓ Estudiar el protocolo HDLC.

5.1 INTRODUCCIÓN

Las funciones llevadas a cabo en el nivel físico sirven para transmitir información a través de un enlace, sin embargo, para que exista verdadera comunicación, es necesario implementar los mecanismos necesarios para que ese intercambio de información sea eficiente. Se pueden destacar tres funciones fundamentales que convierten la simple transmisión de bits a través de un medio físico en una verdadera comunicación:

- ✓ Control de acceso al medio
- ✓ Control de flujo
- ✓ Control de errores

Como se vio en el capítulo 3, estas tres funciones están englobadas en el nivel de enlace, por tanto, el estudio de las técnicas para llevar a cabo las funciones citadas es, en el fondo, el estudio del propio nivel de enlace.

5.2 FUNCIONES DEL NIVEL DE ENLACE

5.2.1 CONTROL DE ACCESO AL MEDIO

El control de acceso al medio se lleva a cabo cuando es necesaria una coordinación entre los dispositivos que se quieren comunicar, esencialmente para decidir cuándo hacer uso del medio de transmisión para transmitir los datos. En definitiva, se trata de controlar qué dispositivo puede acceder al medio de transmisión en un instante dado.

Recordemos que existen dos formas de enlazar o unir dispositivos para la transmisión de datos a través de un medio: mediante enlaces dedicados (o líneas punto a punto) y mediante enlaces multipunto. Lógicamente el control de acceso al medio en líneas multipunto toma especial relevancia siendo, de hecho, imprescindible la existencia de algún mecanismo que regule el uso de un enlace común a varios (o incluso muchos) dispositivos.

Para líneas dedicadas en las que el medio es compartido por sólo dos dispositivos, no suele ser necesario ningún control de acceso al medio, ya que normalmente se utilizan transmisiones full-dúplex, con lo cual cada dispositivo tiene un canal de comunicación independiente.

En estos casos sin embargo, puede ser necesario establecer algún mecanismo para controlar la disponibilidad del receptor. Cuando un dispositivo quiere transmitir, debe asegurarse de que el receptor está activo y preparado para aceptar sus datos. Una de las técnicas empleadas en este caso es la llamada **solicitud y reconocimiento**, usada tanto para comunicaciones full-dúplex como half-dúplex en líneas dedicadas.

El funcionamiento de esta técnica es sencillo. Cuando un dispositivo quiere transmitir datos, debe enviar primero una trama de control llamada **solicitud** (también llamada trama ENQ). Esta trama sirve para preguntar al receptor si está listo para recibir datos. El receptor debe responder con otra trama de control que indique respuesta afirmativa o negativa. Las tramas de respuesta afirmativa se conocen como tramas **ACK** (**reconocimiento**) y las tramas de respuesta negativa se conocen como tramas **NAK (no reconocimiento)**.

Si el emisor recibe una respuesta ACK comienza a transmitir tramas de datos. Normalmente, para cada trama de datos que se envía, el receptor manda una trama ACK para confirmar que la recepción se ha producido y se pueden seguir enviando datos. Cuando finaliza el envío de datos se envía una trama de control llamada **EOT (End Of Transmission, Fin de Transmisión)** para indicar que ya no se enviarán más datos.

Cuando la respuesta a una trama de solicitud es negativa, es decir, es una trama NAK, el emisor sabe que no puede enviar datos. En estos casos, normalmente se suelen hacer varios reintentos antes de abandonar la conexión.

A continuación se muestra un diagrama donde se representan dos ejemplos de transmisión utilizando la técnica de solicitud y reconocimiento. Este tipo de diagrama utilizado es muy útil para representar gráficamente la relación entre el emisor y el receptor de la transmisión. Los ejes verticales representan el tiempo y cada flecha entre el emisor y el receptor representa la transmisión de una trama, de datos o de control. La inclinación de la flecha representa el tiempo de propagación de la trama a través del medio de transmisión.

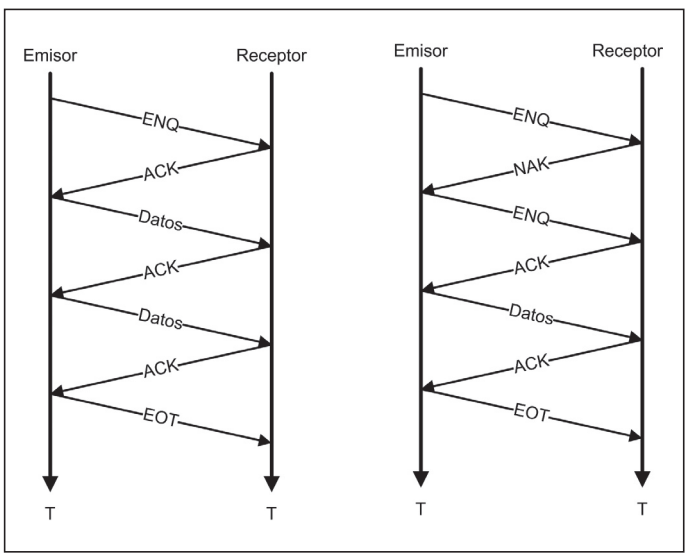


Figura 5.1. *Ejemplos de flujo de datos con la técnica de solicitud y reconocimiento.*

La técnica de solicitud y reconocimiento se utiliza esencialmente en líneas dedicadas o líneas punto a punto. Para líneas multipunto son necesarias técnicas que realmente aseguren un control de acceso al medio de transmisión que está compartido por varios dispositivos. Las técnicas utilizadas para ello son:

- ✓ Sondeo y selección
- ✓ Contienda
- ✓ Paso de testigo

Estas técnicas se estudian en los próximos apartados.

▪ 5.2.1.1 Sondeo y selección

La técnica de sondeo y selección se utiliza en enlaces multipunto, es decir, donde el medio está compartido por varios dispositivos, con configuraciones centralizadas, donde uno de los dispositivos ejerce de estación primaria o maestro, y el resto de dispositivos ejercen de estaciones secundarias o esclavos.

En este caso, el dispositivo maestro controla el enlace y todas las comunicaciones se llevan a cabo a través del mismo, incluso las comunicaciones entre dos dispositivos esclavos. Los dispositivos esclavos siguen las instrucciones del maestro.

Para utilizar esta técnica es necesario establecer un mecanismo de direccionamiento, es decir, cada dispositivo debe tener asignada una dirección que se usa para su identificación. Con la técnica de sondeo y selección se pueden producir dos tipos de comunicaciones:

Comunicación desde el maestro a un esclavo.

Se lleva a cabo mediante el **modo selección** en el que el dispositivo maestro envía una trama de selección, para verificar que el dispositivo destino está preparado para recibir los datos. Dicha trama debe contener la dirección del dispositivo esclavo al que se va a enviar los datos. Esta trama irá pasando por los diferentes dispositivos del enlace, cada uno de los cuales comprobará la dirección incluida en la trama hasta llegar al dispositivo destino, que responderá con una trama ACK si está preparado para aceptar los datos.

Comunicación entre un esclavo y el maestro.

En este caso se utiliza el **modo sondeo** en el que el dispositivo primario envía una trama de sondeo a cada dispositivo secundario. Esta trama se utiliza para preguntar a cada dispositivo secundario si tiene algo que enviar. En caso negativo el dispositivo secundario envía una trama NAK y en caso afirmativo, el dispositivo envía los datos que necesita enviar. La estación primaria responderá con una trama ACK para indicar que ha recibido los datos.

Como se observa, un dispositivo secundario no puede iniciar una comunicación sino que tiene que esperar a que el dispositivo primario le envíe una trama de sondeo para poder enviar sus datos.

Si el destino de los datos es otro dispositivo secundario, los datos son enviados al primario que es el que se encarga de dirigirlos al secundario correspondiente.

■ 5.2.1.2 Contienda

El método de **contienda** se utiliza en enlaces multipunto distribuidos en los que existen varios equipos conectados al mismo enlace y en los que no existen dispositivos que actúan como maestros.

En este caso, se trata de establecer un mecanismo de arbitraje para resolver el conflicto ocasionado cuando dos equipos quieren acceder al mismo tiempo al medio de transmisión.

Existen varias técnicas de contienda que se presentan a continuación:

ALOHA

Inicialmente desarrollado para radiotrasmisiones aunque aplicable a cualquier sistema en el que dispositivos no coordinados compiten por el uso de un solo canal compartido.

En esta técnica, los dispositivos transmiten cuando tengan algo que transmitir. El problema se produce si dos (o más) dispositivos intentan transmitir sus datos al mismo tiempo. Cuando esto ocurre, el resultado es la alteración de las señales eléctricas originales y la consiguiente pérdida de la información. Esta situación se denomina **colisión**.

NOTA 5.1

Una colisión se produce cuando dos dispositivos transmiten datos simultáneamente. Las señales se solapan y convierten dichas señales en ruido.

Para solucionar el problema de las colisiones, cuando un dispositivo transmite una trama debe escuchar el canal para comprobar si ha habido colisión. Básicamente esto consiste en comprobar que los niveles de tensión de las señales que se han propagado por el medio no han variado como consecuencia de una colisión.

Si se comprueba que ha habido una colisión, el dispositivo espera un tiempo aleatorio y vuelve a transmitir la trama. Es fundamental que el tiempo de espera sea aleatorio para asegurar que las transmisiones no vuelvan a coincidir y vuelvan a producir una colisión.

ALOHA ranurado (Slotted Aloha)

Esta técnica es una mejora de la ALOHA original. Su funcionamiento es igual que en ALOHA excepto que, en este caso, se divide el tiempo en intervalos discre-

tos correspondientes al tiempo de retransmisión de una trama, de forma que sólo se puede comenzar a transmitir una trama en el comienzo de un intervalo o ranura de tiempo. Si se produce colisión, se espera un número aleatorio de intervalos de tiempo discretos o ranuras para realizar la retransmisión.

Para poder sincronizar los diferentes dispositivos del sistema, uno de los dispositivos se puede encargar de emitir una señal especial para señalizar el comienzo de cada ranura.

CSMA persistente (Carrier Sense Multiple Access, Acceso Múltiple por Detección de Portadora)

En esta técnica, cuando una estación quiere transmitir primero escucha, es decir, comprueba si hay datos propagándose por el medio. Si detecta que se están transmitiendo datos, es decir, que el canal está ocupado, espera a que se libere y entonces comienza su transmisión.

Si se produce una colisión, espera un tiempo aleatorio y vuelve a comenzar el proceso. De nuevo, la aplicación de esta técnica mejora el rendimiento respecto a ALOHA ranurado.

CSMA no persistente

En CSMA persistente se puede dar el caso de que dos dispositivos quieran transmitir una trama y el canal se encuentre ocupado. Cuando finalice la ocupación, los dos dispositivos que estaban esperando intentarán transmitir al mismo tiempo y se producirá una colisión que se resolverá con las respectivas retransmisiones.

Sin embargo la transmisión sería más eficiente si se pudiera evitar este tipo de colisión. Para ello, en CSMA no persistente, cuando el canal está ocupado, una estación no escucha continuamente para transmitir inmediatamente después de que el canal quede libre sino que cuando el canal está ocupado, se espera un tiempo aleatorio y se vuelve a comprobar si el canal está ocupado. Con este cambio se reduce el número de colisiones y por tanto se mejora la eficacia.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection, Acceso Múltiple por detección de portadora y con detección de colisiones)

Esta técnica es una evolución de la anterior en la que se añade otra característica que mejora la eficacia. Cuando un dispositivo comienza a transmitir una trama y detecta una colisión, finaliza inmediatamente de transmisión. Este comportamiento mejora el uso del canal sobre todo en aquellas colisiones que se producen en los primeros bits de la trama.

Por tanto, una vez que se detecta y finaliza la transmisión de la trama en curso, el dispositivo espera un tiempo aleatorio e intenta de nuevo la transmisión.

A continuación se presentan las principales características de CSMA/CD:

- ✓ Si el medio está libre, la estación transmite su trama.
- ✓ Si el medio está ocupado, la estación espera hasta que quede libre y transmite su trama.
- ✓ Mientras se transmite la trama se comprueba si se produce colisión.
- ✓ Si se detecta una colisión se deja de transmitir inmediatamente, se espera un tiempo aleatorio y se intenta transmitir de nuevo.

Solamente se comprueba si hay colisión mientras se transmite la trama, por lo que es importante que los sistemas que utilicen CSMA/CD estén correctamente diseñados para que no se produzcan colisiones después de que el transmisor deje de transmitir.

El principal campo de aplicación de CSMA/CD han sido las redes de área local (LAN) cableadas.

MACA (Multiple Access with Collision Avoidance, Acceso Múltiple con Prevención de Colisiones)

Este método se utiliza en redes LAN inalámbricas donde el método CSMA/CD no resulta adecuado, ya que no se puede asegurar la detección de colisiones en todas las estaciones que forman parte de la red debido a la naturaleza de las señales utilizadas en la transmisión, las señales radioeléctricas.

La técnica consiste en que cuando un dispositivo quiere enviar datos, primero envía una pequeña trama de solicitud (trama RTS). El dispositivo receptor contesta a esta trama con otra trama de respuesta (trama CTS). Tanto la trama RTS como CTS contienen el número de bytes que se transmitirán en la trama de datos. Por tanto, cualquier dispositivo que reciba las tramas RTS o CTS sabrá que se va a iniciar una comunicación y sabrá además cuanto va a durar la transmisión de los datos. Cuando finalice dicha transmisión, podrá enviar su trama de solicitud RTS.

La única posibilidad de producirse una colisión es cuando dos dispositivos envían tramas RTS simultáneamente. En este caso, se espera un tiempo aleatorio y se retransmite la trama de solicitud.

Se añadieron algunas mejoras a la técnica original MACA y al resultado se le denominó MACAW.

■ 5.2.1.3 Paso de testigo

Al igual que en el tipo anterior, se utiliza en enlaces multipunto distribuidos. Este método está basado en el uso de una trama de control llamada **testigo** (o token). Sólo la estación que tenga el testigo puede transmitir datos a través del enlace. Cuando finaliza su transmisión cede el testigo a la siguiente estación siguiendo un orden determinado.

Esta técnica se utiliza en redes de área local con topologías en anillo y se verá con más detalle en el próximo capítulo dedicado a redes de área local.

5.2.2 CONTROL DE FLUJO

El segundo aspecto que se necesita controlar en la gestión de un enlace de comunicación es el control de flujo, el cual es necesario para poder adaptar la velocidad de envío de datos con la velocidad de procesamiento de los datos en el receptor. El control de flujo es un conjunto de mecanismos que permiten saber al emisor cuando puede transmitir.

Hay que tener en cuenta que en muchas ocasiones, la velocidad de transmisión no está determinada por el ancho de banda de la línea de transmisión, es decir, la velocidad a la que el medio puede transmitir datos, sino que depende de la velocidad a la que los datos pueden ser procesados por el receptor. De esta forma, si los datos le llegan al receptor más rápido de lo que puede procesarlos, inevitablemente los datos se perderán. Podría pensarse en una solución basada en un buffer o memoria intermedia donde almacenar los datos hasta que el receptor los puede procesar. Pero esta solución sólo retrasaría el problema de la pérdida de información, ya que los buffers tienen una capacidad limitada.

Por ello se debe establecer un mecanismo para que el receptor pueda notificar al emisor cuándo puede enviar datos. Existen básicamente dos métodos: parada y espera, y ventana deslizante.

5.2.2.1 Parada y espera

En este método de control de flujo, el emisor envía una trama y espera el reconocimiento de la misma antes de enviar la siguiente, dicho reconocimiento se envía mediante una trama ACK. Este proceso se repite hasta que el emisor no tiene más datos y envía una trama EOT para indicar el final de la transmisión. Debido a que el método lleva implícita una alternancia en el flujo de los datos, se puede utilizar tanto en transmisiones half-dúplex como full-dúplex.

Este método tiene como principal ventaja su extremada sencillez pero tiene un gran inconveniente, que es su lentitud.

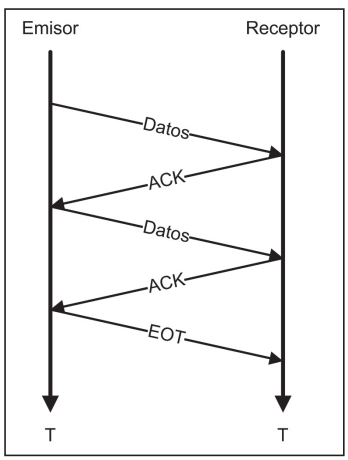


Figura 5.2. *Ejemplo de flujo de datos en la técnica de parada y espera.*

5.2.2.2 Ventana deslizante

En el método de ventana deslizante, a diferencia del de parada y espera, el emisor puede enviar varias tramas consecutivas antes de esperar por la confirmación de las mismas. Así mismo, el receptor puede enviar una sola confirmación para varias tramas de datos. Para implementar esta técnica es necesaria la existencia de buffers tanto en el emisor como en el receptor. Cada trama se numera con un número de secuencia.

El nombre completo de esta técnica sería "ventana deslizante de módulo n". El valor de *n* está directamente relacionado con el tamaño máximo de las ventanas de transmisión. Por ejemplo, la más común es la técnica de Ventana deslizante de módulo 8. Las tramas se numeran de 0 a n-1, y el tamaño máximo de la ventana es n-1. Para el ejemplo de ventana deslizante módulo 8, las tramas se numerarían de 0 a 7 y el tamaño máximo de la ventana es de siete tramas, uno menos del módulo. Esto es debido a que se pueden producir situaciones de ambigüedades que se resuelven reduciendo el tamaño máximo de la ventana.

Funcionamiento en el emisor

- En todo momento el emisor mantiene un grupo de números de secuencia que corresponde a las tramas que tiene permitido enviar. Ésta es la **ventana de emisión**.
- Inicialmente llenamos el buffer con todas las tramas que quepan, es decir, el tamaño máximo de la ventana. El tamaño máximo de la ventana se corresponde con el máximo número de tramas que pueden ser enviadas sin ser confirmadas. Si utilizamos ventana deslizante módulo 8, el tamaño máximo de la ventana será de 7. La ventana de emisión contendrá siete tramas y éstas se almacenan en el buffer.
- Cada vez que se envía una trama, la ventana de emisión se reduce "por la izquierda" una posición.
- Cada vez que llegue un asentimiento, la ventana de emisión se expande "por la derecha" tantas posiciones como tramas se confirmen en el asentimiento.
- El buffer contiene en todo momento las tramas que se pueden transmitir y las que están pendientes de confirmarse.

Funcionamiento en el receptor

- **Ventana de recepción**: grupo de tramas que el receptor tiene permitido aceptar. Toda trama que se reciba con un número de secuencia fuera de la ventana será descartada.

NOTA 5.2

Cuidado, la ventana del receptor no representa el número de tramas recibidas sino las que todavía se pueden recibir antes de enviar una confirmación.

- Cuando se recibe una trama, se reduce "por la izquierda" una posición la ventana del receptor.

- ✓ Cuando se envía una confirmación, se expande "por la derecha" la ventana del receptor tantas posiciones como tramas se confirmen.
- ✓ Las confirmaciones (ACK) se envían numeradas con la siguiente trama que se desea recibir. Un solo ACK puede confirmar varias tramas simultáneamente. Por ejemplo, si se envía una trama ACK 3, significa que el receptor confirma la recepción correcta de todas las tramas hasta la 2 inclusive.

En la siguiente figura se puede ver un ejemplo.

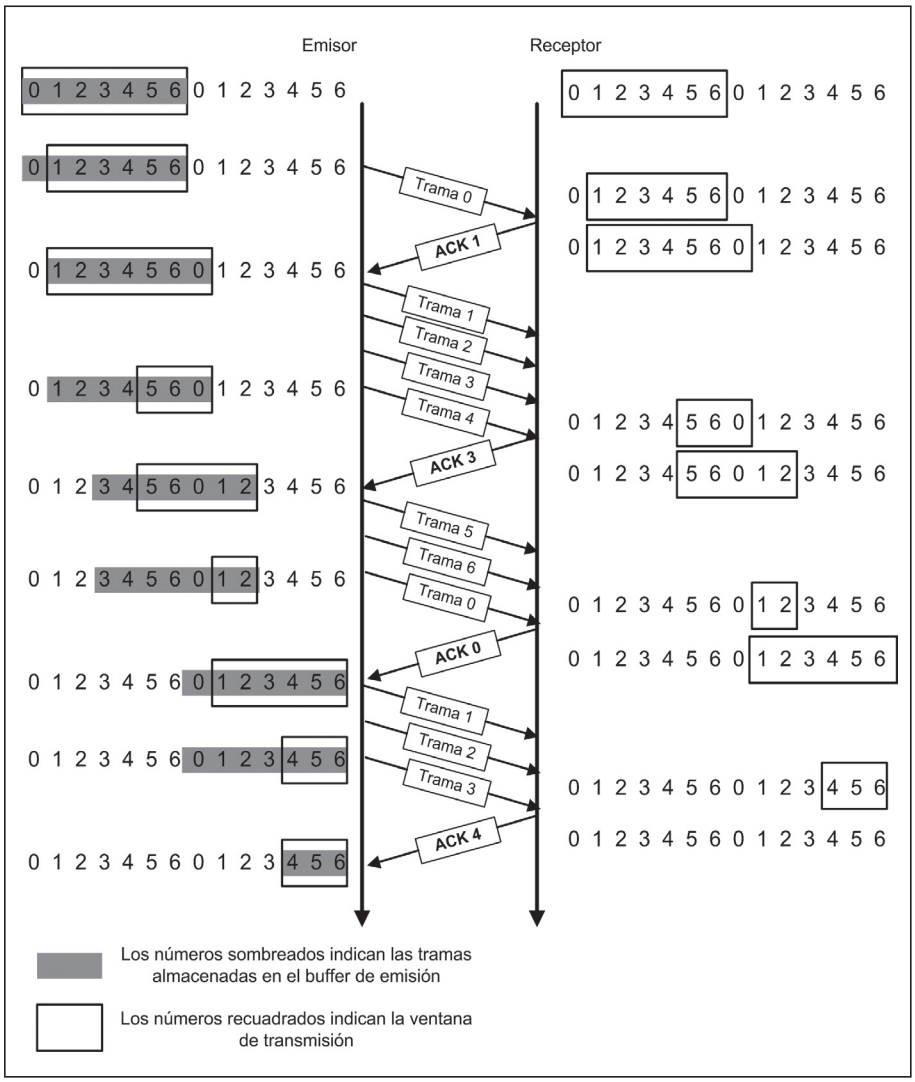


Figura 5.3. *Ejemplo de control de flujo mediante ventana deslizante.*

El método de ventana deslizante es útil sobre todo para transmisiones full-dúplex en las que las tramas de confirmación se pueden enviar junto con los datos que se envían en el otro sentido de la transmisión, lo cual es más eficiente que enviar tramas separadas de control. Efectivamente, al llegar una trama de datos, en lugar de enviar inmediatamente una trama de confirmación el receptor espera a que se tengan datos que transmitir. Cuando esto ocurre, aprovecha la trama de datos para incluir en su cabecera la confirmación a la trama recibida. La mayor parte de las veces es mucho más eficiente enviar las confirmaciones dentro de una trama de datos (en la cabecera de la trama) que utilizar una trama específica sólo para enviar la confirmación, ya que ésta debe incluir una cabecera propia y un campo de comprobación de errores. En el protocolo HDLC que se verá más adelante en este capítulo, se utiliza un solo bit para enviar una confirmación dentro de una trama de datos. Está claro que esta opción es mucho más eficiente. Esta técnica de retardar el envío de la confirmación para poder anexarlo a la siguiente trama de datos de salida se conoce como **piggybacking** (incorporación) .

NOTA 5.3

La técnica de ventana deslizante es especialmente útil en transmisiones full-dúplex ya que se pueden aprovechar las tramas de datos para enviar confirmaciones.

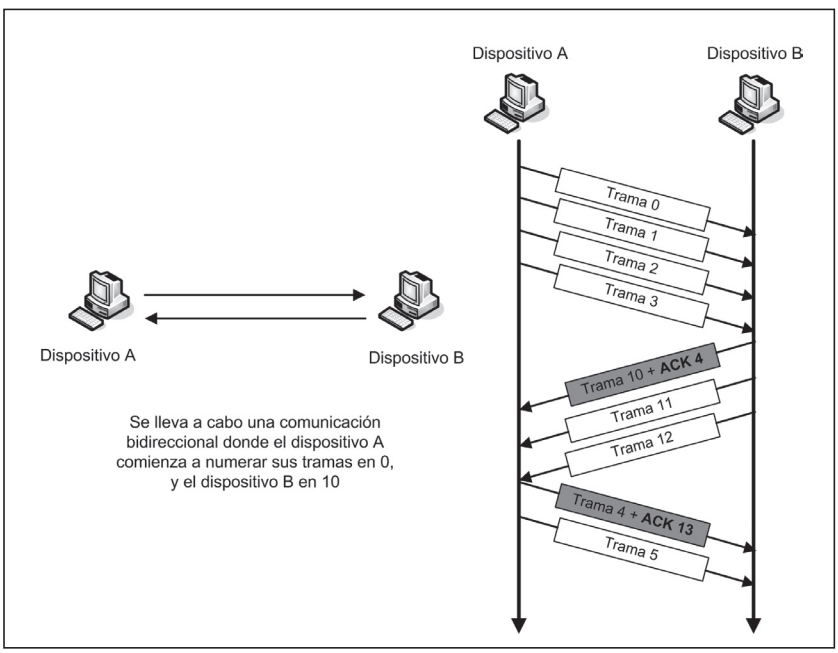


Figura 5.4. *Funcionamiento de la técnica piggybacking.*

Hay algunas implementaciones de ventana deslizante donde la ventana del transmisor y receptor no tienen el mismo tamaño. En algunos protocolos las ventanas pueden disminuir y aumentar a medida que se envían y reciben tramas.

5.2.3 CONTROL DE ERRORES

El control de errores es una de las principales funciones del nivel de enlace. Se trata de detectar y corregir todos los errores que se produzcan en el medio de transmisión.

El método más ampliamente utilizado para llevar a cabo la corrección de los errores detectados en el receptor se llama **Petición de Repetición Automática o ARQ (Automatic Repeat Request)** y está basado en la retransmisión de las tramas en tres situaciones diferentes de error: tramas dañadas, tramas perdidas y reconocimiento perdido.

En la práctica, el control de errores con ARQ se implementa en el nivel de enlace como parte del control de flujo. De esta forma existe parada y espera con ARQ y ventana deslizante con ARQ.

5.2.3.1 Parada y espera con ARQ

Este método es básicamente utilizar como control de flujo parada y espera pero añadiendo la funcionalidad de la retransmisión de tramas perdidas o dañadas. Para ello se añaden cuatro características al mecanismo básico de control de flujo:

- ✓ Se mantiene en el emisor una copia de la trama enviada hasta que se recibe su reconocimiento. Esto es necesario para el caso en el que haya que retransmitir la trama con algún error o pérdida.
- ✓ Para permitir la identificación de las tramas de datos en el caso de que haya una transmisión duplicada, se numeran las tramas de datos y las tramas ACK alternativamente con 0 y 1.
- ✓ Cuando se detecta un error en el receptor, se envía una trama NAK sin numeración. Esta trama le indica al emisor que debe retransmitir la última trama enviada.

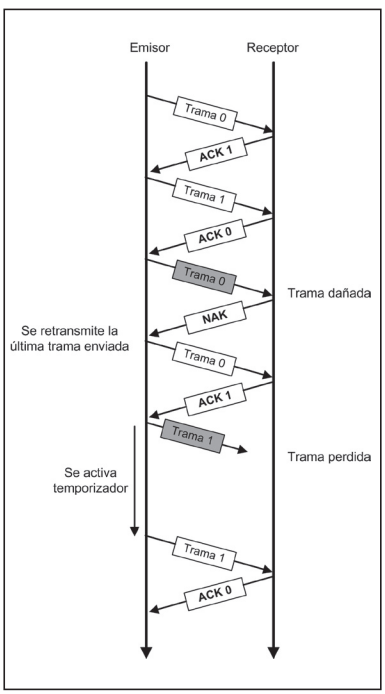


Figura 5.5. *Ejemplo de transmisión usando parada y espera con ARQ.*

- ✓ Se utiliza un temporizador en el emisor. Si el reconocimiento a la trama de datos no se recibe en un tiempo determinado, se asume que la trama se perdió y se retransmite.

Cuando se detecta en el receptor una trama con error se envía una trama NAK y el emisor retransmite la trama.

La detección de tramas perdidas se realiza con el temporizador implementado en el emisor. Cada vez que se envía una trama se inicializa el temporizador y si el mismo vence sin haber recibido asentimiento (positivo o negativo) se retransmite la trama de datos.

El tratamiento de reconocimientos perdidos (tramas ACK o NAK) se basa también en la retransmisión de las tramas de datos. Si la trama perdida fue un NAK, el receptor acepta la nueva copia recibida y devuelve un ACK. Si se perdió en ACK, el receptor detecta que la trama es duplicada, ya que las tramas se envían numeradas y por tanto descarta la misma y envía una trama ACK.

■ 5.2.3.2 Ventana deslizante vuelta atrás con ARQ

En este caso se utiliza el método de ventana deslizante para llevar a cabo el control de flujo pero añadiendo las características de ARQ para el control de errores. Para ello se añaden las siguientes funcionalidades al método de ventana deslizante original:

- ✓ Si en el receptor se detecta que la trama llega con error se envía una trama NAK para indicar al emisor que debe retransmitir la trama con error. La trama NAK debe incluir el número de la trama en la que se ha producido el error. Una trama NAK además, confirma la recepción de todas las tramas pendientes de confirmación anteriores a la trama con error.
- ✓ Cuando el emisor recibe una trama NAK con un número de secuencia determinado, retransmite la trama con ese número de secuencia y todas las tramas que se hubiesen enviado después de la trama con error.
- ✓ Se implementa un temporizador en el emisor para solucionar el problema de las tramas de datos

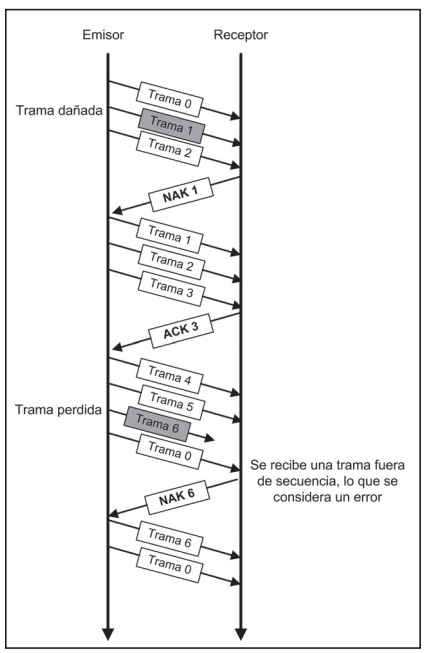


Figura 5.6. *Ejemplo de transmisión usando ventana deslizante vuelta atrás con ARQ.*

perdidas o los asentimientos perdidos. Cuando se envían todas las tramas posibles (tamaño de ventana 0) se activa el temporizador en el emisor. Cuando éste vence, se retransmiten todas las tramas pendientes de confirmación.

- ✓ Si se recibe una trama con un número de secuencia diferente del esperado se considera una trama con error y se envía una trama NAK. Esta situación se suele producir cuando se pierde una trama de datos.

5.2.3.3 Ventana deslizante rechazo selectivo con ARQ

La técnica de rechazo selectivo utiliza también ventana deslizante como control de flujo y ARQ como control de errores. Por tanto es muy similar al método de vuelta atrás aunque presenta algunas diferencias. La principal diferencia es que cuando llega una NAK sólo se retransmite la trama cuyo número de secuencia indica la trama NAK, es decir, la trama que llegó con error.

Sus características son:

- ✓ Al igual que en vuelta atrás, cuando el receptor detecta que la trama llega con error se envía una trama NAK para indicar al emisor que debe retransmitir la trama con error. La trama NAK debe incluir el número de la trama en la que se ha producido el error. Una trama NAK, además, confirma la recepción de todas las tramas pendientes de confirmación anteriores a la trama con error.
- ✓ Una trama NAK, además, confirma la recepción de todas las tramas pendientes de confirmación anteriores a la trama con error.
- ✓ Cuando el emisor recibe una trama NAK con un número de secuencia determinado, retransmite sólo la trama con ese número de secuencia. Esta característica hace que puedan llegar al receptor tramas desordenadas, por lo que hay que implementar en el receptor un método de ordenación de tramas. Ésta es la principal diferencia con el método de vuelta atrás.
- ✓ A diferencia de en el método de ventana deslizante, los números de secuencia enviados en las tramas ACK se refieren a la trama recibida no a la siguiente esperada.
- ✓ Se utiliza un tamaño máximo de la ventana más pequeño que en el método general de ventana deslizante. Para la implementación de ventana deslizante de módulo *n* con rechazo selectivo se utiliza un tamaño de ventana de (n + 1)/2. En vuelta atrás se utilizaría el tamaño del método genérico: n – 1.
- ✓ Al igual que en vuelta atrás, se implementa un temporizador en el emisor para solucionar el problema de las tramas de datos perdidas o los asentimientos perdidos. Cuando éste vence, se retransmiten todas las tramas pendientes de confirmación.

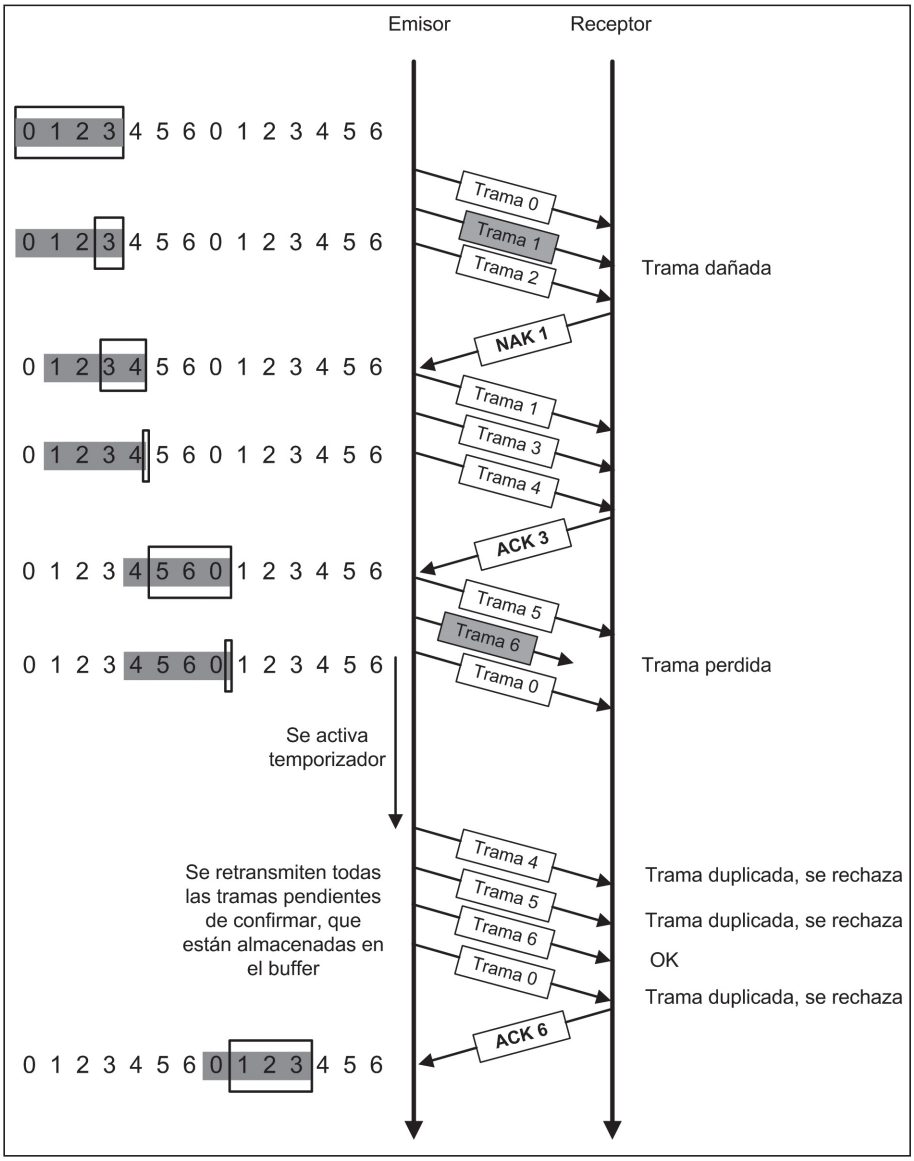


Figura 5.7. *Ejemplo de transmisión usando ventana deslizante rechazo selectivo con ARQ.*

5.2.4 TÉCNICA DE DETECCIÓN DE ERRORES: CRC

La técnica ARQ se utiliza en el nivel de enlace, en combinación con el control de flujo para la corrección de los errores de transmisión. Este método se basa en la detección de los errores de transmisión en la recepción, por lo cual es necesario implementar en el nivel de enlace un mecanismo de detección de los errores.

Existen diferentes técnicas para verificar que un bloque de datos se transfiere de un sistema a otro sin errores, aunque el más utilizado en el nivel de enlace se conoce como **CRC (Cyclic Redundancy Code, Código de redundancia cíclica)**.

Esta técnica se basa en añadir al bloque de datos una secuencia de bits, llamada CRC, obtenida a partir de la información contenida en el propio bloque de datos. Esta secuencia de bits es calculada por el emisor y transmitida junto con los datos. El receptor, cuando recibe los datos realiza el mismo cálculo. Si el CRC calculado por el receptor coincide con el recibido es que los datos no han sido alterados en la transmisión, es decir, no ha habido errores y por tanto la trama se acepta. Cuando el CRC calculado no coincide con el recibido es que ha habido errores en la transmisión, con lo cual la trama se rechaza.

La secuencia de bits o CRC se calcula realizando la operación división binaria de los datos entre un divisor predeterminado. A este divisor se le conoce como **polinomio generador**. El resto obtenido de la división es el CRC.

Se conoce como polinomio generador porque la secuencia de bits del divisor se expresa como un polinomio. Por ejemplo, el número binario 1100101 se puede expresar de forma polinomial como:

$$1X^6 + 1X^5 + 0X^4 + 0X^3 + 1X^2 + 0X^1 + 1X^0$$

o lo que es lo mismo, suprimiendo los términos cuyo coeficiente es 0:

$$X^6 + X^5 + X^2 + 1$$

El exponente más alto se conoce como orden, de forma que, en el ejemplo anterior, se dice que es un polinomio de orden 6.

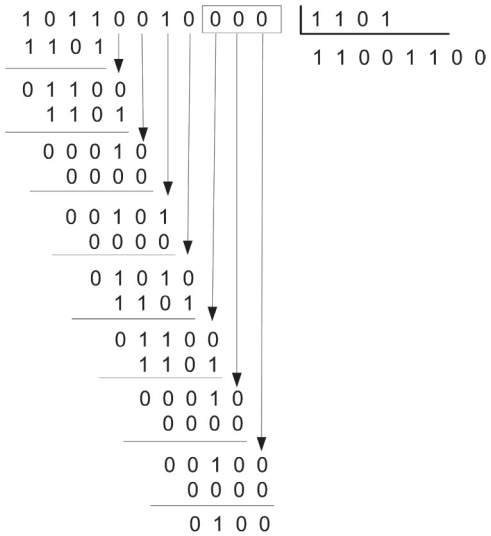
Los pasos que se siguen para el cálculo del CRC son:

1. Llamamos *n* al orden del polinomio generador.
2. A los datos para los que se quiera obtener su CRC se añaden a la derecha *n* ceros.
3. Se lleva a cabo la división binaria entre los datos (con los ceros añadidos) y el polinomio generador.
4. El resto que se obtiene en la división es el CRC que tendrá *n* bits.

En el siguiente ejemplo se quiere calcular el CRC para el bloque de bits 10110010. En este ejemplo utilizamos un bloque de datos de sólo 8 bits pero el proceso es el mismo para bloques de datos más grandes.

En el ejemplo se va a utilizar el siguiente polinomio generador de orden 3: $X^3 + X^2 + 1$ que expresado como número binario queda: 1101.

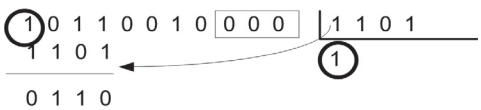
Como el polinomio generador es de orden 3 se añaden tres ceros a la derecha de los datos y se efectúa la división binaria.



Como se puede observar, la división binaria utiliza las mismas reglas que la división aritmética. La obtención de los cocientes parciales es sencilla:

- ✓ Si el bit más significativo del dividendo parcial es 1, el cociente parcial es 1.
- ✓ Si el bit más significativo del dividendo parcial es 0, el cociente parcial es 0.

Por ejemplo para el primer cociente parcial. El dividendo parcial es 1011, por tanto el cociente parcial es 1. Se pasa el divisor para restarse al dividendo parcial:

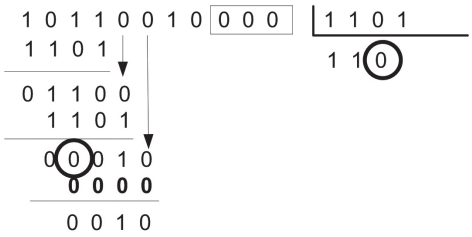


La resta binaria también es sencilla:

$$0 - 0 = 0$$
$$0 - 1 = 1$$
$$1 - 0 = 1$$
$$1 - 1 = 0$$

Después de cada resta se toma el siguiente bit del dividendo y se descarta el que está más a la izquierda, que siempre va a ser un 0.

Si el cociente parcial es 0, se ponen todos los bits a cero:



Para el cálculo del CRC se descarta el cero de la izquierda del resto. Para el ejemplo queda como resto 100, que por tanto será el CRC obtenido.

5.3 PROTOCOLOS DEL ENLACE DE DATOS

Los protocolos del nivel de enlace son los que implementan las funciones de dicho nivel y para ello hacen uso de las técnicas estudiadas en el apartado anterior. Dichos protocolos cubren básicamente las funciones de control de flujo y control de errores. Además, todos los protocolos del nivel de enlace especifican el formato de trama utilizado para la transmisión de los datos, incluyendo la información que se incluye en la cabecera. Si es necesario, los protocolos también incluyen mecanismos de direccionamiento físico.

Para enlaces multipunto compartidos, donde es necesario llevar a cabo un control de acceso al medio, se suelen utilizar protocolos diferentes a los protocolos que cubren las funciones de control de errores y control de flujo. Incluso se utilizan subniveles diferentes, como ocurre en redes de área local IEEE donde el nivel de enlace se divide en dos subniveles: MAC y LLC. MAC se ocupa del control de acceso al medio y LLC se ocupa del control de flujo y control de errores.

Los protocolos desarrollados en el nivel de enlace se pueden dividir en dos grupos:

- ✓ Asíncronos
- ✓ Síncronos. Éstos a su vez pueden ser orientados a carácter u orientados a bits.

5.3.1 PROTOCOLOS ASÍNCRONOS

Los protocolos asíncronos son los primeros protocolos implementados en el nivel de enlace y se utilizaron sobre todo en las transmisiones de ficheros por módem. Su principal ventaja es que son fáciles (y, por tanto, baratos) de implementar. Lógicamente utiliza transmisiones asíncronas, es decir, cada unidad de información se envía entre bits de inicio y parada. Su principal desventaja es su lentitud. De hecho actualmente apenas se utilizan y han sido sustituidos por protocolos síncronos, más rápidos.

A continuación se presentan algunos de estos protocolos asíncronos:

XMODEM

Desarrollado en el año 1977. Se utilizaba para transferir ficheros entre dos ordenadores a través de la línea telefónica, utilizando módems. Es un protocolo half-dúplex de tipo parada y espera con ARQ. La información se transfiere utilizando tramas con la siguiente estructura:

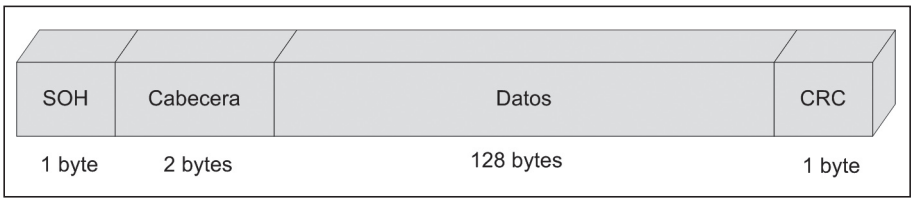


Figura 5.8. *Trama XMODEM.*

- **Comienzo de cabecera: SOH (Start Of Header).** Es un byte que indica el comienzo de la trama.
- **Cabecera.** Son dos bytes donde se incluyen el número de secuencia de la trama.
- **Datos.** Con un tamaño fijo de 128 bytes.
- **CRC.** Código de redundancia cíclica utilizado para comprobar que no se producen errores en los datos.

Por tanto, la trama de datos completa son un total de 132 bytes. Además, se utiliza la trama ACK para confirmar una trama de datos y la trama NAK para pedir la retransmisión de una trama con error. Se puede utilizar también una trama **CAN (Cancelación)** para abortar la transmisión.

YMODEM

Fue desarrollado como continuación del protocolo XMODEM con los siguientes cambios:

- ✓ Antes de transferir el fichero se envía en una trama el nombre y el tamaño del fichero que se va a transmitir. Esto permite el envío de varios ficheros en la misma comunicación y soluciona algunos problemas de transparencia en los datos.
- ✓ En cada trama se envían 1024 bytes de datos en lugar de 128.
- ✓ Se utiliza un código CRC de 2 bytes.
- ✓ Para abortar la transferencia de un fichero se envían dos tramas CAN en lugar de una.

ZMODEM

El protocolo ZMODEM se desarrolló en 1986 y fue muy utilizado en las transferencias de ficheros a comienzos de los años 90, sustituyendo en muchos casos los protocolos XMODEM e YMODEM.

La principal mejora que introduce este protocolo respecto a los anteriores es que utiliza la técnica de ventana deslizante para el control de flujo.

Utiliza un código de comprobación de errores de 32 bits (4 bytes) y, como YMODEM, permite la transferencia de varios ficheros.

5.3.2 PROTOCOLOS SÍNCRONOS ORIENTADOS A CARÁCTER: BSC

Los protocolos asíncronos, aunque son sencillos y baratos de implementar, no son eficaces especialmente para velocidades más altas, por lo que se utilizan protocolos síncronos. Existen dos tipos de protocolos síncronos: orientados a carácter y orientados a bits.

Actualmente todos los protocolos en el nivel de enlace utilizados en las principales arquitecturas y tecnologías de red son orientados a bits, fundamentalmente por una razón: la eficiencia. Sin embargo, los protocolos orientados a carácter son más fáciles de comprender, aunque utilizan los mismos principios de funcionamiento que los protocolos orientados a bits. Por ello el estudio de los protocolos orientados a carácter puede ser útil para establecer una base de cara a afrontar el estudio de los protocolos orientados a bits.

En los protocolos orientados a carácter la unidad básica de información es el carácter o byte. Se utilizan bytes de control para llevar a cabo las funciones del protocolo y se debe utilizar algún tipo de codificación basada en bytes para los datos, por ejemplo, el código ASCII. Por tanto, estos protocolos suelen ser dependientes de la codificación de los datos.

El protocolo orientado a carácter más importante es **BSC (Binary Synchronuos Communication, Comunicación Síncrona Binaria)** desarrollado por IBM en los años 60.

Este protocolo se puede utilizar tanto en comunicaciones punto a punto como en multipunto, y utiliza la técnica de parada y espera con ARQ para el control de flujo y errores.

El formato general de una trama BSC es el siguiente:

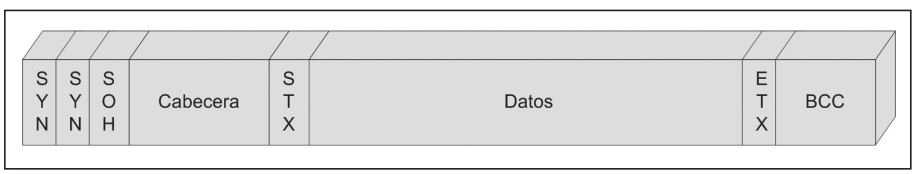


Figura 5.9. *Trama de datos en BSC.*

Como se observa, dentro de la trama se utilizan los siguientes caracteres de control:

- **SYN.** Al comienzo de cada trama se envían dos caracteres de sincronización utilizados para proporcionar un patrón de bits usado por el receptor para sincronizar su temporizador con el emisor. El patrón utilizado para un carácter SYN es: 00010110.
- **SOH (Start Of Header, Comienzo de cabecera).** Indica el comienzo de la cabecera. A continuación se incluye la cabecera de la trama donde se incluye información de control como las direcciones origen y destino y el número de secuencia de la trama (0 y 1).
- **STX (Start Of Transmission, Comienzo del bloque de texto).** Es un carácter de control que indica el fin de los datos de la cabecera y el comienzo de los datos de la trama.
- **ETX (End Of Transmission, Fin de bloque de datos).** Es el carácter de control para indicar el final de los datos de la trama.
- **BCC (Block Check Count, Contador de comprobación de bloque).** Este campo se utiliza para el control de errores, se utiliza un código CRC normalmente de dos bytes para verificar que la trama llega sin errores.

Además de las tramas de datos, el protocolo BSC utiliza tramas de control. El formato general de una trama de control BSC es el siguiente:

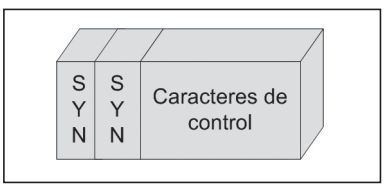


Figura 5.10. *Trama de control en BSC.*

Los principales caracteres de control utilizados en BSC son:

- **EOT:** final de la transmisión.
- **NAK:** reconocimiento negativo.
- **ACK:** reconocimiento positivo.
- **ENQ:** solicitud de conexión en configuraciones punto a punto, o selección de un dispositivo esclavo en configuraciones multipunto maestro-esclavo.
- **WACK:** confirma la recepción de la última trama (ACK) pero indica que temporalmente no puede recibir más tramas.

- **RVI:** petición de interrupción de la transmisión, normalmente para enviar una trama de mayor prioridad.
- **TTD:** indica que el emisor no va a enviar datos temporalmente pero desea mantener el control de la línea.

Uno de los principales problemas que existe en BSC es que fue un protocolo diseñado originalmente para enviar sólo texto, utilizando una codificación (por ejemplo, la codificación ASCII) donde existen códigos reservados a los caracteres de control, de forma que los datos de tipo texto no pueden contener dichos caracteres de control.

Sin embargo, si se utiliza este protocolo para enviar información binaria (programas, gráficos, audio…) puede ocurrir que los datos contengan secuencias de bits que se correspondan con los caracteres de control. Por ejemplo, si dentro de los datos se encuentra una secuencia de bits que se corresponde con el código utilizado para codificar el carácter ETX, el receptor confundirá esto con el final del bloque de datos.

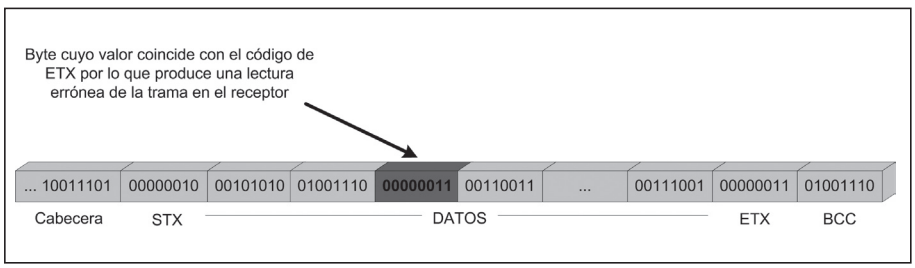


Figura 5.11. *Las tramas de datos con contenido binario causan problemas de falta de transparencia.*

A la confusión entre la información de control y los datos se la denomina normalmente **falta de transparencia**. Un protocolo que ofrezca transparencia de los datos es aquél que permite enviar cualquier combinación de bits en los datos. Para conseguir esto, en BSC se marcan los bloques de datos donde se envían datos que puedan confundirse con caracteres de control. A pesar de ello, en BSC se pueden producir situaciones de falta de transparencia.

5.3.3 PROTOCOLOS SÍNCRONOS ORIENTADOS A BIT: HDLC

Como hemos visto, el principal problema de los protocolos orientados a carácter es la falta de transparencia en los datos. Este problema se reduce en gran medida utilizando protocolos orientados a bit ya que utilizan patrones de bits en lugar de caracteres de control. De hecho, los protocolos orientados a bit no están asociados a ninguna codificación. Además, estos protocolos ofrecen una mayor eficiencia en la transmisión ya que utiliza menos información de control que los protocolos orientados a carácter.

Actualmente, la mayor parte de los protocolos utilizados en el nivel de enlace en las diferentes arquitecturas y tecnologías de red se basan en el estándar propuesto por la ISO, llamado HDLC. Originalmente se desarrollaron varias recomendaciones para completar el protocolo, pero actualmente están todos los aspectos del mismo agrupados en la recomendación ISO 13239.

HDLC (High-level Data Link Control, Control de enlace de datos de alto nivel) es un protocolo del nivel de enlace orientado a bits que se puede utilizar para comunicaciones half-dúplex o full-dúplex y en configuraciones punto a punto o multipunto.

NOTA 5.4

HDLC se ha convertido en la base de todos los protocolos orientados a bits que se usan en la actualidad.

Pero si el protocolo HDLC es el padre del resto de protocolos orientados a bit, SDLC es el abuelo. **SDLC (Synchronous Data Link Control, control síncrono del enlace de datos)** es el protocolo de nivel de enlace síncrono y orientado a bits que IBM desarrolló a mediados de los años 70 para su arquitectura de red SNA. La ISO desarrolló el protocolo HDLC basado en el protocolo SDLC.

A su vez, la ITU-T modificó HDLC para crear su familia de protocolos LAP (Link Access Procedure) a partir de la cual se especificaron varios protocolos:

- **LAPB (Link Access Procedure Balanced)** como protocolo del nivel de enlace para redes X.25.
- **LAPD (Link Access Procedure – Channel D)** como protocolo del nivel de enlace de RDSI.
- **LAPM (Link Access Procedure for Modems)**, protocolo incluido en la norma V.42bis como protocolo de corrección de errores para módems.
- **LAPF (Link Access Procedure – Frame)**, protocolo de nivel de enlace para Frame Relay.

La organización IEEE también utilizó HDLC para crear su estándar IEEE 802.2 también conocido como **LLC (Logical Link Control)**. El organismo IETF (Internet Engineering Task Force) desarrolló el protocolo **PPP (Point to Point Protocol)**, cómo no, utilizando como base el protocolo HDLC.

Por tanto, el conocimiento del protocolo HDLC es muy útil para entender la gran mayoría de los protocolos usados actualmente.

HDLC proporciona tanto servicios orientados a conexión como no orientados a conexión.

5.3.3.1 Tipos de estación

En comunicaciones que utilicen HDLC como protocolo pueden existir tres tipos de dispositivos:

- **Estación primaria.** Dispositivo que tiene el control del enlace, tanto en líneas punto a punto como en líneas multipunto. Las tramas que envía se denominan órdenes.
- **Estación secundaria.** Sólo puede enviar datos como respuesta a las órdenes de una estación primaria. Por ello sus tramas se suelen llamar respuestas.
- **Estación combinada.** Envía tanto órdenes como respuestas.

5.3.3.2 Configuración del enlace

La configuración del enlace se refiere a cómo están conectados los dispositivos al medio. Existen dos tipos:

- **No balanceada.** En esta configuración, un dispositivo es primario y el resto son secundarios. Puede ser una configuración punto a punto o multipunto.
- **Balanceada.** En esta configuración se utiliza una topología punto a punto con dos dispositivos configurados como estaciones combinadas.

5.3.3.3 Modos de comunicación

Los modos de comunicación describen la relación entre dos dispositivos que se comunican a través del protocolo HDLC. Los modos de configuración son:

- **Modo de respuesta normal (NRM, Normal Response Mode).** Utilizado en configuración no balanceada, es decir, existe una estación primaria y una secundaria que sólo puede enviar datos como respuesta a órdenes de la estación primaria.
- **Modo de respuesta asíncrono (ARM, Asynchronous Response Mode).** Utilizado en configuración no balanceada, es decir, también existe estación primaria y estaciones secundarias. La única diferencia es que una estación secundaria puede iniciar una transmisión sin recibir permiso de la estación primaria. Sin embargo, la estación primaria sigue llevando el control de la línea. Esta configuración no se utiliza mucho.
- **Modo asíncrono balanceado (ABM, Asynchronous Balanced Mode).** Utilizado en configuración balanceada, es decir, estaciones combinadas en topologías punto a punto. Cualquier estación puede iniciar una transmisión. Es el modo más utilizado.

Un detalle importante: HDLC no proporciona ningún modo de comunicación multipunto balanceado, que es la configuración utilizada, por ejemplo en las redes de área local (LAN). Por ello, en este tipo de redes existe un subnivel que

se encarga del control de acceso al medio (se verá en el próximo capítulo) con su protocolo correspondiente.

5.3.3.4 Formato y tipos de tramas en hdlc

Hay tres tipos de tramas en HDLC:

- **Tramas de información o tramas I.** Son las tramas más sencillas. Se utilizan para transportar los datos y los reconocimientos incorporados (ACK o NAK).
- **Tramas de supervisión o tramas S.** Utilizadas para transportar información de control.
- **Tramas sin numeración o tramas U.** Tramas utilizadas para la gestión del sistema.

A continuación se muestra el formato de cada uno de los tipos de tramas:

El significado de cada campo es el siguiente:

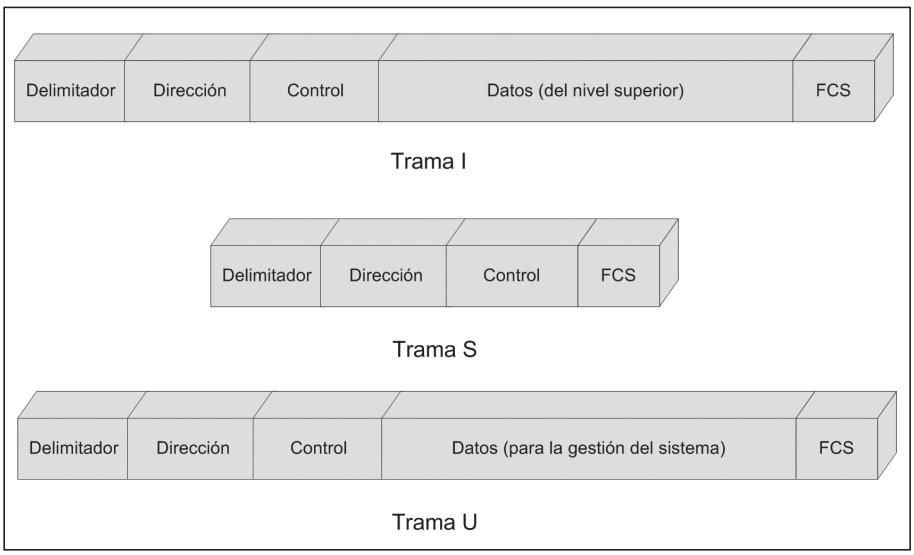


Figura 5.12. *Formatos de trama HDLC.*

- **Delimitador.** Campo utilizado para identificar el principio y el final de la trama. También se utiliza como patrón de sincronización para el receptor. Está formado por la secuencia de bits 01111110.
- **Dirección.** Si la trama la genera una estación primaria o una estación combinada funcionando como primaria contiene la dirección del destino. Si la trama la genera una estación secundaria o una combinada funcionando

como secundaria este campo contiene la dirección de origen, es decir, de la estación que genera la trama. Tiene un tamaño de uno o varios bytes.

- **Datos.** Este campo contiene los datos del nivel superior en las tramas I. Contiene información de gestión de red en las tramas U. Las tramas S no incluyen campo de datos.
- **FCS** (Secuencia de comprobación de trama) contiene un código CRC de dos o cuatro bytes para llevar a cabo el control de errores.
- **Control.** El campo de control puede estar formado por uno o dos bytes. Si tiene un tamaño de 1 byte su estructura es la siguiente:

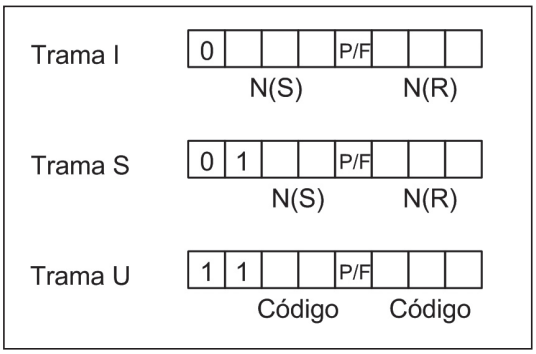


Figura 5.13. *Campo de control HDLC.*

Como se observa, cuando el primer bit del campo de control es un 0, indica que es una trama de información (trama I). Cuando el primer bit es 1 y el segundo es 0, indica que es una trama de supervisión (trama S). Cuando el primer bit es 1 y el segundo es 1 indica que es una trama sin numeración (trama U).

A continuación se explica con más detalle el significado de la información que aparece en el campo de control:

El protocolo HDLC usa la técnica de ventana deslizante y para el caso del campo de control simple se utilizan 3 bits para almacenar el número de trama, por lo que las tramas se pueden numerar desde 0 (000) hasta 7 (111), es decir, ventana deslizante de orden 8.

El bit P/F, que aparece en todos los tipos de tramas, cuando tiene valor 1 y la trama se envía de una estación primaria a una estación secundaria significa sondeo, es decir, la estación primaria pide datos a una estación secundaria (es decir, la función de sondeo de la técnica de sondeo y selección). Cuando se envía de una estación secundaria a una primaria significa final, es decir, la estación secundaria indica el final de los datos, es decir, que es la última trama enviada.

Para la trama de información (trama I):

- **N(S)** indica el número de trama enviado. Como ya se ha indicado, se utilizan 3 bits por lo que los números de secuencia pueden ser de 0 a 7.
- **N(R)** es un campo de asentimiento que contiene el próximo número de trama que se espera recibir si la última que llegó fue correcta (ACK), o el número de trama que llegó con errores (NAK).

Puede haber cuatro tipos diferentes de tramas de supervisión (tipo S), en función del valor de los bits de campo tipo:

- **Tipo 0: RR(Receive Ready, recepto listo).** Se utiliza para enviar un asentimiento (ACK). El campo secuencia indica la próxima trama que se debe enviar, confirmando así todas las anteriores. Este tipo de trama de supervisión se utiliza cuando no hay datos que enviar en el sentido contrario de la transmisión donde poder incluir el asentimiento (piggybacking) .
- **Tipo 1: REJ (Reject, Rechazo).** Trama utilizada para enviar un NAK, es decir, la recepción de una trama con error. El campo secuencia indica el número de trama en la que se produjo el error. En este caso, se utiliza la técnica ventana deslizante vuelta atrás y, por tanto, se deben retransmitir la trama errónea y todas las posteriores.
- **Tipo 2: RNR (Receive Not Ready, Receptor no listo).** Sirve para confirmar todas las tramas pendientes de asentimiento hasta el número indicado en el campo secuencia, sin incluirlo. Además indica al transmisor que detenga temporalmente el envío de datos. Normalmente indica problemas temporales en el receptor. Cuando se resuelven se reanuda la comunicación con el envío de una trama RR o REJ.
- **Tipo 3: SREJ (Selective Reject, Rechazo selectivo).** Se utiliza para pedir la retransmisión sólo de la trama indicada en el campo secuencia. Es decir, tiene la función de asentimiento negativo (NAK) en la técnica de ventana deslizante con rechazo selectivo.

Además, los tipos RR y RNR se utilizan, junto con el bit P/F para implementar la técnica de sondeo/selección. A continuación se muestran las diferentes combinaciones con su significado:

Tabla 5.1

Operación	P/F	Tipo de trama
Sondeo	P=1	RR
Respuesta positiva al sondeo	F=0	tramas de datos
	F=1	última trama de datos
Respuesta negativa al sondeo	F=1	RR
Selección	P=1	RNR
Respuesta positiva a selección	F=1	RNR
Respuesta negativa a selección	F=1	RNR

Los bits de código en las tramas U se utilizan para codificar el tipo de trama y su función. Esta información depende de la implementación concreta de HDLC.

Por último, en la siguiente figura se muestra el formato del campo de control en el modo extendido:

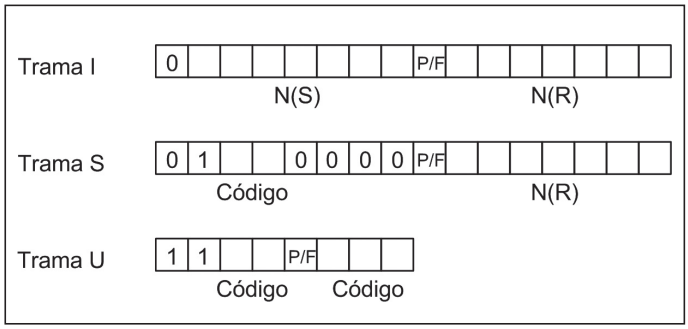


Figura 5.14. *Campo de control extendido de HDLC.*

5.3.3.5 Transparencia a nivel de bits

Como se ha visto anteriormente, las tramas HDLC están contenidas entre campos de delimitación de trama con un patrón fijo de bits: 01111110. Este campo es el único que puede causar problemas de transparencia en los datos cuando aparezca esta combinación de bits en cualquiera del resto de los campos de la trama.

Para solucionar el problema se utiliza la técnica llamada relleno de bits que consiste en detectar la presencia de cinco unos consecutivos en la trama. Cuando esto ocurre se inserta automáticamente un cero. En el receptor se lleva a cabo el proceso contrario, cuando se leen cinco unos seguidos, se elimina el siguiente bit, que será el bit de relleno. De esta forma sólo en el campo delimitador aparecerá el patrón con los seis unos consecutivos: 01111110.

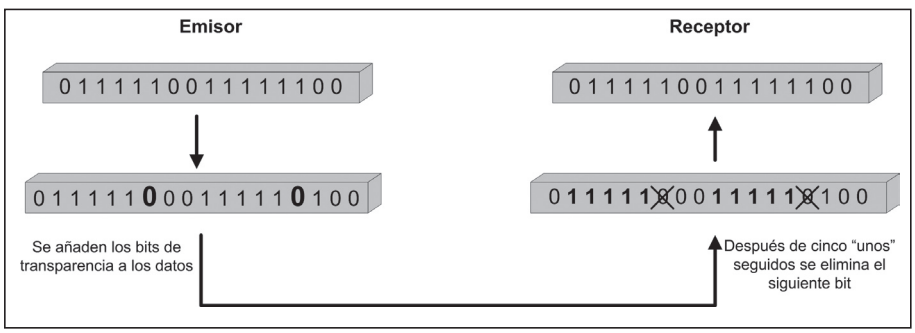


Figura 5.15. *Relleno de bits en HDLC.*

RESUMEN DEL CAPÍTULO

En la primera parte de este capítulo se exponen las principales funciones del nivel de enlace. Se explican las técnicas utilizadas para implementar dichas funciones.

Para el control de acceso al medio se estudian las técnicas de sondeo y selección, paso de testigo y sobre todo las técnicas de contienda.

Se estudian las dos técnicas utilizadas para el control de flujo en el nivel de enlace: parada y espera, y ventana deslizante. Para llevar a cabo el control de errores se añade a las anteriores la técnica ARQ basada en la retransmisión de las tramas con error.

Además, se expone una de las técnicas utilizadas más ampliamente para la detección de tramas con error, conocida como CRC.

En la segunda parte se hace un repaso a los principales protocolos implementados en el nivel de enlace:

- ✓ Los antiguos protocolos síncronos, hoy en día prácticamente en desuso.
- ✓ Los protocolos asíncronos orientados a carácter, representados por el protocolo BSC y que también se puede considerar obsoleto actualmente.
- ✓ Como ejemplo de protocolo asíncrono orientado a bit se estudia HDLC desarrollado por la ISO y utilizado como base para la implementación de muchos de los protocolos de nivel de enlace utilizados en la actualidad.

EJERCICIOS PROPUESTOS

1. En el método de parada y espera con ARQ los asentimientos se numeran, ya que se podría dar la siguiente situación de error:

- ✓ El emisor envía una trama de datos (trama 0). El receptor envía el asentimiento pero antes de que llegue al emisor vence el temporizador con lo que la trama 0 se retransmite.
- ✓ Después de la retransmisión llega el asentimiento del primer envío. El emisor lo interpreta como el asentimiento de la retransmisión.
- ✓ Se envía la trama 1 y después se recibe el asentimiento de la retransmisión que el emisor interpreta como el asentimiento de la trama 1.
- ✓ Sin embargo, la trama 1 puede llegar con error y el receptor enviaría un NAK, que el emisor interpretaría como un error de la siguiente trama (de nuevo numerada como trama 0).
- ✓ Dibujar el diagrama de la comunicación. Comprobar que numerando los asentimientos (ACK) el error se evita.

2. Calcular el tiempo del temporizador del emisor de un sistema de transmisión que utiliza ventana deslizante módulo 8 en un enlace de 4.000 Km con un tiempo de propagación de 5 µs/Km. La velocidad de transmisión del emisor es de 1 Mbps. El tamaño de la trama es de 5.000 bits. Se considera que el tiempo máximo que el receptor puede tardar en procesar una trama es de 50 ms.

3. El porcentaje de ocupación de un canal se calcula como el cociente del tiempo que está el canal transmitiendo datos entre el tiempo total de la transmisión. Para un sistema que utiliza el control de flujo parada y espera, la velocidad de transmisión es de 100 Kbps y el tiempo de propagación es de 100 ms, calcular el porcentaje de ocupación del canal en los siguientes casos:

- **a)** Para un tamaño de trama de 5.000 bits
- **b)** Para un tamaño de trama de 50.000 bits
- **c)** Para un tamaño de trama de 100.000 bits

A partir de los resultados anteriores, ¿qué tamaño de trama es el más eficiente?

4. En el estudio anterior no se han tenido en cuenta los errores. Calcular la tasa de transmisión real de 100.000 bits para los apartados b y c suponiendo que se produce error en un bit y es necesario retransmitir tramas. A partir de los resultados obtener las nuevas conclusiones.

5. Calcular el CRC de la secuencia de bits 1111000011 a partir del polinomio generador X3 + X1 + 1.

6. Dibujar el esquema de transmisión y la ventana del emisor para un sistema que usa ventana deslizante módulo 8, vuelta atrás (rechazo simple) con ARQ a partir de la siguiente secuencia de operaciones:

- ✓ Trama 0 enviada, trama 0 reconocida.
- ✓ Tramas 1 y 2 enviadas, tramas 1 y 2 reconocidas.
- ✓ Tramas 3, 4 y 5 enviadas, recibido NAK 4.
- ✓ Tramas 4, 5, 6 y 7 enviadas, tramas 4 a 7 reconocidas.

7. Dibujar el esquema de transmisión y la ventana del emisor para la siguiente secuencia de operaciones:

- ✓ Trama 0 enviada
- ✓ Trama 1 enviada
- ✓ Trama 2 enviada
- ✓ Trama 3 enviada
- ✓ Trama 4 enviada
- ✓ Recibido ACK 3
- ✓ Trama 5 enviada
- ✓ Recibido NAK 3
- ✓ Enviadas tramas 3, 4 y 5
- ✓ Recibido ACK 6

Asumir tamaño de la ventana 7. ¿Qué técnica de ventana deslizante se está utilizando?

TEST DE CONOCIMIENTOS

1 La técnica de solicitud y reconocimiento se utiliza:

- **a)** En enlaces multipunto half-dúplex.
- **b)** En enlaces multipunto full-dúplex.
- **c)** Exclusivamente en enlaces punto a punto full-dúplex.
- **d)** En enlaces punto a punto, tanto half-dúplex como full-dúplex.

2 En enlaces multipunto donde se utiliza una configuración centralizada en la que una estación tiene la función de estación primaria y el resto son estaciones secundarias se utiliza como método de acceso al medio:

- **a)** Sondeo y selección.
- **b)** Cualquiera de los métodos de contienda.
- **c)** Paso de testigo.
- **d)** Las dos últimas son correctas.

3 La mejora que introduce CSMA/CD respecto a otras técnicas de contienda es que:

- **a)** Primero escucha el medio antes de transmitir.
- **b)** Si detecta una colisión realiza la retransmisión de la trama.
- **c)** Si detecta una colisión deja de transmitir y espera un tiempo aleatorio antes de retransmitir.
- **d)** Divide el tiempo en intervalos discretos y sólo puede transmitir al comienzo de cada intervalo.

4 El principal problema de la técnica de parada y espera es:

- **a)** Que es muy compleja de implementar.
- **b)** Que es lenta.
- **c)** Que sólo sirve para comunicaciones full-dúplex.
- **d)** Que las tramas de datos tienen que tener una longitud fija.

5 En la técnica de ventana deslizante, la ventana de emisión contiene en todo momento:
- **a)** Todas las tramas que se tienen que enviar.
- **b)** Los números de secuencia de las tramas pendientes de enviar.
- **c)** Los números de secuencia de las tramas que pueden ser enviadas.
- **d)** Los números de secuencia de las tramas pendientes de confirmación.

6 En ventana deslizante vuelta atrás con ARQ, si se recibe un NAK con un número de secuencia:
- **a)** Se debe retransmitir la trama con ese número de secuencia.
- **b)** Se debe retransmitir la trama anterior a ese número de secuencia.
- **c)** Se debe retransmitir la trama con ese número de secuencia y todas las anteriores sin confirmar.
- **d)** No se utilizan tramas NAK.

7 La falta de transparencia en protocolos del nivel de enlace se refiere:
- **a)** A la confusión entre información de control y datos.
- **b)** A la posible confusión producida entre dos protocolos cuando son muy parecidos.
- **c)** A la problema que puede surgir cuando se utiliza una codificación para los datos no conocida en el receptor.
- **d)** No se aplica a los protocolos del nivel de enlace. Es propio del nivel físico.

8 El principal problema de los protocolos síncronos orientados a carácter es:
- **a)** Que son complejos de implementar.
- **b)** Sólo son válidos para comunicaciones punto a punto.
- **c)** Que suelen ser protocolos dependientes de la codificación de los datos.
- **d)** Que sólo se pueden utilizar en arquitecturas IBM.

9 El protocolo HDLC:
- **a)** Es un protocolo síncrono orientado a bit.
- **b)** No proporciona ningún modo de comunicación multipunto balanceado.
- **c)** Se usa como base para muchos otros protocolos del nivel de enlace.
- **d)** Todas las anteriores son válidas.

10 El campo de datos en una trama S del protocolo HDLC contiene:
- **a)** Datos del nivel superior.
- **b)** Información de gestión de la red.
- **c)** Asentimientos y códigos de control.
- **d)** Las tramas S no tienen campo de datos.

6 Módem

Objetivos del capítulo

- ✓ Estudiar las principales característica de un módem analógico.
- ✓ Conocer la evolución y los estándares para los módems analógicos.
- ✓ Entender el funcionamiento de los módems V.90.
- ✓ Conocer las características de los módems de cable.
- ✓ Conocer las características de los módems ADSL.

6.1 INTRODUCCIÓN

La palabra módem proviene de la contracción de las palabras moduladordemodulador. El módem es el dispositivo que adapta las señales digitales provenientes de un ordenador para poder transmitirlas a través de la Red Telefónica Conmutada (RTC). La red telefónica en sus orígenes se diseñó para la transmisión de señales vocales. Con esta filosofía se construyó una red mundial. La necesidad de transmitir datos digitales entre ordenadores planteó la posibilidad de utilizar la red telefónica para aprovechar la gran cobertura que ofrecía. Para ello se necesitaban convertir los datos digitales generados en los ordenadores en señales analógicas capaces de ser transmitidas por las líneas telefónicas. Esta conversión, llamada modulación, la lleva a cabo el módem al igual que el proceso inverso, la demodulación, es decir, transformar la señal analógica en una señal digital.

Actualmente, la red telefónica se ha adaptado a la tecnología digital excepto el bucle de abonado, que sigue siendo analógico, es por ello que sigue siendo necesario utilizar un módem para llevar a cabo una transmisión de datos digitales.

La transmisión de datos sobre líneas telefónicas está normalizada por medio de las recomendaciones de la serie V del organismo de estandarización ITU-T (Unión Internacional de Telecomunicaciones). El objetivo de la normalización es poder llevar a cabo una comunicación con módems de distintos fabricantes.

Debido a las limitaciones de velocidad de las comunicaciones utilizando el ancho de banda de las líneas telefónicas, se han desarrollado módems que utilizan otras tecnologías, como son los módems de cable y los módems ADSL, que también serán estudiados al final del capítulo. De hecho, la utilización de las tecnologías de cable y ADSL han desplazado el uso de los módems tradicionales, especialmente en los grandes núcleos urbanos donde estas tecnologías están muy implantadas.

6.2 FUNCIONES DE UN MÓDEM

El módem se considera un DCE, es decir, un dispositivo utilizado para el intercambio de datos en un sistema telemático, mientras que el ordenador sería el DTE, es decir, el dispositivo que genera los datos que se tienen que transmitir. Las funciones que debe realizar un módem son:

- ✓ Convierte los datos digitales provenientes del DTE en una señal analógica apta para su transmisión a través de la línea telefónica.
- ✓ Convierte la señal analógica modulada proveniente de la línea telefónica en una señal digital y enviarla al DTE.
- ✓ Establece un flujo de comunicación adecuado con el DTE y el DCE remoto para establecer, mantener y finalizar una conexión.

La principal técnica de transmisión de datos utilizada en los módems es la modulación, que se utiliza para convertir la señal digital del DTE en una señal analógica. Por tanto, se pueden utilizar cualquiera de las modulaciones vistas en el capítulo 2, como son ASK, FSK, PSK y QAM.

6.3 CARACTERÍSTICAS

6.3.1 VELOCIDAD DE TRANSMISIÓN

El módem utiliza como medio de transmisión el bucle local de abonado del sistema telefónico. Para no tener que hacer ningún cambio en el sistema telefónico, se debe utilizar el mismo ancho de banda que la señal de voz, es decir, el rango de frecuencias que va de los 300 Hz a los 3.300 Hz. Sin embargo, en los primeros diseños de módems y para evitar deformaciones de la señal en los límites del ancho de banda debido a los filtros del sistema telefónico, se hizo necesario acortar el ancho de banda útil, por lo que en muchos de los diseños se utiliza el rango de frecuencias de 600 Hz a los 3.000 Hz, es decir, un ancho de banda total de 2.400 Hz.

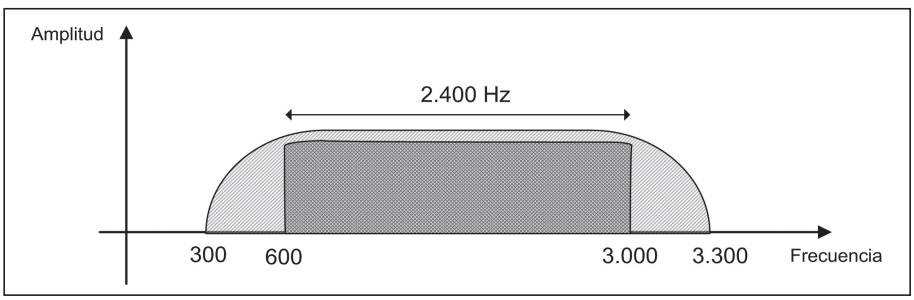


Figura 6.1. *Ancho de banda vocal y ancho de banda utilizado para datos.*

El ancho de banda disponible en el bucle de abonado, en principio de 2.400 Hz, es uno de los factores de los que depende la velocidad de transmisión. El otro factor del que depende es de la técnica de modulación utilizada. Por ejemplo, si utilizamos ASK, tendremos una tasa de transmisión de 2.400 bps. Si transmitimos en full-dúplex, la tasa por cada canal será la mitad, es decir, 1.200 bps. Si se utiliza, por ejemplo 8-PSK, la tasa de baudios será de 2.400 baudios que se corresponde con una tasa de bits de 7.200 bps. Si la transmisión es full-dúplex serían 3.600 bps por cada canal.

NOTA 6.1

La velocidad de transmisión de un módem depende de dos factores: el ancho de banda del medio utilizado y la técnica de modulación empleada.

6.3.2 MÓDEMS EXTERNOS: INTERFAZ DTE-DCE

Los módems externos pueden utilizar tanto un puerto serie como un puerto USB para su conexión con un ordenador o en general con un DTE. Cuando la conexión se realiza por un puerto serie, la interfaz utilizada (conocida como interfaz DTE-DCE) sigue alguno de los estándares para puerto serie estudiados en el capítulo 4:

- **RS-232:** es el estándar americano de la EIA (Electronic Industries Association).
- **V.24/V.28:** estándar de la ITU. Es el equivalente europeo. La recomendación V.24 define las características funcionales de la interfaz DTE-DCE. La recomendación V.28 define las características eléctricas de los circuitos de la interfaz DTE-DCE.

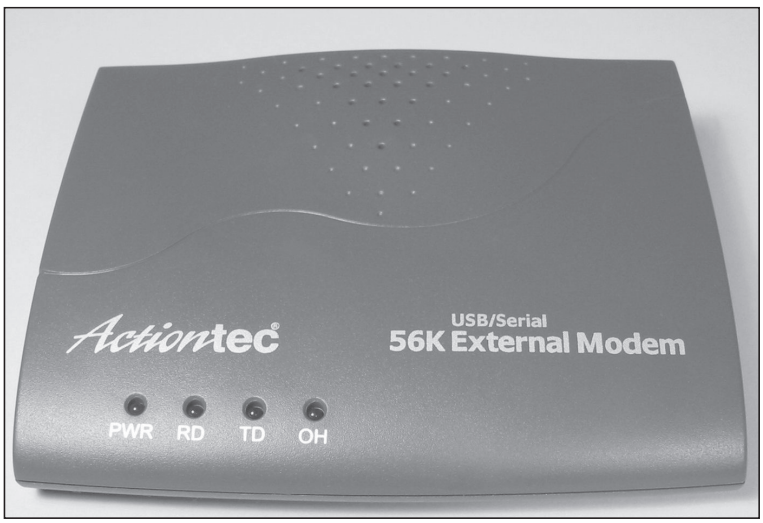


Figura 6.2. *Módem externo.*

Para velocidades superiores existen otras interfaces:

- Velocidad media (48 Kbps a 100 Kbps): estándares V.35, V.10/V.11, G.703.
- Alta velocidad (2.048 Kbps o mayor): estándares G.703, G.704.

6.3.3 MÓDEMS INTERNOS

Los módems internos se utilizan principalmente para conectar ordenadores a la red telefónica. Estos módems son tarjetas que se conectan directamente en un bus interno del PC, normalmente al bus PCI, y por tanto utilizan dicho bus interno del PC como interfaz.

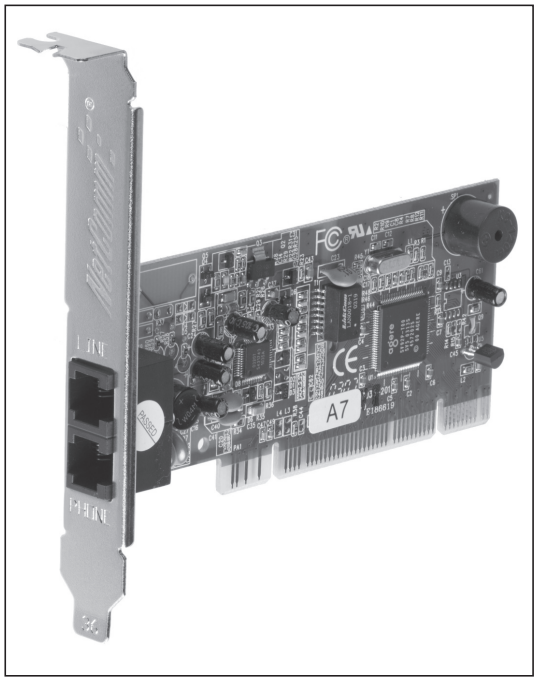


Figura 6.3. *Módem interno.*

Actualmente, con los sistemas operativos modernos como Windows XP o Linux, el proceso de configuración de los módems en un PC es prácticamente transparente al usuario.

6.3.4 DETECCIÓN Y CORRECCIÓN DE ERRORES

Los módems implementan, además, protocolos de detección y corrección de errores normalizados en la recomendación V.42, como son:

- **MNP4.** Utiliza una técnica de empaquetado adaptativo basado en el uso de códigos CRC sobre bloques de tamaño variable. El tamaño depende de las condiciones de la línea: cuando éstas son buenas utiliza bloques largos y cuando son malas utiliza bloques más cortos.
- **LAPM (Link Access Protocol for Modems).** Está basado en el protocolo HDLC (nivel de enlace) y utiliza una estructura de trama distinta a la de MNP4.

6.3.5 OTRAS CARACTERÍSTICAS

Las líneas públicas de datos que utilizan el sistema telefónico pueden ser de dos tipos:

- **Línea a 2 hilos:** se utiliza un solo circuito físico para la transmisión de datos.
- **Línea a 4 hilos:** se utilizan dos circuitos de datos independientes, normalmente utilizados para cada sentido de la transmisión.

Por tanto, existen especificaciones para módems de 2 hilos y 4 hilos. La mayor parte de las líneas telefónicas utilizadas en España son a 2 hilos. No confundir 2 y 4 hilos con full-dúplex y half-dúplex.

En los sistemas telefónicos, la transmisión full-dúplex a 2 hilos se consigue utilizando un transformador híbrido de 4 a 2 hilos (o bobina híbrida) y canceladores de eco. De esta forma, la transmisión de los dos canales, de envío y de recepción, se realiza sobre sólo 2 hilos (1 solo canal). Por tanto, a través de la RTC sólo se utilizan módems a 2 hilos. En líneas punto a punto pueden utilizarse módems a 2 hilos y a 4 hilos.

La mayor parte de los módems también incorporan algoritmos de compresión de datos especificados en la norma V.42bis, llamados MNP5 y MNP7.

Igualmente, los módems más recientes incorporan la posibilidad de enviar y recibir faxes siguiendo las recomendaciones correspondientes a los faxes Clase 1 o Clase 2:

- ✓ V.17 publicada en 1991, Grupo III a 14.400 bps
- ✓ V.27ter publicada en 1988, Grupo III a 2.400 bps y 4.800 bps
- ✓ V.29 publicada en 1988, Grupo III a 7.200 bps y 9.600 bps

Además todos los módems cumplen la recomendación V.25 donde se especifica la forma de establecer y finalizar una conexión. Por ejemplo, se especifica de forma precisa cómo se tiene que establecer la conexión:

- ✓ El módem llamante emite un tono de 1.300 Hz durante 0'5 segundos alternando con silencios de 2 segundos.
- ✓ El módem destino responde con un tono de 2.000 Hz durante 3 segundos con lo que queda establecido el enlace.

6.4 COMANDOS HAYES

Prácticamente todos los módems actualmente los incorporan. Son un conjunto de instrucciones software que el módem es capaz de reconocer y ejecutar. Fueron desarrollados por el fabricante *Hayes Microcomputer Products* y se ha convertido en un estándar de facto. Las funciones de los comandos Hayes son, principalmente:

- ✓ Gestión de la llamadas, salientes, entrantes, reintentos
- ✓ Selección de la velocidad de transmisión
- ✓ Configuración del módem
- ✓ Mantenimiento

Salvo alguna excepción, todos los comandos Hayes empiezan por los caracteres AT, por eso también reciben el nombre de comandos AT. Los comandos AT son enviados desde el DCE, es decir, desde el ordenador en el que está conectado el módem. Estos comandos pueden ser enviados por un usuario con un programa de comunicaciones apropiado o pueden ser gestionados directamente por el software de red, con lo cual su uso es transparente al usuario.

Los módems que soportan los comandos Hayes tienen dos modos de funcionamiento:

Modo comando

Es el modo en el que se inicia el módem. En este modo, cualquier dato que se envíe del ordenador al módem será interpretado como un comando. El módem responde a los comandos enviando el mensaje correspondiente:

- OK si ejecuta el comando correctamente.
- ERROR si no reconoce el comando.
- CONNECT si el módem consigue establecer conexión con el módem remoto.
- RING indica que se está produciendo una llamada entrante.
- NO CARRIER indica que la línea telefónica no está activa.
- NO ANSWER indica que no se establece comunicación porque el equipo remoto no contesta la llamada.
- BUSY indica que no se establece la comunicación porque el equipo remoto tiene la línea ocupada.

Modo conectado

Después de un comando de marcación, por ejemplo, el comando ATD, si el módem consigue establecer la comunicación responde con el mensaje CONNECT. A partir de ese momento se pasa al modo conectado u on-line, por tanto, todo lo que el módem reciba del ordenador se envía al módem remoto.

En la siguiente tabla se especifican algunos de los comandos AT más comunes:

Tabla 6.1

Comando AT	Descripción
ATA	Responde una llamada entrante
ATDT *número*	Realiza la marcación del número por tonos
ATDP *número*	Realiza la marcación del número por pulsos
ATE0	Deshabilita el eco de los comandos
ATE1	Habilita el eco de los comandos
ATH	Cuelga la línea y finaliza la llamada
ATI	Obtener información del módem
ATI0	Información sobre el código del módem
ATI3	Información sobre la versión del módem
ATI4	Información de las prestaciones del módem
ATM0	Desactiva el altavoz del módem
ATM1	Activa el altavoz del módem hasta que detecte portadora
ATM2	Altavoz siempre conectado
ATZ	Restablece la configuración por defecto
+++	Código de escape para pasar al modo comando desde el modo conectado
ATO	Vuelve al modo conectado desde el modo comando

Además, los módems implementan una serie de registros internos donde se almacena información de configuración que puede ser consultada y modificada por medio de comandos AT. Dichos comandos son los siguientes:

Tabla 6.2

ATSn?	Pregunta por el valor del registro n
ATSn=x	Almacena el valor x en el registro n

A continuación se explica el contenido de algunos de estos registros:

Tabla 6.3

S0	Número de tonos que deben producirse antes de que el módem descuelgue
S1	Almacena el número de tonos de llamada que se producen
S2	Contiene el carácter de escape en ASCII, por defecto almacena el 43 (carácter +)
S6	Tiempo de espera desde que el módem descuelga la línea hasta que comienza la marcación
S7	Tiempo de espera de la portadora del módem remoto. Pasado ese tiempo el módem cuelga la línea y devuelve la cadena NO CARRIER
S12	Tiempo de retardo para la introducción de la secuencia de escape para pasar a modo comando desde modo conectado

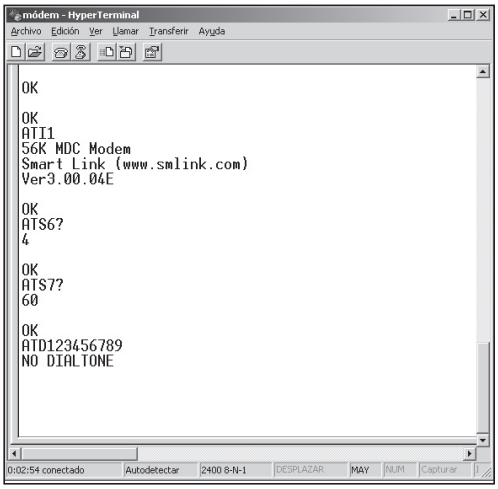


Figura 6.4. *La aplicación Hyperterminal de Windows ejecutando comandos Hayes.*

6.5 ESTÁNDAR Y EVOLUCIÓN DE LOS MÓDEMS

La posibilidad de utilizar la Red Telefónica Conmutada (RTC) para comunicar dos ordenadores surgió a finales de los años 50.

Fue la empresa norteamericana *AT&T* la que desarrolló los primeros modelos de módems a través de su filial de investigación y desarrollo *Bell Telephone Laboratories Inc.* (también conocida como *Bell Labs* y actualmente propiedad de *Lucent Technologies*).

El primer modelo fue conocido como **Bell 103** y se lanzó en 1960. Los modelos desarrollados en Bell se convirtieron durante los primeros años en estándares gracias al control que ejercía AT&T sobre el sistema telefónico norteamericano. De hecho, los primeros estándares publicados por el CCITT (actualmente denominado ITU-T) están basados en los primeros modelos de Bell.

Así ocurre con el primer estándar de la ITU-T llamado **V.21**, el cual está basado en el modelo Bell 103. Se consigue una velocidad de transmisión de 300 bps full-dúplex sobre líneas conmutadas de 2 hilos, utilizando modulación FSK.

El siguiente modelo desarrollado por AT&T fue el **Bell 202** y se utilizó como referencia para la recomendación **V.23** de la ITU-T. Éste era un módem half-dúplex que alcanzaba una velocidad de transmisión de 1.200 bps través de líneas conmutadas de 2 hilos, utilizando modulación FSK.

El modelo de AT&T llamado **Bell 212** fue adoptado por la ITU-T como **V.22**. Tiene dos velocidades, la más baja, a 600 bps, utiliza modulación FSK y la más alta, a 1.200 bps, utiliza modulación 4-PSK y transmite en modo full-dúplex.

La recomendación **V.26** basada en el modelo de AT&T **Bell 201** utiliza una sola frecuencia portadora por canal, modulando con 4-PSK y con una tasa de modulación de 1.200 baudios. Con ello se obtiene una velocidad de 2.400 bps en half-dúplex sobre líneas a 2 hilos o en full-dúplex en líneas a 4 hilos.

A continuación se muestra una tabla que resume las características de todas las recomendaciones sobre especificaciones de módems:

Tabla 6.4

Norm.	Nbaud.	Nbits	T.Explo.	Modulación	Línea	Fecha	Observaciones
V.21	300	300	Full	FSK	2H	1960	Equivale a Bell 103
V.22	600	600 1200	Full	FSK PSK-4	2H	1980	Equivale a Bell 212
V.23	1200	1200	Half	FSK	2H	1964	Equivale a Bell 202
V.26	1200	2400	Half Full	4-PSK	2H 4H	1970	Equivale a Bell 201
V.27	1600	4800	Full	8-PSK	4H	1984	
V.29	2400	9600	Full	16-QAM	4H	1976	
V.32	2400	9600	Full*	32-QAM	2H	1984	Primera en utilizar cancelación de eco y TCM
V.32bis	2400	14400	Full* Full	QAM/TCM	2H 4H	1991	
V.33	2400	14400	Full*	128-QAM	4H	1988	
V.34	2400 3429	28800 33600	Full*	TCM	2H 4H	1994	
V.90		33600 56000	Full*	TCM	2H	1998	

*Full-dúplex por cancelación de eco.

6.6 RECOMENDACIÓN V.32

La técnica de transmisión full-dúplex con cancelación de eco se introdujo por primera vez en la recomendación V.32.

El sistema telefónico utiliza dos hilos para transportar las señales de los dos sentidos de la comunicación. Esto se lleva a cabo gracias a las bobinas híbridas, las cuales son capaces de separar las señales de ambos sentidos en el receptor.

Como la adaptación de estas bobinas a la línea de transmisión no es perfecta (impedancia teórica de 600 ohmios) se producen reflexiones de la señal de salida a la entrada y esto produce un efecto denominado eco. Este efecto, para la comunicación vocal, no es perjudicial si el nivel de la señal reflejada no es muy elevado. Sin embargo, para la transmisión de datos éste es un efecto indeseable que produce errores en la demodulación. Para evitar este efecto, las transmisiones

full-dúplex utilizan dos portadoras separadas, es decir, se multiplexan los dos sentidos de la comunicación.

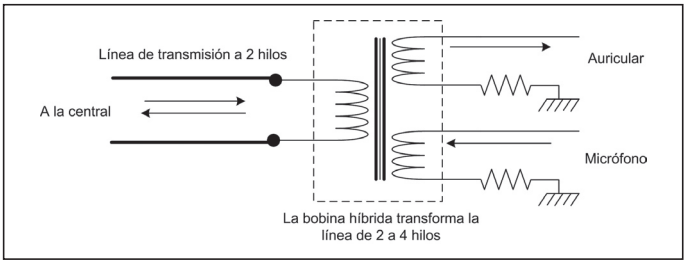


Figura 6.5. *Bobinas híbridas en el sistema telefónico.*

Con las técnicas de cancelación de eco se consigue transmitir en los dos sentidos a través de una línea a 2 hilos sin necesidad de multiplexar los dos sentidos de la comunicación y con el consiguiente aumento de ancho de banda disponible.

En las recomendaciones V.32 y V.33 se utiliza codificación **TCM (Modulación codificada trellis)**. TCM está basado en QAM pero una parte de los bits enviados en cada unidad de señal (símbolo) son bits de redundancia no utilizados como datos sino para ofrecer un mecanismo de detección y corrección de los errores de transmisión. En el caso de la V.32 se envían 4 bits de datos y 1 bit de redundancia.

6.7 RECOMENDACIÓN V.34

Utiliza modulación TCM. Se lleva a cabo una transmisión full-dúplex con cancelación de eco. Esta recomendación admite varias combinaciones de tipo de modulación con velocidades de modulación por lo que se establece un período de negociación de la velocidad. Las diferentes velocidades (en baudios) son: 2.400, 2.743, 2.800, 3.000, 3.200 y 3.429.

Las velocidades superiores a 2.400 se consiguen aumentando el ancho de banda utilizado para la transmisión. Por ejemplo, para la velocidad más alta de 3.429, se utiliza el rango de frecuencias de 244 Hz a 3.674 Hz.

Por tanto, en función de las velocidades de modulación anteriores esta norma admite varias velocidades de transmisión. La más alta utiliza una modulación TCM con 8'4 bits/baudio. Se puede obtener la velocidad de transmisión multiplicando el número de bits/baudio por la velocidad de modulación:

$$3429*8'4 = 28.803 \text{ bps} = 28.800 \text{ bps}$$

En el año 1996 se especifica la norma V.34+ que mantiene la tasa de baudios pero utiliza la técnica de modulación TCM hasta 9'8 bits/baudio, por tanto su velocidad de transmisión será:

$$3429*9'8 = 33.604 = 33.600 \text{ bps}$$

6.8 MÓDEMS DE 56K: NORMA V.90

La limitación de velocidad de la norma V.34 viene dada por la forma en que se transmiten las señales a través de la red telefónica. Como ya se ha dicho, actualmente sólo el bucle local de abonado es analógico. El resto de la red telefónica es digital. Esto significa que cuando la señal llega a la central, se convierte a digital utilizando PCM con una frecuencia de muestreo de 8.000 muestras/s y 8 bits/muestra. De esto resulta una tasa de bits de la señal digitalizada de 64 Kbps.

En la conversión PCM se lleva a cabo la cuantificación de la señal, lo que produce el llamado error de cuantificación o **ruido de cuantificación** que hace que al recuperar la señal analógica mediante PCM inversa, la señal que se obtiene no sea igual a la señal original (para más detalles sobre PCM ver el capítulo 2).

Podemos aplicar la fórmula de Shannon para calcular la capacidad máxima de un canal en bps teniendo en cuenta el ruido de cuantificación:

$$C = BW * \log_2 (1 + S/N)$$

La relación entre la señal y el error de cuantificación en las líneas telefónicas es habitualmente 3.162. Por tanto se obtiene:

$$C = 3000 * \log_2 (3.163) = 3000 * 11{,}62 = 34.860 \text{ bps}$$

Por tanto, la capacidad máxima del canal telefónico teniendo en cuenta el error de cuantificación es de 34.860 bps. Como hemos visto, la norma V.34 sitúa el límite real en 33.600 bps que será la velocidad máxima de transmisión debida al error de cuantificación que se introduce al llevar a cabo la conversión analógica-digital en la central telefónica.

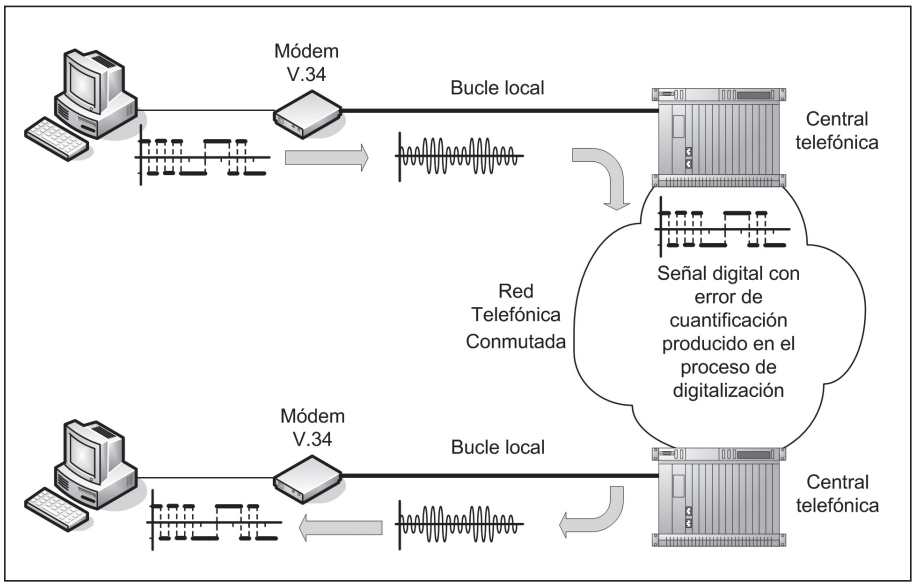


Figura 6.6. *Comunicación entre módems V.34.*

V.90 es un estándar de transmisión de datos a través de líneas analógicas desarrollado por el ITU-T y publicado en febrero de 1998 que permite velocidades de 56 Kbps en la recepción del usuario. Utiliza como técnica de modulación **TCM (Modulación codificada trellis)**.

Un proveedor de servicios de Internet o **ISP (Internet Service Provider)** está implementado de forma totalmente digital, por tanto, la conexión entre el ISP y la red telefónica es digital y no se realiza ninguna conversión PCM, por tanto, en el sentido ISP-usuario no se produce error de cuantificación y se puede aumentar la tasa de bits.

Sin embargo en sentido usuario-ISP la velocidad de transmisión seguirá estando limitada a los 33'6 Kbps debido al error de cuantificación que introduce la central a la que se conecta el usuario.

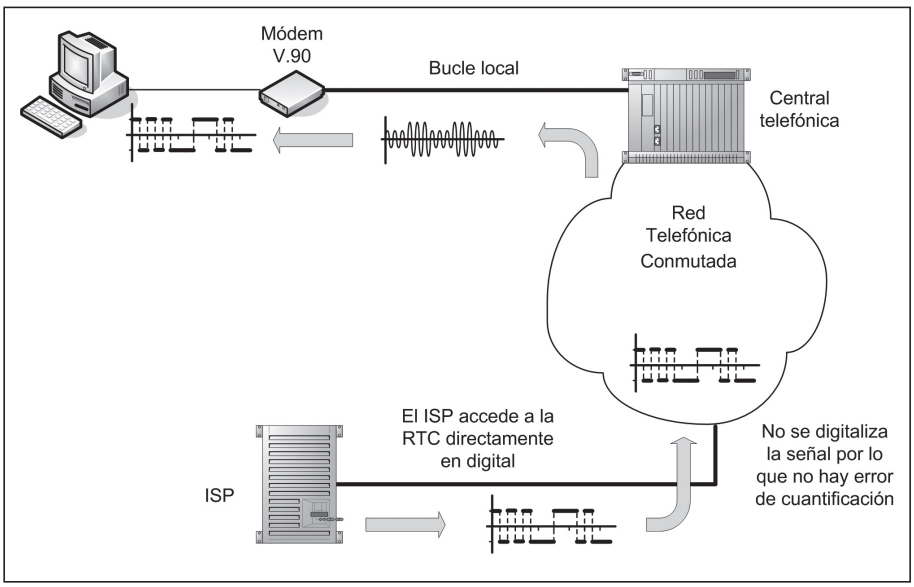


Figura 6.7. *Comunicación mediante módem V.90.*

Cabría pensar que en este caso no existe una limitación en la tasa de transmisión, pero lo cierto es que sí. Como ya se ha visto, la señal digital se transmite a través de la red telefónica a una velocidad de 64 Kbps que es consecuencia de la conversión PCM, con lo que ésta sería en teoría la velocidad máxima. Sin embargo, en la conversión PCM se utiliza una cuantificación no uniforme con el objeto de mejorar la cuantificación para señales vocales, de forma que los niveles del cuantificador no uniforme están muy juntos para niveles bajos de amplitud.

Esto es así porque el ruido es más molesto cuando la señal de voz presenta poca amplitud que cuando la amplitud es elevada, puesto que en este último caso el ruido queda enmascarado por la propia señal de voz y el oído humano lo apre-

cia menos. Esta característica resulta negativa a la hora de transmitir datos, puesto que interesa que los niveles de amplitud estén lo más separados posible a efectos de inmunidad frente al ruido. Además, algunos de los bits menos significativos de cada muestra son usados para varias funciones internas de la red telefónica. Por ello, para la transmisión de datos se usan únicamente 7 bits por muestra y, por tanto, la tasa de bits es 8.000 muestras/s * 7 bits = 56.000 bps.

Por tanto, los módems que cumplen la norma V.90 sólo aprovechan esta característica si uno de los componentes de la comunicación está usando una conexión digital con la central, normalmente éste será un ISP.

Como se puede observar, los módems 56 K son módems asimétricos ya que la velocidad de transmisión es diferente para cada sentido de la comunicación 33.600 bps en sentido usuario-ISP y 56.000 bps sentido ISP-usuario.

6.9 LA EVOLUCIÓN: MÓDEM ADSL

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

Actualmente el desarrollo de las redes digitales así como el uso de nuevas tecnologías como ADSL y cable han propiciado que en muchos casos los módems tradicionales hayan dejado de utilizarse. Además, la velocidad de transmisión de datos utilizando dichos módems había alcanzado techo con la recomendación V.90.

En el capítulo 2 se estudió la tecnología ADSL utilizada para aprovechar todo el ancho de banda que ofrece el bucle local de abonado y multiplexar las señales de voz y datos. De esta forma, la tecnología ADSL ofrece lo que se conoce comúnmente como acceso de banda ancha a las redes de datos, especialmente Internet. El inconveniente de esta tecnología es que requiere la adaptación de las infraestructuras de comunicaciones de los operadores, además su uso depende de un factor importante que es la longitud del bucle de abonado, siendo imposible su uso para distancias mayores a 5 Km.

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

Lógicamente, para hacer uso de la tecnología ADSL es necesario utilizar un módem diseñado a tal efecto. Los módems ADSL, al igual que los módems de

banda vocal, pueden ser internos o externos aunque la mayor parte de los que se han comercializado son externos. A diferencia de los módems de banda vocal, los módems ADSL externos utilizan la interfaz USB para su conexión con el DTE (ordenador) debido sobre todo a las velocidades más altas que se alcanzan con esta interfaz.

Como ya se vio en el capítulo 2, ADSL utiliza modulación DMT en la que se divide el ancho de banda disponible en canales, y en cada uno de los canales se modula una subportadora utilizando QAM. Los estándares que se han desarrollado para la tecnología ADSL son los siguientes:

Tabla 6.5

ANSI T1.413	Especificación de ADSL en ANSI, el organismo de estandarización americano
ITU G.992.1	Especificación de ADSL igual que el anterior pero de la ITU-T, también se llama G.DMT. Se publica en 1999
ITU G.992.2	Especificación de ADSL de baja velocidad
ITU G.992.3	Especificación de ADSL2
ITU G.992.4	Especificación de ADSL2
ITU G.992.5	Especificación de ADSL2+ (o ADSL2Plus). Publicada en enero de 2003
ITU G.998.1	Especificación de Bonded ADSL2. Publicada en enero de 2005
ITU G.993.2	VDSL2. Publicada en mayo de 2005

El uso de módems ADSL permite el uso simultáneo del servicio telefónico convencional ya que, como se vio en el capítulo 2, se utilizan las frecuencias más altas del ancho de banda del par trenzado por lo que no interfiere con la señal vocal. Lo único a tener en cuenta es la colocación de unos sencillos dispositivos conocidos como **filtros o splitter** entre el acceso a la red telefónica y los dispositivos que utilicen el canal vocal como los terminales telefónicos o los módems RTC. Estos

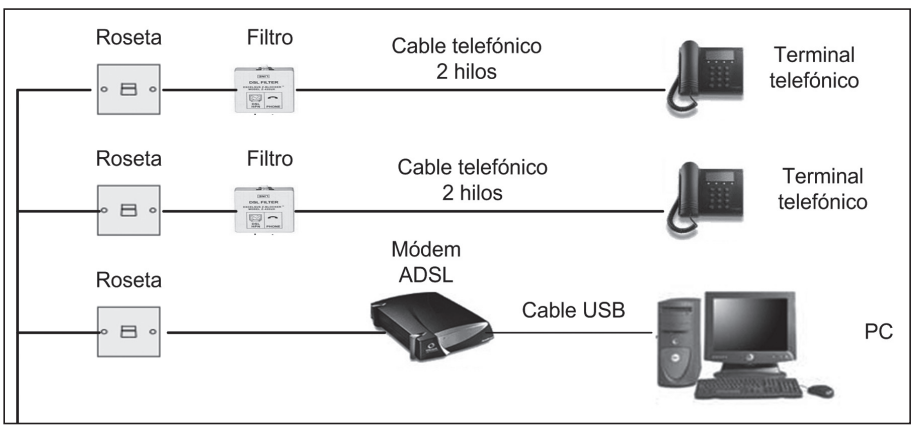


Figura 6.8. *Conexión de un módem ADSL utilizando filtros.*

filtros son realmente filtros paso-bajo que permiten el paso sólo de las frecuencias vocales hacia y desde el teléfono (o el módem RTC). Los módems ADSL incluyen internamente un filtro paso-alto para descartar la banda vocal de los datos.

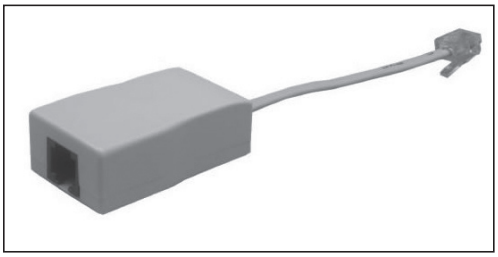


Figura 6.9. *Filtro para su uso en líneas ADSL.*

Actualmente, los operadores que dan acceso a Internet a través de tecnología ADSL proporcionan como dispositivo de conexión un router ADSL. Dicho dispositivo proporciona funciones de enrutamiento entre la red del ISP y la red del usuario y lógicamente incluye las funciones de módem ADSL.

Figura 6.10. *Módem ADSL.*

6.10 MÓDEM DE CABLE

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

Los operadores de cable han ofrecido tradicionalmente servicios de televisión por cable utilizando una infraestructura conocida como CATV basada en el cable coaxial. Sin embargo, la modernización de estas infraestructuras ha permitido a dichos operadores proporcionar servicios de datos bidireccionales, especialmente el servicio de conexión a Internet. La arquitectura de red utilizada actualmente por los operadores de cable se conoce como **HFC (Hybrid Fiber Coaxial, Híbrido de fibra y coaxial)** en la cual se combina la fibra óptica y el cable coaxial para la transmisión de los datos. Normalmente la red troncal del operador está constituida por fibra óptica y se utiliza el cable coaxial para la acometida a los usuarios finales.

El acceso a la red troncal del operador normalmente se hace desde un punto de acceso común a los usuarios de una zona determinada, por lo tanto, el ancho de banda está compartido entre dichos usuarios. Esta característica podría ser un potencial problema cuando hay muchos usuarios conectados a un mismo punto de acceso, aunque actualmente los operadores de cable suelen dimensionar correctamente su infraestructura para garantizar a los usuarios el ancho de banda contratado.

Tanto la señal de televisión como la de datos viaja en formato digital a través de la red del operador, sin embargo, en el tramo final de cable coaxial la señal es analógica y, por lo tanto, la función del módem de cable es extraer el canal de datos de la señal que llega al punto de acceso del usuario y convertirlo en digital.

El funcionamiento de la mayor parte de los módems de cable se basa en un estándar conocido como **DOCSIS (Data Over Cable Service Interface Specification, Especificación de interfaz sobre servicios de datos por cable)**. Para Europa este estándar tiene algunas variaciones y se conoce como **EuroDOCSIS**.

La primera especificación de DOCSIS se publicó en 1997 y fue aprobado por la ITU-T en 1998. La versión 2.0 de DOCSIS se publicó en 2002, y la última versión, la DOCSIS 3.0, se ha publicado en 2006.

DOCSIS especifica el uso de canales de 6 MHz para transportar señales de televisión NTSC, mientras que en EuroDOCSIS se utiliza canales de 8 MHz para transportar señales de televisión PAL. Uno de estos canales se utiliza para datos en sentido descendente (también conocido como downstream), es decir, del operador al usuario. Por tanto el ancho de banda disponible para datos de bajada es de 6 MHz (DOCSIS) o de 8 MHz (EuroDOCSIS). Para los datos ascendentes (también conocido como upstream), es decir, del usuario al operador, se utiliza la banda de frecuencia para la comunicación usuario-operador. Las bandas de frecuencia utilizadas en DOCSIS y EuroDOCSIS se pueden ver en la siguiente figura:

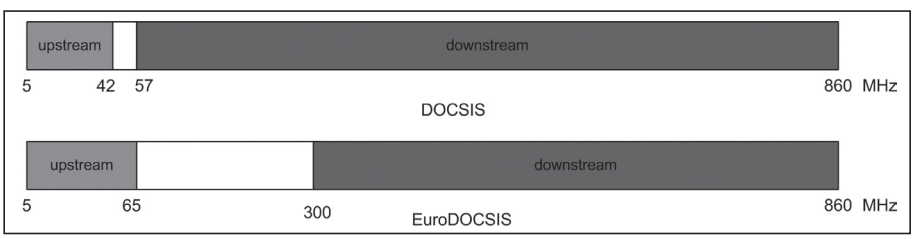


Figura 6.11. *Bandas de frecuencia utilizadas en DOCSIS.*

La velocidad de transferencia de datos depende de la modulación utilizada. En la versión 1.0 de DOCSIS se especifica la utilización de 64-QAM o 256-QAM para el sentido bajada, y QPSK o 16-QAM para el sentido subida. En la versión 2.0 se puede utilizar además, 64-QAM en sentido subida. En las siguientes tablas se resumen las velocidades de transferencia alcanzada para todas las posibles configuraciones:

Tabla 6.6 Tasas de transmisión en sentido bajada (downstream) en Mbps

	64-QAM	256-QAM
6 MHz	30'34	42'88
8 MHz	40'44	57'20

Tabla 6.7 Tasa de transmisión en sentido subida (upstream) en Mbps

	QPSK	16-QAM	64-QAM
0'2 MHz	0'32	0'64	1'28
0'4 MHz	0'64	1'28	1'92
0'8 MHz	1'28	2'56	3'84
1'6 MHz	2'56	5'12	7'68
3'2 MHz	5'12	10'24	15'36
6'4 MHz	10'24	20'48	30'72

La modulación 64-QAM en sentido subida y el ancho de banda de 6'4 MHz están definidos a partir de la versión 2.0 de DOCSIS.

La mayor parte de los módems de cable utilizan un conector BNC para el cable coaxial que conecta el módem a la red del operador. Para conectar el módem de cable al PC del usuario se suele incluir un conector USB o RJ-45.

Figura 6.12. *Módem de cable.*

6.11 PRÁCTICA

El objetivo de esta práctica es comprobar el funcionamiento de un módem tradicional de banda vocal, conocido como **módem RTC**.

6.11.1 MATERIAL NECESARIO POR PUESTO

- ✓ 1 Ordenador con Windows 98/2000/XP que disponga de un puerto serie
- ✓ 1 Módem RTB externo
- ✓ 1 Cable EIA-232 para conectar el módem al ordenador
- ✓ 1 Línea telefónica operativa
- ✓ Conexión a Internet

6.11.2 DESARROLLO DE LA PRÁCTICA

1. Buscar información en Internet sobre tres modelos diferentes de módem RTC e incluir en la memoria las características técnicas, modo de configuración, modo de utilización y precios.
2. Buscar información en Internet sobre el protocolo V.92. ¿Qué ventajas añade esta nueva especificación respecto a la especificación V.90?
3. Instalar y configurar un módem externo en el PC del aula. Incluir en la memoria las características más relevantes del módem utilizado, el procedimiento seguido para su instalación, así como cualquier incidencia producida.
4. Utilizando un programa de comunicaciones (por ejemplo, el programa Hyper Terminal incluido en sistemas Windows), intentar el envío de comandos Hayes al módem. Incluir los resultados en la memoria.
5. Configurar una conexión a un proveedor gratuito de Internet utilizando el módem. Comprobar que funciona correctamente y explicar los pasos seguidos. Obtener la tarificación de la llamada al ISP.

6.11.3 APARTADO OPCIONAL

6. Comprobar si el módem utilizado para la práctica tiene soporte de fax. Si es así instalar y configurar el PC para el envío y la recepción de faxes. Comprobar su funcionamiento.

RESUMEN DEL CAPÍTULO

En este capítulo se ha estudiado uno de los dispositivos de transmisión de datos más utilizado históricamente: el módem. Este dispositivo se ha utilizado durante más de 30 años para conectar dispositivos digitales de forma remota utilizando las infraestructuras de la red telefónica.

Se hace un repaso de sus principales características así como de su evolución reflejada en la aparición de los distintos estándares de la ITU-T, dedicando más atención a los más actuales como V.32, V.34 y V.90.

El techo de velocidad alcanzada con los módems RTC está en la V.90 con 56 Kbps. Para poder aumentar esta velocidad se ha recurrido a tecnologías alternativas como las redes de televisión por cable y ADSL (cuyo funcionamiento se ha expuesto en el capítulo 2). En la última parte del capítulo se repasan las principales características de los módems de última generación, los módems ADSL y los módems de cable, que permiten el acceso a redes de datos a alta velocidad.

TEST DE CONOCIMIENTOS

1 La tasa de datos máxima de un módem 2-PSK half-dupléx usando dos cables de la línea telefónica normal es:

a) 1.200 bps.
b) 2.400 bps.
c) 3.600 bps.
d) Ninguna de las anteriores.

2 La tasa de bits de un módem que transmite modulando en 16-QAM, 2.400 baudios en full-dúplex y a 4 hilos es de:

a) 1.200 bps.
b) 2.400 bps.
c) 4.800 bps.
d) 9.600 bps.

3 La tasa de datos máxima en una conexión entre dos módems V.90 es de:

a) 33'6 Kbps.
b) 56 Kbps.
c) 28'8 Kbps.
d) Depende del usuario que establece la comunicación.

4 ¿Cuál es el objetivo de la codificación TCM?
- **a)** Disminuir el ancho de banda.
- **b)** Simplificar el proceso de modulación.
- **c)** Aumentar las tasa de bits.
- **d)** Reducir la tasa de errores.

5 La técnica de cancelación de eco permite:
- **a)** Transmitir datos y voz simultáneamente por la línea telefónica.
- **b)** Utilizar el mismo rango de frecuencias para los dos canales ida y retorno.
- **c)** La compatibilidad de los módems más antiguos.
- **d)** Esta técnica no se utiliza para datos sólo para voz.

6 La tasa de datos de un módem depende:
- **a)** Del interfaz DTE-DCE.
- **b)** Del tipo de modulación empleada.
- **c)** De la velocidad del extremo opuesto de la comunicación.
- **d)** Todas las anteriores son correctas.

7 Un módem de 56K puede enviar datos a:
- **a)** 56 Kbps.
- **b)** 33,6 Kbps.
- **c)** 128 Kbps.
- **d)** 14,4 Kbps.

8 ¿Cuál de las siguientes afirmaciones sobre los módems de cable es falsa?
- **a)** Los canales de subida y bajada utilizan diferente velocidad.
- **b)** La mayoría siguen la especificación DOCSIS o EuroDOCSIS.
- **c)** Utilizan una interfaz serie EIA-232 o USB para su conexión al PC.
- **d)** Utilizan modulación QAM en sentido bajada y utilizan QAM y QPSK en sentido subida.

9 Para realizar una conexión a través de un módem RTC es necesario:
- **a)** Simplemente conectar el módem al PC.
- **b)** Ejecutar manualmente los comandos AT correspondientes.
- **c)** Configurar la aplicación de comunicaciones correspondiente.
- **d)** Las dos anteriores son válidas.

10 ¿Sería posible utilizar simultáneamente los tres tipos de módem: RTC, de cable y ADSL en una misma demarcación?
- **a)** No, imposible.
- **b)** Sí, si hay cobertura ADSL y cobertura de cable.
- **c)** No, sólo pueden compatibilizarse el módem ADSL y el de cable.
- **d)** No, sólo pueden compatibilizarse el módem ADSL y RTC.

7 Redes de área local (LAN)

Objetivos del capítulo

- ✓ Entender las funciones de los estándares IEEE para redes locales.
- ✓ Conocer las principales características de las redes Ethernet así como su evolución hacia las redes Fast Ethernet y Gigabit Ethernet.
- ✓ Diferenciar los modos half-dúplex (CSMA/CD) y full-dúplex en redes Ethernet.
- ✓ Conocer el estándar IEEE 802.11 o Wi-Fi para redes inalámbricas.
- ✓ Conocer la existencia de otras tecnologías LAN como Token Ring y FDDI.
- ✓ Estudiar los diferentes equipos de interconexión especialmente los más utilizados en las redes LAN actuales, los switches o conmutadores.

7.1 INTRODUCCIÓN

Las Redes de Área Local, también conocidas como **LAN (Local Area Network)**, son redes telemáticas formadas por un conjunto de dispositivos (generalmente ordenadores) interconectados entre sí en una área de extensión limitada. Esta área puede abarcar desde una sala de unas decenas de metros cuadrados, hasta la extensión ocupada por varios edificios próximos entre sí.

Las condiciones de diseño de las redes de área local son principalmente dos:

- La utilización de conexiones de alta velocidad pero con una baja tasa de errores.
- Proporcionar interconexión de dispositivos autónomos a nivel de comunicación. Esto último no impide el uso de servicios de tipo cliente-servidor en los niveles superiores, generalmente en el nivel de aplicación.

Actualmente, nadie pone en duda las ventajas que se generan al interconectar equipos próximos entre sí o que pertenezcan a una misma unidad organizativa en un edificio (o varios próximos entre sí). Desde pequeñas oficinas, naves o talleres hasta grandes empresas con cientos o miles de empleados, se utilizan las tecnologías de las redes LAN para interconectar sus equipos y aprovecharse de todas las ventajas que ello supone, principalmente el uso compartido de ficheros, impresoras y otros periféricos, así como el acceso a Internet, el acceso a aplicaciones corporativas...

Incluso cada vez son más frecuentes los hogares donde montan sus redes LAN a pequeña escala, con dos o tres ordenadores, una impresora y un router de acceso a Internet.

Salvo alguna excepción, el diseño de las diferentes arquitecturas LAN se centra en la definición de las funciones de los niveles físico y de enlace. En este capítulo haremos un repaso a las principales tecnologías utilizadas en la implementación de redes de área local.

- **Ethernet (IEEE)**
- Bus con paso de testigo (Token Bus) (IEEE)
- Red en anillo con paso de testigo (Token Ring) (IEEE)
- **Red inalámbrica Wi-Fi (IEEE)**
- FDDI: interfaz de datos distribuidos de fibra (ANSI)

Como se indica entre paréntesis, los cuatro primeros tipos de la lista anterior fueron especificados por la organización IEEE mientras que el último tipo fue desarrollado por el ANSI. Actualmente los únicos estándares de redes LAN que están vigentes son Ethernet y Wi-Fi.

NOTA 7.1

Las arquitecturas LAN implementan las funciones de los niveles físico y de enlace.

7.2 ESTÁNDARES IEEE

El impulso a las tecnologías LAN se dio cuando la organización IEEE creó en 1980 un proyecto llamado IEEE 802 cuyo objetivo era la definición de estándares para LAN. Es decir, la especificación de las funciones del nivel físico y del nivel de enlace (también, en menor medida del nivel de red). De esta forma se crearon las siguientes normas con sus respectivas funciones:

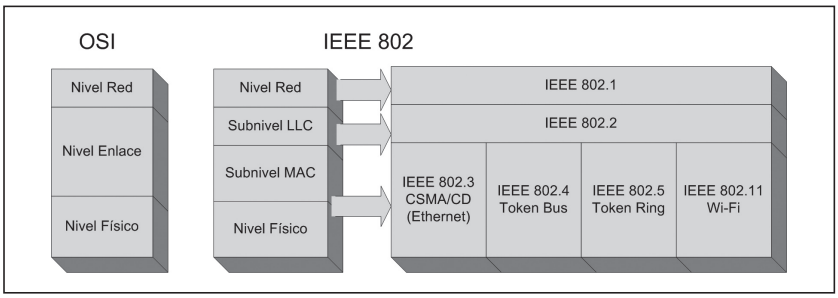


Figura 7.1. *Relación Niveles IEEE y OSI.*

Como se observa, el nivel de enlace en las redes LAN definidas por el proyecto IEEE 802 se subdivide de dos niveles, uno superior y común a todas las implementaciones LAN, llamado LLC, y otro inferior llamado MAC, que depende de cada implementación.

Nivel de enlace en redes LAN:

- **LLC (Logical Link Control)** Control de Enlace Lógico
- **MAC (Medium Access Control)** Control de Acceso al Medio

NOTA 7.2

Se pueden obtener las especificaciones de todas las redes del IEEE en la dirección:
http://standards.ieee.org/getieee802/
Eso sí, los documentos están escritos en inglés.

7.3 CONTROL DEL ENLACE LÓGICO (LLC): 802.2

El subnivel LLC (Control de enlace lógico) está definido dentro del estándar IEEE 802.2. Es el subnivel superior del nivel de enlace en todas las tecnologías LAN definidas por el IEEE. Es decir, este subnivel no depende de ninguna implementación de red concreta y es común a todas ellas.

La principal función de este subnivel es proporcionar un formato único de datos y una interfaz común al nivel superior, es decir, al nivel de red. De esta forma

se esconden al nivel de red las diferencias de formatos en los diferentes tipos de redes LAN. LLC proporciona servicios basados en datagramas, tanto orientados a conexión como no orientados a conexión

La unidad de datos del nivel LLC se denomina Unidad de datos del protocolo o **PDU (Protocol Data Unit)** y su estructura está basada en la estructura de una trama HDLC.

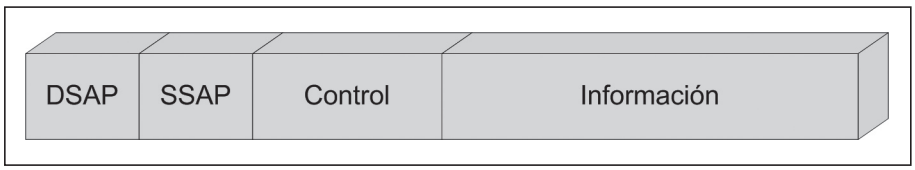


Figura 7.2. *Formato de trama LLC.*

- **DSAP (Destination Service Access Point, Punto de acceso al servicio en destino).** Contiene la dirección del punto acceso al servicio al que va dirigida la información del campo de datos. Esta dirección es un número que identifica la pila de protocolos que deberá recoger la trama LLC.
- **SSAP (Source Service Access Point, Punto de acceso al servicio en origen).** Contiene la dirección del punto de acceso al servicio desde el que se originó la trama LLC. Esta dirección es un número que identifica la pila de protocolos que genera la trama LLC.
- **Control.** El formato de este campo es el mismo que HDLC. Puede haber tramas I, S o U.
- **Información.** Contiene los datos del nivel superior, normalmente el nivel de red.

Los identificadores para los campos SSAP y DSAP son asignados por el IEEE. Algunos ejemplos de identificadores SAP son:

Pila de protocolos	SAP
IBM SNA	04
IP	06
XNS	80
Banyan	BC
Novell NetWare	E0
NetBIOS	F0
X.25	7E
SNAP	AA

NOTA 7.3

XNS (Xerox Network System), Banyan o Novell NetWare son arquitecturas de red que actualmente están prácticamente en desuso.

El último identificador de la lista anterior llamado **SNAP (SubNetwork Access Protocol)** se utiliza para servicios que no tienen asignado un identificador SAP del IEEE. En este caso, el formato de trama es el siguiente:

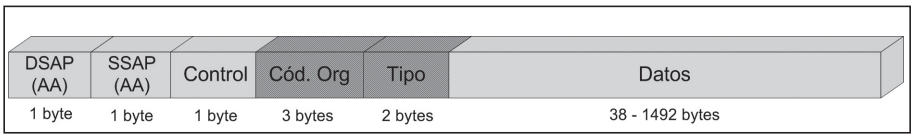


Figura 7.3. *Formato de trama LLC con SNAP (para IEEE 802.3).*

Se utiliza el código AA (1010 1010) para los campos DSAP y SSAP indicando que los puntos de acceso al servicio no tienen asignada numeración.

Después del campo de control se utilizan 3 bytes para identificar el fabricante o empresa (normalmente se deja siempre a 0) y 2 bytes que identifican el protocolo del punto de acceso.

Es importante destacar que el subnivel LLC está definido sólo en redes basadas en los estándares del IEEE. Por ejemplo, como veremos en el siguiente apartado, Ethernet no utiliza el subnivel LLC.

7.4 IEEE 802.3 Y ETHERNET

Ethernet es una tecnología para redes LAN que fue desarrollada inicialmente por la empresa Xerox en 1973 y que funcionaba a una velocidad de 2'94 Mbps. Posteriormente la colaboración entre las empresas Xerox, Intel y Digital (conocida como DIX) dio lugar a su primera versión oficial que fue publicada en 1980 donde ya se especificaba una velocidad de 10 Mbps.

Ethernet no fue un desarrollo cerrado, Xerox permitió el uso de esta tecnología mediante el pago de una pequeña cuota, de forma que cualquier empresa pudo utilizarlo, propiciando su rápida difusión. En 1982 se publicó la segunda versión de Ethernet conocida como Ethernet II. Esta versión fue la última especificada por DIX y de hecho ese mismo año Xerox liberó la marca registrada sobre el nombre Ethernet.

Es una tecnología para redes de área local donde quedan especificadas las funciones de los niveles físicos y de enlace, es decir, aspectos tales como los niveles eléctricos de las señales, tipo de medio, control de acceso al medio, topología física, formato de tramas, control de errores, control de flujo, direccionamiento...

La organización IEEE utilizó las características de Ethernet como base para desarrollar su estándar IEEE 802.3. Ambas implementaciones, aunque compatibles, no son iguales. Actualmente se utiliza la denominación Ethernet para referirse tanto a la especificación original como a la especificación IEEE 802.3.

La principal diferencia entre las implementaciones Ethernet e IEEE 802.3 es el formato de trama. En el apartado correspondiente se estudiarán dichos formatos y sus diferencias.

Como ya se adelantó en el apartado anterior, la otra diferencia importante entre redes basadas en Ethernet y redes basadas en IEEE 802.3 es que las redes basadas en Ethernet no utilizan el subnivel LLC.

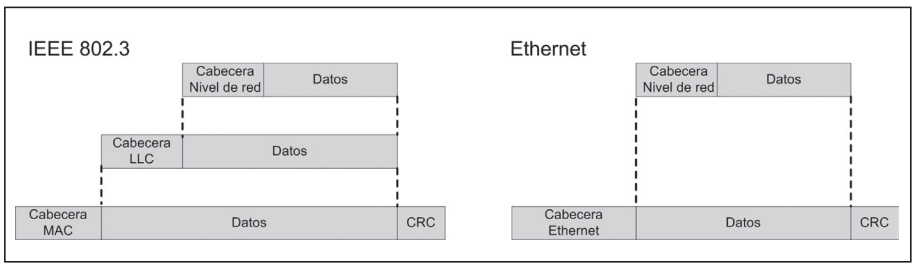


Figura 7.4. *Comparación entre Ethernet y IEEE 802.3.*

En el resto de características, ambas tecnologías son iguales y por tanto se usará el término Ethernet de forma genérica, excepto cuando se mencione alguna característica concreta de alguna de ellas, en cuyo caso se mencionará a cual se refiere.

7.4.1 PRIMERAS IMPLEMENTACIONES DEL NIVEL FÍSICO

A lo largo del tiempo y desde su primera especificación se han definido varias implementaciones físicas de redes Ethernet donde se definen aspectos del nivel físico como tipo de cableado, conectores, velocidad de transmisión y longitud máxima de los cables. Las más importantes de estas implementaciones son:

- ✓ 10BASE5
- ✓ 10BASE2
- ✓ 10BASE-T

Todas ellas trabajan a una velocidad máxima de 10 Mbps y actualmente las dos primeras se pueden considerar obsoletas ya que posiblemente no haya ninguna LAN que las utilice. A pesar de ello y para tener una perspectiva histórica de las redes Ethernet se estudiarán sus principales características.

NOTA 7.4

Existen algunas implementaciones más, como por ejemplo 10BROAD36, 1BASE5 o 10BASE-F, que tuvieron muy poca repercusión.

10BASE5 (Thick Ethernet) Ethernet de cable grueso

Esta implementación física fue la primera utilizada en redes Ethernet y se incluyó como primera implementación física publicada en el estándar IEEE 802.3 en 1983, aunque como ya se ha mencionado, hoy en día no se encuentran redes de este tipo. El nombre de la implementación indica la velocidad máxima (10 indica 10 Mbps), el tipo de transmisión (BASE indica banda base) y la longitud máxima de un segmento (5 indica 500 metros). Sus principales características se detallan a continuación:

- ✓ Utiliza una topología en bus físico, es decir, un cable como medio de interconexión común a todos los dispositivos que forman la red.

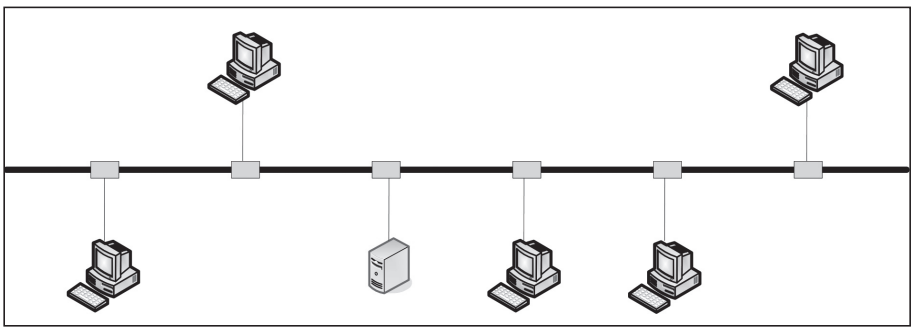


Figura 7.5. *Topología en bus de Ethernet.*

- ✓ Se utiliza cable coaxial grueso tipo RG-8 (diámetro externo de 10'2 mm) para implementar el bus físico. Aunque la norma no obliga a ello, este cable suele ser de color amarillo.
- ✓ Codificación Manchester en banda base con valores de tensión de +/- 0'85 v.
- ✓ Velocidad de transmisión de 10 Mbps.
- ✓ La longitud máxima permitida de un segmento único de cable coaxial es de 500 metros.
- ✓ La longitud máxima total de una red 10BASE5 es de 2.500 metros. Es decir, un máximo de 5 segmentos de 500 metros de longitud.
- ✓ La separación mínima entre estaciones conectadas al bus es de 2'5 metros. De hecho el cable Thick Ethernet solía incluir marcas cada 2'5 metros para indicar esta característica. Con esta limitación se pueden conectar en un segmento un máximo de 200 estaciones. En una red 10BASE5 puede haber un máximo total de 1.000 estaciones.
- ✓ Para la conexión de una estación a la red se utilizan los llamados transceptores o también **MAU (Medium Attachment Unit, Unidad de conexión al medio)**. Estos dispositivos incluían conectores de tipo vampiro para su

conexión con el cable coaxial. El conector vampiro estaba diseñado para atravesar la funda protectora del cable coaxial y establecer contacto eléctrico con el cable propiamente dicho.

- Para la conexión del transceptor a la estación se utiliza el llamado cable **AUI (Attachment Unit Interface, Interfaz de unidad de conexión)**. Dicho cable está formado de 15 hilos con conectores DB-15 y puede tener una longitud máxima de 50 metros. Por tanto, las tarjetas de red 10BASE5 incluyen un conector de 15 pines.

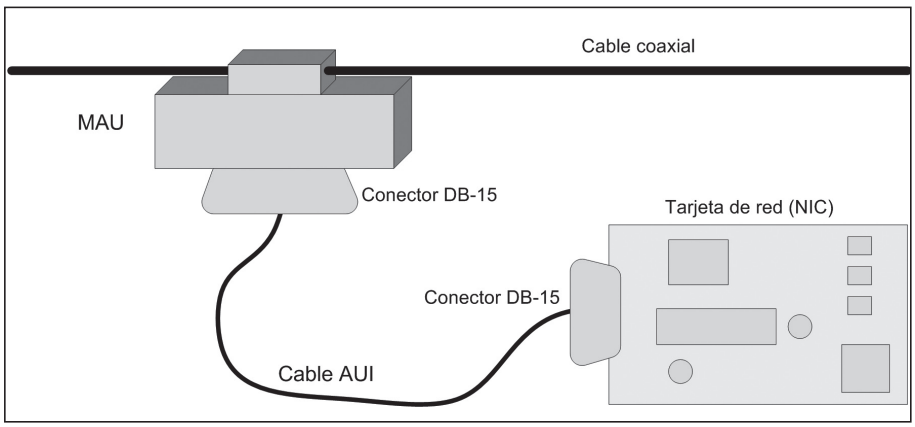


Figura 7.6. *Conexión MAU.*

10BASE2 (Thin Ethernet) Ethernet de cable fino

Esta segunda implementación de redes Ethernet, publicada por el IEEE en 1985, se desarrolló para ofrecer una alternativa a menor coste que 10BASE5. Actualmente está prácticamente en desuso. En este caso, como indica su nombre, se mantiene la velocidad y el tipo de transmisión pero se ve reducida la longitud máxima de un segmento a 200 metros (realmente se hace un redondeo para acortar el nombre, pero la longitud exacta es de 185 metros). Sus principales características son:

- Utiliza una topología en bus físico al igual que 10BASE5.
- Utiliza cable coaxial fino de tipo RG-58 (diámetro externo de 5 mm) para implementar el bus físico.
- Al igual que en 10BASE5 la velocidad de transmisión

Figura 7.7. *Conector BNC-T.*

es de 10 Mbps y se utiliza codificación Manchester en banda base con valores de tensión de +/- 0'85 v.

- ✓ La longitud máxima de un segmento es de 185 metros, con un máximo de 30 estaciones por segmento de cable.
- ✓ No se utilizan transceptores. Se conecta la estación directamente al bus utilizando un conector BNC-T, que es un conector con forma de T y con tres puertos: uno para la tarjeta de red y los otros dos para la entrada y salida del cable de red. Por tanto, las tarjetas de red 10BASE2 incluyen un conector BNC.

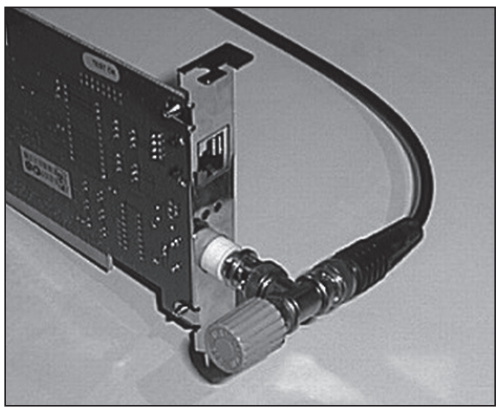


Figura 7.8. *Conexión 10BASE2.*

10BASE-T: Ethernet de par trenzado

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

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

Paralelamente al desarrollo de los estándares para redes locales se desarrollaron normativas de cableado de telecomunicaciones para edificios comerciales que permiten constituir lo que se conoce como cableado estructurado. Las primeras normas de cableado estructurado fueron publicadas como EIA/TIA 568 en 1991. Esta circunstancia propició aún más el despliegue de redes 10BASE-T. Actualmente las dos normativas más utilizadas en cableado estructurado son la EIA/TIA 568-A y la ISO/IEC 11801 publicadas en 1995.

A continuación se enumeran las principales características de 10BASE-T:

- La topología física es en estrella física aunque a nivel lógico se sigue comportando como un bus.

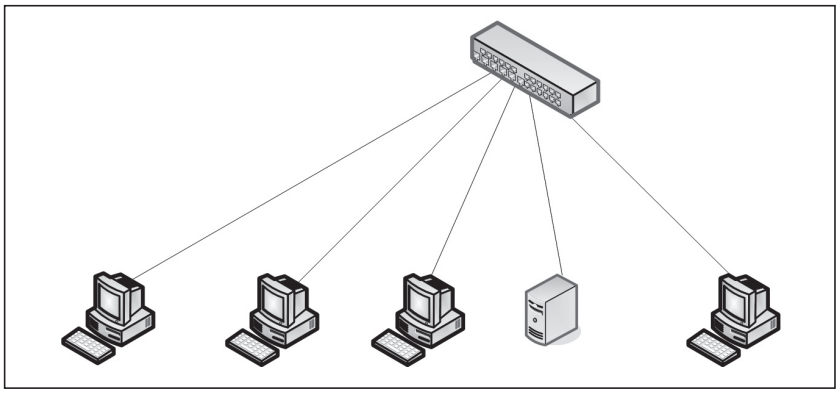


Figura 7.9. *Topología en estrella física en 10BASE-T.*

- Se utiliza cable de par trenzado sin apantallar (UTP) de Categoría 3. Las categorías de cables están definidas en la norma EIA/TIA 568.
- Los cables UTP utilizados son de cuatro pares (ocho conductores) con conectores RJ-45 en ambos extremos. De estos cuatro pares sólo se utilizan dos.

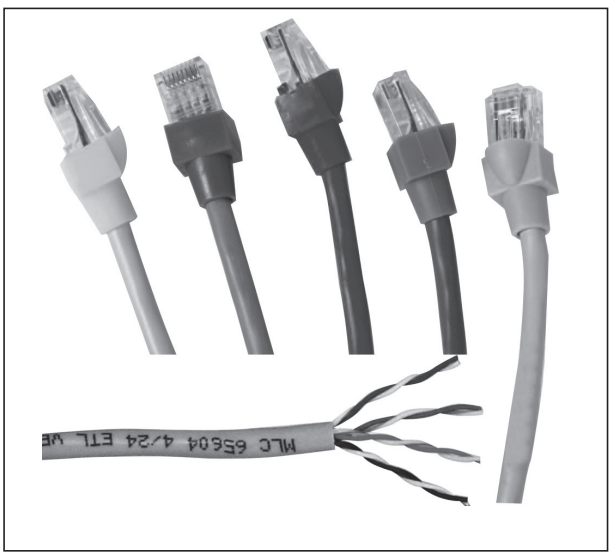


Figura 7.10. *Cable UTP con conectores RJ-45.*

- La velocidad de transmisión es de 10 Mbps.
- La codificación utilizada es Manchester en banda base con valores de tensión de +/- 5 v.

- Todas las operaciones de red se sitúan en un dispositivo de red llamado **concentrador o hub**, el cual tiene un puerto de entrada de tipo RJ-45 por cada estación. Todas las estaciones de la red se conectan al hub. En el interior del hub se implementa un bus lógico.

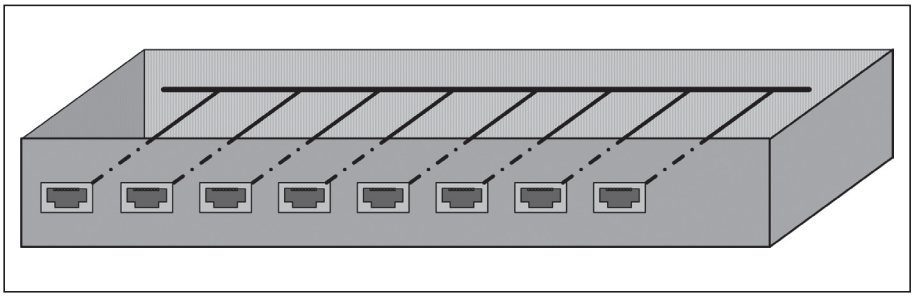


Figura 7.11. *Implementación de un bus lógico en el hub.*

- La longitud máxima del cable entre una estación y el hub es de 100 metros. Esta limitación no viene impuesta por la ventana de colisión como en los tipos 10BASE5 y 10BASE2 (se verá en los próximos apartados) si no por las características del cable de par trenzado.
- El hub retransmite todas las tramas recibidas a las estaciones que tiene conectadas. Cada tarjeta de red comprueba si la trama le pertenece comprobando la dirección de destino. Si no coincide con la dirección física la trama se desecha. Con este modo de operación la topología lógica sigue siendo en bus, ya que cualquier trama enviada por una estación se propagará por el resto de estaciones.

NOTA 7.5

El hub o concentrador es el elemento central de las redes 10BASE-T. Retransmite una trama recibida por un puerto al resto de puertos.

7.4.2 DIRECCIONAMIENTO

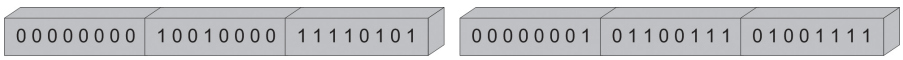
Una de las funciones que se llevan a cabo en el nivel de enlace es el direccionamiento, es decir, proporcionar un mecanismo para identificar cada equipo conectado a la red. Esta función está implementada en las propias **tarjetas de interfaz de red** (NIC, Network Interface Card) que permiten la conexión de cada equipo a la red Ethernet. Dicha tarjeta proporciona lo que se conoce como **dirección física**, que es un número binario formado por 48 bits (6 bytes). A este número también se le conoce como **dirección MAC**.

Esta dirección debe ser única para toda la red. Para conseguir esto, cada tarjeta de interfaz de red se configura de fábrica con una dirección física diferente. De esta forma se asegura que no va a haber dos tarjetas conectadas en la misma red con la misma dirección física. Los 24 bits de mayor peso los asigna el IEEE e identifica a la empresa fabricante de la tarjeta de red. Este número de 24 bits se conoce como **OUI (Organizationally Unique Identifier)**. Los 24 bits de menor peso los asigna el fabricante a cada tarjeta.

NOTA 7.6

Asignación de los 24 primeros bits a fabricantes:
http://standards.ieee.org/regauth/oui/oui.txt

Un ejemplo de dirección física podría ser el siguiente:



Asignada por IEEE — Asignada por el fabricante

Sin embargo la notación binaria es incómoda de manejar por lo que normalmente se utiliza la notación hexadecimal. En dicha notación se utilizan guiones (-) o dos puntos (:) como separadores de cada dos dígitos hexadecimales. El ejemplo anterior se representaría en formato hexadecimal de la siguiente forma:

00-90-F5-01-67-4F
ó
00:90:F5:01:67:4F

Se ha definido una dirección especial llamada **Dirección de broadcast o de difusión** utilizada para enviar una trama a todos los dispositivos de una red. Es la dirección FF:FF:FF:FF:FF:FF, es decir, todos los bits a valor 1.

La dirección física asignada por el fabricante a una tarjeta de red en el proceso de fabricación no puede ser cambiada. Sin embargo, en la actualidad existen mecanismos que permiten llevar a cabo un cambio ficticio de la dirección física por software, normalmente a través de los sistemas operativos más actuales como Windows 2000, XP o Linux. En este caso, la dirección física de la tarjeta no se altera pero los servicios de red del sistema operativo proporcionan una dirección física ficticia, es decir, enmascaran la verdadera dirección.

7.4.3 FORMATO DE TRAMA

A continuación se presenta el formato de trama especificado en el estándar IEEE 802.3:

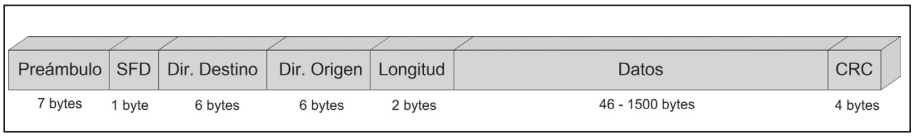


Figura 7.12. *Trama IEEE 802.3.*

- **Preámbulo.** Está formado por 7 bytes (56 bits) con valores 0 y 1 alternados. Es decir, cada byte contiene los bits 10101010. Este campo se utiliza para realizar la sincronización entre el emisor y el receptor.
- **SFD (Start Frame Delimiter).** Delimitador del comienzo de trama. Es 1 byte con el valor 10101011. Este campo indica el inicio de la trama.
- **Dirección de destino.** Campo con un tamaño de 6 bytes que contiene la dirección física del dispositivo de destino.
- **Dirección fuente u origen.** Campo con un tamaño de 6 bytes que contiene la dirección física del dispositivo que envía la trama.
- **Longitud.** Este campo está formado por 2 bytes que indican la longitud de los datos. El valor mínimo es 0 y el máximo es 1.500.
- **Datos.** Longitud entre 46 y 1.500 bytes dependiendo del tipo de trama y de la longitud del campo de información. El tamaño mínimo de los datos debe ser de 46 bytes de forma que si se envían menos datos en la trama, se envían bytes de relleno hasta completar esta cantidad. Esto se debe a que el tamaño mínimo total de la trama debe ser de 64 bytes para asegurar que se detecte un colisión en el caso más desfavorable.
- **CRC:** código utilizado para detección de errores, con un tamaño de 4 bytes (32 bits). Este código se calcula sobre todas la trama, incluidos los campos de direcciones y longitud. El polinomio generador de orden 32 utilizado es:

$$X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^{8} + X^{7} + X^{5} + X^{4} + X^{2} + X + 1$$

El formato de una trama Ethernet es muy parecido al de IEEE 802.3. De hecho se consideran formatos de tramas compatibles.

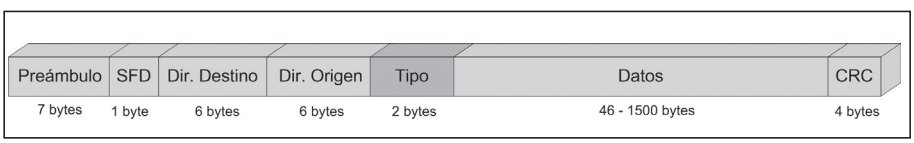


Figura 7.13. *Trama Ethernet.*

Como se observa, la única diferencia es el campo Tipo (en lugar del campo Longitud) utilizado para especificar un código que identifica el protocolo de nivel superior. En la siguiente tabla se pueden ver algunos ejemplos de códigos asociados a protocolos de nivel 3 que se pueden especificar en el campo Tipo.

Protocolo	Código (hexadecimal)
IPv4	0800
ARP	0806
IPX	8137
IPv6	86DD
EtherTalk (AppleTalk sobre Ethernet)	809B
Servicios SNA sobre Ethernet	80D5
Nivel 3 X.25	0805
Banyan Systems	0BAD

Además, y como ya se explicó anteriormente, las redes basadas en Ethernet no utilizan IEEE 802.2 por lo que la trama Ethernet no incluye la trama LLC. En la siguiente figura se observa la estructura de trama IEEE 802.3 incluyendo LLC.

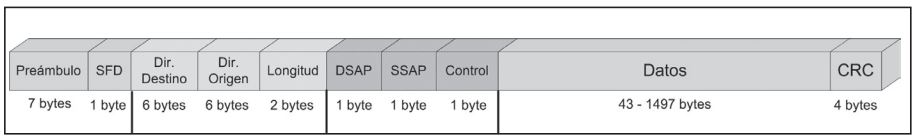


Figura 7.14. *Trama IEEE 802.3 conteniendo trama LLC.*

Los bytes de preámbulo y SFD no se consideran parte de la trama propiamente dicha. De hecho, los bytes de preámbulo no son necesarios en las implementaciones más modernas de Ethernet como Fast Ethernet.

Una tarjeta de red puede manejar tanto tramas Ethernet como tramas IEEE 802.3 simplemente analizando los dos siguiente bytes de la dirección origen. Si es un número inferior a 1.500 es una trama IEEE 802.3 y este campo indica la longitud de la trama y si es un número superior a 1.500 es una trama Ethernet y el campo indica el tipo de protocolo de nivel superior.

NOTA 7.7

Si el número contenido en los bytes 13 y 14 es igual o mayor a 1501 (5DD en hexadecimal) es una trama Ethernet. Si es menor es una trama IEEE 802.3.

7.4.4 MÉTODO DE ACCESO AL MEDIO: CSMA/CD

En las redes Ethernet se utiliza un medio físico compartido por varios dispositivos y por tanto es necesario establecer un mecanismo para la coordinación del tráfico y la gestión de las colisiones.

Como ya se vio en el capítulo anterior, una colisión se produce cuando dos dispositivos transmiten datos simultáneamente a través de un canal común. Las señales se solapan y convierten dichas señales en ruido.

El mecanismo de acceso al medio utilizado en Ethernet es CSMA/CD (Acceso múltiple por detección de portadora y con detección de colisiones), cuyos principios de funcionamiento se vieron en el capítulo 5. Se recuerdan estas características:

- ✓ Si el medio está libre, la estación transmite su trama.
- ✓ Si el medio está ocupado, la estación espera hasta que quede libre y transmite su trama.
- ✓ Mientras se transmite la trama se comprueba si se produce colisión.
- ✓ Si se detecta una colisión se deja de transmitir inmediatamente, se espera un tiempo aleatorio y se intenta transmitir de nuevo.

NOTA 7.8

El uso de CSMA/CD como método de acceso al medio es prácticamente la única característica común a todas las diferentes implementaciones de redes Ethernet desarrolladas a lo largo del tiempo.

7.4.5 LÍMITE EN LA LONGITUD DE LAS REDES ETHERNET: LA VENTANA DE COLISIÓN

Se conoce como **ventana de colisión (Slot Time)** al tiempo de propagación ida y vuelta de extremo a extremo de los datos. Este tiempo depende de dos factores, la velocidad de propagación de la señal por el medio de transmisión y de la distancia que deba recorrer. Estos factores quedan relacionados por la fórmula:

$$\text{Ventana de colisión} = \text{Distancia} / V_{prop}$$

Cuando se transmite una trama, el emisor escucha el canal para detectar las colisiones hasta que acaba de transmitir dicha trama. Por tanto, la transmisión de una trama debe durar como mínimo la ventana de colisión para poder detectar una posible colisión.

El caso más desfavorable se presenta cuando se tiene que transmitir la trama más pequeña posible. El tamaño de trama más pequeño en redes Ethernet es de 64 bytes, es decir, 512 bits. La ventana de colisión debe ser menor o como mucho igual al tiempo que se tarda en transmitir estos 512 bits. Como la velocidad de transmisión es de 10 Mbps:

$$\text{Ventana de colisión} \leq 512 / 10\text{Mbps} = 51'2\ \mu s$$

Para que la ventana de colisión no supere este retardo, la distancia máxima entre dos estaciones de la red debe ser 2.500 metros (es decir, 5.000 metros ida y vuelta) teniendo en cuenta que la velocidad de propagación utilizada es de 100.000.000 m/s.

Por tanto se puede concluir que la ventana de colisión es el factor limitante de la longitud máxima de una red Ethernet (de 2.500 metros).

NOTA 7.9

La ventana de colisión también se conoce como dominio de colisión.

7.4.6 TRATAMIENTO DE REINTENTOS EN CSMA/CD: ALGORITMO DE RETROCESO EXPONENCIAL BINARIO

Los sucesivos reintentos que se realizan cuando se produce una colisión siguen el llamado **Algoritmo de Retroceso Exponencial Binario (Backoff)**. Después de una colisión y antes de reintentar la transmisión, se espera un tiempo igual a:

$$T_{retrans} = R*(\text{Ventana de colisión})$$

R es una variable entera aleatoria que puede tomar valores entre 0 y 2^K-1.

K es el número de retransmisión hasta un máximo de 10. Es decir, para la retransmisión número 11 el valor de K seguirá siendo 10.

El número máximo de reintentos que se llevan a cabo es de 16.

Considerando que la ventana de colisión para redes Ethernet a 10 Mbps es de 51'2 μs, cuando una estación intenta transmitir y se produce una colisión, el tiempo que se espera para hacer un reintento será:

$$T_{retrans} = \{0, 1\}*51'2 = \begin{matrix} 0\ \mu s \\ 51'2\ \mu s \end{matrix}$$

En el caso de que el resultado sea 0 la retransmisión no se lleva a cabo instantáneamente sino que se espera un tiempo mínimo llamado **Interframe Gap**, que es la distancia mínima que debe haber entre tramas consecutivas y que es el tiempo necesario para transmitir 96 bits (para 10 Mbps se tardaría 9'6 μs).

Si se produce una nueva colisión para el primer reintento, el tiempo de retransmisión del segundo reintento será:

$$T_{retrans} = \{0, 1, 2, 3\}*51'2 = \begin{matrix} 0\ \mu s \\ 51'2\ \mu s \\ 102'4\ \mu s \\ 153'6\ \mu s \end{matrix}$$

El máximo tiempo de espera para una retransmisión se producirá a partir del reintento 10, cuando R sea 1023:

$$T_{retrans} = 1023 * 51'2 = 52'38 \text{ ms}$$

Este algoritmo asegura que cuando haya pocas colisiones el retardo introducido con los reintentos sea pequeño, pero cuando haya muchas colisiones se aumenta el período aleatorio de retransmisión para disminuir la posibilidad de nuevas colisiones.

Este algoritmo se implementa en la tarjeta de red al igual que la mayor parte de las funciones del nivel de enlace.

7.5 EVOLUCIÓN DE LAS REDES ETHERNET

El éxito de las redes Ethernet especialmente de la implementación 10BASE-T hizo que la evolución de las redes de área local se encaminase a este tipo de redes. De esta forma han surgido varios estándares que consiguen aumentar las prestaciones de forma significativa: Ethernet conmutada, Fast Ethernet, Gigabit Ethernet y recientemente 10 Gigabit Ethernet.

7.5.1 FAST ETHERNET

El rápido crecimiento y utilización de las redes Ethernet produjo a su vez un aumento de los requerimientos de velocidad. Las redes Ethernet estaban formadas cada vez por más equipos y las transferencias de información a través de las mismas también iban en aumento.

La solución adoptada por el IEEE fue **Fast Ethernet**, publicada en 1995 como **IEEE 802.3u**. Su principal característica es el aumento de la velocidad de transmisión de 10 a 100 Mbps.

Fast Ethernet utiliza la especificación 10BASE-T como referencia, de forma que se intenta mantener las características de ésta. Por ejemplo, se mantiene la topología en estrella física y lógica en bus, se sigue utilizando CSMA/CD como método de acceso al medio y se mantiene el formato de la trama.

Para poder detectar colisiones mediante CSMA/CD la ventana de colisión debe ser como mucho igual al tiempo de retransmisión de la trama más pequeña, que son 64 bytes o 512 bits. Este tiempo, a 10 Mbps es de 51'2 μs. Si aumentamos la velocidad a 100 Mbps, la ventana de colisión se reduce a 5'12 μs. La ventana de colisión, o lo que es lo mismo, el tiempo de ida y vuelta entre los dos puntos más alejados de las red debe ser 10 veces menor. Como la velocidad de propagación es un valor fijo lo que debe disminuir es la distancia máxima, que debe ser 10 veces menor, es decir, 250 metros.

En la topología en estrella física la distancia máxima entre dos estaciones es igual a la mitad de la distancia máxima entre una estación y el hub, que debe ser por tanto, 125 metros. Para las LAN 10BASE-T esto no supone ningún problema ya que la longitud máxima entre estaciones y hub está limitada a 100 metros por lo que la migración a Fast Ethernet es más sencilla.

NOTA 7.10

Aumentar la velocidad en Fast Ethenet supone disminuir la ventana de colisión de forma proporcional.

Para dar diferentes alternativas en función de los medios de transmisión disponibles, el IEEE publicó tres alternativas de redes Fast Ethernet:

100BASE-TX

Esta versión de Fast Ethernet es la que se ha impuesto y actualmente es uno de los tipos de redes más utilizados.

Utiliza cable de cobre de par trenzado sin blindaje (UTP) de categoría 5. La principal diferencia entre categoría 3 y categoría 5 es la frecuencia máxima, que lógicamente debe ser mayor en categoría 5. Se utilizan dos pares, uno para transmisión y otro para recepción de forma que este tipo de redes admite operaciones full-dúplex (ver el siguiente apartado).

La distancia máxima entre una estación y el hub, al igual que en 10BASE-T, es de 100 metros.

Se utilizan las codificaciones 4B/5B y MLT-3. La codificación **MLT-3** es parecida a NRZ-I pero utilizando tres polaridades diferentes en lugar de dos: positiva, negativa y cero. Un valor 0 lógico se codifica sin cambio de polaridad y un valor 1 lógico con cambio de polaridad. Esta codificación tiene el mismo problema que NRZ-I, puede producir pérdidas de sincronismo ante secuencias largas de ceros. Para solucionarlo se utiliza la codificación 4B/5B aplicada antes de la codificación MLT-3. En **4B/5B** cada grupo de 4 bits se convierte a un código de 5 bits especialmente preparado para que no se produzcan combinaciones largas de ceros. De

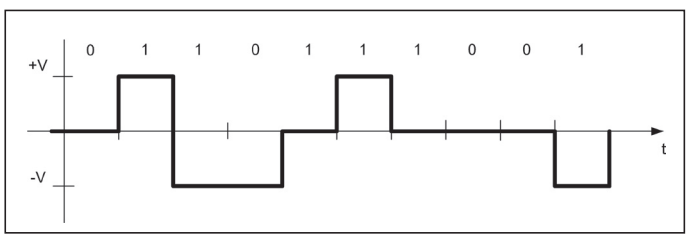


Figura 7.15. *Codificación MLT-3.*

hecho, una secuencia de datos codificados en 4B/5B no contiene nunca secuencias de más de tres ceros. Además, algunas de las combinaciones sobrantes se utilizan para funciones de control.

Tabla 7.1 Tabla de codificación 4B/5B

Binario	4B/5B	Binario	4B/5B
0000	11110	1000	10010
0001	01001	1001	10011
0010	10100	1010	10110
0011	10101	1011	10111
0100	01010	1100	11010
0101	01011	1101	11011
0110	01110	1110	11100
0111	01111	1111	11101

100BASE-FX

Esta versión, al igual que la siguiente, no ha tenido mucha repercusión y actualmente no hay muchas redes que la utilicen. Sus principales características son:

- ✓ Utiliza como medio de transmisión fibra óptica multimodo.
- ✓ La codificación utilizada es 4B/5B y NRZ-I. Elegida por compatibilidad con las redes FDDI.
- ✓ Distancia máxima entre el concentrador y una estación es de 2.000 metros en modo full-dúplex

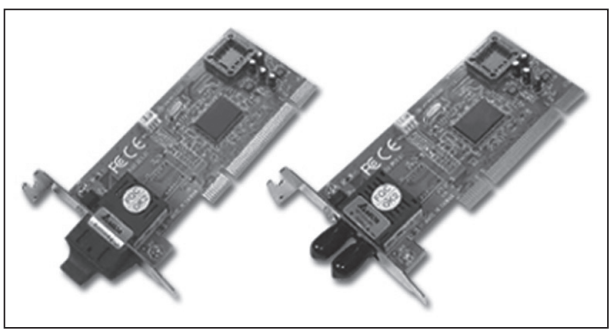


Figura 7.16. *Tarjeta y cable 100BASE-FX.*

100BASE-T4

Esta versión de Fast Ethernet se especificó para dar la opción de aprovechar cableado instalado de categoría 3. Aunque, al igual que la anterior, no tuvo mucha penetración en el mercado.

Utiliza cables de par trenzado categoría 3. Sin embargo, utiliza cuatro pares en lugar de dos para repartir el flujo de datos a 100 Mbps en tres de 33'3 Mbps. Dos de los pares utilizados se utilizan en modo half-dúplex por lo que este tipo de redes no admite operaciones full-dúplex.

Utiliza codificaciones 8B/6T y NRZ-I. La codificación **8B/6T** sustituye un grupo de 8 bits en seis símbolos ternarios, es decir, se utilizan tres niveles de tensión diferentes en lugar de dos. Se utiliza esta codificación para mejorar la tasa de baudios de la señal.

La distancia máxima entre una estación y el hub, al igual que en 100BASE-TX, es de 100 metros.

Actualmente, la tecnología Fast Ethernet se considera el principal y más importante tipo de red LAN. Un estudio llevado a cabo en el año 2000 por IDC (International Data Corporation) muestra que el 85% de las redes LAN utilizaban Ethernet. Y según Infonetics Rechearch Inc., en el año 2000, el 85% de las redes Ethernet son Fast Ethernet. Actualmente el porcentaje debe ser sensiblemente superior.

7.5.2 ETHERNET CONMUTADA (SWITCHED ETHERNET) Y FULL-DÚPLEX

Las redes Ethernet conmutadas se basan en la utilización como elemento central de la topología física en estrella de un **switch o conmutador** en lugar de un hub.

Un switch o conmutador es un dispositivo de interconexión que posee varios puertos de entrada, normalmente de tipo RJ-45. Externamente es parecido a un hub, sin embargo y a diferencia de éste, un switch es capaz de leer las tramas

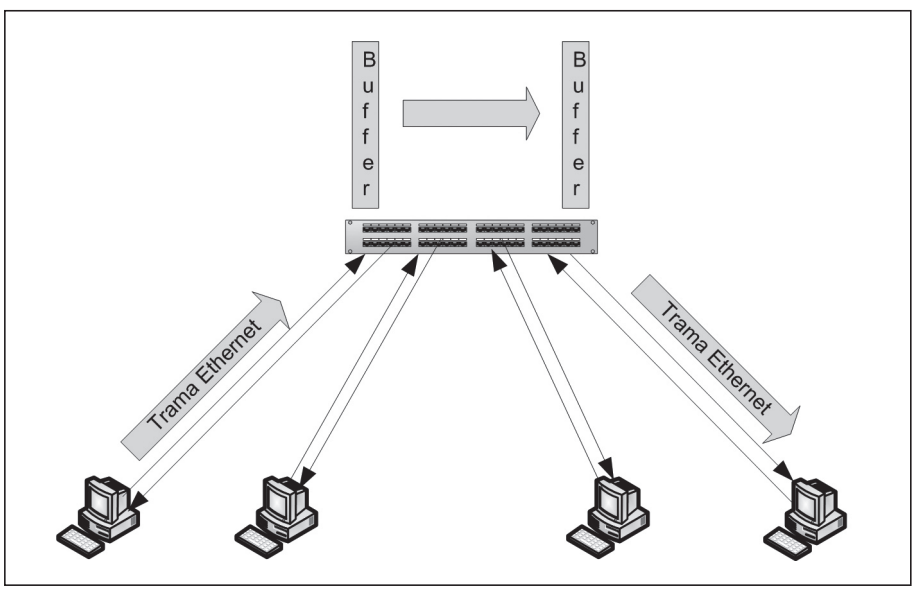


Figura 7.17. *Ethernet conmutada.*

Ethernet que recibe por cualquiera de sus puertos, analizar la dirección física de destino y reenviar la trama sólo al puerto donde esté conectada la estación con dicha dirección. Es decir, no hace una simple difusión de las señales eléctricas al resto de puertos. De esta forma se reduce drásticamente el número de colisiones. En un apartado posterior, en este mismo capítulo se verán en detalle las características más importantes de los conmutadores.

La otra característica interesante que añaden los conmutadores es que permiten comunicación full-dúplex. Para que este funcionamiento sea posible tanto la tarjeta de red (NIC) como el switch deben estar diseñados para ello. En el modo de funcionamiento full-dúplex no se utiliza el método de acceso al medio CSMA/CD por ser innecesario ya que la conexión de cada NIC al switch utiliza un canal dedicado por cada sentido de la comunicación.

NOTA 7.11

En modo full-dúplex no es necesario utilizar el método CSMA/CD de acceso al medio ya que cada conexión estación-switch se comporta como una línea punto a punto.

Para operaciones full-dúplex también se ha definido dentro del estándar IEEE la especificación **IEEE 802.3x** (publicado en el año 1997), donde además se incluye un método de control de flujo. Esto es necesario ya que es posible que un dispositivo transmita tramas más rápido de lo que el receptor puede procesarlas, lo que provocaría pérdidas de información. Este control de flujo se implementa mediante el envío de un comando llamado PAUSE desde el receptor, donde le indica al emisor el tiempo que debe permanecer sin enviar datos. Durante el tiempo de inactividad el receptor puede volver a enviar comandos PAUSE para prolongar, reducir o suprimir la pausa inicial.

El buen funcionamiento de esta operación depende sobre todo de lo rápido que se identifiquen las tramas de control de flujo. El comité IEEE comprobó que el formato Ethernet original era el más adecuado para este propósito ya que permitía identificar las tramas de control de flujo mediante el campo Tipo mientras que en el formato IEEE esta información debe incluirse en la trama LLC. Por tanto IEEE decidió estandarizar el formato de trama Ethernet. Este formato forma parte del estándar desde 1997 utilizando el campo Tipo/Longitud para distinguir el tipo de trama utilizado.

NOTA 7.12

Las tramas que contienen los comandos PAUSE se identifican porque contienen el valor 0x8808 en el campo Tipo.

El ancho de banda efectivo de las redes que utilizan el modo full-dúplex se duplica respecto al modo half-dúplex. Así, una red half-dúplex funcionando a 100 Mbps aumentará su velocidad a 200 Mbps si utiliza el modo full-dúplex, ya que cada estación conectada podrá tener un flujo máximo de información de 100 Mbps en un sentido y otros 100 Mbps en el sentido contrario de forma simultánea.

Una de las características incluidas en la especificación **IEEE 802.3u** fue la capacidad de **autonegociación** entre switch y las estaciones para determinar principalmente dos características, la velocidad de transmisión 10/100 Mbps y el tipo de transmisión half-dúplex o full-dúplex.

La mayor parte de los dispositivos de interconexión admiten esta característica, de forma que la comunicación entre los mismos y las estaciones es autoconfigurable de forma transparente al usuario.

7.5.3 GIGABIT ETHERNET

Entre los años 1998 y 1999 el IEEE amplió el estándar IEEE 802.3 para incluir un nuevo tipo de redes, llamado de forma genérica **Gigabit Ethernet**. Este estándar se desarrolló bajo dos especificaciones: la primera desarrollada en 1998 llamada **IEEE 802.3z** o también **1000BASE-X** que utiliza fibra óptica. La segunda desarrollada en 1999 llamada **IEEE 802.3ab** también conocida como **1000BASE-T** que utiliza cable de cobre de par trenzado. La principal característica de Gigabit Ethernet es que la velocidad de transmisión es de 1.000 Mbps o 1 Gbps.

1000BASE-X está basado en la utilización de fibra óptica como medio de transmisión. Además utiliza las especificaciones a nivel físico del estándar **Fiber Channel** (ANSI X3 T11), pero mantiene la compatibilidad con Ethernet en el nivel de enlace. La arquitectura Fiber Channel utiliza cuatro capas, aunque la especificación 1000BASE-X utiliza sólo las dos primeras llamadas FC-0 y FC-1.

1000BASE-T

El otro grupo especificado es el 1000BASE-T basado en la utilización de cable UTP de categorías 5, 5e o 6. Para este diseño se intentó mantener la compatibilidad con las versiones anteriores.

El diseño de 1000BASE-T planteó algunos problemas, además del aumento de la complejidad de los circuitos digitales en las tarjetas de red.

En primer lugar, las características del cable de categoría 5 permiten transmitir señales con una frecuencia de hasta 100 MHz lo que es insuficiente para transmitir datos a 1.000 Mbps. Para aumentar la velocidad de transmisión, en 1000BASE-T se utilizan los cuatro pares del cable tanto para la transmisión como para la recepción. La transmisión de los dos sentidos de la comunicación por los mismos pares es posible gracias a la utilización de técnicas de cancelación eco. De esta forma se lograría una velocidad de 400 Mbps. Para llegar a 1 Gbps se utiliza una técnica de

modulación por amplitud de pulso que utiliza cinco niveles para la cuantificación llamada PAM-5. Después de este tratamiento y para el envío de la señal en banda base se utiliza codificación 8B/10B.

El segundo gran problema planteado en Gigabit Ethernet es la ventana de colisión. Al aumentar 10 veces la velocidad respecto a Fast Ethernet y manteniendo el mismo tamaño mínimo de trama, es decir, 64 bytes, disminuye 10 veces la ventana de colisión, es decir, se quedaría en 0'512 μs, por lo que sería necesario reducir la distancia máxima 10 veces, es decir, a 25 metros, lo que en la mayoría de los casos sería insuficiente. Para solucionarlo, en Gigabit Ethernet se incorpora un segundo relleno llamado **Extensión de Portadora (Carrier Extension)** que se añade al final de trama para garantizar que la longitud mínima nunca será inferior a 512 bytes (4096 bits). De esta forma, la ventana de colisión aumenta a 4'096 μs lo que permite mantener la distancia máxima en 100 metros. Esta solución repercute negativamente en la eficiencia de la red cuando se transmiten muchas tramas pequeñas, ya que una gran parte del ancho de banda se emplea en transmitir bits de relleno. Para paliar en parte este efecto, en Gigabit Ethernet se pueden agrupar varias tramas pequeñas en lo que se conoce como **Modo Ráfaga (Frame Bursting)** en el cual se pueden enviar varias tramas pequeñas consecutivas hasta un máximo de 65536 bits.

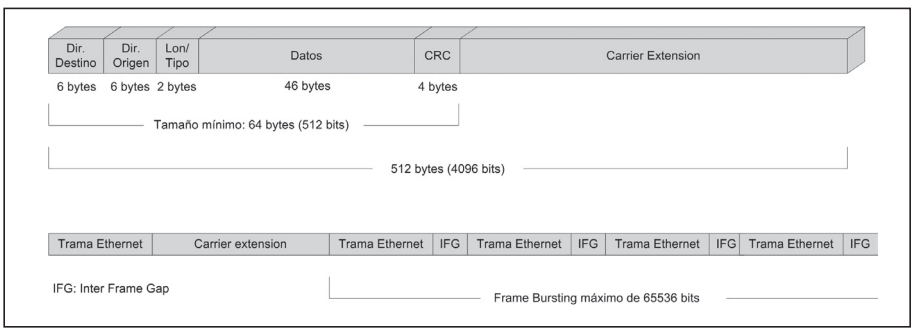


Figura 7.18. *Extensión de portadora y el modo ráfaga.*

Gigabit Ethernet puede funcionar tanto en modo half-dúplex como en modo full-dúplex. En modo half-dúplex se sigue usando el método CSMA/CD de acceso al medio como en las implementaciones anteriores de 10 y 100 Mbps. En modo full-dúplex, al no utilizarse CSMA/CD tampoco es necesario utilizar el relleno de portadora o Carrier Extension ni el modo ráfaga. De hecho en la práctica casi todos los sistemas que utilizan Gigabit Ethernet lo hacen en modo full-dúplex.

En resumen, las principales características de 1000BASE-T son:

- ✓ Cable de cobre de par trenzado categorías 5, 5e o 6.
- ✓ Velocidad de transmisión: 1000 Mbps.
- ✓ Longitud máxima del cable: 100 metros.
- ✓ Técnica de transmisión PAM-5 con codificación 8B/10B.
- ✓ Transmisión half-dúplex o full-dúplex.

Las implementaciones 1000BASE-X utilizan como medio de transmisión la fibra óptica. Sus principales características son las siguientes:

1000BASE-SX

- ✓ Emplea las codificaciones 8B/10B y NRZ-I.
- ✓ Se utiliza fibra óptica multimodo.
- ✓ La distancia máxima es de 275 metros para fibra de 62'5/125 µm o de 550 metros para fibra de 50/125 µm.

1000BASE-LX

- ✓ Emplea las codificaciones 8B/10B y NRZ-I.
- ✓ Se utiliza tanto fibra óptica monomodo como multimodo.
- ✓ La distancia máxima para fibra multimodo es de 550 metros o de 2 Km para fibra monomodo.

Ambas implementaciones de Gigabit Ethernet son utilizadas en modo full-dúplex principalmente para dar soporte a las redes troncales (backbone).

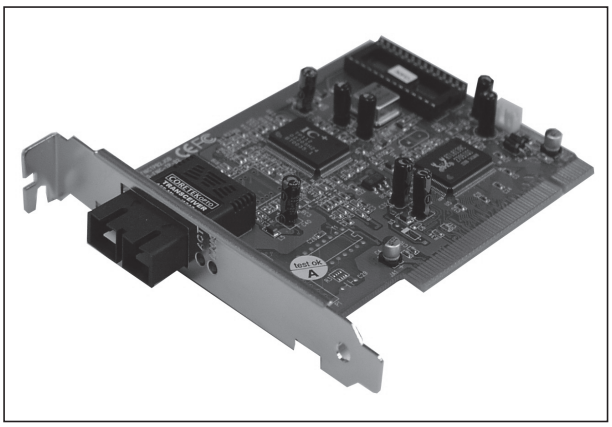


Figura 7.19. *Tarjeta de red Gigabit Ethernet.*

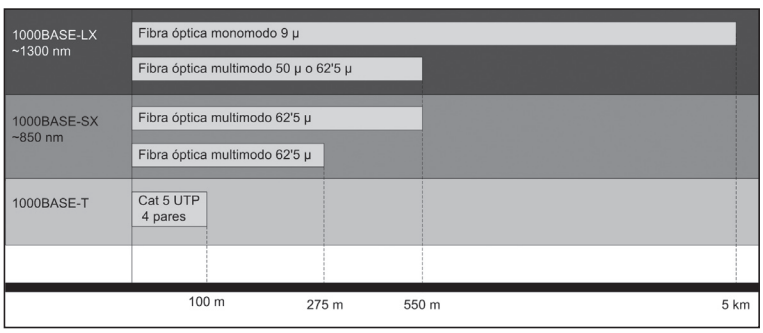


Figura 7.20. *Distancias máximas para Gigabit Ethernet.*

Tabla 7.2 Tabla resumen Ethernet

Implementación	Estándar IEEE	Año	Velocidad (Mbps)	Codificación	Tipo de cable	Full-dúplex
10BASE5	802.3	1983	10	Manchester	Coaxial	No
10BASE2	802.3a	1985	10	Manchester	Coaxial	No
10BASE-T	802.3i	1990	10	Manchester	UTP Cat.3	Sí*
100BASE-TX	802.3u	1995	100	4B/5B y MLT-3	UTP Cat.5	Sí*
100BASE-FX	802.3u	1995	100	4B/5B y NRZ-I	Fibra óptica	Sí*
100BASE-T4	802.3u	1995	100	8B/6T y NRZ-I	UTP Cat.3	No
1000BASE-T	802.3ab	1999	1000	PAM-5 y 8B/10B	UTP Cat.5, 5e ó 6	Sí
1000BASE-X	802.3z	1998	1000	NRZ-I y 8B/10B	Fibra óptica	Sí

*El modo full-dúplex no está especificado en el estándar original. Este modo es admitido a partir del estándar IEEE 802.3x en el año 1997.

7.5.4 10-GIGABIT ETHERNET

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

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

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

NOTA 7.13

InfiniBand es una interfaz de comunicaciones punto a punto de altas prestaciones cuyas primeras especificaciones fueron desarrolladas por varias empresas entre las que se encuentran Intel, AMD, Sun, IBM, Dell, Cisco o Silicon Graphics y que se publicaron en el año 2000.

7.6 LAN INALÁMBRICA: 802.11

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

Inicialmente se desarrollaron varios estándares para las redes WLAN, como por ejemplo el estándar **HomeRF**, desarrollado en 1999, entre otras, por empresas como Compaq, HP, IBM, Intel, Microsoft y que fue abandonado en 2003. O el estándar **HiperLAN** desarrollado por la ETSI (European Telecomunication Standard Institute), aprobado en 1996 y del que existen dos versiones, la última, conocida como HiperLAN/2 puede operar a velocidades de 54 Mbps. En Japón se desarrolló un estándar inalámbrico basado en HiperLAN llamado **HiSWAN**. Además, y sin un estándar claro que dominase el mercado, algunas empresas ofrecieron sus propias soluciones inalámbricas propietarias.

Con este escenario de diversidad en cuanto a soluciones inalámbricas para redes LAN, el organismo IEEE decidió desarrollar su propio estándar para redes WLAN dentro del proyecto 802, y al que le asignó la codificación **IEEE 802.11**.

A su vez, en el año 1999 algunos de los más importantes fabricantes de soluciones inalámbricas crearon una organización llamada **WECA** (Wireless Ethernet Compatibility Alliance) con el objetivo de fomentar la compatibilidad de los dispositivos inalámbricos desarrollados bajo los estándares del IEEE. Unos años más tarde, esta organización cambia su nombre a **Wi-Fi Alliance**.

Los dispositivos que cumplen los estándares IEEE 802.11 son comercializados con la denominación **Wi-Fi** (Wireless Fidelity) lo que asegura su compatibilidad con el resto de dispositivos Wi-Fi del mercado.

NOTA 7.14

Se puede obtener la lista de dispositivos Wi-Fi certificados por la Wi-Fi Alliance en: http://certifications.wi-fi.org/wbcs_certified_products.php.

Por tanto, hay que diferenciar el nombre del estándar, que es IEEE 802.11, del nombre comercial asignado para garantizar que un dispositivo cumple con el estándar IEEE 802.11 y que es Wi-Fi. Este distintivo es asignado a los dispositivos por la Wi-Fi Alliance.

Figura 7.21. *Logo de Wi-Fi.*

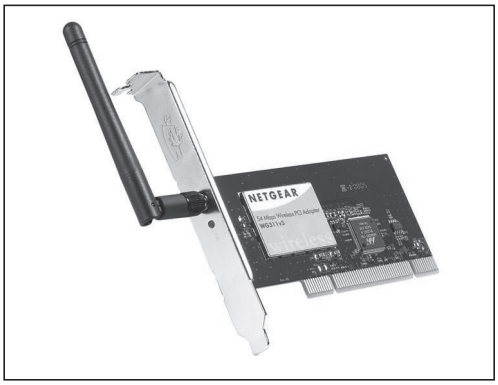


Figura 7.22. *Tarjeta de red Wi-Fi.*

7.6.1 EL ESTÁNDAR IEEE 802.11

El estándar IEEE 802.11, al igual que el resto de estándares de redes LAN, cubre las funciones del nivel físico y del subnivel MAC del nivel de enlace.

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

La especificación de la frecuencia de trabajo de 2'4 GHz realmente se refiere a una banda de frecuencias que va desde 2'4 GHz hasta 2'4835 GHz (es decir, ocupa un ancho de banda de 83'5 MHz).

Lo interesante de esta banda de frecuencias es que no requiere licencia de uso. Por el contrario, ya que esta banda de frecuencias es de libre uso, es utilizada por otros dispositivos, como hornos microondas, teléfonos inalámbricos o dispositivos Bluetooth con los que podría tener interferencias.

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

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

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

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

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

En 2003, se publica el estándar **IEEE 802.11g**. Es la última especificación publicada y la que más penetración en el mercado ha tenido. Sus características son las siguientes:

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

Además, el IEEE ha desarrollado otras especificaciones sobre redes WLAN que complementan las anteriores:

802.11e	Especificaciones de un conjunto de mejoras para la Calidad del servicio (QoS) en redes Wi-Fi
802.11h	Especificaciones para la gestión del espectro y de la potencia de transmisión en redes Wi-Fi
802.11i	Especificación de mecanismos de seguridad (sistema TKIP)

Actualmente se está desarrollando una nueva implementación que permitirá velocidades máximas de hasta 540 Mbps, llamada **IEEE 802.11n**.

7.6.2 TÉCNICAS DE TRANSMISIÓN

Se utilizan básicamente dos técnicas de transmisión en las especificaciones IEEE 802.11. DSSS es la técnica de espectro expandido utilizada en IEEE 802.11b y OFDM es la técnica de modulación utilizada en IEEE 802.11a y IEEE 802.11g.

- **Espectro expandido (Spread Spectrum)** La técnica de transmisión denominada espectro expandido se basa en utilizar un ancho de banda superior al necesario para ser más inmune a las interferencias. Hay dos tipos:
  - **FHSS (Frequency-Hopping Spread Spectrum, Espectro expandido por salto de frecuencias).** En este tipo se divide la banda de frecuencias en canales y se transmite saltando de canales con un patrón de salto preestablecido. Esta técnica se encuentra contemplada en la versión original de IEEE 802.11 sin embargo nunca ha llegado a utilizarse. Donde sí se ha utilizado FHSS es en la tecnología de transmisión inalámbrica Bluetooth.
  - **DSSS (Direct-Sequence Spread Spectrum, Espectro expandido por secuencia directa).** En este tipo de transmisión se sustituye cada bit de

información a transmitir por una secuencia de bits llamada chipping code (código de chip). Sólo los receptores que conocen el código de chip utilizado por el emisor pueden leer los datos. La longitud mínima de código de chip es de 11 bits. Esta técnica de transmisión está especificada para la implementación original IEEE 802.11 y para la implementación IEEE 802.11b.

Debido a las características de esta técnica, sólo puede haber tres sistemas utilizando DSSS en la misma área. Esto se deduce fácilmente ya que en IEEE 802.11b la velocidad máxima es de 11 Mbps para lo que es necesario un ancho de banda de 22 MHz. Como el ancho de banda total en 2'4 GHz es de 83'5 MHz con tres sistemas DSSS ya cubriríamos en ancho de banda de este canal.

- **OFDM (Orthogonal Frequency-Division Multiplexing, Multiplexación ortogonal por división de frecuencias).** La técnica es similar a DMT, es decir, se utilizan múltiples subportadoras y cada una de ellas se modula normalmente en QAM. La principal ventaja de OFDM es su buen comportamiento ante el multitrayecto típico de los sistemas radioeléctricos. También tiene buena respuesta ante interferencias. Se utiliza en IEEE 802.11a y 802.11g.

7.6.3 OTRAS CARACTERÍSTICAS

Algunas otras características de las redes IEEE 802.11 son las siguientes:

- ✓ El método de acceso al medio utilizado es **MACA (Multiple Access with Collision Avoidance)** que es una mejora de la técnica original llamada CSMA/CA (Acceso múltiple por detección de portadora y con evitación de colisiones).
- ✓ El alcance máximo y libre de obstáculos es de unos 100 metros en la banda de 2'4 GHz.
- ✓ Debido a las características del tipo de medio de transmisión, las comunicaciones inalámbricas son **half-dúplex**.

7.6.4 MODOS DE OPERACIÓN

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

- ✓ Ad hoc.
- ✓ Infraestructura.

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

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

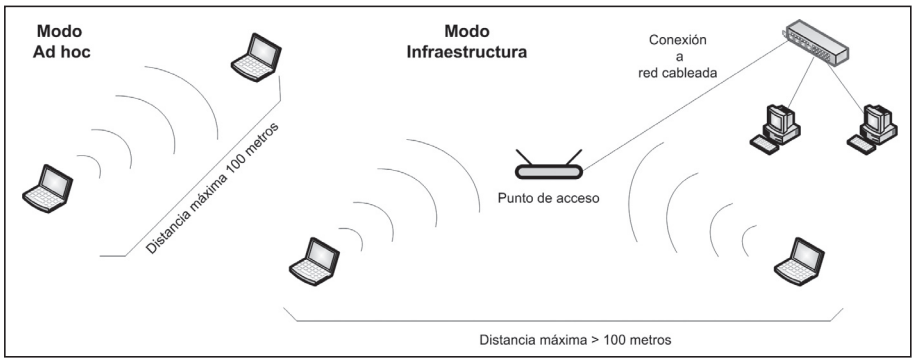


Figura 7.23. *Comparación de alcance Ad hoc e infraestructura.*

Normalmente un punto de acceso es un dispositivo fabricado específicamente como punto de acceso aunque también es posible utilizar un PC con una tarjeta Wi-Fi y software específico para realizar las funciones de punto de acceso.

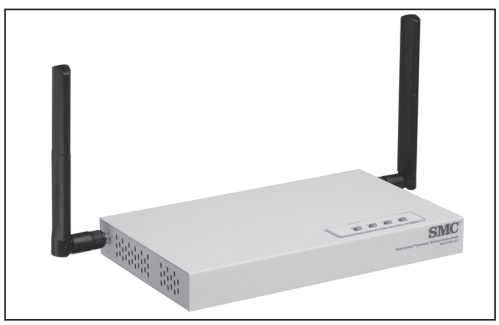


Figura 7.24. *Punto de acceso.*

El funcionamiento con un punto de acceso se puede llevar a cabo de dos formas:

- **BSS (Basic Service Set):** se utiliza un solo punto de acceso y se define una sola red inalámbrica formada por las estaciones conectadas a dicho punto de acceso
- **ESS (Extended Service Set):** se utilizan varios puntos de acceso para cubrir un área más extensa.

Los puntos de acceso transmiten una trama modelo de administración a intervalos fijos. La trama modelo identifica el punto de acceso incorporando su nombre de red. El nombre de red se conoce técnicamente como **SSID (identificador del conjunto de servicios)**.

7.6.5 SEGURIDAD

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

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

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

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

WPA utiliza, además, un proceso de autentificación desarrollado bajo el estándar **IEEE 802.1x** y que define un procedimiento de control de acceso al nivel de acceso al medio (MAC). El componente más importante de este estándar es el llamado **EAP (Extensible Authentication Protocol)** que surgió como mejora del método de autenticación utilizado en PPP. En WPA se admiten dos procesos de autentificación. El primero, conocido como **WPA Enterprise**, se lleva a cabo a través de un servidor de autentificación (normalmente un servidor RADIUS) y se utili-

za habitualmente en entornos profesionales. El segundo, que se conoce como **WPA Personal** o **WPA-PSK**, se lleva a cabo través de una clave pre-compartida **(PSK, Pre-shared Key)** y se utiliza en entornos menos restrictivos y entornos domésticos.

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

Tabla 7.3 Tabla resumen de los mecanismos de seguridad estandarizados

Estándar	Mecanismo de seguridad	Encriptación	Autenticación
IEEE 802.11	WEP	RC4	No hay
WPA (Wi-Fi Alliance)	TKIP	RC4	IEEE 802.1x (EAP)
IEEE 802.11i (WPA2)	TKIP	AES	IEEE 802.1x (EAP)

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

7.7 OTRAS ARQUITECTURAS LAN

Debido a la aceptación de las redes Ethernet, el resto de tecnologías LAN actualmente están en desuso. A continuación se presenta brevemente las principales características de dichas tecnologías:

7.7.1 BUS DE PASO DE TESTIGO (TOKEN BUS): IEEE 802.4

Uno de los principales problemas que tenían las primeras implementaciones Ethernet es que el tiempo de envío de los datos no es predecible debido a que no se conoce el número de colisiones producidas.

La utilización de redes LAN en el control de procesos requiere que el retardo de propagación de los datos sea muy pequeño o por lo menos predecible para poder llevar a cabo el procesamiento en tiempo real. Esta condición no se cumplía en las primeras implementaciones Ethernet por lo que se desarrolló una tecnología LAN cuya topología se adaptara a las líneas de producción (Bus) y que el retardo de propagación de los datos fuese predecible. Esta tecnología se conoce como Bus de paso de testigo o Token Bus, cuyo estándar se publicó en el IEEE 802.4.

Esta implementación LAN se desarrolló para el control de procesos o sistemas que necesiten un proceso de transmisión con retrasos predecibles. Ethernet no resultaba apropiado debido a que las colisiones no permiten predecir cuánto tiempo se necesita para realizar una transmisión.

Este tipo de redes utiliza una topología física en bus pero con una topología lógica en anillo (conocido como anillo lógico).

El control de la transmisión se realiza mediante una trama especial de control llamada **Testigo (Token)**. Solamente el dispositivo que tenga el testigo puede transmitir datos. Cuando acaba su transmisión le pasa el testigo al siguiente dispositivo. No hay correspondencia entre el orden físico y el orden lógico de los dispositivos.

Algunas otras características de las redes Token Bus son:

- ✓ Se especificó como medio de transmisión el cable coaxial grueso.
- ✓ La velocidad de transmisión oscilaba entre 1'5 y 10 Mbps.
- ✓ El formato de trama MAC es el siguiente:

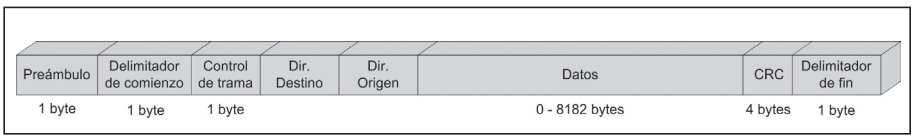


Figura 7.25. *Trama MAC en Token Bus.*

El campo control de trama puede tener los siguientes valores:

00000000	Reclamo de testigo (inicialización del anillo)
00000001	Permiso para entrar en el anillo
00001100	Permiso para salir del anillo
01xxxxxx	Trama de datos

Las direcciones pueden ser iguales a las utilizadas en las redes IEEE 802.3.

7.7.2 RED DE ANILLO CON PASO DE TESTIGO (TOKEN RING): IEEE 802.5

Fue un tipo de red diseñado originalmente por IBM y que tuvo cierto grado de implantación entre los años 80 y 90 aunque progresivamente las redes Token Ring han sido sustituidas por Ethernet.

Método de acceso

El método de acceso al medio utilizado en redes Token Ring, al igual que la anterior, es el paso de testigo. Cada dispositivo puede transmitir sólo si tiene el testigo, que es una trama especial de control con una longitud de 3 bytes.

Una vez generado el testigo en el bus, éste se va pasando de estación en estación hasta que llegue a una estación que tenga datos que transmitir. Dicha estación retiene el testigo y envía su trama de datos.

La trama se propaga por el anillo. Cada estación a la que le llega, lee el campo dirección y si no se corresponde con su dirección, reenvía la trama. Esto ocurre hasta que la trama llega a la estación destino. La estación destino lee la trama, comprueba los errores, añade a la propia trama una marca que indica que ya ha ido leída, y la reenvía a la siguiente estación del anillo. La trama irá pasando por las sucesivas estaciones del anillo hasta que llega de vuelta a la estación que envío la trama.

Dicha estación reconoce su trama leyendo el campo dirección origen y comprueba la marca de trama leída correctamente. Si esto ocurre, descarta la trama y vuelve a poner el testigo en el bus.

En este tipo de redes existe un mecanismo de prioridades en el que un dispositivo con alta prioridad puede reservar el testigo para poder transmitir datos antes de que le llegue el turno.

Las redes Token Ring necesitan la designación de una estación de la red como **estación monitora**. Su función es regenerar el testigo en caso de pérdida del mismo. Además, se encarga de evitar que haya tramas de datos circulando permanentemente por el anillo (por ejemplo, debido a que no se encuentra en la red la dirección de destino).

Otras características de las redes Token Ring

- Implementación del nivel físico: topología lógica y física en anillo.

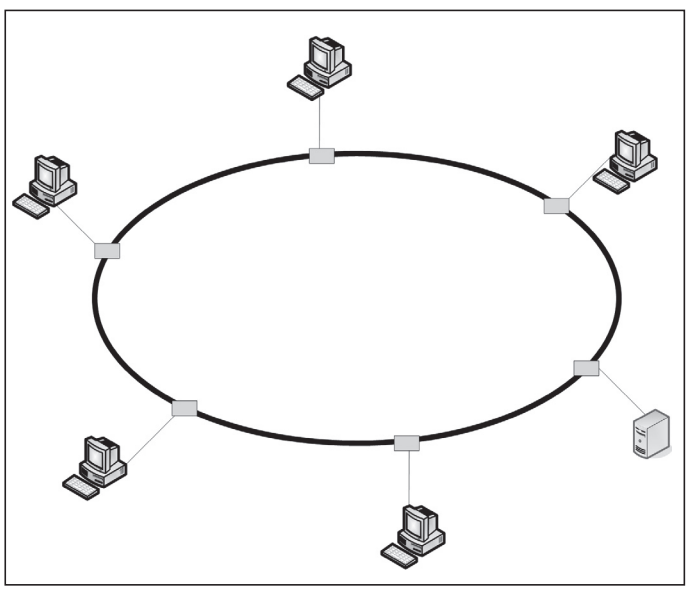


Figura 7.26. *Topología de una red Token Ring.*

- Se utiliza cable de cobre de par trenzado blindado (STP) que conecta un puerto de salida de una estación con el puerto de entrada de la siguiente.
- La codificación es del tipo Manchester diferencial.
- Velocidad de transmisión: 16 Mbps.
- Direccionamiento. Se usan direcciones de 6 bytes contenidas en la NIC de forma similar a Ethernet.
- Formato de trama.

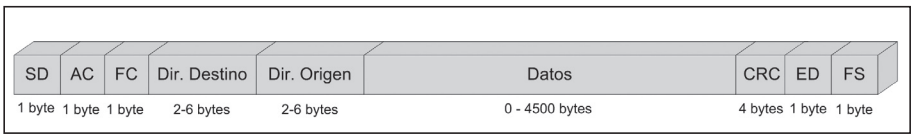


Figura 7.27. *Trama Token Ring.*

El campo SD o Delimitador de inicio marca el inicio de la trama y se utiliza para sincronización.

El campo AC o Control de acceso incluye cuatro subcampos:

- Prioridad (3 bits)
- Testigo (1 bit)
- Monitor (1 bit)
- Reserva (3 bits)

El campo FS o Estado de la trama incluye un bit para indicar que la trama ya ha sido leída por el receptor. Incluye otro bit utilizado por el monitor para comprobar si una trama ya ha circulado por el anillo. Estos bits están duplicados para llevar a cabo un control de errores sobre los mismos ya que el CRC de la trama no incluye este campo.

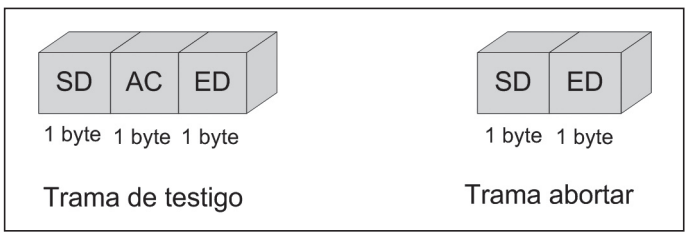


Figura 7.28. *Tramas de control en Token Ring.*

Una mejora introducida en las redes Token Ring es la de utilizar un dispositivo llamado **MAU (Multistation Access Unit, Unidad de acceso multiestación)**. Este dispositivo implementa internamente un anillo Token Ring y proporciona puertos de acceso para las estaciones, de forma que su utilización convierte la topología

de la red en estrella física, aunque sigue utilizando la topología lógica en anillo. Además, cada puerto de entrada incluye un conmutador para cerrar el anillo cuando no haya ningún dispositivo conectado.

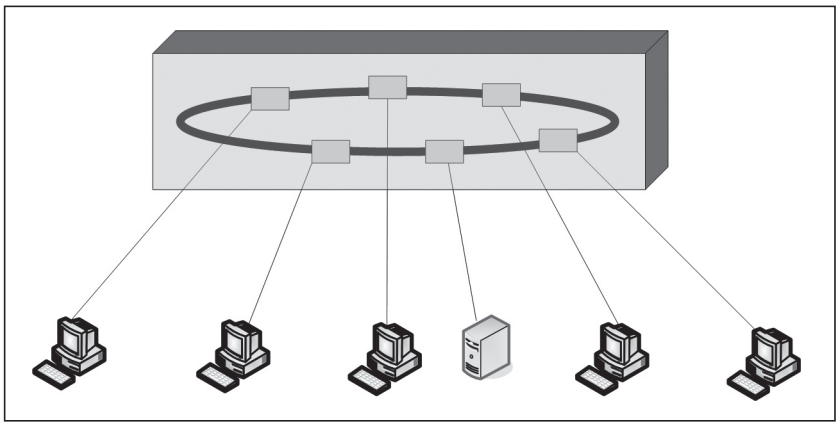


Figura 7.29. *MAU.*

7.7.3 FDDI

Las redes **FDDI (Fiber Distribuited Data Interface, Interfaz de datos distribuidos para fibra)** han sido desarrolladas bajo los estándares ANSI X3T9.5 e ISO 9314. Su objetivo de diseño fue conseguir alcanzar una velocidad de transmisión de 100 Mbps para lo cual se utilizó como medio de transmisión la fibra óptica. Posteriormente se desarrolló el estándar CDDI que es la implementación de FDDI pero utilizando cable de par trenzado, el cual no ha tenido mucha repercusión. Los desarrollos posteriores de Ethernet, como Fast Ethernet y Gigabit Ethernet, han hecho que este tipo de redes haya dejado de utilizarse.

El principal uso que han tenido las redes FDDI es como backbone (red troncal) de redes LAN, especialmente si la distancia a cubrir es elevada, ya que esta tecnología, al utilizar fibra óptica, alcanza distancias más grandes que el cable de par trenzado.

Las características más relevantes de las redes FDDI son:

- ✓ **Método de acceso:** paso de testigo, ya que utiliza topología lógica en anillo.
- ✓ **Direccionamiento:** se usan direcciones de 6 bytes contenidas en la NIC de forma similar a Ethernet.
- ✓ **Trama MAC:** parecida a la red en anillo.
- ✓ **Medio de transmisión:** fibra óptica multimodo.
- ✓ **Codificación:** NRZ-I y 4B/5B.

✓ **Velocidad de transmisión:** 100 Mbps.

✓ **Longitud máxima:** las redes FDDI pueden utilizan un anillo de hasta 200 Km de diámetro con un máximo de 1.000 estaciones conectadas.

Implementación del nivel físico

Las redes FDDI utilizan una topología en doble anillo físico. Cada nodo se conecta a un anillo por medio del llamado **MIC (Medium Interface Connector, Conector de interfaz al medio)**. Pueden existir tres tipos de nodos en una red FDDI:

- **DAS (Dual Attachment Station, Estación de conexión dual).** Este tipo de nodo tiene dos MIC y se conecta a los dos anillos de la red por lo que estos nodos tienen un alto grado de fiabilidad ya que en caso de fallo en uno de los anillos pueden conmutar al otro.
- **DAC (Dual Attachment Concentrator, Concentradores de conexión dual).** Este tipo de nodos se utilizan para conectar varios nodos sencillos (SAS) al anillo FDDI. Tiene dos MIC para conectarse al anillo dual y además una MIC por cada estación simple a la que da acceso. Este tipo de nodo proporciona una topología en estrella a partir del anillo dual.
- **SAS (Single Attachment Station, Estación de conexión simple).** Es el tipo de nodo más habitual en las redes FDDI y es el usado por ordenadores o servidores que forman parte de la red. No está conectada directamente al anillo sino que lo hace a través de un DAC.

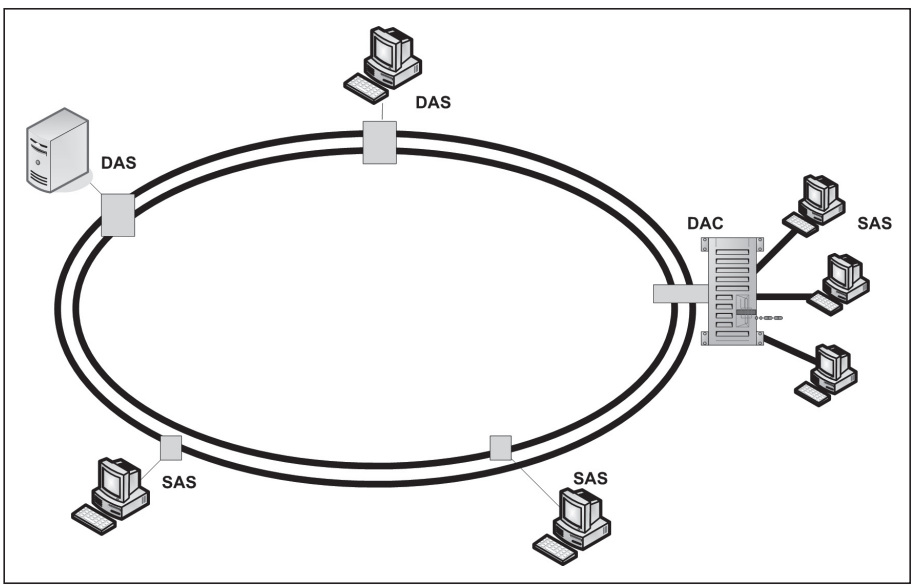


Figura 7.30. *Anillo dual FDDI.*

7.8 DISPOSITIVOS DE RED Y DE INTERCONEXIÓN DE REDES

7.8.1 REPETIDORES

Los repetidores operan sólo a nivel físico, por lo que se les considera dispositivos de interconexión de nivel 1. Se utilizan para unir dos segmentos de red, realizando la función de regeneración de los niveles eléctricos de la señal (no de amplificación).

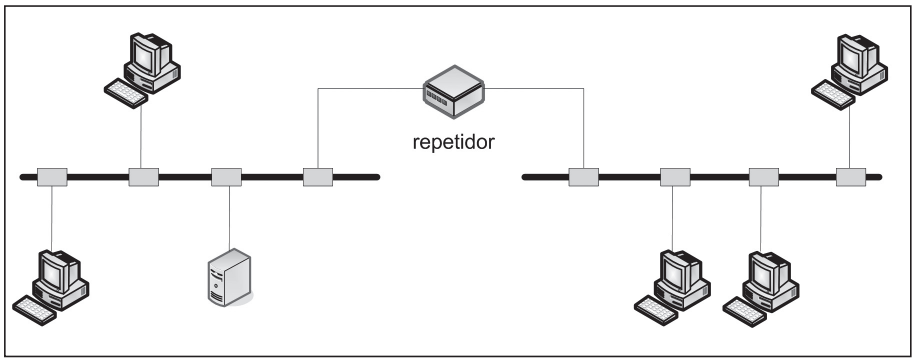


Figura 7.31. *Conexión de un repetidor.*

Permite extender la longitud física de la red pero no cambia la funcionalidad de la red. Las dos secciones que une un repetidor se denominan segmentos y forman parte de la misma red, con el mismo dominio de colisión.

Su uso fue común para redes 10BASE5 y 10BASE2 pero actualmente no se utilizan.

7.8.2 PUENTES (BRIDGES)

Los puentes operan en el nivel físico y de enlace por lo que se les considera dispositivos de interconexión de nivel 2. Su función principal es la de dividir una red grande en segmentos más pequeños. Para llevar a cabo esta función los puentes contienen la lógica necesaria para separar el tráfico de cada segmento.

Los puentes normalmente tienen dos puertos, en cada uno de los cuales se conecta un segmento de red. Cuando se recibe una trama por uno de los puertos, el puente lee la trama para obtener la dirección de destino, si dicha dirección se corresponde a una estación conectada al segmento de red desde el que se envió la trama, ésta es devuelta a la red y no se propaga al otro segmento. Si la dirección de destino se corresponde con una estación conectada al otro segmento, lo reenvía por el puerto correspondiente.

Debido a las características de su funcionamiento, se dice que los puentes reducen el dominio de colisión. Un **dominio de colisión** está formado por todas las estaciones que propagan sus tramas por un medio común y que por tanto son susceptibles de producir colisión. Lógicamente, cuantas más estaciones formen un dominio de colisión, más tráfico se generará, y habrá más posibilidades de colisión y más posibilidades de sobrecarga. Otro concepto utilizado es el llamado **dominio de difusión** formado por todas las estaciones que recibirían una trama de broadcast dentro de una red. Los puentes reducen los dominios de colisión pero mantienen los dominios de difusión.

Por tanto, al introducir un puente en una red se generan dos dominios de colisión más pequeños. Esta característica va a favorecer el rendimiento de una red sobrecargada.

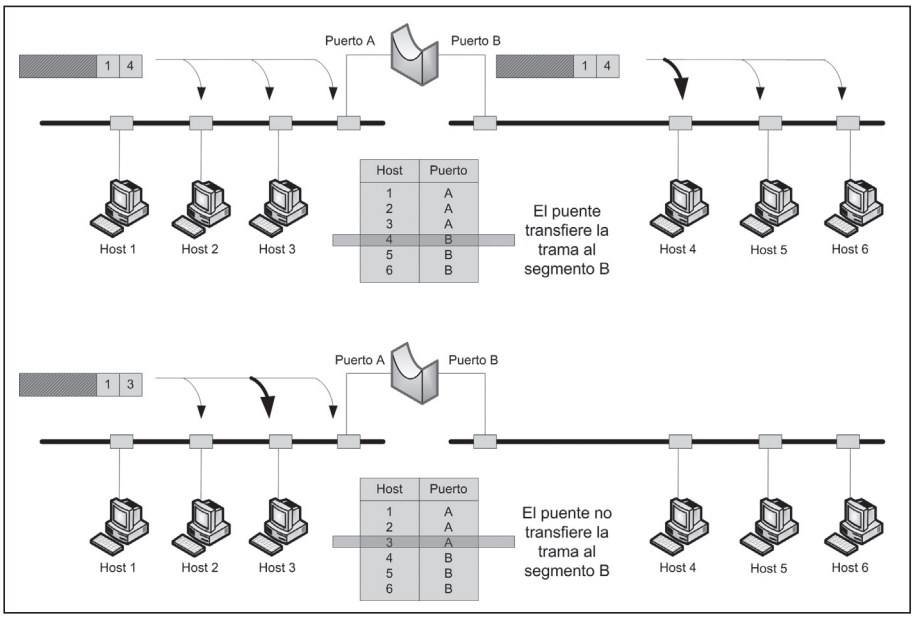


Figura 7.32. *Funcionamiento de un puente.*

Como se observa en la figura, el puente debe almacenar en una tabla interna todas las direcciones físicas de la red y el segmento al que pertenecen. En función de la forma en la que se obtenga esta información existen dos tipos de puentes:

- **Puente simple.** La tabla se gestiona de forma manual, es decir, un técnico debe introducir los datos adecuados. Es una técnica fácil de implementar pero difícil de mantener.
- **Puente transparente.** Han sido los más utilizados. La tabla se genera de forma dinámica por medio de un proceso de aprendizaje.

La construcción de la tabla de encaminamiento en los puentes transparente sigue el siguiente procedimiento:

1. Inicialmente la tabla estará vacía.
2. Cuando el puente recibe una trama por uno de sus puertos con una dirección de destino que no está en la tabla reenvía la trama.
3. Si la dirección origen de una trama no está en la tabla, almacena dicha dirección y el segmento desde el que ha recibido la trama.

La otra gran función de los puentes es la de conectar dos redes LAN que utilicen protocolos diferentes en el nivel de enlace, como por ejemplo, Ethernet y Token Ring. En este caso el puente debe resolver los problemas de adaptación como pueden ser:

- ✓ Velocidades de transmisión distintas
- ✓ Generación de testigo
- ✓ Formato de trama
- ✓ Formato de direcciones
- ✓ Detección de colisiones

Además el hecho de que los puentes acceden a la información de la trama MAC hace posible que se pueda realizar filtrado de tramas basándose en los campos del nivel MAC.

Con la aparición de los conmutadores, los puentes han ido progresivamente desapareciendo y actualmente se pueden considerar extinguidos.

7.8.3 CONMUTADORES O SWITCHES

Un **conmutador o switch** se puede definir como un puente transparente multipuerto. Se le puede considerar un dispositivo de interconexión de nivel 2. Un switch realiza prácticamente la misma función que un puente, utilizando la técnica del aprendizaje transparente para la gestión de la tabla de encaminamiento. En lugar de tener sólo dos puertos, un switch puede tener múltiples puertos.

El proceso de aprendizaje de los switches es similar al de los puentes. Cuando un switch recibe una trama cuya dirección de destino no está en la tabla de encaminamiento, reenvía la trama por todos sus puertos excepto por el que recibió la trama. Si la dirección de origen de una trama no está incluida en la tabla de encaminamiento, añade dicha dirección a la tabla junto con el número de puerto por el que se ha recibido la trama.

Al igual que en los puentes, cada puerto en un switch es un dominio de colisión separado, con lo cual no propaga colisiones. Si se conectan estaciones a cada uno de los puertos del conmutador, cada estación forma su propio dominio de colisión. Al igual que los puentes, todas las estaciones conectadas a un conmutador pertenecen al mismo dominio de difusión.

Tabla 7.4 Ejemplo de tabla de encaminamiento en un switch

Dirección MAC	Puerto
00:04:3B:8C:A5:73	8
00:0C:29:95:1F:B1	3
00:17:D8:65:20:03	1
00:09:7D:27:77:A8	2
00:24:98:C2:23:44	4

Buffers

Un switch debe usar buffers para almacenar los datos que llegan a los puertos antes de poder ser reenviados. Esto permite al switch transferir tramas a través de su arquitectura interna y conectar puertos que trabajen a diferentes velocidades.

Los buffers pueden ser implementados en la salida de los puertos, en la entrada de los puertos o una combinación de ambos. Lo más habitual es implementarlos en la salida ya que es el modo más eficiente, consiguiéndose unos índices de eficacia cercanos al 98%.

Los buffers utilizan la memoria RAM que incluye internamente el switch. Aunque, hay algunos switches que utilizan una cantidad de memoria fija para cada puerto, lo más habitual y efectivo es que el tamaño de memoria RAM utilizada por cada buffer sea variable en función de la carga de datos. Así, un puerto que tenga poca actividad, utilizará poca memoria para su buffer, de forma que otros puertos con más actividad pueden disponer de más cantidad de memoria para los suyos.

Half/Full-dúplex

Como se ha visto en los apartados anteriores, el método de acceso al medio CSMA/CD obliga a que las comunicaciones en una LAN sean half-dúplex. Sin embargo, el uso de conmutadores permite las comunicaciones full-dúplex, por lo que el ancho de banda efectivo respecto a redes con hub se duplica. Así, una red Fast Ethernet con una velocidad de 100 Mbps aumentará a 200 Mbps utilizando un switch que permita el modo full-dúplex. Lógicamente, este modo de funcionamiento también lo deben soportar las tarjetas de red de los dispositivos conectados al switch.

Técnicas de conmutación

Existen dos técnicas para llevar a cabo la transferencia de los datos entre puertos de un switch:

- **Reenvío directo (cut-through).** En esta técnica, cuando un switch comienza a recibir datos por un puerto, no espera a leer la trama completa para reenviarla al puerto destino. En cuanto lee la dirección de destino de la trama MAC, comienza a transferir los datos al puerto destino.

Esta técnica proporciona unos tiempos de retardo bastante bajos, del orden de los 20 μs. Sin embargo, tiene como inconveniente que sólo puede usarse cuando las velocidades de todos los puertos son iguales.

Otro problema que plantea la técnica cut-through, debido a su forma de funcionamiento, es que los switches propagan tramas erróneas o tramas afectadas por colisiones. Una posible mejora para evitar la propagación de tramas con colisiones es retrasar el reenvío hasta que se lean los primeros 64 bytes de trama, ya que las colisiones sólo se pueden producir en los primeros 64 bytes de la trama. Esta mejora sin embargo aumenta el tiempo de retardo hasta los 50 μs.

- **Almacenamiento y reenvío (Store and Forward).** En este caso, cuando un switch recibe datos por un puerto, almacena la trama completa en el buffer para luego reenviarla al puerto destino. La utilización de esta técnica permite realizar algunas comprobaciones de error antes de ser enviada al puerto de destino.

  El tiempo de retardo introducido es variable ya que depende del tamaño de la trama, oscilando en unos valores de 50 a 2.000 μs. Sin embargo, es imprescindible utilizar esta técnica cuando existen puertos funcionando a diferentes velocidades.

Sea cual sea la técnica utilizada, la conmutación de puertos que se lleva a cabo en los switches es mucho más rápida que en los puentes ya que se lleva a cabo en el hardware, mientras que en los puentes se implementa mediante software.

Tipos de switches

Una red LAN puede estar formada por unas pocas estaciones o por cientos o miles de dispositivos. Para las redes más grandes es necesario establecer una jerarquía de conectividad apoyada en las normas de cableado estructurado. Se han diseñado diferentes tipos de switches en función del lugar que ocupen en la jerarquía que ocupan en la red.

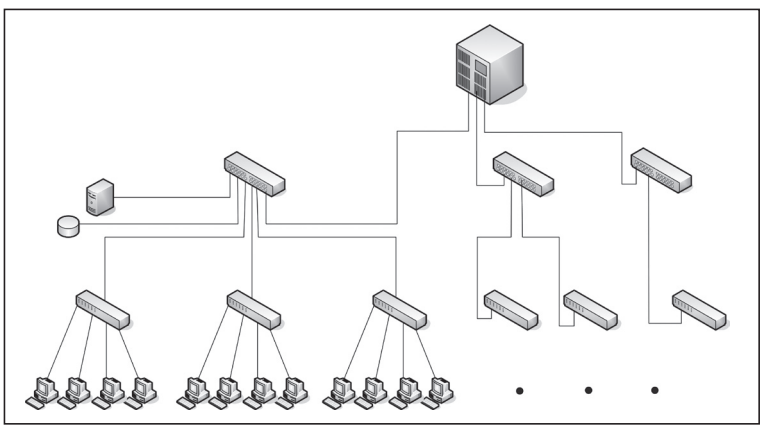


Figura 7.33. *Esquema jerárquico de una red con switches.*

Para implementar esta topología, los switches incluyen puertos especiales denominados **puertos uplink** que son utilizados para la conexión con otro dispositivo de interconexión (normalmente otro switch) de jerarquía superior. Los puertos uplink incluso suelen admitir velocidades superiores al resto de puertos del switch. Los hubs también necesitan puertos uplink para su conexión con dispositivos de jerarquía superior. Lo que hace este puerto es intercambiar los sentidos de transmisión, con lo que su función es equivalente a utilizar un cable de par trenzado cruzado.

- **Switch Desktop:** este tipo de switch está diseñado para sustituir a los hubs tradicionales, es decir, a cada puerto del switch se conecta un solo dispositivo de red (ordenador, impresora...). Normalmente la sustitución de un hub por un switch de este tipo es muy sencilla. Suelen proporcionar pocas opciones de configuración.

Figura 7.34. *Switch.*

- **Switch Workgroup o de departamento:** suelen ser switches modulares (se aumenta la capacidad añadiendo tarjetas) o apilables para poder aumentar el número de puertos. Suelen tener los dos tipos de puertos, un tipo para conectarse a dispositivos inferiores en la estructura jerárquica de la red, que podrían ser hubs, switch desktop o servidores. Y el otro tipo de puertos a mayor velocidad para su conexión al backbone de la red.

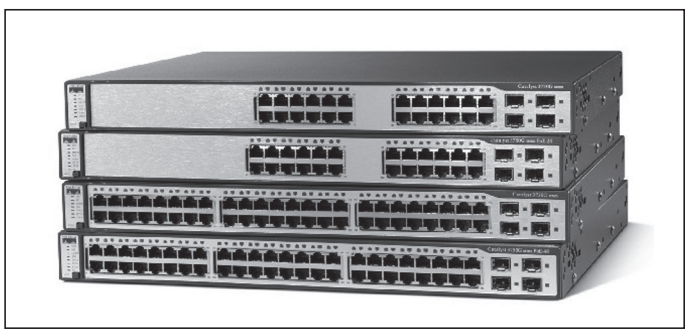


Figura 7.35. *Switch apilable.*

- **Switch backbone (también llamados Enterprise):** son utilizados en el corazón de las grandes redes LAN. Ofrecen características avanzadas de configuración, gestión y mantenimiento. Normalmente son modulares, es decir, se puede aumentar su capacidad añadiendo tarjetas. Además, permiten la ampliación de sus capacidades "en caliente", es decir, sin desconectar el dispositivo.

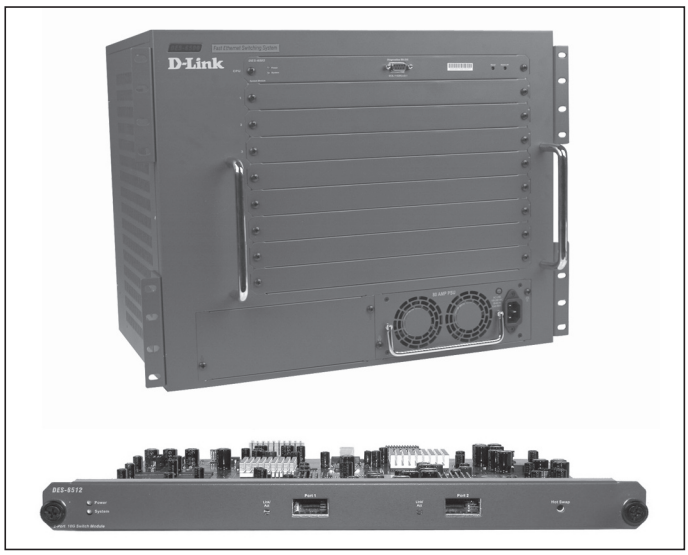


Figura 7.36. *Chasis para switch de backbone y tarjeta 10-Gigabit Ethernet.*

Según en la categoría en la que se engloben, las prestaciones serán superiores, es decir, mayor velocidad, mayor número de puertos, mayor variedad de medios físicos y mayores tablas de encaminamiento.

Actualmente existen switches con funciones de nivel 3 que pueden encaminar paquetes en función de la dirección IP. Estos conmutadores también tienen capacidades avanzadas de gestión. Pueden ser configurados a nivel de red y normalmente habilitan una interfaz web para su gestión.

Algoritmo Spanning Tree

El algoritmo Spanning Tree (árbol de expansión) se utiliza en los switches para prevenir los bucles lógicos que pueden aparecer en una red. Los bucles se producen cuando existen varios caminos distintos entre dos puntos de la red y su efecto es que las tramas pueden circular de forma indefinida atrapadas en un bucle sin conseguir alcanzar su destino, lo que además afectará negativamente al rendimiento de la red.

El algoritmo Spanning Tree ayuda a los switches a elegir el camino más idóneo y, por tanto, elimina los bucles. Se utiliza sobre todo en switches workgroup o en switches de backbone.

El uso de este algoritmo está especificado en el estándar IEEE 802.1D. En 1998 se hizo una revisión del mismo añadiendo variaciones para optimizar su funcionamiento, el resultado se llamó **Spanning tree rápido** y está especificado en la norma IEEE 802.1w

Redes virtuales: VLAN

Una de las características más importantes que añaden los conmutadores es la posibilidad de configurar redes LAN virtuales, también llamadas VLAN. El funcionamiento VLAN se basa en agrupar los dispositivos conectados al switch en subredes virtuales o segmentos VLAN. Dichos segmentos, a todos los efectos, se comportan como subredes diferentes y forman dominios de difusión separados. Una estación situada en una VLAN determinada no podrá comunicarse con otra estación situada en otra VLAN diferente, aunque, lógicamente compartan el medio de transmisión o el dispositivo de interconexión. Para poder comunicar dos estaciones situadas en dos VLAN diferentes será necesario utilizar un dispositivo de interconexión de redes de nivel 3, es decir, un router.

Se dice que los switches con la funcionalidad VLAN llevan a cabo una segmentación de la red a nivel lógico. La definición de una VLAN en un switch se puede hacer por alguno de los siguientes criterios:

- ✓ Por puerto (nivel 2)
- ✓ Por direcciones MAC (nivel 2)
- ✓ Por el tipo de protocolo
- ✓ Por nivel 3

El funcionamiento de VLAN está especificado en el estándar IEEE 802.1q. En dicho estándar se especifica la etiqueta (también conocida como tag) que se añade a la trama Ethernet original. Dicha etiqueta está formada por 4 bytes.

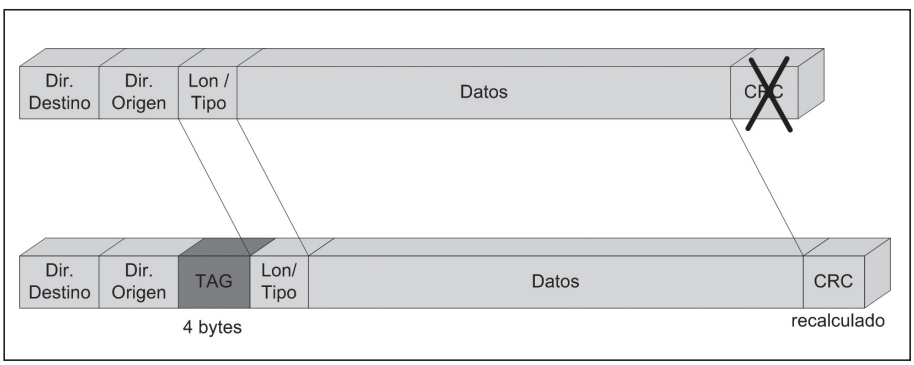


Figura 7.37. *Trama IEEE 802.1Q.*

Los campos de los que consta la etiqueta VLAN son los siguientes:

- **TPID (Tag Protocol Identifier).** Contiene el valor 0x8100 para identificar una trama 802.1q.
- **Prioridad.** Campo formado por 3 bits, por lo que se pueden representar hasta ocho niveles de prioridad.
- **Indicador canónico.** Formado por un bit que normalmente está a 0.
- **VID.** Son 12 bits y contiene el número identificador de la VLAN a la que pertenece la trama.

Las tramas que contienen una etiqueta VLAN podrán tener una longitud total de entre 68 y 1522 bytes.

Hay que tener en cuenta que como la etiqueta se añade a la trama Ethernet original, se hace necesario recalcular el CRC de la trama antes de su envío.

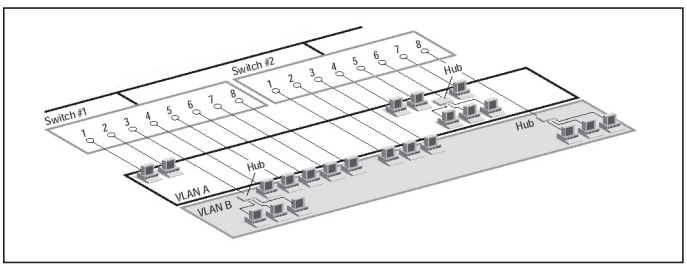


Figura 7.38. *Redes VLAN.*

En algunos modelos de switches, la configuración de las redes VLAN y en general de los parámetros de funcionamiento del switch se lleva a cabo conectando un PC al switch a través de un puerto serie y utilizando un software específico proporcionado por el fabricante. Se puede ver un ejemplo en la siguiente figura.

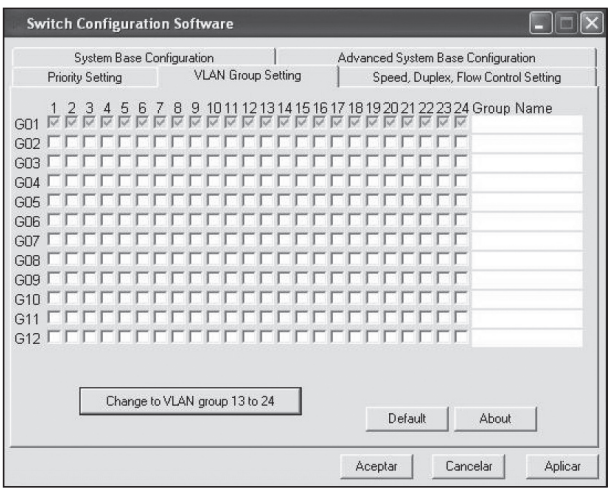


Figura 7.39. *Ejemplo de software de configuración de VLAN.*

En los modelos de switch más avanzados la configuración del switch incluidas las funciones de VLAN se puede hacer además vía web. En este caso, el switch implementa un servidor http interno que proporciona las páginas web para llevar a cabo la configuración. En este caso, el switch deberá tener una dirección IP válida.

7.8.4 OTROS DISPOSITIVOS DE INTERCONEXIÓN

Routers o encaminadores

Son dispositivos más sofisticados que los repetidores y puentes. Actúan en los niveles físico, de enlace y de red. Es el dispositivo usado para unir dos o más redes. Su funcionamiento se verá con detalle en el próximo capítulo.

Gateways

Término utilizado para designar a los dispositivos que actúan en los siete niveles del modelo OSI. También se pueden denominar convertidores de protocolos. Normalmente se implementan como software instalado dentro de un router. Se utilizan para enlazar redes con protocolos muy diferentes, por ejemplo SNA y TCP/IP.

7.9 PRÁCTICA

El objetivo de esta práctica es comprobar el funcionamiento de las redes Ethernet.

7.9.1 MATERIAL UTILIZADO POR GRUPO

- ✓ 1 Cable UTP Categoría 5
- ✓ 4 Conectores RJ-45
- ✓ 1 Herramienta crimpadora
- ✓ 3 Ordenadores con una tarjeta de red instalada
- ✓ 1 Hub
- ✓ 1 Switch
- ✓ 1 Aplicación de captura de tramas: Ethereal (software libre)

7.9.2 LAN CON CABLE ETHERNET CRUZADO

Se puede construir una red de área local de dos equipos utilizando simplemente un cable UTP de cuatro pares y cruzando los pares de transmisión y recepción. Es lo que se conoce como cable Ethernet cruzado.

1. Obtener la información necesaria para construir un cable Ethernet cruzado.
2. Utilizando cable UTP de categoría 5, dos conectores RJ-45 y la herramienta de crimpar construir un cable Ethernet cruzado.
3. Conectar dos ordenadores utilizando dicho cable.
4. Si es necesario, configurar los parámetros de red de los ordenadores (dirección IP y máscara de red).
5. Comprobar la conectividad utilizando el comando ping desde el símbolo de sistema. Para conocer las opciones de uso: ping /?.
6. Comprobar el funcionamiento de la red utilizando el protocolo de compartición de ficheros y directorios de Windows.

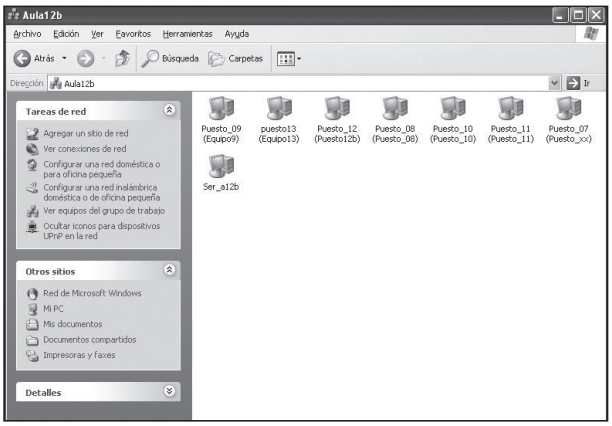


Figura 7.40. *Ventana de Entorno de Red de Windows desde donde se accede a los recursos compartidos de equipos Windows.*

7. Comprobar si se pueden configurar manualmente los parámetros de velocidad y modo half/full-dúplex de la tarjeta de red. En caso afirmativo comprobar el funcionamiento de la comunicación con las diferentes combinaciones admitidas.
8. Medir la velocidad de transmisión mediante la transferencia de ficheros entre los dos equipos. Realizar pruebas con ficheros de diferente tamaño y a diferente velocidad. Probar la velocidad con dos transmisiones simultáneas.

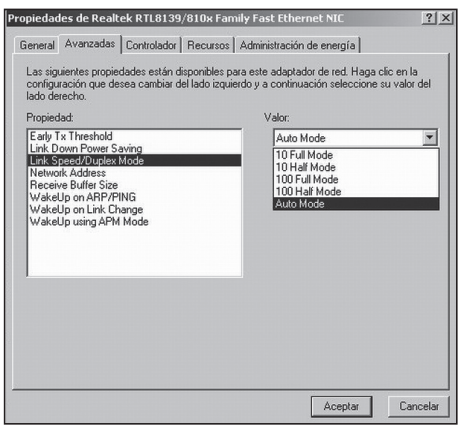


Figura 7.41. *Ventana de configuración de la tarjeta de red.*

9 Incluir en la memoria:

- ✓ La descripción del proceso de realización del ejercicio.
- ✓ La información obtenida para la construcción del cable Ethernet cruzado.
- ✓ Información de la tarjeta de red (NIC) de los equipos, incluida la dirección física o dirección MAC (para ver la dirección MAC se puede utilizar el comando ipconfig /all).
- ✓ Salida de las ejecuciones del comando ping.
- ✓ Tabla comparativa de las velocidades de transmisión para los diferentes supuestos planteados.

7.9.3 LAN CON HUB

Construir una red de área local utilizando un hub. Para ello será necesario utilizar cables Ethernet.

1 Obtener la información necesaria para construir un cable Ethernet.

2 Utilizando cable UTP de categoría 5, dos conectores RJ-45 y la herramienta de crimpar construir un cable Ethernet.

3 Conectar dos ordenadores utilizando un hub. Se pueden utilizar los mismos parámetros de conexión que en el apartado anterior.

4 Comprobar la conectividad utilizando el comando ping.

5 Comprobar el funcionamiento de la red utilizando el protocolo de compartición de ficheros y directorios de Windows.

6 Medir la velocidad de transmisión mediante la transferencia de ficheros. Realizar pruebas con ficheros de diferente tamaño. Probar la velocidad con dos transmisiones simultáneas.

7 Responder a las siguientes cuestiones:

- ✓ ¿Cómo se podría distinguir un cable Ethernet de un cable Ethernet cruzado de forma visual?
- ✓ ¿Cómo se comprueba que existe un equipo conectado al puerto del hub?
- ✓ ¿Cómo se indica la existencia de colisiones en el hub?
- ✓ ¿De las dos topologías implementadas cuál alcanza mayor velocidad? ¿De qué factores depende dicha velocidad? ¿Alguna de las dos topologías es full-dúplex?

8 Incluir en la memoria:

- ✓ La descripción del proceso de realización del ejercicio.
- ✓ La información obtenida para la construcción del cable Ethernet.
- ✓ Tabla comparativa de las velocidades de transmisión para los diferentes supuestos planteados.
- ✓ La respuesta a las cuestiones planteadas.

7.9.4 CAPTURA DE TRAMAS

Conectar y configurar un tercer equipo en la red del apartado anterior. Instalar en uno de los equipos la aplicación Ethereal (software libre bajo licencia GNU, recientemente ha cambiado de nombre a Wireshark) para la captura y análisis de datos en una red.

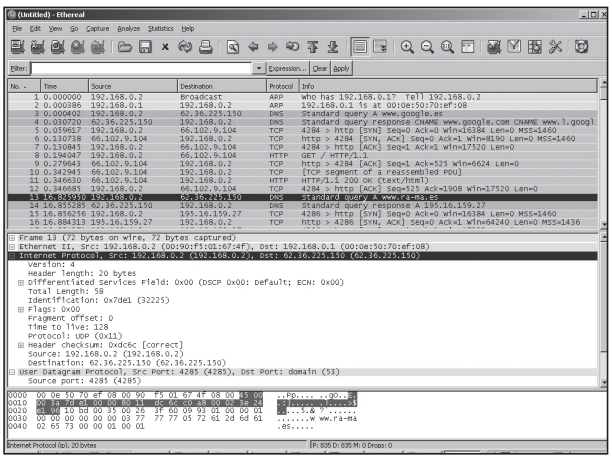


Figura 7.42. *Aplicación Ethereal.*

1. Comprobar la conectividad de los tres equipos utilizando el comando ping.
2. Comprobar que se producen colisiones realizando envíos simultáneos de datos.
3. Configurar la aplicación Ethereal en modo promiscuo (captura de todos los paquetes que lleguen a la NIC). Iniciar la captura y ejecutar el comando ping entre los otros dos equipos de la red. Comprobar que el hub reenvía los paquetes

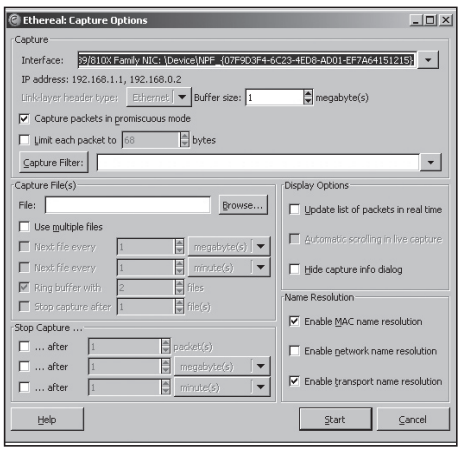


Figura 7.43. *Ventana de configuración de Ethereal.*

a todos sus puertos y por tanto el comando ping también le llega al equipo donde está instalado Ethereal, aunque no sea el destino de los datos.

4 Incluir en la memoria:

- ✓ La configuración de los parámetros de red del tercer equipo.
- ✓ La descripción del proceso de realización del tercer apartado.

7.9.5 EXTENDER LA LAN

1 Unir las redes de dos grupos de trabajo uniendo sus hubs.

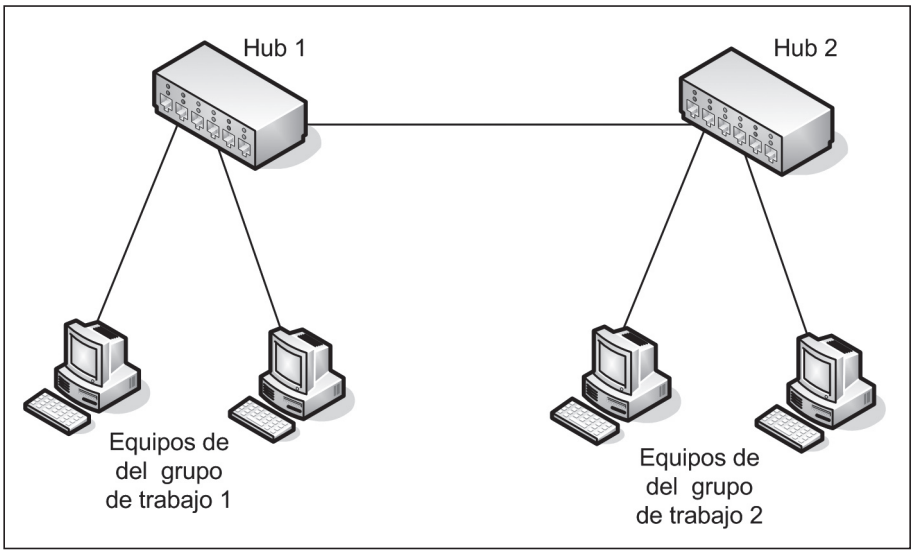


Figura 7.44. *Esquema de conexionado uniendo los hubs.*

2 Configurar los equipos para que cada equipo se pueda comunicar con el resto de equipos.

3 Comprobar que los paquetes enviados entre dos equipos conectados al mismo hub se retransmiten a los equipos del otro hub.

4 Incluir en la memoria:

- ✓ La descripción del proceso de realización de este apartado.
- ✓ Configuración de todos los equipos.

7.9.6 USO DE UN SWITCH

1 Unir las redes de dos grupos de trabajo esta vez utilizando un switch.

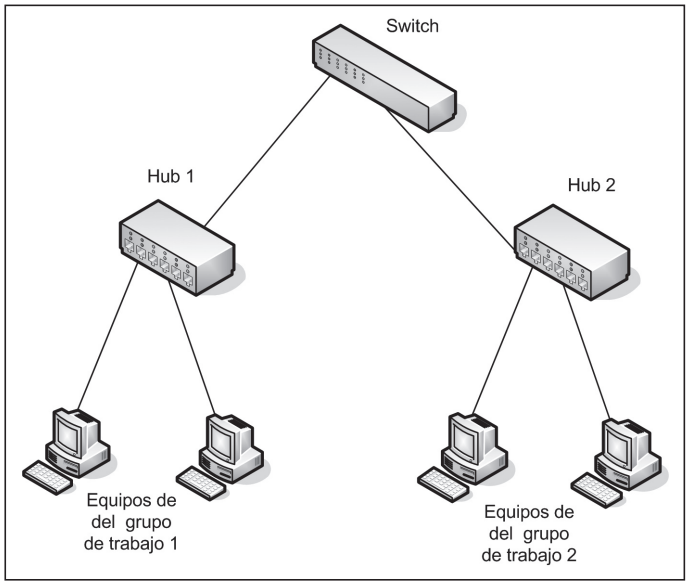


Figura 7.45. *Esquema de conexionado uniendo los hubs mediante un switch.*

2 Sin realizar ningún cambio en la configuración comprobar que los paquetes enviados entre dos equipos de un segmento no se retransmiten al otro segmento.

3 Incluir en la memoria:

- ✓ La descripción del proceso de realización de este apartado.
- ✓ Configuración de todos los equipos.

RESUMEN DEL CAPÍTULO

Posiblemente uno de los sistemas telemáticos más extendidos actualmente sean las redes de área local o LAN. Las tecnologías LAN se encargan de especificar los dos primeros niveles de la arquitectura de red, el nivel físico y el nivel de enlace.

En este capítulo se ha dado una extensa visión a las tecnologías de redes LAN especialmente las que están actualmente en vigor: Ethernet, con todas sus evoluciones, como Fast Ethernet y Gigabit Ethernet, y las redes inalámbricas conocidas como redes Wi-Fi. Se ha hecho un repaso histórico a las redes Ethernet explicando las implementaciones más utilizadas hasta llegar al estándar que se ha impuesto, 10BASE-T. Todas ellas utilizan CSMA/CD como mecanismo de acceso al medio.

En la segunda mitad de los años 90 se produce un espectacular desarrollo de las redes Ethernet con la llegada de Fast Ethernet a 100 Mbps, que sigue siendo el tipo de red más utilizado en la actualidad. Además se desarrollan las redes Ethernet conmutadas donde se sustituye el hub o concentrador por un switch o conmutador, elemento clave del aumento de prestaciones de las redes LAN. Por último, en el año 1997 aparece el modo de funcionamiento full-dúplex que hace innecesario el uso de CSMA/CD y duplica el ancho de banda efectivo de las redes.

El otro tipo de redes LAN en plena expansión en la actualidad son las redes inalámbricas. Se estudia el principal estándar, el IEEE 802.11, conocido también como Wi-Fi. Un apartado especialmente importante habla sobre los mecanismos de seguridad utilizados en Wi-Fi.

A pesar de estar prácticamente extinguidas, se muestran brevemente algunos de los principales aspectos de otros tipos de redes LAN como Token Bus, Token Ring y FDDI.

Para acabar el capítulo se estudian los dispositivos de interconexión utilizados en redes LAN, especialmente el dispositivo más extendido en la actualidad, el switch o conmutador.

Las redes LAN, hoy

Actualmente se han impuesto como tecnologías LAN las redes Fast Ethernet para redes LAN cableadas. Y Wi-Fi para redes LAN

inalámbricas. Las redes FDDI utilizadas como backbone de las LAN han sido sustituidas por el estándar ATM, que se estudiará en el capítulo 9, o por Gigabit Ethernet.

El resto de tecnologías LAN están prácticamente en desuso actualmente.

EJERCICIOS PROPUESTOS

- **1.** Representa gráficamente la señal eléctrica producida por una tarjeta de red 100BASE-TX para el envío del dato 010100000011.

- **2.** Calcular la proporción entre bits de información sobre el total de bits transmitidos para el caso del tamaño máximo de trama Ethernet. Repetirlo para el caso del tamaño mínimo de trama. Repetir los cálculos anteriores para la trama Ethernet con Carrier Extension utilizada en Gigabit Ethernet. Obtener conclusiones sobre los resultados.

- **3.** Explicar razonablemente por qué no se pueden conectar dos hubs o dos switch directamente por medio de un puerto normal, sino que es necesario utilizar un puerto especial o puerto uplink.

- **4.** Con un capturador de tramas se ha obtenido la siguiente información, expresada en formato hexadecimal. No se incluye el preámbulo y el byte de comienzo de trama.

*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00	FF	FF	FF	FF	FF	FF	00	00	48	B7	E7	B2	00	2B	E0	E0
16	03	FF	FF	00	28	00	01	00	00	00	00	FF	FF	FF	FF	FF
32	FF	04	53	00	00	00	00	00	00	48	B7	E7	B2	57	FD	00
48	01	FF	FF	FF	FF	00	00	00	00	00	00	00	B3	78	12	C9

¿De qué tipo de trama se trata? Obtener los valores de todos los campos de la cabecera y su función.

■ **5.** Repetir el ejercicio anterior con las siguientes capturas:

*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00	00	A0	C5	38	70	70	00	13	8F	73	76	DA	08	00	45	00
16	00	28	AA	99	40	00	80	06	81	42	0A	0C	02	0D	D4	AA
32	EE	30	09	FE	00	50	BD	B2	FF	5E	7B	EB	A8	89	50	10
64	44	70	B0	9B	00	00	00	00	00	00	00	00	F6	A1	06	BA

*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00	00	13	8F	73	76	DA	00	20	EA	2F	E5	EE	81	00	00	03
16	08	06	00	01	08	00	06	04	00	02	00	20	EA	2F	E5	EE
32	AC	00	00	01	00	13	8F	73	76	DA	AC	A8	64	0D	88	88
64	88	88	88	88	88	88	88	88	88	88	88	88	4A	26	09	C4

■ **6.** Se quiere mejorar el rendimiento de la red que aparece en la figura añadiendo un switch de ocho puertos. Dibujar la nueva topología mejorada.

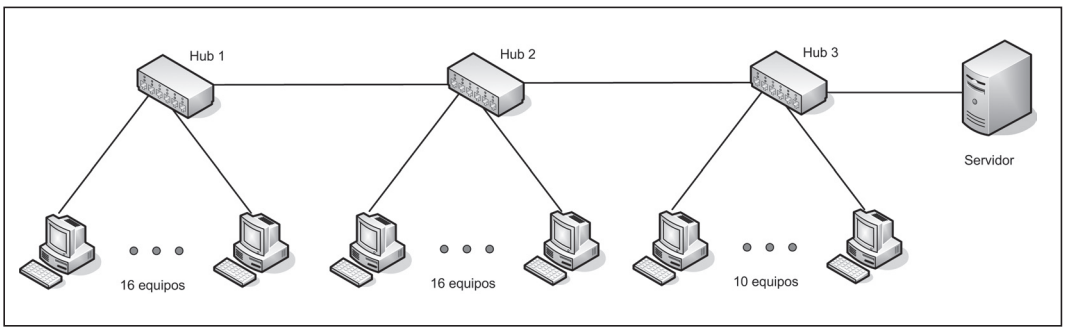


Figura 7.46. *Red del ejercicio 6.*

■ **7.** A partir de la topología de red en un departamento:
- ✓ ¿Cuántos dominios de colisión hay?
- ✓ ¿Cuántos dominios de difusión hay?
- ✓ Dibujar una nueva topología que cumpla las siguientes características:
- ✓ PC1 es un servidor con un alto volumen de datos.
- ✓ PC2, PC3 y PC4 forman un dominio de colisión.
- ✓ PC5, PC6 y PC7 forman un dominio de colisión.
- ✓ Se quiere añadir una impresora láser en red para todo el departamento.

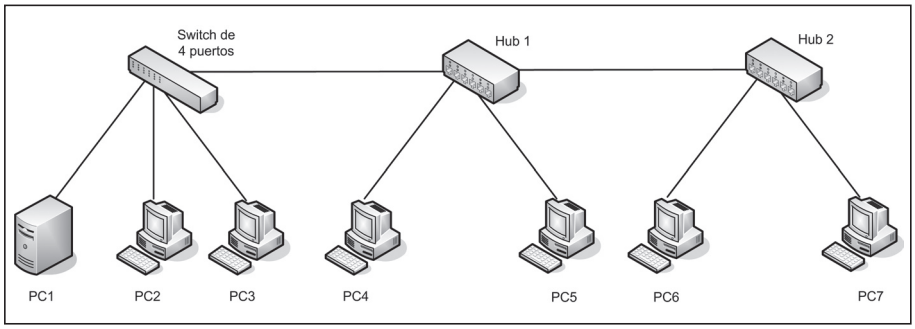


Figura 7.47. *Topología de red del ejercicio 7.*

TEST DE CONOCIMIENTOS

1 La principal diferencia entre IEEE 802.11b y IEEE 802.11g es:
- **a)** IEEE 802.11b no es un estándar abierto y IEEE 802.11g sí lo es.
- **b)** IEEE 802.11b no incluye mecanismos de seguridad y IEEE 802.11g sí los incluye.
- **c)** IEEE 802.11b alcanza 11 Mbps y IEEE 802.11g alcanza hasta 54 Mbps.
- **d)** IEEE 802.11b opera en la banda de 2.4 GHz y IEEE 802.11g en la banda de 5 GHz.

2 El dispositivo utilizado para crear redes virtuales (VLAN) es:
- **a)** Puente.
- **b)** Switch.
- **c)** Router.
- **d)** Cualquiera de los anteriores.

3 Las tecnologías de redes LAN implementan las funciones OSI:
- **a)** De todos los niveles excepto el de aplicación.
- **b)** De los niveles físico y de enlace.
- **c)** De los niveles físico, de enlace y de red.
- **d)** Depende del tipo de red.

4 Para el subnivel LLC en las redes IEEE se cumple que:
- **a)** El formato de trama utilizado depende del tipo de red.
- **b)** En los campos DSAP y SSAP de la trama se almacenan las direcciones físicas de los dispositivos que se comunican.
- **c)** El campo de control no se utiliza.
- **d)** Una de sus funciones es proporcionar un formato único de datos al nivel superior.

5 Una de las diferencias entre las redes Ethernet y las redes IEEE 802.3 es:
- **a)** Ethernet es un estándar propietario y 802.3 es un estándar abierto.
- **b)** Las tramas Ethernet son mayores a las tramas 802.3, aun así son compatibles.

c) Las redes Ethernet no utilizan el subnivel LLC y las redes 802.3 sí.
d) Las redes Ethernet sólo utilizan cable de par trenzado y las redes 802.3 también pueden usar cable coaxial.

6 Una de las diferencias entre redes 10BASE2 y 10BASE-T es:
a) La longitud máxima, que es el doble en las redes 10BASE-T.
b) La topología lógica, que es un bus en 10BASE2 y una estrella en 10BASE-T.
c) El medio de transmisión, que es cable coaxial en 10BASE2 y cable de par trenzado en 10BASE-T.
d) Todas las anteriores son correctas.

7 La conmutación Ethernet se puede utilizar:
a) Sobre cualquier rede 10BASE-T.
b) Sobre cualquier red Fast Ethernet.
c) Sobre cualquier red Fast Ethernet o Gigabit Ethernet.
d) Sobre cualquier red Ethernet que utilice un switch en lugar de un hub.

8 La dirección MAC en las redes Ethernet las configura:
a) El usuario del equipo.
b) El administrador de la red.
c) Cualquier usuario con permisos de administración.
d) No se puede cambiar.

9 La diferencia entre una trama Ethernet y una trama IEEE 802.3 es:
a) El tercer campo de la cabecera es el Tipo en Ethernet, y la Longitud en IEEE 802.3.
b) No hay diferencia en la trama MAC, la diferencia es que la trama IEEE 802.3 encapsula una trama LLC.
c) Las direcciones de la trama Ethernet son de 6 bytes y en IEEE 802.3 son de 2 bytes.
d) La trama Ethernet necesita una longitud mínima de los datos de 46 bytes y la trama IEEE 802.3 no.

10 En las redes 100BASE-TX se utiliza la codificación:
a) Manchester.
b) Manchester diferencial.
c) MLT-3 junto con la codificación binaria 4B/5B.
d) NRZ-I junto con la codificación binaria 4B/5B.

11 El modo de operación full-dúplex:
a) No funciona utilizando un hub.
b) No necesita CSMA/CD.
c) Se puede utilizar tanto en Fast Ethernet como en Gigabit Ethernet.
d) Todas las anteriores son correctas.

12 El sistema de seguridad Wi-Fi conocido como WPA:
a) Fue el primer sistema de seguridad implementado y el más inseguro.
b) Fue desarrollado por la Wi-Fi Alliance como una mejora de WEP.
c) No se utiliza actualmente por ser demasiado complejo.
d) Es incompatible a nivel hardware con WEP.

13 Los puentes:
a) Son los dispositivos de interconexión más utilizados actualmente.
b) Reducen tanto el dominio de colisión como el de difusión.
c) Son capaces de acceder a la trama MAC por lo que se les considera dispositivos de interconexión de nivel 2.
d) Todas las anteriores son correctas.

14 Los puertos uplink en los switch se utilizan:
a) Para la conexión a dispositivos de interconexión de una jerarquía superior.
b) Para la conexión del switch con servidores.
c) Para la conexión del switch a los equipos que no admitan full-dúplex.
d) Para la conexión de un switch de backup.

15 Las redes Token Ring:
a) Son compatibles con Ethernet a nivel de trama aunque cambia la topología de la red.
b) Admiten tanto topología en bus como en anillo.
c) Utilizan codificación Manchester diferencial.
d) Alcanzan una velocidad máxima de 100 Mbps.

8 Arquitectura TCP/IP

Objetivos del capítulo

- Conocer las características principales de la arquitectura TCP/IP.
- Estudiar en detalle el protocolo IP así como los protocolos de red asociados (ARP, RARP e ICMP).
- Estudiar las principales características de los protocolos del nivel de transporte TCP y UDP.
- Entender el funcionamiento de los routers y los protocolos de encaminamiento.
- Conocer los principales protocolos del nivel de aplicación en la arquitectura TCP/IP.
- Estudiar algunos de los conceptos más avanzados utilizados en las redes TCP/IP actuales como Proxy, NAT, Firewall y VPN.
- Conocer las nuevas características que aporta el protocolo IPv6.

8.1 INTRODUCCIÓN

Durante los últimos capítulos se han estudiado con cierto detalle algunos tipos de comunicaciones que cubren las funciones de los niveles físico y de enlace de nuestro (teórico) modelo OSI de arquitectura de red.

En el capítulo 4 se estudian las interfaces serie, principalmente implementaciones del nivel físico (la interfaz USB, sin embargo, implementa funciones tanto del nivel físico como de enlace). En el capítulo 5 se profundiza en las técnicas para llevar a cabo las funciones del nivel de enlace y se dan a conocer algunos de los protocolos del nivel de enlace más populares, especialmente HDLC. Por último, en el capítulo 6 se da un amplio repaso a las redes de área local que cubren los niveles 1 y 2, es decir, físico y de enlace.

Es el momento de ascender al siguiente nivel del modelo OSI, el nivel 3 o nivel de red. Sin ninguna duda, el protocolo del nivel de red más importante actualmente en telemática es el protocolo IP, y lógicamente es el que se estudiará en este capítulo. Ocurre algo parecido con el nivel 4 o nivel de transporte, donde el protocolo TCP se impone de forma rotunda.

Estos dos protocolos además no se presentan aislados en los sistemas telemáticos sino que pertenecen a toda una arquitectura de red que incluye algunos otros protocolos auxiliares y que se conoce como arquitectura TCP/IP.

Por tanto, antes de adentrarnos en el estudio de los protocolos propiamente dichos vamos a ubicar adecuadamente la arquitectura a la que pertenecen.

8.2 ARQUITECTURA TCP/IP

Como ya se adelantó en el capítulo 3, la arquitectura de red TCP/IP es la que se ha impuesto en la actualidad y es la que se utiliza en Internet y, por extensión, en las millones de redes de área local que se interconectan.

En la arquitectura TCP/IP realmente no existe un modelo de red dividido en niveles, fundamentalmente por que su diseño se enfocó a implementar protocolos que solucionasen los requisitos de interconexión que se plantearon en su desarrollo inicial, y para ello no se partió de ningún modelo concreto. Así pues, el modelo en niveles de la arquitectura TCP/IP es un intento de acercamiento a OSI y se puede considerar sólo como una descripción de los protocolos existentes.

Aunque en el capítulo 3 se hizo una comparación en la que los modelos OSI y TCP/IP parecían muy similares, la figura 8.1 se acerca más a la realidad.

El modelo TCP/IP no diferencia los niveles físico y de enlace. Los protocolos TCP/IP comienzan en el nivel 3 de OSI de forma que se puede utilizar cualquier protocolo y cualquier tecnología en estos niveles inferiores. Posiblemente éste sea uno de los factores que más ha ayudado a la expansión de la arquitectura TCP/IP.

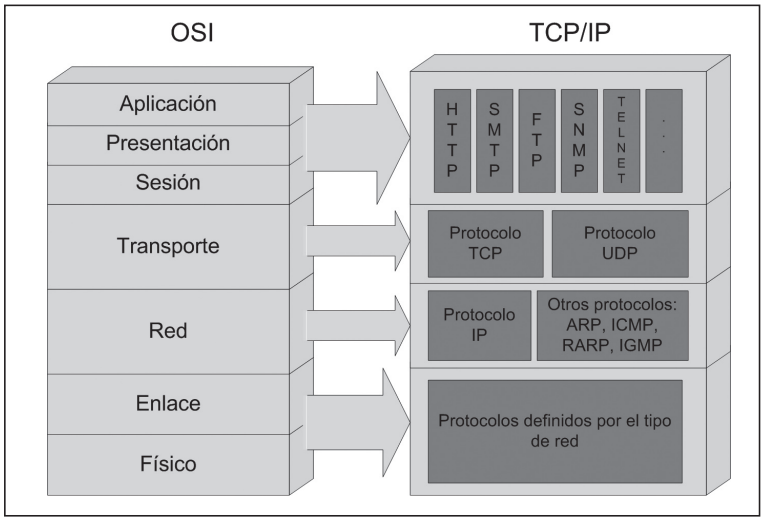


Figura 8.1. *Comparativa OSI- TCP/IP de cuatro capas.*

Como se observa, el grueso de la arquitectura se encuentra en los equivalentes a los niveles de red y de transporte, los cuales curiosamente cubren prácticamente las mismas funciones que sus homónimos en el modelo OSI. A partir de ahí, todo pertenece al nivel de aplicación.

También se puede establecer un cierto paralelismo con el modelo OSI, en la forma en la que se pasan los datos entre los diferentes niveles en la arquitectura TCP/IP. Como ocurre en el modelo OSI, los dispositivos de interconexión sólo implementan como máximo hasta el nivel de red.

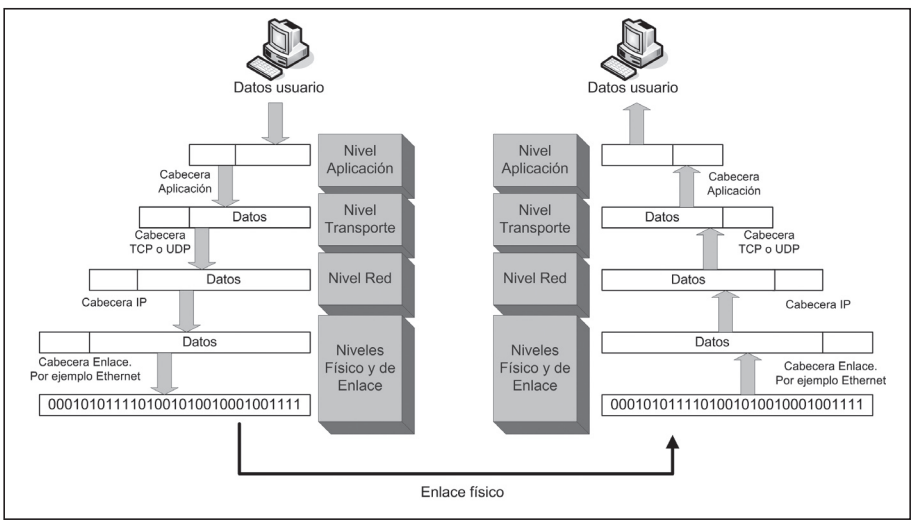


Figura 8.2. *Paso de datos entre capas.*

Por tanto, dichos dispositivos de interconexión no necesitan implementar la complejidad del protocolo de transporte, encargado de proporcionar fiabilidad a la comunicación. Esto tiene una importante consecuencia, las comunicaciones intermedias entre nodos de la red (normalmente llevadas a cabo por los llamados encaminadores o routers) son relativamente fáciles de hacer, y esto proporciona eficacia y rapidez a las operaciones de encaminamiento de datos, algo que también ha sido crucial en el desarrollo de esta arquitectura.

8.3 HISTORIA DE TCP/IP E INTERNET

La historia de la arquitectura TCP/IP va unida estrechamente a la historia de la propia Internet. El origen de Internet, así como de TCP/IP, fue la petición del Departamento de Defensa de Estados Unidos a su agencia de investigación llamada **ARPA (Advanced Research Projects Agency, Agencia de proyectos de investigación avanzados)** del diseño de una red confiable que uniera sus centros de datos. Aunque la razón de este encargo fue que el Departamento de Defensa de Estados Unidos consideraba que el tipo de líneas utilizadas en esa época (básicamente líneas telefónica alquiladas) no era muy fiable, hay bibliografía al respecto que sugiere que el verdadero motivo fue ofrecer fiabilidad a las comunicaciones en caso de una guerra nuclear, ya que todo esto ocurría a mediados de los años 60, en plena Guerra Fría.

NOTA 8.1

La agencia de investigación ARPA también ha recibido el nombre en diferentes fases de la historia de DARPA (Defense Advanced Research Projects Agency).

En cualquier caso, y para ofrecer fiabilidad a las transmisiones en caso de caídas de nodos de comunicación, se decidió diseñar una red basada en la conmutación de paquetes, a la que se llamó **ARPANET (ARPA Network)**. El mecanismo de conmutación facilitaba el uso eficiente de rutas alternativas, aumentando de esa forma la fiabilidad en caso de pérdidas de conexiones. Las primeras comunicaciones con esta red se llevaron a cabo de forma experimental en 1969 uniendo entre sí cuatro nodos a través de líneas telefónicas alquiladas. Cada nodo estaba unido con otros dos para ofrecer una mayor fiabilidad. El primer protocolo desarrollado para esta red fue **NCP (Network Control Protocol)**.

La mayor parte de las investigaciones de ARPA eran encargadas a universidades o empresas externas. Por ello, las primeras investigaciones sobre redes de conmutación de paquetes se llevaron a cabo en universidades americanas (por ejemplo, la Universidad de Utah) por encargo de ARPA. Así mismo, se concedió un contrato de investigación a la Universidad de Berkeley para integrar los protocolos de ARPANET en el sistema operativo Unix.

En el año 1981 se publicaron los estándares de los protocolos TCP/IP, para que, dos años más tarde, en 1983, TCP/IP se convirtiera de manera oficial en el

grupo de protocolos oficiales de ARPANET. Ese mismo año se decidió separar de ARPANET una red dedicada exclusivamente a usos militares llamada MILNET, que actualmente sigue en operación.

Aunque se puede considerar a ARPANET la predecesora de Internet, fue otra red, llamada **NSFNET,** la que se considera la primera red que hace la función de columna vertebral o troncal (backbone) de Internet. NSFNET fue creada por la **NSF (National Science Foundation, Fundación Nacional de ciencia)** en Estados Unidos con la idea de interconectar todas las universidades americanas y así poder compartir datos y resultados de investigaciones. Por tanto, NSFNET tenía un marcado carácter académico e investigador. Esta red comenzó a operar en 1986 utilizando la misma tecnología y protocolos de ARPANET, y tuvo un éxito inmediato, de hecho, en 1990 ARPANET deja de estar operativa de forma definitiva. A partir de entonces, el aumento del número de nodos conectados a NSFNET fue vertiginoso y estuvo operativa hasta 1995, año en el que dejó de dar servicio ya que se crearon numerosas compañías a nivel regional que proporcionaban conexión a Internet. En ese momento estaban conectadas al troncal de Internet más de 100.000 redes.

En Europa la situación era bastante distinta. En 1984 la ISO publicó el modelo de interconexión de sistemas abiertos, es decir, el modelo OSI, y por tanto, era de esperar que la interconexión de redes se llevase a cabo utilizando protocolos basados en dicho modelo.

Hasta finales de los años 80, los avances sobre la arquitectura TCP/IP llevados a cabo en Estados Unidos apenas tuvieron repercusión en Europa, que veía TCP/IP como un experimento americano antes de la llegada de los protocolos OSI definitivos. Sin embargo, hubo dos razones que provocaron que Europa empezara a interesarse por la arquitectura TCP/IP. La primera razón fue la ralentización del desarrollo de los protocolos del modelo OSI y la segunda razón fue la progresiva implantación en entornos académicos de sistemas basados en Unix, el cual incluía los protocolos TCP/IP de forma nativa.

En España fue en 1990 a través de RedIRIS cuando se estableció el primer enlace al backbone de Internet utilizando los protocolos TCP/IP. Para entonces, la arquitectura TCP/IP se empezaba a consolidar como el estándar de facto para la interconexión de sistemas abiertos, en detrimento de la arquitectura propuesta en el modelo OSI en el que la mayoría de los protocolos propuestos no llegó a despegar más allá de versiones experimentales.

NOTA 8.2

Todas las especificaciones técnicas sobre los protocolos y procedimientos usados en Internet se publican en unos documentos llamados RFC (Request For Comment), que se pueden obtener en www.ietf.org.
Muchos de estos documentos están traducidos al español en www.rfc-es.org.

En la actualidad, el organismo que gestiona Internet es la **Internet Society (ISOC)**.

8.4 PROTOCOLO IP

El principal protocolo que utiliza la arquitectura TCP/IP en el nivel de red es el protocolo **IP (Internet Protocol)**. IP es un protocolo del nivel de red no orientado a conexión, basado en datagramas y no fiable.

- ✓ Se dice que un protocolo está basado en datagramas cuando la información que debe transmitir se divide en fragmentos. Por tanto, cada uno de los paquetes o fragmentos de información que transporta IP se le denomina datagrama.
- ✓ IP es un protocolo no orientado a conexión, es decir, no se establece un camino previamente, con lo cual cada datagrama viaja de forma independiente pudiendo llegar al destino fuera de secuencia o duplicado. No se crean circuitos virtuales.
- ✓ Y además es un protocolo no fiable, es decir, no ofrece comprobaciones ni seguimientos. IP intenta que la transmisión llegue a su destino lo mejor que puede pero sin ofrecer garantías.

NOTA 8.3

La unidad básica de información en el nivel 2 o nivel de enlace se denomina **trama**. La unidad básica de información en el nivel 3 o nivel de red es el **datagrama**.

Se puede comparar IP con el servicio de correo postal donde, al igual que en IP, no se realiza ningún seguimiento de que una carta se reciba correctamente. Deben ser el remitente o el destinatario los que estén pendientes de que el envío llegue correctamente.

Si se necesita llevar a cabo una comunicación fiable utilizando IP, es necesario añadir otro protocolo que le dé fiabilidad a la transmisión; este protocolo es TCP en la arquitectura TCP/IP. Del mismo modo, para dar más fiabilidad a la entrega del correo postal, se puede utilizar el envío postal con acuse de recibo. En esta modalidad, cuando la carta llega a su destino, se envía un acuse de recibo al remitente. Si no se recibe acuse de recibo, el remitente puede suponer que la carta no llegó correctamente y volver a enviarla.

Aunque pueda parecer que IP es un protocolo con carencias, realmente no es así. Este funcionamiento permite gran flexibilidad para implementar los servicios en los niveles superiores.

La versión actualmente implantada en la mayor parte de los sistemas es la versión 4, conocida como IPv4. Sin embargo, algunas limitaciones de la versión 4 llevaron al desarrollo de la versión 6 (hay una versión 5 experimental no utilizada de forma comercial). La versión 6 de IP, conocida como IPv6 (también conocida como IPng de IP Next Generation), fue adoptada por el organismo encargado de la publicación de los estándares en Internet llamado **IETF (Internet Engineering Task Force)** en 1994, sin embargo su uso aún es muy limitado.

8.4.1 DATAGRAMA IP

La transmisión de los datos en el nivel de red utilizando el protocolo IP se realiza en unidades de información llamadas datagramas. Como es de suponer, un datagrama consta de dos partes, una cabecera y los datos. La longitud de un datagrama es variable, pudiendo alcanzar un tamaño máximo de 65.535 bytes. A continuación se muestra la estructura de un datagrama IP. Los números mostrados en la parte inferior de la figura son los tamaños de los campos de la cabecera expresados en bits.

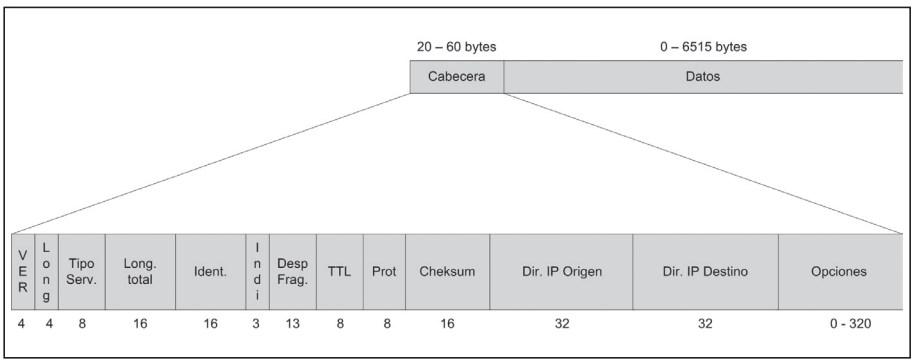


Figura 8.3. *Datagrama IP.*

La descripción de cada uno de los campos es la siguiente:

- **Versión.** Se incluye la versión del protocolo IP. Actualmente la mayor parte de las redes utiliza la versión 4, por tanto este campo contiene el valor 4 en binario: 0100.
- **Longitud de la cabecera.** La cabecera de un datagrama IP no tiene un tamaño fijo. Su longitud puede estar entre 20 y 60 bytes. En este campo se define la longitud de la cabecera en un valor múltiplo de 4, es decir, el valor almacenado en este campo se multiplica por 4 para obtener el número total de bytes de la cabecera.
- **Tipo de servicio.** En la especificación original de IP este campo se utilizaba para incluir información sobre el nivel de retardo, fiabilidad y prestaciones, en función del tipo de servicio que se estuviera utilizando. En la práctica

este campo apenas ha sido utilizado, de forma que el IETF redefinió su uso como **ECN (Explicit Congestion Notification)**, utilizado para enviar información sobre congestión de la red (RFC 3168).

- **Longitud total.** Almacena la longitud total del datagrama IP incluyendo la cabecera y los datos. Es un campo de 16 bits por lo que puede almacenar hasta una longitud de 65.535 bytes.
- **Identificación.** Este campo se utiliza cuando un datagrama original se fragmenta al pasar a una red diferente que trabaja con tamaños menores. A cada fragmento del datagrama original se le asigna un número de secuencia que es almacenado en este campo.
- **Indicadores.** Campo formado por tres bits, el primero es de uso reservado y debe ser 0. El segundo se utiliza para indicar si el datagrama está fragmentado, este bit estará activo para todos los datagramas resultantes de la fragmentación. El último bit indica si el datagrama es el último fragmento.
- **Desplazamiento del fragmento.** Este campo se utiliza para indicar el desplazamiento de los datos incluidos en el datagrama fragmentado respecto al datagrama original.
- **TTL (Time To Live, Tiempo de vida).** Este campo es un número que indica el número de saltos que el datagrama puede realizar antes de ser descartado. Cuando se crea el datagrama se asigna a este campo un valor inicial (normalmente 127). Un salto se produce cuando el datagrama cambia de red, esto lo lleva a cabo un router. El router es el que decrementa el valor de este campo en una unidad. Si el valor del campo llega a cero, el datagrama se descarta. Este funcionamiento se utiliza para evitar que los datagramas permanezcan de forma indefinida en la red.
- **Protocolo.** Este campo es un identificador del protocolo de nivel superior utilizado. Los valores más comunes son: TCP (6), UDP (17) o ICMP (1).
- **Cheksum o suma de comprobación.** Este campo se utiliza para la detección de errores en la cabecera. Para su cálculo no se tiene en cuenta los datos. Los errores de los datos deben ser detectados por los niveles superiores.

NOTA 8.4

El código checksum se calcula de forma más sencilla que el CRC. Simplemente se efectúa la suma aritmética de los datos ajustando el resultado para representarlo con 16 bits.

- **Dirección lógica de origen.** Este campo identifica el dispositivo de red del que parte el datagrama. El formato de la dirección lógica utilizado en IP se especifica en el siguiente apartado.

- **Dirección lógica de destino.** Este campo identifica el dispositivo de red al que va dirigido el datagrama.
- **Opciones.** Este campo se puede utilizar para enviar información adicional en la cabecera del datagrama aunque se utiliza con poca frecuencia.

8.4.2 DIRECCIONAMIENTO IP

En el nivel de red es necesario definir lo que se conoce como dirección lógica como se vio en el capítulo 3. En el protocolo IP, cada dispositivo debe tener asignada una dirección lógica conocida como dirección de red o dirección IP. La principal diferencia del direccionamiento lógico respecto al direccionamiento físico es que el primero es un direccionamiento jerárquico, donde una parte de la numeración se utiliza para identificar la red y otra parte para identificar el equipo dentro de la red.

La dirección IP está formada de 32 bits (4 bytes) y consta de tres campos de longitud variable dependiendo de la clase a la que pertenezca la dirección. Estos campos son la clase, el identificador de red y el identificador de estación.

Las **clases** se definieron en el protocolo IP para cubrir las necesidades de los diferentes tipos de organizaciones ya que cada tipo de clase permite un máximo de direcciones IP en cada red que pertenezca a dicha clase. Las clases que están definidas son:

- **Clase A.** En esta clase, el bit más significativo de la dirección IP vale 0. Se utilizan 7 bits para identificar la red y el resto de bits, es decir, 24, se utilizan para identificar un dispositivo dentro de la red.
- **Clase B.** En este caso, el valor de los dos primeros bits de la dirección es 10. Se utilizan 14 bits para identificar la red y 16 bits para identificar un dispositivo dentro de la red.
- **Clase C.** En este caso, el valor que se utiliza en los tres primeros bits para asignar la clase C es el 110. Se utilizan 21 bits para identificar la red y 8 bits para identificar un dispositivo dentro de la red.
- **Clase D.** Esta clase se identifica por contener en los cuatro primeros bits el valor 1110 y se utiliza para establecer direcciones de multienvío.
- **Clase E.** Identificada por sus primeros 4 bits tiene el valor 1111. Estas direcciones están reservadas inicialmente para usos futuros aunque en la práctica nunca se ha llegado a definir ningún uso para estas direcciones.

El resumen del direccionamiento se puede ver en la siguiente figura:

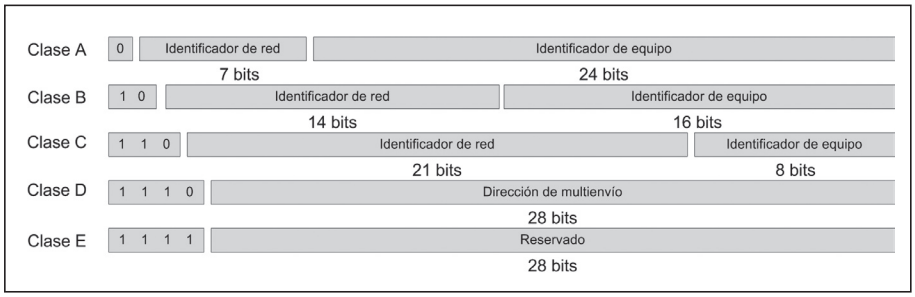


Figura 8.4. *Direccionamiento IP por clases.*

De las definiciones anteriores se pueden deducir fácilmente las capacidades teóricas de las clases A, B y C:

- ✓ Puede haber un máximo de 128 redes de clase A. Cada red de clase A puede contener un máximo de 16.777.216 dispositivos.
- ✓ Puede haber un máximo de 16.384 redes de clase B. Cada red de clase B puede contener un máximo de 65.536 dispositivos.
- ✓ Puede haber un máximo de 2.097.152 redes de clase C. Cada red de clase C puede contener un máximo de 256 dispositivos.

Lógicamente, los diseñadores del protocolo IP nunca esperaron el espectacular desarrollo de su tecnología y, aunque en el momento de su desarrollo este esquema de direccionamiento parecía más que suficiente para proporcionar direcciones lógicas a todos los dispositivos, en la actualidad, las capacidades de direccionamiento de IP están completamente sobrepasadas.

Debido a la incomodidad que supone trabajar con direcciones IP en formato binario utilizando 32 bits, se ha definido una notación más práctica para representar las direcciones IP, conocida como **notación punto-decimal**. La representación en dicha notación simplemente consiste en agrupar los bits en grupos de ocho y representar cada grupo en notación decimal en lugar de binaria. Por último, se utiliza el punto (.) para separar cada grupo.

Por ejemplo, la dirección IP:

00111011 10100011 11000010 00001101

Se agrupa en grupos de 8 bits y se convierte en decimal:

00111011. 10100011. 11000010. 00001101
59. 163. 194. 13

Los rangos de direcciones IP de las diferentes clases, utilizando la notación punto-decimal, es la siguiente:

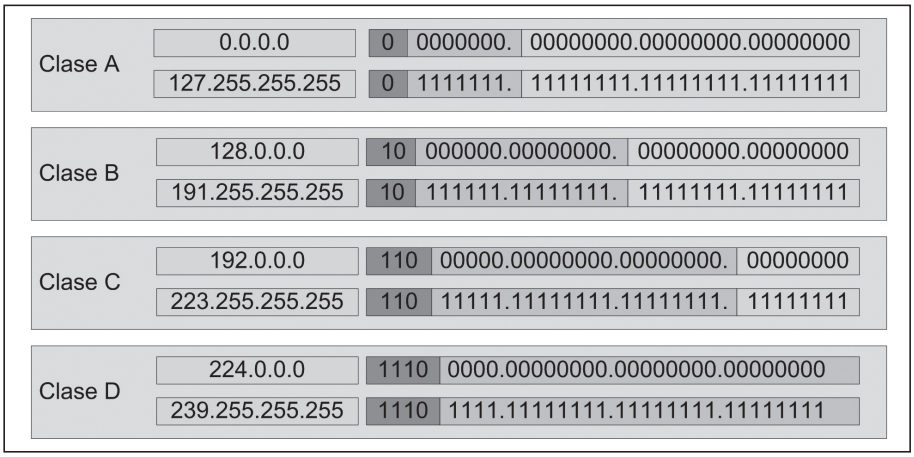


Figura 8.5. *Rangos de direcciones IP.*

Direcciones reservadas. Existen algunas direcciones IP reservadas para usos concretos. Éstas son:

Tabla 8.1

0.0.0.0	Dirección utilizada para referirse al propio host. Utilizada exclusivamente en las tablas de encaminamiento internas de los hosts.
127.0.0.1	Dirección de loopback o de bucle local. Utilizada por el software de red para propósitos de test de los hosts.
X.255.255.255 X.X.255.255 X.X.X.255	Direcciones de difusión de las redes de clase A, B y C respectivamente.

Las direcciones de difusión, también llamadas de broadcast, se utilizan para llevar a cabo envíos simultáneos a todos los dispositivos de una red. Las direcciones de difusión sólo se pueden utilizar como direcciones destino en un datagrama IP.

También se han reservado direcciones de red para su uso en redes privadas:

Tabla 8.2

Rangos de direcciones IP	Descripción
10.0.0.0	Dirección red privada de clase A
172.16.0.0 – 172.31.0.0	Rango para definir 16 direcciones privadas de clase B
192.168.0.0 – 192.168.255.0	Rango para definir 256 direcciones privadas de clase C

Estos rangos de direcciones privadas no pueden encaminarse fuera de las redes privadas y no se puede acceder directamente a redes públicas desde hosts dentro de las redes privadas, por ello reciben el nombre de **direcciones no enrrutables**.

Además, se reserva la primera dirección de cada red, es decir, la dirección en la que todos los bits reservados para identificar el host están a cero, para identificar la propia red. Por lo tanto, con estas consideraciones, las capacidades reales del direccionamiento por clases son:

NOTA 8.5

Cuando en una dirección IP todos los bits reservados para identificar los equipos de una red están a cero, esa dirección no se refiere a ningún equipo sino que es la dirección de la red.

- **Clase A.** De las 128 posibles redes no se pueden utilizar 0.0.0.0 ni 127.0.0.0 ni 10.0.0.0 por lo que quedan 125 para redes reales. Cada red de clase A tiene reservadas dos direcciones, una para identificar la red y otra dirección de broadcast por lo que quedan 16.777.214 direcciones de hosts.
- **Clase B.** De las 16.834 redes, están reservadas 16 para redes privadas por lo que quedan disponibles 16.818 redes de clase B. Cada red puede tener un máximo de 65.534 direcciones de hosts.
- **Clase C.** Descontando las direcciones Clase C para redes privadas quedan disponibles 2.096.896 redes de clase C. Cada red puede tener un máximo de 254 hosts, descontando las direcciones de identificación de red y de broadcast.

8.4.3 SUBREDES

Las direcciones IP incluyen dos niveles jerárquicos. Cada dirección de red incluye la identificación de la red y la identificación de un equipo o hosts dentro de la red.

El protocolo IP permite la utilización de un tercer nivel de jerarquía entre los dos niveles jerárquicos definidos por defecto, es el nivel de subred. Esta característica se utiliza cuando una organización, que tiene asignado un rango de direcciones públicas que se corresponderá a una clase determinada, necesita organizar de forma interna el uso de las direcciones IP.

Para ello, se aplica una técnica llamado **enmascaramiento**, que es el proceso por el cual se puede obtener la dirección de red o de subred de una dirección IP dada. El enmascaramiento se puede aplicar tanto en redes que utilicen subredes como en redes que no las utilicen. De hecho actualmente, y para ofrecer un método homogéneo del tratamiento de las direcciones de red, se aplica el enmascaramiento aún en redes que no utilizan subredes.

Para aplicar esta técnica se define un parámetro llamado **máscara de subred** o simplemente máscara. La máscara es un número de 32 bits que define qué bits de una dirección IP se utilizan para identificar la red o subred y qué bits se utilizan para identificar el equipo. Lógicamente el valor de la máscara estará condicionado por la clase a la que pertenezca la dirección de red. Los bits que identifican la red o subred toman el valor 1 en la máscara. Los bits que identifican el equipo toman el valor 0 en la máscara.

Las máscaras utilizadas para redes que no utilizan subredes están acordes con las características de las clases utilizadas.

Clase	Máscara	Máscara en binario
Clase A	255.0.0.0	11111111.00000000.00000000.00000000
Clase B	255.255.0.0	11111111.11111111.00000000.00000000
Clase C	255.255.255.0	11111111.11111111.11111111.00000000

Cuando se utilizan subredes la máscara especifica cuántos bits de la dirección IP se utilizan para la red y la subred.

Por ejemplo, una empresa tiene reservada para su uso la dirección de clase B 180.30.0.0. Esto le permite utilizar hasta 65.534 direcciones de hosts diferentes. Al ser un número elevado de direcciones y por razones de organización, puede crear subredes. El número máximo de subredes que se pueden crear depende de la máscara elegida y debe ser potencia de dos, es decir, 2, 4, 8, 16, 32…

Si se decide utilizar una máscara que permita crear hasta ocho subredes, se deben añadir tres 'unos' a la máscara original sin subredes para clase B. Para la clase B, la máscara es 255.255.0.0. Para llevar a cabo este proceso es más sencillo utilizar la notación binaria:

11111111.11111111.00000000.00000000

Para el uso de ocho subredes se añaden tres 'unos' a la máscara y se pasa de nuevo a notación punto-decimal:

11111111.11111111.11100000.00000000

255.255.224.0

Las direcciones de las subredes definidas en el ejemplo serían:

180.30.0.0 10110100.00011110. 000 00000.00000000
180.30.32.0 10110100.00011110. 001 00000.00000000
180.30.64.0 10110100.00011110. 010 00000.00000000
180.30.96.0 10110100.00011110. 011 00000.00000000
180.30.128.010110100.00011110. 100 00000.00000000
180.30.160.010110100.00011110. 101 00000.00000000
180.30.192.010110100.00011110. 110 00000.00000000
180.30.224.010110100.00011110. 111 00000.00000000

Para obtener la dirección de subred a partir de una dirección de red y una máscara se sigue el siguiente procedimiento:

- ✓ Los bytes de la dirección IP que se correspondan con el número 255 en la máscara se repiten en la dirección de la subred.
- ✓ Los bytes de la dirección IP que se correspondan con 0 en la máscara se cambian por un 0 en la dirección de la subred.
- ✓ Para números diferentes a 0 y 255 se aplica el operador AND entre el byte de la dirección IP y el byte de la máscara.

En los siguientes ejemplos se obtienen las direcciones de subred y de red de una dirección IP y su máscara:

Ejemplo 1:

79.199.217.111
255.255.0.0
Dirección de subred: 79.199.0.0
Dirección de red: 79.0.0.0
Se pueden definir hasta 256 subredes de 65534 hosts cada una.

Ejemplo 2:
133.210.51.8
255.255.255.0
Dirección de subred: 133.210.51.0
Dirección de red: 133.210.0.0
Se pueden definir hasta 256 subredes de 254 hosts cada una

Ejemplo 3:

200.45.67.77	77	01001101	
255.255.255.192	192	11000000	
	AND	01000000	64

Dirección de subred: 200.45.67.64
Dirección de red: 200.45.67.0

Se pueden definir hasta cuatro subredes de 62 hosts cada una.

NOTA 8.6

Algunas correspondencias útiles entre valores binarios y decimales:

10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254

8.4.4 DIRECCIONAMIENTO CIDR

El gran desarrollo que tuvo Internet, y por extensión la arquitectura TCP/IP, durante los años 90 hizo que, en pocos años, el ritmo de crecimiento de los hosts conectados a Internet y que necesitaban una dirección IP creciese muy rápido. La consecuencia inmediata es que el direccionamiento propuesto en el estándar original se quedase corto, es decir, el rango de direcciones IP se comenzaba a agotar.

Este problema se agudizaba por la poca eficacia que proporcionaba el mecanismo de clases utilizado hasta entonces, en el que se desperdiciaban muchos rangos de direcciones IP asignados a empresas o entidades que los infrautilizaban.

Por todo ello, en el año 1993 se desarrolló una nueva técnica para aprovechar mejor el escaso direccionamiento que proporcionaba el estándar IPv4. Esta técnica se conoce como **CIDR (Classless Inter-Domain Routing, Encaminamiento Inter-Dominios sin clase)**. La clave del uso de esta técnica es la eliminación del concepto de clases.

Para la asignación de un rango de direcciones públicas a una entidad ya no se utiliza el concepto de clase, es decir, no se le proporciona una dirección de red de una clase determinada. En CIDR se asigna una dirección de red cuya dirección base puede tener cualquier longitud.

Recordemos que en la asignación tradicional por clases las direcciones base de cada clase eran de longitud fija. Para la clase A, la identificación de la red siempre son los primeros 8 bits. Para la clase B, son 16 bits y para la clase C son de 24 bits. En CIDR la identificación de red puede tener cualquier número de bits, es decir, se pueden asignar rangos de direcciones con 8, 9 10, 11… bits que identifican la red y el resto, que serán gestionados por la entidad, que identifican los hosts dentro de la red.

Para referirse a un rango de direcciones CIDR se utiliza la notación: A.B.C.D/N donde A.B.C.D sigue siendo la dirección IP de la red y cada dígito, un número entre 0 y 255. El valor N sustituye a la máscara y es el número de bits de la dirección IP que identifican la red. Por tanto el resto identificará el host dentro de esa red.

A esta técnica de direccionamiento, cuando se aplica a redes privadas, se la conoce como **VLSM (Variable-Length Subnet Masking, Máscara de subred de longitud variable)**.

Todavía hoy se sigue hablando de direcciones de clase A, B o C, sin embargo a efectos de asignación de direcciones por el organismo competente (llamado IANA) hace ya algunos años que se dejaron de asignar direcciones de red utilizando clases. Ahora, cuando una entidad solicita un rango de direcciones se le proporciona lo que se conoce como un bloque CIDR, es decir, una dirección base y el prefijo que identifica todos los bits que son comunes a esa dirección base.

Por ejemplo, para la asignación:
195.77.128.0/24

Tendría fijos los 24 primeros bits de la dirección y la entidad podría asignar direcciones variando los últimos 8 bits, es decir, 254 direcciones. Sería equivalente a una clase C.
62.101.152.0/21

En este caso, la dirección de base son los primeros 21 bits y la entidad puede asignar 11 bits, es decir 2.046 posibles direcciones. Como se puede ver, esta asignación no se corresponde a ninguna clase.

8.4.5 ARQUITECTURA DE UNA RED IP

El direccionamiento lógico proporcionado por IP es el principal mecanismo para establecer los límites de una red. El rango de direcciones IP que una empresa u organización de cualquier tipo tiene asignado constituye la manera de identificar los equipos que pertenecen a la red interna.

Un elemento fundamental en la arquitectura TCP/IP son los encaminadores o routers.

Estos dispositivos son capaces de transferir los datagramas IP de unas redes a otras dirigiéndolos a su destino final. Los routers están conectados, al menos, a dos redes lógicas diferentes, por tanto, se puede decir que los routers pertenecen a más

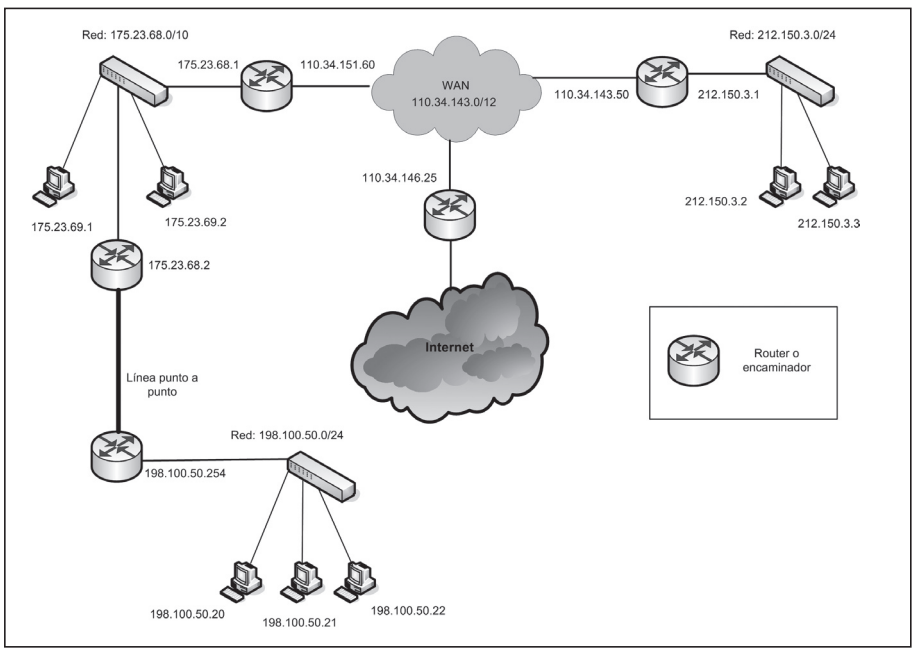


Figura 8.6. *Ejemplo de la arquitectura de red IP.*

de una red a la vez, y deben tener asignadas direcciones IP válidas en cada una de las redes a la que pertenezca.

El direccionamiento jerárquico que proporciona IP permite llevar a cabo un encaminamiento efectivo de los datagramas IP en los routers. Más adelante en este capítulo se verán algunas características adicionales de los routers. En la siguiente figura se puede observar claramente la función de los mismos al unir redes con un rango de direcciones IP diferente permitiendo intercambiar tráfico entre ellas. Se ha utilizado para especificar los rangos de cada red direccionamiento CIDR.

Desde el punto de vista de direccionamiento, el protocolo IP es capaz de llevar a cabo la entrega de datagramas a un destino que se encuentre en la misma red. Para comprobar que el host de destino está en la misma red que el host origen se utiliza la máscara, de forma que todos los bits de la máscara que estén a 1 deben coincidir en la dirección IP origen y destino para considerar que el destino está en la misma red. Sin embargo, si el host de destino no se encuentra en la misma red es necesario un dispositivo de interconexión como el router, que sea capaz de encaminar los datagramas a través de una determinada ruta que conducirá a la red donde se encuentra el host de destino.

8.5 OTROS PROTOCOLOS DEL NIVEL DE RED

8.5.1 PROTOCOLO ARP

ARP (Adress Resolution Protocol, Protocolo de resolución de direcciones) es un protocolo utilizado para obtener la dirección física (dirección MAC) de un equipo a través de su dirección IP.

Cuando un equipo quiere enviar datos a otro dentro de una red (por ejemplo, una red Ethernet) utilizando la arquitectura TCP/IP, el equipo emisor debe generar uno (o más) datagramas, y éstos deben ser pasados al nivel inferior (nivel de enlace) y encapsulados en una (o más) tramas Ethernet. En esta situación, la referencia al equipo destino suele ser su dirección IP, pero para poder generar las tramas Ethernet también es necesario conocer la dirección MAC.

Este problema se resuelve mediante dos soluciones. La primera es almacenar en cada equipo una tabla que contenga las direcciones IP de cada equipo y sus correspondientes direcciones MAC. De esa forma, cuando se quiera enviar un datagrama a un equipo cuya dirección IP es conocida, se puede consultar en dicha tabla cuál es la dirección MAC y generar de esta manera la trama Ethernet.

Esta primera solución sería poco práctica si hubiera que mantener de forma manual el contenido de esta tabla. Para ello se utiliza la segunda solución: el protocolo ARP se encarga de obtener la dirección MAC del equipo de destino a partir de su dirección IP y de almacenarlo en la tabla. Es decir, ARP hace el trabajo de mantenimiento de la tabla de direcciones MAC; esta tabla se conoce como **tabla ARP**.

Si la dirección MAC del equipo destino no se encuentra en la tabla ARP, se envía una trama conocida como **Petición ARP (ARP Request)**. Esta petición contiene la dirección IP del destinatario del que queremos averiguar su dirección MAC. La petición ARP debe llegar a todos los equipos de la red y aquél que tenga la dirección IP del equipo del que se pretende obtener su dirección MAC deberá responder a esta petición con otra trama conocida como **Respuesta ARP (ARP Reply)** que contendrá, precisamente, su dirección MAC. Para conseguir que la Petición ARP llegue a todos los equipos de la red, se utiliza como dirección MAC de destino la dirección de broadcast (FF:FF:FF:FF:FF:FF).

En la siguiente figura se representa el formato de una trama ARP.

HTYPE	PTYPE	HLEN	PLEN	Cod. Operac	Dirección Física Origen	Dirección IP Origen	Dirección Física Destino	Dirección IP Destino
16	16	8	8	16				

Figura 8.7. *Trama ARP.*

Los campos que forman parte de la trama son:

- **HTYPE.** Este campo indica el protocolo utilizado en el nivel de enlace. Normalmente este protocolo es Ethernet, que tiene asignado el código 1.
- **PTYPE.** Este campo indica el protocolo utilizado en el nivel de red. Normalmente este protocolo será IP, que tiene asignado el código 0800 expresado en valor hexadecimal.
- **HLEN.** Este campo indica el tamaño en bytes de la dirección utilizada en el protocolo de enlace, es decir, de la dirección física. Para Ethernet, la dirección es de 6 bytes.
- **PLEN.** Este campo indica el tamaño en bytes de la dirección lógica o dirección establecida en el nivel de red. Para IP es de 4 bytes.
- **Cód. Operar.** Este campo es el código de operación de la trama. Puede tener dos valores. El código 1 indica que es una trama ARP Request y el código 2 indica que es una trama ARP Reply.
- **SHA (Sender Hardware Adress).** Contiene la dirección MAC del dispositivo que ha enviado la trama ARP.
- **SPA (Sender Protocol Adress).** Contiene la dirección lógica (IP) del dispositivo que ha enviado la trama.
- **THA (Target Hardware Adress).** Contiene la dirección MAC del destinatario de la trama ARP. En una petición ARP este campo está a cero.
- **TPA (Target Protocol Adress).** Contiene la dirección lógica (IP) del destinatario de la trama ARP.

Por tanto, el formato de trama es el mismo para la petición ARP y para la respuesta ARP, el tipo de trama se indica en el campo Cód.Operar. En la trama de petición ARP, el campo THA está a cero ya que es precisamente la información que se solicita.

Los datagramas ARP van encapsulados en tramas Ethernet como se muestra en la siguiente figura:

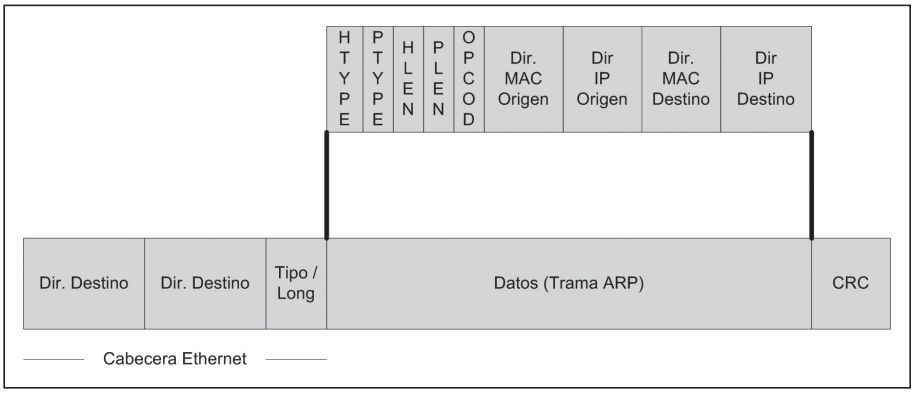


Figura 8.8. *Trama ARP encapsulada en una trama Ethernet.*

8.5.2 PROTOCOLO RARP

El protocolo **RARP (Reverse Address Resolution Protocol, Protocolo de resolución inversa de direcciones)** se utiliza para que un dispositivo obtenga su dirección IP a partir de su dirección MAC.

Este protocolo se utiliza cuando un dispositivo conectado a la red no tiene almacenada su configuración de red de forma que tiene que solicitarla. Debe haber un equipo que almacene las direcciones IP correspondientes y responda a los mensajes del protocolo RARP. Su funcionamiento es similar a ARP.

Actualmente este protocolo apenas se utiliza ya que existe un servicio de red que proporciona toda la configuración de red (no sólo la dirección IP) de forma dinámica. Este servicio es DHCP y se estudiará en el apartado dedicado a protocolos del nivel de aplicación.

8.5.3 PROTOCOLO ICMP

El protocolo **ICMP (Internet Control Message Protocol, Protocolo de mensajes de control de Internet)** se utiliza para enviar notificaciones sobre datagramas con problemas. Los mensajes ICMP son generados normalmente en respuesta a errores producidos sobre datagramas IP o para propósitos de diagnóstico y enrutamiento.

ICMP es un protocolo utilizado en el nivel de red de la arquitectura TCP/IP para el envío de mensajes de estado sobre datagramas IP. Uno de los usos más frecuentes de ICMP es el envío de mensajes para notificar al emisor de un datagrama IP sobre algún tipo de problema en la entrega de dicho datagrama al destino.

A pesar de considerarse un protocolo del nivel de red, los mensajes ICMP van encapsulados dentro de un datagrama IP:

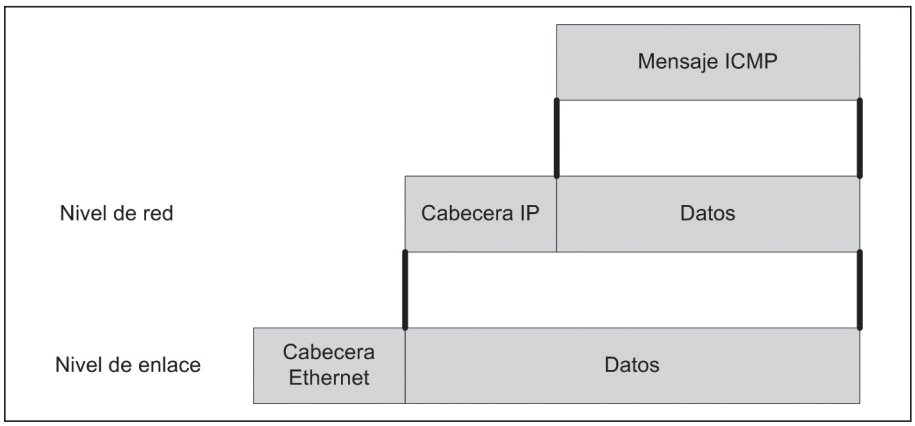


Figura 8.9. *Encapsulación de un mensaje ICMP.*

El formato de un mensaje ICMP es el siguiente:

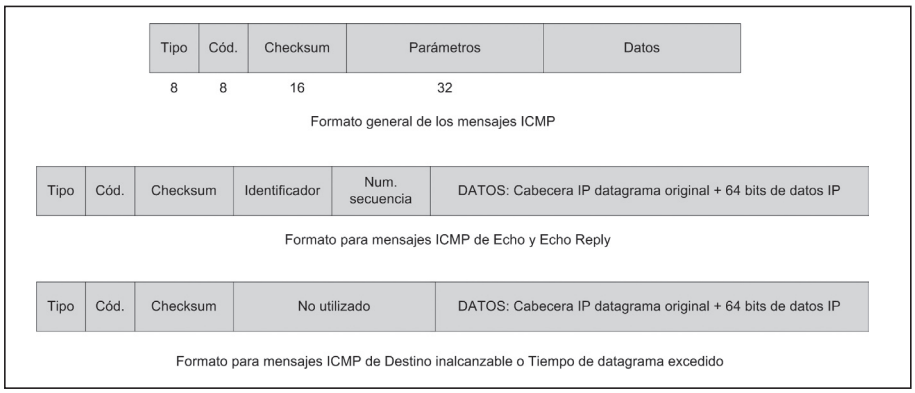


Figura 8.10. *Formato de un mensaje ICMP.*

Los capos de los que consta un mensaje ICMP son:

- **Tipo:** identifica el tipo de mensaje ICMP.
- **Código:** especifica un código de operación dentro de tipo de mensaje ICMP.
- **Checksum:** código de comprobación de errores.

Pueden aparecer otros campos opcionales que dependen del tipo de mensaje ICMP. Algunos de los mensajes ICMP más comunes se muestran en la siguiente tabla:

Tabla 8.3

Tipo	Código	Descripción original	Descripción
8	0	Echo	Petición de eco
0	0	Echo reply	Respuesta de eco
3	0	Net unreachable	Red inalcanzable
3	1	Host unreachable	Host inalcanzable
11	0	Time Exceeded	Tiempo de datagrama excedido

Uno de los mensajes ICMP más populares son los de **Echo** (Eco). Estos mensajes se utilizan para comprobar que existe conectividad con un host por medio del protocolo IP. Los mensajes ICMP de Eco son utilizados por el comando ping, implementado en todos los sistemas operativos actuales. Este comando envía el mensaje ICMP Eco (Tipo 8) a la dirección IP especificada como parámetro. Si el mensaje ICMP llega al destino, éste responde con el mensaje ICMP de **Respuesta de Eco** (Tipo 0).

Cuando un router no puede enviar un datagrama IP envía un mensaje ICMP de tipo 3 (Destination unreachable) al emisor de dicho datagrama. El código indica el motivo del error. Los más frecuentes son el código 0 (Net unreachable) y el código 1 (Host unreachable).

Como se ve, el protocolo ICMP permite el control de ciertas condiciones de error producidas en el nivel de red, sin embargo, su función es simplemente informar de dichos problemas pero no los corrige. De hecho, el protocolo tampoco se asegura de la llegada de los mensajes ICMP. Por tanto, a pesar del uso de mensajes ICMP, el protocolo IP sigue siendo un protocolo no fiable.

8.6 NIVEL DE TRANSPORTE

El nivel de transporte está implementado en la arquitectura TCP/IP por dos protocolos, TCP y UDP. El protocolo TCP implementa las principales funciones del nivel de transporte del modelo OSI vistas en el capítulo 3, es decir, proporciona la entrega fiable de mensajes completos desde un origen a un destino. UDP es un protocolo más sencillo que proporciona la entrega de mensaje de origen a destino pero no ofrece la fiabilidad de TCP por lo que cuando se usa UDP deben ser los protocolos del nivel de aplicación los que se encarguen del control de errores.

Una de las funciones importantes implementadas en el nivel de transporte es la definición de los **puertos del protocolo**, llamados simplemente puertos, que ofrecen un mecanismo para identificar la comunicación de un proceso individual

dentro de un host. En la arquitectura TCP/IP los puertos son números de 16 bits, es decir, el rango de puertos válidos es de 0 a 65.535.

8.6.1 PROTOCOLO UDP

El protocolo **UDP (User Datagram Protocol, Protocolo de datagramas de usuario)** es un protocolo del nivel de transporte en la arquitectura TCP/IP no orientado a conexión, que proporciona las funciones básicas necesarias para la entrega de datos de un origen a un destino. No se lleva a cabo control de flujo ni de errores, además UDP no proporciona funciones de secuenciamiento ni de reordenación de paquetes. No puede especificar el paquete dañado cuando se produce un error ni detecta paquetes perdidos.

Como se puede ver, las funciones de UDP son muy limitadas. Realmente, la principal función de UDP es proporcionar el direccionamiento de los puntos de acceso a los diferentes protocolos del nivel de aplicación, es decir, los puertos. Por tanto, los protocolos del nivel de aplicación que utilicen UDP deben implementar mecanismos de control de flujo y de errores para llevar a cabo una comunicación fiable.

El formato del paquete UDP es el siguiente:

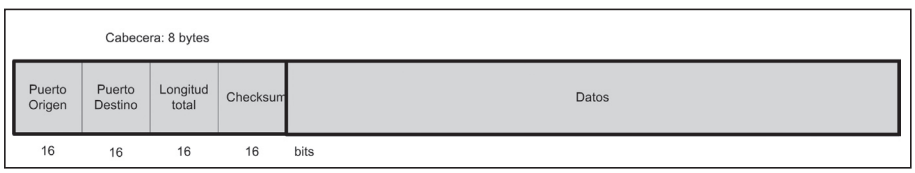


Figura 8.11. *Formato del paquete UDP.*

- **Dirección del puerto origen.** Identificador del puerto del proceso origen.
- **Dirección del puerto destino.** Identificador del puerto del proceso destino.
- **Longitud total.** Es el tamaño en bytes del datagrama UDP incluida la cabecera.
- **Checksum.** Suma de comprobación utilizada para la detección de errores.

8.6.2 PROTOCOLO TCP

El protocolo **TCP (Transmission Control Protocol, Protocolo de control de transmisión)** proporciona todas las funciones de un protocolo de nivel de transporte, es decir, es un protocolo orientado a conexión que permite la comunicación fiable de datos de un origen a un destino. Implementa funciones de control de flujo y control de errores.

Las unidades de datos en el protocolo TCP se conocen como segmentos. La estructura de un segmento TCP es la siguiente:

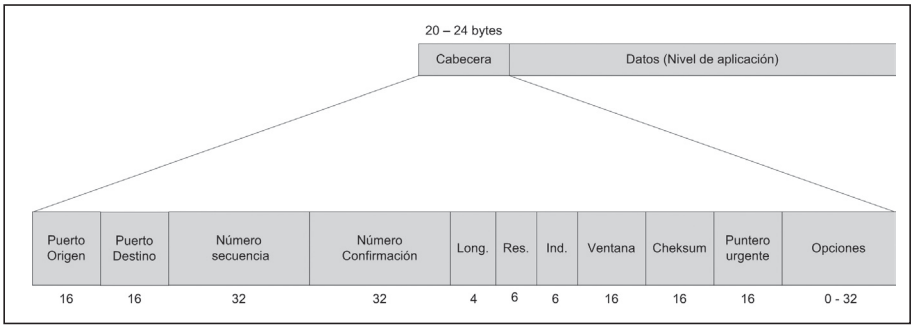


Figura 8.12. *Formato del segmento TCP.*

- **Puerto origen.** Dirección del puerto en el proceso origen.
- **Puerto destino.** Dirección del puerto en el proceso destino.
- **Número de secuencia.** Cada uno de los segmentos en los que se dividen los datos en una comunicación por medio de TCP se numera.
- **Número confirmación.** Si el bit ACK del campo de control está activo este campo identifica el número de secuencia del segmento que se confirma.
- **Longitud.** Este campo contiene el tamaño en bytes de la cabecera del segmento TCP.
- **Reservado.** Campo reservado.
- **Indicadores.** Este campo contiene los siguientes flags o indicadores:
  - **URG,** indica que hay datos urgentes. El campo Puntero urgente indica la cantidad de datos urgentes en el segmento.
  - **ACK,** bit utilizado para validar segmentos recibidos.
  - **PSH,** indica al receptor que entregue al nivel superior todos los datos que tenga disponibles en el buffer de recepción.
  - **RST,** indica que se necesita reiniciar la comunicación.
  - **SYN,** bit utilizado para sincronizar los números de secuencia
  - **FIN,** bit utilizado para indicar el fin de la comunicación.
- **Tamaño de ventana.** Indica el tamaño de ventana deslizante.
- **Checksum.** Suma de comprobación utilizado para la comprobación de errores. Se calcula con los datos de la cabecera y los datos.

- **Puntero urgente.** Este campo contiene un puntero al final de los datos urgentes por lo que a partir de la posición indicada en este campo, comienza los datos con prioridad normal.

Como hemos visto, TCP es un protocolo orientado a conexión y por lo tanto implementa mecanismos para establecer y finalizar conexiones. Además, para llevar a cabo el control de flujo de los datos se emplea la técnica de ventana deslizante pero orientada a bytes. En este caso, la ventana de recepción contiene el número de bytes que pueden ser incluidos en el buffer de recepción.

El procedimiento para establecer una conexión se lleva a cabo en tres pasos. El origen de la conexión (normalmente un cliente de un servicio de red) envía un segmento TCP con un número de secuencia inicial N y el indicador SYN activo. El destinatario de la conexión (normalmente un servidor de un servicio de red) responde con un segmento TCP con otro número de secuencia M, el indicador SYN activo y el ACK activo con un número de confirmación N+1. En el último paso, el origen de la conexión envía otro segmento TCP con el número de secuencia N+1 y con el indicador de ACK activo y el número de confirmación M+1.

En la siguiente figura se puede ver un ejemplo del establecimiento de una conexión TCP:

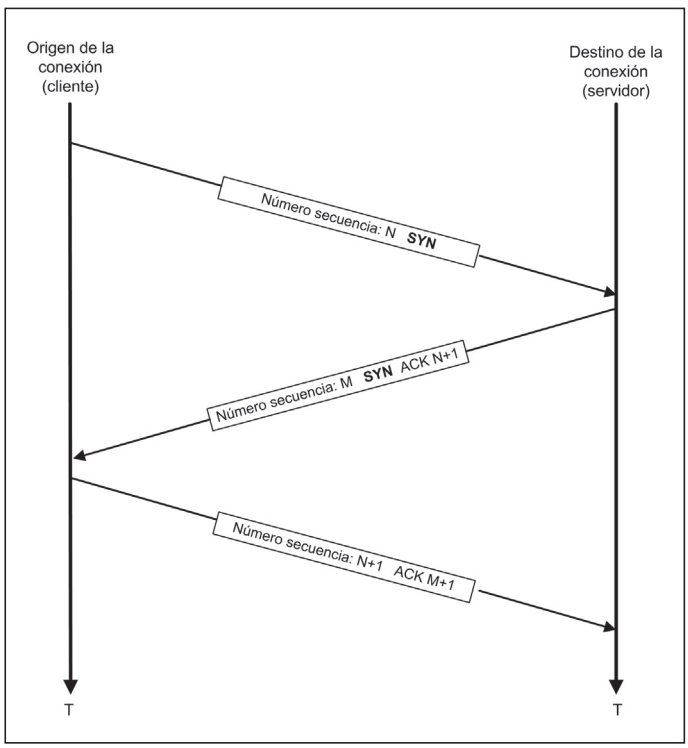


Figura 8.13. *Establecimiento de una conexión TCP.*

Para finalizar una conexión TCP se establece un mecanismo de cuatro pasos. El proceso que desea finalizar la conexión envía un segmento TCP con el indicador FIN activo y un número de secuencia inicial N. El proceso en el otro extremo de la conexión envía entonces un segmento TCP con un número de secuencia inicial M y el indicador ACK activo, con el número de confirmación N+1. A continuación, este último proceso envía otro segmento TCP, esta vez con el indicador FIN activo y número de secuencia M+1. El primer proceso, cuando recibe los segmentos anteriores, genera un segmento TCP con número de secuencia N+1 y el indicador ACK activo con el número de confirmación M+2. En la siguiente figura se puede ver un ejemplo de finalización:

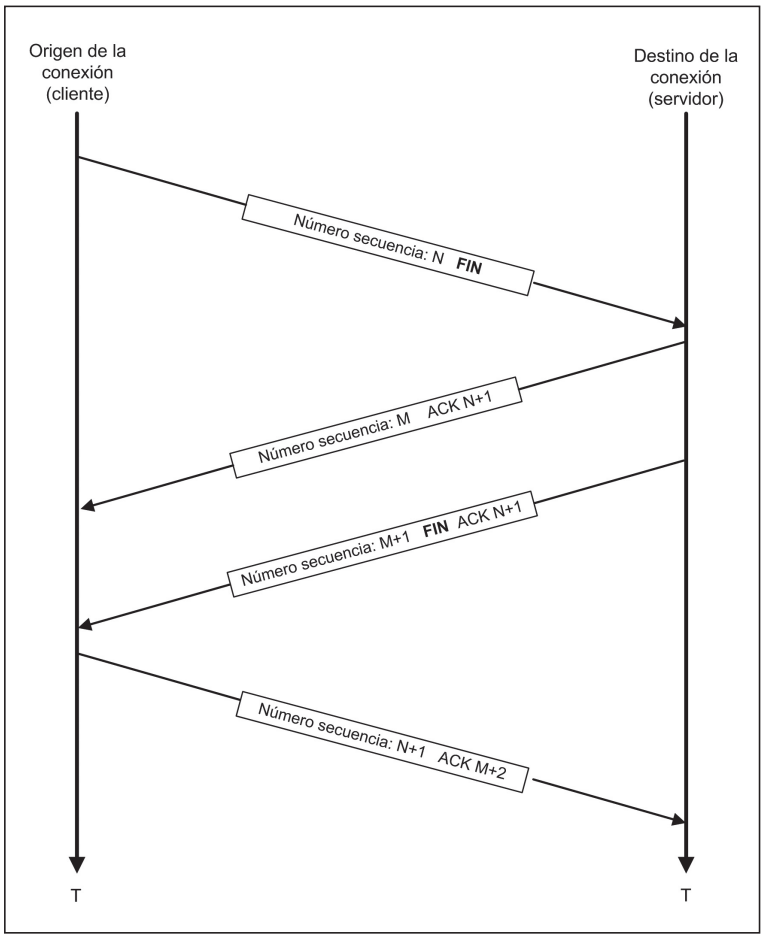


Figura 8.14. *Finalización de una conexión TCP.*

Las conexiones TCP pueden encontrarse en varios estados que definen su comportamiento inmediato. Estos estados se muestran en la siguiente tabla:

Tabla 8.4

Estado	Descripción
CLOSED	No hay conexión
LISTEN	Un proceso servidor espera las peticiones de procesos clientes
SYN-SENT	Se ha enviado una petición de conexión. En espera del reconocimiento
SYN-RCVD	Se ha recibido una petición de conexión
ESTABLISHED	Conexión establecida
FIN-WAIT-1	Se ha solicitado el cierre de la conexión
FIN-WAIT-2	El equipo remoto ha aceptado el cierre de la conexión
TIME-WAIT	Esperando la retransmisión de segmentos
CLOSE-WAIT	Un proceso servidor espera el cierre del proceso cliente
LAST-ACK	El proceso servidor espera el último reconocimiento

8.7 INTERCONEXIÓN DE REDES

8.7.1 ENCAMINADORES O ROUTERS

Los routers o encaminadores son dispositivos más sofisticados que los repetidores y puentes. Actúan en los niveles físico, de enlace y de red por lo que se les conoce como dispositivos de interconexión de nivel 3.

Un router tiene una interfaz de red por cada red a la que se conecta. Si dichas redes utilizan IP en el nivel de red, cada interfaz de red tendrá asignada una dirección IP que deberá pertenecer al rango de direcciones de la red a la que se conecta. De esta forma, un router conectado a una red IP sólo procesará las tramas que vayan dirigidas a su dirección.

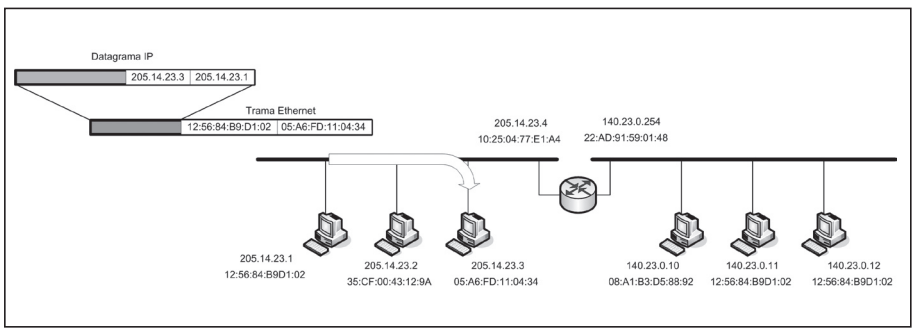


Figura 8.15. *Encaminamiento IP en la misma red.*

Cuando se envía un datagrama dentro de la red el router no lleva a cabo ningún procesamiento.

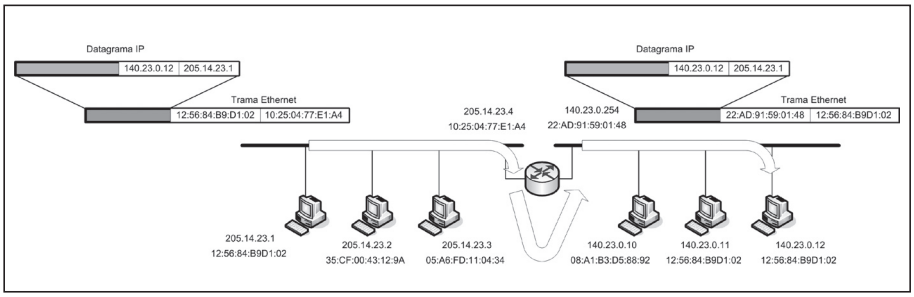


Figura 8.16. *Encaminamiento IP entre redes diferentes.*

Cuando el destino de un datagrama tiene que pasar a otra red, la trama Ethernet va dirigida al router y éste analiza el datagrama IP para llevar a cabo el encaminamiento, ajustando además los valores de las direcciones físicas.

La función primaria de un router es unir redes. Para ello, retransmite paquetes entre las redes a las que está conectado, adaptando si es necesario la información (tramas) entre los distintos protocolos que soporta.

Además de la función de interconectar redes, los routers implementan funciones de encaminamiento de paquetes. De hecho, los routers utilizados en los backbones de las grandes redes están especializados en esta función.

Cuando un router está conectado a dos redes sin otros routers adyacentes, el mecanismo de encaminamiento es bastante simple. Éste es el caso de un router de conexión a Internet como en la figura proporcionado por un ISP a sus clientes. El router conecta la red del ISP con la red local del usuario. Los paquetes de la red local con una dirección de destino que no pertenezca a la red son encaminados a la red del ISP.

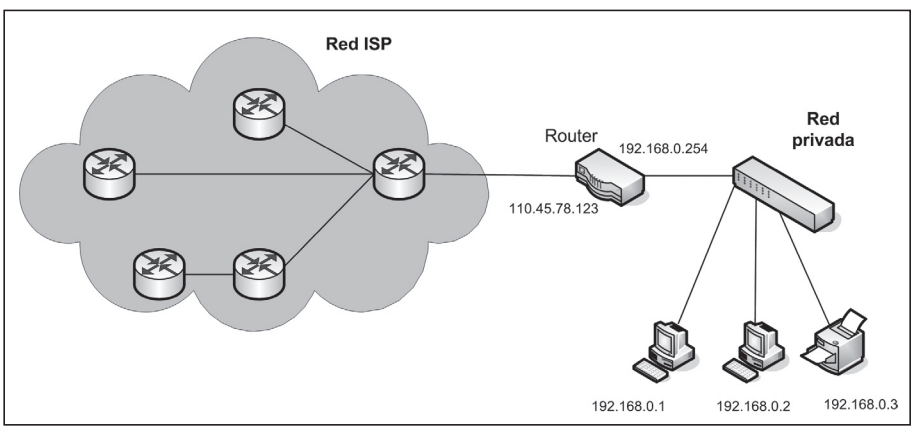


Figura 8.17. *Router para conexión a Internet.*

Sin embargo, el encaminamiento de los paquetes se vuelve una tarea fundamental cuando un router tiene más de dos interfaces de red, es decir, está conectado a más de dos redes y en dichas redes existen otros routers conectados. En este caso, los routers deben almacenar información que le permita decidir la interfaz de red por la que tiene que redirigir un paquete. Esta información se almacena en la llamada **tabla de encaminamiento**. Además, los routers deben implementar algún mecanismo que obtenga y actualice periódicamente la información de dicha tabla. Estos mecanismos son los llamados algoritmos de encaminamiento. En la interconexión de grandes redes, especialmente en Internet, la elección de un algoritmo de encaminamiento eficiente es fundamental para el rendimiento de las propias redes.

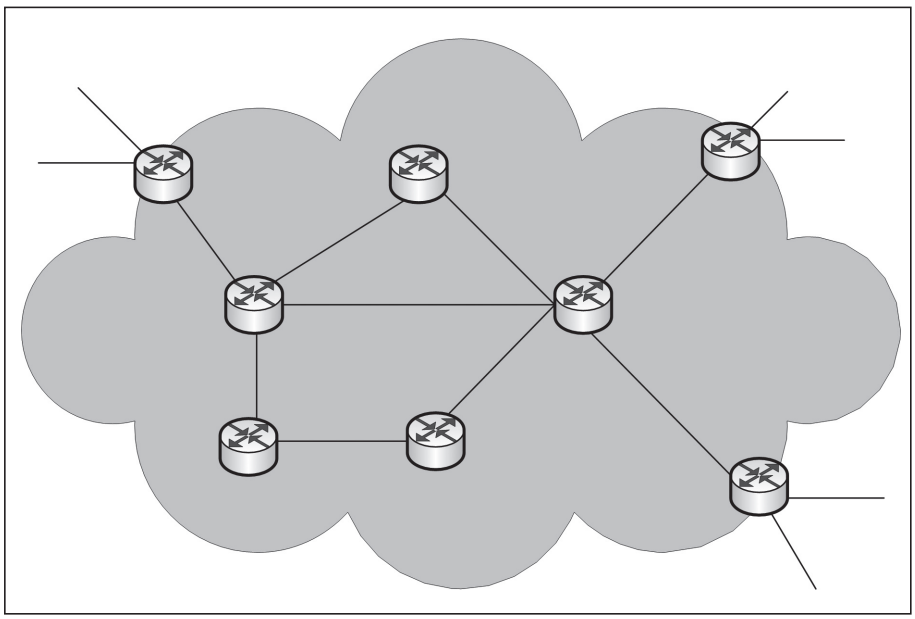


Figura 8.18. *Routers en un ISP.*

Es importante destacar que cuando un router elige el camino por el que se debe enviar un datagrama, se envía dicho datagrama al siguiente router y se olvida del mismo. El siguiente router puede elegir el mismo camino u otro diferente. Esto es positivo ya que permite mantener en cada router la lógica mínima necesaria.

Sin embargo este procedimiento tiene asociado un inconveniente. Cuando las tablas de encaminamiento no están convenientemente actualizadas y sincronizadas puede ocurrir que un datagrama pase de router a router sin alcanzar su destino de forma indefinida. Para evitar esta situación se utiliza el campo TTL del datagrama IP. Cada paso por un router decrementa este campo una unidad. Cuando llega a 0 el paquete es descartado.

Otra característica interesante de los routers es que no propagan los envíos de difusión por lo que se dice que cada red a la que está conectado un router forma un dominio de difusión.

El encaminamiento de los paquetes en un router se basa en la información de la tabla de encaminamiento. Esta información es dinámica ya que periódicamente los routers reciben información con los posibles cambios de topología de las redes que pueden suponer cambios en dicha tabla. Sin embargo, los routers permiten la configuración de rutas estáticas, introducidas manualmente por el administrador de la red.

La tabla de encaminamiento está formada al menos por los campos:

- **Identificador de red,** donde se almacena la dirección IP de la red de destino.
- **Coste,** contiene un valor que pretende cuantificar en base a algún criterio el coste que supone alcanzar dicha red. Un valor bajo indicará una ruta rápida y un valor alto indicará una ruta lenta.
- **Siguiente salto,** este campo contiene la dirección del próximo router al que tiene que dirigirse el paquete para alcanzar una red de destino dada.

La tabla de encaminamiento inicial sólo incluye información de las redes a las que el router está conectado. Posteriormente se irá recibiendo información de los routers adyacentes y se irá completando la tabla de encaminamiento.

Existen dos tipos de algoritmos de encaminamiento:

- **Encaminamiento basado en el vector distancia.** En este tipo de encaminamiento se asume el coste de una unidad por cada enlace. Por tanto, el coste de una ruta determinada es la suma de los costes de cada enlace. En este caso la ruta óptima se considera a aquélla que necesita menos retransmisiones o saltos. La eficiencia de la transmisión, por tanto, es función sólo del número de enlaces requeridos para alcanzar el destino.
- **Encaminamiento basado en el estado del enlace.** En este caso, el coste no se refiere al número de saltos hasta la red de destino sino que es un valor con peso basado en una variedad de factores como el tráfico, estado del enlace... Por tanto el coste asociado a una ruta representa una valoración de la eficacia de la misma.

El encaminamiento basado en el vector distancia es más sencillo de implementar y más rápido pero el coste no refleja a veces las situaciones de tráfico reales. Esta situación está mejor reflejada en el encaminamiento basado en el estado del enlace, pero por el contrario es más complejo de implementar.

8.7.2 PROTOCOLOS DE ENCAMINAMIENTO

A efectos de encaminamiento de información se define un **Sistema autónomo** como una colección de redes que están bajo el control administrativo de una única organización y que comparten una misma estrategia de encaminamiento. Ejemplos de sistemas autónomos: redes de empresas, proveedores de servicio, organismos oficiales, universidades.

En función de donde se lleve a cabo el encaminamiento existen dos tipos de protocolos de encaminamiento:

- **Protocolos de pasarela interior:** protocolos de encaminamiento que operan dentro de un sistema autónomo. Los principales protocolos de pasarela interior son:
  - **RIP (Routing Information Protocol),** tipo vector distancia y de los primeros utilizados. Muy extendido. Para solucionar algunas limitaciones de RIP se implementó RIP2.
  - **IGRP (Interior Gateway Routing Protocol),** tipo vector distancia, más robusto que RIP. Desarrollado por CISCO y por tanto es propietario.
  - **EIGRP,** mejora de IGRP, se considera un protocolo híbrido.
  - **OSPF (Open Shortest Path First),** estándar abierto basado en el estado del enlace.
- **Protocolos de pasarela exterior:** se ejecutan en los routers situados en los extremos de los sistemas autónomos y que intercambian información con otros sistemas autónomos. Los protocolos de pasarela interior más comunes son:
  - **BGP (Border Gateway Protocol).** Estándar actual (de facto). Hace posible el crecimiento y la propia existencia de Internet. Soporta el direccionamiento CIDR lo que hace posible un uso más eficiente de las tablas de encaminamiento. Actualmente se utiliza la versión 4.
  - **EGP (Exterior Gateway Protocol).** Antiguo protocolo de pasarela exterior que ha sido sustituido por BGP. En extinción.

8.8 PROTOCOLOS DEL NIVEL DE APLICACIÓN

El nivel de aplicación es el nivel más alto del modelo TCP/IP y su funcionalidad está asociada generalmente a cubrir las necesidades del usuario final. Sin embargo, en TCP/IP también se utiliza el nivel de aplicación para proporcionar funcionalidades que atienden a la gestión y mantenimiento de las redes.

La implementación de las funcionalidades del nivel de aplicación se lleva a cabo, como en el resto de niveles, a través de protocolos. Los protocolos del nivel

de aplicación en TCP/IP siguen todos un modelo cliente-servidor. Uno de los extremos de la comunicación será el que solicita datos (cliente) y el otro extremo de la comunicación se encarga de proporcionar dichos datos (servidor).

En este contexto, la funcionalidad aportada por una aplicación que utiliza alguno de los protocolos del nivel de aplicación se conoce como **servicio**. De esta forma, una aplicación cliente se ejecuta en un equipo para solicitar un servicio (envío de datos) a una aplicación servidor que estará en ejecución en otro equipo atendiendo cualquier petición de servicio que reciba.

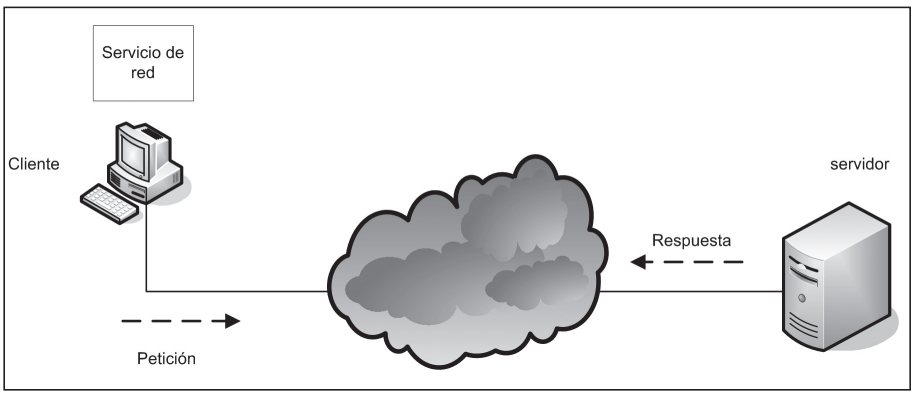


Figura 8.19. *Modelo cliente-servidor de los protocolos TCP/IP en el nivel de aplicación.*

En los próximos apartados se describirán brevemente los principales protocolos utilizados en TCP/IP. Dichos protocolos se pueden dividir en aquellos destinados a proporcionar una determinada funcionalidad al usuario final, como son FTP, Telnet, SMTP, SNMP y HTTP, y aquellos destinados a tareas de gestión y mantenimiento de la red, como son BOOTP, DHCP y DNS.

8.8.1 PROTOCOLO BOOTP

BOOTP (Bootstrap Protocol) es un protocolo cliente-servidor que proporciona a un equipo la información de configuración para su conexión a una red, es decir, una dirección IP, una máscara de red, la dirección IP de la puerta de enlace y la dirección IP de un servidor DNS.

Su principal uso ha sido proporcionar una configuración de red válida a equipos que no disponían de unidades de almacenamiento (discos) donde almacenar dicha configuración. Este protocolo se diseñó para mejorar el protocolo RARP que tenía una función similar pero que sólo proporcionaba una dirección IP, lo cual en la mayoría de los casos no era suficiente. Actualmente BOOTP ha sido sustituido en la mayoría de los casos por el protocolo DHCP.

BOOTP utiliza el protocolo UDP en el nivel de transporte. El servidor lleva a cabo sus comunicaciones por el puerto 67 y los clientes utilizan el puerto 68.

El servidor BOOTP almacena una tabla con las direcciones IP y las direcciones físicas de los dispositivos. Esta tabla contiene la información de forma estática, siendo el administrador del servicio BOOTP el que debe añadir o eliminar datos de la misma.

8.8.2 PROTOCOLO DHCP

DHCP (Dynamic Host Configuration Protocol, Protocolo de configuración dinámica de estación) es un protocolo cliente-servidor para proporcionar la configuración de parámetros de red, por tanto su funcionalidad es muy similar a BOOTP.

DHCP es un protocolo implementado para sustituir a BOOTP, añadiendo características adicionales. DHCP es por tanto compatible con BOOTP, utiliza UDP, mantiene prácticamente sin cambios el formato de trama y utiliza los mismos puertos que BOOTP (67 para el servidor y 68 para los clientes). Los parámetros de configuración de red obtenidos son los mismos que en BOOTP, es decir, la dirección IP, máscara de red, puerta de enlace y servidor DNS. De esta forma, un cliente BOOTP puede solicitar su configuración de red a un servidor DHCP.

Para solicitar una configuración de red a un servidor DHCP se envía una solicitud utilizando la dirección IP de broadcast genérica 255.255.255.255 o la dirección de broadcast de la subred.

La principal mejora que aporta DHCP es que la asignación de los parámetros de red es dinámica y por tanto más flexible que en BOOTP. Esto implica que las asignaciones son temporales, es decir, se asigna un tiempo de validez y transcurrido el mismo se deben renegociar los parámetros de red.

Actualmente el uso de servidores DHCP está muy extendido. La mayoría de los ISP utilizan un servidor DHCP para asignar las direcciones públicas a sus clientes. Y la mayor parte de los routers actuales también implementan un servidor DHCP para la asignación de direcciones privadas en una red de área local. Los sistemas operativos de tipo servidor como Windows 2000/2003 Server o Linux incluyen también servidores DHCP.

8.8.3 PROTOCOLO DNS

DNS (Domain Name System, Sistema de nombres de dominio) es el protocolo utilizado para poder asociar a una dirección IP un nombre. DNS utiliza el modelo cliente-servidor donde se mantiene una base de datos jerárquica y distribuida para almacenar todas las correspondencias entre nombres y direcciones IP.

La asignación de un nombre de dominio es el método utilizado para asociar un nombre a un recurso dentro de Internet. Un nombre de dominio está formado por una sucesión de nombres (dominios) separados por puntos y siguiendo una determinada jerarquía. El dominio de nivel superior (también conocido como **TLD, Top**

Level Domain) es el que aparece en última posición. Por ejemplo, para el nombre **www.ra-ma.es**, el domino de nivel superior es 'es'.

Los dominios de nivel superior más frecuentes son 'com', 'org', 'edu', 'net' o los nombres de dominios asignados por países, como 'es' para España, 'ar' para Argentina, 'br' para Brasil, 'de' para Alemania, 'nl' para Holanda…

Muchos servicios del nivel de aplicación utilizan nombres para referirse a equipos, sin embargo, para llevar a cabo una comunicación con ese equipo es necesario conocer su dirección IP. Para ello se genera una petición DNS que se envía a un servidor DNS (name server). La información que se mantiene en el sistema DNS es distribuida y si dicho servidor no es capaz de resolver la petición puede redirigirla a otro servidor. Los servidores que gestionan los dominios de nivel superior o TLD se conocen como **root servers**, que se pueden considerar como los nodos primarios del sistema DNS. Actualmente hay 13 root servers operativos en Internet.

El envío de la información DNS, tanto de las peticiones como de las respuestas, se lleva a través del puerto 53 y se utiliza tanto UDP como TCP.

8.8.4 PROTOCOLO FTP

FTP (File Transfer Protocol, Protocolo de transferencia de ficheros) es uno de los primeros protocolos del nivel de aplicación desarrollados en redes TCP/IP. Es un protocolo cliente-servidor utilizado para el intercambio de ficheros, que es una de las tareas más habituales realizadas en un entorno de red. Se utilizan dos conexiones TCP para realizar las transferencias, una para los datos que utiliza el puerto 20 y otra para información de control que utiliza el puerto 21.

El servicio de transferencia de ficheros es proporcionado por un servidor FTP que es un proceso ejecutándose en un equipo y que escucha las peticiones recibidas a través del puerto 21. Este protocolo utiliza la validación de la conexión mediante la introducción de un nombre de usuario y una contraseña aunque la mayor parte de los servidores FTP admiten la posibilidad de activar lo que se conoce como usuario anónimo (anonymous) para permitir el acceso anónimo a un servidor FTP, normalmente con acceso restringido.

Las primeras implementaciones de clientes FTP se usaban sobre líneas de comandos. Este tipo de clientes todavía están disponible en los sistemas Windows o en Linux, a través del comando ftp. Actualmente existen clientes FTP que se ejecutan en los avanzados entornos gráficos y que son mucho más sencillos de utilizar. Incluso los navegadores web implementan la funcionalidad del protocolo FTP.

Una de las principales carencias del protocolo FTP es que todos los datos intercambiados, incluidos los datos de validación (nombre de usuario y contraseña), se transfieren sin ningún tipo de encriptación. Actualmente se han desarrollado otros protocolos de transferencia de ficheros en modo seguro, con encriptación de los datos, como FTP sobre SSH (conocido como **Secure FTP**), **FTPS** (FTP/SSL) o **SCP (Secure Copy Protocol)**.

8.8.5 PROTOCOLO TELNET

Telnet (Terminal Network, Terminal de red) es un protocolo cliente-servidor que permite la conexión a un equipo remoto a través de un terminal desde el cual se pueden ejecutar comandos y aplicaciones como si se ejecutasen de forma local. El protocolo Telnet envía los caracteres tecleados en el equipo local (cliente) al equipo remoto (servidor), el cual los interpreta como si se hubiesen tecleado en un terminal de comandos local. La salida producida en el equipo remoto se envía al equipo local donde se visualiza. Telnet utiliza el puerto 23.

Es uno de los primeros protocolos implementados en redes TCP/IP. En los sistemas Unix ha sido ampliamente utilizado para llevar a cabo la administración de equipos de forma remota.

Al igual que el protocolo FTP, uno de sus principales problemas es la seguridad ya que ni siquiera el nombre de usuario y la contraseña de validación se envían encriptados. Por ello, se ha desarrollado el protocolo **SSH (Secure Shell)** con la misma funcionalidad que Telnet pero llevando a cabo la encriptación de todos los datos que se transmite. SSH utiliza el puerto 23 y se utiliza ampliamente en los sistemas Linux.

8.8.6 PROTOCOLO SMTP

SMTP (Simple Mail Transfer Protocol, Protocolo simple de transferencia de correo) es un protocolo cliente-servidor que sirve para el envío de mensajes de correo electrónico de un usuario a otro o de un usuario a un servidor SMTP. El envío de correo entre un cliente y un servidor se lleva a cabo a través del puerto 25 de una conexión TCP.

Para el envío de correo se utiliza un sistema de direccionamiento con el siguiente formato:

Parte local @ nombre de dominio

SMTP sólo se puede utilizar para enviar texto ASCII. Debido a esta limitación se desarrolló **MIME (Multipurpose Internet Mail Extensions)** como una extensión a SMTP para permitir el envío de datos no ASCII.

Otro protocolo asociado al servicio de correo electrónico es **POP3 (Post Office Protocol, protocolo de oficina de correos versión 3)** que es un protocolo cliente-servidor utilizado para descargar mensajes de correo electrónico desde un servidor (normalmente SMTP). POP3 lleva a cabo la comunicación mediante conexiones TCP utilizando el puerto 110.

En el modelo OSI existía otro protocolo que implementaba el servicio de correo electrónico llamado X.400, pero actualmente apenas se utiliza debido a la gran aceptación de SMTP.

8.8.7 PROTOCOLO SNMP

SNMP (Simple Network Management Protocol, protocolo simple de gestión de red) es un protocolo para gestionar dispositivos de red a través del protocolo TCP/IP. Está basado en el concepto de gestor y agente. Un gestor es normalmente un equipo que controla y monitoriza un conjunto de agentes, normalmente routers. Como este protocolo está definido en el nivel de aplicación, puede gestionar redes con características y tecnologías diferentes.

Los equipos gestores ejecutan un cliente SNMP. Los dispositivos gestionados o agentes ejecutan un servidor SNMP.

El protocolo SNMP proporciona un mecanismo útil y eficaz para monitorizar redes. Sin embargo, el intercambio de información entre gestores y agentes hace que el tráfico de red aumente.

La transferencia de los datos del protocolo SNMP se lleva a cabo mediante UDP a través de los puertos 161 (agente) y 162 (gestor).

8.8.8 PROTOCOLO HTTP

HTTP (Hypertext Transfer Protocol, Protocolo de transferencia de hipertexto) actualmente es el principal protocolo para el acceso a datos en el nivel de aplicación de la arquitectura TCP/IP. Utilizado en el servicio más extendido en Internet, la World Wide Web. Este protocolo permite la transferencia tanto de texto sin formato, como de texto con formato, hipertexto (permite saltos rápidos entre documentos), imágenes, sonido y video. La comunicación a través del protocolo HTTP se lleva por defecto por el puerto 80.

Es un protocolo cliente-servidor en el cual, el cliente HTTP (normalmente un navegador web) envía mensajes, llamados peticiones, a un servidor HTTP. El servidor responde enviando una respuesta al cliente, esta respuesta contiene normalmente la página web solicitada por el cliente en la petición. Dicha página web en realidad es un archivo.

Localizador uniforme de recursos (URL)

URL es un formato estándar para especificar cualquier tipo de información en Internet. HTTP utiliza este formato para el acceso a los recursos. Un URL está formado por cuatro elementos:

- **Método:** protocolo utilizado para obtener el recurso, por ejemplo HTTP.
- **Servidor:** equipo donde se encuentra la información a la que se quiere acceder.
- **Puerto:** es opcional y contiene el número de puerto del servidor. Por defecto se utiliza el puerto 80.

- **Ruta:** camino para llegar al recurso al que se quiere acceder. Se utiliza el carácter / para separar los nombres de los directorios.

  Método :// Servidor : puerto / ruta

  http://www.google.es
  http://www.uc3m.es/depar/operativos/index.html
  http://www.servidor.com:3500/ejemplo/graficos.html

La **World Wide Web** (www) o simplemente la web es un servicio cliente-servidor distribuido que utiliza principalmente el protocolo HTTP para su funcionamiento. La web es un repositorio de información mundial y enlazada entre sí.

Los documentos contenidos en la web pueden ser de tres tipos:

- **Estáticos:** documentos de contenido fijo que se crean y almacenan en un servidor. El cliente sólo puede obtener una copia de los mismos. El lenguaje utilizado para crear páginas web estáticas es HTML. Este lenguaje permite especificar etiquetas para dar formato al texto. Estas etiquetas son leídas e interpretadas por los navegadores web.
- **Dinámicos:** un documento dinámico se crea en el servidor cuando un cliente lo solicita. Cuando llega la petición, el servidor web ejecuta un programa que crea el documento y le envía el resultado al cliente. El contenido del documento dinámico puede variar de una petición a otra.

  CGI es una tecnología para crear y gestionar documentos dinámicos. CGI no es un lenguaje, es un conjunto de estándares que definen cómo escribir un documento dinámico, cómo proporcionar la entrada al programa y cómo se debería utilizar el resultado de salida. Un programa CGI puede estar escrito en cualquier lenguaje de programación.
- **Activos:** los documentos activos son realmente programas que necesitan ejecutarse en el cliente. Cuando un navegador solicita un documento activo, el servidor envía una copia del documento en formato binario y ésta es ejecutada en el cliente.

El lenguaje de programación más utilizado para crear documentos activos es Java. Los programas escritos en Java y ejecutados a través de un navegador web se conocen como applets.

8.8.9 PROTOCOLO NETBIOS

NetBIOS (Network Basic Input Output System) inicialmente fue desarrollado por IBM como un API para proporcionar funciones básicas de acceso a una red para la compartición de recursos en una red de área local.

Basado en el API NetBIOS, IBM también desarrolló el **protocolo NetBEUI**. Es un protocolo muy básico donde a cada dispositivo de la red se le asigna un nombre de 15 caracteres (no confundir el nombre NetBIOS con el nombre de host en TCP/IP). No es un protocolo enrrutable por lo que sólo se puede utilizar en redes LAN.

Posteriormente se desarrolló NetBIOS sobre TCP/IP que es el protocolo que se sigue utilizando en redes LAN basadas en el sistema operativo Windows. NetBIOS utiliza los puertos 137, 138 y 139.

8.9 COMANDOS TCP/IP

Todos los sistemas operativos actuales implementan los protocolos TCP/IP para proporcionar conectividad al sistema. Junto con la implantación de los protocolos existen una serie de herramientas ejecutadas en línea de comandos para llevar a cabo tareas de mantenimiento, gestión y monitorización.

A continuación se presentan los comandos TCP/IP disponibles en los sistemas Windows 2000/XP, la mayor parte de ellos también está disponibles en otros sistemas como Linux. Los valores a sustituir en un comando van encerrados entre paréntesis angulares "< >", pero dichos símbolos no se han de teclear para ejecutar el comando.

8.9.1 COMANDO PING

El comando ping se ejecuta en un equipo para comprobar si es posible el intercambio de datagramas IP con otro equipo cuya dirección se especifica como parámetro. Para llevar a cabo esta acción el comando ping envía un mensaje ICMP de tipo Echo-Request. Si este menaje ICMP llega al receptor, éste responderá con otro mensaje ICMP de tipo Echo-Reply dirigido al remitente del mensaje Echo-Request.

Coloquialmente se utiliza la expresión "hacer ping" para referirse a ejecutar el comando ping sobre el nombre o dirección IP de un equipo.

Se puede utilizar como parámetro tanto una dirección IP como un nombre de red, siempre que el equipo tenga configurado algún método de resolución de ese nombre en su IP correspondiente. Lo normal es configurar en las propiedades de la conexión un servidor DNS para llevar a cabo esta función.

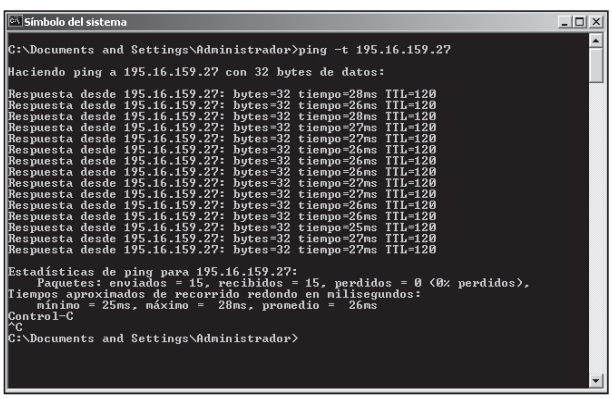


Figura 8.20. *Ejecución del comando ping en Windows XP.*

El comando ping se desarrolló como método para comprobar la conectividad a nivel IP entre dos equipos utilizando el protocolo ICMP. Actualmente los mecanismos de seguridad implementados tanto en los dispositivos de red (routers) como en los propios equipos, como antivirus o firewalls, pueden estar configurados para rechazar los paquetes ICMP y por tanto, a pesar de que haya conectividad entre equipos, el comando ping no obtendrá respuesta.

A continuación se presenta la forma de uso del comando ping y algunas de las opciones más interesantes:

ping <-opción> <dirección_IP>

Opciones:

Tabla 8.5

Opción	Significado
t	Envía mensajes ICMP Echo-request hasta que se para la ejecución del comando con las teclas [Control]+[C]. Se pueden ver las estadísticas y continuar con las teclas [Control]+[Inter]
n cuenta	Opción para especificar el número de peticiones eco para enviar. Por defecto son cuatro
l tamaño	Opción para especificar el número de bytes que se enviará en cada paquete ICMP. Por defecto son 32 bytes
f	Activa el indicador de no fragmentación en la cabecera IP de cada paquete ICMP
i TTL	Opción para especificar el valor del campo TTL (Time To Live, Tiempo de vida) de la cabecera IP
v TOS	Opción para especificar el campo TOS (Type Of service, Tipo de servicio) de la cabecera IP
w tiempo de espera	Tiempo de espera en milisegundos para esperar cada respuesta. Por defecto es 1 segundo (1000 milisegundos)
r cuenta	Ruta del registro para la cuenta de saltos
a	Resolver direcciones en nombres de host
s saltos	Indica la marca de hora para la cuenta de saltos indicado
j lista-host	Encamina los paquetes mediante la lista de equipos indicada (el número máximo de equipos que se pueden indicar es nueve). Los equipos consecutivos pueden separarse por puertas de enlace intermedias
k lista-host	Encamina los paquetes mediante la lista de equipos indicada (el número máximo de equipos que se pueden indicar es nueve). Los equipos consecutivos no pueden separarse por puertas de enlace intermedias

8.9.2 COMANDO IPCONFIG

Muestra todos los valores actuales de la configuración TCP/IP. Es especialmente útil en los sistemas que ejecutan DHCP ya que permite averiguar las direcciones IP que se han adjudicado.

La forma de escribir este comando es:

ipconfig </opción>

Opciones:

Este comando tiene las siguientes opciones:

Tabla 8.6

Opción	Significado
all	Muestra la presentación completa de datos (sin esta opción, únicamente mostrará la dirección *IP*, la máscara de subred y la dirección *IP* de la puerta de enlace predeterminada para cada tarjeta de red).
release <adaptador>	Libera la configuración actual de *DHCP*, desactivando *TCP/IP* (en *<adaptador>* hay que poner el nombre que aparece cuando se utiliza *IPCONFIG* sin ninguna opción).
renew <adaptador>	Renueva los parámetros de configuración de *DHCP* (en <adaptador> hay que poner el nombre que aparece cuando se utiliza *IPCONFIG* sin ninguna opción).
flushdns	Borra la caché de resoluciones DNS.
registerdns	Actualiza todas las concesiones DHCP y vuelve a registrar los nombres DNS.
displaydns	Muestra el contenido de la caché de resolución de DNS.

Ejemplo:

Para ver todo los parámetros de configuración de TCP/IP, introduzca:

ipconfig /all

Para ver el contenido de la caché de DNS:

ipconfig /displaydns

El comando equivalente en Linux es **ifconfig**.

8.9.3 COMANDO NETSTAT

Muestra las estadísticas de protocolo y las conexiones actuales de la red TCP/IP.

La forma de escribir este comando es:

netstat <-opción> <intervalo>

<intervalo> indica el tiempo (en segundos) de pausa que esperará antes de volver a mostrar las estadísticas (deberá pulsar [**Ctrl**]+[**C**] para interrumpir la presentación de las estadísticas).

Opciones:

Este comando tiene las siguientes opciones:

Tabla 8.7

Opción	Significado
a	Presenta todas las conexiones y puertos de escucha.
e	Presenta estadísticas relativas a *Ethernet*.
n	Presenta las direcciones y los números de puerto en formato numérico.
p <protocolo>	Muestra las conexiones del protocolo indicado que puede ser *TCP* o *UDP* (si se utiliza junto a la opción s, el protocolo podrá ser *ICMP, IP, TCP* o *UDP*).
r	Presenta el contenido de la tabla de enrutamiento.
s	Presenta estadísticas de cada protocolo (*ICMP, IP, TCP* y *UDP*). Si se utiliza junto a la opción **p**, presentará un subconjunto de dichas estadísticas.

Ejemplo:

Para ver las estadísticas de protocolo y conexiones actuales *TCP/IP* de todos los protocolos cada 30 segundos, introduzca:

netstat -s 30

En los resultados obtenidos por este comando se obtiene una tabla en la que aparece un campo llamado Estado. Los valores que puede tomar este campo se explican a continuación:

Tabla 8.8

ESTABLISHED	Conexión establecida
SYN_SENT	Se está intentando iniciar una conexión
SYN_RECV	Una petición de conexión fue recibida por la red
FIN_WAIT1	La conexión esta finalizándose
FIN_WAIT2	La conexión está cerrada, y se está esperando que finalice la conexión remota
TIME_WAIT	Se está esperando después de cerrarse que concluyan los paquetes que siguen en la red
CLOSED	La conexión no se está usando
CLOSE_WAIT	La conexión remota finaliza, y se espera que se cierre el socket
LAST_ACK	La conexión remota finaliza, y se espera que se cierre el socket. Esperando el ACK
LISTEN	El socket está esperando posibles conexiones entrantes
CLOSING	Ambos sockets han finalizado pero aún no fueron enviados todos los datos
UNKNOWN	El estado del socket no se conoce

8.9.4 COMANDO ROUTE

Controla las tablas de enrutamiento de la red.

La forma de escribir este comando es:

route <-opción> <comando> <destino> <máscara> <puerta> <métrica>

- *<destino>* indica el equipo al que se enviará el comando.

- *<máscara>* especifica una máscara de red que se va a asociar con el camino (si no se indica se tomará 255.255.255.255).
- *<puerta>* especifica una puerta de enlace.
- *<métrica>* asigna una medida de costo para calcular las rutas más rápidas.

Opciones:

Este comando tiene las siguientes opciones:

Tabla 8.9

Opción	Significado
f	Borra las tablas de enrutamiento de todas las entradas de puerta de enlace (si se utiliza junto a algún comando, se borrarán antes de la ejecución de éste).
p	Se puede utilizar con el comando *ADD* (establecerá una ruta permanente para todos los inicios del sistema) o *PRINT* (mostrará la lista de rutas permanentes registradas).

Los posibles comandos son:

Comando	Significado
ADD	Agrega un camino.
CHANGE	Modifica el camino existente.
DELETE	Elimina un camino.
PRINT	Imprime un camino

Ejemplo:

Para borrar todas las entradas de las tablas de enrutamiento, introduzca:

route –f

8.9.5 COMANDO ARP

Muestra o modifica las tablas de traducción de las direcciones IP a direcciones Ethernet para que sean utilizadas por el protocolo de resolución de direcciones ARP.

La forma de escribir este comando es:

arp <-opción> <dirección_IP> <dirección_ethernet> <dirección_interfaz>

donde:

- *<dirección_IP>* indica la dirección *IP* en notación decimal con puntos.
- *<dirección_ethernet>* corresponde a la dirección física y se ha de indicar como 6 *bytes* hexadecimales separados por guiones.

- *<dirección_interfaz>* indica la dirección *IP* de la interfaz cuya tabla de conversión de direcciones se desea modificar (si no se indica ninguna, se usará la primera disponible).

Opciones:

Este comando tiene las siguientes opciones:

Tabla 8.10

Opción	Significado
a	Muestra las entradas actuales de *ARP*. Si se especifica *<dirección_IP>*, únicamente mostrará las direcciones IP y físicas del equipo al que corresponde dicha dirección IP.
d	Elimina de la tabla la entrada indicada en *<dirección_IP>*.
N	Se usa únicamente con *<dirección_interfaz>*. Muestra las entradas de la tabla para la interfaz de red especificada.
s	Añade una entrada en la tabla para asociar la *<dirección_IP>* con la *<dirección_ethernet>*.

Ejemplos:

Para añadir a la tabla de traducción de direcciones la dirección IP 172.16.132.1 asociada con la dirección física 00C0DFA00CBE, introduzca:

arp -s 172.16.132.1 00-C0-DF-A0-0C-BE

Para ver el contenido de la tabla de traducción de direcciones, introduzca:

arp -a

8.9.6 COMANDO TRACERT

Comando para obtener información del camino que siguen los paquetes IP para llegar a un determinado equipo.

El proceso que lleva a cabo es el siguiente. El comando tracert envía mensajes ICMP de Echo-Request. El primer mensaje lo envía con el campo TTL = 1. Por lo que el primer router por el que pasan los paquetes al destino especificado decrementará el valor de este campo y al quedarse en 0, devolverá un mensaje de tipo 11 (Tiempo de datagrama excedido). El comando tracert interpreta este mensaje como una respuesta del primer router. A continuación envía otro mensaje ICMP Echo-Request con el valor de TTL=2. Esta vez será el segundo router por el que pasa el paquete el que responda con el mensaje de tipo 11. El siguiente mensaje ICMP se envía con TTL=3 y será el tercer router de la ruta el que responda. Esta operación se repite hasta que se especifica un número de saltos suficientes para llevar al destino. Éste responderá con un mensaje ICMP Echo-Reply y con ello el comando tracert sabe que se ha alcanzado el destino y finaliza la ejecución.

Al igual que en el comando ping, puede ocurrir que algunos de los routers por los que pasan los paquetes ICMP de tracert sean rechazados por algún mecanismo de seguridad, típicamente un firewall.

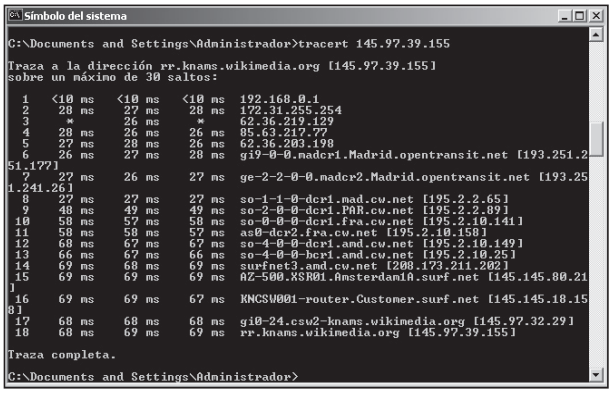


Figura 8.21. *Ejecución del comando tracert en Windows XP.*

La forma de escribir este comando es:

tracert <-opción> <destino>

- *<destino>* especifica el nombre del equipo destino.

Opciones:

Este comando tiene las siguientes opciones:

Tabla 8.11

Opción	Significado
D	Indica que las direcciones no se deben resolver en nombres de equipos.
h <saltos>	Especifica el número máximo de saltos que se han de dar para buscar el destino.
j <equipos>	Indica los posibles caminos a través de los equipos que se indican.
w <tiempo>	Espera cada respuesta el número de milisegundos indicado.

Ejemplo:

Para determinar el camino hasta el equipo *PRINCIPAL* con un número máximo de nueve saltos y con un tiempo de espera de 10 milisegundos, introduzca:

tracert -h 9 -w 10 PRINCIPAL

El comando equivalente en Linux es traceroute.

8.9.7 COMANDO NSLOOKUP

Muestra información de los servidores de nombres *DNS*.

La forma de escribir este comando es:

nslookup <-opción> <equipo> <servidor>

- *<equipo>* indica la dirección *IP* o el nombre del equipo a buscar. Si se escribe un guión en lugar de un valor, se pasa al modo interactivo (se distingue porque el indicador del sistema es el signo >).
- *<servidor>* indica el servidor *DNS* que se desea utilizar en lugar del predeterminado.

Para obtener una lista de las opciones disponibles desde el modo interactivo teclear *help*.

8.9.8 COMANDO HOSTNAME

Indica el nombre del equipo actual.

La forma de escribir este comando es:

hostname

Opciones:

Este comando no tiene ninguna opción.

Ejemplo:

Para ver el nombre del equipo actual, introduzca en la línea de comandos:

hostname

8.9.9 COMANDO NBTSTAT

Muestra las estadísticas de protocolo y las conexiones *TCP/IP* actuales que utilizan *NBT* (*NetBIOS sobre TCP/IP*).

La forma de escribir este comando es:

nbstat <-a nombre> <-A dirección_IP> <-opción> <intervalo>

- *<nombre>* especifica la tabla de nombres del equipo remoto utilizando su nombre.
- *<dirección_IP>* especifica la tabla de nombres del equipo remoto utilizando su dirección *IP*.
- *<intervalo>* indica el tiempo (en segundos) de pausa que esperará antes de volver a mostrar las estadísticas (deberá pulsar [**Ctrl**]+[**C**] para interrumpir la presentación de las estadísticas).

Opciones:

Este comando tiene las siguientes opciones:

Tabla 8.12

Opción	Significado
c	Presenta el contenido del caché de nombres *NetBIOS* indicando la dirección IP de cada nombre.
n	Presenta una lista de los nombres *NetBIOS* locales.
r	Presenta las estadísticas de resolución de nombres de red de Windows. Si utiliza *WINS*, devolverá el número de nombres resueltos y registrados mediante **WINS** o mediante difusión amplia.
R	Vuelve a cargar el archivo *LMHOSTS* después de limpiar la memoria caché de nombres *NetBIOS*.
s	Presenta las sesiones de cliente y servidor intentando convertir la dirección IP del equipo remoto en un nombre utilizando el archivo *HOSTS*.
S	Presenta las sesiones de cliente y servidor indicando los equipos remotos mediante su dirección *IP*.

Ejemplo:

Para ver las estadísticas de protocolo y conexiones *TCP/IP* actuales que usan *NBT* del equipo remoto con la dirección *IP* 172.54.23.4 cada 30 segundos, introduzca:

```
nbtstat -A 172.54.23.4 30
```

8.10 TÉCNICAS AVANZADAS EN REDES TCP/IP

8.10.1 NAT

NAT (Network Address Translation, Traducción de Dirección de Red) es un estándar creado por la IETF (Internet Engineering Task Force) que utiliza una o más direcciones IP para conectar varios ordenadores de una red interna a otra red externa (normalmente a Internet), los cuales tiene una dirección IP completamente distinta (normalmente una IP no válida de Internet llamada dirección no enrrutable). Para llevar a cabo este proceso, las direcciones IP se mapean desde el dominio interno de direcciones al dominio externo, proporcionando encaminamiento transparente a las máquinas finales.

Por lo tanto, NAT se puede utilizar para dar salida a redes públicas (normalmente Internet) a ordenadores que se encuentran dentro de una red con direccionamiento privado o para proteger máquinas públicas.

La finalidad inicial es la de poder realizar cambios en la topología de la red interna y que dichos cambios no sean visibles en la red externa, es decir, se trata de ocultar información sobre la topología de una red interna a otra externa.

Posteriormente se ha utilizado una variante de NAT como solución a la escasez de direcciones públicas para Internet. De esta forma, una organización utiliza un rango de direcciones de red privadas (y por tanto no válidas para Internet) para sus equipos, y puede dar acceso a todos los servicios que proporciona Internet utilizando una sola dirección de red pública. Debido a ello, el uso de NAT está muy extendido actualmente y prácticamente todos los routers lo implementan.

En este ámbito se conoce como red privada a una red cuyos dispositivos utilizan un rango de direcciones privadas, no válidas en Internet:

Clase A. 10.0.0.0
Clase B: 172.16.0.0 - 172.31.0.0
Clase C: 192.168.0.0 - 192.168.255.0

El proceso de traducción de direcciones se lleva a cabo en el dispositivo de red que une la red interna y la red externa, normalmente un router. Hay varios tipos de NAT:

- **NAT estático:** se realiza un mapeo uno a uno de direcciones, es decir, a cada dirección de la red privada se le asigna una dirección de red externa. Por ejemplo: 192.168.0. x -> 210.34.48.x
- **NAT dinámico:** se realiza una asignación dinámica de las direcciones externas. Cuando un ordenador de la red privada manda un paquete a la red externa, el dispositivo donde se implementa NAT le asigna una dirección de forma dinámica. Cuando la sesión que utiliza una dirección finaliza, la dirección de la red externa reservada se libera.
- **NAPT: Network Address and Port Translation.** Este método se lleva a cabo utilizando un mapeo tanto de la dirección IP fuente como del puerto fuente de la red interna. Este método se utiliza para que redes privadas puedan acceder a Internet a través de una única dirección IP.

Para llevar a cabo tanto NAT estático como dinámico, el dispositivo donde se implementa NAT debe alterar la cabecera de los paquetes IP. Sin embargo, para NAPT se debe alterar la información tanto de IP como de TCP o UDP.

Gracias a NAPT se ha solucionado en parte el problema de la falta de direcciones IP para IPv4. Sin embargo, en la versión 6 de IP (IPv6) y gracias al gran rango de direccionamiento utilizado, cada dispositivo tendrá asignado una dirección global y por tanto no será necesario utilizar NAT.

8.10.2 PROXY

El término **Proxy** se aplica generalmente a una aplicación que actúa como intermediario entre dos sistemas finales y que es conocida como servidor proxy. Los servidores proxy funcionan en el nivel de aplicación, por tanto es necesario ejecutar un servicio proxy por cada tipo de aplicación.

El tipo de servidor proxy más utilizado es el servidor proxy web, el cual se utiliza para centralizar todas las conexiones a páginas web de una red. Esta característica ofrece la posibilidad de llevar a cabo mecanismos de seguridad como filtrado de direcciones, validación de usuarios... Un servidor proxy permite el acceso a páginas web a todos los equipos de una red en la que sólo un equipo tiene conexión real (e IP pública asignada).

Los servidores proxy web también pueden proporcionar un mecanismo llamado Proxy-caché, que consiste en almacenar las páginas web a las que se ha accedido en una caché. Esta característica acelera la conexión a las páginas web más visitadas. Los proxy-cachés implementan algoritmos para decidir cuándo una página debe ser descartada de la caché.

Para que un cliente acceda a páginas web a través de un proxy es necesario configurar adecuadamente el navegador web.

Proxy transparente, las conexiones a páginas web son enrutadas a servidores proxy de forma transparente sin llevar a cabo ninguna configuración en el ordenador del usuario. Normalmente estos servidores proxy interceptan el tráfico dirigido al puerto 80.

8.10.3 PROXY ARP

Proxy ARP es una técnica en la cual un dispositivo de red, normalmente un router, responde a peticiones ARP dirigidas a otra máquina. El router se encarga de redirigir los paquetes de datos al destino real. Esta técnica se utiliza para acceder a ordenadores de otras subredes sin configurar router o puerta de enlace.

Esto se utiliza cuando queremos unir en la misma red lógica (nivel de red) dos dispositivos que se encuentran en diferentes redes físicas.

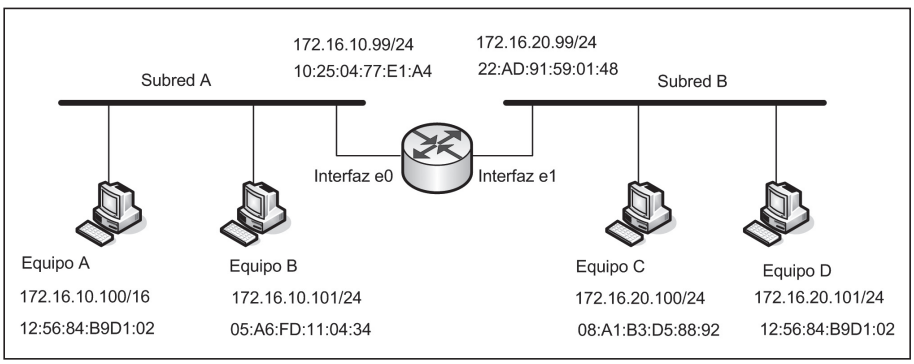


Figura 8.22. *Proxy ARP.*

Queremos enviar datos desde el host A (subred A) al host D (subred B).

Debido a la máscara de subred configurada en A, este host cree tener al host D en su misma subred (172.16.0.0). Por ello, para enviar información a D, el host A enviará una petición ARP para conocer su dirección MAC utilizando la dirección MAC de broadcast FF:FF:FF:FF:FF:FF.

Esta petición no llegará a D, llegará a la interfaz e0 del router (los routers no propagan broadcast). Si el router tiene implementado Proxy ARP, éste responderá a la petición ARP de A con su dirección física. Con lo cual, todos los envíos a D desde el host A se realizarán especificando la dirección MAC del router.

La ventaja de esto es poder añadir host a la subred sin necesidad de conocer información sobre el router.

8.10.4 FIREWALL O CORTAFUEGOS

El concepto de firewall o cortafuegos se aplica a aquellos dispositivos que tienen como parte o la totalidad de sus funciones la de inspeccionar el tráfico intercambiado entre dos redes para que, en función de unas determinadas reglas, permitan o no el traspaso de los datos entre dichas redes.

A este proceso de inspección de paquetes intercambiados entre dos redes para permitir o denegar el propio intercambio se le denomina generalmente **filtrado**. La función de filtrado se puede implementar tanto en software como en hardware. Sea como fuere, los dispositivos donde se encuentre implementada la función de cortafuegos debe poder llevar a cabo funciones de encaminamiento, es decir, un firewall se comporta como un router que une redes pero llevando a cabo un filtrado de la información que se transfiere entre ambas.

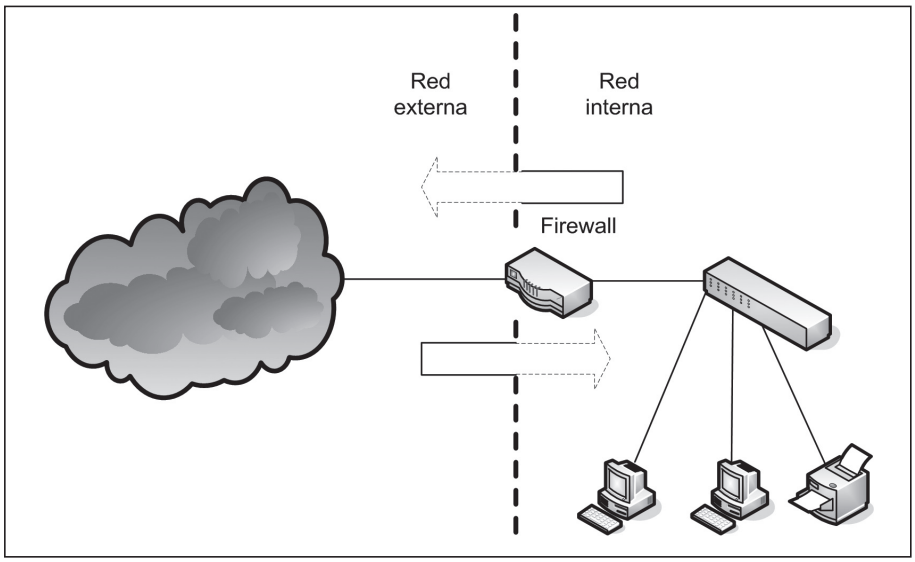


Figura 8.23. *Firewall.*

De hecho, aunque existen en el mercado dispositivos hardware comercializados específicamente como firewall, muchos modelos de routers llevan implementada la función de firewall.

El uso de un firewall implementado por software requiere su uso en un equipo que disponga de dos tarjetas de red y que permita el encaminamiento de tráfico entre dichas tarjetas.

El uso más frecuente de un firewall es filtrar el tráfico de entrada de una red pública (normalmente Internet) hacia una red privada, con objeto de evitar accesos no autorizados a la red privada. Lógicamente, para que el nivel de seguridad que proporciona un firewall sea efectivo, todo el tráfico de entrada debe pasar por el firewall. También puede llevar a cabo el filtrado de información que viaja desde la red privada a la pública.

Las reglas que se utilizan para decidir qué información proveniente de la red exterior puede entrar en la red privada son definidas por un administrador y suelen estar basadas en la información contenida en los niveles 3 ó 4. Ejemplo típicos son el filtrado por puertos, por direcciones IP o por tipo de protocolo.

En alguna de la literatura sobre redes se considera un servidor proxy como un firewall de nivel de aplicación, ya que se realiza un función similar a la de los firewall pero utilizando como criterios de filtrado la información intercambiada en el nivel de aplicación.

En la siguiente figura, se indica una posible configuración de un firewall utilizando lo que se conoce como **DMZ o zona desmilitarizada**. En la DMZ se sitúan equipos que proporcionan servicios a través de la red externa y que, por tanto, no deben ser filtrados, como servidores web, servidores de correo, etc.

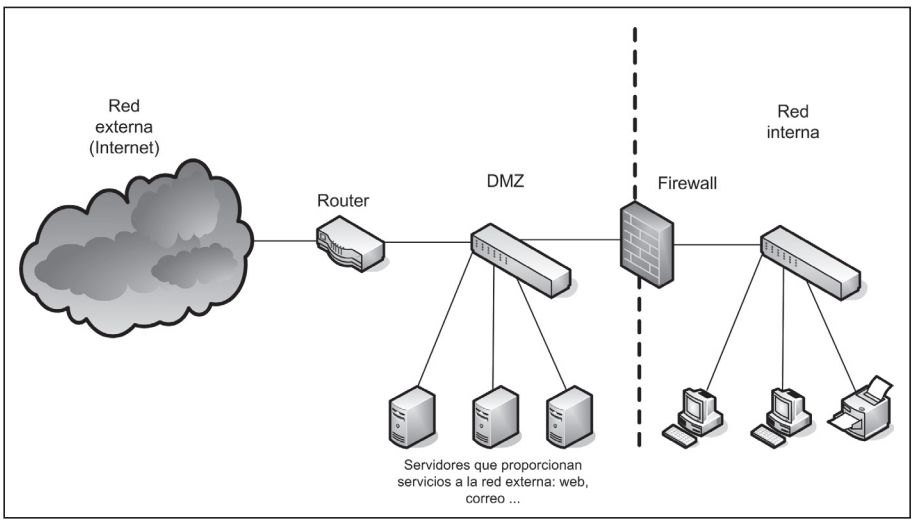


Figura 8.24. *Uso de un firewall con DMZ.*

8.10.5 IPSEC

Conjunto de protocolos implementados para proporcionar seguridad a las comunicaciones a través de redes IP. Inicialmente IPsec fue diseñado para IPv6 pero debido a las fuertes necesidades de seguridad actuales se ha adaptado para poder utilizarlo sobre IPv4.

IPsec proporciona servicios de seguridad incluyendo control de acceso, integridad en las comunicaciones sin conexión, autenticación del origen de los datos, protección contra ataques de repetición, confidencialidad mediante encriptado… Estos servicios son proporcionados en el nivel IP (nivel 3) y ofrece protección para éste y los niveles superiores.

Para ofrecer tales servicios, IPsec utiliza dos protocolos de seguridad, **AH (Authentication Header)** y **ESP (Encapsulating Security Payload)** además del uso de protocolos y procedimientos de administración de claves criptográficas. El protocolo de administración automática de claves por defecto es **IKE (Internet Key Exchange)**. IKE es usado para establecer una política de seguridad compartida y claves autenticadas para servicios que los requieran (como IPsec). Antes del envío de tráfico IPsec, cada router/firewall/host debe ser capaz de verificar la identidad de su par.

El conjunto de protocolos de seguridad utilizados y la forma en que son empleados estará determinado por requerimientos del sistema y de seguridad de los usuarios y aplicaciones.

Los mecanismos utilizados por IPsec están diseñados para ser independientes de los algoritmos empleados. Esta modularidad permite la selección de diferentes conjuntos de algoritmos sin afectar al resto del sistema.

El protocolo AH proporciona autenticación, integridad y antirreproducción para todo el paquete. AH firma el paquete entero pero no cifra la información, por lo que no proporciona confidencialidad. La información es legible, pero está protegida contra modificaciones. Utiliza algoritmos *hash* con claves que se denominan **HMAC** (**Códigos hash de autenticación de mensajes**), para firmar el paquete.

El protocolo ESP proporciona confidencialidad (además de autenticación, integridad y antirreproducción) para la carga *IP*. No firma, normalmente, el paquete entero (a no ser que se esté realizando un túnel), ya que sólo protege la información, y no el encabezado *IP*. Puede utilizarse por sí solo o en combinación con *AH*.

Existen dos modos de utilización de IPsec:

- **Modo túnel,** se utiliza para comunicaciones red a red, red a host o host a host a través de Internet. El encabezado IP interno (encapsulado) es encriptado ocultando la identidad del destinatario y el origen del tráfico.
- **Modo transporte,** utilizado para comunicaciones de extremo a extremo, es decir, de host a host. Sólo se cifran los datos. La cabecera no va encriptada pero sí puede ir firmada por lo que no se puede modificar.

Todo el proceso de encapsulación, encaminamiento y desencapsulación se denomina túnel.

8.10.6 TÚNELES

Un túnel es un canal virtual, configurado entre dos sistemas remotos que se encuentran en diferentes redes, sobre una conexión real que involucra más de un nodo intermedio.

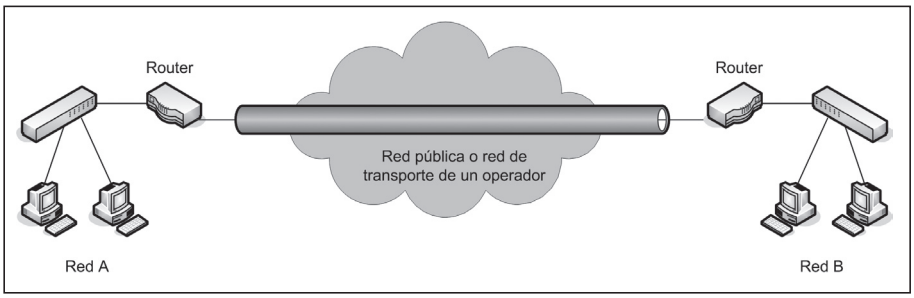


Figura 8.25. *Concepto de túnel.*

La técnica de "tunneling" consiste en encapsular un mensaje de un protocolo dentro de sí mismo aprovechando ciertas propiedades del paquete externo con el objetivo de que el mensaje sea tratado de forma diferente a como habría sido tratado sin la aplicación de esta técnica. Además, el paquete encapsulado es encriptado por el emisor, de acuerdo con el receptor (el sistema que se encuentra en el otro lado del túnel), de manera que sólo ambos extremos pueden acceder a los datos transportados.

De esta forma, el túnel es simplemente una ruta que toman los paquetes encapsulados (y encriptados), dentro de un paquete del mismo protocolo, entre las dos redes. Si un posible atacante intercepta los mensajes que viajan por el túnel no podrá acceder a la información ya que ésta estará encriptada.

Gracias a esto, una organización puede usar de forma segura una red pública para interconectar sus sedes.

Para utilizar un túnel es necesario disponer de un protocolo que lo implemente. Las características más importantes que deben incorporar los protocolos que soporten "tunneling" es el encriptado de datos, autenticación, autorización e integridad de los datos.

8.10.7 PROTOCOLOS DE TUNNELING

Dos de los protocolos más importantes, que surgieron en 1996, son el **Point-to-Point Tunneling Protocolo (PPTP)** desarrollado por Microsoft y el **Layer Two**

Forwarding (L2F) desarrollado por Cisco. La principal diferencia que existe entre ellos es que aplican túneles en diferentes niveles: los túneles PPTP encapsulan paquetes PPP en IP (nivel 3) y L2F utiliza protocolos de nivel 2, como Frame Relay y ATM, para crear los túneles.

A partir de estos protocolos ha surgido un tercero, que utiliza las características de los dos anteriores: **Layer Two Tunneling Protocol (L2TP)**.

L2TP encapsula los paquetes originales dentro de una trama *PPP*, los comprime cuando es posible y, después, los encapsula dentro de un paquete de tipo *UDP* asignado al puerto 1701. Puesto que el paquete con formato *UDP* es un paquete *IP*, *L2TP* utiliza el modo de transporte *IPSec* para asegurar el túnel, basándose en la configuración de seguridad establecida en la configuración del usuario para el túnel *L2TP*. De forma predeterminada, *IKE* negocia la seguridad para el túnel *L2TP* mediante la autenticación basada en certificados (que utiliza certificados de equipo, no de usuario, para comprobar que los equipos de origen y de destino confían el uno en el otro) y mediante autenticación por claves compartidas previamente. Este tipo de autenticación no se recomienda porque es un método relativamente débil.

Debido a ello se suelen utilizar L2TP para crear el túnel y los protocolos de IPsec para proteger la información que viaja por el túnel. La creación de túneles VPN con esta técnica se conoce como **L2TP/IPsec**.

8.10.8 VPN

Una **VPN (Virtual Private Network, Red privada virtual)** consiste en un conjunto de sistemas o dispositivos interconectados a través de canales seguros, sobre una red pública, permitiendo el acceso remoto de los recursos y servicios de la red de forma transparente y segura como si los usuarios estuvieran conectados de forma local. Por tanto, el uso de VPN es una alternativa sobre el acceso remoto tradicional y las líneas dedicadas.

De esta forma se puede aprovechar la conectividad que ofrece una red pública (por ejemplo, Internet) o una red privada de un operador para proporcionar conectividad de forma segura.

En este esquema de comunicación, un usuario remoto solicita un recurso autenticado de la red (privada) de la organización y crea una conexión lógica al servidor VPN. Éste autentica al cliente y efectúa operaciones de encriptado y encapsulación sobre las transmisiones entre el cliente y los recursos de la red. La conexión al servidor VPN utiliza un protocolo que soporte "tunneling" que permite a la empresa u organización extender su red mediante canales privados encriptados sobre la red pública.

Las redes privadas son implementadas en routers (generalmente como parte de una solución firewall), ya que un dispositivo de VPN opera a nivel de red, a través de conexiones seguras utilizando encapsulación, encriptado y autenticación. De

esta forma se transportan de forma segura datagramas IP estableciendo túneles en ambos puntos de la conexión que negocian un esquema de encriptado y autenticación previo al transporte.

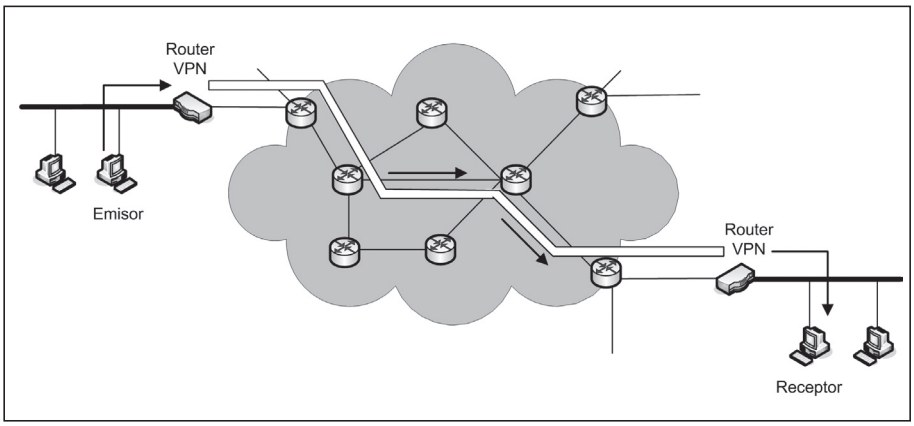


Figura 8.26. *VPN.*

Existe una consideración muy importante para hacer posible el uso global de las VPN y es la necesidad de estandarización. Es deseable que cualquier sistema de conexión o firewall sea capaz de establecer una red privada con cualquier otro en cualquier parte del mundo. El estándar que se ha impuesto actualmente es el propuesto en la arquitectura TCP/IP llamado IPsec. Este protocolo se puede utilizar bajo IPv4 de forma opcional pero en IPv6 es obligatorio su uso.

8.11 PROTOCOLO IPV6

IPv6, que originalmente se llamó **IPng (IP Next Generation)**, fue desarrollado por la IETF (Internet Engineering Task Force) en 1994 sobre todo para solventar uno de los principales problemas que aparecieron en la IPv4, que es la falta de direcciones IP. Esta cuestión queda resuelta en IPv6 al utilizar direcciones de 128 bits, lo que supone que existirán 2^{128} (algo así como 600.000 billones de direcciones por mm^2 de la superficie de la tierra), un número prácticamente inagotable.

Las principales mejoras introducidas en IPv6 respecto a IPv4 son:

- ✓ **Espacio de direcciones ampliado.** Como ya se ha mencionado, IPv6 utiliza direcciones de 128 *bits* (supone un incremento del espacio de direcciones por un factor de 2^{96}).
- ✓ **Mecanismo de opciones mejorado.** Las opciones de IPv6 se encuentran en cabeceras separadas opcionales situadas entre la cabecera IPv6 y la cabecera de la capa de transporte. La mayoría de estas cabeceras opcionales no

se examinan ni procesan por ningún dispositivo de encaminamiento en la trayectoria del paquete. Esto simplifica y acelera el procesamiento que realiza un dispositivo de encaminamiento sobre los datagramas IPv6 en comparación a los datagramas IPv4, y hace que sea más fácil incorporar opciones adicionales.

- ✓ **Direcciones de autoconfiguración.** Esta capacidad proporciona una asignación dinámica de direcciones IPv6, siendo por tanto innecesario el uso de DHCP.
- ✓ **Aumento de la flexibilidad en el direccionamiento.** IPv6 incluye el concepto de una dirección monodistribución o envío a uno (anycast), mediante la cual un paquete se entrega solamente a un nodo seleccionado entre un conjunto de nodos.
- ✓ **Facilidad para la asignación de recursos.** IPv6 habilita el etiquetado de los paquetes como pertenecientes a un flujo de tráfico particular para el cual el emisor solicita un tratamiento especial. Esto ayuda al tratamiento del tráfico especializado, como puede ser el video o la voz en tiempo real.
- ✓ **Capacidades de seguridad.** IPv6 incluye características que permiten la autenticación y la privacidad.
- ✓ **Eliminación de control de errores de cabecera.**
- ✓ **Fragmentación sólo en la fuente.**

8.11.1 ESTRUCTURA DE LA TRAMA IPV6

La unidad de datos del protocolo IPv6 también llamada datagrama tiene la siguiente estructura general:

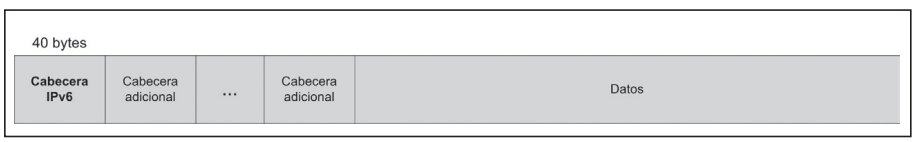


Figura 8.27. *Estructura de datagrama IPv6.*

Como se observa IPv6 utiliza una cabecera principal con la información imprescindible para el encaminamiento de los datagramas, y el resto de información se incluye de forma opcional en cabeceras secundarias, que pueden o no enviarse. Esta característica facilita el procesamiento de los datagramas en los routers permitiendo incluso implementar los mecanismos de encaminamiento por hardware (como los switches) en lugar de por software, que es como se realiza con IPv4, lo que provoca una mejora significativa en las prestaciones de los routers.

La única cabecera obligatoria es conocida como la **cabecera IPv6**. Tiene una longitud fija de 40 bytes, comparados con los 20 bytes de la parte obligatoria de la cabecera IPv4. Sin embargo, la cabecera IPv6 tiene ocho campos, frente a los 13 campos de la cabecera de IPv4, que como se ha indicado facilita su procesamiento en los routers.

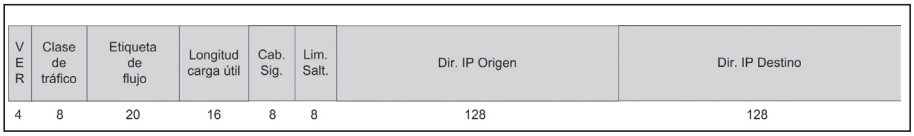


Figura 8.28. *Cabecera principal IPv6.*

En la figura anterior se representa la cabecera fija de IPv6, que consta de los siguientes campos:

- **Versión.** Tiene una longitud de 4 bits. Indica el número de la versión del IP (el valor es 6).
- **Clase de tráfico.** Tiene una longitud de 8 bits. Indica la prioridad. Permite diferenciación de tráfico (por ejemplo, interactivo o flujo) y posibilidad de descarte en caso de congestión.
- **Etiqueta de flujo.** Tiene una longitud de 20 bits. Puede ser utilizado por un nodo para etiquetar aquellos paquetes para los que requiere un tratamiento especial en los dispositivos de encaminamiento dentro de la red.
- **Longitud de la carga útil.** Tiene una longitud de 16 bits. Indica la longitud en bytes del resto del paquete IPv6 excluida la cabecera principal. Representa la longitud total de todas las cabeceras adicionales más la *PDU* de la capa de transporte.
- **Cabecera siguiente.** Tiene una longitud de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera IPv6.
- **Límite de saltos.** Tiene una longitud de 8 bits. Indica el número restante de saltos permitidos para este paquete. El límite de saltos se establece por la fuente a algún valor máximo deseado. Se decrementa en 1 en cada nodo que reenvía el paquete. Es equivalente al campo TTL de IPv4.
- **Dirección origen.** Tiene una longitud de 128 bits (16 bytes). Indica la dirección que identifica al emisor del datagrama.
- **Dirección destino.** Tiene una longitud de 128 bits (16 bytes). Indica la dirección que identifica al receptor del datagrama. Si se utiliza encaminamiento desde el origen, este campo contiene la dirección del siguiente router.

8.11.2 DIRECCIONAMIENTO IPV6

La notación usada para especificar direcciones IPv6 es:

A:B:C:D:E:F:G:H

donde cada letra representa un número de 16 bits. Utilizando la notación hexadecimal (recordar que en IPv4 se utiliza la notación decimal), una dirección tendría el siguiente aspecto:

5401:AB10:F562:1203:C76A:E993:7109:B540

La notación utilizada para las direcciones IPv6 admite dos simplificaciones:

Se pueden eliminar los ceros de mayor peso en cada palabra de 16 bits.

Si una palabra completa tiene el valor 0, se puede eliminar, dejando el carácter ':'. Por ejemplo, la dirección IPv6:

12B7:0000:0000:0000:00BD:0F10:9E72:5FF4

se puede sustituir por:

12B7::::BD:F10:9E72:5FF4

Para proporcionar compatibilidad con el direccionamiento IPv4 se utilizan las dos primeras palabras. Por ejemplo:

80:124:199:36
10100000:

En IPv6 no existe fragmentación de las tramas.

8.11.3 CABECERAS ADICIONALES EN IPV6

En la nueva versión, ciertas informaciones complementarias se codifican en cabeceras que deben colocarse en el paquete entre la cabecera IPv6 y la cabecera del nivel de transporte. Hay un pequeño número de extensiones a la cabecera IPv6 (cada una de ellas identificada por un valor *Próxima cabecera* distinto). Un paquete IPv6 puede contener ninguna, una o varias cabeceras suplementarias.

Salvo excepciones, las cabeceras suplementarias apenas son examinadas o manipuladas por los nodos alcanzados por el paquete a lo largo de su camino hasta que éste llega al nodo (o a cada grupo de nodos en el caso del multicast) identificados por el campo dirección de destino de la cabecera IPv6. En este momento se trata la primera cabecera suplementaria, o la cabecera de transporte en el caso de no haber cabeceras suplementarias. El contenido de cada cabecera determinará si es necesario tratar la cabecera siguiente.

La única excepción es la cabecera nodo por nodo (Hop-by-Hop), que lleva información que deberá ser examinada por los nodos de la red. Cuando está presente, tiene que seguir inmediatamente a la cabecera IPv6.

Cada cabecera suplementaria es de una longitud de un múltiplo de ocho octetos, para conservar una alineación de 8 bytes en las cabeceras suplementarias.

Cuando hay más de una cabecera suplementaria en un mismo paquete, las cabeceras deben aparecer en el orden siguiente:

- **1.** Cabecera *IPv6* (**IPv6 Header**).
- **2.** Cabecera nodo por nodo (**Hop-by-Hop Header**).
- **3.** Cabecera de encaminamiento (**Routing Header**).
- **4.** Cabecera de fragmentación (**Fragment Header**).
- **5.** Cabecera de autentificación (**Authentication Header**).
- **6.** Cabecera de confidencialidad (**Privacy Header**).
- **7.** Cabecera de extremo a extremo (**End-to-End Header**).

Cada tipo de cabecera debe aparecer una sola vez en el paquete (excepto en el caso de un encapsulado IPv6 en IPv6, donde cada cabecera IPv6 encapsulada debe estar seguida por su propia cabecera suplementaria).

8.12 PRÁCTICA

8.12.1 MATERIAL NECESARIO

- ✓ 1 PC con conexión a Internet
- ✓ 1 Software Ethereal

8.12.2 COMANDOS TCP/IP

Indicar cómo obtener la siguiente información a través de los comandos TCP/IP. Incluir en la memoria de la práctica el resultado de su ejecución en el PC del aula.

1 Obtener la dirección IP y comprobar la conectividad con los equipos:
www.rediris.es
www.nasa.gov
www.theaustralian.news.com.au

¿En cuál de los equipos hay menos retardo en la comunicación?

2 Obtener todas las direcciones IP de los routers por los que se pasa para llegar hasta los equipos anteriores. ¿Hay alguna relación entre los tiempos obtenidos por el comando ping y el número de saltos necesarios para alcanzar dichos equipos?

3 Ejecutar el comando ping sobre dos de los equipos del aula. Visualizar el contenido de la tabla ARP y justificar el resultado.

4. Obtener la dirección física o dirección MAC del PC del aula.
5. Enmascarar la dirección MAC de un equipo y comprobar qué dirección MAC se almacena en la tabla ARP de otro equipo de la red.
6. Obtener la tabla de encaminamiento del PC
7. Abrir con el navegador una página web. Comprobar cuántas conexiones TCP se establecen.
8. Obtener la lista de puertos TCP y UDP abiertos en el PC del aula. Obtener información sobre el uso de cuatro de ellos.

8.12.3 PROTOCOLOS ICMP. ESTUDIO DE TRAMAS CON ETHEREAL

1. Desactivar el modo promiscuo y capturar con Ethereal los paquetes enviados a través de la red al ejecutar el comando:

```
ping –n 1 dirección_IP
```

donde dirección_IP es la dirección IP de un PC del aula que esté conectado en la red.

- ✓ ¿Qué tipos de mensajes ICMP aparecen?
- ✓ Comprobar y justificar la procedencia de cada dirección IP y MAC.
- ✓ ¿Cuántos bytes tiene un paquete ICMP? ¿Cuántos son datos y cuántos son cabeceras?
- ✓ Incluir captura de pantalla del programa Ethereal donde aparezcan los paquetes capturados.

2. Ejecutar el comando:

```
ping –n 1 –l 2000 dirección_IP
```

- ✓ Comprobar cuántas tramas Ethernet se generan para el paquete ICMP generado para el comando ping anterior. Justificar la respuesta. Incluir captura de pantalla del programa Ethereal donde aparezcan los paquetes capturados.
- ✓ Identificar los campos involucrados en la fragmentación y la longitud de cada fragmento.

8.12.4 ESTUDIO DE UNA TRANSFERENCIA HTTP

Estudiar la comunicación (tipos de tramas, protocolos utilizados) entre un cliente y un servidor HTTP.

1. Identificar los paquetes DNS utilizados para obtener la dirección IP del nombre solicitado. Localizar el campo dentro de la respuesta DNS donde se incluye la dirección IP de dicho nombre.

2. Identificar los paquetes TCP que sirven para establecer y finalizar una conexión TCP.
3. Identificar las tramas que incluyen los datos de la página web solicitada.

8.12.5 PROTOCOLO NETBIOS SOBRE TCP/IP

NetBIOS es un protocolo utilizado en los sistemas Windows para la compartición de ficheros e impresoras.

NetBIOS utiliza nombres para identificar los equipos en una red. Sin embargo, como NetBIOS se utiliza sobre TCP/IP hay que convertir las direcciones NetBIOS a direcciones IP. Para ello se sigue la siguiente secuencia de resolución de nombres NetBIOS:

1. Se comprueba la **Caché NetBIOS**, que es una tabla dinámica almacenada en memoria y que contiene los nombres de los PC a los que se ha accedido anteriormente. Para visualizar la caché de nombres NetBIOS ejecutar el comando **nbtstat –c.**
2. Si no está en la tabla se hace un **Broadcasting** para obtener la dirección IP de un equipo identificado por su nombre NetBIOS, es decir, se envían mensajes de broadcast. Comando para obtener estadísticas de los nombres resueltos por difusión: **nbtstat –r.**
3. La anterior secuencia es el método estándar aunque existe la posibilidad de utilizar el **archivo LMHOSTS** que contiene una lista de direcciones IP y sus correspondientes nombres NetBIOS.

   Este fichero se crea manualmente con el siguiente formato:

```
Formato de archivo LMHOSTS
# Ejemplo de archivo LMHOSTS
192.168.0.1   router   #PRE
192.168.0.5   minerva  #PRE
192.168.0.6   saturno  #PRE
```

   La ruta donde se debe almacenar el fichero LMHOSTS en Windows XP es:

   \WINDOWS\SYSTEM32\DRIVERS\ETC

   Para que se tomen los cambios en el fichero, es necesario ejecutar el comando **nbtstat –R.**

4. Por último, existe la posibilidad de ejecutar en la red un **servidor WINS**. Dicho servidor se encarga de resolver las peticiones de direcciones IP para nombres NetBIOS.

   Resolver las siguientes cuestiones:

- ✓ NetBIOS utiliza los puertos 137, 138 y 139. Comprobar que estos puertos están abiertos con el comando netstat.
- ✓ Analizar con el software Ethereal los paquetes intercambiados en el acceso a un recurso compartido con NetBIOS. ¿Qué puertos se utilizan?
- ✓ Desactivar los puertos NetBIOS. Para ello desactivar la opción **Netbios sobre TCP/IP** dentro de: Propiedades de la Conexión de área local, Protocolo Internet (TCP/IP), Propiedades, Opciones avanzadas, WINS.
- ✓ Intentar el acceso a los recursos compartidos en el PC donde se ha deshabilitado NetBIOS sobre TCP/IP. ¿Qué ocurre? ¿Qué puertos se utilizan? Buscar información sobre esta funcionalidad.

RESUMEN DEL CAPÍTULO

En este capítulo se ha hecho un amplio repaso de las principales características de la arquitectura TCP/IP. Después de ver el modelo en niveles y la evolución de TCP/IP se revisan todos los protocolos involucrados en la arquitectura.

En el nivel 3 se estudia el protocolo IP y todas sus características incluido el direccionamiento CIDR. Después se repasan el resto de protocolo ARP, RARP e ICMP. Se estudian los protocolos del nivel de transporte TCP y UDP.

Se dedica un apartado para estudiar el comportamiento y características de los routers, para continuar con otro apartado donde se hace un repaso de los principales servicios del nivel de aplicación.

Por último, se muestran los principales mecanismos aplicados sobre redes TCP/IP y que se utilizan ampliamente en la actualidad. Muchos de ellos han debido su desarrollo para ofrecer seguridad a las redes.

EJERCICIOS PROPUESTOS

1. Indicar la clase y la dirección de red de las siguientes direcciones IP:
- **a)** 203.56.125.12
- **b)** 238.56.112.78
- **c)** 109.235.1.90
- **d)** 129.157.221.2
- **e)** 191.1.23.44

2. ¿Cuál es el máximo número de subredes en una red de clase A utilizando las siguientes máscaras?
- **a)** 255.192.0.0
- **b)** 255.255.128.0
- **c)** 255.255.255.0
- **d)** 255.255.248.0

3. ¿Cuál es el máximo número de subredes en una red de clase B utilizando las siguientes máscaras?
- **a)** 255.255.255.0
- **b)** 255.255.252.0
- **c)** 255.255.255.128
- **d)** 255.255.192.0

4. ¿Cuál es el máximo número de subredes en una red de clase C utilizando las siguientes máscaras?
- **a)** 255.255.255.248
- **b)** 255.255.255.192
- **c)** 255.255.255.252
- **d)** 255.255.255.224

5. Indicar la dirección de subred de cada una de las siguientes direcciones IP:
- **a)** IP: 121.63.120.56
  Máscara: 255.255.0.0
- **b)** IP: 98.231.126.198
  Máscara: 255.255.128.0
- **c)** IP: 168.50.121.5
  Máscara: 255.255.224.0
- **d)** IP: 180.4.30.101
  Máscara: 255.255.192.0
- **e)** IP: 205.78.44.153
  Máscara: 255.255.255.240

6. Establecer el direccionamiento para obtener seis subredes a partir del rango 193.105.10.0/24.

Tabla 8.13

Dir. subred	Rango direcciones	Máscara	Dir. broadcast

7. A partir del esquema de la figura se desea configurar tres subredes. La subred 1 formada por los equipos PC01, PC02 y PC03. La subred 2 formada por los equipos PC04 y PC06. La subred 3 formada por los equipos PC05 y PC07. La capacidad máxima de cada subred debe ser de 60 equipos.

Dirección de red: 204.34.56.0/24

a) Especificar la configuración de red (dirección IP, máscara y puerta de enlace) de todos los PC, así como las direcciones IP y máscaras de las interfaces de red de los routers.

b) ¿Los datagramas enviados de PC06 a PC07 serán procesados por el router R02? Justificar la respuesta.

c) ¿Los datagramas enviados de PC04 a PC06 serán procesados por el router R02? Justificar la respuesta.

d) Para pasar el equipo PC03 a la subred 2, ¿sería necesario algún cambio en la configuración física de la red? Justifica la respuesta.

e) Para pasar el equipo 5 a la subred 2, ¿sería necesario algún cambio en la configuración física de la red? Justifica la respuesta.

8. Un ISP dispone de los siguientes rangos de direcciones IP sin asignar:

181.55.0.0 / 17

181.60.64.0 / 19

El ISP recibe las siguientes peticiones de cinco clientes:

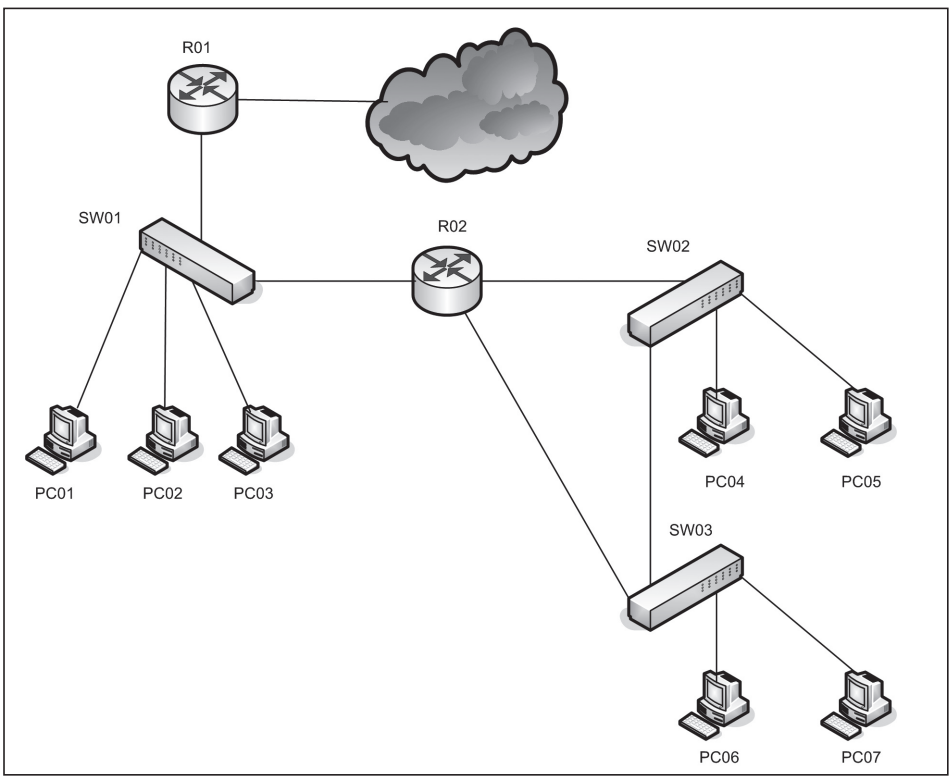


Figura 8.29. *Esquema de ejercicio 7.*

Cliente 1: 200
Cliente 2: 5000
Cliente 3: 800
Cliente 4: 6000
Cliente 5: 10000

- ✓ ¿Dispone el ISP de direcciones suficientes para las peticiones de los clientes? Justificar la respuesta.
- ✓ Realizar la asignación de los correspondientes bloques de direcciones a los clientes optimizando el uso de las mismas para que se utilicen las mínimas posibles. Utilizar formato CIDR.

9. Se dispone del siguiente rango de direcciones 132.50.32.0/19. Se desea crear siete subredes e interconectarlas a través de cuatro routers siguiendo el siguiente esquema:

- ✓ R1: conectado a la subred 1 (556 equipos) y a la subred 2 (41 equipos).
- ✓ R2: conectado a la subred 3 (220 equipos) y a la subred 4 (311 equipos).
- ✓ R3: conectado a la subred 5 (60 equipos).
- ✓ R4: conectado a la subred 6 (55 equipos) y a la subred 7 (46 equipos).
- ✓ Todos los routers están conectados a R4.

a) Dibujar el esquema de la red.
b) ¿Cuántas direcciones IP se necesitan dentro del bloque CIDR?
c) ¿De qué orden debe ser el rango CIDR necesario para albergar las direcciones IP para todas las subredes?
d) Establecer los rangos CIDR de las siete subredes.

TEST DE CONOCIMIENTOS

1 El modelo de niveles de la arquitectura TCP/IP:
- **a)** Es prácticamente igual al modelo OSI.
- **b)** Sólo están definidos los niveles de red y de transporte.
- **c)** No se hace distinción entre los niveles físico y de enlace.
- **d)** Las funcionalidades del nivel de sesión se incluyen en el nivel de red.

2 IP es un protocolo:
- **a)** Orientado a conexión.
- **b)** Basado en datagramas.
- **c)** Del nivel de transporte.
- **d)** Todas las respuestas anteriores son correctas.

3 Una de las principales funciones de IP:
- **a)** Llevar a cabo el control de flujo de la comunicación.

b) Evitar las congestiones en las redes.
c) Identificar errores en la transmisión.
d) Proporcionar un direccionamiento lógico.

4 Una dirección de difusión (broadcast) en IP:
a) Tiene todos los bits a 1.
b) Tiene a 1 todos los bits que identifican la red.
c) Tiene a 1 todos los bits que identifican los equipos en una red.
d) No existe la dirección de difusión en IP sólo en Ethernet.

5 Una petición ARP (ARP Request) se envía:
a) Cada vez que se solicita el envío de un datagrama IP.
b) Si la dirección IP no se encuentra en la tabla ARP.
c) Si la dirección IP está fuera de la red.
d) Si lo solicita el usuario con un comando ping.

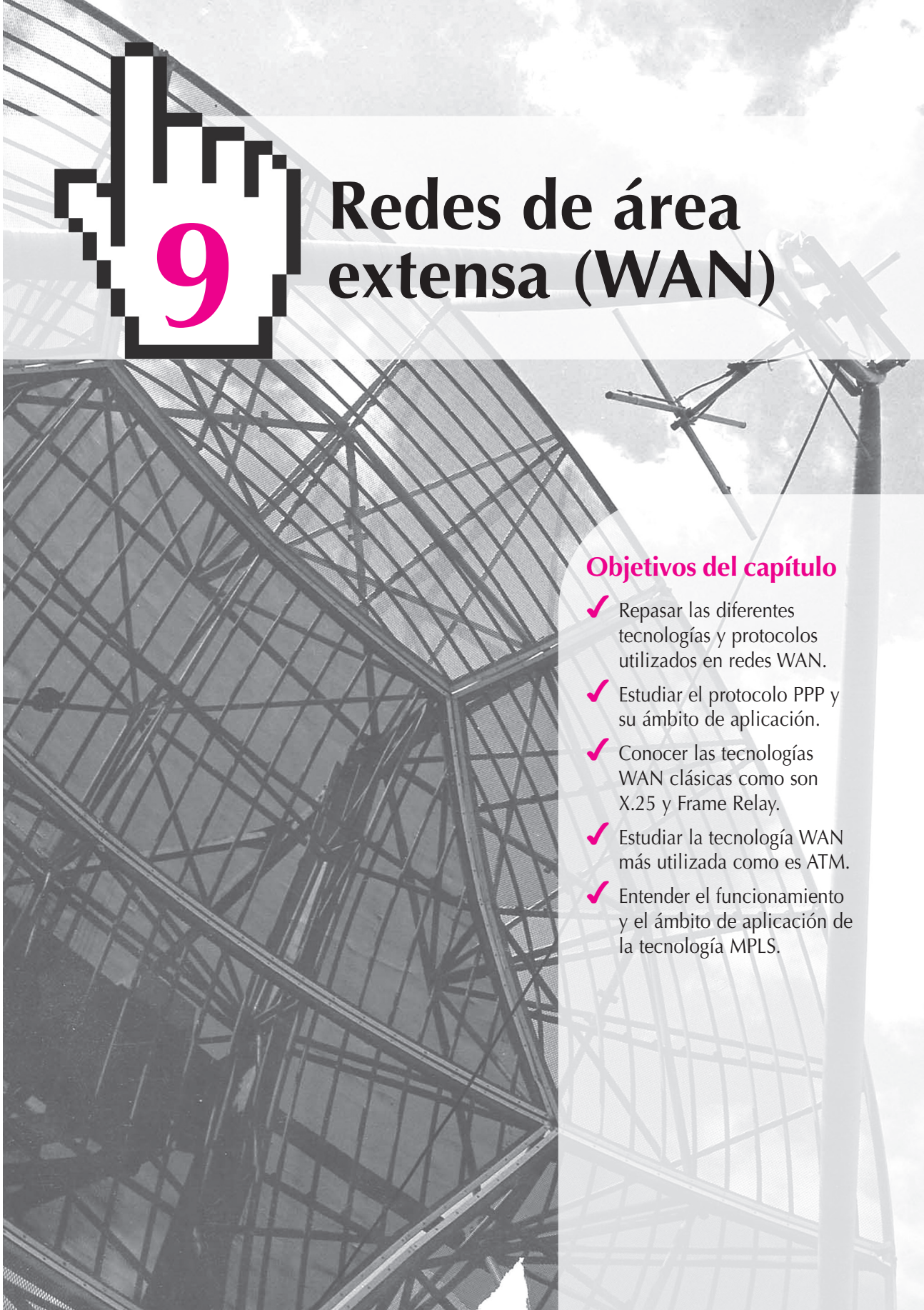
6 De las cinco clases de direcciones IP definidas se utilizan para asignación a redes:
a) Todas las clases.
b) Sólo las clases A, B y C.
c) Sólo las clases A, B, C y D.
d) Sólo las clases A y B. La clase C es sólo para subredes.

7 El enmascaramiento se utiliza:
a) Sólo en redes que utilicen subredes.
b) Sólo en redes de clase C.
c) Tanto en redes con subredes como en redes sin subredes.
d) Sólo en los routers.

8 Con el uso del direccionamiento CIDR:
a) Se soluciona el problema de la falta de direcciones IP.
b) Se optimiza la asignación de direcciones IP.
c) No se pueden implementar subredes.
d) Se necesitan direcciones de 64 bits.

9 Un rango CIDR /21 contiene:
a) Un rango de clase C.
b) Cuatro rangos de clase C.
c) Ocho rangos de clase C.
d) Un rango de clase B.

10 Los paquetes de respuesta ARP (ARP Reply):
a) Se envían siempre a la dirección MAC de la puerta de enlace.
b) Se envían a la dirección de broadcast.
c) Se envían encapsulados en un datagrama IP.
d) Se envían encapsulados en una trama Ethernet.



9 Redes de área extensa (WAN)

Objetivos del capítulo

- ✓ Repasar las diferentes tecnologías y protocolos utilizados en redes WAN.
- ✓ Estudiar el protocolo PPP y su ámbito de aplicación.
- ✓ Conocer las tecnologías WAN clásicas como son X.25 y Frame Relay.
- ✓ Estudiar la tecnología WAN más utilizada como es ATM.
- ✓ Entender el funcionamiento y el ámbito de aplicación de la tecnología MPLS.

9.1 INTRODUCCIÓN

Una red WAN es una red de comunicaciones que permite la comunicación de dispositivos sin límite de distancia. Para ello, generalmente se hace uso de los servicios e infraestructuras de comunicaciones proporcionados por los operadores de telecomunicación.

Las tecnologías WAN pueden funcionar en los tres primeros niveles del modelo OSI. Sin embargo, en la actualidad, las tecnologías más empleadas cubren hasta el nivel 2.

La conectividad entre equipos en una red WAN se puede proporcionar de varias formas:

- ✓ **Circuitos punto a punto.** Establecen un enlace dedicado entre dos equipos que forman parte de una red WAN. Los circuitos punto a punto normalmente los proporcionan los operadores de telecomunicaciones. Son líneas alquiladas cuyo precio normalmente es función del ancho de banda y de la distancia entre los dos puntos que se conectan.

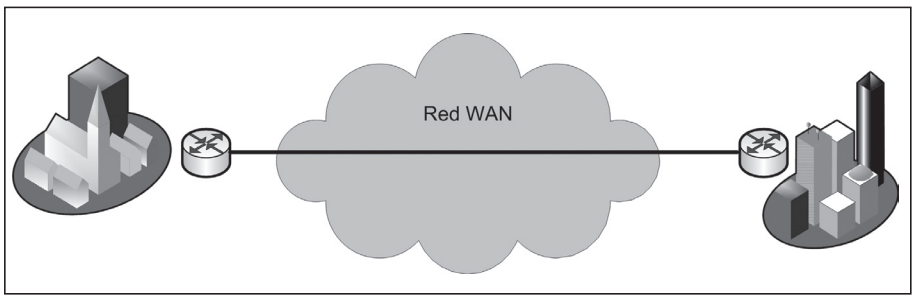


Figura 9.1. *Esquema de una conexión punto a punto.*

- ✓ **Circuitos conmutados.** Proporciona un enlace entre dos dispositivos a través de una conexión a una red de conmutación de circuitos, por ejemplo la red telefónica (RTB o RDSI).

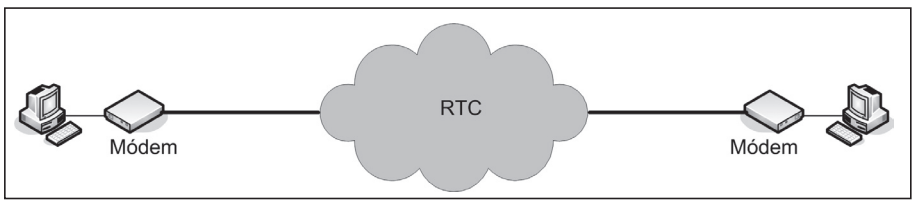


Figura 9.2. *Esquema de una conexión a través de la red telefónica.*

- ✓ **Conmutación de paquetes.** Proporciona un enlace entre dos equipos a través de la red de conmutación de paquetes de un operador de telecomunicaciones. Éste es un método que optimiza los costes respecto a los circui-

tos punto a punto, proporcionando además una alta calidad de servicio. Ejemplo: X.25, Frame Relay y ATM, y SMDS.

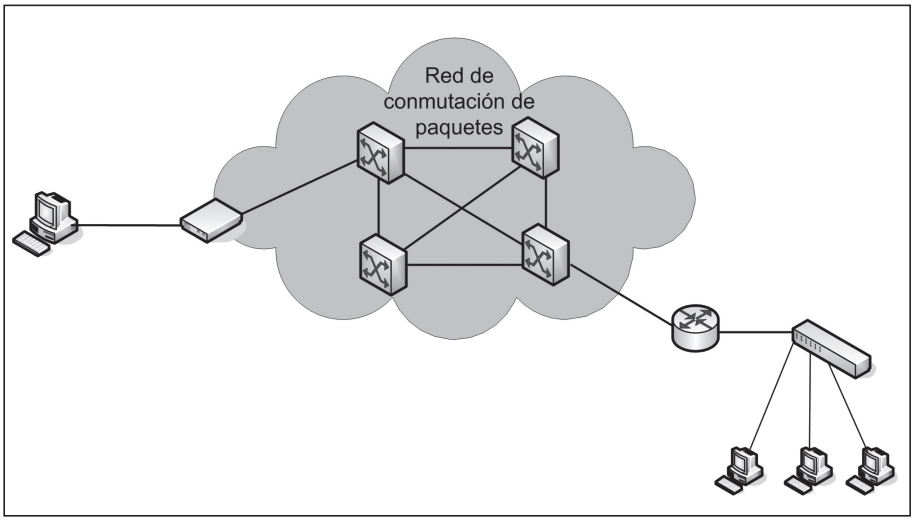


Figura 9.3. *Conexión a través de una red de conmutación de paquetes.*

Los principales dispositivos utilizados para el acceso a una red WAN son:

- **Switch WAN.** Son utilizados en los operadores para acceder a su red. Normalmente se puede conectar un router a estos switches.
- **Servidor de acceso.** Actúa como concentrador para conexiones de marcado. Es el punto de acceso típico que proporcionan los ISP.
- **Módem.** Utilizado para enlaces WAN punto a punto que utilizan líneas analógicas. Actualmente están en desuso.
- **CSU/DSU (Channel Service Unit/Digital Service Unit)** dispositivo usado normalmente para conectar un router a una línea digital, por ejemplo, una E1/T1.

9.2 PPP

El protocolo **PPP (Point-To-Point Protocol, Protocolo punto a punto)** se diseñó inicialmente para transportar tráfico IP sobre un enlace punto a punto. Es un estándar para transmitir datagramas a través de un enlace punto a punto. Actualmente admite otros protocolos de red como IPX, AppleTalk, DECnet...

Algunas de las características que ofrece PPP son:

- **Notificación de la dirección de red.** Esto permite a un servidor de acceso telefónico notificar a un cliente su dirección de red (típicamente IP) para esa sesión de conexión.
- **Autentificación.** Existen dos métodos de autentificación soportados en el protocolo PPP, PAP y CHAP. Esta característica permite la validación de un cliente mediante un nombre de usuario y contraseña.
- **Multiplexación de protocolos.** El protocolo PPP permite la utilización de varios protocolos de red simultáneamente en un enlace.
- **Monitorización del enlace.** Se incluyen funciones que permiten comprobar periódicamente el funcionamiento del enlace.

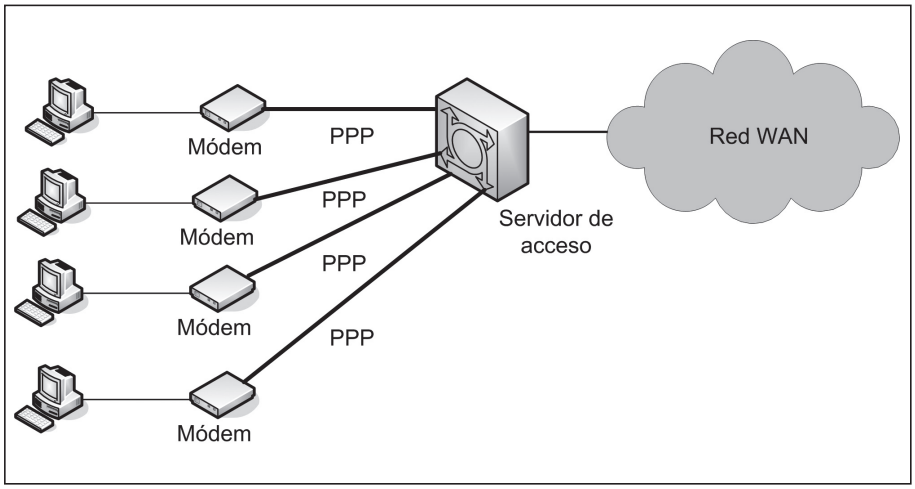


Figura 9.4. *Conexión PPP.*

La mayor parte de los ISP utilizan este protocolo para dar acceso a sus clientes a Internet utilizando líneas analógicas. También se han desarrollado variantes para utilizar PPP sobre líneas ADSL:

- ✓ PPPoE (PPP over Ethernet)
- ✓ PPPoA (PPP over ATM)

NOTA 9.1

PPP se utiliza para la transmisión de datagramas a través de un enlace punto a punto. Muy utilizado como nivel de enlace en las conexiones a Internet a través de un ISP utilizando líneas telefónicas.

9.2.1 NIVELES EN PPP

PPP se puede considerar un protocolo del nivel de enlace que está basado en el protocolo HDLC con la diferencia de que PPP está basado en carácter y no en bits como HDLC. Las funciones que proporciona HDLC están divididas en dos subniveles:

- **LCP (Link Control Protocol)** proporciona los mecanismos necesarios para establecer, configurar, mantener y terminar la conexión.
- **NCP (Network Control Protocol)** permite establecer y configurar diferentes protocolos del nivel de red.

Nivel físico

PPP es capaz de operar en cualquier interfaz DTE/DCE. Por ejemplo, puede utilizar interfaz EIA-232-C, EIA-442, EIA-423 o V.35. La única condición que se debe cumplir es que sea una línea full-dúplex (conmutada o dedicada) que puede operar tanto en modo síncrono como asíncrono.

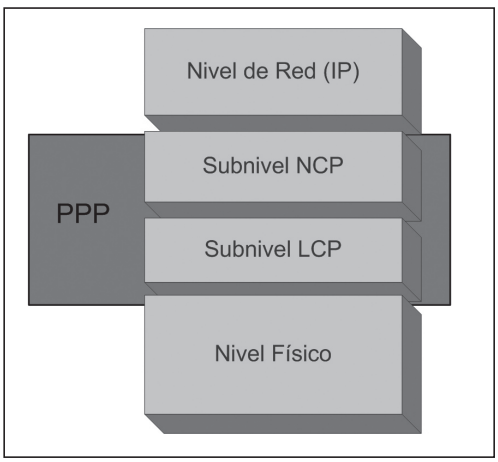


Figura 9.5. *Niveles en PPP.*

9.2.2 FORMATO DE TRAMAS

Como una de las funciones típicas de un protocolo del nivel de enlace, PPP lleva a cabo el tramado de la información a enviar. La estructura de la trama PPP es la siguiente:

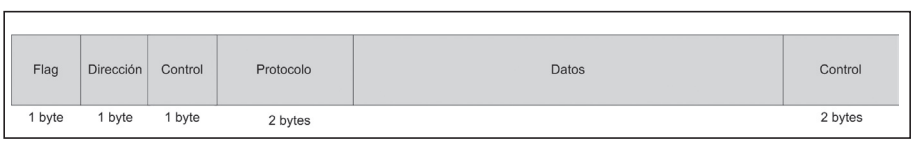


Figura 9.6. *Formato de la trama PPP.*

- **Flag (Preámbulo).** Indica el comienzo de la trama. Es un byte con el valor fijo: 01111110.
- **Dirección.** (1 byte). El protocolo PPP no utiliza direcciones por lo que este campo contiene siempre un valor fijo: 11111111.
- **Control.** (1 byte). También con un valor fijo: 00000011.
- **Protocolo.** (2 bytes). Este campo identifica el protocolo encapsulado en la trama PPP.
- **Datos.** El tamaño máximo es de 1.500 bytes. Aunque puede ser mayor si se negocia.
- **FCS (Frame Check Sequence).** El tamaño por defecto es de 2 bytes aunque puede ser de 4 bytes si se negocia. Al igual que en HDLC, este campo se utiliza para llevar a cabo el control de errores.

9.2.3 MODO DE OPERACIÓN

Para establecer una comunicación a través de un enlace punto a punto mediante PPP se siguen los siguientes pasos:

1. El equipo que genera la comunicación envía tramas LCP para configurar y establecer el enlace de datos.
2. Opcionalmente se lleva a cabo la obtención de los niveles de calidad del enlace.
3. Después de establecerse la comunicación se envían tramas NCP para elegir y configurar los protocolos de red que se van a utilizar.
4. El enlace ya está establecido y se podrán enviar datos a través del mismo hasta que se envíe alguna trama LCP o NCP para cerrar la conexión.

9.2.4 AUTENTIFICACIÓN

En PPP se puede llevar a cabo dos tipos de autentificación: **PAP (Protocol Authentication Protocol)** y **CHAP (Challenge Handshake Authentication Protocol).**

PAP proporciona un método sencillo de que un nodo remoto establezca su identidad. Se utiliza un método de autentificación llamado de dos vías. Después de completarse la negociación LCP, el originador de la llamada envía el par usuario/contraseña. El servidor de acceso comprueba entonces la identidad del usuario enviando una aceptación o un rechazo. Si el usuario no es reconocido se cierra la conexión.

PAP no es un método de autentificación robusto ya que el envío de la contraseña a través del enlace se hace sin ningún cifrado. Tampoco hay protección ante ataques repetidos de prueba y error.

CHAP es un protocolo de autentificación de tipo desafío mutuo que utiliza un establecimiento de la conexión de tres vías. Este proceso se lleva a cabo en tres pasos. Primero, el autentificador manda un mensaje de "desafío" al usuario generado de forma aleatoria. El usuario responde con un valor calculado a partir del desafío y de su contraseña de acceso. Este valor se calcula utilizando una función hash basada normalmente en el algoritmo MD5. El autentificador verifica la respuesta realizando el cálculo y verificando que el resultado es el mismo.

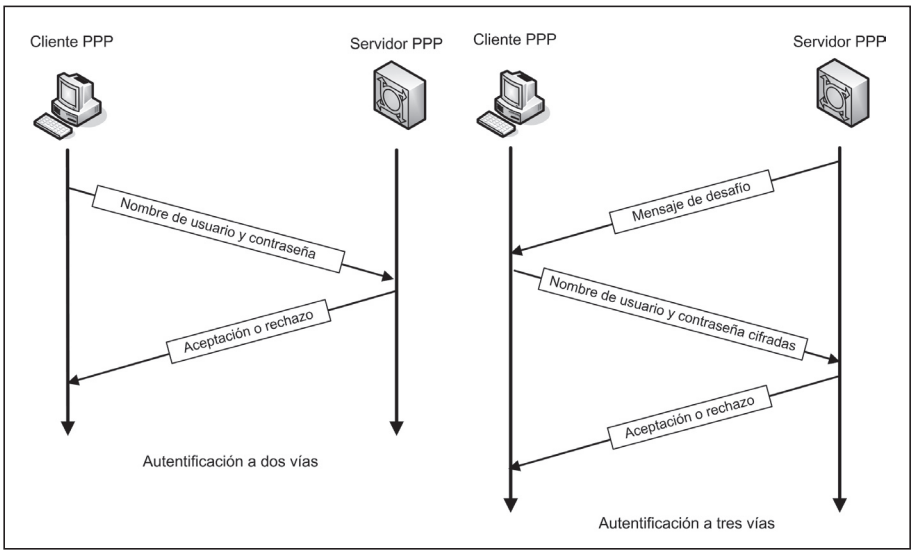


Figura 9.7. *Autentificación PAP de dos vías y CHAP de tres vías.*

Otra característica importante de CHAP es que la verificación de la identidad utilizando el método anterior no sólo se hace en el establecimiento de la conexión sino que se repite de forma periódica. El desafío enviado por el autentificador es un valor aleatorio por lo que el valor calculado por la función hash en el usuario será diferente cada vez. Esta característica proporciona protección frente a ataques de prueba y error.

Debido a la mayor protección que ofrece CHAP, es el método de autentificación más utilizado en PPP.

9.3 X.25

9.3.1 CARACTERÍSTICAS PRINCIPALES

X.25 es un protocolo de acceso a redes públicas de conmutación de paquetes desarrollado por el ITU-T. Su primera especificación se publicó en 1976, aunque ha habido varias revisiones posteriores. Se puede considerar, por tanto, el primer

protocolo de tecnología WAN que, además, ha sido utilizado de forma muy amplia en los años 80 y principios de los 90.

El protocolo X.25 define la interfaz entre un equipo de datos y una red de conmutación de paquetes, es decir, define la comunicación entre un DTE y un DCE. Es importante destacar que X.25 no define la comunicación interna en la red pública, que se lleva a cabo utilizando los llamados nodos de conmutación de paquetes o simplemente nodos de red.

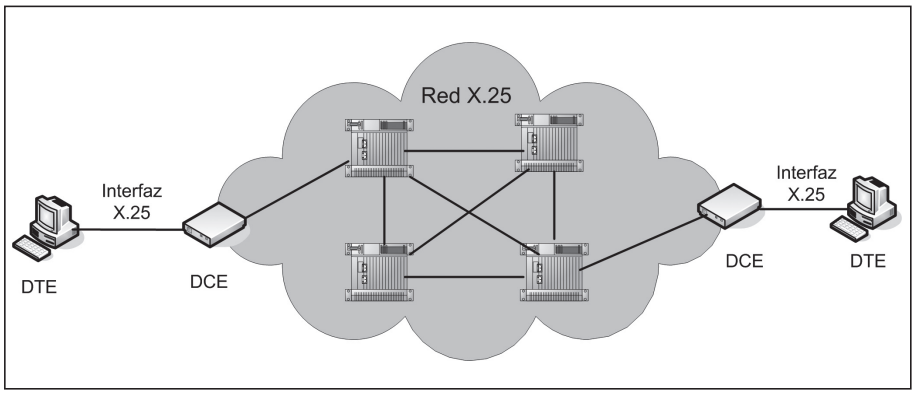


Figura 9.8. *Conexión a través de X.25.*

Las principales características de X.25 son:

- Es un protocolo orientado a conexión, por lo tanto, se definen los mecanismos para establecer, mantener y finalizar las conexiones.
- Utiliza conmutación de paquetes mediante circuitos virtuales. Antes de establecerse una comunicación, se reserva un camino lógico para los datos a través de los circuitos virtuales. Cuando la conexión finaliza, el circuito virtual se libera.
- Se utiliza TDM (Multiplexación por división en el tiempo) asíncrona para multiplexar los datos. Un DTE puede establecer hasta 4.095 circuitos virtuales full-dúplex con otros DTE sobre el mismo enlace físico DTE-DCE.
- El protocolo X.25 proporciona un alto grado de fiabilidad. Además, las redes públicas a las que da acceso suelen tener una arquitectura redundante y con una gran capacidad de supervisión para añadir fiabilidad adicional a las transmisiones.
- Es una alternativa a un circuito dedicado punto a punto que es mucho más caro y cuyo coste depende de la distancia entre los nodos. X.25 utiliza la red de conmutación de un operador por lo que el coste es menor y no depende de la distancia entre los puntos que se quieren conectar.

✓ Los servicios de datos basados en redes X.25 han ofrecido tradicionalmente varias tasas de datos hasta un máximo de 64 Kbps. Durante los años en los que estuvo en auge X.25, esta velocidad máxima cubría los requisitos de la mayor parte de clientes. Actualmente se puede considerar insuficiente en muchos casos.

X.25 ofrece un alto nivel de fiabilidad en las comunicaciones ya que, cuando se diseñó, el soporte físico en el que se debían implementar las redes basadas en X.25 (básicamente la red analógica del servicio telefónico) era de baja calidad con un índice alto de errores. Sin embargo, la paulatina mejora de las infraestructuras de comunicaciones propiciada principalmente por la utilización de líneas digitales y fibra óptica hace innecesario el robusto mecanismo de control de flujo y de errores de X.25, que por otra parte impide alcanzar las velocidades de transmisión de datos demandados en la actualidad.

En los años 90, con la aparición de la tecnología Frame Relay, cuyo estudio se abordará en el próximo apartado, las redes X.25 comenzaron su declive. Frame Relay es también una tecnología basa en la conmutación de paquetes pero aprovecha las características de las modernas infraestructuras de comunicación.

En la actualidad, la velocidad máxima de conexión a una red X.25 puede llegar a 2 Mbps aunque queda muy lejos de las velocidades alcanzadas por ATM con una velocidad típica de 622 Mbps. Aunque muchas de las redes X.25 continúan operativas, su uso ha quedado restringido sólo a algunos tipos de aplicaciones que requieren una alta fiabilidad pero no necesitan un gran ancho de banda.

En España, Telefónica es el operador que provee el uso de redes X.25 con el servicio denominado **IBERPAC** que comenzó su funcionamiento en 1985. Los principales clientes del servicio IBERPAC son las entidades bancarias.

9.3.2 NIVELES EN X.25

Se definen tres niveles: nivel físico, nivel de trama (enlace), nivel de paquetes (red).

Nivel físico

El protocolo que especifica el nivel físico de X.25 es X.21 o X.21bis. Está basado en el estándar EIA-232 (V.24 en ITU-T) con el cual es compatible.

Nivel de trama

Ofrece control de enlace de datos utilizando un protocolo orientado a bit denominado **LAPB (Link Access Protocol Balanced, Protocolo balanceado de acceso al enlace)**, que está basado en HDLC. De hecho, el formato de la trama es igual que en HDLC, con sus campos Delimitador, Dirección, Control, FCS. También existen tres categorías de tramas:

- **Tramas I** utilizadas para datos del nivel de paquetes (red).
- **Tramas S** utilizadas para control de errores y flujo en el nivel de trama.
- **Tramas U** utilizadas para establecer y desconectar enlaces entre un DTE y un DCE.

La comunicación entre un DTE y un DCE en el nivel de trama se lleva a cabo en tres fases:

- ✓ Establecimiento del enlace utilizando tramas U.
- ✓ Transferencia de datos utilizando tramas I para los datos y tramas S para el control de flujo y errores.
- ✓ Desconexión del enlace, utilizando tramas U.

El control de flujo que se lleva a cabo en el nivel de trama de X.25 es prácticamente igual que el de HDLC. Se utiliza la técnica de ventana deslizante vuelta atrás con ARQ. Por defecto utiliza números de secuencia de 3 bits (módulo 8) pero permite el empleo de 7 ó 15 bits para los números de secuencia (módulo 128 o 32.768).

Nivel de paquetes

El protocolo que implementa el nivel de paquetes (nivel de red) se denomina **PLP (protocolo de nivel de paquetes)**. Este nivel es responsable del establecimiento, transferencia de datos y finalización de la conexión entre dos DTE, es decir, se encarga de la conexión de extremo a extremo. Este nivel también se encarga de crear los circuitos virtuales.

NOTA 9.2

Importante: el nivel de paquetes en X.25, a pesar de considerarse nivel 3, no incluye algoritmos de encaminamiento.

Un circuito virtual es el circuito o canal lógico que se establece para llevar a cabo la comunicación entre dos DTE. Los circuitos virtuales se crean en el nivel de paquetes en X.25. Cada circuito virtual se identifica mediante el denominado **LCN (Logical Channel Number, Número de canal lógico)**. En la comunicación entre dos DTE se definen dos LCN, uno define el circuito virtual entre el DCE y el DTE locales y el otro define el circuito virtual entre el DCE y DTE remotos. Existen dos tipos de circuitos virtuales:

- **SVC: circuitos virtuales conmutados.** Se establece la conexión, se asignan los números de canales lógicos, se lleva a cabo la transferencia de datos y se realiza la desconexión, liberándose los números de canales lógicos utilizados.

- **PVC: circuitos virtuales permanentes.** Los circuitos virtuales se establecen por el proveedor de la red de conmutación de paquetes, por tanto, la asignación de canales lógicos es permanente. Conceptualmente es parecido al alquiler de una línea dedicada. No es necesario establecer ni liberar la conexión para los circuitos virtuales permanentes.

Los números de canales lógicos se envían en la cabecera del paquete PLP con una longitud de 12 bits, por tanto, se permiten hasta 4.096 (realmente 4.095, el 0 está reservado). Existen dos tipos de paquetes de datos en PLP: paquetes de datos y de control; éstos últimos se utilizan para establecer y finalizar las conexiones, ejecutar reinicios y rearranques de conexiones.

Aunque el nivel de paquetes no proporciona algoritmos de encaminamiento, las redes que transportan el tráfico X.25, lógicamente, utilizan algoritmos de encaminamiento para establecer la ruta entre dos DTE. Estos algoritmos no están incluidos en las especificaciones X.25.

9.3.3 OTROS PROTOCOLOS ASOCIADOS A X.25

X.121

Especificación que establece un direccionamiento global para los DTE que se conecten a redes públicas de conmutación de paquetes de tipo X.25. Aunque este protocolo no forma parte de X.25, en la práctica se utiliza en la mayoría de las redes X.25. Es similar al número de abonado de la red telefónica. Es un código de 14 dígitos decimales que se codifica usando BCD, y por lo tanto se usa un octeto para cada dos dígitos. Este código se divide en dos partes:

- **DNIC (Data Network Identification Code, código de identificación de red de datos),** son los cuatro primeros dígitos y definen una red específica. De estos cuatro bits, los tres primeros son el código del país y el cuarto bit define la red del operador. El código de España es el 214.
- **NTN (National Terminal Number, número de terminal nacional),** son los 10 dígitos siguientes y definen los DTE de una red concreta.

X.75

Protocolo para interconectar redes X.25. Utilizado sobre todo para enlaces internacionales de redes X.25

Conexión de terminales en modo carácter a X.25: X.3, X.28 y X.29

Existe la posibilidad de conectar a una red X.25 terminales en modo carácter (también llamados terminales "tontos") en lugar de DTE que funcionan en modo paquete. Para ello se utiliza un dispositivo denominado **PAD (Packet Assembler / Disassembler, Ensamblador / desensamblador de paquetes)**. Para el funcionamiento de este tipo de terminales se han desarrollado tres protocolos:

- **X.3** define las características de los PAD.
- **X.28** define la comunicación entre el terminal y el PAD.
- **X.29** define la comunicación entre un PAD y un terminal remoto (DTE o PAD).

9.4 FRAME RELAY

9.4.1 CARACTERÍSTICAS PRINCIPALES

Frame Relay (también se conoce como **Retransmisión de tramas**) es una tecnología WAN de conmutación de paquetes basada en circuitos virtuales y desarrollada para sustituir a X.25 ya que proporciona velocidades de conexión más altas a un coste menor. La primera especificación de Frame Relay se desarrolló en 1988, aunque fue a comienzos de los años 90 cuando empezó a utilizarse de forma generalizada.

X.25 fue desarrollado para redes de conmutación de paquetes, teniendo en cuenta la baja calidad de los medios de transmisión donde se producía una alta tasa de errores. Esto justificaba los abundantes controles de errores y sus redundantes mecanismos para el control de flujo, junto al pequeño tamaño de los paquetes. Cada trama que se envía se comprueba en cada conmutador por el que pasa hasta el destino final. Por tanto, gran parte del tráfico en X.25 se gasta en comprobación de errores y en asegurar una fiabilidad completa del servicio.

Frame Relay, por el contrario, maximiza la eficacia, aprovechándose para ello de las modernas infraestructuras, de mucha mayor calidad y con muy bajos índices de error, y además permite mayores flujos de información. La comprobación de errores en Frame Relay se lleva a cabo de extremo a extremo y no en cada nodo de conmutación.

Frame Relay opera en el nivel físico y de enlace. Por tanto puede utilizarse como red troncal para ofrecer servicios a protocolos que ya tienen nivel de red, como TCP/IP. Esto no ocurre en X.25 donde se produce una duplicación de las funciones de red entre X.25 y TCP/IP.

Una característica muy interesante de Frame Relay es que soporta el envío de datos a ráfagas. Este tipo de transmisión se ajusta más a la forma en que se transmiten los datos en muchos de los usuarios de redes WAN. Para la utilización de una conexión X.25 o un circuito dedicado punto a punto se debe contratar una velocidad de conexión, que no se puede superar. Mientras que Frame Relay puede soportar picos con envíos superiores a la velocidad contratada. Estos picos de transmisión se conocen como ráfagas.

La velocidad que ofrecen las redes Frame Relay va de 64 Kbps hasta 2.048 Kbps.

Su principal desventaja es que, al permitir tramas de longitud variable, se pueden producir retardos variables e impredecibles. Frame Relay en principio no es adecuado, por ejemplo, para la transmisión de audio y video en tiempo real a menos que la red donde esté implementada Frame Relay esté adecuadamente sobredimensionada para que no se produzcan retardos apreciables.

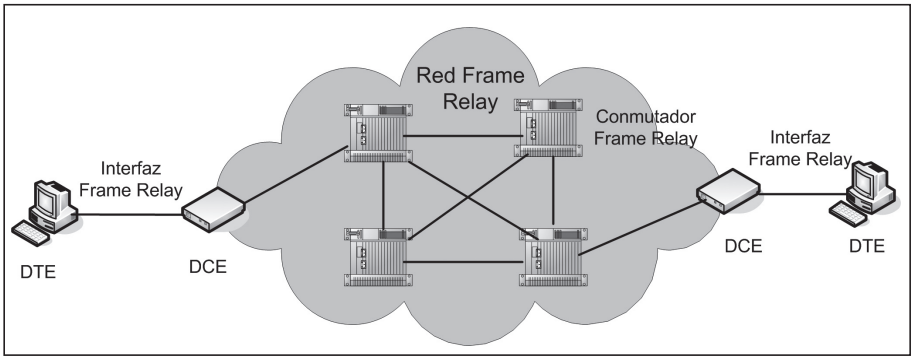


Figura 9.9. *Conexión a través de Frame Relay.*

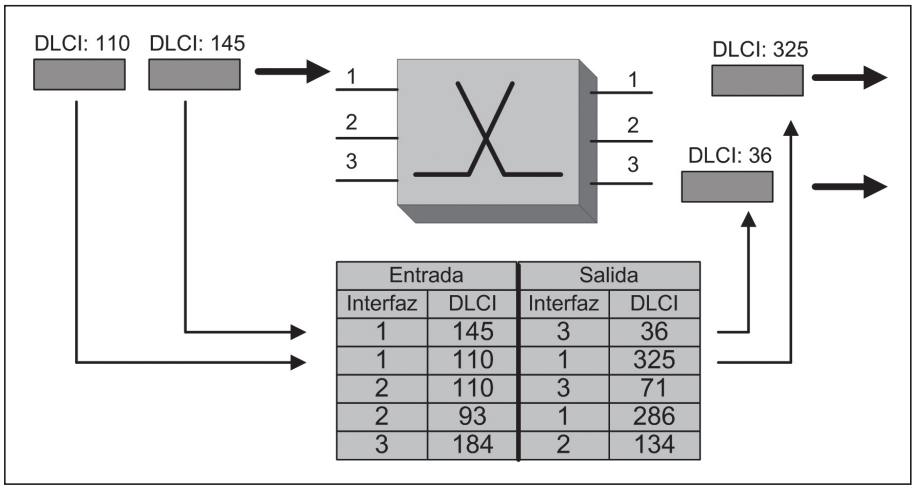
Una red Frame Relay estará formada por conmutadores Frame Relay. Además de dichos conmutadores pueden existir otros dispositivos denominados **FRAD (Frame Relay Assembler / Disassembler)** que se utilizan en una red Frame Relay para adaptar datos que lleguen de otros protocolos WAN (por ejemplo X.25, ATM, PPP).

9.4.2 CIRCUITOS VIRTUALES

Al igual que X.25, Frame Relay es una tecnología orientada a conexión que utiliza circuitos virtuales para establecer las conexiones. La creación de circuitos virtuales se lleva a cabo en el nivel de enlace, a diferencia que en X.25 que se realiza en el nivel de red. El identificador de circuito virtual se denomina **DLCI (Data Link Connection Identifier, Identificador de Conexión de Enlace de Datos)**. Hay dos tipos de conexiones en Frame Relay:

- **PVC: circuito virtual permanente.** Se establece un circuito virtual entre dos DTE a través del proveedor de la red. Se asignan de forma permanente dos DLCI, uno para cada DTE. En las primeras implementaciones de Frame Relay sólo existía esta opción de conexión.
- **SVC: circuito virtual conmutado.** En este caso es necesario establecer una conexión. Para ello, se necesita un protocolo que implemente un nivel de red (por ejemplo IP) o un método de direccionamiento (por ejemplo RDSI). Después de la fase de conexión se establece el circuito virtual asignando los DLCI. Cuando la conexión finaliza, los DLCI se liberan.

Los DLCI no sólo se utilizan para definir circuitos virtuales entre un DTE y un DCE (conmutador) sino que también se utilizan para crear circuitos virtuales entre los conmutadores de la red Frame Relay. Cada conmutador almacena una tabla de encaminamiento de tramas para todos los circuitos virtuales establecidos.



Entrada		Salida	
Interfaz	DLCI	Interfaz	DLCI
1	145	3	36
1	110	1	325
2	110	3	71
2	93	1	286
3	184	2	134

Figura 9.10. *Funcionamiento de conmutadores Frame Relay.*

9.4.3 CONTROL DE LA CONGESTIÓN

La congestión en una red se produce cuando se envían datos a una tasa mayor de la que pueden permitir los recursos de red.

En X.25 se realiza un control de flujo en el nivel de enlace de datos y en el nivel de red. Este doble mecanismo de control de flujo evita la existencia de congestión. Sin embargo en Frame Relay no existe nivel de red ni tampoco control de flujo, y además se permite el envío de datos a ráfagas. Todo ello hace que se pueda producir congestión en una red Frame Relay y por lo tanto se necesita realizar un control de dicha congestión.

El control de la congestión se lleva a cabo por los siguientes métodos:

- ✓ Frame Relay utiliza dos bits de la trama para avisar al origen y al destino de la presencia de congestión. Tanto el emisor como el receptor pueden iniciar mecanismos para reducir el flujo de información intercambiada. El funcionamiento de estos bits se explica en el próximo apartado.
- ✓ Los conmutadores implementan un buffer de datos funcionando como una cola para poder adaptar las velocidades variables de las ráfagas en una velocidad de salida fija, lo cual minimiza el riesgo de congestión debido a las ráfagas.

- ✓ Ante situaciones con congestión se utiliza el mecanismo de descarte de tramas. Existe un bit en la trama utilizado para marcar las tramas descartables.
- ✓ Se llevan a cabo medidas del control de tráfico para determinar cuándo se tienen que activar los bits de congestión en las tramas y cuándo se tienen que descartar tramas.

Se utilizan cuatro atributos diferentes para llevar a cabo el control del tráfico. Estos atributos se fijan en el momento del establecimiento de la conexión. Para conexiones PVC se establecen sólo una vez.

- **Velocidad de acceso.** Esta velocidad de acceso depende del ancho de banda del canal que conecta el usuario con la red. Puede ser un circuito dedicado punto a punto, una línea RDSI o incluso una línea ADSL. Lógicamente la velocidad de acceso será la que marque el límite de acceso a la red Frame Relay.
- **Tamaño de ráfaga comprometido (B_c, Committed Burst Size).** Número máximo de bits durante un período predefinido de tiempo que la red se compromete a transferir sin descartar ninguna trama o marcar las tramas como descartables.
- **Velocidad de información comprometida (CIR, Committed Information Rate).** Parecido al anterior parámetro excepto que se refiere a una velocidad media en bps. Este parámetro se obtiene dividiendo Bc entre el período tomado como referencia.
- **Tamaño de ráfaga en exceso (B_e, Exceed Burst Size).** Número de bits por encima del tamaño de ráfaga comprometido que la red se compromete a enviar si no hay congestión. Las tramas enviadas cuando se supera el tamaño de ráfaga comprometido se marcan como descartables de forma que si se produce congestión en la red, estas tramas podrán ser eliminadas. Este parámetro también se conoce como **EIR (Exceed Information Rate, Tasa de Información excedida)**.

Por tanto, todos los datos enviados a una velocidad inferior a B_c serán enviados a través de la red. Se pueden enviar ráfagas a una velocidad superior siempre que el parámetro CIR no sea superado. Los bits enviados de forma continua a una tasa superior a B_c e inferior a B_e serán enviados a través de la red en tramas marcadas como descartables de forma que si se produce congestión en la red dichas tramas se eliminarán. Todas las tramas que se envíen a una velocidad superior a B_e serán descartadas por el conmutador que las reciba.

Un caso muy común es utilizar una línea E1 para el acceso a una red Frame Relay por lo que la velocidad de acceso a la red será de 2.048 Kbps. Lógicamente ningún parámetro de velocidad (B_e, B_e o CIR) podrá superar la velocidad de acceso de 2.048 Kbps.

9.4.4 NIVEL DE ENLACE EN FRAME RELAY

En Frame Relay se establecen dos tipos de servicios de transmisión (llamados también planos):

- ✓ Los **servicios de control** utilizados para transmitir información de control del enlace. Se utiliza el protocolo **LAPD (Link Access Procedure D Channel, Procedimiento de acceso al enlace al canal D)** especificado para el canal de control D de las líneas RDSI.
- ✓ Los **servicios de datos** de usuario utilizados para transmitir la información del usuario de la red Frame Relay. Se utiliza el llamado protocolo **LAPF (Link Access Procedure for Frame Relay)** basado en el protocolo HDLC aunque con muchas de las funcionalidades de éste último eliminadas ya que Frame Relay no utiliza en los servicios de datos, ni control de flujo ni control de errores.

La trama utilizada en LAPF es la siguiente:

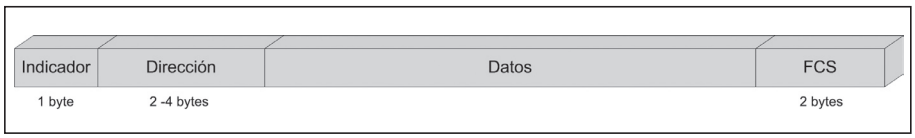


Figura 9.11. *Formato de una trama LAPF.*

El campo de información tiene una longitud variable que está comprendida entre 1 y 8.250 bytes, aunque se utiliza un tamaño típico de 1.600 bytes.

El campo Dirección no sólo contiene la dirección, que en Frame Relay se conoce como DLCI, sino que incluye algunos otros bits de control. Además, existen tres formatos del campo Dirección diferentes que permiten utilizar tres longitudes diferentes para la dirección DLCI.

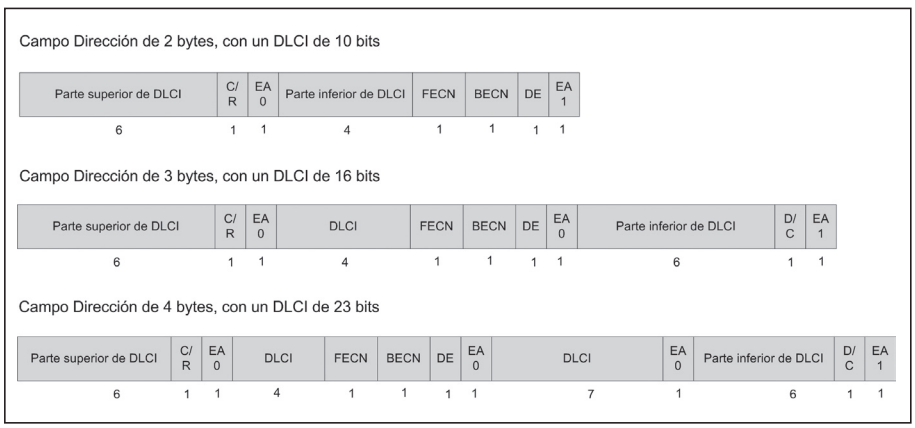


Figura 9.12. *Formatos del campo Dirección en la trama LAPF.*

- **DLCI (Data Link Connection Identifier, Identificador de Conexión de Enlace de Datos).** Identificador de circuito virtual con una longitud por defecto de 10 bits. Aunque, como se observa en la figura anterior, existen otros dos formatos de trama que admiten longitudes de DLCI de 16 y 23 bits. Este valor es único en el ámbito local, es decir, en la conexión entre dos dispositivos Frame Relay.
- **EA (Extended Adress, Dirección extendida).** Cuando el valor de EA es 1 indica que el byte donde se incluye este bit en el campo dirección es el último. Si este bit es un 0 indica que hay más bytes que forman parte del campo dirección.
- **FECN (Forward Explicit Congestion Notification, Notificación de congestión explícita de envío).** Este bit lo activa el conmutador por el que pasa la trama para indicar al destinatario que hay congestión en la red. El destinatario podrá utilizar mecanismos en los niveles superiores a Frame Relay para ralentizar el envío de datos.
- **BECN (Backward Explicit Congestion Notification, Notificación de congestión explícita de envío hacia atrás).** Este bit se utiliza para avisar al emisor de una trama de una situación de congestión en la red. Como la trama no puede volver de nuevo al emisor, existen dos posibles métodos para realizar esto, activar este bit en la respuesta del receptor o utilizar una conexión reservada para este tipo de comunicaciones (en este caso se suele utilizar el DLCI 1023). Cuando el emisor recibe una trama con este bit activo, la acción que se lleva a cabo es reducir la velocidad de transmisión.
- **C/R (Command / Response, Orden / Respuesta).** Originalmente este campo se incluyó para permitir a los niveles superiores distinguir entre una orden enviada por un dispositivo primario, o una respuesta enviada por un dispositivo secundario. No se usa en Frame Relay.
- **DE (Discard Elegibility, Elegible para ser descartada).** Este bit se utiliza para marcar tramas descartables. En caso de la congestión en la red, los conmutadores podrán eliminar de la red las tramas con este bit activo reduciéndose así el flujo de información en la red.

9.4.5 APLICACIONES DE FRAME RELAY

Como ya se indicó al comienzo de la sección, Frame Relay fue originalmente diseñada para sustituir las redes X.25 aprovechando las características de las nuevas infraestructuras de comunicación.

Los servicios basados en la tecnología Frame Relay están especialmente indicados para el intercambio de datos. Una de las principales aplicaciones de dichos servicios ha sido la interconexión de redes de área local. El flujo de información generada en la interconexión de LAN no es uniforme sino que es un flujo de datos a ráfagas. Este tipo de tráfico, como se ha visto, es perfectamente manejado por

Frame Relay, a diferencia de las redes X.25 o los circuitos dedicados punto a punto que funcionan con una tasa de transmisión fija.

Sin embargo y debido a la existencia de tramas de distinto tamaño y por tanto de la existencia de retardos imprevisibles en los conmutadores, las redes Frame Relay no son apropiadas para la transmisión de audio o video que requieren, al menos, un retardo previsible. Sin embargo, en redes Frame Relay convenientemente dimensionadas es posible llevar a cabo el intercambio de audio y video en tiempo real.

En cualquier caso, la aparición de una nueva tecnología, ATM, que admite todo tipo de tráfico y alcanza velocidades de transmisión elevadas ha hecho que Frame Relay actualmente haya quedado relegado a un segundo plano como tecnología utilizada en redes WAN. A pesar del auge de ATM, en España hay varios operadores que ofrecen servicios de datos a través de redes Frame Relay a diferentes velocidades. Normalmente la velocidad más alta de conexión se consigue conectando el usuario con la red Frame Relay del operador a través de un enlace E1, con una tasa de transmisión de 2.048 Kbps (para las líneas T1 americanas, la tasa sería de 1.544 Kbps).

9.5 ATM

ATM (Asynchronous Transfer Mode, Modo de transferencia asíncrona) es una tecnología de conmutación de celdas desarrollada para proporcionar interconexión a alta velocidad para el intercambio de todo tipo de información, tanto datos, como voz y video. Su uso no está restringido a ningún tipo de redes, por ello, esta tecnología se puede utilizar tanto en redes privadas (LAN) como en redes públicas (WAN) aunque en la práctica, se utiliza principalmente en redes WAN, por ello se ha decidido incluir ATM en este capítulo. Inicialmente ATM fue desarrollado por el llamado **ATM Forum**, organismo creado para el desarrollo y la difusión de la tecnología ATM, aunque posteriormente fue adoptado por la ITU-T.

Las celdas ATM son las unidades de información utilizadas para transferir datos. Su principal característica es que tienen un tamaño fijo de 53 bytes, 48 para datos y 5 para cabecera. Las tramas manejadas en redes X.25 y Frame Relay son de tamaño variable lo cual añade complejidad en su tratamiento en los conmutadores, además de añadir retardos impredecibles en su procesamiento. La transmisión de celdas de tamaño fijo proporciona tiempos de procesamiento predecibles y simplifica el procesamiento en los conmutadores.

ATM usa multiplexación asíncrona donde el time slot es una celda. En la multiplexación asíncrona, los canales no tienen reservado ningún time slot dentro de la trama, de esta forma se asegura el aprovechamiento de todo el ancho de banda disponible.

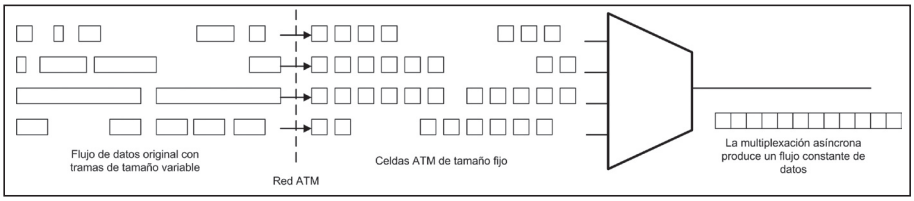


Figura 9.13. *Multiplexación de celdas en ATM.*

Al igual que Frame Relay, ATM apenas implementa mecanismos de control de flujo y control de errores.

9.5.1 ARQUITECTURA ATM

Una red ATM está formada por conmutadores ATM cuya función es encaminar las celdas a través de la red, y por los sistemas finales que generan la información. La interfaz que conecta dos conmutadores ATM se denomina **NNI (Network-to-Network Interface)** mientras que la interfaz que conecta un sistema final con un conmutador ATM se denomina **UNI (User-to-Network Interface)**.

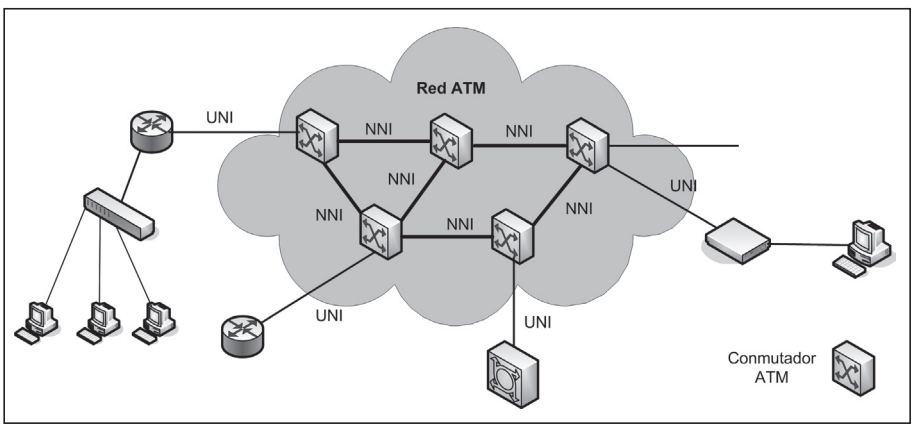


Figura 9.14. *Arquitectura de red ATM.*

Como se observa en la figura, las interfaces UNI conectan un sistema final de la red (como un router) a un switch ATM. Las interfaces NNI conectan dos switches ATM. Todos los enlaces en una red ATM son punto a punto.

ATM es una tecnología orientada a conexión, por lo tanto, antes de llevar a cabo el envío de información es necesario establecer una conexión. Las conexiones en los dispositivos se establecen mediante conexiones lógicas a través de canales virtuales de forma similar a Frame Relay. La capacidad de un canal de transmisión físico entre dos dispositivos ATM se divide en canales lógicos llamados **VC (Virtual circuit, circuito virtual)**. Cada VC es un canal virtual por el que

se envían datos de usuario o datos de gestión de red. Los VC se agrupan con fines de gestión en lo que se conoce como **VP (Virtual Path, Camino Virtual)**. Un VP se forma por la agrupación de VC con los mismos extremos, de manera que todas las celdas transmitidas a través de todas las VC de la misma VP se conmutan conjuntamente.

El hecho de establecer en ATM dos niveles de conexiones lógicas proporciona las siguientes ventajas:

- ✓ Posibilidad de estructurar una red en conexiones de caminos virtuales independiente de la estructura física de soporte.
- ✓ La red debe gestionar menos entidades, dado que los circuitos virtuales dentro de un camino virtual se pueden gestionar de forma conjunta. De hecho, existen conmutadores más sencillo de implementar que sólo encaminan celdas por el VP.
- ✓ El proceso de establecimiento y liberación de las conexiones se reduce. La adición de nuevas conexiones a un camino virtual ya existente no requiere ningún proceso en los nodos intermedios.

Por tanto, una conexión ATM se define cuando se establece una conexión lógica formada por un canal VP y un canal VC. Para ello se utilizan los llamados **VPI (Virtual Path Identifier, Identificador de camino virtual)** y **VCI (Virtual Circuit Identifier, Identificador de circuito virtual)**.

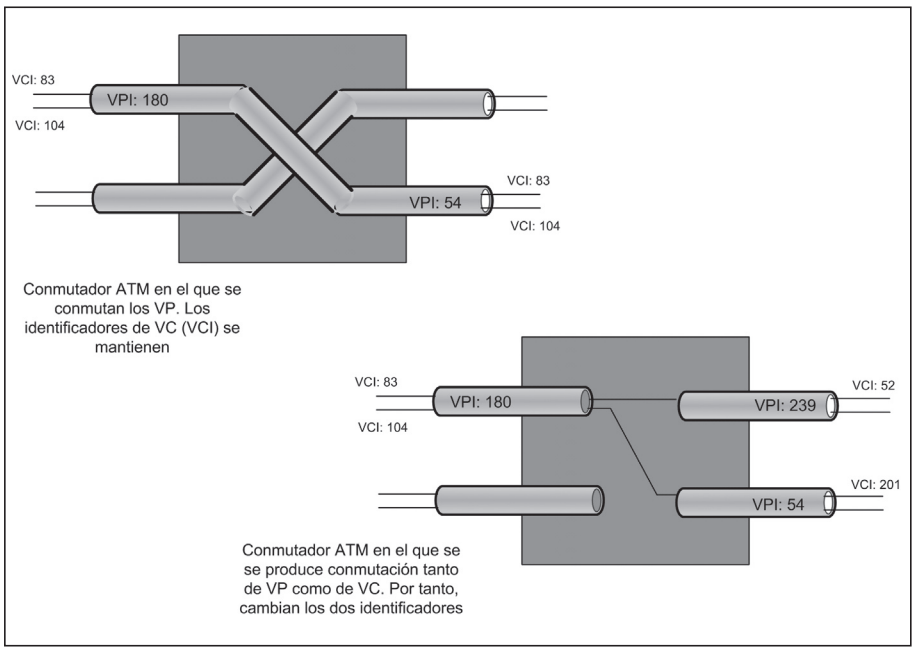


Figura 9.15. *Conexiones lógicas en ATM.*

9.5.2 NIVELES EN ATM

Las funciones ATM se implementan en dos niveles enmarcados en el nivel 2 del modelo OSI.

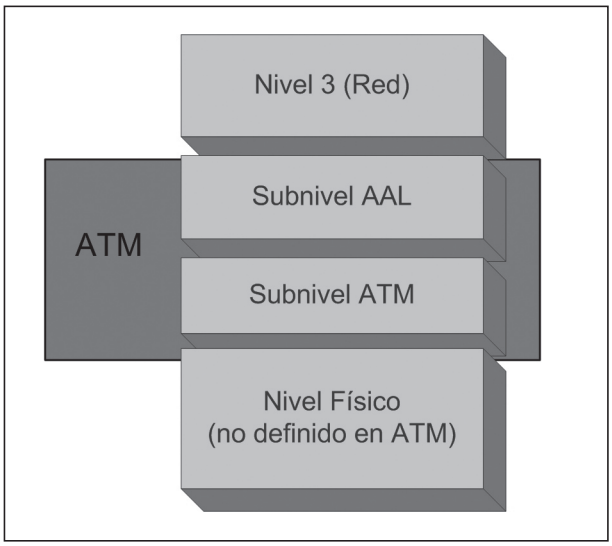


Figura 9.16. *Niveles en ATM.*

Nivel físico

El nivel físico no está especificado en ATM. Los estándares más utilizados son SDH/SONET (DS-3/E-3) sobre fibra multimodo con codificación 8B/10B (155 Mbps) o cable de cobre apantallado STP con codificación 8B/10B a 155 Mbps.

Nivel de enlace

El nivel de enlace se divide en ATM en dos subniveles: el subnivel ATM y subnivel **AAL (ATM Adaptation Layer)**.

El **subnivel ATM** ofrece servicios de encaminamiento, gestión de tráfico, conmutación y multiplexación. Acepta el tráfico proveniente del nivel superior y lo divide en fragmentos de 48 bytes, añade la cabecera de 5 bits y genera la celda ATM.

El **subnivel AAL** permite la conexión de redes con otros protocolos (por ejemplo, IP) a las redes ATM. En este subnivel existen varias categorías, cada una de las cuales se utiliza para adaptar los protocolos de red superiores al subnivel inferior de ATM. Las categorías especificadas son: AAL1, AAL2, AAL3, AAL4 y AAL5.

En la práctica, las categorías AAL3 y AAL4 se han combinado en una única categoría AAL3/4. La categoría AAL2 no se utiliza.

9.5.3 FORMATO DE CELDA ATM

Como ya se ha indicado, una celda ATM consta de una cabecera de 5 bytes y un campo de información de 48 bytes, también conocido como **Payload**. Se especifican dos formatos de celdas, un tipo para la interfaz **UNI** y otro tipo para la interfaz **NNI**. La diferencia radica en la necesidad de que la interfaz UNI disponga del campo GFC. En la figura se representan los formatos de las celdas.

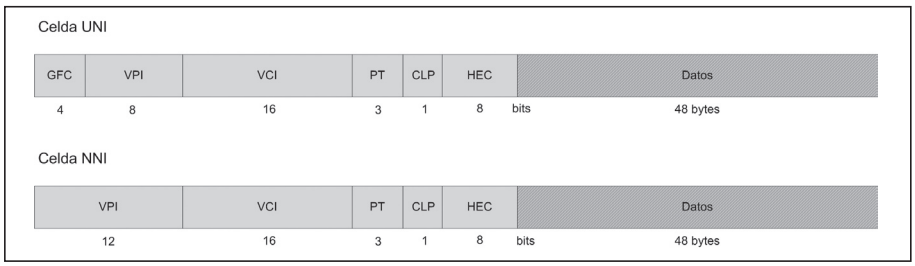


Figura 9.17. *Formato de las cabeceras de las células ATM en la UNI y la NNI.*

Los campos de las celdas *ATM* son los siguientes:

- **GFC (Generic Flow Control, Control de flujo genérico).** Campo presente sólo en las celdas UNI. Consta de 4 bits y se utiliza para establecer un control de flujo de tráfico en la interfaz usuario-red con objeto de solucionar la aparición esporádica de sobrecarga.
- **VCI/VPI.** Estos campos contienen los identificadores de camino virtual y circuito virtual. En la celda UNI, el VPI está formado por 8 bits y el VCI por 16 bits. En la celda NNI, el VPI consta de 12 bits el VCI de 16 bits. Los 4 bits de diferencia se deben al campo GFC de la UNI.
- **PT (Payload Type Identifier, Tipo de carga útil).** Está constituido por 3 bits. Indica el contenido de carga útil (datos de usuario, información de gestión), así como situación de congestión en algún punto de la red.
- **CLP (Cell Loss Priority, Prioridad de Pérdida de Células).** Tiene un bit de longitud. Las células con este bit a 1 son las primeras en ser descartadas en caso de congestión.
- **HEC (Header Error Connection, Control de Error de cabecera).** Consta de 8 bits. Es un campo utilizado para detectar errores en la cabecera. Se emplea un código CRC que permite la corrección de errores simples o detección de errores múltiples.

9.5.4 SERVICIOS PROPORCIONADOS POR ATM

En ATM se han normalizado cinco categorías de servicios que proporcionan diferentes niveles de calidad de servicio. Cada una de ellas garantiza unos deter-

minados parámetros de calidad de servicio y supone la adhesión a unos parámetros de descripción de tráfico. Estas categorías de servicio son las siguientes:

CBR (Constant Bit Rate, Velocidad Binaria Constante)

Esta categoría supone que el usuario final emite datos de forma que el flujo de celdas se hace a una velocidad fija. Es adecuada para tráfico de voz o de video con velocidad constante, que requieren características estrictas de retardo y variación de retardo.

RT-VBR (Real-Time Variable Bit Rate, Velocidad Binaria Variable en Tiempo Real)

Es adecuada para los servicios de datos que requieren características estrictas de retardo y variación de retardo, a velocidad variable, por ejemplo para flujos de video de calidad constante (velocidad variable).

NRT-VBR (Non-Real-Time Variable Bit Rate, Velocidad Binaria Variable en Tiempo no Real)

Es adecuada para aplicaciones muy sensibles a la pérdida de celdas, en general para tráfico transaccional, por ejemplo, las transacciones bancarias.

UBR (Unspecified Bit Rate, Velocidad Binaria No Especificada)

Es equivalente al concepto de "mejor esfuerzo". Esta categoría no garantiza ningún valor respecto a la capacidad, al retardo o a la pérdida de celdas. Conceptualmente, puede asimilarse a la idea de datagrama y se utiliza para correo electrónico, transferencia de ficheros, etc.

ABR (Available Bit Rate, Velocidad Binaria Disponible)

Esta categoría garantiza un valor bajo para las pérdidas de celdas a costa de no proporcionar ninguna garantía respecto a la variación de retardo. En ella, el terminal debe ser capaz de ajustar su tasa de emisión de células por la conexión al ancho de banda disponible en cada momento y que la red notifica como una variable denominada **ACR** (**Allowed Cell Rate**). El mecanismo de gestión de tráfico utilizado es el control de flujo y garantiza una capacidad mínima.

9.5.5 CONTROL DE FLUJO

El **Control de Flujo** (**Flow Control**) comprende el conjunto de mecanismos coordinados que permiten, en función de la carga de la red, que los terminales ATM ajusten sus tasas de emisión de celdas.

El control de flujo se consigue ajustando en origen periódicamente el intervalo temporal de emisión de las celdas de cada conexión. Para ello, el terminal emisor deberá insertar celdas **RM** (**Resource Management**, **Administración de recursos**)

en el flujo de celdas de datos, que serán devueltas por el terminal destino para informar sobre la necesidad de ajustar la emisión de celdas de datos en función del estado de la red.

El control de flujo es un mecanismo de gestión de tráfico que tiene una escala temporal de actuación intermedia, ya que toma decisiones que tardan en tener efecto varios **RTT** (**Round-Trip Time**, **Retardos de ida y vuelta**). Un RTT es el tiempo que tarda una celda RM en llegar al terminal destino de la conexión y volver al terminal emisor.

9.5.6 NIVELES AAL

Dentro del subnivel AAL existe otros dos subniveles: **CS (subnivel de convergencia)**, dependiente del servicio de nivel superior, y **SAR (subnivel de segmentación y ensamblado)**, éste último encargado de empaquetar la información proveniente del subnivel CS. Tanto el subnivel CS como el subnivel SAR pueden añadir una cabecera y una cola. En la siguiente figura se puede observar la encapsulación de los datos en cada subnivel.

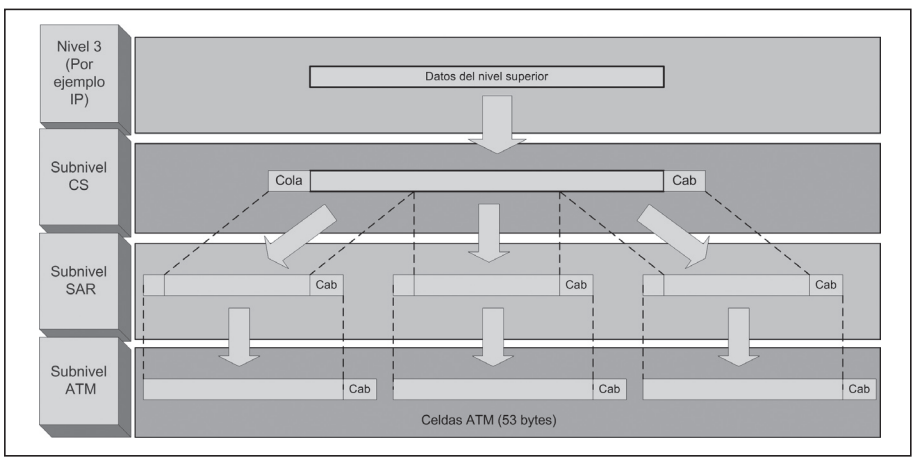


Figura 9.18. *Encapsulación de los datos en los niveles ATM.*

Para poder ofrecer la adecuada adaptación de protocolos y arquitecturas de niveles superiores a ATM existen varios tipos de subniveles AAL.

AAL1

Ofrece un servicio orientado a conexión para el uso de fuentes de datos de velocidad constante (CBR), como tráfico de voz y video. ATM transporta tráfico CBR usando servicios de emulación de circuitos. AAL1 requiere temporizaciones para la sincronización entre la fuente y el destino de los datos, por ello, AAL1 depende del medio utilizado. Por ejemplo, SONET o SDH soportan esta característica.

El subnivel SAR añade una cabecera con dos campos:

- **SN: Número de secuencia,** de 4 bits. Se utiliza para la detección de celdas perdidas o desordenadas y para proporcionar una estructura en tramas de ocho celdas.
- **SNP: Protección del número de secuencia.** Este campo se utiliza para la detección y posible corrección de errores en el número de secuencia. Está formado por 4 bits, 3 bits incluyen un código CRC de comprobación de errores y el bit restante es un indicador de paridad.

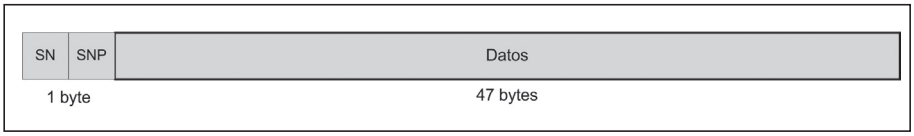


Figura 9.19. *PDU del subnivel SAR en AAL1.*

AAL3/4

Este tipo soporta tanto servicios orientados a conexión como no orientados a conexión. Este nivel fue diseñado para los proveedores de servicios de red y se adapta perfectamente a **SMDS (Switched Multimegabit Data Service)**.

El subnivel SAR añade una cabecera de 16 bits con tres campos en el tipo AAL3/4:

- **ST: Tipo de segmento.** 2 bits. Este identificador indica si el segmento pertenece al comienzo, al medio o al final del mensaje, o por el contrario es un mensaje de un solo segmento.
- **SN: Número de secuencia.** 4 bits. Igual que para AAL1.
- **MID: Identificación de multiplexación.** 10 bits. Este campo identifica las celdas que vienen de flujos de datos diferentes y se multiplexan en la misma conexión virtual.

Añade también una cola de 16 bits con dos campos:

- **LI: Indicador de longitud.** 6 bits. Este campo se utiliza junto con el campo ST para indicar qué parte del último segmento son datos y qué parte es relleno. Por tanto este campo sólo se utiliza cuando es el último segmento de un mensaje.
- **CRC: Código de redundancia cíclica.** 10 bits. Código de comprobación de errores de los datos.

Por tanto, la carga de datos útil en la PDU del subnivel SAR en AAL3/4 es de 44 bytes, que junto con la cabecera de 2 bytes y la cola de 2 bytes forman la unidad de datos de 48 bytes que se pasa al subnivel ATM.

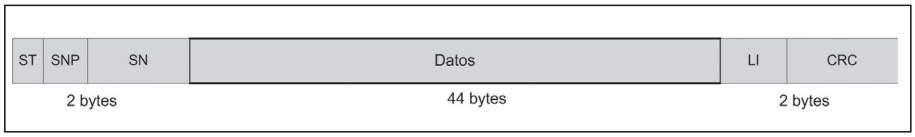


Figura 9.20. *PDU del subnivel SAR en AAL3/4.*

NOTA 9.3

SMDS (Switched Multimegabit Data Service) es un servicio no orientado a conexión usado para conectar redes LAN, MAN o WAN. Actualmente apenas se usa ya que esta función ha sido suplantada por MPLS (ver el próximo apartado).

AAL5

AAL5 es el tipo de subnivel AAL para transferencia de datos y proporciona tanto servicios orientados a conexión como no orientados a conexión. Se usa para la transmisión de datos que no utilicen SMDS, como por ejemplo tráfico IP.

En este caso, el nivel de convergencia (CS) acepta un paquete de datos de no más de 65.535 bytes de un servicio del nivel superior y añade una cola de 8 bytes así como el relleno necesario.

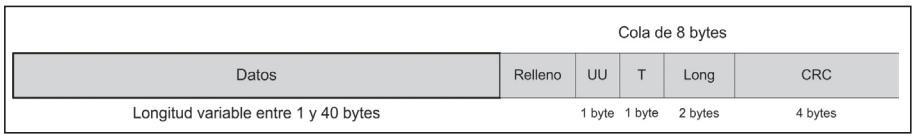


Figura 9.21. *PDU del subnivel CS en AAL5.*

- **PAD: Relleno.** Se añade un relleno de entre 0 y 47 bytes para que el tamaño del PDU resultante sea múltiplo de 48.
- **UU: Identificador usuario-usuario.** 1 byte. Campo reservado para el servicio usuario, por lo tanto no está definido en ATM.
- **T: Tipo.** 1 byte. No está definida su función.
- **L: Longitud.** 2 bytes. Indica la cantidad de datos que hay en el mensaje.
- **CRC.** 4 bytes. Código de redundancia cíclica para la comprobación de errores en el mensaje.

Una vez generada la PDU del subnivel CS, el resultado se pasa al subnivel SAR en bloques de 48 bytes. Por tanto, el subnivel SAR no añade ninguna información adicional.

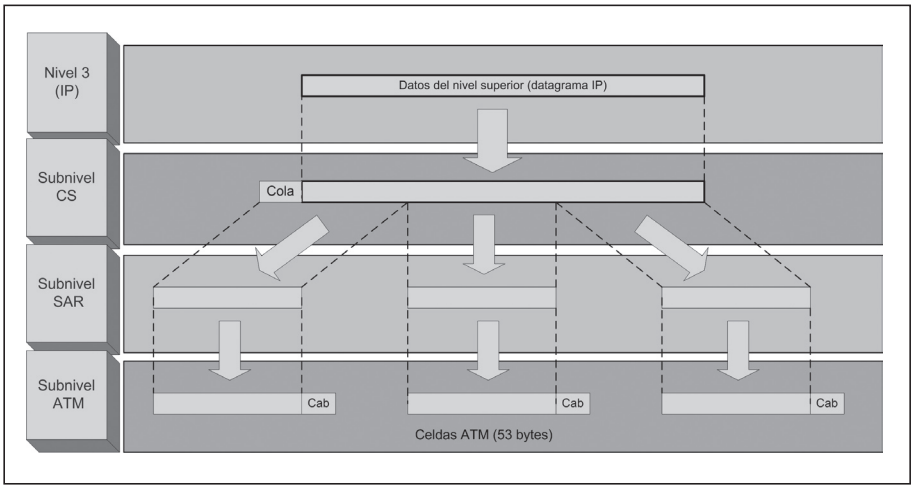


Figura 9.22. *Encapsulación de datos en AAL5.*

Por último, señalar que existe una especificación dentro de ATM para el funcionamiento de ATM dentro de una red local conocida como **LANE (Local Area Network Emulation, Emulación de red de área local)**.

9.5.7 ATM VS. GIGABIT ETHERNET

Tanto ATM como Gigabit Ethernet son tecnologías que han competido en el sector de las redes de alta velocidad, Gigabit Ethernet con una velocidad de 1 Gbps y ATM a 622 Mbps. ATM se diseñó para proporcionar una solución de conectividad a alta velocidad tanto a redes WAN como a redes MAN o LAN. Gigabit Ethernet se diseñó con el objetivo de proporcionar alta velocidad a los segmentos troncales de las redes LAN.

La realidad es que actualmente, ATM se ha consolidado como tecnología de alta velocidad para redes WAN, sin embargo para redes LAN, ATM no ha llegado nunca a tener una gran aceptación. En el sector de las redes MAN, ATM ha conseguido consolidarse aunque en la actualidad tiene una fuerte competencia con la tecnología Gigabit Ethernet, que al utilizar como medio de transmisión la fibra óptica, las distancias alcanzadas cubren perfectamente el ámbito de aplicación de las redes MAN y permiten una conectividad más eficiente con las redes LAN con tecnología Ethernet.

Por tanto, ATM sigue siendo una de las tecnologías más utilizadas en redes WAN. Aunque ATM ha sido la solución preferida por muchos operadores para la implementación de redes MAN, la aparición de Gigabit Ethernet que proporciona un alto nivel de interconectividad con las redes LAN Ethernet y sus prestaciones más elevadas en muchos casos ha hecho que actualmente muchas redes MAN

hayan sido sustituidas por redes Gigabit Ethernet. En el ámbito de las redes LAN, Gigabit Ethernet se ha consolidado con la solución de alta velocidad.

9.6 MPLS

9.6.1 ANTECEDENTES DE MPLS

En una red IP convencional, los mecanismos de reenvío de los paquetes se basan en que cada nodo de la red examina la cabecera de los paquetes y se decide el siguiente salto en el camino. Cuando el tamaño de la red aumenta y el número de paquetes que debe procesar cada nodo de la misma se incrementa, la primera solución posible es aumentar la capacidad de procesado de los routers pero, como es fácilmente imaginable, este aumento de potencia tiene un límite, por lo que es necesario encontrar otro tipo de soluciones que no tengan estas limitaciones.

Una solución al problema descrito, conocida como **conmutación de etiquetas**, se basa en las siguientes premisas:

- ✓ La asignación del camino a seguir por un paquete sólo se realiza en el nodo de entrada. Esta asignación se basa en la cabecera del paquete.
- ✓ El camino asignado se codifica mediante una etiqueta.
- ✓ Los siguientes nodos de la red no analizan la cabecera del paquete. El reenvío hacia el nodo siguiente (*forwarding*) se realiza basándose en la etiqueta asignada en la entrada de la red. Por tanto, la cabecera sólo se analiza una vez.

Este tipo de soluciones presenta las siguientes ventajas:

- ✓ La inteligencia para la asignación de caminos se concentra en la frontera de la red.
- ✓ El reenvío lo puede realizar un conmutador (no son necesarias funciones de encaminamiento paquete a paquete en los nodos intermedios).
- ✓ La asignación de un paquete a un camino particular se puede basar en información que no está presente en la cabecera (por ejemplo, criterios de gestión de red).
- ✓ Permite la definición de rutas explícitas desde el sistema de gestión.

Por ello, desde principios de los años 90 se han elaborado teorías y desarrollado distintas tecnologías que trataban de sustentar estos principios y aprovechar estas ventajas teóricas.

De alguna manera, y teniendo en cuenta la situación de la tecnología en aquel momento (despegue de las redes IP, eclosión de ATM, incremento de capacidad

en las redes de transmisión) se investigaban soluciones tecnológicas que de alguna manera intentaban combinar las ventajas de la rapidez de conmutación ATM con la potencia de los algoritmos de encaminamiento desarrollados en el entorno del mundo IP. Se desarrollaron varias soluciones propietarias pero la que finalmente se ha impuesto ha sido el estándar propuesto por el IETF, desarrollado en 1997 y conocido como **MPLS (Multiprotocol Label Switching)**.

9.6.2 CARACTERÍSTICAS

MPLS es una tecnología de transporte de datos que opera entre el nivel de enlace y el nivel de red y que ofrece un servicio de transporte de datos tanto para redes basadas en circuitos como para redes basadas en datagramas.

Las características de diseño de MPLS son:

- ✓ Debe ser aplicable a cualquier protocolo del nivel de red (multiprotocolo) y al mismo tiempo debe ser independiente del nivel de enlace que se utilice.
- ✓ El envío hacia adelante (forwarding) de los paquetes está basado en la conmutación de una etiqueta (label switching).

Los principales objetivos establecidos en la elaboración del estándar son los siguientes:

- ✓ MPLS no está restringido a ninguna tecnología de nivel 2 (nivel de enlace). Es decir, debe funcionar sobre cualquier medio en el que los datagramas del nivel de red puedan ser intercambiados entre las propias entidades de nivel de red.
- ✓ Los esfuerzos iniciales se concentran en el protocolo del nivel de red IPv4, pero el núcleo de la tecnología MPLS debe ser extensible a múltiples protocolos del nivel de red (IPv6, IPX, Appletalk, etc.).
- ✓ MPLS debe soportar tanto el modo punto a punto (unicast) como el punto-multipunto (multicast).
- ✓ MPLS debe ser compatible con el Modelo de Servicios Integrados del IETF.
- ✓ Debe ser posible la coexistencia en la misma red de conmutadores MPLS y no-MPLS.
- ✓ MPLS debe ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP.

9.6.3 ARQUITECTURA

Las redes que utilizan MPLS siguen una arquitectura similar a la mostrada en la figura:

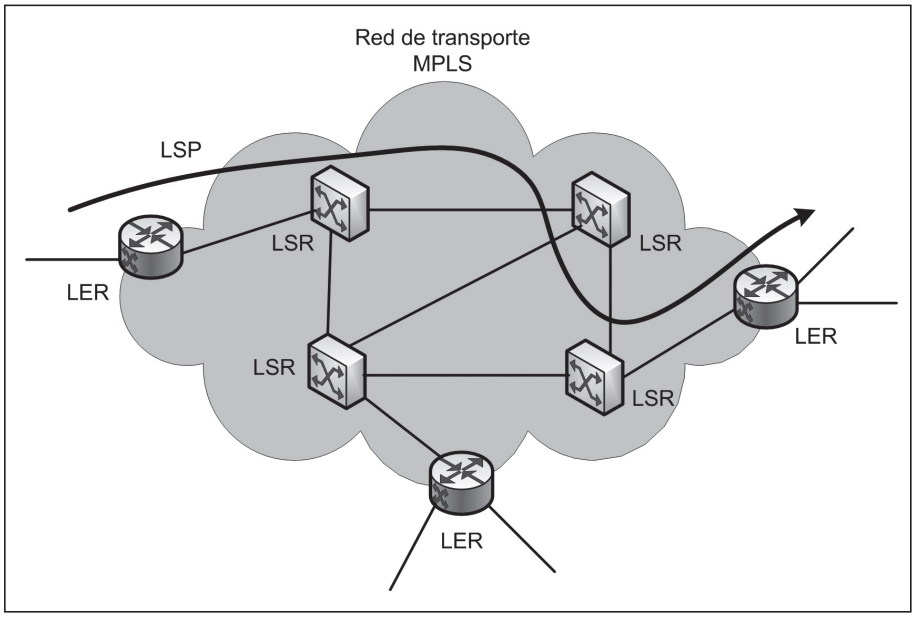


Figura 9.23. *Arquitectura MPLS.*

Los elementos que aparecen en la figura son:

- **LER (Label Edge Router).** Elemento que inicia o termina el túnel, es decir, añade o elimina las etiquetas. Es el punto de entrada / salida de la red MPLS.
- **LSR (Label Switching Router).** Elemento que conmuta paquetes.
- **LSP (Label Switched Path).** Nombre genérico de un camino MPLS, es decir, del túnel MPLS establecido de extremo a extremo.
- **LDP (Label Distribution Protocol).** Protocolo para la distribución de etiquetas en MPLS.
- **FEC (Forwarding Equivalente Class).** Nombre que se le da al tráfico que se encamina bajo una etiqueta.

9.6.4 APLICACIONES DE MPLS

Los sectores que más provecho pueden sacar de MPLS son los proveedores de servicio y las grandes empresas o instituciones oficiales, donde MPLS se puede utilizar de forma eficiente en redes MAN o incluso WAN.

Las principales aplicaciones que actualmente tiene MPLS en las redes IP son:

- ✓ Ingeniería de tráfico.
- ✓ Soporte a las Clases de Servicio.
- ✓ Redes privadas virtuales (VPN) .

A continuación se describen brevemente cada una de ellas.

Ingeniería de tráfico

La **ingeniería de tráfico** (o **dimensionado de tráfico** como algunos autores prefieren traducir la expresión inglesa *Traffic Engineering*) puede ser definida como el proceso de controlar los flujos de datos a través de una red. Es decir, el proceso de optimizar la utilización de los recursos disponibles por parte de los distintos flujos y, por tanto, optimizar el uso global de los recursos y las prestaciones de la red.

Otra definición clarificadora de este mismo concepto es la que establece que la ingeniería de tráfico como "un proceso iterativo de planificación y optimización de red con el propósito de optimizar el uso de los recursos y las prestaciones de la red".

En un entorno de redes que utilizan IP como protocolo de nivel de red, el encaminamiento de los paquetes se basa en los resultados de los algoritmos de encaminamiento y éstos suelen utilizar el criterio de escoger el camino más corto para decidir el camino que deben seguir los paquetes.

Este tipo de algoritmos, diseñados hace unos años, trataba de minimizar el uso de recursos de red escogiendo el camino más corto, pero este criterio de selección puede producir congestión en algunos enlaces de la red (tradicionalmente este problema se resolvía aumentando la capacidad de los enlaces congestionados), mientras que otros enlaces pueden estar infrautilizados.

Aunque en la literatura pueden encontrarse abundantes opiniones sobre la disminución del coste del ancho de banda (si el coste del ancho de banda tiende a cero, los operadores de red pueden ofrecer un ancho de banda muy superior a un coste muy bajo, lo que eliminaría, al menos en teoría, los problemas antes mencionados), la situación actual es que la gestión del tráfico sobre los recursos existentes sigue siendo una realidad para los gestores de las redes.

Para resolver este tipo de problemas, MPLS es una herramienta efectiva de ingeniería de tráfico en grandes redes troncales, ya que:

- ✓ Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un *LSP*.
- ✓ Permite realizar un **encaminamiento restringido** (**Constraint-Based Routing**, **CBR**), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales con distintos niveles de calidad (por ejemplo, garantías explícitas de retardo, ancho de banda, fluctuación, pérdida de paquetes, etc.).
- ✓ El encaminamiento restringido (CBR) puede computar las rutas sujetas a restricciones (por ejemplo, ancho de banda disponible, restricciones administrativas, etc.); es decir, que este tipo de soluciones considera más datos que la estricta topología de la red para calcular el camino más conveniente.

Como resumen puede afirmarse que para poder hacer la ingeniería de tráfico de forma efectiva en una red IP (modelo de red sin conexión) el administrador de la misma debe disponer de mecanismos para controlar el camino que siguen los paquetes; es decir, debe ser capaz de establecer algún tipo de conexión o circuito en una red sin conexión, lo que es capaz de llevarse a cabo con MPLS.

Soporte a las Clases de Servicio

Aunque tradicionalmente las redes IP sólo ofrecían una **clase de servicio** (*Best effort*), los usuarios actuales de dichas redes están interesados actualmente en cursar todo tipo de tráfico (por ejemplo, voz, video, etc.) y no sólo datos como ocurría originalmente.

Estos nuevos tipos de servicios añaden requisitos adicionales a la red de transporte (por ejemplo, el tráfico de voz es muy sensible al retardo y a su variación, mientras que las comunicaciones de video suelen ser muy exigentes desde el punto de vista del ancho de banda que necesitan) y los usuarios de las mismas quieren garantías de que las prestaciones de la red son suficientes para que los servicios finales no sufran degradación.

Esta circunstancia obliga a que los operadores dispongan de mecanismos para satisfacer estas garantías de calidad de servicio, entendiendo este concepto como "la capacidad que tiene un sistema de asegurar, con un grado de fiabilidad preestablecido, que se cumplan los requisitos de tráfico, en términos de perfil y ancho de banda, para un flujo de información dado".

Una primera estrategia que pueden adoptar los proveedores de conectividad, de hecho se ha hecho en algunas ocasiones, es sobredimensionar los enlaces, pero como se ha comentado anteriormente, esta alternativa es costosa desde el punto de vista económico.

Una alternativa es utilizar MPLS, ya que permite asignar un camino específico (LSP) y asignar al mismo los recursos necesarios en cada nodo y en los enlaces entre ellos, para cada tipo de flujo (por ejemplo, video, voz, correo electrónico, etc.), utilizando las capacidades que ofrece el encaminamiento restringido (CBR).

Redes privadas virtuales (VPN)

Una **red privada virtual** (**VPN**) es un modo de permitir a los usuarios el extender sus redes privadas sobre la infraestructura de la red pública de forma segura. Básicamente una red privada virtual (VPN) se construye utilizando conexiones realizadas sobre una infraestructura compartida con funcionalidades de encaminamiento y de seguridad similares a las que existen en una red privada. El objetivo de las VPN es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos y video sobre infraestructuras de comunicaciones eficaces y rentables. Las dos características más importantes, desde el punto de vista del usuario de una *VPN* son:

- **Seguridad.** La seguridad supone aislamiento, es decir, que sus datos son suyos y por tanto no son accesibles al resto del mundo.
- **Privacidad.** La idea de *privada* significa que el usuario *siente* que los enlaces utilizados para construir la red son sólo suyos.

La solución original para construir VPN sobre redes *IP* fue el establecimiento de túneles IP (el objetivo de un túnel sobre IP es crear una asociación permanente entre dos extremos, de modo que funcionalmente aparezcan conectados), utilizando para ello las distintas soluciones existentes actualmente. Este tipo de soluciones tiene inconvenientes como son:

- ✓ Están basadas en conexiones punto a punto.
- ✓ La configuración es manual, por los que la provisión y gestión son complicadas.
- ✓ Es una solución escalable de forma costosa.
- ✓ La gestión de calidad de servicio sólo es posible de forma limitada.

En un entorno MPLS, en lugar de conexiones entre los distintos emplazamientos de la VPN lo que hay son conexiones IP a una nube común en las que solamente pueden entrar los miembros de la VPN. Dicha nube se construye mediante los LSP que definen los caminos en un entorno MPLS.

Por las razones expuestas, la solución MPLS para VPN presenta las siguientes ventajas:

- ✓ Evita la complejidad de los túneles.
- ✓ La provisión es más sencilla.
- ✓ Es más fácilmente escalable.
- ✓ Ofrece garantías de calidad de servicio extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases.
- ✓ Permite aprovechar las posibilidades de ingeniería de tráfico para poder garantizar los parámetros críticos y la respuesta global de la red.

En resumen, se podría decir que la arquitectura MPLS está teniendo un notable éxito, por su capacidad de coexistir con cualquier protocolo de red y, sobre todo, por su coexistencia con cualquier tecnología de red subyacente. No cabe duda de que esta independencia permite que el movimiento de las capas inferiores, desde ATM a SDH y DWDM, pueda ser controlado sin crear situaciones traumáticas y sin que los tiempos de decisión sean críticos, por lo que no hay que depender del conocimiento anticipado y arriesgado de las tecnologías emergentes y de su evolución.

RESUMEN DEL CAPÍTULO

En este capítulo se ha hecho un recorrido por las principales tecnologías desarrolladas para dar soporte a las redes WAN.

El protocolo PPP es uno de los más utilizados para la conexión WAN de un usuario a un proveedor de servicios de Internet a través de líneas telefónicas. PPP es capaz de transportar en líneas punto a punto conmutadas tráfico IP. Además proporciona dos posibles mecanismos de comprobación de identidad como son PAP y CHAP.

Se proporciona una visión general de una de las tecnologías de acceso a redes WAN más utilizadas, como es X.25, si bien actualmente ha sido superada por otras tecnologías que aprovechan mucho mejor las nuevas infraestructuras digitales.

Frame Relay fue la tecnología WAN desarrollada para sustituir a X.25. Al igual que ésta, está basada en la conmutación de paquetes pero minimizando la gestión de flujo y de errores para conseguir mejores prestaciones. Frame Relay tuvo su despegue definitivo a mediados de los 90.

ATM se puede considerar actualmente la tecnología WAN más extendida, aunque inicialmente se desarrolló para poder aplicarse en cualquier tipo de redes, incluidas redes LAN y MAN. Está basada en la conmutación de celdas por lo que es válida para cualquier tipo de tráfico.

El último apartado del capítulo trata sobre MPLS, una de las últimas tecnologías utilizadas en redes WAN y MAN. MPLS está basada en la técnica de conmutación de etiquetas y ha demostrado su eficacia para ofrecer servicios de conmutación de paquetes sobre protocolos basados en datagramas como IP.

TEST DE CONOCIMIENTOS

1 Una de las diferencias entre X.25 y Frame Relay es:
- **a)** En X.25 se alcanzan velocidades más altas.
- **b)** En la especificación del nivel físico.
- **c)** En X.25 se utiliza conmutadores y en Frame Relay multiplexores.
- **d)** X.25 implementa tres niveles y Frame Relay sólo dos.

2 En X.25, el algoritmo de encaminamiento:
- **a)** X.25 no incluye algoritmos de encaminamiento.
- **b)** Se implementa en el nivel de paquetes.
- **c)** Se implementa en el nivel de trama.
- **d)** Se implementa en el protocolo X.121.

3 ¿Para qué se utiliza el subnivel NCP en PPP?
- **a)** Para establecer los enlaces.
- **b)** Para encapsular múltiples protocolos.
- **c)** Para convertir paquetes en celdas.
- **d)** Para establecer conexiones.

4 ¿Cuál es una de las diferencias entre PAP y CHAP?
- **a)** PAP es un método de dos vías más sencillo y CHAP es más complejo utilizando tres vías.
- **b)** PAP envía la contraseña de validación sin cifrado y CHAP no.
- **c)** PAP sólo verifica la identidad al comienzo y CHAP lo hace periódicamente.
- **d)** Todas las respuestas anteriores son válidas.

5 El nivel físico en Frame Relay:
- **a)** Está especificado como compatible con el estándar EIA-232.
- **b)** Está especificado como compatible con X.25.
- **c)** Está especificado como compatible con V.24 de la ITU-T.
- **d)** No está especificado, se admite cualquier protocolo estándar.

6 ATM es una tecnología que se puede utilizar:
- **a)** Exclusivamente en redes WAN.
- **b)** Exclusivamente en redes LAN.
- **c)** Exclusivamente en redes MAN.
- **d)** En cualquier tipo red, si bien su uso más extendido es en redes WAN.

7 Una conexión lógica en ATM se identifica:
- **a)** Por la dirección IP origen y destino de la celda.
- **b)** Por el VCI para conexiones locales.
- **c)** Por el VPI para conexiones remotas.
- **d)** Tanto por el VCI como por el VPI.

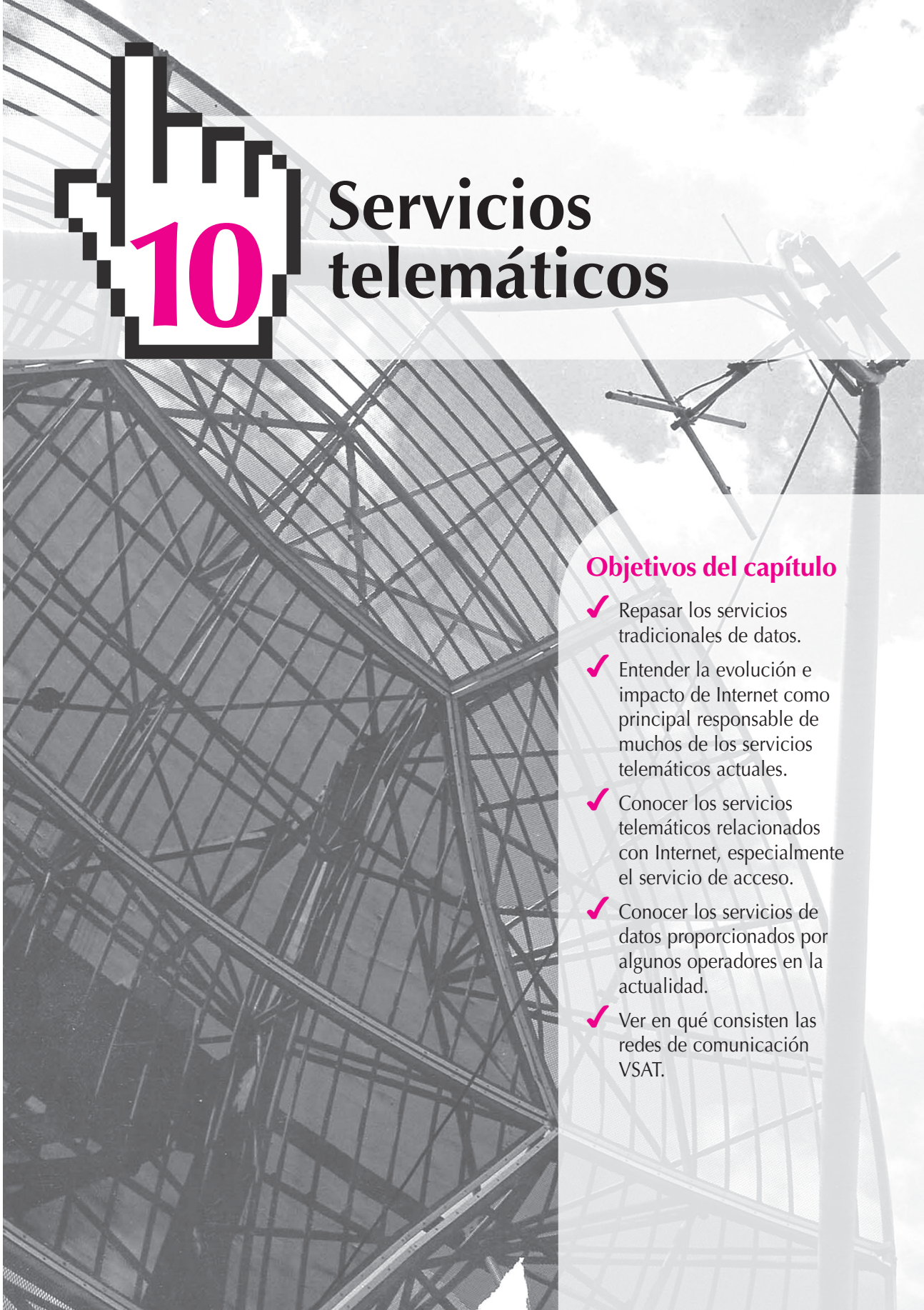
8 En qué nivel del modelo OSI se enmarca la tecnología MPLS:
- **a)** En el nivel 2.
- **b)** En el nivel 3.
- **c)** Entre el nivel 2 y el nivel 3.
- **d)** En el nivel 4.

9 ¿Qué sector utiliza con grandes beneficios MPLS?

a) Los usuarios particulares.
b) Los proveedores de servicios de datos.
c) Las pequeñas empresas.
d) Todas las anteriores son válidas.

10 El subnivel AAL5 se utiliza en ATM para:

a) Transferencia de datos que no utilicen SMDS como tráfico IP.
b) Transferencia de datos basada en SMDS.
c) Transferencia de datos a velocidad constante como voz y video.
d) Transferencia de datos a través de redes públicas.



10 Servicios telemáticos

Objetivos del capítulo

- ✓ Repasar los servicios tradicionales de datos.
- ✓ Entender la evolución e impacto de Internet como principal responsable de muchos de los servicios telemáticos actuales.
- ✓ Conocer los servicios telemáticos relacionados con Internet, especialmente el servicio de acceso.
- ✓ Conocer los servicios de datos proporcionados por algunos operadores en la actualidad.
- ✓ Ver en qué consisten las redes de comunicación VSAT.

10.1 INTRODUCCIÓN

Todos las técnicas, protocolos, estándares, conceptos y modelos estudiados a lo largo del libro tienen como finalidad última la de proporcionar servicios de comunicaciones a los usuarios finales. El concepto de servicio telemático se podría aplicar en cualquier ámbito en el que se proporcionen mecanismos para la interconexión de sistemas para el intercambio de datos. De esta forma, sería perfectamente válido, por ejemplo, considerar un servicio telemático al proporcionado por la interconexión de equipos a través de una red de área local. Sin embargo, el concepto de servicio telemático normalmente está asociado al servicio prestado por empresas especializadas de telecomunicaciones.

Estos servicios se pueden agrupar en dos grandes bloques. Los servicios telemáticos orientados a proporcionar interconexión entre dos o más puntos situados más o menos alejados entre sí. Y los servicios telemáticos que proporcionan acceso a redes de datos, especialmente a una, Internet. Posiblemente Internet sea el servicio telemático más extendido y demandado en la actualidad.

10.2 SERVICIOS TELEMÁTICOS TRADICIONALES

El servicio telegráfico es posiblemente el primer y más antiguo servicio telemático del mundo. Fue Morse el que desarrolló el primer sistema de transmisión empleando señales eléctricas. En el sistema radioeléctrico, la información transmitida eran mensajes de texto codificados en el sistema Morse. En los primeros momentos, la telegrafía fue un medio de comunicación por el cual una persona que tenía un mensaje que enviar, entregaba dicho mensaje en forma escrita en la oficina de telégrafos más cercana y desde aquí, el mensaje se transmitía a la siguiente oficina. El proceso se repetía hasta alcanzar la oficina destino. El mensaje era enviado de la oficina al destinatario mediante un mensajero.

La evolución del servicio telegráfico es la evolución de la propia telemática. Primero con la llegada de los teleimpresores, dispositivos capaces de interpretar las señales eléctricas e imprimir el mensaje sin necesidad de un operador. Y después, la llegada de la conmutación de circuitos como técnica de transmisión.

El servicio Télex es un servicio público para la comunicación de datos (texto) entre abonados en la cual la información transmitida se imprime en dispositivos conocidos como teleimpresores o terminales télex. El servicio Télex normalmente está asociado a las comunicaciones telegráficas entre abonados. Mientras que para la telegrafía pública se utiliza el conocido como **Servicio Gentex**.

El servicio télex empezó a funcionar el España en 1954, con una única central instalada en Madrid. Posteriormente se implantó una red Télex por todo el territorio nacional. Este servicio tuvo un gran auge en los años posteriores alcanzando una cifra de 36.000 abonados en el año 1989, en el cual empezó su declive.

Otro servicio ya prácticamente desaparecido en la actualidad es el llamado **Servicio de Videotexto**. Este servicio consistía en la transmisión de los datos a través de líneas telefónicas y la presentación de la información transmitida se hacía en una pantalla de televisión.

En España, este servicio lo desplegó Telefónica a principios de los años 90 como **Servicio Ibertex**, aunque no tuvo mucho éxito.

Otro de los servicio telemáticos clásicos es el conocido como **FAX (o facsímil)**. Este servicio se basa en el envío de imágenes o gráficos en baja resolución. La imagen que se desea enviar se descompone en una matriz de puntos que se convierten en una señal eléctrica digital que es lo que se transmite a través de la red RTC (Red Telefónica Conmutada).

10.3 LA REVOLUCIÓN DE LOS SERVICIOS TELEMÁTICOS: INTERNET

Qué duda cabe que actualmente Internet es el paradigma de los sistemas telemáticos y, por extensión, una gran parte de los servicios proporcionados por la telemática se proporcionan a través de la Red de redes. En este apartado se ofrece una visión general de su evolución histórica, así como su gestión y su arquitectura.

10.3.1 EVOLUCIÓN DE INTERNET

En el capítulo 8 se presentó un apartado dedicado a la historia de TCP/IP, inevitablemente unida a la historia de Internet. No hay un consenso claro de en qué momento nace Internet. Algunos autores sitúan este momento en el nacimiento de ARPANET en 1969. Este hecho se puede considerar el embrión de Internet por ser el primer intento de unir ordenadores situados en distintos lugares, pero no se puede considerar Internet todavía. La definición más extendida de Internet es la de red de redes. ARPANET no es una red de redes sino unas cuantas computadoras unidas entre sí mediante conexiones telefónicas (las primeras redes WAN).

Sería más correcto señalar como el nacimiento de Internet a la puesta en servicio de la red NSFNET, una red que ya utiliza los protocolos TCP/IP y cuya misión es la de ser troncal para la conexión de redes. Este hecho se produce en 1986 aún cuando ARPANET sigue en servicio. Es por ello, que NSFNET se considera una evolución o continuación de ARPANET cuando realmente su objetivo es ya claramente la interconexión de redes, eso sí, utilizando todos los desarrollos y éxitos de ARPANET.

La red NSFNET la crea en Estados Unidos una fundación llamada NSF **(National Science Foundation, Fundación Nacional de ciencia)**, que es algo así como una agencia de investigación científica financiada por el propio gobierno de Estados

Unidos. Por tanto NSF se puede considerar el organismo responsable de los primeros pasos de Internet. De hecho, este organismo ya había participado en el desarrollo de ARPANET.

En 1990 se desmantela definitivamente ARPANET (quedando operativa la rama militar MILNET) quedando NSFNET como único troncal de la Red. Sin embargo, el gran desarrollo de Internet comienza cuando algunas empresas empiezan a implementar sus propias redes y a ofrecer servicios de conexión de Internet a través de ellas.

En paralelo a estos acontecimientos, se produce otro hecho fundamental en la evolución de Internet. En 1989, Tim Berners-Lee, un licenciado en Física que trabajaba en el **Laboratorio Europeo de Física de Partículas** (CERN, Organisation Européenne pour la Recherche Nucléaire), propuso un proyecto para la creación de un sistema de gestión de la información. Tres años más tarde, en 1992, empezaban a funcionar los primeros servicios para compartir información a través de la Red, era el nacimiento del **World Wide Web** (www) o simplemente Web. El éxito de este sistema fue inmediato ya que permitía la publicación de documentos en Internet con la posibilidad de incluir enlaces a otros documentos alojados en otros servidores (hipertexto). El impulso definitivo del servicio web se produjo cuando apareció el primer navegador con capacidades gráficas llamado **Mosaic**, en 1993.

Mientras tanto, la NSF decide ceder el control del backbone de Internet a las empresas proveedoras de los servicios de conexión. Esta decisión implica que el control de Internet dejaba de estar en manos de un país (la NSF estaba financiada por dinero de Estados Unidos) para ser una red descentralizada. Esta característica ha sido fundamental en el desarrollo posterior de la Red.

En 1995, la NSF transfiere el control de Internet de forma provisional a cuatro operadoras norteamericanas: **MFS Datanet**, **Sprint**, **Ameritech** y **Pacific Bell**. Estas empresas constituyen los llamados NAP (Network Access Point) o Puntos de acceso a la red, que proporcionan conectividad al resto de empresas que ofrecen servicios de conexión a Internet, los llamados **ISP (Internet Service Provider)**. Sin embargo, durante los siguientes años el proceso de descentralización de la Red sigue avanzando desapareciendo estos primeros NAP para establecerse la arquitectura definitiva y que se mantiene en la actualidad a través de los llamados **IXP (Internet eXchange Points)**. Un IXP es una infraestructura física que permite la interconexión de varios ISP para intercambiar tráfico entre ellos y con otros IXP. La conexión entre los diferentes IXP forma el backbone actual de Internet.

Como veíamos, a pesar que Internet ofrecía casi desde sus inicios diferentes servicios basados todos en la arquitectura TCP/IP, como correo electrónico, transferencia de ficheros, búsqueda de información, etc., fue el servicio Web el que hizo explotar definitivamente el potencial de la Red a nivel comercial. El primer navegador que se ejecutó en un entorno gráfico (concretamente en entornos X de

sistemas Unix) fue Mosaic y tuvo una gran aceptación debido sobre todo a que era gratuito.

Unos años más tarde, Microsoft desarrolla su propio navegador Web llamado Internet Explorer, también gratuito y Mosaic se convierte en Netscape, estableciéndose una dura competencia entre ellos. Actualmente Microsoft sigue ofreciendo su navegador web incluido en los sistemas operativos Windows mientras que Netscape evolucionó a Mozilla Firefox. El servicio web es, con diferencia, el servicio más utilizado en Internet debido sobre todo a los grandes avances técnicos conseguidos en la tecnología de navegación que permite a su vez la visualización o ejecución de numerosos formatos multimedia y es capaz de proporcionar a los documentos web un alto grado de dinamismo.

10.3.2 HISTORIA DE INTERNET EN ESPAÑA

A mediados de los años 80 existían en España varias redes (FAENET, EUnet, EARN...) sobre todo en ámbitos académicos, diferentes e incompatibles entre sí.

El primer intento de ofrecer un servicio de interconexión homogéneo surge en 1988 con la creación del **Programa IRIS** dentro del **Plan Nacional de Investigación Científica y Desarrollo Tecnológico**. La infraestructura utilizada para crear esta nueva red era la red pública de datos X.25, proporcionada por Telefónica a través del servicio **Iberpac**. Inicialmente se decidió la utilización de los servicios basados en los protocolos del modelo OSI.

En 1990 el Programa IRIS cambia su denominación a **RedIRIS**. Se decide la creación de un troncal propio de alcance nacional basado en X.25. Para ello se emplean líneas punto a punto de 64 Kbps. Inicialmente se conectaron tres nodos: Madrid, Barcelona y Sevilla.

Debido a que el desarrollo de los protocolos OSI no acababa de despegar, se tomó la decisión de comenzar a utilizar los protocolos TCP/IP. Decisión propiciada además por el cambio en el modelo de interconexión de sistemas que estaba pasando de la interconexión de grandes equipos entre sí, a los que se accedía a través de terminales, a la interconexión de equipos por medio de redes de área local, donde los protocolos TCP/IP empezaban a consolidarse ampliamente.

La primera conexión de RedIRIS a Internet se estableció a mediados de 1990 a través de un enlace punto a punto internacional a 64 Kbps.

En 1992 se crea el primer ISP español llamado **Goya Servicios Telemáticos**. RedIRIS extiende su conectividad prácticamente a todas las universidades.

En 1994 existen más de 20.000 equipos y más de 100 organizaciones conectados a la RedIRIS con acceso a Internet. RedIRIS pasa a depender del **CSIC (Consejo Superior de Investigaciones Científicas)**. En este mismo año aparece **SERVICOM**, el segundo ISP español.

En 1995 se produce la explosión definitiva en España del acceso a Internet. A finales de este año habría más de 30 ISP. Telefónica crea el primer servicio de acceso a Internet llamado **Infovía**.

En 1997 se crea **ESPANIX**, el punto neutro español de interconexión a Internet.

En 2000 se presenta una nueva tecnología de acceso de banda ancha a Internet llamado ADSL. En 2001 comienza a proporcionarse servicios de conexión mediante ADSL.

10.3.3 ORGANISMOS DE GESTIÓN DE LA RED

Actualmente, Internet está gestionada desde varias organizaciones:

ISOC (Internet Society)

La ISOC es una organización no gubernamental dedicada al desarrollo a nivel global de Internet, formada por instituciones comerciales, gubernamentales y educativas. Su objetivo principal es ser un centro de cooperación y coordinación global para el desarrollo de protocolos y estándares compatibles para Internet.

La ISOC es la organización principal de la Internet Engineering Task Force (IETF), que provee la infraestructura corporativa, así como el financiamiento, apoyo jurídico y fiscal. ISOC ha constituido también las siguientes asociaciones: Internet Architecture Board (IAB), Internet Engineering Steering Group (IESG), Internet Assigned Numbers Authority (IANA). Estas agrupaciones desempeñan un papel importante en la estructura global de Internet.

Anualmente ISOC aporta a la IEFT alrededor de un millón de dólares para la elaboración de los **RFC** (**Requests for Comments**), considerados los estándares de Internet que se determinan mediante equipos de trabajo que operan de manera abierta y democrática para asegurar la evolución transparente de Internet.

www.isoc.org

IAB (Internet Architecture Board)

Comisión creada para gestionar los protocolos usados en la red. Creado inicialmente por DARPA en 1979 como Internet Configuration Control Board. Inicialmente estaban representados: DARPA, NASA, Dep. Energía, NSF. Presidida por Vinton G. Cerf uno de los desarrolladores de los protocolos TCP/IP junto a Robert E. Kahn. A partir de 1992, depende de la ISOC. Entre otras funciones el IAB es responsable de la publicación de los RFC y de la supervisión de los trabajos del IETF. Los **RFC (Request For Comments)** son los documentos donde se publican todos los estándares que forman parte de Internet. Por ejemplo, la arquitectura TCP/IP está publicada bajo documentos RFC.

Los documentos RFC están publicados en ficheros con formato ASCII y en inglés en la página web oficial: http://www.rfc-editor.org/

Existe además una página donde algunos de los más importantes RFC han sido traducidos al español: http://www.rfc-es.org/

Página web de IAB: www.iab.org

IETF (Internet Engineering Task Force)

La IETF es una organización formada por grupos de trabajo encargados de diversos aspectos relacionados con la evolución de la arquitectura de Internet. Los grupos de trabajo se constituyen para llevar a cabo estudios de las diferentes tecnologías utilizadas en Internet. Los trabajos de la IETF son supervisados por la IAB.

IRTF (Internet Research Task Force)

Al igual que la anterior, es una organización formada por grupos de trabajo dedicados a tareas de investigación de las nuevas tecnologías que se pueden aplicar a Internet.

IANA (Internet Assigned Numbers Authority)

Agencia de asignación de números en Internet. Asigna a los **registradores nacionales de Internet (RIR)**. RIPE es el RIR para Europa. ARIN es el RIR para Norteamérica.

ICANN (Internet Corporation for Assigned Names and Numbers)

Es una organización sin fines de lucro que opera a nivel internacional, responsable de asignar espacio de direcciones numéricas del protocolo IP, identificadores de protocolo y de las funciones de gestión (o administración) del sistema de nombres de dominio de primer nivel genéricos y de códigos de países, así como de la administración del sistema de servidores raíz. Aunque en un principio estos servicios los desempeñaba Internet Assigned Numbers Authority (IANA) y otras entidades bajo contrato con el gobierno de EEUU, actualmente son responsabilidad de ICANN.

Como asociación privada-pública, ICANN está dedicada a preservar la estabilidad operacional de Internet, promover la competencia, lograr una amplia representación de las comunidades mundiales de Internet y desarrollar las normativas adecuadas a su misión por medio de procesos “de abajo hacia arriba” basados en el consenso.

www.icann.org

10.3.4 ESTRUCTURA DE LA RED

Como se ha visto en el apartado sobre la evolución de Internet, actualmente la Red tiene una estructura distribuida de forma que no existe un troncal propiamente dicho de Internet aunque el núcleo más importante se sigue localizando en Estados Unidos, donde el backbone de Internet está formado más de 130.000 routers. Las principales compañías que proporcionan la conectividad son Verizon (a través de su división UUnet), AT&T, Qwest, Level 3 Communication, Sprint Nextel.

La topología de Internet es tremendamente compleja pero a grandes rasgos se podría decir que el backbone de Internet sigue una tendencia de topología mallada y en los extremos se sigue más la topología en estrella.

Los llamados "Carriers" son empresas de Telecomunicaciones que proporcionan conectividad entre los ISP de diferentes localizaciones. Sus clientes son operadores, ISP o administraciones públicas. Algunos ejemplos son Global Crossing, Teleglobe o Telia-Sonera.

Las empresas que proporcionan conectividad a los usuarios finales, tanto usuarios residenciales como a empresas se denominan **ISP (Internet Service Provider)**.

La arquitectura actual de Internet está basada en los llamados IXP.

IXP (Internet Exchange Point) es una infraestructura física que permite a diferentes ISP intercambiar tráfico Internet entre sus redes (sistemas autónomos). Un IXP típico es una red de conmutadores cada uno de los cuales ofrece conectividad a un ISP.

El concepto de un IXP es, por tanto, sencillo. Se podría decir que un IXP es un lugar donde varios ISP intercambian tráfico entre ellos. Esta arquitectura permite aislar el tráfico de Internet entre operadores y no utilizar los troncales por lo que el uso del ancho de banda disponible es más eficiente.

En Europa existe una asociación de IXP llamada Euro-IX (http://www.euro-ix.net/) que agrupa a todos los IXP europeos y algunos IXP de Japón y Estados Unidos.

En España existen dos IXP:

- **ESPANIX,** llamado también Punto Neutro Español. Permite el mantenimiento del tráfico de Internet en España. Está situado físicamente en Madrid, concretamente en el CPD (Centro de Proceso de Datos) de Banesto y que proporciona conectividad a ISP que operan a nivel nacional. De hecho, ESPANIX conmuta un tráfico de 4 Gbps, lo que supone un 95% del tráfico Internet intercambiado en España.
- **CATNIX,** situado en Barcelona, está orientado a ofrecer conectividad a operadores que operen en Cataluña. Se puede ver el equipamiento de red en el nodo CATNIX en: http://www.catnix.net/es/que/infraestructura.html

A continuación se muestra una lista de los IXP más utilizados según un informe publicado el día 02-01-2007 con los datos obtenidos en diciembre de 2006.

Tabla 10.1

Cód.	Nombre	Situación	Miembros	Velocidad máxima (Gbps)
AMS-IX	Amsterdam Internet Exchange	Amsterdam, Holanda	259	218
LINX	London Internet Exchange	Londres, Reino Unido	221	164
DE-CIX	Deutscher Commercial Internet Exchange	Frankfurt, Alemania	196	122
JPNAP	Japan Network Acces Point	Tokyo, Japón	88	105
Netnod	Netnod Internet Exchange i Sverige	Estocolmo, Suecia	53	67
ESPANIX	España Internet Exchange	Madrid, España	36	64

Como se puede observar, ESPANIX ocupa la sexta posición con una velocidad máxima de 64 Gbps.

En la lista anterior faltan algunos IXP, especialmente de Estados Unidos, donde la forma de funcionamiento de los IXP es diferente al resto de países. En cualquier caso, uno de los IXP más importantes es **MAE-East** (http://www.mae.net/) que es un IXP que opera en la costa este de Estados Unidos y está gestionado por **Verizon**.

Otro IXP que merece la pena mencionar es **FreeIX**, ubicado en Francia y que proporciona servicios de conexión a ISP de manera gratuita.

10.4 SERVICIOS TELEMÁTICOS RELACIONADOS CON INTERNET

Lógicamente, los servicios telemáticos relacionados con Internet son muchos y algunos de ellos gozan de gran popularidad. Se puede decir que prácticamente todas las actividades comerciales tienen un servicio correspondiente en Internet.

La mayor parte de los servicios relacionados con Internet están basados en el **Servicio Web** aunque muchos de ellos se apoyan en otras tecnologías para llevarlo a cabo. Algunos ejemplos:

- Servicios de correo electrónico.
- Servicios de difusión de radio y video. Existen cada vez más operadores y pequeñas emisoras que proporcionan emisiones digitales de sus programas, tanto de radio como de televisión. Incluso existen emisiones de radio exclusivamente digitales, es decir, sólo emitidas por Internet.
- Servicios de comercio electrónico. A través de páginas web, las empresas ofrecen completos catálogos y venden sus productos, proporcionando medios de pago cada vez más seguros.

- Servicios de banca virtual. La mayor parte de las entidades bancarias proporcionan la posibilidad de efectuar todo tipo de operaciones bancarias desde Internet con un alto grado de seguridad.

Pero quizás, en el ámbito de los sistemas telemáticos, el servicio relacionado con Internet más representativo es precisamente el servicio de acceso a Internet, proporcionado por los llamados **ISP (Internet Service Provider, Proveedor de servicios de Internet)**.

Actualmente, el acceso a Internet a clientes residenciales se proporciona mediante las siguientes tecnologías:

- RTC
- RDSI
- Cable
- ADSL

Además de algunas tecnologías minoritarias actualmente como Wi-Fi, WiMAX o VSAT.

La tecnología ADSL, cuyos principios de funcionamiento se han estudiado en el capítulo 2, surge por la necesidad de proporcionar nuevos servicio que necesitan una infraestructura de acceso con gran ancho de banda. Hasta ese momento, el acceso residencial a Internet más común era por medio de la red telefónica utilizando un módem de banda vocal que ofrecía una velocidad de transmisión teórica de 56 Kbps, aunque en la práctica no superaba nunca los 45 Kbps.

En España y en la mayor parte de los países europeos ADSL es la tecnología de acceso a Internet más extendida. En Estados Unidos, sin embargo, son las redes de televisión por cable la tecnología de acceso a Internet más utilizado.

El acceso a Internet a clientes residenciales se ofrece por varias operadores:

Servicios de acceso a Internet de banca ancha a través de líneas ADSL los proporcionan operadoras como:

- Telefónica
- Orange
- Ya.com
- Jazztel
- Tele2

Todas ellas además proporcionan servicios de acceso a Internet a través de líneas RTC, con velocidades máximas de 56 Kbps.

Además, los siguientes operadores ofrecen servicios de acceso Internet de banda ancha a través de cable con varias modalidades:

- ONO, con velocidad de acceso de 4 Mbps
- R, con velocidades de conexión de 1, 2, 3, 6 y 9 Mbps
- Euskaltel, con las siguientes velocidades de acceso: 300 Kbps/150 Kbps, 3 Mbps/600 Kbps, 12 Mbps/600 Kbps, 24 Mbps/1 Mbps

10.5 SERVICIOS DE DATOS

En este apartado se van a exponer los principales servicios de datos para empresas que proporcionan algunos de los operadores de Telecomunicaciones más importantes de España, entre los que se encuentran:

- Telefónica
- ONO Empresas
- Jazztel
- Colt Telecom
- Ya.com Empresas
- Operador R
- Euskaltel

Algunos de los servicios más comunes ofrecidos se presentan a continuación.

10.5.1 CIRCUITOS PUNTO A PUNTO

Se presentan dos ejemplos de servicios de alquiler de circuitos punto a punto.

Telefónica ofrece servicios de alquiler de circuitos punto a punto con las siguientes características:

- **Baja velocidad.** Con velocidades desde 200 bps hasta 19.200 bps. Interfaces V.24 /V.28.
- **Media velocidad.** Desde 64 Kbps hasta 1.920 Kbps. Se soportan sobre la red Ibermic de Telefónica. Interfaces V.24, V.35, V.10/V.11 y G.703.
- **Alta velocidad.** Velocidad de 2 Mbps. Interfaces G.703 Y G.704.

COLT ofrece servicios de alquiler de circuitos punto a punto a través de su producto llamado **COLT Link** que tiene las siguientes características:

- **COLT Link Metro,** para conexiones entre edificios de la misma ciudad.
- **COLT Link National,** para conexiones entre ciudades del mismo país.
- **COLT Link International,** para conexiones entre ciudades de diferentes países.

Las conexiones pueden ser:

- **Punto a punto,** entre dos sedes, que a su vez pueden ser circuitos no estructurados y circuitos estructurados.
- **Punto a multipunto,** donde una sede central se conecta a varias sedes secundarias. El ancho de banda de las sedes secundarias es menor y su suma no puede ser mayor al ancho de banda de la sede central. Por ejemplo, se puede configurar una sede principal con una velocidad de 2'048 Mbps y ocho sedes secundarias a 256 Kbps (8 x 256 Kbps).

Anchos de banda disponibles van desde 64 Kbps hasta 2'5 Gbps (STM-16).

Interfaces soportados son los siguientes: X.21 y V.35 hasta 2'048 Mbps. G.703 desde 2'048 Mbps hasta 155 Mbps. G.957 (fibra óptica) para 155 Mbps, 622 Mbps y 2'5 Gbps.

Otros operadores que proporcionan servicio de alquiler de circuitos punto a punto son R, con velocidades desde 64 Kbps hasta 622 Mbps. Euskaltel, con velocidades desde 64 Kbps hasta 34 Mbps. ONO ofrece su servicio Enlace Portador con velocidades desde 64 Kbps hasta 2'5 Gbps.

10.5.2 X.25

La conectividad a través de redes X.25 se proporciona principalmente por los servicios **Iberpac** e **Iberpac Plus** de **Telefónica**. La principal diferencia es que Iberpac Plus ofrece tarifa plana de conexión independiente de la utilización. Este servicio de datos está indicado a empresas que necesiten fiabilidad y robustez con poco consumo de ancho de banda.

El servicio X.25 utiliza la red de datos multiservicio de Telefónica conocida como red UNO. Aunque fue el primer servicio WAN utilizado, actualmente este servicio tiene un grado de utilización pequeño.

Ofrece velocidades desde 1'2 Kbps hasta 1.984 Kbps utilizando interfaces V.24/V.28, V.35 y G.703/G.704

Servicio de transmisión de datos basado en el protocolo X.25. Se puede considerar el primer servicio WAN.

10.5.3 FRAME RELAY

Existen varios operadores que proporcionan este servicio de conexión a través de red WAN. Al igual que el servicio X.25, el servicio Frame Relay está orientado a ofrecer conectividad de las sedes de una empresa a través de la red WAN Frame Relay de un operador. Las velocidades de conexión típicas van de 64 Kbps hasta 1.984 Kbps

En el servicio ofrecido por Telefónica existen dos modalidades de acceso, a través de líneas punto a punto desde las dependencias del cliente hasta el nodo de acceso a la red UNO. Y por línea ADSL, en este caso, la velocidad mínima que se puede contratar es de 256 Kbps.

10.5.4 ATM

Existen varios operadores que proporcionan acceso a sus redes WAN a través de la tecnología ATM. Las velocidades de acceso más comunes son a través de la interfaz eléctrica E3 a 34 Mbps o a través de la interfaz óptica STM-1 a 155 Mbps.

10.5.5 SERVICIO DE REDES PRIVADAS VIRTUALES

Este servicio se utiliza para la interconexión de las sedes de una empresa con necesidades de conectividad mallada. Normalmente se ofrece el servicio a través de una red de transporte IP del operador basada en la tecnología MPLS. El servicio de Redes Privadas Virtuales es uno de los servicios de datos más demandados en la actualidad.

Telefónica ofrece este servicio con el nombre de **VPN IP**. Sus principales características son:

- ✓ El acceso al servicio se puede realizar mediante diferentes opciones: Frame Relay, ATM, ADSL.
- ✓ Se puede combinar este servicio con DataInternet para proporcionar acceso a Internet a las sedes que forman parte de la VPN.
- ✓ Router en el domicilio del cliente que forma parte del servicio.
- ✓ Servicio gestionado, incluyendo el router.
- ✓ Los servicios Frame Relay y ATM soportan el establecimiento de Clases de Servicio para priorizar sus datos.
- ✓ El acceso ADSL está orientado a pequeñas oficinas donde no importa la simetría de las comunicaciones.
- ✓ Se puede configurar un backup por línea RDSI de hasta 256 Kbps.
- ✓ Las velocidades de acceso al servicio están sujetas a la tecnología de acceso utilizada:
  - Frame Relay: 64 Kbps, 128 Kbps, 192 Kbps, 256 Kbps, 384 Kbps, 512 Kbps y 2 Mbps
  - RDSI: 64 Kbps, 128 Kbps, 192 Kbps y 256 Kbps
  - ATM: 34 Mbps y 155 Mbps
  - ADSL: 1 Mbps/ 300 Kbps, 2 Mbps / 300 Kbps, 4 Mbps / 512 Kbps, 8 Mbps / 640 Kbps

Otro de los operadores que ofrece el servicio VPN es **COLT** a través de su producto **COLT IP VPN Corporate**, con las siguientes características:

- ✓ Existen varias posibilidades de contratación de este servicio:
  - IP VPN Corporate Plus
    Servicio IP VPN basado en MPLS, que se considera la mejor solución si se necesita conectividad totalmente mallada.
  - IP VPN Corporate Connect

Opción ofrecida para soluciones de conectividad en estrella. Las conexiones de las sedes a la red de COLT son a través de ATM o Frame Relay.

- IP VPN Corporate National
  Proporciona un método de acceso basado en ADSL o SDSL de bajo coste para oficinas pequeñas y medianas.

✓ Se ofrecen opciones de acceso remoto para teletrabajadores que permiten la conexión a la red IP VPN desde Internet o desde la red IP de otros operadores.

✓ Se ofrece también la posibilidad de acceso integrado a Internet a través del servicio IP VPN Corporate Plus o IP VPN Corporate Connect. El ancho de banda contratado para el acceso a Internet es independiente del ancho de banda contratado para el tráfico IP VPN.

✓ Las velocidades de conexión son: desde 64 Kbps hasta 155 Mbps para IP VPN Corporate Plus e IP VPN Corporate Connect. Y desde 64 Kbps hasta 4 Mbps para IP VPN Corporate Nacional.

ONO también proporciona este servicio con el nombre de **VPN MPLS**, que como su nombre indica proporciona VPN a sus clientes a través de su red IP multiservicio utilizando tecnología MPLS. Además ofrece cuatro clases de servicio para adaptarse a la prioridad de los datos.

Otros operadores que ofrecen este servicio son **Jazztel** (a través de su red privada multiservicio IP llamada I2P), **Ya.com** o **R** (también utiliza una red propia con tecnología MPLS).

10.5.6 SERVICIO DE CONEXIÓN DE REDES LAN

Servicio de datos que ofrece la posibilidad de interconexión de redes LAN situadas en ubicaciones diferentes como si fueran una única red.

Telefónica ofrece este servicio con el nombre de **MacroLAN** con las siguientes características:

✓ El servicio se proporciona a través de la Red de Tránsito Nacional de Telefónica basada en la tecnología MPLS y el acceso al mismo se lleva a cabo en la mayoría de los casos mediante fibra óptica.

✓ El acceso a la red de tránsito se lleva a cabo a través de un proveedor de acceso Ethernet en ámbito metropolitano (MAN), por ejemplo, el servicio MetroLAN. MetroLAN es un servicio que proporciona interconexión entre redes de área local situadas en distintos lugares dentro del ámbito metropolitano.

✓ Acceso Ethernet se lleva a cabo a 2, 10, 100 ó 1000 Mbps. Se proporcionan interfaces Ethernet, Fast Ethernet o Gigabit Ethernet.

- Puntos de acceso a la red de banda ancha:
  - En accesos de 10 y 100 Mbps la conexión a MetroLAN es un adaptador de fibra óptica a RJ-45, 10BaseT o 100BaseTX dependiendo de la velocidad de acceso.
  - En accesos de 1 Gbps, no es necesario un convertidor de medios ya que el PTR de MetroLAN es el punto de terminación de la fibra. Se ofrece una interfaz 1000BaseLX con conector SC/APC de fibra monomodo.
  - En accesos a 2 Mbps, la conexión entre el nodo de acceso y el cliente se hace por cable de cobre utilizando modulación SHDSL. Se proporciona una interfaz Ethernet RJ-45 10BaseT aunque la velocidad será de 2 Mbps.
- Se puede contratar un caudal de datos específico que puede ser inferior a la velocidad que soportan los sistemas de acceso al servicio. Por ejemplo:

Tabla 10.2

Velocidad de acceso MetroLAN	Caudal de acceso MetroLAN
2 Mbps	2
10 Mbps	1, 2, 3, 4, 5, 6, 7, 8, 9 y 10
100 Mbps	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 20, 30, 40, 50, 60, 70, 80, 90 y 100
1 Gbps	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 200, 300, 400, 500, 600, 700, 800, 900 y 1000

- Se definen varias clases de servicio contratables por el cliente: Plata (tráfico normal), Oro (tráfico crítico) y Multimedia (tráfico sensible al retardo como VoIP).
- El servicio MacroLAN permite además la utilización del servicio DataInternet para el acceso a Internet de la red del cliente, este servicio sólo se podrá activar en una de las sedes del servicio MacroLAN.

COLT ofrece también este servicio con el nombre de **COLT LANLink**. Hay tres opciones en función del ámbito geográfico:

- LANLink Metro, dentro de la misma ciudad, con velocidades de conexión entre 2 Mbps y 1 Gbps.
- LANLink National, dentro del mismo país.
- LANLink Internacional, entre países diferentes.

Si se utiliza tecnología de acceso DSL las velocidades están entre 256 Kbps y 4 Mbps.

ONO proporciona servicio de interconexión de redes LAN a través del producto **ONO LAN VPLS**, con velocidades de 100 Mbps y 1 Gbps y cuatro clases de servicio. **Jazztel** proporciona este servicio a través del producto **Trans Ethernet** entre 4 Mbps y 100 Mbps.

10.5.7 SERVICIO DE REDES PRIVADAS VIRTUALES

La mayor parte de las empresas ofrecen también servicios de conexión Internet a empresas, que se diferencian del acceso ADSL residencial en que este acceso se realiza a través de las redes propias que están continuamente monitorizadas y gestionadas proporcionando mejor calidad de conexión. Algunos ejemplos son:

Telefónica ofrece su servicio DataInternet que se puede contratar junto con otros servicios de datos como VPN IP o MacroLAN.

ONO ofrece accesos a Internet a empresas de hasta 10 Mbps con opción de tráfico simétrico o asimétrico. El servicio Internet garantizado proporciona conectividad a Internet de forma dedicada con un rango de velocidades desde 1 Mbps hasta 1 Gbps.

Ya.com ofrece también acceso corporativo a Internet a través de su red de datos conocida como Albura.

Jazztel ofrece su servicio Internet Directo con accesos a través de fibra óptica o radio (LMDS) y con velocidades desde 256 Kbps hasta 8 Mbps.

El operador de cable R proporciona acceso a Internet a través de fibra óptica en configuraciones asimétricas (velocidades de 6, 9 y 10 Mbps) y simétricas (velocidades de 1, 2, 4 y 6 Mbps).

El operador de cable Euskaltel, además del acceso a través de fibra, también proporciona acceso a Internet mediante la tecnología MAN inalámbrica WiMAX con velocidades de 300 Kbps/150 Kbps, 1 Mbps/600 Kbps y 2 Mbps/600 Kbps.

10.6 REDES DE COMUNICACIÓN VSAT

Los sistemas **VSAT (Very Small Aperture Terminal, Terminal de Apertura muy pequeña)** son sistemas de comunicación de datos vía satélite.

Aunque las comunicaciones vía satélite están enmarcadas dentro de las Telecomunicaciones propiamente dichas (y no de la Telemática), en este apartado se presenta un tipo de comunicaciones vía satélite que sustituye en determinadas circunstancias a las redes de datos estudiadas a lo largo del libro, las redes VSAT.

10.6.1 LOS SATÉLITES DE COMUNICACIÓN

Antes de estudiar las características principales de los sistemas VSAT se ofrece una visión general de uno de sus principales elementos, los satélites de comunicaciones.

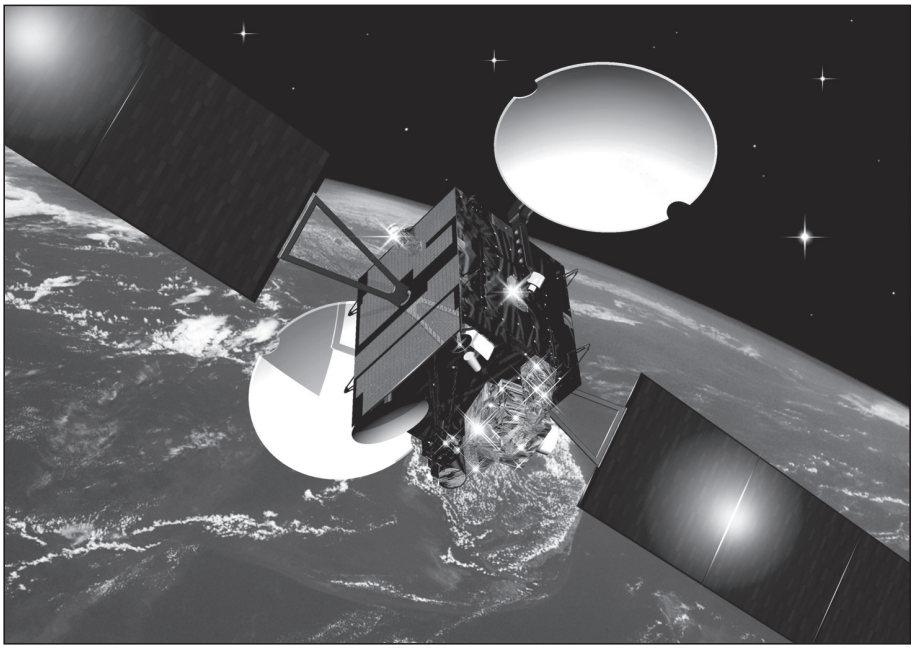


Figura 10.1. *Satélite de comunicaciones.*

Los satélites de comunicaciones son complejos sistemas repetidores situados a gran distancia de la superficie de la Tierra desde donde cubren una gran zona de cobertura. En función de la órbita en la que se sitúen, hay tres tipos de satélites:

- **GEO (Geostationary Earth Orbit).** Situados en órbitas geoestacionarias a una altura en torno a los 36.000 km. A esta altura el período de rotación es de 24 horas por lo que el satélite está siempre en el mismo lugar visto desde la Tierra. Su principal ventaja es que cubren áreas muy extensas aunque tienen el inconveniente de su elevada latencia debido a la gran distancia que recorre la señal.
- **MEO (Medium Earth Orbit).** Satélites situados a una distancia menor de la superficie terrestre, entre 10.000 y 20.000 km. Debido a ello su período de rotación no coincide con el de la Tierra por lo que su posición relativa respecto a ésta no es fija. Además, los satélites MEO ofrecen menor cobertura que los GEO y por lo tanto se necesitan varios satélites para cubrir una zona de gran extensión. Su latencia, lógicamente, es menor.
- **LEO (Low Earth Orbit).** Satélites de órbita baja. La distancia a la superficie terrestre está entre 500 Km y 5.000 por lo que su latencia es muy baja. Sin embargo, debido a su baja situación cubren un área reducida por lo que son necesarios muchos satélites (constelaciones) para cubrir un área extensa.

Las bandas de frecuencia utilizadas en comunicaciones por satélite son:

Tabla 10.3

Nombre	Frecuencias (GHz)	Banda descendente (GHz)	Banda ascendente (GHz)
C	4/6	3'7 – 4'2	5'9 – 6'4
Ku	11/14	10'7 – 12'7	14'0 – 14'5
Ka	20/30	17'7 – 21'7	27'5 – 30'5

Las transmisiones en banda C requieren antenas parabólicas relativamente grandes. Esta banda de frecuencias es más inmune a las condiciones atmosféricas pero sufre más interferencias terrestres. La banda Ku es la más susceptible a las condiciones atmosféricas.

10.6.2 SISTEMAS VSAT

Un sistema VSAT está basado en la comunicación de dos o más terminales terrestres a través de un satélite de comunicaciones de órbita geoestacionaria (GEO). La primera banda utilizada en comunicaciones VSAT fue la banda C, aunque actualmente se usa la Ku.

Tradicionalmente, los satélites se han empleado para radiodifusión y videodifusión en una topología punto multipunto. Sin embargo, la transmisión de datos es fundamentalmente bidireccional e interactiva. Los sistemas VSAT permiten comunicación bidireccional. El estándar utilizado que permite comunicación bidireccional se conoce como DVB-RCS.

Los sistemas VSAT se utilizan para proporcionar conectividad entre dos o más puntos, normalmente cuando los lugares que se desea conectar no tienen acceso a infraestructuras cableadas. Esto sucede en zonas alejadas de grandes núcleos urbanos o zonas de difícil acceso. También se utiliza para proporcionar conectividad a embarcaciones.

Además, los sistemas VSAT se emplean para proporcionar acceso a Internet a usuarios que, al igual que en el caso anterior, no tienen acceso a infraestructuras cableadas.

La principal desventaja es la latencia, es decir, el retardo de propagación de las señales debido a las grandes distancias que tienen que recorrer. Lógicamente también, se puede ver afectado por fenómenos atmosféricos que produzcan desvanecimientos de la señal.

Hay dos topologías en las que un sistema VSAT puede funcionar:

- **Bidireccional en estrella.** Es ideal para organizaciones que utilicen una estructura de procesamiento centralizada. Es decir, un gran número de sucursales que se comuniquen a menudo y en tiempo real con la estación central (como entidades financieras, puntos de venta remotos, sistemas SCADA...). Las comunicaciones se llevan a cabo a través de una estación maestra llamada hub. En esta configuración se proporcionan velocidades que van desde 64 Kbps hasta 2.048 Kbps.

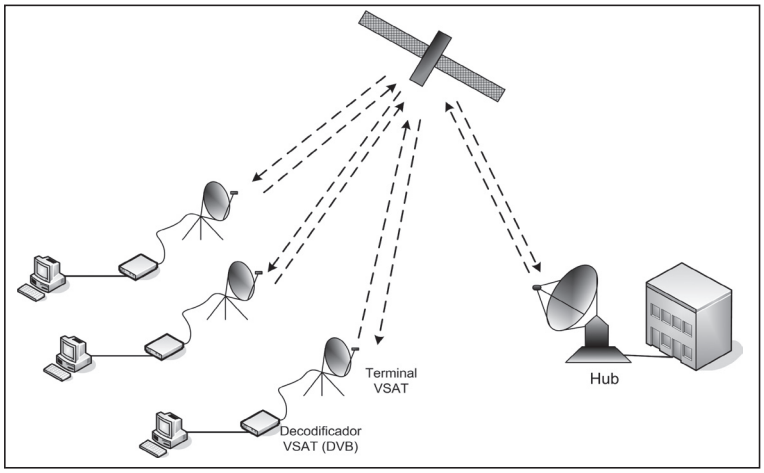


Figura 10.2. *VSAT en estrella.*

- **Sistemas mallados.** Utilizados en redes corporativas. Esta configuración ofrece comunicación directa de todos los nodos. La comunicación bidireccional se consigue mediante multiplexación por división en el tiempo (MDT). Se utiliza una frecuencia de transmisión que contiene varios canales, cada uno de ellos asignado a una estación receptora. En esta configuración se proporcionan velocidades entre 2 Mbps y 34 Mbps.

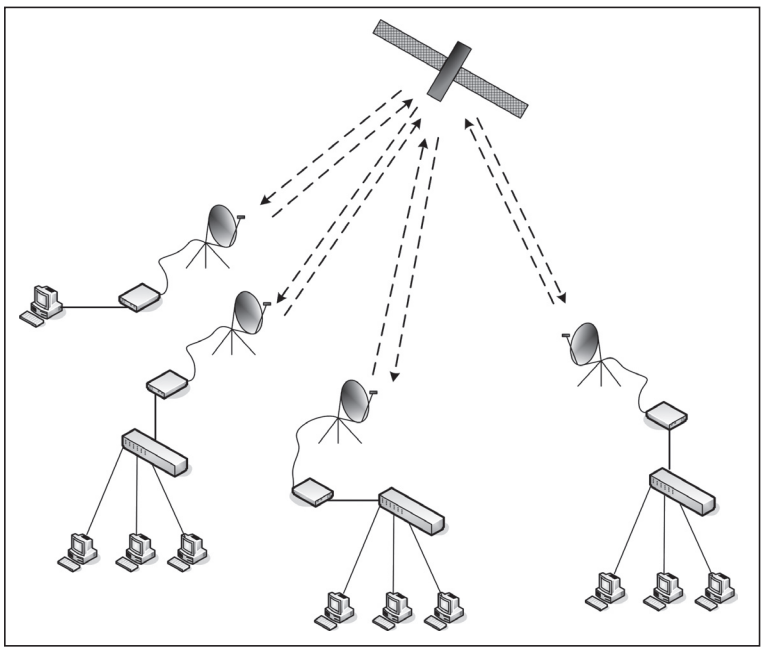


Figura 10.3. *Configuración en malla.*

El terminal VSAT consta de una antena parabólica de pequeño diámetro que oscila entre 0'5 y 3 metros dependiendo del nivel de señal, aunque los valores típicos están en torno a 1 metro.

Además, el terminal VSAT utiliza un dispositivo para decodificar la señal y proporcionar la señal adecuada a la instalación del usuario. Normalmente la conexión entre la antena parabólica y el dispositivo decodificador (también llamado módem DVB) se realiza por cable coaxial. Mientras que la conexión entre el decodificador y el equipamiento del cliente se hace por cable Ethernet RJ-45 o por cable USB.

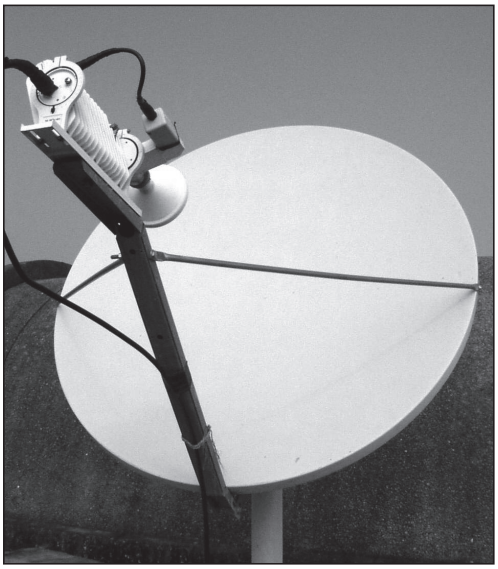


Figura 10.4. *Antena parabólica VSAT.*

10.6.3 SERVICIOS PROPORCIONADOS POR LOS SISTEMAS VSAT

Los principales servicios de datos proporcionados por los sistemas VSAT son:

- ✓ Conectividad entre redes locales distribuidas en diferentes localizaciones
- ✓ Conexión a Internet
- ✓ Servicios de videoconferencia
- ✓ Servicios VPN
- ✓ Servicios de Voz sobre IP (VoIP)
- ✓ Soporte para sistemas **SCADA (Supervisory Control and Data Adquisition, Control supervisor y adquisición de datos)**

NOTA 10.1

Los sistemas SCADA son soluciones para la adquisición de datos de un proceso con la finalidad de llevar a cabo su mantenimiento, gestión o supervisión. Cuando el sistema se encuentra en zonas aisladas o de difícil acceso se instala un sistema de adquisición de datos conectado a una antena VSAT para el envío de la información. Los sistemas SCADA son muy utilizados en aplicaciones de control de parámetros medioambientales.

En España, la sociedad HISPASAT es la encargada de proporcionar comunicaciones por satélite con cobertura nacional. Tiene operativos tres satélites: 1D, 1B

y 1C. También el tiene operativo el Amazonas para la zona de Sudamérica. Otros satélites que pertenecen a HISPASAT son Xtar-Eur y Spainsat utilizados para comunicaciones gubernamentales por satélite.

HISPASAT ofrece un servicio mayorista. Es decir, hay otras empresas proveedoras de servicios VSAT que lo hacen a través de HISPASAT. En total, operan más de 40 redes VSAT con un total de 6.000 terminales utilizando los satélites de HISPASAT.

Otro operador que proporciona servicios de satélite en Europa, entre ellos servicios VSAT, es ASTRA. ASTRA opera con 12 satélites geoestacionarios, que al igual que HISPASAT ofrece servicios como mayorista.

Un ejemplo de proveedor de servicios de telecomunicaciones que utiliza ASTRA es **YA.COM**. Su servicio se denomina Banda Ancha Satélite y ofrece un servicio de conexión unidireccional a Internet a través de ASTRA. Este servicio proporciona un canal de bajada (downstream) a través del satélite mientras que el canal de subida (upstream) se proporciona por una línea RTC. Se utiliza un módem DVB.

Las velocidades ofrecidas son de 512 Kbps para el producto Banda Ancha Sat Home, hasta 1 Mbps en el producto Banda Ancha Sat Pro. En todas las configuraciones, la velocidad de subida es la que proporciona una línea telefónica RTC, es decir, 56 Kbps.

Telefónica es otro proveedor de soluciones VSAT que utiliza en este caso los servicios de HISPASAT. Telefónica ofrece un servicio de Internet vía satélite bidireccional con unas velocidades de conexión que van desde 256K (bajada) / 128K (subida) del producto Básico, hasta 2 Mbps (bajada) / 300Kbps (subida) del producto Premium. Además, se puede elegir el acceso para un solo equipo (monopuesto) o para una red de área local (multipuesto).

RESUMEN DEL CAPÍTULO

En este capítulo se hace un repaso de los principales servicios de datos proporcionados por los sistemas telemáticos actualmente.

Después de un repaso a los servicios tradicionales como el sistema telegráfico o el FAX se ofrece una extensa visión de la evolución, gestión y arquitectura de Internet como el paradigma de los servicios telemáticos actuales.

Se repasan los principales servicios basados en Internet, especialmente el relacionado con el propio acceso a la red.

Otro de los sectores con mayor expansión es el dedicado a ofrecer servicios de conectividad a empresas. Aquí se cubren todos los servicios de datos más importantes en la actualidad.

Por último, se estudian los sistemas VSAT como una alternativa a la transmisión de datos vía satélite, utilizada en lugares donde no existen infraestructuras cableadas.

TEST DE CONOCIMIENTOS

1 El despegue definitivo del uso de Internet se produjo:
- **a)** Por la inversión económica de Estados Unidos.
- **b)** Por la implantación de la tecnología VSAT.
- **c)** Por la aparición del servicio Web.
- **d)** Por el cambio de IPv4 a IPv6.

2 El backbone de Internet está formado actualmente:
- **a)** Por la red NFSNET.
- **b)** Principalmente por la conexión de los IXP.
- **c)** Principalmente por la conexión de los ISP.
- **d)** Por un troncal de fibra óptica que conecta Europa y América.

3 Los IXP son:
- **a)** Infraestructuras que permiten la conexión de varios ISP.
- **b)** ISP de gran cobertura, normalmente internacional.
- **c)** Conexiones directas a Internet sin necesidad de ISP.
- **d)** Los antiguos ISP.

4 El organismo oficial encargado de la asignación del espacio de direcciones numéricas de Internet es:
- **a)** ICANN.
- **b)** ISOC.
- **c)** IETF.
- **d)** IANA.

5 Uno de los servicios utilizados en Internet es:
- **a)** El servicio de banca virtual.
- **b)** El servicio de comercio electrónico.
- **c)** El servicio de difusión de radio.
- **d)** Todas las anteriores son válidas.

6 Uno de los servicios de datos más demandados por las empresas en la actualidad:
- **a)** Servicio de Redes Privadas Virtuales.
- **b)** Servicio de conexión Frame Relay.
- **c)** Servicio de conexión X.25.
- **d)** Servicios de conexión punto a punto a baja velocidad.

7 La tecnología de acceso a Internet para clientes residenciales más extendida en España es:
- **a)** Las redes de televisión por cable.
- **b)** RDSI.
- **c)** ADSL.
- **d)** RTC.

8 Los sistemas VSAT utilizan satélites de tipo:
- **a)** GEO.
- **b)** MEO.
- **c)** LEO.
- **d)** Cualquiera de los anteriores.

9 Los sistemas VSAT utilizan para transmitir:
- **a)** La banda C.
- **b)** La banda Ku.
- **c)** La banda Ka.
- **d)** Cualquiera de las anteriores.

10 El acceso a Internet mediante VSAT unidireccional:
- **a)** No es posible.
- **b)** Es posible en modo broadcasting.
- **c)** Es posible informando a la compañía proveedora de las páginas que se quieren visitar.
- **d)** Es posible utilizando una línea RTC para el canal de subida.

Índice alfabético

D

E

Bibliografía

[RECO04]
Redes de computadores
José María Barceló Ordinas, Jordi Iñigo Griera, Ramón Martí Escalé, Enric Peig Olivé, Xavier Perramón Tornil
UOC, 2004

[TANE97]
Redes de computadoras
Andrew S. Tanenbaum
Prentice Hall, 1997, 3.ª ed.

[STAL00]
Comunicaciones y Redes de Computadores
William Stallings
Prentice Hall, 2000, 6.ª ed.

[FORO03]
Transmisión de Datos y Redes de Comunicaciones
Behrouz A. Forouzan
McGraw-Hill, 2002, 2.ª ed.

[HUID06]
Redes y Servicios de Telecomunicaciones
José Manuel Huidobro Moya
Paraninfo, 2006