

Tema 1 Redes de Comunicaciones de datos.

1. INTRODUCCIÓN.	3
2. REDES DE COMUNICACIONES.	3
2.1. CONCEPTOS SOBRE LA COMUNICACIÓN	3
2.1.1. <i>Emisor y Receptor</i>	5
2.1.2. <i>Canal y Señal</i>	5
2.1.3. <i>Código y Mensaje</i>	6
2.2. RED DE DATOS.	9
3. ESTANDARIZACIÓN DE REDES DE COMUNICACIONES.	11
3.1. ESTÁNDARES Y SISTEMAS ABIERTOS	11
3.2. ORGANISMOS DE ESTANDARIZACIÓN EN COMUNICACIONES	13
3.2.1. <i>ITU International Telecom Union</i>	14
3.2.2. <i>ISO International Standards Organization</i>	14
3.2.3. <i>ANSI (American National Standards Institute)</i>	15
3.2.4. <i>IEEE Institute of Electrical and Electronics Engineers</i>	15
3.2.5. <i>EIA Electronic Industries Alliance</i>	15
3.2.6. <i>TIA Telecommunications Industry Association</i>	15
3.3. ORGANISMOS DE ESTANDARIZACIÓN EN INTERNET	16
3.3.1. <i>ISOC Internet Society</i>	17
3.3.2. <i>IETF (Internet Engineering Task Force)</i>	17
3.3.3. <i>IANA Internet Assigned Numbers Authority</i>	17
3.3.4. <i>ICANN Internet Corporation for Assigned Names and Numbers</i>	18
3.3.5. <i>IAB Internet Architecture Board</i>	18
3.3.6. <i>W3C World Wide Web Consortium</i>	18
4. CLASIFICACIÓN DE REDES DE COMUNICACIONES.	19
4.1. SEGÚN LAS TECNOLOGÍAS DE TRANSMISIÓN.	19
4.1.1. <i>Redes de difusión.</i>	19
4.1.2. <i>Redes punto a punto.</i>	20
4.2. TOPOLOGÍAS EN REDES DE COMUNICACIONES.	21
4.2.1. <i>Topología en bus.</i>	21
4.2.2. <i>Topología en estrella.</i>	22
4.2.3. <i>Topología en anillo y doble anillo.</i>	23
4.2.4. <i>Topología en árbol.</i>	25
4.2.5. <i>Topología de interconexión total.</i>	27
4.2.6. <i>Topología irregular.</i>	27
4.2.7. <i>Topologías híbridas.</i>	28
4.3. SEGÚN LAS TECNOLOGÍAS DE CONMUTACIÓN.	28
4.3.1. <i>Red de conmutación de circuitos.</i>	29
4.3.2. <i>Red de conmutación de mensajes.</i>	30
4.3.3. <i>Red de conmutación de paquetes.</i>	31
4.4. CLASIFICACIÓN EN FUNCIÓN DE LA TITULARIDAD.	31
4.5. CLASIFICACIÓN EN FUNCIÓN DE LA ESCALA.	32
4.5.1. <i>Redes de área personal o PAN.</i>	32
4.5.2. <i>Redes de área local o LAN.</i>	33
4.5.3. <i>Redes de área de campus o CAN.</i>	35
4.5.4. <i>Redes de área metropolitana o MAN.</i>	36
4.5.5. <i>Redes de área extensa o WAN.</i>	37
4.6. CLASIFICACIÓN EN FUNCIÓN DEL MEDIO (GUIADO O INALÁMBRICO).	38
4.6.1. <i>Redes Cableadas</i>	38
4.6.2. <i>Redes Inalámbricas WLAN</i>	38
5. ARQUITECTURA DE RED DE COMUNICACIONES.	39
5.1. INTRODUCCIÓN	39
5.2. ARQUITECTURAS BASADAS EN CAPAS O NIVELES	41
5.2.1. <i>Interfaz.</i>	42
5.2.2. <i>Protocolo.</i>	42
5.2.3. <i>Arquitectura de red</i>	43

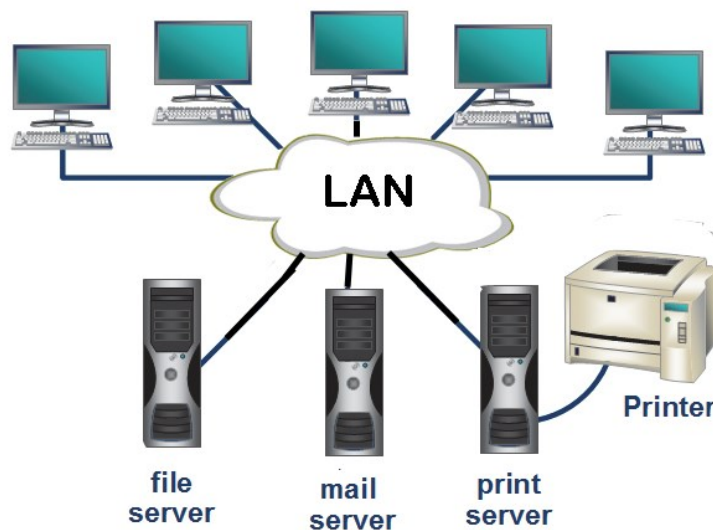
5.3. EL MODELO DE REFERENCIA OSI.....	43
5.3.1. <i>La capa física.</i>	44
5.3.2. <i>La capa de enlace de datos.</i>	45
5.3.3. <i>La capa de red.</i>	45
5.3.4. <i>La capa de transporte.</i>	46
5.3.5. <i>La capa de sesión.</i>	47
5.3.6. <i>La capa de presentación.</i>	47
5.3.7. <i>La capa de aplicación.</i>	47
5.3.8. <i>Transmisión de datos en el modelo OSI.</i>	48
5.4. LA ARQUITECTURA TCP/IP.	49
5.4.1. <i>La capa de Interred (capa de Internet).</i>	49
5.4.2. <i>La capa de Transporte.</i>	50
5.4.3. <i>La capa de Aplicación.</i>	50
5.4.4. <i>La capa host a red.</i>	50
6. LAS REDES DE ÁREA LOCAL.	50
6.1. CARACTERÍSTICAS DE UNA RED LOCAL.	50
6.2. VENTAJAS E INCONVENIENTES DE UNA RED LOCAL	52
6.3. APLICACIONES DE LAS REDES DE ÁREA LOCAL	54

1. Introducción.

En la actualidad, utilizamos las redes de comunicaciones en la vida diaria en multitud de ocasiones: cuando encendemos el receptor de televisión, hacemos una llamada de teléfono, escuchamos la radio, chateamos con el *smartphone*, o visitamos páginas Web.

Las redes de comunicaciones se pueden clasificar en función de algunas de sus características. Por ejemplo, la red de televisión o radio, son redes de comunicaciones al igual que la red telefónica, sin embargo, se diferencian en varios aspectos. Por ejemplo, la red telefónica permite la comunicación en ambos sentidos, mientras que las redes de radio y televisión sólo permiten la comunicación en un sentido, desde las estaciones de emisión a los receptores. En este ejemplo, hablamos de redes unidireccionales o de difusión para la televisión y la radio, mientras que consideramos a la red telefónica como una red de comunicaciones bidireccional.

En este primer tema del módulo, comenzaremos con los conceptos básicos sobre redes de comunicaciones. Veremos las redes de comunicación de datos, sus características fundamentales, los tipos y clasificación de redes de comunicación de datos, su arquitectura, y los estándares en redes.



Red de área local (Local Area Network)

De entre todas las redes de comunicaciones, en este módulo nos vamos a centrar en las "**redes de comunicación de datos**", y especialmente en las denominadas "**redes de área local**". Estudiaremos este tipo de redes, sus características fundamentales, ventajas e inconvenientes, tipos y componentes.

2. Redes de comunicaciones.

2.1. Conceptos sobre la comunicación

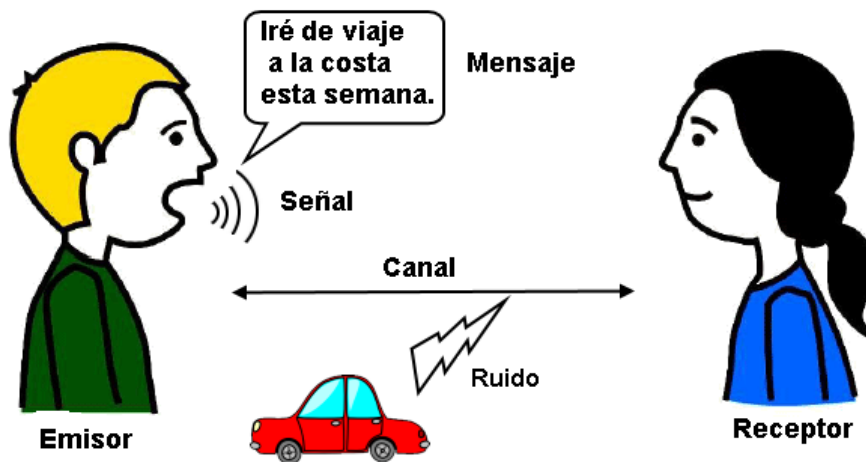
La **comunicación** consiste básicamente en el envío de un mensaje o información entre un agente que lo transmite y otro que lo recibe. Por ejemplo, cuando una persona habla con otra persona, le comunica un mensaje mediante la voz.

Son varios los **elementos que intervienen en una comunicación**:

- **Emisor** es quien envía el mensaje.
- **Receptor** es quien recibe el mensaje.
- **Mensaje** es la información a comunicar.

- **Canal** es el medio físico por el que viajan las señales que contienen el mensaje.
- **Señal** es la magnitud física que viaja por el canal conteniendo el mensaje.
- **Ruido** es cualquier elemento que afecta negativamente a las señales que viajan por el canal.
- **Código** es el sistema mediante el que el mensaje se representa mediante señales que pueden viajar por el canal.

Un caso de comunicación en el que todos estamos familiarizados es la comunicación verbal entre personas.



Por ejemplo: una persona le dice a otra persona que el fin de semana irá de viaje a la costa en una conversación. En este tipo de comunicación los elementos serían:

- **Emisor**: la persona que hará el viaje y desea comunicarlo a su interlocutor.
- **Receptor**: la persona a quien el emisor desea comunicar que desea ir de viaje.
- **Mensaje**: la idea a comunicar sería "iré de viaje a la costa este fin de semana".
- **Canal**: dado que se trata de una conversación, el canal por el que viajan las señales es el aire que rellena el espacio que separa los dos interlocutores que están conversando.
- **Señal**: en este caso, la señal que viaja del emisor al receptor es el sonido, que atraviesa el espacio que los separa a través del aire.
- **Ruido**: cualquier sonido que afecte a la correcta recepción de la voz. Por ejemplo, si la conversación se realiza en la calle, y un vehículo pasa cerca de donde las personas están hablando, el sonido de la voz del emisor se mezclará con el del vehículo y el receptor podría no comprender bien lo que le está diciendo el emisor.
- **Código**: el mensaje "iré de viaje a la costa este fin de semana" se expresa mediante la voz con señales acústicas que pueden viajar a través del medio que separa a los interlocutores. El código que nos permite expresar ideas mediante sonidos podría denominarse "lenguaje hablado". Ambos interlocutores deben conocer el código utilizado para que la comunicación sea posible, es decir, ambos deben hablar el mismo idioma. El código también debe adecuarse al canal de comunicación, por ejemplo, si el receptor es sordo, no podrá escuchar la voz del emisor, por lo que el código a utilizar en este caso sería cualquiera de los lenguajes de signos que existen en el mundo que expresan mensajes mediante señales visuales.

Actividades propuestas:

- 1) Identifica los elementos de la comunicación mediante el correo tradicional.

2) Identifica los elementos de la comunicación mediante el servicio de mensajería SMS.

Para que exista una comunicación efectiva es preciso que el receptor reciba las señales y sea capaz de extraer el mensaje correctamente. No hay comunicación si las señales no son recibidas o llegan tan alteradas que no es posible extraer el mensaje, por ejemplo a causa del ruido, o de encontrarse muy lejos del emisor. Tampoco existe comunicación si el código utilizado por el emisor no es comprendido por el receptor, por ejemplo cuando el receptor no entiende el código utilizado (le hablan en otro idioma).

2.1.1. Emisor y Receptor

Se suele definir al **emisor** como el elemento de la comunicación que desea enviar un mensaje, y el **receptor** el agente a quien va destinado el mensaje. Las particularidades de emisores y receptores pueden dar lugar a diversos tipos de comunicaciones.

En ocasiones los papeles de emisor y receptor son intercambiables en una comunicación como por ejemplo en una conversación entre dos personas. Cuando dos personas conversan, habitualmente se turnan para hablar y escuchar. En otros casos, el emisor es el único que envía mensajes y el receptor es incapaz de enviar mensajes, por ejemplo en una conferencia en la que sólo habla el ponente, y los asistentes no deberían interrumpir.

También se puede caracterizar la comunicación por el número de emisores y receptores. Por ejemplo en el caso de una conversación entre dos personas la comunicación es uno a uno, pero en el caso de la conferencia, la comunicación es uno a muchos o de difusión.

También se puede diferenciar las comunicaciones por el tipo de emisores y receptores. En este módulo nos centraremos en estudiar los casos en los que tanto emisor como receptor son máquinas, más concretamente, equipos informáticos.

2.1.2. Canal y Señal

El canal es el medio por el que viaja la señal entre los interlocutores. La **señal** es una magnitud física que es capaz de viajar desde el emisor hasta el receptor atravesando el medio.

El **canal** debe ser el adecuado para que las señales puedan llegar al receptor, y las señales deben ser adecuadas para que puedan viajar por el canal hasta el receptor con suficiente calidad para ser comprendidas correctamente.

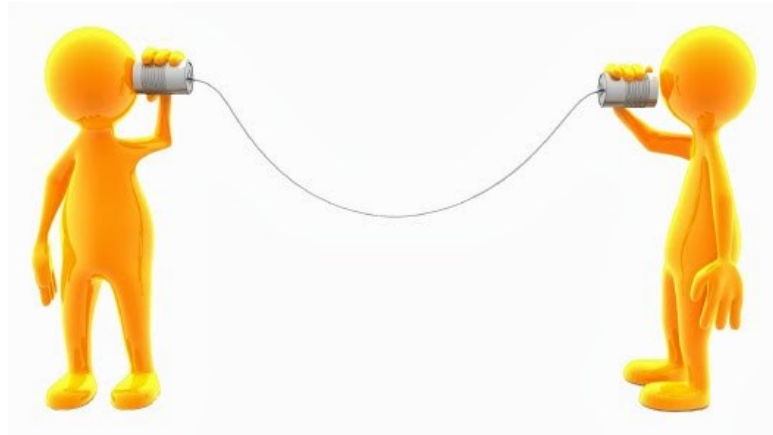
Por ejemplo, en una conversación entre dos personas, el canal es el espacio que los separa, y la señal el sonido de la voz que puede viajar de emisor a receptor a través del aire que rellena el espacio que los separa.



Cuando emisor y receptor están a cierta distancia, no se puede utilizar la voz para realizar la comunicación ya que el receptor no podría la voz del emisor a gran distancia por mucho que gritara.

Incluso cuando la distancia es relativamente corta, la comunicación de voz puede hacerse imposible cuando el ruido presente en el ambiente es elevado.

En estas circunstancias se pueden utilizar canales que permiten llevar la señal de la voz a más distancia y protegida del ruido.



Para conversaciones donde la voz no llega puede usarse un canal como en el teléfono de hilo.

Incluso cuando utilizamos canales para la comunicación, las señales tienen otras limitaciones. Por ejemplo, el sonido se atenúa enormemente (reduce su potencia) en relación a la distancia, por lo que no es un tipo de señal adecuada para comunicaciones de más de una decena de metros.

Si queremos mantener una comunicación de voz con una persona situada a gran distancia transformamos las señales de sonido de la voz en señales eléctricas que viajan a través de cables conductores ya que nos permite cubrir grandes distancias. De esta manera funciona el teléfono. También podemos usar señales ópticas circulando por medios adecuados como fibra óptica para comunicaciones de larga distancia.

Cada canal de comunicación puede transmitir bien unos tipos de señales, mientras que otros tipos de señales no las transmite en absoluto, o lo hace con mucha dificultad. Por ejemplo, un cable de teléfono puede transmitir señales eléctricas pero no transmitirá señales de luz, mientras que un cable de fibra óptica transmite señales de luz, pero actúa como aislante cuando queremos enviar señales eléctricas.

El diseño de los sistemas de comunicaciones debe tener en cuenta estas circunstancias para garantizar que las señales lleguen correctamente al receptor desde el emisor, con la suficiente calidad para que pueda extraer correctamente el mensaje.

2.1.3. Código y Mensaje

Ya hemos visto que las señales deben llegar al receptor a través del canal, pero sólo con recibir señales no se puede hablar de que exista una comunicación. Para que una comunicación sea efectiva, es preciso que el receptor reciba el mensaje que le envía el emisor, y para ello debe extraer el mensaje de las señales.

Ejemplo: cuando hablamos con una persona cara a cara, existe una gran cantidad de información transmitida mediante gestos y tonos de voz (lenguaje no verbal), que cuando la comunicación se realiza de forma escrita, por ejemplo mediante un chat, deben representarse mediante lo que se denominan "emojiconos", que son la forma de expresar información emocional mediante textos o imágenes. Si una parte importante del mensaje reside en estas formas de comunicación que se pierden en el canal de transmisión, la comunicación no es adecuada.

El mensaje a enviar se codifica en señales para que pueda viajar por el canal hasta el receptor. Por ejemplo, el mensaje se puede expresar mediante sonidos con la voz en una conversación, pero cuando no es posible enviar sonidos al receptor, podemos usar la escritura para expresar el mensaje y enviarlo por un canal que permita que las señales escritas lleguen al receptor, por ejemplo mediante el sistema de correos.

De esta manera, para que exista una comunicación, el emisor deberá **codificar** el mensaje antes de enviarlo por el canal y el receptor deberá **decodificar** las señales que recibe por el canal para extraer el mensaje enviado.

Para codificar y decodificar un mensaje se emplea un "**código**" que consiste en una serie señales a utilizar y las reglas que deben utilizarse para que pueda expresarse el mensaje mediante estas señales.

Las señales utilizadas en el código dependerán del medio empleado para que lleguen al receptor. La comunicación que realizamos con más naturalidad consiste en expresar ideas mediante sonidos en lo que llamamos el "lenguaje hablado". En este caso las señales consisten en sonidos que a nivel de lenguaje consisten en fonemas sin significado por sí mismos, que son utilizados para construir palabras con las que se construyen oraciones que son las que expresan mensajes.

Por ejemplo, en este texto se emplean letras del alfabeto latino, que provienen de señales diseñadas para ser utilizadas mediante trazos en papel, pergamino, arena o en cualquier otro soporte que lo permita.

NOMBRE Y SIGNIFICADO	FENICIO ANT.	FENICIO	GRIEGO ANT.	GRIEGO	LATÍN
ALEF buey					A
BETH construcción					B
GIMEL esquina					G
MEM agua					M
NUUN cobra					N
AYIN ojo					O
RESH cabeza					R
TAU cruz					T
SHIN diente					S

El alfabeto latino es una evolución de otros alfabetos utilizados más antiguamente

En las comunicaciones se utilizan códigos adaptados al medio de transmisión usado. El sistema telegráfico más empleado, consistía en dos hilos conductores de la electricidad a través de los que se podía enviar una corriente eléctrica. El código empleado en este sistema de comunicación podía tener por lo tanto dos valores posibles (envío corriente/no envío corriente) y acabó evolucionando en lo que se conoce como **Código Morse**.

A	.-	J	.-.-.-	S	...	2	..-.-
B	K	-.-	T	-	3	...--
C	L	..-..	U	...	4-
D	---	M	--	V	...-	5
E	.	N	--.	W	..--	6	-....
F	...-	O	---	X	...-	7	-....
G	---	P	..-..	Y	..-.-	8	-----
H	Q	---.	Z	---.	9	-----
I	..	R	...-	1	0	-----

Código Morse utilizado en telegrafía.

En este módulo, nos interesa estudiar las comunicaciones entre ordenadores o sistemas informáticos, que debido a su naturaleza utiliza un sistema de codificación especial que nos resulta extraño a las personas. En lugar de utilizar decenas de símbolos distintos, los

equipos informáticos trabajan internamente con símbolos que disponen únicamente de dos valores. Mientras el alfabeto español es una variante del alfabeto latino que dispone de 27 letras, el alfabeto de los equipos informáticos se denomina **binario**, y sólo dispone de dos "letras".

A una letra del alfabeto de los ordenadores se le denomina **"bit"** y sus dos posibles valores se suelen denominar como "0" y "1". Con el valor de un bit es posible expresar datos sencillos con tan solo dos posibles valores como por ejemplo: Si/No, Verdadero/Falso, Casado/Soltero. Pero con un bit no es posible expresar mensajes completos.

Nota: La unidad de medida de capacidad de información en los equipos informáticos es el **byte**, denominado también carácter o palabra. Un byte está compuesto por 8 bits. El origen de esta forma de expresar la cantidad de información manejada en equipos informáticos se debe a la arquitectura de los microprocesadores, más concretamente al tamaño en bits de sus registros, que es lo que delimita la cantidad de información que lee/guarda en memoria en un solo ciclo de reloj. Por lo tanto, los equipos informáticos en los que se basa la definición tenían registros de 8 bits (un byte), y ese era el tamaño de palabra del microprocesador. Los tamaños de los registros han crecido en múltiplos de 8 bits por lo que se sigue utilizando dicha nomenclatura. También se ha denominado "carácter" al byte, ya que con 8 bits puede expresarse una letra del alfabeto o un símbolo del lenguaje mediante el código ASCII.

En especial, se ha desarrollado un código que nos permite expresar símbolos del alfabeto latino junto a otros símbolos de formato y control, en secuencias de varios bits.

El **código ASCII** (*American Standard Code for Information Interchange* - Código Estándar Estadounidense para el Intercambio de Información) inicialmente expresaba mediante 7 bits un total de 128 símbolos entre los que se encuentran todos los caracteres del alfabeto latino inglés en mayúsculas y minúsculas, números, y símbolos comunes (matemáticos, de puntuación, etc...). El código ASCII también dispone de varios valores con significado especial que permiten controlar una comunicación o dar formato a un texto, que se denominan caracteres no imprimibles o caracteres de control.

Caracteres de control ASCII				Caracteres ASCII imprimibles												ASCII extendido											
DEC	HEX	Símbolo ASCII		DEC	HEX	Símbolo	DEC	HEX	Símbolo	DEC	HEX	Símbolo	DEC	HEX	Símbolo	DEC	HEX	Símbolo	DEC	HEX	Símbolo	DEC	HEX	Símbolo	DEC	HEX	Símbolo
00	00h	NULL		(carácter nulo)	32	20h	espacio	64	40h	@	96	60h	`	128	80h	Ç	160	A0h	à	192	C0h	À	224	E0h	Ó		
01	01h	SOH		(inicio encabezado)	33	21h	!	65	41h	A	97	61h	a	129	81h	Ù	161	A1h	á	193	C1h	Á	225	E1h	Ô		
02	02h	STX		(inicio texto)	34	22h	"	66	42h	B	98	62h	b	130	82h	Ú	162	A2h	â	194	C2h	Â	226	E2h	Õ		
03	03h	ETX		(fin de texto)	35	23h	#	67	43h	C	99	63h	c	131	83h	Û	163	A3h	ã	195	C3h	Ã	227	E3h	Ö		
04	04h	EOT		(fin transmisión)	36	24h	\$	68	44h	D	100	64h	d	132	84h	Ü	164	A4h	ä	196	C4h	Ä	228	E4h	Ø		
05	05h	ENQ		(enquiry)	37	25h	%	69	45h	E	101	65h	e	133	85h	Ý	165	A5h	å	197	C5h	Å	229	E5h	Ù		
06	06h	ACK		(acknowledgement)	38	26h	&	70	46h	F	102	66h	f	134	86h	ÿ	166	A6h	ä	198	C6h	Ö	230	E6h	Ú		
07	07h	BEL		(timbre)	39	27h	'	71	47h	G	103	67h	g	135	87h	ÿ	167	A7h	ö	199	C7h	Û	231	E7h	Û		
08	08h	BS		(retroceso)	40	28h	(72	48h	H	104	68h	h	136	88h	ÿ	168	A8h	ø	200	C8h	Ü	232	E8h	Ü		
09	09h	HT		(tab horizontal)	41	29h)	73	49h	I	105	69h	i	137	89h	ÿ	169	A9h	º	201	C9h	Ý	233	E9h	Ý		
10	0Ah	LF		(salto de línea)	42	2Ah	,	74	4Ah	J	106	6Ah	j	138	8Ah	ÿ	170	AAh	º	202	CAh	Þ	234	EAh	Þ		
11	0Bh	VT		(tab vertical)	43	2Bh	+	75	4Bh	K	107	6Bh	k	139	8Bh	ÿ	171	ABh	¼	203	CBh	ß	235	EBh	ß		
12	0Ch	FF		(form feed)	44	2Ch	=	76	4Ch	L	108	6Ch	l	140	8Ch	ÿ	172	ACH	½	204	CDh	ä	236	ECh	ä		
13	0Dh	CR		(retorno de carro)	45	2Dh	-	77	4Dh	M	109	6Dh	m	141	8Dh	ÿ	173	ADh	¾	205	CDh	å	237	EDh	å		
14	0Eh	SO		(shift out)	46	2Eh	.	78	4Eh	N	110	6Eh	n	142	8Eh	ÿ	174	AEh	¸	206	CEh	æ	238	EEh	æ		
15	0Fh	SI		(shift in)	47	2Fh	:	79	4Fh	O	111	6Fh	o	143	8Fh	ÿ	175	AFh	¸	207	CFh	ç	239	EFh	ç		
16	10h	DLE		(data link escape)	48	30h	/	80	50h	P	112	70h	p	144	90h	ÿ	176	B0h	¸	208	D0h	ø	240	F0h			
17	11h	DC1		(device control 1)	49	31h	1	81	51h	Q	113	71h	q	145	91h	ÿ	177	B1h	¸	209	D1h	ø	241	F1h	±		
18	12h	DC2		(device control 2)	50	32h	2	82	52h	R	114	72h	r	146	92h	ÿ	178	B2h	¸	210	D2h	ø	242	F2h	±		
19	13h	DC3		(device control 3)	51	33h	3	83	53h	S	115	73h	s	147	93h	ÿ	179	B3h	¸	211	D3h	ø	243	F3h	±		
20	14h	DC4		(device control 4)	52	34h	4	84	54h	T	116	74h	t	148	94h	ÿ	180	B4h	¸	212	D4h	ø	244	F4h	±		
21	15h	NAK		(negative acknowledge)	53	35h	5	85	55h	U	117	75h	u	149	95h	ÿ	181	B5h	¸	213	D5h	ø	245	F5h	±		
22	16h	SYN		(synchronous idle)	54	36h	6	86	56h	V	118	76h	v	150	96h	ÿ	182	B6h	¸	214	D6h	ø	246	F6h	±		
23	17h	ETB		(end of trans. block)	55	37h	7	87	57h	W	119	77h	w	151	97h	ÿ	183	B7h	¸	215	D7h	ø	247	F7h	±		
24	18h	CAN		(cancel)	56	38h	8	88	58h	X	120	78h	x	152	98h	ÿ	184	B8h	¸	216	D8h	ø	248	F8h	±		
25	19h	EM		(end of medium)	57	39h	9	89	59h	Y	121	79h	y	153	99h	ÿ	185	B9h	¸	217	D9h	ø	249	F9h	±		
26	1Ah	SUB		(substitute)	58	3Ah	:	90	5Ah	Z	122	7Ah	z	154	9Ah	ÿ	186	BAh	¸	218	DAh	ø	250	FAh	±		
27	1Bh	ESC		(escape)	59	3Bh	;	91	5Bh	[123	7Bh	{	155	9Bh	ÿ	187	BBh	¸	219	DBh	ø	251	FBh	±		
28	1Ch	FS		(file separator)	60	3Ch	<	92	5Ch	\	124	7Ch		156	9Ch	ÿ	188	BCh	¸	220	DCh	ø	252	FCh	±		
29	1Dh	GS		(group separator)	61	3Dh	=	93	5Dh]	125	7Dh	}	157	9Dh	ÿ	189	BDh	¸	221	DDh	ø	253	FDh	±		
30	1Eh	RS		(record separator)	62	3Eh	>	94	5Eh	^	126	7Eh	~	158	9Eh	ÿ	190	BEh	¸	222	DEh	ø	254	FEh	±		
31	1Fh	US		(unit separator)	63	3Fh	?	95	5Fh	_				159	9Fh	ÿ	191	BFh	¸	223	DFh	ø	255	FFh	±		
127	20h	DEL		(delete)																							

Tabla de valores ASCII

En el código ASCII, a cada símbolo se le asigna un número que es expresado en código binario. Por ejemplo la letra "A" tiene asignado el número "65", lo que corresponde en binario de 8 bits a "01000001". También se suele expresar el número asociado al símbolo ASCII en la numeración hexadecimal, que es mucho más cercana a la máquina que la numeración decimal. En el caso de la letra "A", el 65 en decimal se expresaría como "41 en hexadecimal", o abreviadamente "41h".

Cuando se generalizó el uso del código ASCII en el resto de países, se necesitó codificar símbolos que no existen en el alfabeto inglés (como por ejemplo la ñ), y para ello se amplió el código ASCII con 128 caracteres más, pasando a ocupar 8 bits cada símbolo. Al código ASCII de 8 bits se denomina "código ASCII extendido".

El código ASCII es muy utilizado en todo el mundo, pero sólo sirve para expresar caracteres del alfabeto latino, no sirve para otros símbolos como los utilizados en la lengua árabe, china, hebrea, etc....

Existe un estándar de codificación que permite expresar en un sistema informático todos estos símbolos e incluso los correspondientes a lenguas muertas que ya no se utilizan. Se trata de Unicode.

"**Unicode** es un estándar de codificación de caracteres diseñado para facilitar el tratamiento informático, transmisión y visualización de textos de múltiples lenguajes y disciplinas técnicas, además de textos clásicos de lenguas muertas. El término Unicode proviene de los tres objetivos perseguidos: universalidad, uniformidad y unicidad" (Definición de la Wikipedia)

Los estándares Unicode son conocidos como **UTF** (*Unicode Transformation Format*) junto con el número de bits a los que está orientada la codificación. Por ejemplo, **UTF-8** es el código Unicode orientado a grupos de 8 bits y compatible con el código ASCII estándar US (el ASCII de 7 bits). Sin embargo, a diferencia del código ASCII, el código UTF-8 es de longitud variable, pudiendo llegar a ocupar hasta cuatro bytes (32 bits). De esta forma, **UTF-8** puede representar las decenas de miles de símbolos que contiene Unicode. También están definidos en Unicode UTF-16 (de tamaño variable) y UTF-32 (de tamaño fijo a 32 bits).

Nota: Los códigos ASCII y Unicode, son utilizados para expresar la información en equipos informáticos, y así es como se almacena, o circula entre sus componentes separados por distancias cortas (unos centímetros). Sin embargo, cuando enviamos la información a distancias mayores (superiores a unos 10 metros), los códigos utilizados en los ordenadores no son adecuados, por lo que se diseñan códigos que permitan mantener una comunicación a largas distancias con la menor cantidad de problemas posible. Por ello, es habitual que los equipos informáticos codifiquen la información binaria de manera específica para el medio por el que va a viajar el mensaje a la hora de transmitirla.

El mensaje a transmitir se codifica para que pueda ser enviado hasta el receptor. En los equipos informáticos, la información se compone de bits, y el código ASCII o Unicode nos permite expresar símbolos con esos bits. Por lo tanto, en una comunicación mediante equipos informáticos la primera codificación consiste en expresar el mensaje en bits.

Cuando enviamos un mensaje chat mediante un smartphone, lo primero que hacemos es escribir el mensaje mediante el teclado, y el dispositivo codifica las letras en símbolos binarios, por ejemplo mediante el código ASCII. La secuencia de bits que compone el mensaje codificado en ASCII, debe ser enviada al receptor mediante señales de microondas. Para ello, el smartphone usa un estándar de comunicación que establece cómo se representa la información binaria mediante señales de microondas y codifica los bits del mensaje de esa manera. La red de telefonía móvil recoge el mensaje y lo transmite hasta que llega al receptor. El smartphone del receptor recibe la señal de microondas y decodifica los bits que contiene. A continuación muestra los caracteres ASCII que corresponden a esos bits en la pantalla, y así la persona que recibe el mensaje puede leerlo. Vemos como el proceso de comunicación mediante equipos informáticos conlleva habitualmente varias codificaciones y decodificaciones para que el mensaje llegue correctamente a su receptor.

2.2. Red de datos.

En la actualidad, podemos comunicarnos con personas situadas en cualquier parte del mundo. Esto es posible gracias a unos dispositivos que recogen el mensaje del emisor y lo van reenviando de unos a otros hasta que llega al destinatario.

La **red de comunicaciones** se podría definir como todos los dispositivos y elementos que nos permite comunicarnos. Por ejemplo, la red telefónica nos permite comunicarnos

mediante la voz con cualquier persona del mundo que tenga acceso a un teléfono. Dado que es imposible que exista un canal, cable, o línea de comunicaciones para cada posible comunicación, se utiliza una la red de telefonía, compuesta por una gran cantidad de centralitas de conmutación, líneas de comunicaciones, y dispositivos, que nos permite hablar con otras personas.

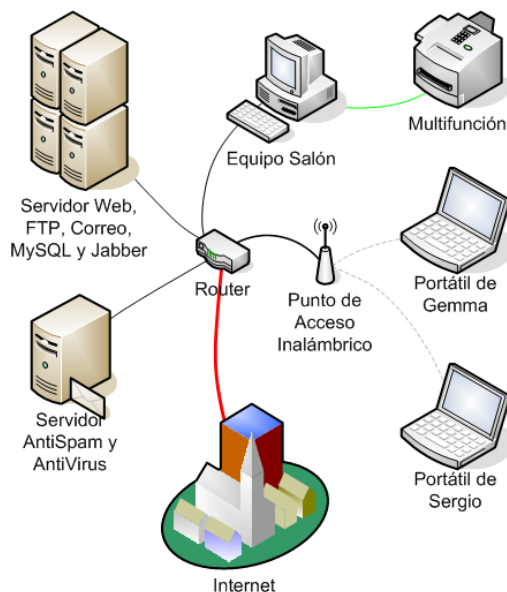


Sin una red de comunicaciones, debemos usar un canal distinto para cada comunicación.

Redes de comunicaciones son por ejemplo: la red telegráfica, la red telefónica, el servicio postal, Internet. En este módulo tenemos como objetivo el estudio de las **redes de comunicaciones de datos** que son aquellas en las que tanto el emisor como el receptor son equipos informáticos. También se denominan **redes de datos**, redes informáticas, o redes de ordenadores.

Las redes de datos pueden comunicar multitud de equipos informáticos de muy diversos tipos: Entre los más comunes, encontramos estaciones de sobremesa (ordenadores personales), ordenadores portátiles, smartphones, impresoras, servidores de red, etc..

Ya hemos visto cómo el código binario es el lenguaje natural de los ordenadores o equipos informáticos. Por lo tanto, las redes de datos transmiten mensajes binarios entre los distintos dispositivos o estaciones que actúan como emisores/receptores.



Red de datos en una vivienda.

A parte de enviar mensajes entre los dispositivos, la gran utilidad de las redes de datos consiste en la posibilidad de compartir datos, dispositivos y servicios entre todos los equipos

que estén conectados. Para ello es preciso que los equipos conectados a la red dispongan de sistemas operativos que le proporcionen dichas funcionalidades.

En una red de datos podemos compartir:

- Datos o información: Como por ejemplo los teléfonos de todos los clientes de una empresa pueden ser consultados y actualizados por cualquier trabajador usando la red de datos. Los apuntes de clase compartidos mediante la red del aula podría ser otro ejemplo.
- Recursos: Componentes o dispositivos tales como impresoras, potencia de cálculo, capacidad gráfica, escaners, líneas de comunicaciones, etc...
- Servicios: tales como chat, streaming de audio o vídeo, juegos, correo electrónico, autoconfiguración de dispositivos, autenticación, seguridad, y otros...

3. Estandarización de redes de comunicaciones.

En la industria en general, es de vital importancia la estandarización. Resulta evidente que si cada fabricante define sus propios tipos de tornillos, sistemas de conexión a la red eléctrica, etc., podemos encontrarnos con gran cantidad de problemas, e incluso con la imposibilidad de operar y mantener esos dispositivos de forma adecuada.

Los estándares ofrecen a las empresas y a los clientes la garantía de que dos dispositivos destinados para la misma tarea, fabricados en distintos países, pero cumpliendo las normas vigente en el país donde se comercialicen, podrán ser utilizados de forma similar y sin costos inesperados.

3.1. Estándares y Sistemas Abiertos

En la industria podemos encontrar dos tipos de estándares. Los estándares que son dictados por organismos de estandarización competentes, se denominan **estándares de derecho** “*de iure*” (“de jure”). En mercados dinámicos como los tecnológicos, en ocasiones los avances van por delante de los organismos de estandarización. Puede ocurrir que un determinado fabricante desarrolle una nueva tecnología, o producto tecnológico para el que no existe estándar todavía. Si esos productos se comercializan y tienen cierta aceptación, otros fabricantes pueden “copiar” la tecnología, con el objetivo de ofrecer productos similares que además puedan operar con los del fabricante original, o con sus accesorios. Estos productos que “adoptan” las especificaciones del fabricante original se comercializan con más facilidad al ser ya conocidos por los clientes los modos en que funciona y poder integrarse con los adquiridos a otros fabricantes. A estos estándares que aparecen en el mercado sin que un organismo los establezca, se les denomina **estándares de hecho** “*de facto*”.

En ocasiones los estándares “de facto” acaban siendo plasmados en estándares “de iure” cuando un organismo de estandarización acepta su amplia utilización en el mercado y decide plasmarlo en una norma.



Terminal DEC VT-100 (izquierda) y CIT-101, un clon fabricado por C. ITOH en Japón

Existen muchos motivos por los cuales aparecen estándares de facto. En ocasiones se deben a la innovación de una pequeña empresa que va muy por delante de los burocráticos

organismos de estandarización. Como ejemplo de estos casos tenemos los terminales VT100 fabricados por Digital Equipment Corporation (DEC), cuyo modo de comunicación ha sido adoptado por muchos otros terminales y aplicaciones de terminal.



Modelo Smartmodem 300 de Hayes, cuyo modo de configuración se convirtió en estándar

Otro ejemplo lo tenemos en el lenguaje de comandos para operación y configuración de los módems Hayes Smartmodem 300 baudios, que fueron adoptados y ampliados por los demás fabricantes de módems RTB.

Existen organismos de estandarización formados para el desarrollo y normalización de una determinada tecnología, para garantizar de este modo la interoperatividad de los dispositivos. Por ejemplo el “DVD Forum”, compuesto por fabricantes de dispositivos y aplicaciones, es responsable de las especificaciones oficiales del formato DVD, publicándolas en formato libro.



IBM PC original (izquierda) y “clónico” fabricado por Leading Edge

Un caso relevante lo podemos encontrar en el IBM PC. A principios de los años 80, IBM lanzó un modelo de ordenador “personal” que obtuvo bastante éxito. El resto de fabricantes aprovecharon para subirse al carro del ordenador personal, fabricando dispositivos que eran “compatibles” con el IBM PC, o también denominados “clónicos”. En un ordenador “clónico” funcionan las mismas aplicaciones que en un IBM PC original, e incluso admite la conexión de componentes hardware, originales de IBM o “compatibles”. De este modo, sin proponérselo, IBM había creado un estándar de ordenador personal que fue adoptado por la industria, y que luego ha evolucionado de manera independiente a su creador.

En otros casos pueden aparecer como el resultado de una asociación de fabricantes que se unen para mejorar o implantar mejoras en determinadas tecnologías. Por ejemplo VESA, Video Electronics Standards Association (Asociación para estándares electrónicos y de video) es una asociación internacional de fabricantes de electrónica que se fundó para desarrollar estándares para la fabricación de pantallas de video con más resolución y colores que los implementados en la interfaz gráfica VGA de IBM.

Otro ejemplo: Wi-Fi, (Wireless Fidelity), marca de la Wi-Fi Alliance que garantiza que los equipos basados en el estándar de comunicación inalámbrica IEEE 802.11 cumplen las especificaciones y son interoperables, independientemente del fabricante. Wi-Fi Alliance es una asociación de fabricantes de dispositivos inalámbricos. Aunque se basan en el estándar IEEE 802.11, algunos modos de funcionamiento son particulares de Wi-Fi y no están contemplados en el IEEE 802.11, por lo que fue estandarizar estas variaciones para que dispositivos de distintos fabricantes pudiesen comunicarse utilizando las extensiones de la 802.11 que no están definidas en el estándar original.

La existencia de estándares es importante para evitar el problema del “cliente cautivo” al tiempo que favorece la competencia y abarata los costes para el cliente. **El problema del cliente cautivo**, aparece cuando un cliente adquiere un sistema a un determinado fabricante, invirtiendo una gran cantidad de dinero y recursos en comprarlo e implantarlo. Cuando este cliente quiere adquirir nuevos sistemas para ampliar o mejorar el funcionamiento del sistema, se encuentra que debe acudir forzosamente al mismo fabricante, ya que ningún producto de otros fabricantes puede interconectarse con los que tiene ya instalados. Si deseara ampliar el sistema con dispositivos de otros fabricantes debería desechar los ya comprados e instalados, para volver a comprarlos a este nuevo proveedor, perdiendo todo el dinero y el esfuerzo realizado. Algunos fabricantes con posición importante en el mercado han tratado de conseguir la exclusividad de sus clientes de este modo.

Se acuña el término “**Sistemas Abiertos**” para aquellos sistemas en los que se plantean soluciones genéricas y no dependientes de un determinado constructor de ordenadores.

La utilización de sistemas abiertos tiene características que resultan interesantes para las organizaciones que los utilicen:

- **Interoperabilidad.** Posibilidad de enlazar diferentes ordenadores de diferentes marcas, dando la sensación de que trabajan como un único sistema.
- **Portabilidad.** Posibilidad de que aplicaciones de diferentes desarrolladores de software funcionen en máquinas de diversos fabricantes.
- **Escalabilidad** o capacidad de crecimiento. Posibilidad de usar el mismo entorno software en diferentes gamas de ordenadores, desde ordenadores de sobremesa hasta mainframes.

De todas estas características se desprende una serie de ventajas para el usuario final:

- **Libertad de elección** tanto software como hardware. Evita el síndrome del cliente cautivo.
- **Protección de la inversión.** Se cubre el riesgo de que el proveedor desaparezca del mercado.
- **Mejor relación precio-rendimiento.** No existe régimen de monopolio por lo que la competencia mejora el precio para el cliente.
- **Garantía de comunicación e interoperabilidad.** Mayor efectividad en la comunicación entre las diferentes unidades y organismos.

3.2. Organismos de estandarización en comunicaciones

En el ámbito de las telecomunicaciones, las compañías telefónicas del mundo varían considerablemente de un país a otro. En un extremo está Estados Unidos, con 1500 compañías telefónicas privadas tras la división en 1984 de AT&T. En el otro extremo se encuentran los países en los que el gobierno nacional tiene un monopolio completo de todas las comunicaciones, de forma que la autoridad en telecomunicaciones es una compañía estatal usualmente conocida como PTT.



Algunos organismos de estandarización importantes en comunicaciones informáticas.

3.2.1. ITU International Telecom Union



En 1865, representantes gobiernos europeos se reunieron para formar el predecesor de la actual **ITU** (*International Telecom Union*). La misión de la ITU fue estandarizar las telecomunicaciones internacionales, lo que en esos días significaba telegrafía. Cuando el teléfono se convirtió en un servicio internacional, la ITU emprendió la tarea de estandarizar también la telefonía. En 1947 la ITU llegó a ser una agencia de las Naciones Unidas.

La ITU tiene tres sectores principales:

1. Sector de radiocomunicaciones (ITU-R), que se ocupa de la asignación de frecuencias de radio en todo el mundo a los grupos de interés en competencia.
2. Sector de estandarización de telecomunicaciones (ITU-T), relacionada con los sistemas telefónicos y de comunicación de datos.
3. Sector de desarrollo (ITU-D).

De 1956 a 1993, la ITU-T fue conocida como **CCITT** (*Comité Consultatif International Télégraphique et Téléphonique*). En 1993 se reorganizó para hacerlo menos burocrático y cambió de nombre para reflejar su nuevo papel. Entre las recomendaciones del CCITT todavía está en uso la X.25.

La tarea de la ITU-T es hacer recomendaciones técnicas acerca de los interfaces de telefonía, telegrafía y comunicación de datos.

3.2.2. ISO International Standards Organization



Los estándares internacionales son producidos por la **ISO** (*International Standards Organization*) Organización Internacional de Normalización, fundada en 1946. Sus miembros son las organizaciones nacionales de estándares de los 89 países miembros. Estos miembros incluyen entre otros: **ANSI** (Estados Unidos), **BSI** (Gran Bretaña), **AFNOR** (Francia), **DIN** (Alemania), **AENOR** (España).

La ISO emite estándares sobre un vasto número de temas, que van desde tuercas y tornillos al revestimiento de los postes telefónicos. Se han emitido más de 5000 estándares, incluido el estándar OSI. La ISO tiene casi 200 comités técnicos (TC), numerados en el orden su creación, cada uno de los cuales se hace cargo de un tema específico. El TC97 se ocupa

ordenadores y procesamiento de información. Cada TC tiene subcomités divididos en grupos de trabajo.

En cuestiones de estándares de telecomunicaciones, la ISO y la ITU-T a menudo cooperan para evitar la ironía de tener dos estándares internacionales oficiales y mutuamente incompatibles (la ISO es un miembro de la ITU-T).

3.2.3. ANSI (American National Standards Institute)



El representante de Estados Unidos en la ISO es el **ANSI** (*American National Standards Institute*) *Instituto Nacional Estadounidense de Estándares*, una organización privada, no gubernamental y no lucrativa. Sus miembros son fabricantes, empresas de telecomunicaciones y otros particulares interesados. La ISO a menudo adopta los estándares ANSI como estándares internacionales.

3.2.4. IEEE Institute of Electrical and Electronics Engineers



Otro protagonista importante en el mundo de los estándares es el **IEEE** (*Institute of Electrical and Electronics Engineers*) Instituto de Ingeniería Eléctrica y Electrónica, la organización profesional más grande del mundo. Además de publicar revistas y organizar numerosas conferencias, el IEEE tiene un grupo de estandarización que elabora estándares en las áreas de ingeniería eléctrica y computación. El estándar 802 del IEEE para redes de área local es el estándar clave para las redes de área local, y posteriormente fue adoptado por la ISO como base para el estándar ISO 8802.

3.2.5. EIA Electronic Industries Alliance



EIA (*Electronic Industries Alliance*), Alianza de Industrias Electrónicas, es una organización formada por la asociación de las compañías electrónicas y de alta tecnología de los Estados Unidos, cuya misión es promover el desarrollo de mercado y la competitividad de la industria de alta tecnología de los Estados Unidos con esfuerzos locales e internacionales de la política.

En redes de comunicaciones son importantes sus especificaciones para los cables de par trenzado en unión con la TIA (*Telecommunications Industry Association*).

3.2.6. TIA Telecommunications Industry Association



TIA (*Telecommunications Industry Association*) Asociación de la Industria de Telecomunicaciones. Es la principal asociación comercial que representa el mundial de la

información y la comunicación (TIC) a través de la elaboración de normas, los asuntos de gobierno, oportunidades de negocios, inteligencia de mercado, la certificación y en todo el mundo el cumplimiento de la normativa ambiental.

Con el apoyo de sus 600 miembros, la TIA mejora el entorno de negocios para las empresas que participan en las telecomunicaciones, banda ancha, móviles inalámbricas, tecnologías de la información, redes, cable, satélite, comunicaciones unificadas, comunicaciones de emergencia y la dimensión ecológica de la tecnología. TIA es acreditado por ANSI. Desarrolla normas de cableado industrial voluntario para muchos productos de las telecomunicaciones.

3.3. Organismos de estandarización en Internet



Logotipos de algunos organismos de estandarización en Internet.

Al igual que hay normas ISO, DIN, UNE, etc... los estándares de Internet se etiquetan bajo el acrónimo “RFC” (Request for Comments) que significa “Solicitud de Comentarios. La propuesta y discusión de RFC’s los realizan los grupos de trabajo de la IETF en colaboración con IANA y el IAB

Los debates sobre las RFC se realizan en listas de correo de suscripción abierta, sin restricciones ni cuotas de socio. Los grupos interesados presentan borradores para su discusión, que tienen su número interno y tradicionalmente se consideraban caducos (se desalojaban de la base de datos) si a los seis meses no había consenso para convertirlos un RFC. Un documento que se consensua para pasar a RFC recibe un número por parte del RFC Editor, que viene a ser algo así como el secretariado de las asambleas, y entra en el “standards track”. Su ascenso en este “track” y su calificación como Estándar de Internet no dependerá de los debates técnicos o decisiones políticas, sino de la percepción que se tenga respecto a la aceptación del documento; esto es, del número y calidad de máquinas en Internet que muestran respetar las sugerencias del documento.

Además del Standards Track, las asambleas pueden emitir RFC's informativas. De estas, dos subcategorías reciben además numeración independiente: las “Best Current Practice” (BCP) y las “For Your Info” (FYI). Estas últimas se emplearon durante el boom de Internet con propósitos educativos. Las BCP se han revitalizado durante el último año ya que permiten reflejar actividad realizada por otras entidades en Internet y la relación entre estas y las Task Forces. La BCP 95, de Octubre del 2004, da por primera vez un “Mission Statement for the IETF”, que en cierto modo evoluciona sobre la FYI 17 de Agosto del 2001, titulada “The Tao of IETF”, y refleja los duros tiempos que ha pasado el modelo de “rough consensus and running code.” (la primera parte del lema, que encabeza este artículo, sólo se menciona en los seminarios y reuniones de educación, pero nunca explícitamente en una RFC. Su no aparición, por tanto, no permite sacar conclusiones sobre el ánimo actual en las asambleas).

3.3.1. ISOC Internet Society



La **ISOC** (*Internet Society*) Sociedad de Internet, es una organización profesional sin ánimo de lucro para la cooperación y coordinación en la evolución de Internet. Está formada por asociados individuales y organizaciones (agencias gubernamentales, operadores de red, empresas, fundaciones, etc.). Publica un boletín trimestral (*On The Net*) y convoca una conferencia anual (INET, <http://www.isoc.org/inet98/>).

ISOC <http://www.isoc.org/>

ISOC-es <http://www.isoc-es.org/news.php>

3.3.2. IETF (Internet Engineering Task Force)



IETF (*Internet Engineering Task Force*) Grupo Especial sobre Ingeniería de Internet, es una comunidad internacional no gubernamental y abierta a la participación de ingenieros, operadores, fabricantes e investigadores de redes, procedentes principalmente de los países industrializados, que se encargan de la evolución de la arquitectura Internet y de su correcto funcionamiento. En este grupo puede participar cualquier persona que lo desee, aportando sus conocimientos personales. La labor técnica real del IETF, que incluye el desarrollo de normas de Internet, se realiza en sus grupos de trabajo que se dividen por temas de diferentes ámbitos (por ejemplo, encaminamiento, transporte, seguridad, etc.). La mayor parte de las actividades se llevan a cabo por listas de correo electrónico. El IETF se reúne tres veces por año.

<http://www.ietf.org/>

3.3.3. IANA Internet Assigned Numbers Authority



IANA (*Internet Assigned Numbers Authority*) Autoridad de Números Asignados en Internet, es responsable de la coordinación global de la raíz DNS, coordina la asignación de las direcciones IP libres a organismos regionales, y gestiona sistemas de numeración en protocolos de Internet (por ejemplo puertos tcp/udp). Inicialmente era la responsable de todos los "parámetros únicos" de Internet: protocolos, direcciones IP, nombres de dominio, etc. En la actualidad muchas de sus funciones han sido asumidas por ICANN.

<http://www.iana.org>

3.3.4. ICANN Internet Corporation for Assigned Names and Numbers



ICANN (*Internet Corporation for Assigned Names and Numbers*) Corporación de Internet para la Asignación de Nombres y Números, es una organización sin fines de lucro que opera a nivel internacional, responsable de asignar espacio de direcciones numéricas del protocolo de Internet (IP), identificadores de protocolo y de las funciones de gestión [o administración] del sistema de nombres de dominio de primer nivel genéricos (gTLD) y de códigos de países (ccTLD), 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 EE.UU., actualmente son responsabilidad de ICANN. (<http://www.icann.org/tr/spanish.html>)

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.

En Europa existe **RIPE** (<http://www.ripe.net/>), que se encarga de la coordinación del registro regional Europeo de dominios y direcciones IP. En cada país existe un registro delegado de Internet. Concretamente, en España es ES-NIC (Centro de Comunicaciones CSIC Red Iris, <http://www.nic.es/>)

3.3.5. IAB Internet Architecture Board



Internet Architecture Board

El **IAB** (*Internet Architecture Board*) es el grupo asesor técnico de ISOC, formado por voluntarios, responsable de la edición y publicación de RFC's (Request for Comments), de la gestión de apelaciones por definiciones o uso de protocolos, etc. Además selecciona a los miembros del IESG y es responsable de supervisar las actividades de la IETF.

<http://www.iab.org/>

3.3.6. W3C World Wide Web Consortium



W3C (*World Wide Web Consortium*) es una comunidad internacional encargada del desarrollo de estándares Web. Entre sus miembros se encuentra Tim Berners-Lee, el creador de la WWW. Se plantea como misión conseguir que la WWW alcance todo su potencial (<http://www.w3c.org/>). Entre las tecnologías que han sido desarrolladas por W3C se encuentran HTML, CSS, DOM, y XML. Estos estándares son publicados y distribuidos de forma libre y gratuita como “recomendaciones del W3C” para su uso en la Internet.

4. Clasificación de Redes de Comunicaciones.

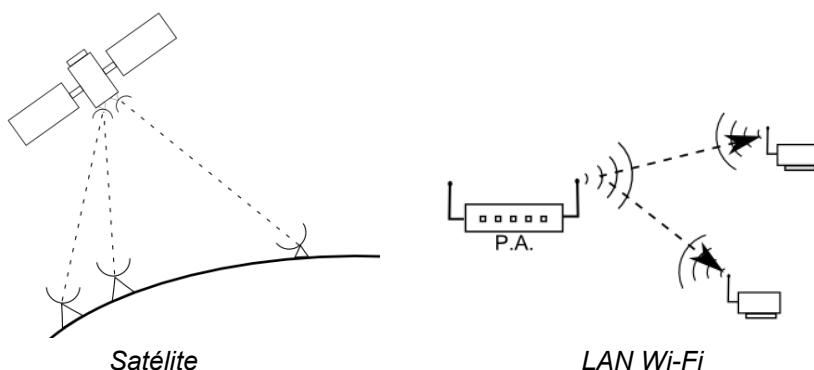
4.1. Según las tecnologías de transmisión.

En términos generales, hay dos tipos de tecnologías de transmisión: redes de difusión o multipunto, y redes punto a punto. Como regla general (con muchas excepciones), las redes pequeñas geográficamente hablando, usan la difusión, mientras que las redes más grandes son punto a punto.

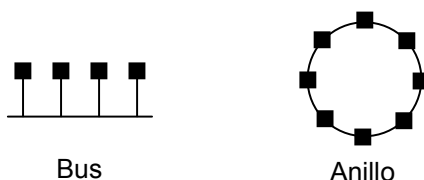
4.1.1. Redes de difusión.

Las redes de difusión tienen un canal de comunicación único, compartido por todos los nodos de la red. Los mensajes que envía un nodo son recibidos por todos los demás.

Las señales radioeléctricas utilizadas en comunicaciones, constituyen un ejemplo típico de redes de difusión dado que se propagan en todas direcciones y alcanzan a muchos receptores. La radio comercial y la televisión son los casos más conocidos, pero también las redes de satélites, las redes inalámbricas de datos packet-radio, Wi-Fi, WiMAX, etc...



También existen implementaciones de redes de difusión mediante líneas de datos, como por ejemplo la topología de conexión en bus, que propaga una señal enviada por una estación, a todas las demás, a través de un cable que las interconecta. También se considera de difusión las topologías en anillo en las que los nodos se conectan formando un anillo en el que los datos circulan de nodo a nodo hasta que son recibidos por quien los envió.



En este tipo de redes, si existe más de un emisor en el canal, es necesario arbitrar algún mecanismo que determine a quién se le asigna el derecho a emitir. Si más de un emisor utiliza el canal compartido a la vez, se mezclan las señales, y la comunicación se hace imposible. Se podría comparar esta situación con un debate en el que varias personas van tomando la palabra, siguiendo unas determinadas reglas para evitar que dos personas hablen a la vez, se interrumpan, e impidan al resto de interlocutores la correcta comprensión de todo lo que se dice.

Cuando en este tipo de canal, un mensaje va destinado a un solo receptor, es recibido igualmente por todos los demás nodos que están escuchando. Por ello, debe identificarse en el mismo mensaje al destinatario o destinatarios de la comunicación para que el resto de receptores lo ignoren.

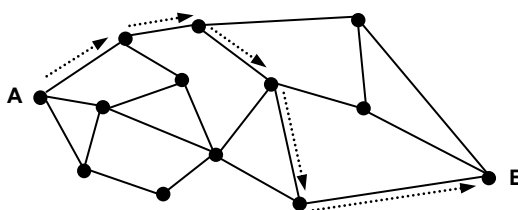
Existen valores para este campo de dirección que indican casos especiales como que el mensaje vaya destinado a todos los nodos de la red (difusión), o solo a un subconjunto de todos los nodos (multidifusión). Por ello, en este tipo de redes es posible enviar una orden o mensaje que será aceptada y procesada por todos los nodos o por un grupo de ellos, sin

necesidad de enviar un mensaje dirigido a cada uno por separado con su dirección de destino particular.

Las comunicaciones de difusión (broadcast) son utilizadas ampliamente en las redes informáticas de área local. Es muy común que los protocolos de redes de área local hagan consultas a todos los nodos de la red, solicitando por ejemplo que se identifique quien tiene determinada característica (servicio, tipo de nodo, dirección). También podemos encontrar diálogos en que el emisor no conoce la dirección del destinatario y dirige el mensaje a todos los nodos conectados esperando que el destinatario se dé por aludido y responda. En definitiva, las redes de área local utilizan profusamente las comunicaciones de difusión y multidifusión en su operativa de funcionamiento, y es difícil que trabajen sin este tipo de comunicación.

4.1.2. Redes punto a punto.

En una red punto a punto, los nodos que la componen están interconectados entre sí mediante enlaces privados entre pares de nodos. Un nodo cualquiera puede tener varios de estos enlaces privados, y todos los nodos de la red se interconectan formando una red o malla, en la que una comunicación se retransmite de nodo a nodo, como en una carrera de relevos, hasta llegar a su destinatario.



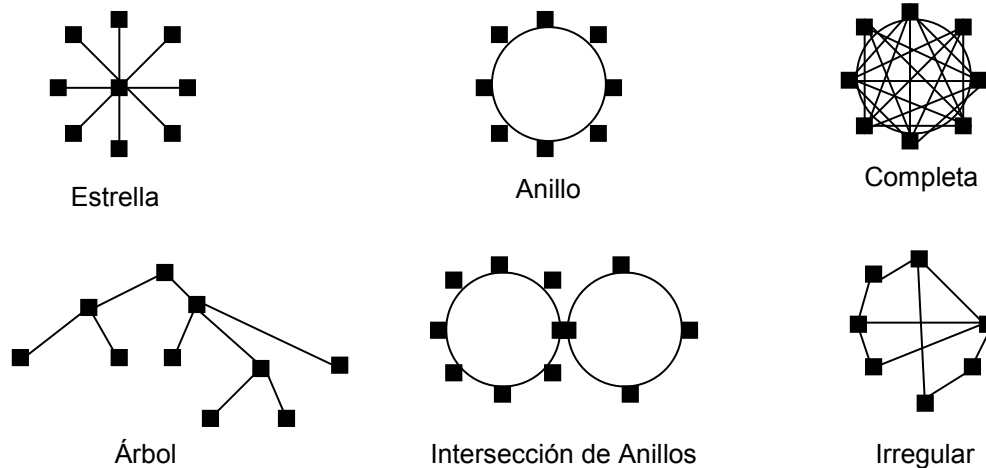
Ejemplo de red punto a punto

En una red punto a punto, lo más normal es que un nodo no cuente con un enlace privado con el nodo al que debe enviar información, de manera que para mandar un mensaje a un nodo con el que no tiene conexión directa, debe entregarlo a uno de los nodos con los que sí tiene comunicación directa. Este nodo puede que tampoco tenga conexión directa con el destinatario por lo que el proceso se repite hasta que el mensaje llega a un nodo conectado directamente al destinatario que lo entrega.

La red de telefonía tradicional es un ejemplo de red punto a punto. En este caso se distingue entre nodos terminales de comunicación que serían los teléfonos de los abonados, y nodos intermedios compuestos por centralitas. Es bastante común diferenciar en este tipo de redes entre red de transporte y nodos terminales de la comunicación. El usuario descuelga el teléfono que está conectado, no a otro teléfono, sino a una centralita. Marca un número que identifica al teléfono del usuario con quien quiere comunicarse. La centralita recoge esta petición de comunicación y la reenvía a otra centralita en el camino hacia el teléfono de destino, y así sucesivamente hasta que llega a la centralita en que está conectado y se establece la comunicación.

De esta forma se va trazando un camino (ruta) en la red de nodos que reexpiden el mensaje hasta llegar al nodo destino. En estas redes suele existir múltiples rutas para interconectar dos nodos (mediante nodos intermedios diferentes), por lo que necesitan de mecanismos de selección de un camino entre los diferentes posibles (encaminadores). Estos dispositivos también se encargan de escoger el nodo más adecuado para que el mensaje llegue al destino.

Algunas posibles topologías (formas de interconexión entre nodos) para las redes punto a punto se muestran en la siguiente figura:



En este tipo de redes es importante determinar cómo se escoge la ruta para llegar al destino, ya que afecta de forma crítica al rendimiento de la red, pudiendo llegar a ser imposible la comunicación si los mecanismos de selección de ruta no funcionan bien.

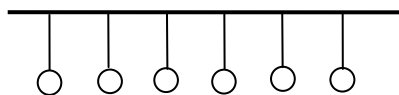
4.2. Topologías en redes de comunicaciones.

En las redes de ordenadores, los nodos (y estaciones) establecen enlaces entre sí, de forma que pueden alcanzar cualquier otro nodo de la red, bien directamente, o bien a través de otros nodos. La forma en que se organizan estas conexiones y en la que los nodos se comunican entre sí para alcanzar a los demás, constituye lo que se denomina “topología de red”

La topología determina muchas de las propiedades, ventajas e inconvenientes de la propia red. En ocasiones la forma de interconectar los nodos y estaciones limita el modo en que los nodos pueden comunicarse (bus) mientras que en otras, es posible que una misma forma de interconexión permita más de un modo de comunicación (anillo).

4.2.1. Topología en bus.

En esta topología todas las estaciones se conectan a un único medio bidireccional lineal o bus con puntos de terminación bien definidos. Cuando una estación transmite, su señal se propaga a ambos lados del emisor hacia todas las estaciones conectadas al bus hasta llegar a los puntos de terminación donde la señal es absorbida; de aquí que el bus reciba también el nombre de canal de difusión.



La mayoría de las redes en bus tienen la ventaja de estar constituidas por elementos pasivos, es decir, todos los componentes activos se encuentran en las estaciones, por lo que una avería en una estación no afecta más que a ella misma. Son por lo tanto redes cuyos componentes son muy fiables ya que no van a fallar por problemas de tensión o desgaste de los componentes electrónicos. Sin embargo, una avería en el cableado afecta a la totalidad de la red, quedando incomunicadas las estaciones de una sección del bus con las de la otra sección, y generándose interferencias (rebotes de la señal) en la rotura que afectan a la comunicación en cada una de las dos secciones.

Otras ventajas importantes son la modularidad (es muy sencillo añadir o retirar estaciones a la red) y la adaptabilidad a la distribución geográfica de las estaciones con un

coste reducido. En general, la topología en bus es la más sencilla desde la óptica del cableado la más económica en su instalación.

Como inconveniente se puede señalar que un fallo en cualquier parte del cableado provoca la imposibilidad total de comunicarse entre estaciones de la red. Además de provocar la caída de toda la red, un error de cable resulta difícil de reparar, debido a que puede haberse producido en cualquier parte de la instalación. En instalaciones extensas puede resultar complejo localizar y reparar el problema lo que conlleva un tiempo de inactividad elevado ante cualquier fallo, que afecta a todas las estaciones.

Otra desventaja proviene del uso de un medio compartido entre todas las estaciones, lo que conlleva cierta complejidad en las estaciones para organizarse a la hora de tomar el canal para transmitir y resolver los problemas asociados. Debe garantizarse que no emitan dos o más estaciones al mismo tiempo, a la vez que cualquier estación que desea emitir, pueda hacerlo de forma adecuada. Comúnmente, en un medio compartido es normal que varias estaciones lleguen a emitir al mismo tiempo, interfiriéndose. Esto debe evitarse en la medida de lo posible ya que provoca una caída de rendimiento de toda la red durante el tiempo en que se resuelve el problema. En casos extremos puede llegar a colapsarse toda la red cuando son muchas las estaciones que desean transmitir al mismo tiempo.

El rendimiento en este tipo de redes es muy bueno cuando unas pocas estaciones desean transmitir, pero decae considerablemente cuando muchas estaciones quieren tomar el canal compartido para comunicarse.



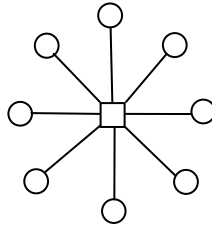
Ejemplo de topología en Bus: Red Ethernet con cable coaxial delgado.

No es una topología adecuada para grandes redes. Se trata de una topología para redes de reducidas dimensiones que resulta muy barata, sencilla de instalar, y fiable (sin elementos activos), pero en la que resulta muy difícil localizar un problema de cableado que además afecta al funcionamiento de todo el sistema, lo que resulta inaceptablemente costoso en la mayoría de las organizaciones.

Existe una variante de esta topología que aunque físicamente es una red en bus para aprovechar todas sus ventajas, se organiza de forma lógica en forma de anillo para realizar las comunicaciones: Token Bus 802.4

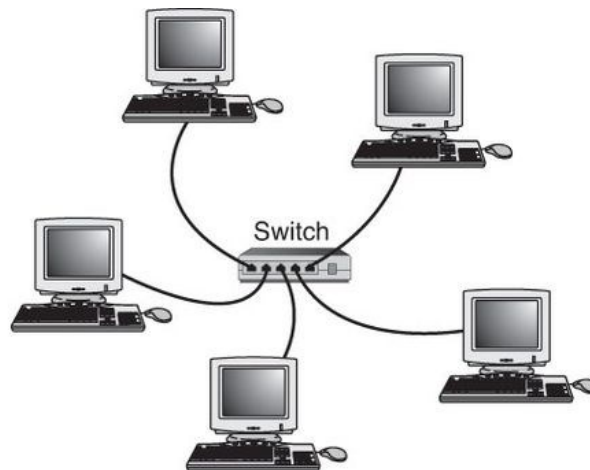
4.2.2. Topología en estrella.

En la topología en estrella todas las estaciones están conectadas mediante enlaces bidireccionales a un nodo central, que asume las funciones de gestión y control de las comunicaciones, proporcionando un camino entre dos dispositivos que deseen comunicarse.



La principal ventaja de la topología en estrella es que el acceso a la red, es decir, la decisión de cuándo una estación puede o no transmitir se halla bajo control central. Las estaciones pueden ser por tanto muy simples y baratas. Además, la flexibilidad en cuanto a configuración y localización de fallos es aceptable al estar toda la funcionalidad localizada en un nodo central.

El nodo central es un elemento crítico ya que su rendimiento debe ser muy superior a los nodos que interconecta si no queremos que se sature, y un fallo del nodo central dejaría toda la red fuera de servicio. El nodo central es un elemento complejo que debe proporcionar un elevado rendimiento y funciones de control y gestión, por lo que resulta bastante caro. El nodo central debe canalizar todos los datos, por lo que en situaciones de gran cantidad de estaciones comunicándose, puede provocar un cuello de botella. Otro problema asociado a esta topología consiste en la posibilidad de que el caro y complejo nodo central falle por algún motivo, lo que dejaría a toda las estaciones sin ninguna posibilidad de comunicación.



Ejemplo de topología en Estrella: Red Ethernet con cable de pares.

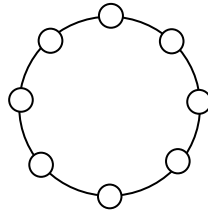
En cuanto al cableado, su longitud es elevada en comparación con otras topologías pero es menos sensible a roturas fallos ya que solo afectarían a un nodo.

Se trata de una red costosa de instalar tanto en dispositivos como en cableado, sin embargo proporciona bastante seguridad ya que un fallo en una estación o cable solo afecta a dicha estación. El nodo central suele ser un elemento especializado en las tareas que realiza, no una estación cualquiera. Es un tipo de topología que se utiliza en redes de reducidas dimensiones ya que el cableado es inviable para grandes longitudes.

Existen variaciones de esta topología que disponen físicamente el cableado en forma de estrella mientras el nodo central consiste en un elemento que une las conexiones bien en bus (concentrador de cableado) o en anillo (MAU). En ambos casos tenemos una topología física en estrella en cuanto al tendido de cables y dispositivos, pero con un funcionamiento distinto a nivel de comunicación de estaciones.

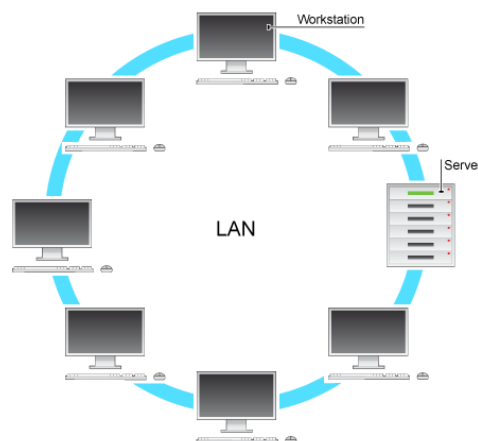
4.2.3. Topología en anillo y doble anillo.

En una topología en anillo, cada estación dispone de una línea de comunicación privada con otros dos nodos, formando por tanto un anillo por el que circula la información.



En general los enlaces son unidireccionales circulando la información de un nodo a otro siempre en el mismo sentido, hasta que alcanza a su destinatario.

Los nodos o estaciones de la red son elementos activos que recogen la información que circula, la examinan para ver si va destinada a ellos y la reexpiden para que llegue a su destinatario.



Red de área local con topología en anillo

Si un nodo se estropea, la comunicación se ve interrumpida y la red entera cae. Para evitar esto, cuando un nodo se apaga o se cae, unos circuitos simples conectan las dos líneas para que la información continúe circulando. Este mecanismo no está exento de problemas ya que cuando se eliminan muchas estaciones de la red (en periodos de baja actividad, por ejemplo), pueden producirse problemas en el funcionamiento del anillo debido a la poca cantidad de nodos operativos y a la excesiva extensión de las líneas sin contar con repetidores.

Es una topología adecuada para redes pequeñas y medianas. El cableado es sencillo de tender y resulta bastante reducido (más o menos como bus). Se suele dibujar como un anillo, pero en realidad sólo debe respetarse que forme un circuito cerrado por lo que se ajusta muy bien a cualquier distribución geográfica tanto en instalaciones pequeñas como de tamaño medio.

Un problema de estas redes consiste en que la rotura de un cable provoca la imposibilidad de funcionamiento de toda la red, a lo sumo permite comunicar los nodos contiguos.

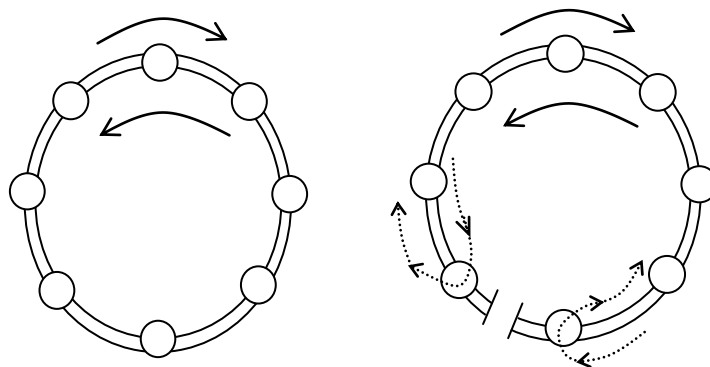
Estas redes pueden actuar como una topología punto a punto en la que cada información es transmitida de nodo a nodo hasta que llega a su destinatario que la extrae de la red, o bien trabajar con una topología de difusión en la que el destinatario no extrae la información del anillo, circulando ésta por todos los nodos hasta que llega al mismo nodo que la envió, y es eliminada de la red.

El funcionamiento de las comunicaciones en estas redes exige a las estaciones conectadas unas complejas tareas de control y gestión de la integridad de las comunicaciones. Por ello no suelen ser redes baratas ya que los nodos deben realizar tareas complejas. Además el hecho de que cada estación actúa como repetidor de las señales introduce retrasos en las comunicaciones.

Como ventaja, este tipo de redes permite un gran control sobre todas las comunicaciones, permitiendo establecer tasas fijas y sostenidas de comunicación a las estaciones, prioridades en los datos y garantizando una calidad en las comunicaciones que jamás podríamos encontrar otras redes como las topologías en bus.

Otra ventaja consiste en la facilidad para detectar y localizar un error de cableado, ya que se puede ver desde qué estación recibimos la información, por lo que la rotura se encontrará entre ésta y la anterior.

Una variante de esta topología, dispone de dos anillos concéntricos a los que se conectan las estaciones. Cada una de las dos líneas del anillo transmite la información en una dirección distinta.



Funcionamiento normal (izquierda) y funcionamiento ante rotura de una línea

Las ventajas del anillo doble no consiste sólo en que disponemos de dos líneas para comunicar cada estación que pueden utilizarse por separado y de forma simultánea, sino que nos proporciona la posibilidad de corregir un fallo en el cableado de forma automática, permitiendo que la red siga funcionando aun si se cortaran todos los cables que comunican dos estaciones.

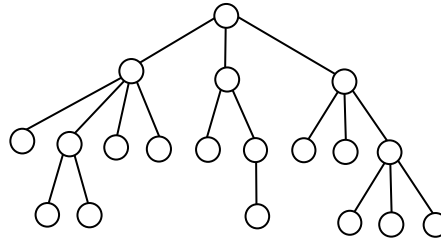
Las estaciones que detectan la rotura, encaminan la información de una de las líneas a la otra, construyendo un anillo simple que permite mantener la comunicación aunque se pierda la línea doble.

En una topología en anillo es posible utilizar un modo de comunicación de difusión, en el que todas las estaciones reciben la información de la red, no solo las que actúan como intermediarias entre origen y destino. También es preciso señalar que los problemas debidos a una rotura de cables se pueden paliar realizando un tendido de líneas bidireccionales en estrella hacia un nodo central denominado MAU. En esta topología física estrella, las comunicaciones se realizan mediante enlaces privados entre nodos adyacentes al igual que en el anillo, pero el fallo de un cable solo dejaría fuera a una estación, ya que la MAU puentearía ese enlace.

4.2.4. Topología en árbol.

En esta topología, existe un nodo central que se denomina “raíz” que se conecta a otros nodos denominados “nodos de primer nivel”. Los nodos del primer nivel no pueden conectarse entre sí, para comunicarse deben enviar la información al nodo raíz de forma obligatoria. A su vez, los nodos de primer nivel pueden tener conexiones a nodos denominados de segundo nivel. En general, un nodo de nivel “n” tendrá una línea que le interconecta a un único nodo del nivel superior n-1, y podrá tener varias líneas de comunicación con nodos del siguiente nivel n+1, pero nunca tendrá líneas de comunicación con nodos de su propio nivel.

De esta forma se obtiene un esquema de conexión que representaría un árbol invertido donde las ramas crecen hacia abajo tal como se muestra en el siguiente dibujo:



En esta topología, cada nodo se encarga de la comunicación de sus nodos de nivel inferior. Al conjunto de un nodo y todos sus nodos conectados de niveles inferiores se le suele denominar “rama”. Cada rama puede considerarse como una pequeña subred independiente capaz de administrar todas las comunicaciones que afecten a sus nodos.

Este tipo de topologías proporciona un buen aprovechamiento de las líneas y pueden utilizarse en redes de cualquier extensión. Si cae un nodo o una línea, quedan incomunicadas las ramas del árbol que se vean afectadas, pero dentro de cada rama las comunicaciones entre nodos no se ven afectadas.

La estructura en árbol proporciona una forma de comunicación que minimiza el número de nodos intermedios que es preciso utilizar para llegar al nodo con el que queremos comunicarnos, lo que es especialmente interesante en redes muy extensas.

Esta topología proporciona una estructura jerárquica de la red, colocando los nodos más cercanos estrechamente relacionados controlados por un nodo superior, mientras que nodos de más alto nivel controlan las comunicaciones de áreas cada vez más grandes conforme nos acercamos a la raíz. El nodo raíz controlaría todo el tráfico de datos entre todas las ramas a las que está conectado, mientras que un nodo de más bajo nivel solo controlaría las comunicaciones de las estaciones directamente conectadas a él. Todo ello permite un gran control de todas las comunicaciones, permitiendo avanzadas funciones de gestión y monitorización.

Pero esta topología también tiene sus desventajas. En primer lugar nos encontramos que las tareas de reenvío de información y control de las comunicaciones son más complejas conforme subimos de nivel, llegando al punto en que el nodo raíz debe ser extraordinariamente complejo y potente para poder llevar a cabo sus funciones. Cuanto más alto es el nivel de un nodo de la red, más información debe manejar y por tanto resulta más caro. Además, los nodos más altos, y especialmente la raíz deben ser muy fiables, ya que un fallo dejaría sin posibilidad de comunicación a amplias zonas de la red.

Podemos encontrar ejemplos de esta topología tanto en redes de área local (100-VG-AnyLAN del IEEE), como en redes de gran extensión como la red telefónica.

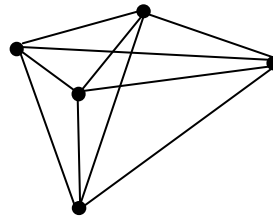
El ejemplo típico de este tipo de redes consiste en la red de telefonía conmutada que todos conocemos y hemos utilizado: Los teléfonos se conectan a una centralita local, las centralitas locales de la ciudad se interconectan en una centralita de la ciudad y ésta a su vez a una centralita de área y así hasta que llegamos al nodo central.

Si realizamos una llamada a un abonado que viva cerca de nuestra vivienda, la llamada posiblemente será encaminada a través de nuestra centralita local, o como mucho pasando por la centralita de la ciudad. Cuanto más lejano se encuentre nuestro interlocutor, más centralitas se ven involucradas en la comunicación y más costos presenta para la operadora de comunicaciones. Éste es el motivo de la tarificación de llamadas en función de la distancia.

Como ejemplo puede consultarse la situación de los nodos de más nivel de la compañía telefónica y comprobar cómo se encuentran muy protegidos tanto ante fallos técnicos como ante sabotajes ya que un mal funcionamiento de los mismos provocaría graves problemas.

4.2.5. Topología de interconexión total.

En esta topología, cada estación dispone de una línea privada con cualquier otra estación con la que puede comunicarse:

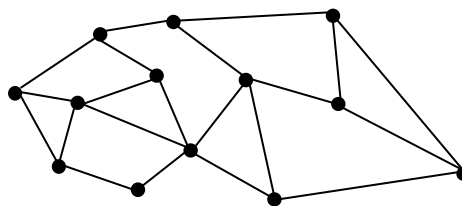


No existe necesidad de reenviar información de un nodo a otro ya que todos pueden comunicarse entre sí de forma directa. La caída de una línea sólo afecta a la comunicación entre dos estaciones, y la caída de una estación o nodo no tiene ninguna repercusión para la red. Es el sistema de comunicación más simple y fiable.

Sin embargo exige un cableado que en la práctica sólo puede instalarse en redes con muy pocos nodos. Pensemos que para los 5 nodos que se pueden ver en el ejemplo, se precisa tender 4 cables para cada uno de ellos, en total $5 * 4 = 20$. Pensemos en una red de comunicaciones con una veintena de estaciones, lo que nos daría $20 * 19 = 380$ líneas independientes. Tengamos en cuenta solo el panel que habría que instalar en cada estación para conectar 19 cables y veremos como resulta imposible plantear este tipo de redes incluso en pequeñas oficinas.

4.2.6. Topología irregular.

En este tipo de topologías, cada nodo se conecta varios otros nodos sin restricciones. Cualquier nodo tendrá conexión con uno o más nodos de la red.



Esta topología se adapta muy bien a redes de gran extensión. Permite tender líneas donde sea más sencillo o cómodo, y aprovechar todos los enlaces para poder llegar al destinatario por distintos caminos.

La caída de un nodo o de un enlace no tiene por qué impedir las comunicaciones, siempre que existan caminos alternativos para llegar al destinatario.

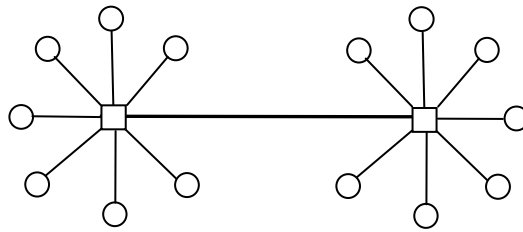
En la parte negativa, cada nodo intermedio debe decidir por qué línea debe enviar los datos para que lleguen correctamente al destino. Esta tarea es compleja cuando la extensión de la red es grande, y cuando existen varias rutas distintas para llegar al mismo destino. Es muy importante cómo se decide el camino por el que se envía la información, para garantizar que llegue al destino, y para evitar problemas en la red como las rutas circulares, congestión de nodos intermedios, caída de algún nodo, o cualquier otra incidencia. También puede ocurrir que un funcionamiento sin optimizar llegue a provocar problemas, como por ejemplo el enviar toda la información siempre por la misma ruta puede llegar a saturar algunos nodos mientras existen vías alternativas sin carga de trabajo. En definitiva, las tareas realizadas por los nodos intermedios son complejas, requieren un conocimiento actualizado del estado de la red, y deben hacerse de una forma rápida. Todo ello tiene como consecuencia que los nodos intermedios son complejos y caros.

Es una topología muy utilizada en redes de gran extensión utilizadas para el intercambio de datos mediante conmutación de paquetes. Como ejemplos podemos citar Internet, IBERPAC o X.25.

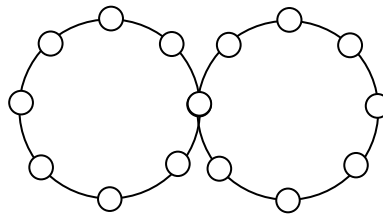
4.2.7. Topologías híbridas.

Las redes de comunicación se instalan en organizaciones muy diversas y deben interconectar gran cantidad de equipos con distintas funciones y necesidades. A veces no existe una sola red que pueda cumplir todos los requerimientos, o nos encontramos con distintas redes que hay que interconectar, o bien es preciso adaptar la topología a las necesidades de la organización. Por todo ello, podemos encontrar combinaciones de las topologías que hemos visto.

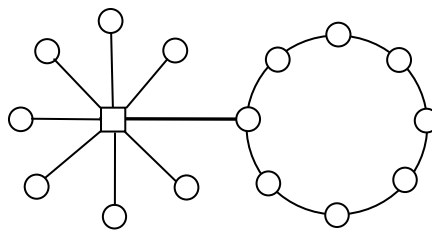
Algunos ejemplos de las combinaciones más simples:



Topología estrella-estrella o estrella extendida.



Intersección de anillos



Topología anillo-estrella

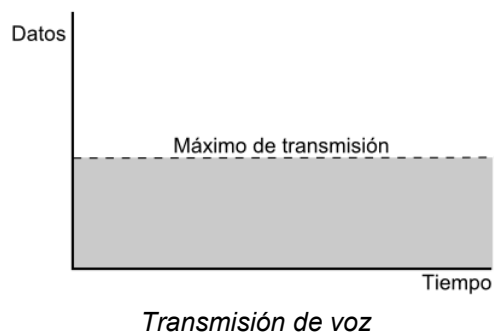
4.3. Según las tecnologías de conmutación.

No siempre es posible tener una línea dedicada entre dos Hosts. Una solución barata es usar la red de transmisión de voz, es decir, la red telefónica. Pero la solución no es óptima por la diferencia entre los dos tipos de señales.

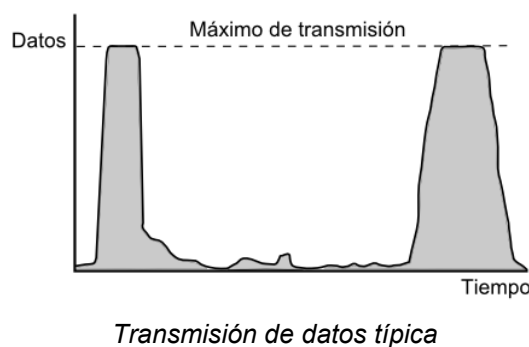
Existen diferencias entre la forma de comunicarse de las personas y los tipos de comunicación de los sistemas informáticos.

Una conversación entre interlocutores humanos, conlleva una baja tasa de transmisión de datos que se mantiene constante durante todo el tiempo que dura la comunicación. Otra

característica de este tipo de comunicaciones es que, una vez iniciada la conversación, su duración suele ser breve (habitualmente), de unos pocos minutos.



Los equipos informáticos, cuando establecen una comunicación, típicamente están inactivos durante la mayor parte del tiempo, requiriendo transmitir grandes cantidades de información en periodos muy breves. Es decir, una comunicación informática se compone de ráfagas cortas con gran cantidad de datos transmitidos entre largos periodos de inactividad. Como característica adicional, las comunicaciones informáticas pueden estar activas durante grandes periodos de tiempo, típicamente varias horas, a diferencia de las comunicaciones humanas.



4.3.1. Red de conmutación de circuitos.

Este es el caso de la red telefónica. Los diferentes circuitos que componen la subred se combinan uniéndose para formar un único circuito que conecta a los interlocutores. Este modo de operación fuerza a que existan 3 fases:

- Fase 1. Establecimiento del circuito. Existirá una fase de búsqueda del camino más adecuado para alcanzar el punto de destino. En esta fase se plantea una demora.
- Fase 2. Establecido el circuito dedicado, se procede al intercambio de información. Durante esta fase nadie fuera de los interlocutores puede utilizar ningún segmento del circuito dedicado formado para el establecimiento de conexión. Esta es una restricción clara de este tipo de subredes y que es poco justificable si los interlocutores, en el caso de ordenadores, pasan gran parte del tiempo sin transmitir nada.
- Fase 3. Liberalización del circuito una vez terminado el proceso de intercambio de información.

Esta red fue diseñada para comunicaciones humanas de voz (conversaciones), y se ajusta muy bien a sus características: Tasa baja de transmisión constante durante toda la comunicación que suele durar unos minutos.

Para llegar a comunicarse en esta red, es necesario dedicar cierto tiempo a establecer el circuito dedicado, lo que conlleva un retraso importante desde el momento de iniciar la comunicación hasta que se transmite efectivamente la información al destinatario. En el caso

de comunicación humana, en que una conversación dura como poco unos minutos, resulta irrelevante perder unos segundos para establecerla. Pero en una comunicación informática, puede llegar a ser inaceptable tardar 10 segundos para iniciar una comunicación de unos pocos milisegundos.

Mientras dure la comunicación, el circuito formado por todas las líneas y enlaces entre conmutadores queda reservado para uso exclusivo de ambos interlocutores. Esto implica que el coste asociado a una comunicación en este tipo de red, depende tanto de la distancia física entre los interlocutores (más distancia implica más líneas y de mayor longitud), como del tiempo que dure la comunicación. Por ello, las comunicaciones telefónicas se han tarificado tradicionalmente en función de la distancia y duración de la llamada.

Un problema asociado a este tipo de redes, consiste en la congestión de los nodos que puede llevar a que todas sus líneas estén ocupadas, siendo imposible establecer la comunicación.

Por ejemplo, en caso de lluvias torrenciales, es común que muchas personas soliciten ayuda de los bomberos debido a inundación de sus casas y locales. Sin embargo, la oficina de bomberos solo tiene tres líneas de teléfono, por lo que puede atender tres solicitudes simultáneamente. Si hay 50 personas intentando llamar al teléfono de los bomberos, 47 verán denegada su solicitud de conexión. Esto puede llegar a ser un problema serio si de las 50 llamadas, dos de ellas corresponde a situaciones peligrosas para la vida de las personas afectadas, ya que incluso llamando continuamente, es posible que no puedan comunicar el problema en un tiempo adecuado. La red telefónica no sabe distinguir las comunicaciones realmente urgentes de vida o muerte, de las que solo piden que desalojen el agua de un local comercial.

Como ventaja de este tipo de redes, puede señalarse que, una vez establecida la comunicación, el circuito proporciona una tasa de transmisión constante y fija, sin reducción de tasas de transmisión por congestiones de la red.

4.3.2. Red de conmutación de mensajes.

Se considera un "mensaje" como una comunicación completa de tamaño arbitrario que un nodo envía a otro. Un mensaje podría ser la respuesta a una consulta "Afirmativo" o bien todo un libro como "El Quijote".

En este tipo de redes, el mensaje se va transmitiendo de un nodo al siguiente hasta llegar al destinatario. No se establece una línea de comunicación directa entre el emisor y el receptor. Cada nodo entrega el mensaje completo al siguiente de la red, con el que puede establecer una conexión, hasta que el mensaje llega al destinatario.

En este tipo de redes, los costos están más asociados al tamaño del mensaje que a la distancia entre origen y destino.

Evidentemente, la comunicación no es tan inmediata como en las redes de conmutación de circuitos, ya que cada mensaje tarda un tiempo no determinado en llegar a su destino. Sin embargo, mejora la ocupación de la línea, ya que en cada momento de la transmisión, el mensaje sólo utiliza el segmento de la red que comunica dos nodos contiguos.

Otra desventaja consiste en la necesidad de almacenar y retransmitir los mensajes, cuyo tamaño puede ser tremendamente variable, y puede obligar a reservar un espacio de almacenamiento elevado. Incluso es posible que un mensaje exceda la capacidad de almacenamiento de uno de los nodos en el camino al destino, y por tanto la comunicación sería inviable.

Es difícil encontrar un ejemplo totalmente válido de este tipo de redes ya que siempre se acaba estableciendo un límite al tamaño del mensaje, bien por la propia reglamentación de uso de la red, bien por los costos asociados. El ejemplo típico de este tipo de redes suele ser el servicio telegráfico o postal. En ambos casos se entregan mensajes completos a la red que son reenviados de nodo a nodo hasta llegar completos al destinatario. El problema del tamaño arbitrario se soluciona con tarifas de transmisión que aumentan con el tamaño del

mensaje/paquete o simplemente prohibiendo mensajes/paquetes que excedan un límite determinado.

4.3.3. Red de conmutación de paquetes.

En una red cuyas conexiones sean punto a punto, la idea es dividir la información que se desee transmitir (mensaje), en bloques de un tamaño prefijado, denominados “*paquetes*”. Los paquetes viajarán por la subred de nodo a nodo hasta llegar al punto de destino, donde se reensamblan para obtener el mensaje completo.

A diferencia de las redes de conmutación de circuitos, las redes de conmutación de paquetes no requieren obligatoriamente de una fase de establecimiento de conexión. Esto evita los retrasos asociados a la fase de establecimiento de conexión a la hora de enviar datos a su destinatario.

Otra diferencia con las redes de conmutación de circuitos, consiste en que las redes de conmutación de paquetes no bloquean ningún recurso durante el proceso de transmisión de la información como hacen las redes de conmutación de circuitos con el canal. Por el canal que une a dos nodos se pueden intercalar paquetes pertenecientes a distintas comunicaciones, lo que aprovecha mejor las líneas que enlazan los nodos. Por otro lado ya no existe la posibilidad de ver rechazada una comunicación a causa de congestión de las líneas.

Por todo ello, los costos en estos tipos de redes se asocian más a la cantidad de paquetes a transmitir (volumen total de datos transmitidos) que a la distancia o tiempo en que mantenga la comunicación. En realidad, una comunicación inactiva (que no transmite paquetes) casi no tiene costo para la operadora.

Al ser los paquetes de un tamaño delimitado (fijo o entre un máximo y mínimo conocidos), los nodos de la red pueden diseñarse para trabajar con estos tamaños, y evitar por tanto los problemas que tienen las redes de conmutación de mensajes de tamaño arbitrario.

Como inconvenientes, se puede señalar la posibilidad congestión que puede producirse en cualquier parte de la red, lo que ralentizaría todas las comunicaciones, así como la complejidad de los métodos para calcular el camino que debe seguir un paquete para llegar a su destino. En consecuencia, es bastante común que en alguna ocasión se pierdan paquetes, o que al seguir caminos diferentes, lleguen al receptor en orden distinto al de emisión. Esto aumenta la complejidad y el costo de los equipos interlocutores, que deben reservar recursos para almacenar paquetes que llegan en desorden, o que no se han recibido en destino, y establecer mecanismos para identificar y retransmitir paquetes perdidos.

4.4. Clasificación en función de la titularidad.

Podemos distinguir dos situaciones distintas en cuanto al despliegue y uso de las redes de ordenadores.

- **Redes Privadas:** Son redes instaladas por una organización que son utilizadas por esa misma organización de manera exclusiva. Suelen ser redes de reducida extensión, típicamente una oficina o un edificio de oficinas. Podría extenderse entre varios edificios cercanos, pero siempre pertenecientes o administrados por la misma empresa u organización. Estas redes son instaladas, utilizadas y mantenidas con recursos de dicha organización y se utilizan para cubrir sus propias necesidades. Como ejemplo típico la red que interconecta los equipos informáticos en una oficina para compartir datos y dispositivos de impresión.
- **Redes Públicas:** Son redes instaladas por una organización que ofrece a sus clientes su utilización a cambio de una remuneración. Por tanto son redes compartidas por quienes las utilizan, que además no son los dueños de la red, sino que pagan un determinado uso o servicio sobre la misma a su dueño. En este caso se trata de redes que por su costo o complejidad no pueden amortizarse con el uso por la empresa que las instala, y por ello debe acometer su instalación una empresa

de comunicaciones. Como ejemplo podemos señalar las redes de telefonía, o de comunicaciones de datos como Iberpac o Internet.

4.5. Clasificación en función de la escala.

Un criterio para clasificar las redes es su escala. La clasificación clásica comprende: redes de área local o LAN (*Local Area Network*), redes metropolitanas o MAN (*Metropolitan Area Network*), y redes de área extensa o WAN (*Wide Area Network*).

4.5.1. Redes de área personal o PAN

Recientemente, han proliferado dispositivos cada vez más reducidos y con mayores capacidades (PDA's, Telefonos móviles de última generación, etc..), que se han añadido a las herramientas habituales de un puesto de trabajo informatizado. Estos dispositivos necesitan comunicarse con la estación de trabajo del usuario para cargar y descargar datos, actualizar agenda, mensajes, etc.. Si unimos esta situación a la ingente cantidad de periféricos con que puede dotarse a una estación de trabajo, podemos llegar a encontrarnos con un área de trabajo saturada de cables de conexión para cada uno de estos dispositivos, lo que resulta molesto, costoso de mantener, y bastante problemático. Por todo ello se viene acuñando el concepto de “**red de área personal**” PAN (*Personal Area Network*) como red de comunicaciones con tecnología inalámbrica, que abarque un puesto de trabajo (menos de 10 metros), y que proporcione una vía común de comunicación a todos estos dispositivos, simplificando las tareas de operación y mantenimiento del puesto de trabajo.

Se trataría de redes inalámbricas, privadas, que permitirían comunicar de forma sencilla dispositivos que pueden estar alimentados por baterías y que suelen ser utilizados en un puesto de trabajo. Como ejemplo podemos encontrar hace ya bastantes años, conexiones de este tipo a través de infrarrojos que comunican teléfonos móviles, impresoras, PDA's con la estación de trabajo del usuario o entre sí.

Pero desde hace ya bastantes años, predomina la tecnología Bluetooth para este tipo de comunicaciones, que utiliza señales de radiofrecuencia en la misma banda de las microondas que las redes Wi-Fi. Bluetooth ha sido desarrollado para proporcionar conectividad a todo tipo de dispositivos con los que interactúa una persona, y actualmente está implementada en multitud de dispositivos: “manos libres”, móviles, PDA's, teclados, ratones, etc...



Red de área personal inalámbrica BlueTooth.

En este tipo de redes se utilizan señales inalámbricas con bajas potencias difíciles de interceptar fuera del espacio donde se utiliza. Las tasas de transferencia de datos son reducidas en comparación con las redes de área local. Se caracterizan por su sencillez de uso, capacidad de autoconfiguración, seguridad, todo ello asociado a su ámbito de uso: Dispositivos

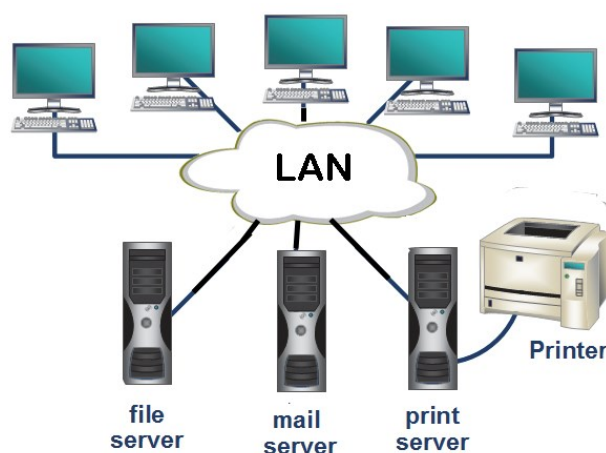
portátiles en el ámbito de trabajo de usuarios comunes que las conectan sin asistencia de técnicos especializados.

En la actualidad, se empieza a popularizar un sistema de comunicaciones de corto alcance denominado comunicación de campo cercano (*Near field communication*, NFC). Este tipo de comunicaciones sólo funcionan al alcance de unos pocos centímetros utilizando señales magnéticas. A diferencia de bluetooth, la comunicación mediante NFC puede realizarse con dispositivos "pasivos", es decir, sin alimentación eléctrica, ya que utilizan el campo generado por un dispositivo activo para poder transferir los datos. Como ejemplo de este tipo de comunicaciones encontramos el nuevo DNI electrónico, también llamado DNI 3.0.

4.5.2. Redes de área local o LAN.

Las redes de área local o LAN son redes privadas de hasta unos pocos kilómetros de extensión, y abarcan desde una habitación, hasta un campus, pasando por sus edificios. Se consideran redes de área local aquellas con una extensión inferior a los dos o tres kilómetros, aunque no hay una norma que establezca valores estrictos.

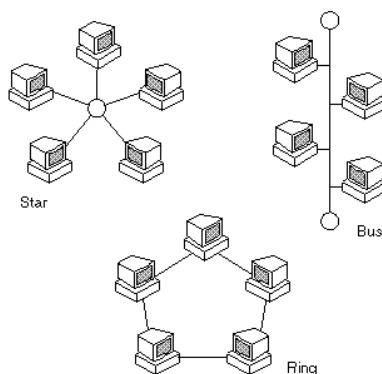
Se usan para conectar ordenadores y estaciones de trabajo con objeto de compartir recursos e intercambiar información.



Al estar restringidas en tamaño, pueden utilizar cables de gran calidad que permiten altas capacidades de transmisión, y pocos errores.

Son **redes privadas** que pertenecen a la misma organización que las utiliza, ya que su instalación es económica, y se restringe a la comunicación de los equipos de la organización que la implanta.

Normalmente usan **redes de difusión**, y pueden presentar diversas topologías, siendo las más comunes bus, anillo, y estrella, tal y como se muestra en la siguiente figura:



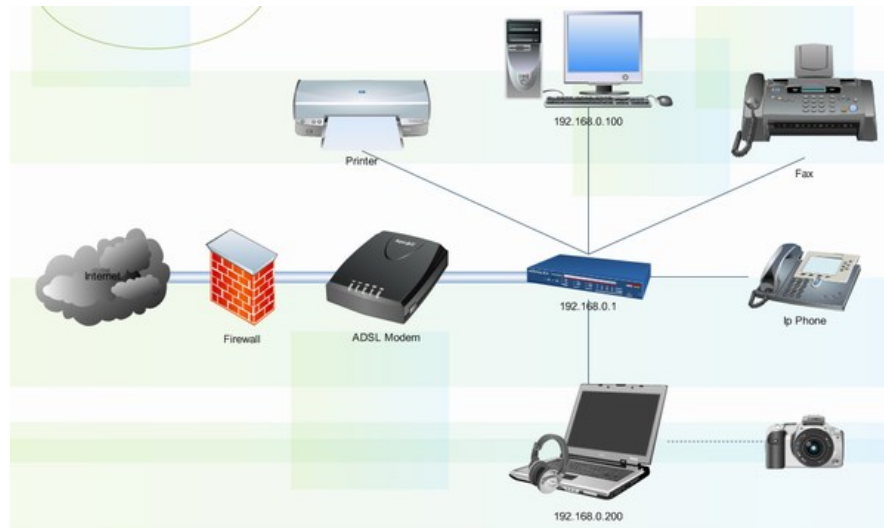
En cualquier caso, al ser redes de difusión, independientemente de la topología presentada, deben poseer algún mecanismo para arbitrar el acceso al medio compartido. Dicho

mecanismo puede ser centralizado o distribuido, y constituye una importante característica de la red.

Un ejemplo de LAN es la IEEE 802.3, también conocida como Ethernet. Es una red de transmisión basada en bus, con control de acceso descentralizado.

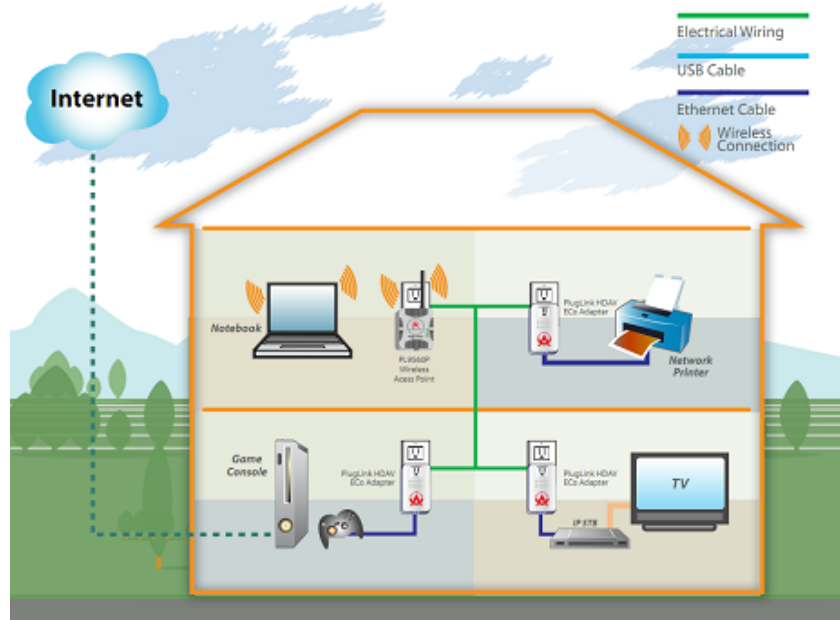
4.5.2.1. Red de área doméstica HAN

La Red de Área Doméstica (HAN - Home-Area Networks), es un caso particular de LAN, que intercomunica todos los dispositivos digitales que podemos encontrar en una vivienda. Entre los objetivos de la HAN encontramos el acceso a Internet de los dispositivos, su control y monitorización, así como la posibilidad de comunicar con ellos de forma remota a través de Internet.



Red de área doméstica.

Las tecnologías son las mismas que en las redes de área local, pudiendo utilizar medios guiados de par trenzado, comunicaciones inalámbricas, o una mezcla de ambas. En un principio, las redes inalámbricas parecen ser las más adecuadas para implementar este tipo de comunicaciones, debido a las ventajas de bajos costes de instalación y reemplazo, frente a instalaciones de cable, más costosas, y engorrosas de implementar. Sin embargo, es posible utilizar una red en la que convivan esos dos tipos de medios, usando cada uno donde tiene más ventajas. También puede utilizarse otras tecnologías como Power Line Communications (PLC) solas o en combinación con las demás



Red de área doméstica implementada con Ethernet, PLC, y WiFi .

Un estándar inalámbrico específico para redes domésticas denominado HomeRF de 1998, fue desarrollado por “Home Radio Frequency Working Group”. La finalidad de HomeRF es la de conseguir la interoperatividad entre en el mayor número de dispositivos diferentes que estén ubicados en cualquier punto de la casa. Para ello establecen un estándar abierto y sin licencia basado en comunicación digital mediante Radio Frecuencia. El resultado ha sido el desarrollo de SWAP (Shared Wireless Access Protocol) basado en el estándar IEEE 802.11 para datos y en DECT para voz, que se usará en esta aplicación. SWAP puede soportar todo tipo de servicios enfocados a la transmisión de datos TCP/IP, así como protocolos para voz, tipo DECT/GAP, en redes domésticas.

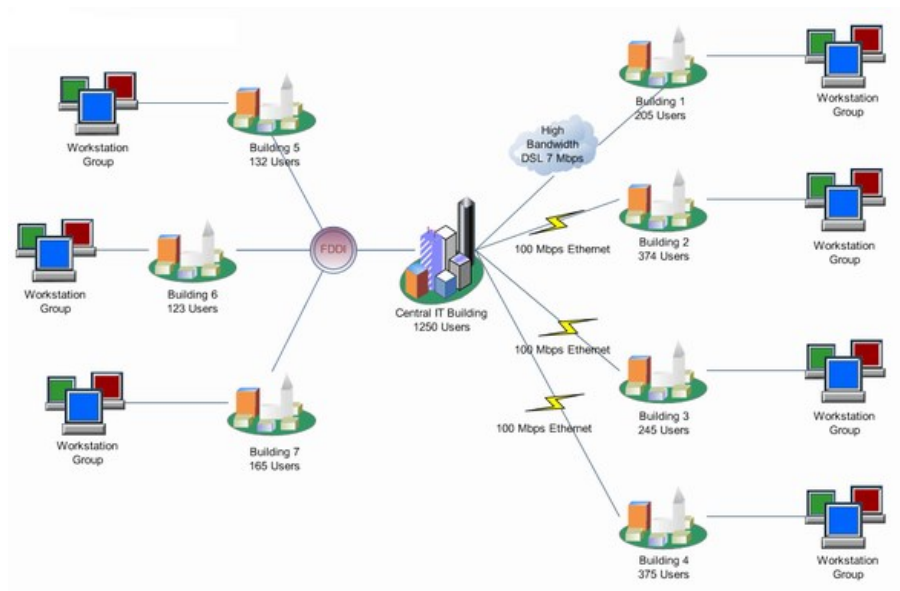
HomeRF no ha tenido éxito debido a la gran difusión de otras redes como Wi-Fi y Bluetooth que han proporcionado a los usuarios domésticos conectividad entre sus dispositivos en el hogar. Actualmente HomeRF se considera obsoleto y el grupo que lo desarrolló ya no existe.

Entre los dispositivos que se comunican en una HAN tenemos smartphones, cámaras, portátiles y estaciones de trabajo, cámaras de fotos y de vídeo, telefonía IP, incluso elementos multimedia como el equipo de música, la televisión o el “media center” HTPC

4.5.3. Redes de área de campus o CAN.

Este tipo de redes, son similares en cuanto a tecnología a las LAN, pero abarcan más extensión, comunicando varias LAN entre sí, en un área geográfica limitada, sin llegar a cubrir un área tan extensa como las redes de área metropolitana. Se trataría de enlazar las diversas LAN's que existen en un campus universitario, una base militar, o un polígono industrial.

En cuanto a sus características, se consideran redes privadas, donde todos los dispositivos y medios pertenecen a la organización que hace uso de la red. Las tecnologías, como ya se ha señalado, son las mismas que las utilizadas en las LAN, utilizando los mismos estándares, aprovechando las capacidades de la fibra óptica para realizar enlaces de varios km.



Ejemplo de red de área de campus

4.5.4. Redes de área metropolitana o MAN.

Una red de área metropolitana o MAN es una red más grande que una LAN y una CAN, que utiliza tecnologías similares, proporcionando por tanto casi las mismas prestaciones.

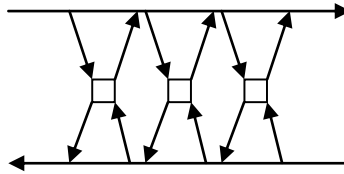
Una MAN puede ser pública o privada (a diferencia de las CAN's), e interconectar varias LAN's o CAN's en un área relativamente extensa (entre decenas y unos pocos centenares de km). En general, este tipo de redes se extienden por una zona urbana o poco más, aunque podría cubrir una región bastante extensa.

Puede ser una red privada, instalada para cubrir las necesidades de comunicación de una determinada organización dentro de la ciudad, pero más comúnmente es una red pública instalada por una empresa de telecomunicaciones, a través de la cual ofrece a sus clientes servicios de telefonía, datos, y televisión.



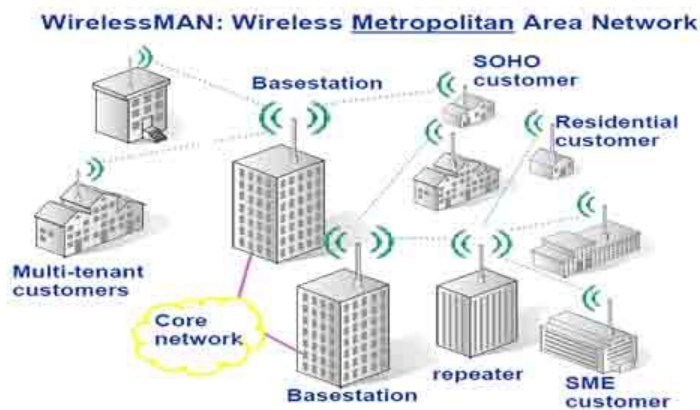
Red de área metropolitana clásica

Aunque los medios y prestaciones son similares a las LAN's y MAN's, existe una norma que define un estándar específico para las MAN: la IEEE 802.6. Este estándar consiste en dos buses unidireccionales, a los que se conectan todos los nodos tal como se muestra en la siguiente figura:



En este ejemplo, vemos que el tráfico hacia la derecha utiliza el bus superior, y el tráfico hacia la izquierda el inferior.

Los medios utilizados son similares a los empleados en LAN's y CAN'S (par trenzado y fibra óptica) lo mismo que sus prestaciones (entre 10 Mbps y 10 Gbps), y suelen ofrecer servicios de datos, voz y televisión. En cable de cobre pueden utilizar tecnologías como Ethernet o MetroEthernet, y en fibra óptica, FDDI, GigaEthernet, etc..



Ejemplo de red MAN implementada con tecnología inalámbrica.

Actualmente se utilizan tecnologías inalámbricas para un despliegue rápido y económico, como las redes WiMax, o las redes Mesh.

4.5.5. Redes de área extensa o WAN.

Una red de área extensa o WAN, se extiende sobre un área geográfica extensa como un país o un continente. Su misión es transportar los mensajes de una estación a otra que puede estar muy alejada.

Estas redes deben dar acceso a estaciones muy alejadas entre sí, para ello, la empresa que la instala, habitualmente utiliza una topología punto a punto, conectando nodos intermediarios en la comunicación, que van retransmitiendo los datos de la estación emisora hasta llegar a su destino.



Una red de área extensa puede abarcar todo el mundo.

Las estaciones que quieren comunicarse, se conectan al nodo más cercano de la red, que recibe y reexpide hacia la red los datos que la estación le entrega.

Estas redes son extraordinariamente caras de instalar y mantener, por lo que sólo grandes empresas de telecomunicaciones las construyen, para ofrecer a sus clientes la posibilidad de utilizarlas. Son por tanto redes públicas a las que se accede pagando a la empresa que la ha instalado.

En general, estas redes son punto a punto, de forma que si dos nodos que no comparten una línea de transmisión desean comunicarse, deben hacerlo indirectamente por medio de otros nodos.

Debido a que las conexiones entre nodos pueden extenderse por cientos de kilómetros, las líneas no pueden ser de la misma capacidad y calidad que en las redes de área local, con tan solo unos cientos de metros de longitud. Por lo tanto, las WAN, típicamente son las redes de menor capacidad y en las que se pueden presentar una mayor tasa de errores. Actualmente, con el uso de fibra óptica, las cosas han cambiado bastante, para mejorar la calidad de las WAN.

Una segunda posibilidad para una WAN es un sistema de satélites o de radio en tierra. Cada router tiene una antena a través de la cual puede enviar y recibir. Algunas veces, los routers están conectados a una red punto a punto de gran tamaño, y sólo algunos de ellos tienen una antena de satélite. Por su naturaleza, las redes de satélites son de difusión.

4.6. Clasificación en función del medio (guiado o inalámbrico)

Es posible clasificar las redes en función del tipo de medio que utiliza, distinguiendo entre redes que emplean medios guiados (cables) para conectar una estación y aquellas que no requieren la instalación de un canal exclusivo para su comunicación con la red, porque utiliza ondas del espectro radioeléctrico para ello.

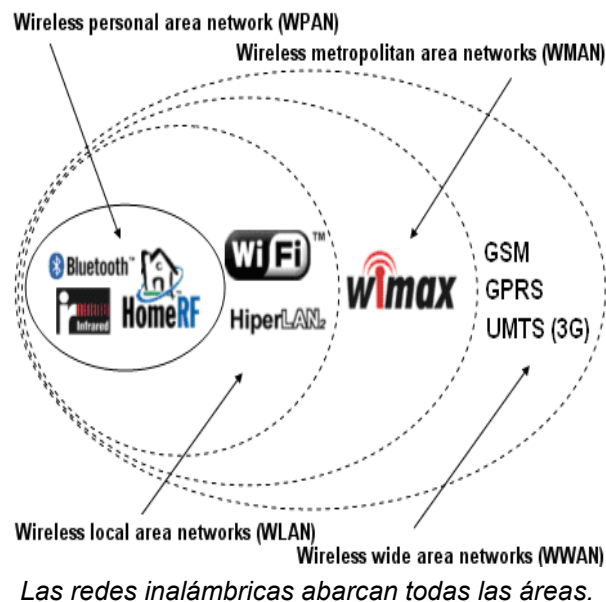
4.6.1. Redes Cableadas

Las redes tradicionales usan medios guiados (cables) para llevar la señal hasta su destinatario. Estos cables pueden ser de muy diversos tipos y materiales, predominando en las redes de área local los cables de cobre de pares trenzados.

Este tipo de redes están muy bien estudiadas, y actualmente ofrecen grandes capacidades de transmisión con una baja tasa de errores. Sin embargo cuentan con el inconveniente de tener que instalar la estación cerca de un punto de conexión a la red y conectarlo mediante un cable. Esta es una desventaja importante cuando necesitamos comunicarnos con dispositivos portátiles, como PDA's, para realizar nuestro trabajo mientras nos desplazamos de un punto a otro de la empresa. Otra desventaja consiste en los enormes costos para tender líneas en zonas remotas o de difícil acceso, dado que los costos son enormes y no compensan los pocos ingresos que se puede obtener.

4.6.2. Redes Inalámbricas WLAN

Actualmente se tiende a la movilidad de los equipos y a eliminar el molesto cableado en la medida de lo posible. El término "Wireless" sin cables, se está haciendo popular, y no solo en las comunicaciones, sino en el ámbito de conexión de periféricos a la unidad central, ya sean teclados, ratones, o impresoras, por mencionar los más comunes.



Las redes inalámbricas tienen una utilidad evidente en la conexión de ordenadores portátiles a la red de área local de la empresa, evitando la molestia de los cables. Además se elimina de incongruencia que consistente en obligar a colocar el equipo portátil cerca de alguno de los limitados puntos de conexión a la red del edificio, con lo que ya no es tan portátil.

Pero el uso de estas redes no está justificado únicamente por la movilidad de los Hosts, ya que pueden resultar una solución más económica cuando el cableado de un edificio presenta problemas técnicos de compleja o costosa solución.

Otra ventaja de estas redes consiste en la facilidad e inmediatez de su instalación (y desinstalación), lo que las hace especialmente indicadas para convenciones, ferias, o cuando la ocupación de la oficina es provisional y no resulta rentable o posible el cableado de la LAN.

En situaciones en las que se necesita conectar dos puntos distantes, entre los que resulta difícil tender un cable, por su extensión (uno o dos kilómetros), por su trazado, o por normativas legales, las redes inalámbricas proporcionan una alternativa al costoso tendido de cables.

En lugares alejados de las infraestructuras de red o de difícil acceso debido a su orografía, las redes inalámbricas ofrecen ventajas tanto en los costos de despliegue como en el tiempo empleado. Es mucho más económico y rápido, tender una torre de transmisión cada 50 Km, o instalar una antena parabólica para la comunicación vía satélite, que llevar un cable a esa vivienda desde el punto más cercano de la red cableada.

Sin embargo, estas redes presentan el inconveniente de facilitar una menor velocidad de transferencia, así como una tasa de error más elevada, además de problemas en la seguridad y confidencialidad de los datos que transmiten a todo el que tenga un receptor adecuado.

Las redes inalámbricas tienen muchas formas, desde el uso de múltiples antenas por ejemplo en un campus, hasta usar un teléfono móvil. Es posible igualmente, tener diferentes combinaciones de redes cableadas e inalámbricas.

5. Arquitectura de red de comunicaciones.

5.1. Introducción

Las redes de comunicaciones de datos ofrecen la posibilidad de transmitir información entre todos los dispositivos conectados. Para que dos o más dispositivos se puedan comunicar sin problemas, deben coincidir en diversos aspectos de la comunicación, como por ejemplo los medios físicos utilizados y cómo se conectan al dispositivo, las señales utilizadas y cómo se

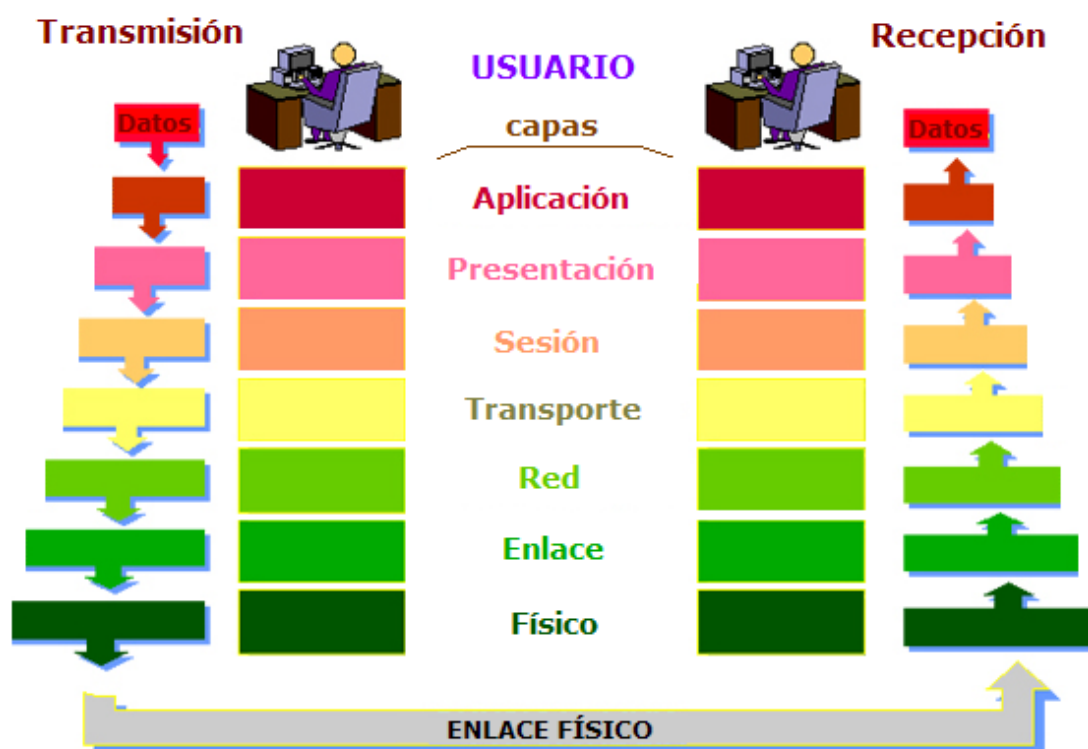
codifican para circular por el canal, los mensajes de control utilizados entre dispositivos, y otros muchos aspectos de la comunicación. Si los dispositivos no utilizan las mismas reglas para enviar y recibir información, la comunicación no es posible.

Por lo tanto, se necesitan estándares que cubran todos los aspectos de la comunicación para que dispositivos fabricados en distintos momentos, por diferentes fabricantes, en distintas partes del mundo, puedan comunicarse entre sí sin problemas a través de una determinada red de comunicaciones.

Por ejemplo: si observamos redes ampliamente difundidas como la red de telefonía básica, resulta evidente que existen unas normas que determinan el tipo de cables y conectores empleados, así como el voltaje que circula por ellos, ya que puedo usar un teléfono adquirido a cualquier fabricante conectado a cualquier proveedor de telefonía. También se puede observar cómo existe una reglamentación que permite por ejemplo direccionar todos los terminales telefónicos del mundo, asignando un identificador único a cada uno. También se observa como las señalizaciones de llamada y de línea ocupada funcionan igual en cualquier terminal de línea telefónica. En definitiva, existen unas reglas que regulan cómo se conectan, comunican, señalizan y direccionan los dispositivos en la red telefónica que coinciden en los aspectos básicos en todos los países del mundo. Esto permite realizar comunicaciones entre terminales conectados a la red, aunque estén en distintos países.

Una vez que tenemos clara la necesidad de la estandarización, vamos a abordar cómo se definen los estándares en las redes de comunicaciones de datos, que son las que nos interesa estudiar en este módulo. Hemos visto la importancia de la estandarización en el punto "Estándares y sistemas abiertos". Si revisamos los ejemplos planteados en el ámbito de las comunicaciones, tanto en el caso de los terminales, como en el caso de los módems, podemos observar que en los inicios de las comunicaciones de datos, no existían normas ni estándares abiertos, por lo que cada fabricante creaba los propios, pudiendo en ocasiones ser aceptados por otros fabricantes (*estándar de facto*).

En esta situación, en la que cada fabricante creaba su propia tecnología de comunicaciones, totalmente incompatible con las del resto de fabricantes, aparece la necesidad de la estandarización de redes de comunicaciones y es la Organización Internacional de Normas (ISO) la que se encarga de abordar el problema. En el año 1980 publica un estándar que se denomina "**Interconexión de Sistemas Abiertos**" **OSI** (*Open System Interconnection*).



OSI plantea un estándar abierto en el que se aborda la comunicación entre dispositivos mediante un sistema basado en capas o niveles. Inicialmente, los primeros sistemas de comunicaciones se implementaban de una vez, en un bloque que realizaba todas las tareas de la comunicación. Pero este tipo de diseño de redes planteaba diversos problemas como la imposibilidad de comunicaciones entre sistemas de distintos fabricantes (incluso entre sistemas del mismo fabricante), la imposibilidad de mejorar o cambiar algún elemento de la comunicación sin sustituir toda la red, o la complejidad de implementación en redes con cada vez más funcionalidades. Ante este problema, algunos fabricantes realizaron diseños de redes de comunicaciones dividiendo las tareas a realizar en lo que se denominan "capas" o "niveles" independientes e interconectados que trabajando unidos, realizaban todas las tareas de la red de comunicaciones. De este modo se resuelven muchos de los problemas mencionados: Se puede cambiar una capa de la arquitectura si afectar al resto de las capas, la complejidad se reduce al implementar en cada capa sólo un conjunto de funciones relacionadas en lugar de todas las tareas de la comunicación, se define la arquitectura como un estándar abierto y libre de derechos.

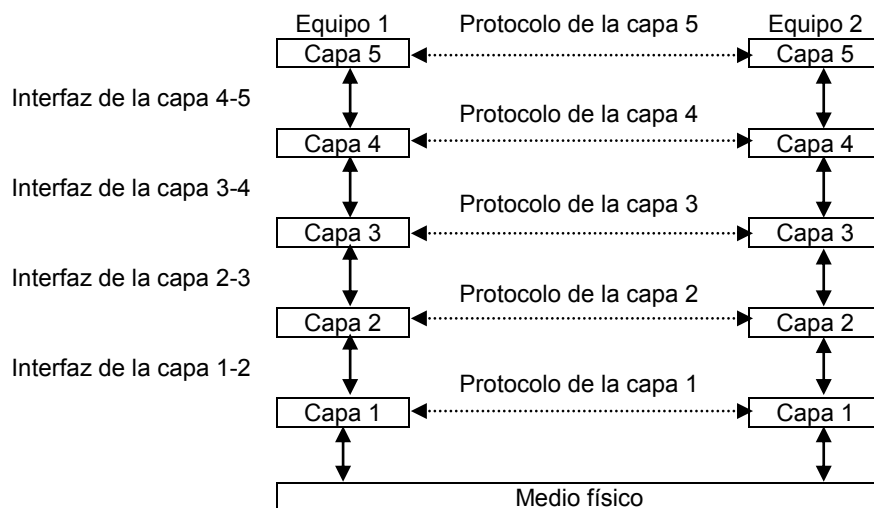
Las primeras redes de comunicaciones diseñadas como una arquitectura basada en capas fueron la Arquitectura de Sistemas de Red (Systems Network Architecture, SNA) de IBM y algunas versiones de DECnet desarrollada por *Digital Equipment Corporation*. La ISO, recoge la experiencia de estas redes y de otras para crear una arquitectura de red estándar y abierta basada en el modelo de capas, a la que denomino OSI.

La arquitectura OSI, como primer estándar de comunicaciones, rápidamente se volvió muy popular y ha influenciado todo el mundo de las comunicaciones hasta hoy. El también llamado "Modelo de referencia OSI" es muy importante en el mundo de las comunicaciones y todos los técnicos deben conocerlo bien para poder realizar su trabajo ya que es de referencia constante en manuales y documentaciones técnicas.

La influencia del modelo de referencia OSI, es tan grande, que arquitecturas de comunicaciones como TCP/IP, que no habían sido diseñadas mediante capas, se reinterpretaron para ser referenciadas como arquitecturas basadas en capas.

5.2. Arquitecturas basadas en capas o niveles

Para reducir la complejidad de su diseño, las redes se organizan mediante una serie de capas o niveles, cada una construida sobre la inferior. Todos los trabajos a realizar y problemas a resolver en la arquitectura se dividen entre las capas definidas. El conjunto de todas las capas realizan las labores de la comunicación, pero cada una de las capas sólo se ocupa de las tareas y problemas que se le han asignado sin tener en cuenta el resto de tareas asignadas a las demás capas. Por lo tanto, para una comunicación efectiva, será preciso que todas las capas realicen sus tareas de forma coordinada, lo que se consigue mediante un sistema de solicitudes de servicios de unas capas a otras. El propósito de cada capa es ofrecer ciertos servicios a las capas superiores de modo que no tengan que ocuparse del detalle de la implementación real de los servicios.



Ejemplo de una arquitectura con cinco capas.

5.2.1. Interfaz

El término "interfaz" se utiliza en muchos ámbitos. En términos generales una interfaz es un sistema de comunicación entre dos elementos. Por ejemplo en un ordenador personal (PC), el teclado se considera una interfaz de entrada de datos, y el monitor, una interfaz de salida de datos. En este sentido de dispositivo de intercomunicación, una "tarjeta de interfaz de red" (Network Interface Card, NIC), es el dispositivo mediante el que el PC se comunica con la red de datos.

A parte de dispositivos para la comunicación, interfaz también puede utilizarse con el sentido de "forma de comunicación lógica". Por ejemplo, un usuario puede comunicar órdenes a un PC mediante la "interfaz de línea de comandos" (*Command line interface*, CLI) que proporciona el sistema operativo, pero también puede realizar esas tareas mediante un "interfaz gráfico de ventanas" que es proporcionado por los sistemas operativos modernos.

En cualquier caso, el término "interfaz" hace referencia a un dispositivo o a unas reglas que permite la comunicación entre dos elementos distintos. Cabe señalar que el término tiene una connotación de cercanía, es decir, en todos los casos, la interfaz actúa de intermediaria entre elementos que están contiguos, "tocándose", muy cercanos.

En el ejemplo anterior de arquitectura con cinco capas, puede observarse como entre cada par de capas adyacentes hay una **interfaz** que regula la manera de interactuar entre dos capas contiguas del mismo equipo. La interfaz determina cómo se realiza la comunicación, qué capa solicita servicios, qué servicios se pueden solicitar, cómo se responde a las solicitudes, que datos se pasan entre las capas, que formatos tienen esos datos, etc..

Las interfaces bien definidas simplifican el reemplazo de la implementación de una capa con una implementación totalmente diferente, pues todo lo que se necesita es que la nueva implementación ofrezca exactamente el mismo conjunto de servicios que ofrecía la antigua.

5.2.2. Protocolo

El término protocolo podría definirse como las reglas que rigen la interacción de elementos del mismo tipo. Por ejemplo: cuando varias personas interactúan, el protocolo establece las reglas a seguir. En este caso, el protocolo determina lo que se puede hacer (saludar, presentarse, preguntar, agradecer, etc..), cómo debe hacerse (por ejemplo, saludar con estrechando las manos, con un abrazo, con un beso, etc...), y también determina límites a lo que se puede hacer para no caer en lo que sería calificado de mala educación. Los protocolos pueden variar entre distintas comunidades o países, de forma que una forma de saludo común en nuestro país, puede ser totalmente inadecuada en otro país.

No hay que confundir protocolo con Interfaz. En el caso de la interfaz, se trata de las reglas de comunicación entre elementos distintos, mientras que el protocolo establece reglas

de comunicación entre elementos del mismo tipo. Además, los protocolos no conllevan el sentido de cercanía física que se asocia con las interfaces.

Básicamente, un **protocolo** es un acuerdo entre las partes que se comunican sobre cómo va a proceder la comunicación.

En las arquitecturas de red, la capa n de una máquina lleva a cabo una conversación con la capa n de otra máquina. Las reglas y conversiones que se siguen en esta conversación se conocen como **protocolo de la capa n** .

5.2.3. Arquitectura de red

El conjunto de capas y protocolos recibe el nombre de **arquitectura de red**. Ni los detalles de la implementación ni la especificación de los interfaces forman parte de la arquitectura porque se encuentran ocultas dentro de las máquinas y no son visibles desde fuera.

Reflexionemos un momento sobre esto: Dos equipos podrán comunicarse si ambos utilizan la misma arquitectura de red. La arquitectura de red consiste en las capas (definiendo las tareas que realizan) y los protocolos mediante los que se comunican las capas del mismo nivel. Las interfaces y las implementaciones de las capas son irrelevantes para la comunicación, y por lo tanto no pertenecen a la arquitectura de red.

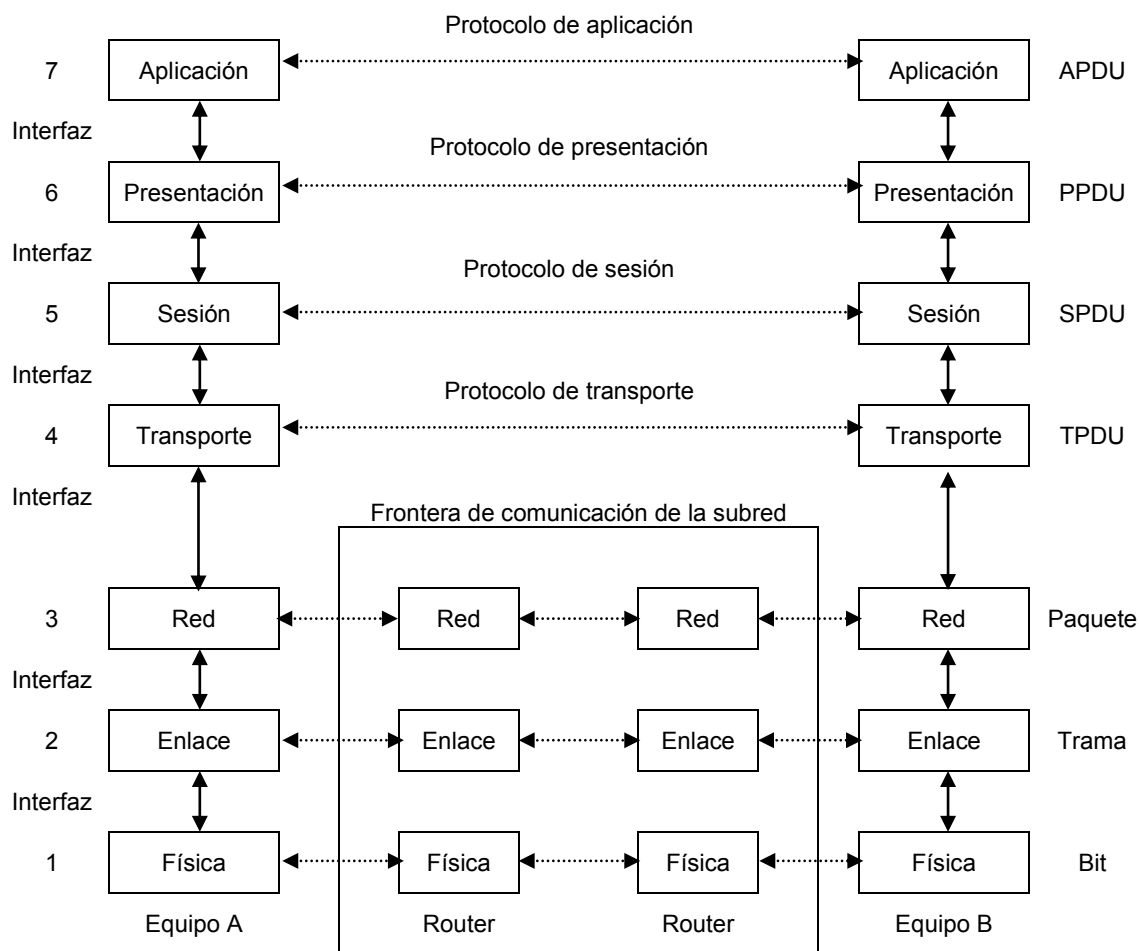
Por ejemplo: Supongamos que deseamos transferir un archivo entre dos máquinas: una máquina es un PC con Windows y la otra un PC con GNU Linux. Ambos PC's utilizan la arquitectura TCP/IP para comunicarse y por ello es posible la transferencia del archivo. Sin embargo, tanto la implementación de las capas, como de las interfaces es distinta en ambas máquinas. El código que implementa las capas de la arquitectura TCP/IP en los sistemas operativos Windows y GNU Linux, es distinto, y los interfaces también, sin embargo, como no forman parte de la arquitectura, es posible la comunicación entre ellos. Dicho de otro modo: el código que implementa las funciones de las capas, y las interfaces entre dichas capas, son internos a cada máquina, y por lo tanto, no afectan a la comunicación con el exterior.

5.3. El modelo de referencia OSI.

Dada la importancia de la arquitectura OSI en el ámbito de las comunicaciones, vamos a verla con detalle. A partir de este momento, en el módulo se realizarán continuas referencias al modelo OSI, por lo que es vital comprenderlo y conocerlo para poder comprender las referencias existentes en toda documentación referente a comunicaciones de datos.

El modelo OSI se basa en una propuesta que desarrolló la Organización Internacional de Normas (ISO, por sus siglas en inglés) como primer paso hacia la estandarización internacional de los protocolos que se usan en las diversas capas. El modelo se llama modelo de referencia OSI (*Open Systems Interconnection*) de la ISO puesto que se ocupa de la conexión de sistemas abiertos, esto es, sistemas que están abiertos a la comunicación con otros sistemas. Usualmente se le conoce como modelo OSI para acortar.

El modelo OSI define las siguientes siete capas:



Nota: En el gráfico se aprecia como los tres primeros niveles se agrupan en lo que se ha venido en denominar "*subred*", diferenciándose del resto de niveles. La **subred** se podría definir como la infraestructura que transporta los datos entre el emisor y el receptor, formada por nodos interconectados entre sí, que se van reenviando los datos hasta que llegan a su destino. En el caso de redes de difusión la subred es inexistente, pero en el caso de redes punto a punto, la subred está compuesta por los nodos intermedios entre los que van viajando los paquetes de datos desde el emisor hasta llegar al receptor. En redes de área extensa con topologías punto a punto, la subred es responsabilidad del proveedor de comunicaciones. De este modo, la subred está compuesta por los nodos intermedios de la topología que encaminan los datos hacia su destino. En este sentido, la subred está compuesta por nodos que trabajan en las tres primeras capas del modelo OSI (*routers* o enrutadores), y no implementarían las capas superiores, por lo que no se comportarían nunca como emisor o receptor de los datos transmitidos.

El modelo de OSI en sí no es una arquitectura de red porque no especifica los servicios y protocolos exactos que se han de usar en cada capa, sólo dice lo que debe hacer cada capa. Sin embargo, la ISO también ha elaborado estándares para todas las capas, aunque no sean parte del modelo de referencia mismo. Cada uno se ha publicado por separado como norma internacional. En revisiones posteriores del estándar, se corrigieron algunos de los problemas que presentaban, entre otros, los protocolos a utilizar, por lo que en la actualidad también puede denominarse arquitectura OSI.

5.3.1. La capa física.

La capa física tiene que ver con **la transmisión de bits por un canal** de comunicación. Las consideraciones de diseño tienen que ver con la acción de asegurarse de que cuando un lado envíe un bit 1, se reciba en el otro lado como bit 1, no como bit 0.

Las preguntas típicas aquí son: cuántos voltios deberán usarse para representar un 1 y cuántos para un 0, cuántos microsegundos dura un bit, si la transmisión se puede efectuar simultáneamente en ambas direcciones o no, cómo se establece la conexión inicial y cómo se interrumpe cuando ambos lados han terminado, y cuántas puntas tiene el conector de la red y para qué sirve cada una.

Aquí las consideraciones de diseño tienen mucho que ver con las interfaces mecánica, eléctrica y de procedimientos, y con el medio de transmisión físico que está bajo la capa física.

5.3.2. La capa de enlace de datos.

La **tarea principal de la capa de enlace de datos** es tomar un medio de transmisión en bruto y transformarlo en una línea que parezca libre de errores de transmisión no detectados a la capa de red. Esta tarea la cumple al hacer que el emisor divida los datos de entrada en tramas de datos (unos cientos o miles de bytes, normalmente), que transmita las tramas en forma secuencial y procese las tramas de acuse de recibo que devuelve el receptor. Puesto que la capa física solamente acepta y transmite una corriente de bits sin preocuparse por su significado o su estructura, corresponde a la capa de enlace de datos crear y reconocer los límites de las tramas. Esto se puede lograr añadiendo patrones especiales de bits al principio y al final de la trama. Si estos patrones de bits ocurrieran en los datos por accidente, se debe tener cuidado especial para asegurar que estos patrones no se interpreten incorrectamente como delimitadores de tramas.

Una ráfaga de ruido en la línea puede destruir por completo una trama. En este caso, el software de la capa de enlace de datos de la máquina fuente puede retransmitir la trama. Sin embargo, las transmisiones repetidas de la misma trama introducen la posibilidad de duplicar tramas. Se podría enviar una trama duplicada si se perdiera la trama del acuse de recibo que el receptor devuelve al emisor. Corresponde a esta capa resolver el problema provocado por las tramas dañadas, perdidas y duplicadas. La capa de enlace de datos puede ofrecer varias clases de servicio distintas a la capa de la red, cada una con diferente calidad y precio.

Otra consideración que surge en la capa de enlace de datos (y también de la mayor parte de las capas más altas) es cómo evitar que un transmisor veloz sature de datos a un receptor lento. Se debe emplear algún mecanismo de regulación de tráfico para que el transmisor sepa cuánto espacio de almacenamiento temporal (buffer) tiene el receptor en ese momento. Con frecuencia esta regulación de flujo y el manejo de errores están integrados.

Si se puede usar la línea para transmitir datos en ambas direcciones, esto introduce una nueva complicación que el software de la capa de enlace de datos debe considerar. El problema es que las tramas de acuse de recibo para el tráfico de *A* a *B* compiten por el uso de la línea con tramas de datos para el tráfico de *B* a *A*.

Las redes de difusión tienen una consideración adicional en la capa de enlace de datos: cómo controlar el acceso al canal compartido. En redes de difusión, el problema de repartir el canal para evitar que dos o más emisores se interfieran se denomina "**el control de acceso al medio**", y se suele abreviar MAC (*Media Access Control*). El control de acceso al medio es crítico en el funcionamiento de las redes de difusión, y puede llegar a ser muy complejo. Por ejemplo, en las redes del IEEE, la forma de implementar el control de acceso al medio (y la capa física subyacente) determina el tipo de red de área local. Las redes definidas por el IEEE (ethernet, token bus, token ring, etc....) tienen en común la forma de resolver las tareas anteriormente mencionadas como responsabilidad de la capa de enlace de datos, pero difieren en la forma de realizar el control de acceso al medio. Como consecuencia se aprecia que el control de acceso al medio puede resolverse de forma independiente y distinta de las tareas de entramado, control de errores, y control de flujo en la capa de enlace de datos. Reflejando esta situación, se llega a definir una subcapa especial de la capa de enlace de datos para encargarse de este problema, la **subcapa de control acceso al medio**.

5.3.3. La capa de red.

La capa de red se ocupa de controlar el funcionamiento de la **subred**. Una consideración clave de diseño es determinar cómo se encaminan los paquetes de la fuente a

su destino. Las rutas se pueden basar en tablas estáticas o bien en tablas que se determinan al inicio de cada conversación. Por último, pueden ser altamente dinámicas, determinándose de nuevo con cada paquete para reflejar la carga actual de la red.

Si en la subred se encuentran presentes demasiados paquetes a la vez, se estorbarán mutuamente, formando cuellos de botella. El control de tal congestión pertenece también a la capa de red.

En vista de que los operadores de la subred podrían esperar remuneración por su labor, con frecuencia hay una función de contabilidad integrada a la capa de red. Cuando menos, el software debe contar cuántos paquetes o caracteres o bits envía cada cliente para producir información de facturación. Cuando un paquete cruza una frontera nacional, con tarifas diferentes de cada lado, la contabilidad se puede complicar.

Cuando un paquete debe viajar de una red a otra para alcanzar su destino, pueden surgir muchos problemas. El tipo de direcciones que usa la segunda red puede ser diferente del de la primera, puede ser que la segunda no acepte en absoluto el paquete por ser demasiado grande, los protocolos pueden diferir, y otras cuestiones. La capa de red debe resolver todos estos problemas para lograr que se interconecten redes heterogéneas.

En las redes de difusión el problema del ruteo es simple y la capa de red con frecuencia es delgada o incluso inexistente.

5.3.4. La capa de transporte.

La función básica de la capa de transporte es aceptar datos de la capa de sesión, dividirlos en unidades más pequeñas si es necesario, pasarlos a la capa de red y asegurar que todos los pedazos lleguen correctamente al otro extremo. Además, todo esto se debe hacer de manera eficiente y en forma que aisle a las capas superiores de los cambios inevitables en la tecnología del hardware.

En condiciones normales, la capa de transporte crea una conexión de red distinta para cada conexión de transporte que requiera la capa de sesión. Sin embargo, si la conexión de transporte requiere un volumen de transmisión alto, la capa de transporte podría crear múltiples conexiones de red, dividiendo los datos entre las conexiones para aumentar el volumen. Por otro lado, si es costoso crear o mantener una conexión de red, la capa de transporte puede multiplexar varias conexiones de transporte en la misma conexión de red para reducir el costo. En todos los casos, la capa de transporte debe lograr que la multiplexión sea transparente para la capa de sesión.

La capa de transporte determina también qué tipo de servicio proporcionará a la capa de sesión y, finalmente, a los usuarios de la red. El tipo más popular de conexión de transporte es un canal punto a punto libre de errores que entrega mensajes o bytes en el orden en que se enviaron. Sin embargo, otras posibles clases de servicio de transporte son el transporte de mensajes aislados sin garantía respecto al orden de entrega y la difusión de mensajes a múltiples destinos. El tipo de servicio se determina al establecer la sesión.

La capa de transporte es una verdadera capa de extremo a extremo, del origen al destino. En otras palabras, un programa en la máquina fuente sostiene una conversación con un programa similar en la máquina de destino, haciendo uso de los encabezados de mensajes y de los mensajes de control. En las capas bajas, los protocolos se usan entre cada máquina y sus vecinas inmediatas, y no entre las máquinas de origen y destino, que pueden estar separadas por muchos routers. La diferencia entre las capas 1 a la 3, que están encadenadas, y las capas 4 a la 7, que son de extremo a extremo, se ilustra en la figura de la arquitectura OSI situada al comienzo de este punto. Muchos nodos están multiprogramados, lo que implica que múltiples conexiones entran y salen de cada nodo. En este caso se necesita una manera de saber qué mensaje pertenece a qué conexión. El encabezado de transporte, es una opción para colocar esta información.

Además de multiplexar varias corrientes de mensajes por un canal, la capa de transporte debe cuidar de establecer y liberar conexiones a través de la red. Esto requiere alguna clase de mecanismo de asignación de nombres, de modo que un proceso en una

máquina pueda describir con quién quiere conversar. También debe haber un mecanismo para regular el flujo de información, a fin de que un nodo rápido no pueda saturar a uno lento. Tal mecanismo se llama control de flujo y desempeña un papel clave en la capa de transporte (también en otras capas). El control de flujo entre nodos es distinto del control de flujo entre routers.

5.3.5. La capa de sesión.

La capa de sesión permite a los usuarios de máquinas diferentes establecer sesiones entre ellos. Una sesión permite el transporte ordinario de datos, como lo hace la capa de transporte, pero también proporciona servicios mejorados que son útiles en algunas aplicaciones. Se podría usar una sesión para que el usuario se conecte a un sistema remoto de tiempo compartido o para transferir un archivo entre dos máquinas.

Uno de los servicios de la capa de sesión es manejar el control del diálogo. Las sesiones pueden permitir que el tráfico vaya en ambas direcciones al mismo tiempo, o sólo en una dirección a la vez. Si el tráfico puede ir únicamente en un sentido a la vez (en analogía con una sola vía de ferrocarril), la capa de sesión puede ayudar a llevar el control de los turnos.

Un servicio de sesión relacionado es el manejo de testigos para acceso exclusivo a recursos. Para algunos protocolos es esencial que ambos lados no intenten la misma operación al mismo tiempo. A fin de controlar estas actividades, la capa de sesión proporciona testigos que se pueden intercambiar. Solamente el lado que posea el testigo podrá efectuar la operación crítica.

Otro servicio de sesión es la sincronización. Consideremos los problemas que pueden ocurrir cuando se trata de efectuar una transferencia de archivos de 2 horas de duración entre dos máquinas que tienen un tiempo medio entre rupturas de 1 hora. Cada transferencia, después de abortar, tendría que empezar de nuevo desde el principio y probablemente fallaría también la siguiente vez. Para eliminar este problema, la capa de sesión ofrece una forma de insertar puntos de verificación en la corriente de datos, de modo que después de cada interrupción sólo se deban repetir los datos que se transfirieron después del último punto de verificación.

5.3.6. La capa de presentación.

La capa de presentación realiza ciertas funciones que se piden con suficiente frecuencia para justificar la búsqueda de una solución general, en lugar de dejar que cada usuario resuelva los problemas. En particular, y a diferencia de todas las capas inferiores que se interesan sólo en mover bits de manera segura de acá para allá, la capa de presentación se ocupa de la sintaxis y la semántica de la información que se transmite.

Un ejemplo típico de servicio de presentación es la codificación de datos en una forma estándar acordada. La mayor parte de los programas de usuario no intercambian cadenas de bits al azar, intercambian cosas como nombres de personas, fechas, cantidades de dinero y cuentas. Estos elementos se representan como cadenas de caracteres, enteros, cantidades de punto flotante y estructuras de datos compuestas de varios elementos más simples. Los diferentes ordenadores tienen códigos diferentes para representar cadenas de caracteres (por ejemplo, ASCII y Unicode), enteros (por ejemplo, en complemento a uno y en complemento a dos), y demás. Con el fin de hacer posible la comunicación entre equipos con representaciones diferentes, las estructuras de datos por intercambiar se pueden definir en forma abstracta, junto con un código estándar que se use "en el cable". La capa de presentación maneja estas estructuras de datos abstractas y las convierte de la representación que se usa dentro del equipo a la representación estándar de la red y viceversa.

5.3.7. La capa de aplicación.

La capa de aplicación define los protocolos que usarán las aplicaciones y procesos de usuario. Elige el protocolo de diálogo adecuado, es decir, mientras que la comunicación entre dos procesos residentes en el mismo host se hace a través de las funciones que a tal efecto proporciona el sistema operativo, para la comunicación entre procesos que residen en

diferentes ordenadores, la capa de aplicación utiliza los servicios de las capas inferiores para producir la conexión.

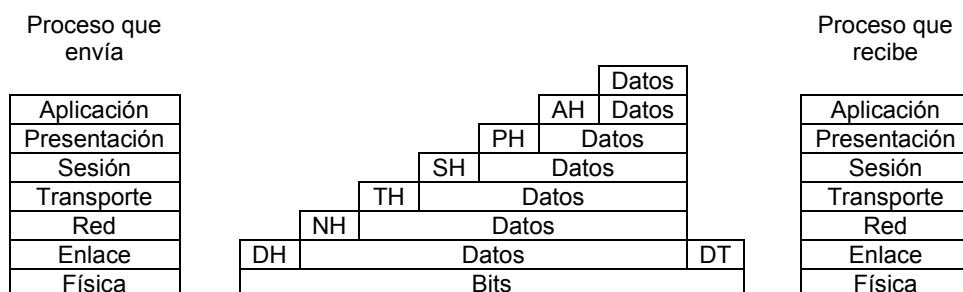
Por ejemplo, existen cientos de tipos de terminales incompatibles en el mundo. Consideremos la situación de un editor de pantalla completa que debe trabajar en una red con muchos tipos diferentes de terminal, cada uno con formatos diferentes de pantalla, secuencias de escape para insertar y eliminar texto, mover el cursor, etcétera.

Una forma de resolver este problema es definir una terminal virtual de red abstracta que los editores y otros programas puedan manejar. Para cada tipo de terminal, se debe escribir un programa para establecer la correspondencia entre las funciones de la terminal virtual de red y las de la terminal real. Por ejemplo, cuando el editor mueva el cursor de la terminal virtual a la esquina superior izquierda de la pantalla, este software debe emitir la secuencia apropiada de órdenes a la terminal real para poner su cursor en ese lugar. Todo el software de terminal virtual está en la capa de aplicación.

Otra función de la capa de aplicación es la transferencia de archivos. Los diferentes sistemas de archivos tienen convenciones diferentes para nombrar los archivos, formas diferentes de representar líneas de texto, etc. La transferencia de un archivo entre dos sistemas diferentes requiere la resolución de éstas y otras incompatibilidades. Este trabajo también pertenece a la capa de aplicación, lo mismo que el correo electrónico, la carga remota de trabajos, la búsqueda en directorios y otros recursos de uso general y especial.

5.3.8. Transmisión de datos en el modelo OSI.

La siguiente figura muestra un ejemplo de cómo se realiza el encapsulamiento de la información en el modelo OSI, para llegar a transmitir los datos entre el emisor y el receptor de la información.



El proceso remitente tiene algunos datos que quiere enviar al proceso receptor, así que entrega los datos a la capa de aplicación, la cual añade entonces al principio el encabezado de aplicación AH (que puede ser nulo) y entrega el elemento resultante a la capa de presentación.

La capa de presentación puede transformar este elemento de diferentes maneras y posiblemente añadir al principio un encabezado, entregando el resultado a la capa de sesión. Es importante darse cuenta que la capa de presentación no sabe qué porción de los datos entregados a ella por la capa de aplicación es la AH, si existe, y cuáles son en verdad los datos del usuario.

Este proceso se repite hasta que los datos alcanzan la capa física, donde son transmitidos realmente a la máquina receptora. En esa máquina se retiran los distintos encabezados, uno por uno, conforme el mensaje se propaga hacia arriba por las capas hasta que por fin llega al proceso receptor.

La idea clave en todo este proceso es que aunque la transmisión real de los datos es vertical en la figura, cada capa se programa como si fuera horizontal. Por ejemplo, cuando la capa de transporte emisora recibe un mensaje de la capa de sesión, le añade un encabezado de transporte y lo envía a la capa de transporte receptora. Desde su punto de vista, el hecho de que en realidad debe dirigir el mensaje a la capa de red de su propia máquina es un tecnicismo sin importancia.

5.4. La arquitectura TCP/IP.

Pasemos ahora del modelo de referencia OSI al modelo que se usa en la abuela de todas las redes de computadoras, la ARPANET, y su sucesora, la red mundial Internet. ARPANET era una red de investigación patrocinada por el DoD (Departamento de Defensa de Estados Unidos).

El proyecto que dio origen a ARPANET tenía como objetivo el comunicar distintos ordenadores para resolver el llamado "problema del terminal": El problema consistía en la necesidad de que un usuario que tuviese que acceder a un ordenador para realizar un trabajo, necesitaba instalar un terminal en su mesa de trabajo, a través del cual podía acceder a ese ordenador. Si por algún motivo, esa persona realizaba trabajos en dos o más ordenadores, debía alojar en su despacho dos o más terminales, lo que resultaba molesto, y costoso. La idea para resolver este problema consistía en establecer comunicación entre todos estos ordenadores, de manera que sólo se colocaba un terminal en la oficina de quien necesitara acceder a ellos. A través del terminal se puede acceder a uno de los ordenadores, de modo que para acceder a los demás se pueden usar las líneas de comunicaciones que los interconectan. De esta forma se evita el problema del terminal. En aquella época, el Ejército de los Estados Unidos era uno de los mayores usuarios de ordenadores del mundo, con lo que el problema del terminal era lo bastante importante para invertir en el desarrollo de un sistema para evitarlo a través de su organización ARPA.

ARPANET conectó a cientos de universidades e instalaciones del gobierno usando líneas telefónicas alquiladas. Cuando más tarde se añadieron redes de satélite y radio, los protocolos existentes tuvieron problemas para interactuar con ellas, de modo que se necesitó una arquitectura nueva. Así, la capacidad de conectar entre sí múltiples redes fue uno de los principales objetivos de diseño desde el principio. Esta arquitectura se popularizó después como la arquitectura TCP/IP, por las iniciales de sus dos protocolos primarios.

En la arquitectura TCP/IP se distinguen cuatro capas: Aplicación, Transporte, Interred, y Host a Red (también denominada de otras formas: Nodo a Red, Subred, Enlace,.....).

En el siguiente esquema se puede apreciar la correspondencia entre las capas de la arquitectura TCP/IP y el modelo de referencia OSI:

OSI		TCP/IP
Aplicación		Aplicación
Presentación		
Sesión		
Transporte		Transporte
Red		Interred
Enlace		Host a red
Física		

5.4.1. La capa de Interred (capa de Internet).

Todos estos requerimientos condujeron a la elección de una red de conmutación de paquetes basada en una capa de interred carente de conexiones. Esta capa, llamada capa de interred, es el eje que mantiene unida toda la arquitectura. La misión de esta capa es permitir que los nodos inyecten paquetes en cualquier red y los hagan viajar de forma independiente a su destino (que podría estar en una red diferente). Los paquetes pueden llegar incluso en un orden diferente a aquel en que se enviaron, en cuyo caso corresponde a las capas superiores reordenarlos, si se desea la entrega ordenada.

La capa de interred define un formato de paquete y protocolo oficial llamado IP (*Internet Protocol*) definido en el RFC 791. El trabajo de la capa de interred es entregar paquetes IP a donde se supone que deben ir. Aquí la consideración más importante es claramente el ruteo de los paquetes, y también evitar la congestión. Por lo anterior es razonable decir que la capa de interred TCP/IP es muy parecida en funcionalidad a la capa de red OSI. La siguiente figura muestra la correspondencia.

5.4.2. La capa de Transporte.

La capa que está sobre la capa de interredes en el modelo TCP/IP se llama capa de transporte. Esta capa se diseñó para permitir que las entidades pares en los nodos de origen y destino lleven a cabo una conversación, lo mismo que en la capa de transporte OSI. Aquí se definieron dos protocolos de extremo a extremo. El primero, TCP (*Transmission Control Protocol*), definido en el RFC 793, es un protocolo seguro orientado a la conexión que permite que una corriente de bytes originada en una máquina se entregue sin errores en cualquier otra máquina de la interred. Este protocolo fragmenta la corriente entrante de bytes en mensajes discretos y pasa cada uno a la capa de interred. En el destino, el proceso TCP receptor reensambla los mensajes recibidos para formar la corriente de salida. TCP también se encarga del control de flujo para asegurar que un emisor rápido no pueda abrumar a un receptor lento con más mensajes de los que pueda manejar.

El segundo protocolo de esta capa, el UDP (*User Datagram Protocol*), definido en RFC el 768, es un protocolo no orientado a conexión y no seguro, para aplicaciones que no necesitan la asignación de secuencia ni el control de flujo del TCP y que desean utilizar los suyos propios. Este protocolo también se usa ampliamente para consultas de petición y respuesta de una sola ocasión, del tipo cliente-servidor, y en aplicaciones en las que la entrega pronta es más importante que la entrega precisa, como las transmisiones de voz o vídeo.

5.4.3. La capa de Aplicación.

El modelo TCP/IP no tiene capas de sesión ni de presentación. No se pensó que fueran necesarias, así que no se incluyeron. La experiencia con el modelo OSI ha comprobado que esta visión fue correcta: se utilizan muy poco en la mayor parte de las aplicaciones.

Encima de la capa de transporte está la capa de aplicación, que contiene todos los protocolos de alto nivel. Entre los protocolos más antiguos están el de terminal virtual (TELNET), el de transferencia de archivos (FTP) y el de correo electrónico (SMTP). El protocolo de terminal virtual permite que un usuario en una máquina acceda a una máquina remota y trabaje ahí. El protocolo de transferencia de archivos ofrece un mecanismo para mover datos de una máquina a otra de forma eficiente. El correo electrónico fue en sus orígenes sólo una clase de transferencia de archivos, pero más adelante se desarrolló para él un protocolo especializado. Con los años, se le han añadido muchos otros protocolos, como el servicio de nombres de dominio, (DNS) para relacionar los nombres de los nodos con sus direcciones de la red, NNTP, el protocolo que se usa para transferir noticias (*news*), HTTP, el protocolo que se usa para recuperar páginas en la World Wide Web y muchos otros.

5.4.4. La capa host a red.

Bajo la capa de interred hay un gran vacío. La arquitectura TCP/IP realmente no dice mucho de lo que aquí sucede, salvo indicar que el nodo se ha de conectar a la red haciendo uso de algún protocolo de modo que pueda enviar por ella paquetes IP. Este protocolo no está definido y varía de un nodo a otro y de red a red. Los libros y artículos sobre el modelo TCP/IP rara vez hablan de él.

6. Las redes de área local.

6.1. Características de una Red Local.

Una definición de red de área local o LAN (Local Area Network) proporcionada por IEEE es: "Una red de área local se distingue de otros tipos de redes de datos en que las comunicaciones están normalmente confinadas en un área geográfica limitada tal como un edificio de oficinas, un almacén o un campus; utilizando un canal de comunicación de velocidad moderada o alta y una tasa de error baja". Esta definición pone de manifiesto los elementos esenciales de cualquier LAN: ámbito, seguridad y velocidad.

Una LAN es por tanto, el conjunto de elementos físicos y lógicos (*hardware* y *software*) que interconectan dispositivos en un área privada y restringida. Sus principales características

son la restricción geográfica, la alta velocidad de transmisión y la fiabilidad de las transmisiones debido a tasas de error bajas.

El escenario que podemos encontrar en este tipo de redes puede ir desde unos pocos equipos informáticos interconectados para compartir información, hasta un sistema complejo que abarca diversas plantas de un edificio, o varios edificios, interconectando dispositivos informáticos, multimedia, de control y seguridad.

En este tema abordaremos las redes de área local, comenzando por sus componentes y elementos comunes, con mención especial al sistema operativo de red (NOS) y a los recursos que habitualmente se utilizan mediante la red de área local.

Tradicionalmente, las LAN's utilizaban medios de difusión, e incluso actualmente, todas las comunicaciones inalámbricas tienen la característica de compartir un único canal, por lo que dos estaciones que emitan señales al mismo tiempo se interfieren. El método que define la manera de resolver este problema se denomina "Control de Acceso al Medio" (MAC), está muy ligado al medio físico utilizado, y es muy importante para la operativa de la LAN, definiendo muchas de sus propiedades.

Entre las distintas redes de área local que ha definido el IEEE o adoptado de otros organismos de estandarización, estudiaremos especialmente dos de ellas, las variantes de la IEEE 802.3 también denominada "Ethernet", y las variantes de la IEEE 802.11 comúnmente conocidas como "Wi-Fi".

Destaquemos las características más importantes de las redes de área local:

- **Extensión limitada:** Una red local interconecta equipos en un domicilio, oficina, plantas de oficinas de un edificio, o edificios cercanos. La distancia máxima entre dos estaciones de la red debe limitarse a unos pocos kilómetros (dos o tres).
- **Titularidad privada:** Las redes locales son pequeñas y pueden ser instaladas por la organización que hará uso de la red, ya que su costo no es muy elevado. Por lo tanto, todos los elementos de la red local pertenecen a la organización que la utiliza, y también debe encargarse de su correcto funcionamiento.
- **Altas velocidades de transmisión:** Los medios utilizados en redes locales cubren distancias cortas y por lo tanto pueden ser de alta calidad sin que los costos resulten elevados. Desde las primeras redes locales a 10 Megabits por segundo, estas redes siempre han proporcionado a los equipos altas velocidades de transmisión de datos comparadas con las ofrecidas por redes de mayor extensión. En la actualidad, las redes locales pueden proporcionar desde 1 Gigabit por segundo hasta 10 Gigabits por segundo. Existen estándares para proporcionar 40 Gigabits por segundo y 100 gigabits por segundo, aunque no son de uso común y algunos de ellos aún están en desarrollo.
- **Baja tasa de errores:** Dado que los medios utilizados en redes locales son de alta calidad, y se suelen instalar específicamente para las comunicaciones de datos, la fiabilidad de las transmisiones es muy alta en comparación con redes de mayor extensión.
- **Privacidad:** Dado que son redes de titularidad privada, no es posible que usuarios que no pertenezcan a la organización accedan libremente a la red o a los dispositivos que la componen. Las instalaciones de red, los equipos desde los que se accede a la red, y los espacios donde se instalan son privados, y habitualmente con acceso restringido. Esto reduce la posibilidad de que usuarios no autorizados puedan llegar a interceptar las comunicaciones para obtener datos de la organización. En el caso de las redes inalámbricas, el problema de la seguridad es uno de los que se deben resolver a la hora de poder utilizarse dentro de una red local de una empresa u organización.
- **Difusión:** Los primeros estándares de redes de área local utilizaban medios de difusión. Aunque en la actualidad se tiende a que las redes de área local trabajen con tecnologías de conmutación, el hecho de que el software (protocolos) usado en

la red haya sido diseñado en redes de difusión, conlleva a que las transmisiones de difusión sean importantes cuando se trata de utilizar una red local. Los medios y dispositivos utilizados en la red local deben permitir las transmisiones de difusión en las que una estación envía datos a varias estaciones de la red (o a todas).

- **Compartición de recursos:** A diferencia de otras redes de comunicaciones, las redes locales se han utilizado ampliamente en entornos privados para compartir recursos entre las distintas estaciones de la red. Esta finalidad fundamental dirige su diseño, características y prestaciones.

6.2. Ventajas e inconvenientes de una red local

En la actualidad no se concibe el funcionamiento de equipos informáticos aislados, sin conexión a una red. Esto es porque las redes proporcionan una gran cantidad de ventajas:

- **Economía.** Las redes locales reducen costos de diversas formas. Reducen el costo de adquisición de dispositivos, ya que mediante la red local es posible compartir dispositivos tales como impresoras, escaners y espacio de almacenamiento entre distintos usuarios en lugar de proporcionar uno de estos dispositivos a cada usuario que lo necesite. Reducen el costo de administración ya que permiten centralizar datos y servicios, lo que facilita el trabajo al administrador. También reducen el costo de las comunicaciones ya es posible compartir una o varias líneas de comunicaciones mediante la red local, e incluso optimizar la utilización de las líneas contratadas.
- **Eficiencia.** Varios aspectos y funcionalidades de las redes locales mejoran la eficiencia. Si los datos están centralizados en un punto, se evita el tener que introducir varias veces los mismos datos, se garantiza la coherencia de los mismos, y permite a cualquier usuario acceder a todos los datos. El hecho de poder acceder a recursos compartidos, permite a cada usuario el poder utilizar los recursos más adecuados en cada momento, y al mismo tiempo, permite que estos recursos estén mejor aprovechados. Por ejemplo: La posibilidad de acceder a todos los datos de la empresa mediante la red proporciona la dirección una información exhaustiva, completa y actualizada con la que poder tomar decisiones. Otro ejemplo: un usuario que suele imprimir documentos en blanco y negro con calidad media, cuando puntualmente necesita imprimir en color con alta calidad, puede escoger entre las impresoras de color disponibles en la red, la que mejor se ajuste a sus necesidades sin tener que pedir a un administrador que le instale una en su equipo. Otro ejemplo: Cada factura debe aparecer en una anotación contable, por lo tanto, cuando se imprime una factura, un usuario de contabilidad debe pasar los datos de dicha factura a la contabilidad de la empresa. Con una aplicación de red, en el momento de realizar la factura los datos pueden pasar a la contabilidad directamente como una anotación contable, evitando el trabajo de introducir datos por duplicado, y evitando también cualquier error, además de que la contabilidad de la facturación está actualizada de forma instantánea.
- **Comunicación.** Posibilita cualquier medio de comunicación interno (mail, Chat, VoIP, Messenger, news, gopher, etc.) y externo, en redes de datos o compartiendo redes de telefonía, televisión, telefonía móvil, etc. Por ejemplo: en muchas empresas se utilizan aplicaciones de mensajería y videoconferencia para las comunicaciones internas, lo que evita en gran medida las costosas reuniones en persona.
- **Administración.** La administración de los sistemas informáticos puede realizarse remotamente lo que permite al administrador realizar más trabajo en menos tiempo al evitarle desplazamientos innecesarios. Además, el administrador dispone de gran cantidad de herramientas para detectar posibles problemas o incidencias, incluso cuando aún no se han producido, adelantando por tanto su resolución. También mejora el trabajo del administrador al centralizar recursos tales como cuentas de seguridad, datos, o acceso a líneas de comunicaciones, ya que es más fácil y

rápido administrar recursos centralizados que recursos distribuidos por toda la empresa. Por ejemplo: si todos los datos residen en los servidores de datos, realizar copias de seguridad de la información es mucho más fácil, rápido, y sencillo que hacer una copia de seguridad de los datos de cada uno de los equipos de trabajo de la organización.

- **Procesamiento distribuido.** Potencialmente se pueden gestionar los equipos trabajando individualmente o en conjunto, compartiendo procesador, RAM y/o sistemas de almacenamiento. Por ejemplo: en una empresa que realiza labores intensivas de procesamiento gráfico, es posible utilizar los recursos gráficos de varios equipos para renderizar una secuencia de vídeo reduciendo drásticamente el tiempo empleado por un solo equipo. Otro ejemplo: mediante una red local de alta velocidad se puede montar un "*cluster*" de procesamiento en el que varias máquinas realizan cálculos al mismo tiempo para resolver un problema, con un rendimiento similar a supercomputadores mucho más costosos.
- **Modularidad.** Las redes locales permiten su ampliación de forma sencilla, tanto en extensión, añadiendo nuevos dispositivos y zonas de cobertura, como en tecnologías, mejorando capacidades de comunicación y servicios sin tener que abandonar los antiguos dispositivos y servicios.
- **Disponibilidad.** Mediante las comunicaciones es posible duplicar los recursos críticos, de forma que si quedara fuera de servicio uno de ellos, el de respaldo asumiría todas las funciones de forma transparente para los usuarios. También es posible asegurar el buen funcionamiento de los equipos donde residen los recursos más importantes a un costo asumible. Por ejemplo: La disponibilidad e integridad de los datos que residen en los servidores que centralizan la información de la empresa pueden protegerse mediante sistemas de alimentación ininterrumpida, discos espejo, fuentes de alimentación redundante, y otras medidas que serían económicamente inviables si se tuvieran que aplicar a todos los equipos de la organización.
- **Movilidad.** Al acceder a los recursos de trabajo a través de la red, tanto los usuarios como los dispositivos pueden reubicarse sin problemas, siempre que en la nueva ubicación se pueda acceder a la red. Por ejemplo, si se estropea una estación de trabajo con la que trabaja un usuario, gracias a la red, el usuario podrá iniciar sesión en cualquier otra estación de trabajo disponible para trabajar con normalidad accediendo a sus datos y recursos ya que están en los servidores.

Pero el uso de redes de datos no solo tiene ventajas, también presenta inconvenientes:

- **Obsolescencia y falta de estandarización.** En las redes de datos las tecnologías evolucionan continuamente, y en muchas ocasiones los fabricantes no esperan a que se desarrolle un estándar consensuado para ofrecer dispositivos a los clientes. Esto puede hacer que dos aplicaciones iguales, en distintas versiones, no sean compatibles y no puedan comunicarse bidireccionalmente, o que la costosa infraestructura de red que se ha instalado en la empresa no pueda soportar las nuevas aplicaciones contratadas al haber quedado obsoleta en poco tiempo. Por ejemplo: en las redes inalámbricas se han comercializado dispositivos cuyas funcionalidades y capacidades de interconexión eran incompatibles con dispositivos de otros fabricantes porque no cumplían estándares (modos WDS en redes WiFi), incluso se han llegado a comercializar dispositivos según las especificaciones provisionales de estándares no aprobados y todavía en una fase muy temprana de desarrollo (dispositivos "*draft*").
- **Complejidad.** La tarea de mantener el buen funcionamiento de los equipos informáticos se complica con la necesidad de que las comunicaciones y los servicios definidos estén disponibles en todo momento. El diseño de los recursos

compartidos y el mantenimiento de su disponibilidad, puede llegar a ser una tarea muy compleja en organizaciones con gran cantidad de dispositivos.

- **Seguridad (confidencialidad).** Las redes complican el mantenimiento de la privacidad. Dado que los usuarios pueden acceder a recursos desde cualquier equipo conectado a la red, una intrusión o un acceso no autorizado a los datos puede estar llevándose a cabo desde cualquier punto de la organización, incluso desde el exterior, a través de la conexión de la red local con otras redes. Esta situación pone en peligro tanto la privacidad de los datos como su integridad.
- **Disponibilidad.** En una red local, existen dispositivos que al quedar fuera de servicio pueden afectar al funcionamiento de todo el sistema. Algunos servidores, y dispositivos de interconexión de red son tan críticos que al quedar fuera de servicio provocarían que la organización entera no pudiera funcionar adecuadamente. Debe ser una tarea prioritaria de la administración de sistemas el garantizar que dichos elementos de la red no queden fuera de servicio cuando son necesarios, o en el peor de los casos, garantizar su puesta en marcha en el menor tiempo posible.

6.3. Aplicaciones de las redes de área local.

Las LAN's se utilizan fundamentalmente para compartir recursos entre los equipos informáticos de una empresa, oficina, o residencia.

Entre los recursos que se distribuyen entre las estaciones mediante una red de área local encontramos:

- **Datos.** Una empresa debe centralizar su información. Los usuarios (estaciones informáticas) consultan y actualizan información como parte de su labor cotidiana. La información debe estar disponible para quien la necesite y además debe estar actualizada. También es importante para garantizar la seguridad y disponibilidad de los datos.
- **Comunicaciones.** Es inviable contratar una línea de comunicaciones para cada estación informática que la necesite. Por ello, se comparten las contratadas entre todas las estaciones que precisen de comunicaciones de área extensa.
- **Capacidad de proceso numérico/gráfico.** Las estaciones con capacidades avanzadas de proceso son caras, y no pueden asignarse a un solo usuario, que la mayor parte del tiempo está interactuando con el interfaz del sistema operativo. Mediante la red, es posible programar un trabajo con altas necesidades de procesamiento numérico o gráfico en una estación barata, enviarlo a una estación de proceso compartida, y recibir los resultados cuando el trabajo sea ejecutado.
- **Dispositivos físicos.** Muchos dispositivos utilizados por las estaciones informáticas se pueden compartir, evitando el tener que adquirir uno para cada equipo que lo precise. Como ejemplo podríamos mencionar los dispositivos de impresión, faxes, o escaners que pueden compartirse a través de la LAN.
- **Servicios.** Una red local permite centralizar gran cantidad de servicios como por ejemplo: correo electrónico, agenda electrónica, notificación de incidencias, control de la seguridad de usuarios, chat, mensajería interna, copia de seguridad, y otros muchos.
- **Aplicaciones.** Una red local facilita a los usuarios el poder trabajar con aplicaciones que, por motivos técnicos o de licencias, no residen en su estación de trabajo sino en un servidor de aplicaciones.