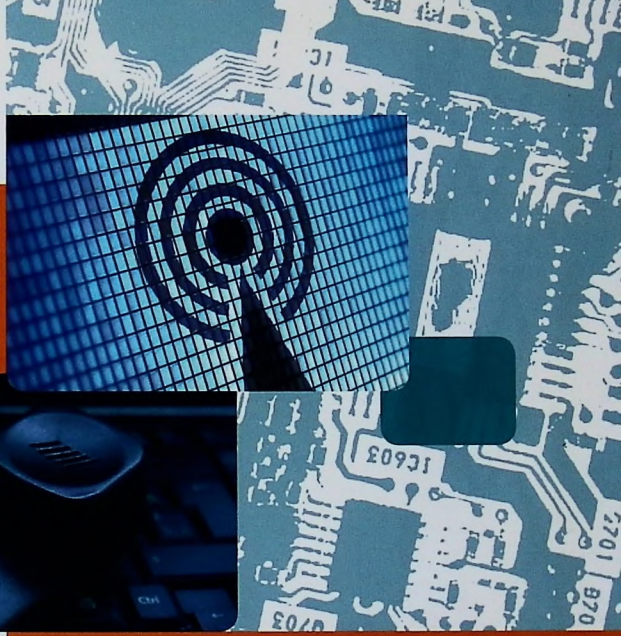


Instalaciones de Telecomunicaciones

Infraestructuras de redes de datos y sistemas de telefonía

Miguel Moro Vallina

ELECTRICIDAD - ELECTRÓNICA

0000014379
6

Paraninfo
ciclos formativos

Títulos relacionados

ELECTRÓNICA APLICADA

PABLO ALCALDE SAN MIGUEL
ISBN: 978-84-9732-780-0

INSTALACIONES DOMÓTICAS

MIGUEL MORO VALLINA
ISBN: 978-84-9732-857-9



Solicítalos en

- Librería
- www.paraninfo.es
- Solicitudes nacionales 902 995 240
- Solicitudes fuera de España +34 913 308 907
  +34 913 308 919

MFN 0000044379
004.6
M67
Inf
2013

Universidad Técnica del Norte
BIBLIOTECA
Ibarra Ecuador

<REDES DE DATOS>
<SISTEMAS DE TELEFONÍA>
<TRANSMISIÓN DE DATOS>

Infraestructuras de redes de datos y sistemas de telefonía

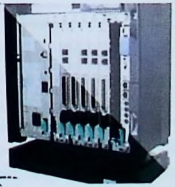












Miguel Moro Vallina

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA
Vía de adquisición: Donación
Documento N°: 03.44895
Fecha: 30/07/2014
Valor unitario: 60.00
Código de Barras: 044806

Paraninfo

Paraninfo

Infraestructuras de redes de datos y sistemas de telefonía

© Miguel Moro Vallina

Gerente Editorial
María José López Raso

Equipo Técnico Editorial
Alicia Cerviño González
Nuria Duarte González

Editora de Adquisiciones
Carmen Lara Carmona

Producción
Nacho Cabal Ramos

Diseño de cubierta
Ediciones Nobel

Preimpresión
Copibook

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

COPYRIGHT © 2013 Ediciones Paraninfo, SA
1ª edición, 2013

Av. Filipinas 50, Bajo A / 28003 Madrid, ESPAÑA
Teléfono: 902 995 240 / Fax: 914 456 218
clientes@paraninfo.es / www.paraninfo.es

ISBN: 978-84-9732-874-6
Depósito legal: M-7009-2013

(10828)

Impreso en España /*Printed in Spain*
Lavel Industria Gráfica
Humanes (Madrid)



Contenido

Agradecimientos VII
Presentacion IX

1. Información y comunicaciones 1

1.1. Conceptos básicos en las comunicaciones.. 2
1.1.1. Las ondas electromagnéticas 2
1.1.2. Emisor, receptor y circuito..... 3
1.1.3. Dígitos binarios 3
1.1.4. Redes de comunicaciones 3
1.1.5. Medios guiados y medios inalámbricos. 5
1.1.6. Atenuación e interferencias sobre la señal 5
1.1.7. El ancho de banda y la onda portadora 5
1.1.8. Modo de transmisión 6
1.2. Señales analógicas y señales digitales 6
1.2.1. Codificación analógica/digital 6
1.2.2. Codificación digital o analógica 7
1.2.3. La conmutación 7
1.2.4. La multiplexación..... 7
1.2.5. Detección y corrección de errores... 8
1.3. Protocolos y estándares 9
1.3.1. Los estándares y su importancia ... 9
1.4. Topologías de red 11
1.5. El modelo OSI 13
1.5.1. Funciones de las capas 13
Mapa conceptual..... 17
Cuestiones 18
Actividades de aplicación 19
Lectura 20

2. Infraestructura de las redes de datos 21

2.1. La infraestructura de las redes de datos y el modelo OSI 22
2.1.1. Ethernet 22
2.1.2. Wi-Fi 23
2.2. Medios de transmisión 24
2.2.1. Par trenzado 24
2.2.2. Cable coaxial..... 26
2.2.3. Fibra óptica..... 28
2.2.4. Medios inalámbricos 28
2.3. Cableado en las redes de datos 31
2.3.1. Suelo técnico 31
2.3.2. Techo técnico 32
2.3.3. Canaletas de superficie 32
2.3.4. Puntos de acceso 33
2.4. Otros elementos de la red de datos..... 34
2.4.1. Cableado estructurado..... 35
2.5. Control de acceso al medio..... 36
Mapa conceptual..... 38
Práctica profesional..... 39
Cuestiones 53
Actividades de aplicación 54

3. Redes de telefonía 55

3.1. El circuito telefónico: historia y características. 56
3.1.1. Historia y evolución de los sistemas telefónicos 56
3.1.2. El sonido en la transmisión telefónica. 57
3.2. La red conmutada..... 58
3.2.1. Jerarquía y sistemas de conmutación 59
3.3. Señalización y transmisión de voz en la red telefónica..... 64
3.3.1. Red SS7 65
3.4. La red de abonados y su infraestructura física. 66
3.4.1. Repartidor de abonados..... 66
3.4.2. Cables de alimentación 66
3.4.3. Cables de distribución 68

3.4.4. Línea de acometida 68
3.4.5. Línea interior de abonado 68
3.4.6. Infraestructuras Comunes de Telecomunicaciones 68
3.5. Telefonía analógica y digital 70
3.5.1. Errores y distorsiones en la transmisión analógica 72
3.5.2. Codificación digital de la voz 72
3.5.3. La Red Digital de Servicios Integrados (RDSI) 72
3.5.4. Errores y distorsiones en la señal digital. 73
3.5.5. Transmisión de datos a través de la red telefónica: ADSL 74
3.6. Redes de telefonía móvil 75
3.6.1. GSM 75
3.6.2. Comunicaciones de datos en la telefonía móvil 77
3.7. Sistemas privados de telefonía (PBX) 77
3.8. Medida del tráfico telefónico 79
Mapa conceptual 81
Práctica profesional 82
Cuestiones 84
Actividades de aplicación 85
Lectura 86

4. Redes de transmisión de datos 87

4.1. La arquitectura TCP/IP 88
4.1.1. Paquetes de datos o datagramas ... 89
4.1.2. Direcciones IP 90
4.1.3. Resolución de direcciones IP 92
4.2. La capa de transporte 93
4.3. La capa de aplicación 94
4.3.1. La resolución de nombres y los servidores DNS 95
Mapa conceptual 97
Práctica profesional 98
Cuestiones 117
Actividades de aplicación 118

5. Telefonía IP y convergencia de voz y datos 119

5.1. ¿Qué es la telefonía IP? 120
5.1.1. Ventajas (e inconvenientes) de la telefonía IP 121
5.1.2. Las capas de una red VoIP 121
5.2. Componentes de un sistema VoIP 123
5.2.1. Servidores VoIP 123
5.2.2. Terminales telefónicos 123
5.2.3. Teléfonos ***software*** o ***softphones*** (***software phones***) 124
5.2.4. Conexión a la red telefónica conmutada. 125
5.3. Protocolos de la red 125
5.3.1. Calidad del servicio (QoS) 126
5.4. Asterisk 127
5.5. Convergencia de voz y datos 129
Mapa conceptual 131
Práctica profesional 132
Cuestiones 145
Actividades de aplicación 146



Agradecimientos

Para la elaboración de este libro he tenido la suerte de contar con el grandísimo apoyo de numerosas personas, instituciones y empresas, sin las que habría sido imposible completar este proyecto. En unos casos (quiero destacar de forma especial la labor de Antonio Pérez Luna), me han proporcionado sugerencias o indicaciones que me han guiado en la estructuración de los contenidos y el sentido global de la obra; en otros, se han cedido amablemente imágenes, dibujos, textos, diagramas... para su inclusión en el libro.

De este modo, no puedo dejar de expresar mi gratitud a Antonio Pérez Luna, Julio Barbancho Concejero, Jaime Benjumea Mondéjar, Octavio Rivera Romero, María del Carmen Romero Ternero, Jorge Ropero Rodríguez, Gemma Sánchez Antón, Francisco Sivianes Castillo, Pedro de Miguel Anasagasti, Isidoro Berral Montero, José Damián Cabezas Pozo, José Manuel Huidobro Moya, Rafael Conesa Pastor y David Ardisana Molleda; además de a empresas e instituciones como Belden Inc., Cisco, Corning Inc., Digium, Legrand, Museum of Communications (Seattle), Organización Internacional de Estándares y Simon.

En todos los casos hemos citado la fuente a la que pertenece el material gráfico empleado. A todos ellos, mi más sincero agradecimiento.



Presentación

Las comunicaciones, el intercambio de información, constituyen el sistema nervioso de nuestra sociedad. Al igual que las neuronas y sus sinapsis en los seres humanos y otros mamíferos transmiten los impulsos del cerebro a todo el cuerpo, también el gran sistema nervioso de las comunicaciones, formado por innumerables nodos y conexiones, transmite la información a todos los lugares del planeta. Aunque con una diferencia importante: si en el sistema nervioso animal existe un centro (el cerebro) que controla todo el proceso, la gran red de comunicaciones tejida en la superficie de nuestro planeta opera como una suerte de inteligencia distribuida por innumerables nodos.

En origen, el desarrollo de las redes de datos aparece vinculado especialmente al proceso productivo y a las necesidades de comunicación de los gobiernos y los centros de decisión militar. Desde ahí, el uso de las redes se ha extendido progresivamente a casi todos los ámbitos de nuestra existencia, replanteando nuestro consumo, nuestro ocio, nuestras necesidades y nuestros pensamientos. Las consecuencias psicológicas, sociales y antropológicas de todo ello son incalculables, y hoy apenas comenzamos a entreverlas.

El intercambio de información a distancia es tan antiguo como la propia humanidad y la existencia del lenguaje y, posteriormente, de la escritura. En el siglo XIX, sin embargo, se produce un avance que revoluciona las comunicaciones: la transmisión de la información a través de un conductor eléctrico. Primero la telegrafía y después la telefonía, ya plenamente establecida (aun en su forma primitiva) a fines del XIX, alumbran un nuevo modelo de comunicación basado en la inmediatez. Durante el siglo XX la red telefónica experimenta un desarrollo exponencial, y a partir de la década de 1960, con el desarrollo de los ordenadores, aparece un nuevo actor en juego: la información digital.

El desarrollo de las redes de comunicaciones y su interconexión ha requerido la formulación de gran número de protocolos y estándares y de la elaboración de un modelo de referencia en el que ubicarlos. Ese modelo de referencia, introducido en la **Unidad 1** —junto con otros conceptos básicos para comprender las comunicaciones—, será una guía para el estudio de las redes de datos y telefonía.

La **Unidad 2** aborda la infraestructura, propiamente dicha, de las redes de datos: se estudiarán los medios de transmisión de las redes, las canalizaciones por las que discurren, los tipos de conectores, etcétera.

La red telefónica es el objeto de la **Unidad 3**. En ella se explica el funcionamiento de la red telefónica pública conmutada, en sus versiones analógica y digital, de la telefonía móvil y de la transmisión de voz y de datos a través de ambas. También se abordan las redes de telefonía privadas o sistemas PBX.

La **Unidad 4** aborda el funcionamiento y la configuración de las capas superiores de las redes de datos. Se estudia la pila de protocolos TCP/IP —que constituyen la médula espinal de Internet— y las funciones asignadas a cada uno de estos protocolos. También se explica extensamente cómo configurar la red en diversos sistemas operativos, además de cómo configurar redes mixtas con equipos Windows y GNU/Linux.

La robustez y la versatilidad de los protocolos TCP/IP parecen marcar una tendencia en la que toda la comunicación (datos, voz, televisión, vídeo) se transmitirá a través de paquetes IP. En particular, las redes de voz sobre IP (VoIP) son una solución de creciente implantación en empresas e instituciones de todo tipo. La **Unidad 5** tiene como objeto el estudio de la telefonía IP y analiza el creciente proceso de convergencia de voz y datos. Por último, se introduce Asterisk, un potente sistema de comunicaciones VoIP con licencia de software libre, explicando su instalación y su configuración básica.

Los contenidos de este libro están adaptados al currículo del módulo formativo Infraestructuras de Redes de Datos y Sistemas de Telefonía, perteneciente al Título de Técnico en Instalaciones de Telecomunicaciones de grado medio, de la familia profesional de Electricidad y Electrónica, según el Real Decreto 1632/2009 (publicado en el BOE de 30 de octubre), y que forma parte de la oferta de formación profesional relativa al Catálogo Nacional de Cualificaciones Profesionales.

Nos hemos esforzado por dar a la obra un marcado contenido práctico, y tratado de combinar este carácter con el rigor y la profundidad en las explicaciones de los conceptos y las tecnologías estudiadas. Además, todas las Unidades cuentan con Actividades propuestas y Actividades resueltas a medida que se avanza en la teoría contenida en ellas, y, al final de estas, con Cuestiones y Actividades de aplicación que permiten al alumno comprobar sus conocimientos y afianzar lo aprendido. Además, las Unidades 2 a 5 cuentan también con extensas **Prácticas profesionales**, en las que se aborda metódicamente la resolución de problemas concretos mediante la aplicación de lo aprendido a lo largo de la Unidad. Por último, cabe destacar que tanto el autor como la editorial aconsejan que dichos ejercicios sean llevados a cabo por el alumno en su propio cuaderno y no sobre el libro.

Universidad Técnica del Norte
BIBLIOTECA
Ibarra Ecuador



1 Información y comunicaciones

¿Cómo se transmite la información a través de una red de comunicaciones? El objetivo de este libro es estudiar la infraestructura en la que se basa una red, ya sea telefónica o de datos. Pero ambas poseen muchos elementos en común y, de hecho, tienden a converger formando una única red de transmisión de información. En esta Unidad estudiaremos los fundamentos de la comunicación a través de una red, sus capas y sus topologías, antes de adentrarnos en los pormenores de cada uno de los tipos específicos de redes.

Contenidos

1.1. Conceptos básicos en las comunicaciones
1.2. Señales analógicas y señales digitales
1.3. Protocolos y estándares
1.4. Topologías de red
1.5. El modelo OSI

Objetivos

- Comprender los conceptos básicos de funcionamiento de un sistema de comunicaciones, sus fundamentos físicos y los problemas de atenuación e interferencias a los que puede verse sometido.
- Conocer la diferencia entre las señales analógicas y digitales, adquiriendo una idea de la importancia de la codificación de una señal analógica en digital y viceversa.
- Entender la importancia del concepto de protocolo, de gran importancia en el establecimiento de una red de comunicaciones.
- Conocer las principales topologías que pueden establecerse en una red de comunicaciones.
- Comprender el concepto de capa en una red de comunicaciones y ser capaces de distinguir las diferentes capas del modelo OSI.

1.1. Conceptos básicos en las comunicaciones

Las comunicaciones que se efectúan en una red telefónica o de datos se basan, todas ellas, en unos principios generales; existen, así, una serie de conceptos básicos de los que nos ocuparemos en este primer apartado.

1.1.1. Las ondas electromagnéticas

Cuando los electrones se mueven, crean ondas electromagnéticas que se propagan en el espacio. James Maxwell predijo la existencia de estas ondas en 1865, que posteriormente fue confirmada por Heinrich Hertz, en 1887. Todas las comunicaciones en la actualidad se basan en la manipulación y el control de diversas clases de ondas electromagnéticas.

> **Recuerda que...**
>
> Se denomina hercio a la unidad de medida de la frecuencia en el Sistema Internacional de unidades; el hercio representa un ciclo por segundo, entendiendo el ciclo como la repetición de cierto suceso. En el caso de las radiaciones electromagnéticas, el hercio es la cantidad de veces que se repite una onda en una duración de un segundo.

Dos parámetros básicos en la determinación de una onda (electromagnética u otra) es la longitud de onda y la frecuencia. Ambas magnitudes están relacionadas entre sí, puesto que al multiplicarlas obtenemos la velocidad a la que se propaga la onda en un medio determinado. La distancia entre dos crestas o dos valles sucesivos en una onda se denomina *longitud de onda*, y el trozo de onda situado entre esos dos puntos se denomina *ciclo de onda* o simplemente *ciclo*. El número de variaciones o ciclos que la onda experimenta en un segundo se mide en una unidad denominada *hercio*.

El conjunto de todos los valores posibles de frecuencia de las radiaciones electromagnéticas conforma su *espectro*, el *espectro electromagnético*, que se representa en la **Figura 1.1**.

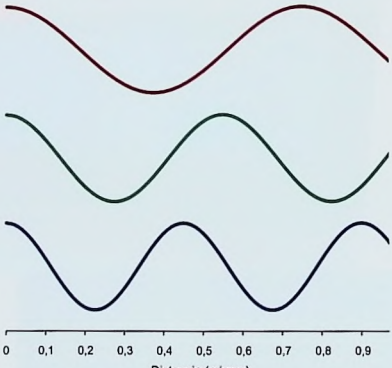


Figura 1.2. Longitudes de onda correspondientes a diversos colores del espectro visible.

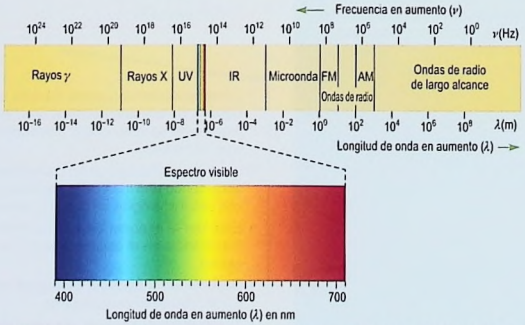


Figura 1.1. Espectro de la radiación electromagnética. Los rayos gamma son los de menor longitud de onda y mayor frecuencia; a la inversa, las ondas de radio son las de mayor longitud de onda y menor frecuencia. La delgada franja que forma el espectro visible va del violeta (menor longitud de onda) al rojo (mayor longitud de onda).

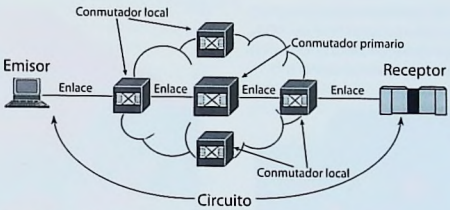


Figura 1.3. Circuito sencillo entre un emisor y un receptor, con varios enlaces y conmutadores.

Actividad resuelta 1.1. Las ondas de radio que se emplean para la comunicación a través de redes Wi-Fi tienen una frecuencia de 2,4 GHz. ¿Cuál es su longitud de onda?

Solución. Para resolver el ejercicio debemos considerar la velocidad de propagación de las ondas electromagnéticas, que tomaremos $c = 3 \times 10^8$ m/s. Según esto, tendremos que:

$$c = v \times \lambda$$

y, por tanto:

$$\lambda = \frac{c}{v} = \frac{3 \times 10^8}{2{,}4 \times 10^9} = 0{,}125 \text{ metros}$$

1.1.2. Emisor, receptor y circuito

En telecomunicaciones, se conoce como *emisor* o *fuente* al dispositivo del que parte la información, y como *destinatario* al receptor de esta. La mayor parte de los dispositivos (excluyendo algunos como los receptores de radio o televisión) son capaces de efectuar ambas funciones.

Un *circuito* es una vía de comunicación, a través de uno o varios medios de transmisión, que atraviesa en ocasiones varios dispositivos, entre el emisor y el receptor. Tal como muestra la **Figura 1.3**, típicamente un circuito estará compuesto por varios *enlaces*, segmentos de comunicación que tienen un dispositivo en cada uno de sus extremos. Fijémonos en que en la figura aparecen también varios *conmutadores*, dispositivos cuya tarea es establecer, mantener y modificar las conexiones entre varios enlaces físicos. La conmutación constituye una operación básica en toda red, tanto telefónica como de intercambio de datos; la estudiaremos enseguida con más profundidad.

Dependiendo del modo de transmisión, se distinguen los siguientes tipos de circuitos: *simplex*, en los que la comunicación es unidireccional (hay un dispositivo que solo puede emitir y otro que solo puede recibir), *half-duplex*, en los que cada estación puede emitir y recibir, pero no al mismo tiempo, y *full-duplex*, en los que ambos dispositivos o estaciones pueden emitir y recibir al unísono.

1.1.3. Dígitos binarios

En los circuitos digitales, la información se transmite mediante dígitos binarios o *bits*. Un *bit* constituye la unidad más pequeña de información y representa dos posibles estados de un sistema: por ejemplo, lleno/vacío, encendido/apagado, sí/no, etcétera.

Mediante n bits podemos representar 2^n estados o valores de una variable. Si, por ejemplo, los mensajes transmitidos a través de una red de comunicaciones emplean ocho bits para representar la dirección del dispositivo al que va destinado el mensaje, podremos conectar a la red 2^8, es decir, 256 dispositivos diferentes, cada uno de ellos con una dirección única. Ocho bits forman un *byte* u octeto.

Puesto que tanto el bit como el byte son unidades muy pequeñas, es muy habitual utilizar múltiplos en las magnitudes que emplean esta unidad de medida (por ejemplo, la capacidad de una memoria o la tasa de bits de un canal de comunicación).

1.1.4. Redes de comunicaciones

Una *red* está formada por el conjunto de elementos necesarios para que se establezca la comunicación; en su sentido más amplio, incluye los emisores, receptores, nodos intermedios, conmutadores, enlaces, etcétera. Una clasificación muy común de las redes de comunicaciones viene dada por su extensión, su ámbito territorial. Según esto, se distinguen los siguientes tipos de redes:

- Se define la **Red de Área Personal** (PAN, *Personal Area Network*) como una red de dispositivos localizados cerca de una persona, con un alcance de unos

pocos metros. Este tipo de redes incluye dispositivos móviles como teléfonos móviles, *Smart Phones*, PDA, dispositivos para la lectura de libros electrónicos y los diversos tipos *híbridos* entre los mencionados.



Figura 1.4. Las *tabletas* y los *Smart Phones* se incluyen en el conjunto de redes de área personal.

- Las **Redes de Área Local** (LAN, *Local Area Network*) son redes generalmente privadas, de extensión limitada, que conectan dispositivos en un área más o menos cerrada. Las redes internas de una empresa, de una oficina, de un campus universitario, son todas ellas LAN. Además del tamaño, las redes de área local se distinguen de otros tipos de redes por su medio de transmisión y su topología. Las LAN suelen usar medios de transmisión dedicados, y las topologías más comunes son el bus, el anillo y la estrella.

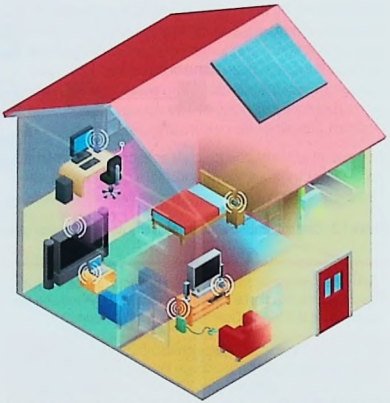


Figura 1.5. La red de datos de una vivienda es un ejemplo de Red de Área Local.

- Una **Red de Área Metropolitana** (MAN, *Metropolitan Area Network*) es un área diseñada para cubrir toda una ciudad. Por ejemplo, puede ser el área de una universidad que conecta las redes locales de todos los campus.
- Por último, las **Redes de Área Extensa** (WAN, *Wide Area Network*) cubren un área geográfica más amplia, como una región, un país o un continente. Un ejemplo de esta clase de redes es la *red telefónica conmutada*, una WAN pública que los usuarios utilizan para efectuar transmisiones de voz. Internet es una WAN orientada a



Figura 1.6. Red de Área Extensa.

Universidad Tecnica del Norte
BIBLIOTECA
Ibarra Ecuador

la transmisión de datos (textos, imágenes, vídeos o también llamadas de voz, todos ellos convertidos a dígitos binarios o *bits*, como veremos más adelante).

Otra clasificación de las redes de comunicaciones viene dada por la *titularidad* de la red. Según esto, se distinguen las redes privadas, públicas y dedicadas.

- Las **redes privadas** son propiedad de una empresa u organismo; solo sus miembros pueden acceder a la red y utilizar sus recursos. En general, las redes de área local son de naturaleza privada.
- Las **redes públicas** son redes de dominio público, aunque pueden ser de titularidad privada u estatal. Que sean de dominio público significa que cualquier persona puede acceder a ellas, normalmente mediante el pago de una cuota fija (tarifa plana) o variable (coste por llamada, coste por cantidad de datos transmitidos).
- Por último, las **redes dedicadas** son redes de titularidad pública pero reservadas para el uso de un grupo determinado de usuarios. Un ejemplo de estas es RedIris, la Red para la Interconexión de los Recursos Informáticos de las universidades y los centros de investigación, patrocinada por el Ministerio de Ciencia e Innovación y que proporciona servicios de conexión a Internet para instituciones educativas y de investigación.

1.1.5. Medios guiados y medios inalámbricos

Los medios de transmisión en una red de comunicaciones se dividen en dos grandes grupos:

- Los **medios guiados** son aquellos en los que existe un conducto físico entre los dos extremos del enlace; entre ellos podemos citar el cable de par trenzado, el cable coaxial y la fibra óptica.
- Los **medios no guiados**, o inalámbricos, se basan en la transmisión de información en forma de ondas electromagnéticas, sin la existencia de un conductor físico entre el emisor y el receptor. Para la transmisión de la información se emplean frecuencias de onda muy diversas, en función de factores como la distancia a la que se precise enviar la información, la potencia del emisor y el receptor, la presencia de interferencias, etcétera.

1.1.6. Atenuación e interferencias sobre la señal

Las señales que se transmiten a través de una red de comunicaciones, ya sea a través de un medio guiado o de forma inalámbrica, experimentan dos fenómenos que pueden degradar la información que transmiten: por una parte, la atenuación o el debilitamiento de la señal, una disminución de su potencia debido a la resistencia que ofrece el medio de transmisión frente a su avance; por otra, las interferencias con diversas clases de ruido. Para tratar de contrarrestar estos efectos, se emplean varios tipos de dispositivos:

- Los **amplificadores** reciben la señal que les llega e incrementan su potencia. Colocados en determinados lugares de la red, permiten contrarrestar la atenuación de la señal transmitida, pero poseen una limitación importante: si la señal llega al amplificador mezclada con ruido, el dispositivo amplifica tanto la una como el otro.
- Los **repetidores** regeneran la señal que reciben y reenvían esta nueva señal, sin el ruido ni la atenuación con la que les haya llegado, a través del siguiente tramo del canal de transmisión. Es un dispositivo más útil que un simple amplificador, pues contrarresta tanto la atenuación como el ruido de la señal.
- Los **filtros** son dispositivos que eliminan determinadas frecuencias no deseadas de la señal. Así, se distinguen entre otros los filtros de paso alto y los filtros de paso bajo, que atenúan respectivamente las componentes de baja y alta frecuencia.

1.1.7. El ancho de banda y la onda portadora

El canal de comunicaciones transmite una onda de una determinada frecuencia o rango de frecuencias. El emisor «imprime» en dicha onda los datos que debe transmitir a través de diversos mecanismos de *modulación* (mecanismos que trataremos en el Apartado 1.2.2). Dicha onda es denominada *portadora*.

El *ancho de banda* representa la capacidad de un circuito o un canal de comunicaciones. Existe una relación directa entre la frecuencia de la *onda portadora* de la información y el ancho de banda del canal, de modo que a mayor frecuencia, mayor es el ancho de banda. En general, se distingue entre el ancho de banda de señal y el ancho de banda de transmisión. No toda la capacidad del canal se emplea para transmitir datos, sino que las señales de control, sincronización, etcétera, ocupan una parte de la capacidad disponible. De ese modo, el ancho de banda de transmisión será siempre menor que el ancho de banda de señal.

Para medir el ancho de banda de un canal de comunicaciones se emplean dos medidas diferentes —aunque a menudo se utilizan incorrectamente como equivalentes—: la tasa de baudios y la tasa de bits.

El término *baudio* se refiere al número de cambios de señal que ocurren por segundo en un circuito analógico. La relación entre la tasa de baudios y la tasa de bits (bits por segundo o bps) depende de la sofisticación del tipo de modulación que se usa para incrustar los datos en la portadora. Si cada bit se representa por una transición de señal, la tasa de baudios y la tasa de bits será la misma. De todos modos, es habitual que una transición de señal pueda representar varios bits, con lo que en general la tasa de bits será superior a la de baudios.

1.1.8. Modo de transmisión

El *modo de transmisión* especifica en qué sentido viaja la señal entre dos dispositivos conectados. Se distinguen tres modos de transmisión diferentes:

- **Simple** o ***simplex***. La comunicación entre los dispositivos es unidireccional, pudiendo transmitir solamente uno de los dispositivos y recibiendo el otro la información. La comunicación entre el ratón o el teclado y el ordenador es un ejemplo de esta clase de transmisión.
- ***Half-duplex***. Cada dispositivo puede emitir y recibir a través del canal, pero no pueden hacerlo al mismo tiempo. Los *walkie-talkies* son un ejemplo de esta forma de comunicación, en la que todo el ancho de banda del canal está ocupado por la transmisión de *uno* de los dispositivos.
- ***Full-duplex***. Los dos dispositivos enlazados pueden transmitir y recibir al mismo tiempo. Las señales de ambos se reparten el ancho de banda del canal, o bien este dispone de dos enlaces físicos diferentes para la señal en una y otra dirección.

1.2. Señales analógicas y señales digitales

El término *analógico* se refiere a una magnitud o un dato continuo, en otras palabras, una magnitud en la cual, entre dos valores cualesquiera, siempre podemos tomar un valor intermedio. El volumen de un altavoz, la velocidad de un vehículo o el propio tiempo son magnitudes analógicas: una hora se puede dividir en cuartos, minutos, segundos, décimas, centésimas, y así *ad infinitum*.

Por el contrario, denominamos *digital* a una magnitud *discreta* o *diferenciada*, que puede tomar un conjunto *finito* de valores. Un reloj digital mide el tiempo de modo discreto: el reloj marca una determinada hora, por ejemplo, las 19:17, y, transcurrido un minuto, pasa a marcar las 19:18, pero no puede mostrar horas intermedias entre esos dos estados.

> **Recuerda que...**
>
> Cuando empleamos la palabra *discreto*, como en *cantidad discreta*, nos referimos a «magnitudes que constan de unidades o partes separadas unas de otras, como los árboles de un monte, los soldados de un ejército, los granos de una espiga, etcétera.» (Diccionario de la Real Academia Española, 22.ª edición).

Si representamos una señal analógica y otra digital mostrando su valor en función del tiempo (véase la **Figura 1.7**), veremos que la señal analógica cambia de modo continuo con el tiempo, mientras que la digital lo hace de modo instantáneo.

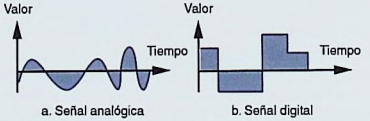


Figura 1.7. Señales analógica y digital.

La forma de onda portadora de la que se parte en las comunicaciones, tanto de datos como de voz, es la onda senoidal, representada en la **Figura 1.8**. Describimos esta onda mediante su *amplitud*, su *frecuencia* o su *período* (recordemos que ambos están relacionados puesto que su producto es la velocidad de propagación de la onda) y su *fase*.

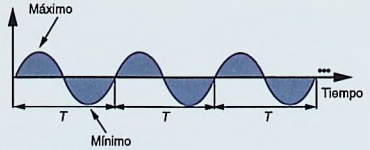


Figura 1.8. Onda senoidal.

1.2.1. Codificación analógica/digital

En muchas ocasiones, es necesario transformar una señal analógica en otra digital. Como sabemos, cualquier sonido (un fragmento de música, un ruido del ambiente o nuestra voz) está formado por ondas que se transmiten a través del aire, es, por tanto, un fenómeno de naturaleza analógica. Sin embargo, cuando lo grabamos en un dispositivo digital (como un *Smart Phone*), dicho sonido debe codificarse como ceros y unos. Para hacerlo, la señal analógica se *muestrea*, es decir, se mide su valor a intervalos regulares, como

muestra la **Figura 1.9**. El valor obtenido se redondea para formar un número entero y se codifica en forma de dígitos binarios.

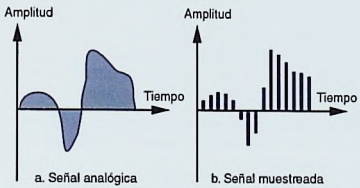


Figura 1.9. Codificación de una señal analógica en forma digital: muestreo de la señal.

¿Sabías que...?

En la codificación digital de una señal analógica, se define la tasa o frecuencia de muestreo como el número de muestras por unidad de tiempo que se toman de la señal analógica para construir la señal digital. El *teorema de Shannon*, muy conocido en la teoría de la codificación y transmisión de la información, afirma que se puede reconstruir la señal analógica a partir de la señal muestreada siempre y cuando la frecuencia de muestreo sea *al menos* el doble de la frecuencia máxima de la señal analógica de partida.

1.2.2. Codificación digital o analógica

Para transmitir los bits a través de un medio físico (ya sea un medio guiado como un cable telefónico o de fibra óptica, o un medio inalámbrico) se precisa una onda portadora que «transporte» los bits. Estos se codifican en una señal analógica que adquirirá una forma diferente según transporte o represente un 0 o un 1. A modo de ejemplo, fijémonos en una de las formas más sencillas de codificación o modulación digital o analógica, la modulación por desplazamiento de amplitud. En esta forma de modulación, la amplitud o potencia de la señal se modifica según deba representarse un 0 o un 1.

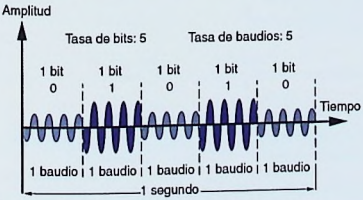


Figura 1.10. Modulación por desplazamiento de amplitud.

1.2.3. La conmutación

Una red de comunicaciones está formada por múltiples nodos conectados entre sí a través de enlaces. Para que dos dispositivos situados a cierta distancia puedan ponerse en comunicación entre sí, se establecen conexiones temporales entre los dispositivos intermedios. A esta práctica se la denomina *conmutación*, y tendremos ocasión de tratarla extensamente tanto en las redes de datos como en las redes telefónicas.

1.2.4. La multiplexación

Siempre que las capacidades de transmisión de un canal sean lo suficientemente grandes, se puede emplear este único canal para comunicar varios dispositivos a la vez, del mismo modo que la acometida eléctrica de un edificio transporta la energía de varias viviendas. La *multiplexación* es la técnica que permite la transmisión simultánea de varias señales a través de un solo enlace físico.

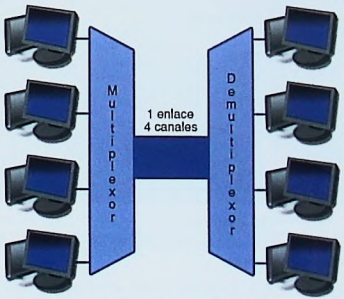


Figura 1.11. Esquema de la comunicación entre cuatro equipos empleando un solo enlace.

En un sistema multiplexado como el que se muestra en la **Figura 1.11**, hay *n* enlaces que comparten la capacidad de un canal. Los equipos que emiten información dirigen sus transmisiones a un dispositivo llamado *multiplexor*, que las combina en un único flujo de datos. En el otro extremo del canal compartido, otro dispositivo complementario del anterior, un *demultiplexor*, separa este flujo en sus componentes y dirige cada uno de ellos a su destinatario particular. Para poder llevar a cabo esta técnica es preciso que los paquetes de datos lleven información sobre la *dirección* de su remitente y de su destinatario.

Las principales técnicas para la multiplexación de un canal se enmarcan en dos grupos:

- La **multiplexación por división de frecuencia** consiste en emplear una onda portadora de distinta frecuencia para cada canal. El ancho de banda del canal compartido debe ser mayor que la suma de los anchos de banda de todas las señales. Las diversas portadoras se separan lo suficiente para evitar interferencias entre ellas (véase la **Figura 1.12**).

- La **multiplexación por división de tiempo** consiste en compartir el canal de comunicaciones intercalando los mensajes de las diversas comunicaciones o «conversaciones» entre los dispositivos: tal como muestra la **Figura 1.13**, el canal va siendo ocupado consecutivamente por las comunicaciones A, B, C, D, E, comenzando otra vez la secuencia hasta que la comunicación finaliza.

1.2.5. Detección y corrección de errores

En una red de comunicaciones, la información se transmite a través de medios físicos en los que pueden surgir errores, debidos, entre otros factores, al ruido y las interferencias. Cuando un paquete de datos viaja entre el emisor y el receptor, hay muchas probabilidades de que alguno de los datos que contiene se altere.

Los mecanismos de *detección* de errores se basan en añadir al mensaje enviado cierta información adicional que se puede calcular a partir del mensaje original. Por ejemplo, el control de paridad consiste en enviar, junto con un determinado grupo de bits, uno adicional que indique si, en dicho grupo, el número de unos es par o impar. Cuando el mensaje llega al destinatario, este efectúa el cálculo y comprueba si la paridad que ha calculado coincide con la que ha transmitido el

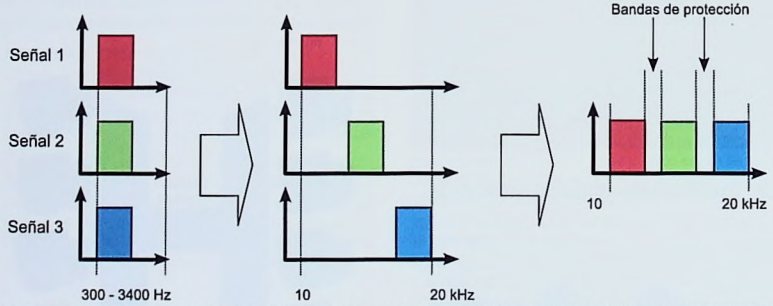


Figura 1.12. En la multiplexación por división de frecuencia, a cada canal se le asigna un determinado rango de frecuencias, separados entre sí para evitar interferencias.

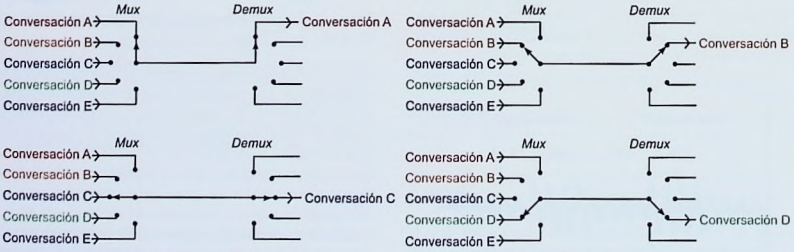


Figura 1.13. En la multiplexación por división de tiempo, el canal va siendo ocupado sucesivamente por las «conversaciones» entre dos equipos.

emisor. Si no coinciden, al menos uno de los bits recibidos es erróneo.

> **¿Sabías que...?**
>
> Dos mecanismos de detección de errores y comprobación que se emplean con mucha frecuencia en las redes de datos son la comprobación de redundancia cíclica y la suma de comprobación. El cálculo que se efectúa con los datos de partida es más complejo que en el simple control de paridad, pero su fundamento es el mismo.

Cuando el receptor detecta la presencia de un error en el mensaje, existen dos maneras de corregirlo: una es pedirle al emisor que vuelva a enviar el paquete de datos que se ha corrompido; la otra es tratar de corregir el error empleando un código

1.3. Protocolos y estándares

Las redes de comunicación relacionan entre sí diversos tipos de sistemas, entidades capaces de transmitir y recibir información. En el caso de las comunicaciones entre sistemas informáticos, la comunicación se transmite, como ya hemos estudiado, en forma de ceros y unos, denominados *bits*. Para comunicarse, no basta con que las dos entidades se envíen grupos de bits, sino que precisan un conjunto de reglas que gobiernen la comunicación. Este conjunto de reglas constituye un **protocolo de comunicaciones**.

En las comunicaciones entre dos dispositivos, el protocolo desempeña el mismo papel que el lenguaje entre dos personas que hablan. Por ejemplo, si una persona de habla inglesa le dice a otra de lengua germana la palabra «*eagle*» (águila), el alemán escuchará «*Igel*» (puercoespín). El alemán escucha exactamente lo que el inglés dice, pero los mismos sonidos remiten a conceptos distintos porque ambos hablan idiomas diferentes. Entre ambos no han establecido previamente un protocolo de comunicaciones que les permita entenderse mutuamente. Del mismo modo, en los dispositivos que intercambian información, el protocolo posibilita la comunicación asegurando, al igual que en el ejemplo anterior, que el dispositivo que emite y el que recibe la información «hablen el mismo lenguaje».

El protocolo define *qué* se comunica, *cómo* se comunica y *cuándo* se comunica. Los elementos básicos del protocolo son la *sintaxis*, la *semántica* y la *temporalización*.

La **sintaxis** define la estructura o el formato de los datos, es decir, el orden en el que se presenta o transmite la información. Imaginemos un protocolo sencillo en el que se envía un paquete de datos cuyos primeros ocho bits corresponden a la dirección del remitente y los ocho bits siguientes, a la del destinatario, mientras que el resto del paquete corresponde al mensaje como tal. La sintaxis especificará esta secuencia para que todos los dispositivos codifiquen las tramas de datos que envíen siguiendo esa misma estructura.

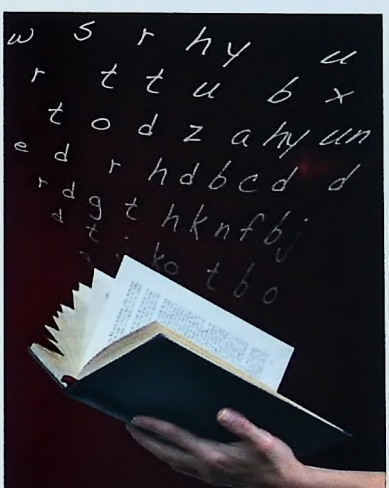


Figura 1.14. Al igual que en el lenguaje humano, los protocolos definen para el lenguaje de las comunicaciones entre dispositivos una sintaxis y una semántica.

La **semántica**, por su parte, se refiere al *significado* de cada conjunto de bits.

Imaginemos que un dispositivo transmite datos a otro a razón de diez millones de bits por segundo, mientras que el destinatario solo es capaz de recibirlos y procesarlos a razón de un millón de bits por segundo. Es evidente que en esta situación se perderá un gran volumen de datos. La **temporalización** especifica cuándo deben enviarse los datos y la velocidad a la que deben transmitirse.

1.3.1. Los estándares y su importancia

Al leer los párrafos anteriores, relativos a los protocolos, hemos adquirido una primera idea de la *complejidad* inherente al proceso de comunicación entre varios

dispositivos. A medida que nos adentremos, a lo largo de los contenidos de este libro, en los pormenores del proceso de comunicación, nos iremos dando cada vez más cuenta del elevado número de aspectos y elementos que es necesario coordinar para que la información se transfiera de modo eficaz y fiable

Entre dispositivos de fabricantes diferentes, ¿podemos asegurar una comunicación adecuada y eficaz? Un mismo fabricante puede garantizar la compatibilidad entre los dispositivos fabricados por él mismo, pero, ¿qué ocurre cuando empleamos dispositivos de empresas distintas? Los *estándares* proporcionan un modelo de desarrollo que garantiza el funcionamiento de un producto independientemente de su fabricante específico.

Recuerda que...

Un estándar es un conjunto de normas, acuerdos y recomendaciones técnicas que regulan la tecnología y los protocolos de los sistemas de comunicación.

Los estándares definen las características físicas, eléctricas y mecánicas, así como los procedimientos de comunicación de los dispositivos. Por ejemplo, un estándar de comunicaciones puede definir el tipo de conector, las tensiones y las intensidades eléctricas que se deben emplear, el formato de codificación de los datos, etcétera. El empleo de estándares presenta ventajas como la compatibilidad entre productos, la reducción de costes y la flexibilidad del mercado para la tecnología estandarizada, proporcionando además un marco para la investigación y el desarrollo en dicha tecnología.

En muchas ocasiones, se distinguen entre estándares *de facto* y estándares *de iure*. Los segundos surgen de una entidad u organización de estándares oficialmente reconocida. Los primeros, por el contrario, proceden habitualmente de las definiciones técnicas de un fabricante o un pequeño grupo de ellos pero, debido normalmente a la extensión en el mercado de la tecnología de dicho fabricante, pasan a ser de aceptación general.

Algunas de las organizaciones de estándares con más relevancia en telecomunicaciones son las siguientes:

- La Organización Internacional de Estándares (**ISO**, *International Standards Organization*) está formada principalmente por los organismos y los comités de estandarización de muchos países; junto a ellos, encontramos una serie de organizaciones observadoras, que no poseen capacidad de voto. Creada en 1947, en la actualidad pertenecen a ella más de cien países.



Figura 1.15. Logotipo de la Organización Internacional de Estándares.

- A comienzos de la década de 1970, ante la proliferación de estándares nacionales para las telecomunicaciones, la Organización de Naciones Unidas creó, como parte de la Unión Internacional de Telecomunicaciones (ITU, *International Telecommunications Union*), el Comité Consultivo para la Telefonía y la Telegrafía Internacional. En 1993 se cambió su nombre por el de **ITU-T** (la *T* es la abreviatura de *Telecommunications Standards Sector*, Sector de Estándares para las Telecomunicaciones). Los proyectos más conocidos de ITU-T son la denominada «serie V», para la comunicación de datos mediante líneas telefónicas, y la «serie X» (a la que pertenecen los protocolos X.25, X.400 y X.500, que mencionaremos más adelante en este libro), para la transmisión de información sobre redes públicas digitales.



Figura 1.16. Logotipo de la Unión Internacional de Telecomunicaciones.

- El Instituto de Ingenieros Eléctricos y Electrónicos (**IEEE**, *Institute of Electrical and Electronic Engineers*) es la mayor organización profesional de ingeniería del mundo. Uno de los objetivos del IEEE es supervisar el desarrollo y la adopción de estándares internacionales en el ámbito de la informática y las comunicaciones. Existe un comité especial en el seno del IEEE dedicado a las Redes de Área Local, en cuyo marco se ha desarrollado el denominado *Proyecto 802* (del que han surgido, entre otros muchos, el grupo de estándares 802.11, claves en el desarrollo de las redes Wi-Fi).



Figura 1.17. Logotipo del Instituto de Ingenieros Eléctricos y Electrónicos.

- **ANSI** (*American National Standards Institute*, Instituto Americano Nacional de Estándares) es una organización privada sin ánimo de lucro. Entre los miembros de ANSI se cuentan sociedades profesionales, asociaciones industriales, grupos de consumidores y organismos de estandarización del gobierno estadounidense.



Figura 1.18. Logotipo del Instituto Americano Nacional de Estándares.

- **EIA** (*Electronic Industries Association*, Asociación de las Industrias Electrónicas) es una asociación de fabricantes con presencia mayoritaria en Estados Unidos. En el ámbito de las comunicaciones, destaca la definición de las interfaces de comunicación y las especificaciones de señales para la transmisión entre dispositivos digitales, entre ellas la EIA-232-D.



Figura 1.19. El conector RS-232, especificado en el estándar EIA-232-D, ha estado muy extendido en la comunicación entre ordenadores y periféricos, aunque en la actualidad ha sido en buena medida sustituido por el Bus Serie Universal (USB).

- El **ETSI** (*European Telecommunications Standards Institute*, Instituto Europeo de Estándares de Telecomunicaciones) es, al igual que ANSI y EIA, una organización independiente sin ánimo de lucro; la Unión Europea lo reconoce como organización de estándares europeos en el ámbito de las telecomunicaciones y posee en la actualidad 766 organizaciones miembro de 63 países.



Figura 1.20. Logotipo del Instituto Europeo de Estándares de Telecomunicaciones.

- **AENOR** (Asociación Española de Normalización): en España, el organismo de normalización reconocido oficialmente. A través de sus comités técnicos de normalización, se encarga de la publicación de las normas UNE y la adopción de normas europeas.

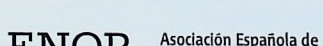


Figura 1.21. Logotipo de AENOR.

1.4. Topologías de red

Los dispositivos de una red de comunicaciones se conectan a través de enlaces físicos (cables, enlaces mediante radiofrecuencia, etcétera.) formando una determinada geometría. A dicha geometría se la conoce como *topología* de la red. En las redes de comunicaciones podemos encontrar las siguientes topologías:

- En la topología en **malla completa** cada nodo se conecta a todos los demás, de modo que los datos pueden viajar del dispositivo fuente (remitente o emisor) al dispositivo destino (destinatario o receptor) siguiendo diversas rutas. Una variante de esta topología es la **malla parcial**, en la que existen varias rutas entre los dispositivos, pero no están todos conectados con todos.



Figura 1.22. Topología en malla completa.

- En la topología en **árbol**, los nodos se organizan jerárquicamente, habitualmente a través de acopladores o concentradores primarios y secundarios.

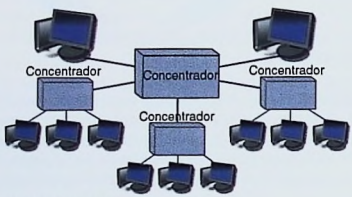


Figura 1.23. Topología en árbol.

- En la topología **lineal** o **en bus**, cada dispositivo cuenta con un cable de poca longitud que lo conecta a una línea troncal o *backbone*. Normalmente, esta línea posee unos *terminadores* que impiden que los datos sean reflejados al final de la misma y obstruyan el envío de nuevos datos.



Figura 1.24. Topología en bus.

- En la topología en **estrella**, los canales de transmisión de todos los dispositivos están conectados entre sí en un punto o dispositivo central.

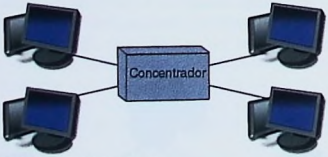


Figura 1.25. Topología en estrella.

- En la topología en **anillo**, cada dispositivo tiene un enlace con el dispositivo siguiente y el anterior. La señal o mensaje pasa de dispositivo en dispositivo en una determinada dirección del anillo hasta que llega a su destino. Cada dispositivo actúa así como un repetidor de señal: cuando llega a él un mensaje destinado a otro dispositivo, el equipo recibe la señal y la vuelve a enviar, como si pasase un testigo.



Figura 1.26. Topología en anillo.

Actividad resuelta 1.2. ¿Cuántos enlaces necesita una empresa que use ocho dispositivos conectados en malla completa? ¿Cuántos puertos de comunicaciones deberá tener cada uno de los dispositivos?

Solución. El número de enlaces viene dado por la fórmula $\frac{n \times (n-1)}{2}$, siendo n el número de dispositivos. De este modo, se precisarán:

$$\frac{n \times (n-1)}{2} = \frac{8 \times (8-1)}{2} = 28 \text{ enlaces.}$$

Por su parte, el número de puertos viene dado por la expresión $n - 1$, de modo que para conectar los ocho dispositivos, cada uno necesitará siete puertos de comunicaciones.

Actividad propuesta 1.1

A continuación se citan algunas ventajas y algunas desventajas de diversas topologías. Explica a qué topologías se aplicarían las características mencionadas.

a) Cuando un dispositivo falla, queda inhabilitada la comunicación en toda la red.

b) Es complejo y costoso añadir un dispositivo a la red de comunicaciones.

c) Cada enlace de comunicaciones entre dos dispositivos cualesquiera es dedicado; de ese modo se elimina cualquier problema de sobrecarga de tráfico, la necesidad del control del canal, etcétera.

d) Si un enlace falla, solo se ve afectada la comunicación de *un* dispositivo, lo que proporciona robustez a la red.

e) Es relativamente fácil y poco costoso añadir un dispositivo a la red.

Actividad propuesta 1.2

¿Te parece adecuada la topología en malla completa para una empresa que necesite conectar 120 dispositivos entre sí? ¿Por qué? ¿Qué topología podríamos emplear en una red de esta clase?

1.5. El modelo OSI

El modelo OSI (Interconexión de Sistemas Abiertos, *Open Systems Interconnection*), de la Organización Internacional de Estándares (ISO) es un estándar internacional que describe cómo crear protocolos de comunicaciones en red estructurados en *capas* o *niveles*.



Figura 1.27. Capas del modelo OSI.

El modelo OSI clasifica las funciones de comunicación en siete capas. Cada dispositivo posee una capa de aplicación en la que se sitúan los programas o herramientas con los que interactúan los usuarios. Los mensajes del dispositivo emisor van atravesando (hacia «abajo») las sucesivas capas hasta llegar al medio de transmisión, al llegar al destinatario, el mensaje efectúa el camino opuesto, moviéndose (hacia «arriba») por las diversas capas hasta llegar a la capa de aplicación. En los dispositivos que emplean el modelo OSI, cada capa proporciona servicios y funciones a la capa inmediatamente superior; a su vez, cada capa emplea las funciones y los servicios que le proporciona la inferior, a través de una serie de *interfaces* de comunicación. En el dispositivo emisor, cada capa recibe el mensaje o el paquete de datos que le proporciona la superior y añade instrucciones e informaciones a los datos, informaciones tales como la dirección del destinatario o ciertos códigos para la detección o la corrección de errores.

En cada uno de los dispositivos, cada capa solicita los servicios de la capa situada inmediatamente por debajo de ella. Entre dispositivos, la capa *x* de uno de ellos se comunica con su homóloga (capa *x*) del otro. Aunque, en la *realidad*, el mensaje atraviesa todas las capas y es emitido a través del medio físico de transmisión, para cada capa se establecen una serie de protocolos de comunicación que establecen un enlace o canal *virtual* entre las máquinas, denominado a menudo canal *peer-to-peer* (literalmente, «entre pares» o «entre iguales»). Así, la aplicación de la máquina A se comunica «directamente» con la aplicación de la máquina B, y del mismo modo ocurre con el resto de capas, tal como muestra la **Figura 1.28**.

La **Figura 1.29** muestra cómo cada capa añade cierta información (cabeceras o *headers*, «H» en la figura, y en algunos casos colas o *trailers*, «T» en la figura) hasta llegar a la capa física, que transmite la secuencia de ceros y unos, en forma de señal electromagnética, a través del canal de transmisión.

1.5.1. Funciones de las capas

En el modelo OSI, cada una de las capas de la red posee una serie de funciones delimitadas y bien definidas. Veamos en qué consiste cada una de ellas.

Capa física. La capa física se encarga de coordinar las funciones necesarias para transmitir una cadena de bits sobre un medio físico. A ella pertenecen, por ejemplo, las especificaciones eléctricas y mecánicas de los conectores, el cableado y las señales electromagnéticas que se envían a través de él. ¿Cómo se conectan los dispositivos? ¿La información fluye en ambas direcciones o en una sola? ¿Cuál es la topología de la red? ¿Qué tipo de señales se usan para la transmisión de la información? ¿Cómo se representan los ceros y los unos de los bits en ellas? ¿Cómo se inicia la transmisión de la información? Estas son algunas de las cuestiones y especificaciones que pertenecen a la capa física. Al estudio de la capa física dedicaremos la Unidad 2 de este libro.

Capa de enlace de datos. Esta capa es la encargada de enviar unidades de información (grupos de bits) entre dos dispositivos a través de un enlace directo, sin errores. Las cabeceras y las colas que añade a los

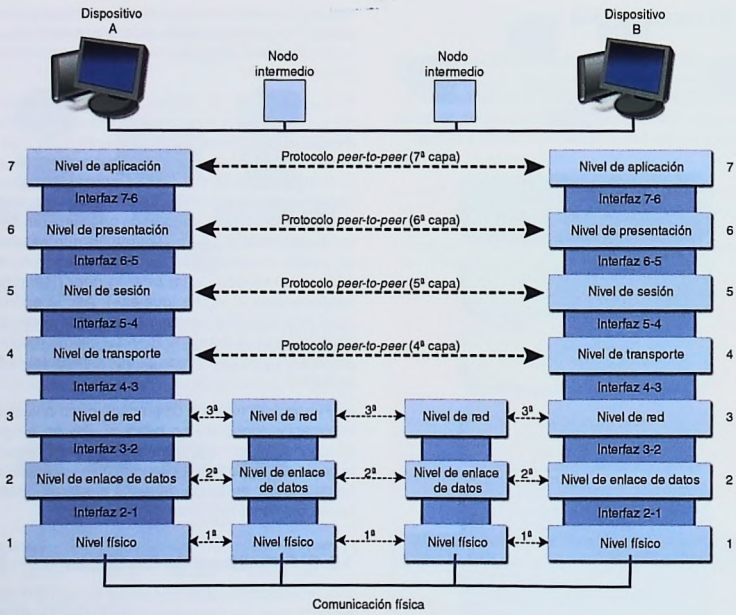


Figura 1.28. Comunicación entre las capas OSI.

mensajes contienen información sobre las direcciones del remitente y el destinatario y mecanismos para la detección y/o corrección de errores, además de información de sincronización, para que ambos dispositivos puedan saber dónde comienza y finaliza el impulso de señal correspondiente a cada bit. Además de ello, esta capa es la responsable del *control de acceso* al medio, implementando mecanismos para decidir qué ocurre cuando dos dispositivos intentan acceder simultáneamente al medio de transmisión.

Capa de red. La función de la capa de red es el envío de mensajes entre el remitente y el destinatario siguiendo varios enlaces de red. A diferencia de la capa anterior, que supervisa la transmisión entre dos dispositivos enlazados directamente, esta asegura que el paquete de datos llegue del origen al destino. Esta capa se encarga de establecer las conmutaciones necesarias para crear el enlace entre el remitente y el destinatario del paquete de información, y de elegir la ruta óptima para establecer este enlace de entre las diversas rutas posibles. A esta operación se la denomina *enrutamiento* del paquete. Los mecanismos para la multiplexación de los canales de transmisión de información también forman parte de los cometidos de esta capa.

Capa de transporte. Esta capa es responsable de la entrega al destinatario del mensaje *entero*. A diferencia de la capa de red, que tiene como objetivo la entrega de *paquetes individuales*, esta capa debe, del lado del emisor, dividir o *segmentar* el mensaje completo en paquetes y, del lado del receptor, ensamblarlos en orden para reconstruir el mensaje original asegurándose de que han llegado todos y están libres de errores. A esta capa le corresponde también entregar el mensaje no solo al dispositivo adecuado, sino también a aquella aplicación del dispositivo al que va destinada. Pensemos, por ejemplo, que a un ordenador pueden llegar mensajes dirigidos a diversas aplicaciones (correo electrónico, navegador web, redes P2P para compartir archivos), normalmente, cada una de estas aplicaciones tiene asignado un *puerto* de comunicaciones que

Universidad Tecnica del Norte
BIBLIOTECA
Ibarra Ecuador

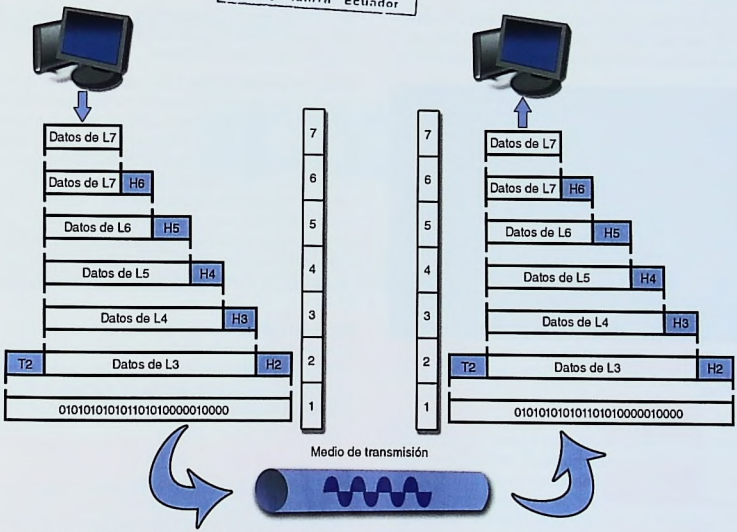


Figura 1.29. Transmisión de datos entre las capas del modelo OSI.

¿Sabías que...?

En otros muchos ámbitos de la ciencia y de la técnica se emplea el enfoque de la diferenciación en capas de análisis para comprender o diseñar una realidad compleja. Así, en teoría de ordenadores es común emplear varios niveles de análisis. Por ejemplo, la clasificación de Levy concibe el ordenador como una cebolla con varios niveles funcionales; cada nivel recibe ciertas instrucciones y las ejecuta siguiendo una lógica propia. En otro orden del conocimiento, la comprensión de un ecosistema requiere de la participación de muchas ciencias: la ecología, la etología o ciencia del comportamiento animal, la fisiología animal, la botánica, la biología, la bioquímica, etcétera. Cada una de estas ciencias aborda una capa o nivel de la realidad de la vida, aportando resultados y herramientas de análisis a las que estudian capas superiores y basándose a su vez en los resultados obtenidos por las ciencias que abordan los niveles inferiores.

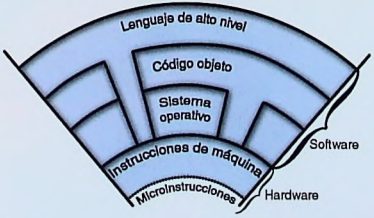


Figura 1.31. Niveles de estudio del ordenador en la clasificación de Levy. Fuente: Pedro de Miguel Anasagasti, *Fundamentos de computadores. Ediciones Paraninfo.*

permite distinguir, entre los diversos mensajes recibidos, los que van destinados a ella. Volveremos sobre esta cuestión al tratar el conjunto de protocolos TCP/IP.



Figura 1.30. Para distinguir los diversos tipos de mensajes que llegan a un ordenador, cada uno de estos tipos se dirige a un puerto determinado.

Capa de sesión. La capa de sesión actúa como una especie de moderadora de la conversación entre emisor y receptor. Es la encargada de establecer y mantener la comunicación y de controlar su sincronismo. Imaginemos que el emisor desea enviar un conjunto de 100 páginas de datos. ¿Qué ocurre si la comunicación se interrumpe por alguna razón cuando se han enviado solo 30? La capa de sesión será la encargada de retomar la comunicación y enviar el resto de la información, cerrando la comunicación correctamente cuando la transmisión finalice.

Capa de presentación. Esta capa garantiza que dos dispositivos diferentes puedan comunicarse entre sí. Los dispositivos que intercambian datos en una red pueden emplear representaciones de datos diferentes. La capa de presentación deberá implementar los mecanismos de traducción necesarios para asegurar la compatibilidad entre sistemas. Además de ello, esta capa incluye mecanismos para la *encriptación* del mensaje, si la seguridad lo requiere, y para la compresión del mismo, con objeto de consumir menos ancho de banda del canal y hacer la comunicación más eficiente.

Capa de aplicación. La capa de aplicación es la que permite al usuario acceder a la red. Proporciona las interfaces necesarias para servicios como el correo electrónico, las transferencias de archivos o el control remoto de otros ordenadores, entre otros muchos.

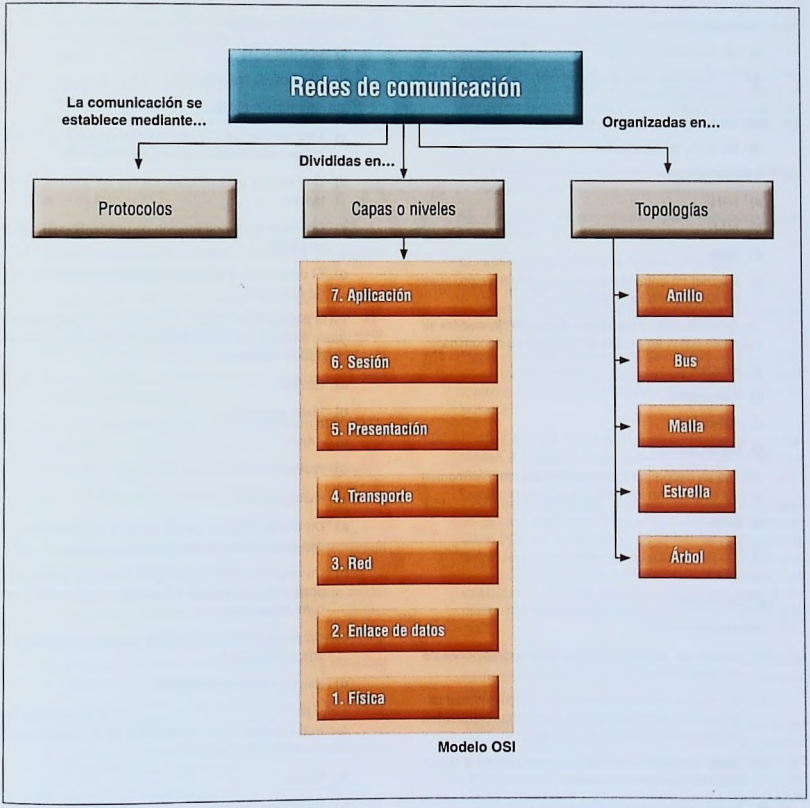
Recuerda que...

En telecomunicaciones, un enlace es un segmento que une dos puntos que transmiten información. Típicamente, se habla de enlace cuando nos referimos a la conexión entre un terminal y un conmutador o central de conmutación.



Figura 1.31. La diversidad de aplicaciones y servicios que empleamos hoy en día a través de Internet es posible gracias a los protocolos y los estándares de comunicaciones.

Mapa conceptual



Cuestiones

1.1. El modelo OSI es:

a) Un protocolo.

b) Un estándar para la descripción de protocolos de comunicaciones.

c) Un tipo de red de área local.

d) Ninguno de los anteriores.

1.2. Internet es una:

a) LAN.

b) MAN.

c) WAN.

d) Internet no entra dentro de esta clasificación, pues su surgimiento es posterior.

1.3. Un canal de comunicación que transmite de manera simultánea datos en ambas direcciones se denomina:

a) *Simplex.*

b) *Half-duplex.*

c) *Full-duplex.*

d) Medio guiado.

1.4. ¿Cómo se denomina la unidad mínima de información que se trasmite en las comunicaciones digitales?

a) Byte.

b) Bit.

c) Octeto.

d) Datagrama.

1.5. En el modelo OSI:

a) La capa de aplicación especifica las direcciones de los dispositivos.

b) En la capa física se especifican protocolos que garanticen la fiabilidad de los datos intercambiados (detección y corrección de errores).

c) Todas las capas conocen los mecanismos y protocolos de las capas inferiores.

d) Todas las opciones anteriores son falsas.

1.6. ¿Cuáles de los siguientes medios son no guiados?

a) La fibra óptica.

b) El cable coaxial.

c) El cable UTP.

d) Ninguno de los anteriores.

1.7. Se denomina *muestreo* a:

a) Una técnica para la representación interna de los bits en los circuitos digitales del ordenador.

b) Una técnica para modular los bits en una onda portadora.

c) Una técnica de codificación de una señal analógica en digital.

d) El control de la fiabilidad y rendimiento de una red de área local.

1.8. En la topología en _____ existen enlaces directos que unen cada uno de los dispositivos con todos los demás:

a) Estrella.

b) Malla completa.

c) Árbol.

d) Anillo.

1.9. Un multiplexor es:

a) Un dispositivo que se usa para la conexión de varios dispositivos en una topología en bus.

b) Un dispositivo que se emplea para que varios dispositivos puedan usar a la vez un mismo enlace de comunicaciones.

c) Un dispositivo para codificar la señal analógica en una señal digital.

d) Ninguno de los anteriores.

1.10. La capa _____ es la encargada de las traducciones en la codificación de los datos entre los dispositivos de la red.

a) Física.

b) De enlace de datos.

c) De presentación.

d) De aplicación.

Actividades de aplicación

1.11. ¿Qué es un mecanismo de detección de errores? Explícalo con tus propias palabras. Puedes ayudarte con un ejemplo.

1.12. Calcula el período y la longitud de onda de las ondas electromagnéticas de frecuencia (supón que la velocidad de propagación de la onda es $c = 3 \times 10^8$ m/s).

a) 24 Hz.

b) 8 MHz.

c) 140 kHz.

d) 20 GHz.

1.13. Explica las diferencias entre un medio de transmisión guiado y uno no guiado.

1.14. Imagina que tenemos cinco dispositivos conectados en una red en forma de malla completa. ¿Cuántos enlaces físicos entre los dispositivos se precisarían? ¿Cuántos puertos debe tener cada uno de los dispositivos?

1.15. En las siguientes topologías de red, ¿qué ocurre si falla uno de los enlaces?

a) Cinco dispositivos en una topología en malla completa.

b) Cinco dispositivos en una topología en estrella.

c) Cinco dispositivos en una topología en bus.

d) Cinco dispositivos en una topología en anillo.

1.16. Especifica a qué capas del modelo OSI pertenece cada una de las funciones de la lista:

a) Supervisión de la transmisión de un paquete de datos entre el emisor y el destinatario.

b) Transmisión de las señales a través del medio físico.

c) Traducción entre diversas codificaciones de datos de los dispositivos que se comunican.

d) Transmisión de un datagrama desde un nodo de la red al siguiente.

e) Proporciona servicios como el correo electrónico o la transferencia de archivos.

f) Controla la conmutación.

g) Proporciona especificaciones mecánicas y eléctricas de las interfaces de red.

h) Proporciona mecanismos para la compresión de la información transmitida.

1.17. Supón que deseamos transmitir 10 imágenes por segundo a través de un canal de comunicaciones. Las imágenes son cuadradas y tienen 5 píxeles de lado. Supón que cada píxel puede tomar un valor de entre 256 posibles («paleta» de 256 colores).

a) ¿Cuántos bits se necesitan para especificar el color de cada píxel?

b) ¿Cuántos bits se necesitan para especificar cada imagen?

c) ¿Cuál debe ser la tasa de bits del canal?

1.18. ¿Es lo mismo tasa de bits y tasa de baudios? ¿En qué se diferencian? ¿Es lo mismo tasa de bits que tasa de bytes? Razona tu respuesta.

1.19. Fíjate en la red de área local de tu casa o de tu centro educativo. Enumera los elementos que la forman. ¿Qué medio o medios de transmisión utiliza? ¿Cuál es su topología?

1.20. Explica con tus palabras qué es un protocolo y un estándar, e indica por qué son tan importantes en una red de comunicaciones.

1.21. ¿En qué se diferencia un medio de transmisión guiado de otro no guiado? Pon un ejemplo de cada uno de ellos. Para la implantación de la red de datos en una empresa de proyectos de ingeniería con 50 trabajadores, ¿qué tipo de medio de transmisión consideras más adecuado? ¿En qué entornos consideras que la implantación de una red inalámbrica es la solución óptima?

1.22. Explica la diferencia entre un bit y un byte. ¿Cuánta información puedes representar con cada uno de estos elementos?

Imagina que una pequeña empresa dispone de conexión a Internet mediante ADSL. ¿Cómo se transmite la información digital a través de la línea telefónica? ¿Es necesario efectuar algún tipo de transformación con la información digital antes de transmitirla? ¿Cómo se llaman los dispositivos que efectúan esta transformación?

Lectura

Interconexión de sistemas abiertos: modelo de referencia básico (extractos)

Organización Internacional de Estándares

Introducción

Este modelo de referencia proporciona una base común para la coordinación en el desarrollo de estándares con el objetivo de la interconexión de sistemas, al mismo tiempo que permite poner en perspectiva, en el modelo de referencia general, a los estándares ya existentes. También identifica áreas para desarrollar y mejorar los estándares y proporciona una referencia común para mantener la coherencia entre todos los estándares relacionados. (...)

Objeto

1.1. El objetivo de este Modelo de Referencia de Interconexión de Sistemas Abiertos es proporcionar una base para la coordinación en el desarrollo de estándares, con el objeto de la interconexión de sistemas, al mismo tiempo que permite poner en perspectiva, en el Modelo de Referencia, los estándares existentes.

1.2. Aplicamos el término Interconexión de Sistemas Abiertos (OSI [*Open System Interconnection*]) a un estándar cuando este permite el intercambio de información entre sistemas que, gracias a ello, están mutuamente «abiertos» o, en otras palabras, son compatibles entre sí.

1.3. El hecho de que un sistema esté abierto no implica la implementación de ningún sistema, tecnología o medio de interconexión en particular, sino que se refiere al reconocimiento mutuo y al soporte de los estándares aplicables.

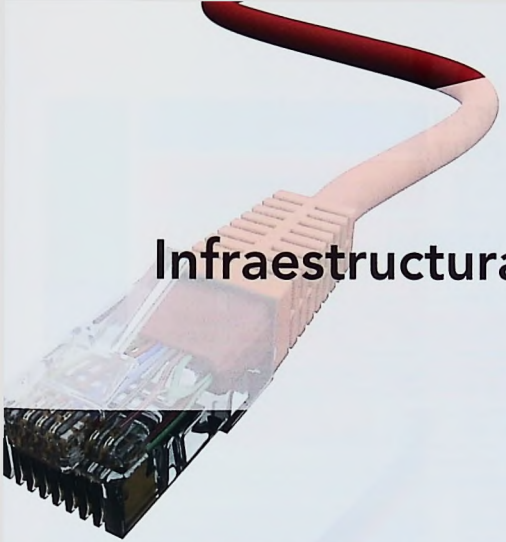
1.4. El objetivo de este Modelo de Referencia es también identificar áreas para el desarrollo o la mejora de los estándares, y proporcionar una referencia común para mantener la coherencia de todos los estándares relacionados. No es la intención de este Modelo de Referencia ni servir como una especificación para la implantación de estándares, ni tampoco constituir la base para evaluar la conformidad a ellos de las implementaciones reales, ni de proporcionar un nivel suficiente de detalle para definir con precisión los servicios y protocolos de la arquitectura de la conexión. Más bien, este Modelo de Referencia proporciona un marco conceptual y funcional que permite a los equipos internacionales de expertos trabajar productiva e independientemente en el desarrollo de estándares para cada capa del Modelo de Referencia OSI.

1.5. El Modelo de Referencia posee flexibilidad suficiente para acomodar los adelantos tecnológicos y el crecimiento de las necesidades de los usuarios. Esta flexibilidad está orientada a facilitar la transición por fases de las implementaciones existentes a los estándares OSI.

(...)

Principios de la estructura en capas

5.2.2.1. La técnica básica de estructuración en el Modelo de Referencia para la Interconexión de Sistemas Abiertos es la estructura en capas. Según esta técnica, se concibe cada sistema abierto compuesto de un conjunto ordenado de *N* subsistemas, representados por conveniencia en una secuencia vertical. Los subsistemas adyacentes a *N* se comunican con él a través de su frontera común. Los subsistemas del mismo rango forman en conjunto la capa *N* del Modelo de Referencia. (...) Las entidades en la misma capa *N* se denominan entidades pares [*peer-entities*].



2

Infraestructura de las redes de datos

El modelo OSI, introducido en la Unidad anterior, nos permite estudiar y describir adecuadamente una red de comunicaciones. En esta Unidad nos centraremos específicamente en la capa inferior de las redes de transmisión de datos: estudiaremos en profundidad los medios físicos que se emplean en ellas, distinguiremos las redes Ethernet y Wi-Fi, y abordaremos la forma de implantar el *cableado estructurado* en la red (canalizaciones, conformación de los cables de transmisión y conexionado de estos en los armarios de distribución).

Contenidos

2.1. La infraestructura de las redes de datos y el modelo OSI
2.2. Medios de transmisión
2.3. Cableado en las redes de datos
2.4. Otros elementos de la red de datos
2.5. Control de acceso al medio

Objetivos

- Conocer el funcionamiento de los niveles inferiores de la red en el modelo OSI, particularmente la capa física y la de enlace de datos, así como las características de los estándares más utilizados en este nivel de la red, especialmente Ethernet y Wi-Fi.
- Conocer los medios de transmisión empleados en las redes de datos y las características diferenciadoras de cada uno de ellos, así como las ventajas y las limitaciones que presenta su uso.
- Identificar los medios para la instalación del cableado de la red de datos que resulten más adecuados para cada instalación particular, identificando los principales rasgos de cada una de las opciones para la canalización del cableado y para los puntos de acceso.
- Conocer el resto de elementos que forma parte de la red de datos y la función que desempeña cada uno de ellos.
- Ser conscientes de la importancia de los mecanismos de control de acceso al medio para garantizar el uso compartido y distribuido de los recursos de la red.

2.1. La infraestructura de las redes de datos y el modelo OSI

Hacia finales de la década de 1970 se había producido, especialmente en Estados Unidos, un crecimiento muy importante de las redes de datos. Cada fabricante imponía su propio protocolo, dando lugar a un problema de incompatibilidad entre redes de distintos fabricantes. Como consecuencia de ello, en 1980 el IEEE (véase la Unidad 1) creó un grupo de trabajo dedicado a establecer un conjunto de estándares para la comunicación en redes LAN y MAN. Ese grupo, numerado **802**, creó diversos subcomités para abordar las diversas áreas y temáticas de esta amplísima tecnología. Entre otros muchos, citaremos el **802.3** (*Ethernet Working Group*, Grupo de Trabajo de Ethernet) y el **802.11** (*Wireless LAN Working Group*, Grupo de Trabajo de Redes Locales Inalámbricas).

Lo que más nos interesa destacar aquí es la relación de los estándares **802** con el modelo de referencia OSI. Los servicios y protocolos surgidos de este grupo de trabajo pertenecen a las dos capas inferiores del modelo, la *capa física* y la *capa de enlace de datos*.

El enfoque de los estándares 802 no se corresponde exactamente con las capas o niveles OSI (véase la **Figura 2.1**). En el enfoque del IEEE, la capa de enlace de datos se divide en dos:

- **Control de acceso al medio** (MAC, *Medium Access Control*). Este subnivel se encarga de definir las reglas de acceso al medio de transmisión, para que los diversos nodos de la red puedan *compartir* dicho medio (véase el Apartado 2.5). Además, este subnivel define unas direcciones de 48 bits denominadas *direcciones MAC*. Los dispositivos de red poseen una dirección MAC única, asignada por el fabricante y almacenada en el *hardware*.

> **Recuerda que...**
>
> La dirección MAC es una dirección única que posee cada dispositivo en la red. Pertenece al nivel 2 de OSI, a diferencia de las direcciones IP (Unidad 4), que pertenecen al nivel 3. Está formada por 48 bits, aunque normalmente se escribe en notación hexadecimal (por ejemplo, ***01:23:45:67:89:ab***).

- **Control de enlace lógico** (LLC, *Logic Link Control*). Las tareas de este subnivel son el control de flujo, la retransmisión de tramas y la comprobación de errores, entre otras.



Figura 2.1. Algunos de los principales grupos de trabajo y estándares IEEE 802 y su relación con las capas del modelo OSI.

2.1.1. Ethernet

Ethernet es una familia de tecnologías para la implantación de redes locales. Se introdujo comercialmente en 1980 y, en la actualidad, ha remplazado casi completamente a otras tecnologías de redes de área local, como *Token Ring*. Desarrollada inicialmente a mediados de la década de 1970 por Xerox, DEC e Intel, Ethernet fue estandarizada en 1985, cuando se publica el estándar IEEE 802.3.

Aunque inicialmente esta tecnología utilizaba el cable coaxial como medio de transmisión, en la actualidad se emplean principalmente el cable de par trenzado y la fibra óptica, la velocidad de transmisión ha ido creciendo rápidamente, desde los 10 Mbits/s originales a los 100 Gbits/s.

> **¿Sabías que...?**
>
> *Token Ring* es una tecnología para la implementación de redes locales con topología en anillo. Para evitar que varios dispositivos transmitan simultáneamente y se produzca una colisión, emplea un control de acceso al medio basado en un testigo (*token*), una trama de tres bytes que viaja por el anillo. Solo el equipo que está en posesión del testigo puede trasmitir a través del medio.

Ethernet divide los paquetes de datos que deben enviarse a través de la red en pequeños trozos denominados *tramas*. Cada trama contiene, además de los datos, la dirección del remitente y del destinatario y mecanismos para la detección de errores.

El estándar IEEE 802.3 de Ethernet está diseñado para que la red pueda implementarse sobre diversos medios físicos, con distintas velocidades de transmisión. Para identificar estos medios se emplea una nomenclatura o notación estándar; la **Figura 2.2** nos ayudará a interpretarla.

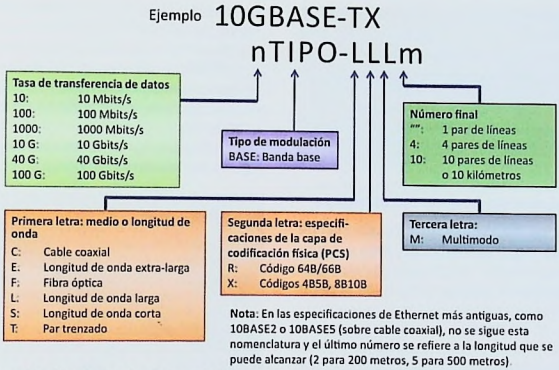


Figura 2.2. Notación para identificar los medios de transmisión empleados en Ethernet.

¿Sabías que...?

¿Qué significa «Banda base»? En telecomunicaciones, se habla de «banda base» cuando el canal de transmisión está ocupado completamente por la señal transmitida. La señal no precisa de dispositivos de modulación (módems), transmitiéndose «tal cual» a través del medio. Se suele emplear exclusivamente para distancias cortas, puesto que es una técnica más susceptible a las interferencias electromagnéticas y a la degradación de la señal que estas generan.

2.1.2. Wi-Fi

Las redes Wi-Fi son redes locales inalámbricas basadas en los estándares **IEEE 802.11**. La transmisión de información a través de estas redes se efectúa a través de ondas de radio, como veremos en detalle más adelante (Apartado 2.2.6). Los dispositivos se conectan a la red a través de un punto de acceso inalámbrico (véase la **Figura 2.3**). El alcance de estos puntos de acceso suele ser de unos 20 metros aproximadamente en el interior de un local o vivienda, la presencia de muchas redes próximas entre sí o la existencia de paredes gruesas pueden hacer que esa distancia se reduzca sensiblemente.



Figura 2.3. Logotipo de Wi-Fi. Cortesía de Wi-Fi Alliance (www.wi-fi.org).

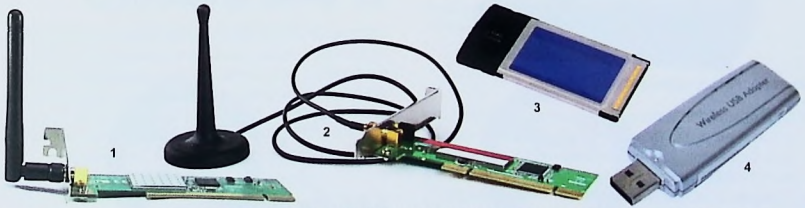


Figura 2.4. Diversos adaptadores para la conexión a redes inalámbricas. **(1)** Adaptador de red PCI con antena incorporada. **(2)** Adaptador de red PCI con antena independiente. **(3)** El adaptador PCMCIA, para su uso principalmente en ordenadores portátiles, se ha visto en buena medida reemplazado por los adaptadores USB **(4)**.

¿Sabías que...?

La *Wi-Fi Alliance* es una organización formada en 1999 por dos fabricantes, Nokia y Symbol Technologies, con el objetivo de crear una marca que potenciase el desarrollo comercial de redes inalámbricas de alta velocidad. La organización certifica aquellos productos que cumplan con ciertos estándares de funcionamiento e interoperatividad.

Seguridad en el acceso a redes inalámbricas

Las redes cableadas, como Ethernet, proporcionan de por sí una forma de seguridad intrínseca: para acceder a ellas es necesario conectar físicamente un cable a un conmutador u otro dispositivo de red, o bien superar un cortafuegos configurado para evitar accesos exteriores a la red local. En cambio, el acceso a una red inalámbrica es mucho más simple, pues basta hallarse dentro del alcance de la red para poder enviar y recibir paquetes de datos. Para evitar accesos no autorizados se emplean una serie de métodos, que se describen a continuación:

- Los puntos de acceso inalámbricos pueden configurarse de tal modo que solo permitan acceder a dispositivos con una dirección MAC conocida. Existen, sin embargo, mecanismos para el «burlado de direcciones MAC» o suplantación de identidad (*MAC spoofing*). Mediante el análisis de los paquetes que circulan por la red, un atacante puede detectar direcciones MAC válidas y posteriormente modificar la dirección MAC asignada al adaptador de red del *intruso*.



Figura 2.5. Punto de acceso inalámbrico.

- Otra posibilidad para evitar el acceso no autorizado a la red es el uso de diversos *algoritmos de seguridad*. Entre ellos, los más importantes son los siguientes: (1) **WEP** (*Wired Equivalent Privacy*, Privacidad Equivalente al Cableado), algoritmo desarrollado en 1999 y con fallos de seguridad bien conocidos, que hacen que, con las herramientas software adecuadas, se puede romper la protección que proporciona en cuestión de minutos. (2) **WPA** (*Wi-Fi Protected Access*, Acceso Wi-Fi protegido), algoritmo más seguro pero que también tiene vulnerabilidades conocidas. (3) **WPA2**, un sistema que conlleva un algoritmo de seguridad sofisticado; aun así, en diciembre de 2011 se publicó una vulnerabilidad de este mecanismo, sobre el que volveremos en la Unidad 4 para aprender cómo configurar correctamente la seguridad del punto de acceso inalámbrico.

¿Sabías que...?

Un «punto caliente» o *hotspot* Wi-Fi es un espacio en el que se ofrece acceso público a Internet (gratuito o de pago) a través de una red inalámbrica. Normalmente la red está dimensionada para soportar una elevada densidad de tráfico, pues los *hotspots* se encuentran en lugares públicos (bibliotecas, aeropuertos, cafeterías, etcétera.) en los que el número de estaciones conectadas a la red puede llegar a ser muy alto.



Figura 2.6. Logotipo de *hotspot* Wi-Fi.

Actividad propuesta 2.1

¿En qué se diferencia una red Ethernet de una red Wi-Fi? ¿Qué estándares se corresponden con cada una de ellas? Pon algunos ejemplos de su ámbito de aplicación: ¿en qué casos emplearías una red cableada y en cuáles una red inalámbrica?

2.2. Medios de transmisión

Los medios de transmisión empleados en las telecomunicaciones pueden clasificarse atendiendo a si la transmisión de la señal se efectúa de modo *guiado* o *no guiado*. Entre los guiados, estudiaremos el par trenzado, el cable coaxial y la fibra óptica; entre los no guiados, las ondas electromagnéticas. En los siguientes apartados nos referiremos en detalle a cada uno de ellos.

2.2.1. Par trenzado

El cable de par trenzado está formado por dos conductores (por lo general, dos hilos de cobre) trenzados

entre sí en forma de hélice a razón de un determinado número de vueltas por metro de longitud de cable. Cada conductor cuenta con un recubrimiento aislante de plástico y el cable en su conjunto posee un aislamiento propio y, en ocasiones, un blindaje metálico. El trenzado proporciona resistencia mecánica y, sobre todo, hace que la señal de ambos cables se vea igualmente afectada por las interferencias externas, con lo que las señales no deseadas se cancelan entre sí.

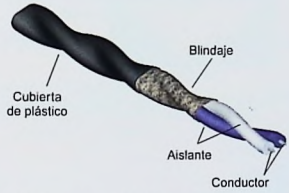


Figura 2.7. Esquema de un cable de par trenzado.

Las principales ventajas de este medio de transmisión son el reducido coste de fabricación y la facilidad para instalarlo. La desventaja es que la velocidad de transmisión disminuye rápidamente con la distancia que debe recorrer la señal.

En las redes de transmisión de datos, el cable de par trenzado suele contener más de un par: existen en el mercado cables de 4 u 8 pares (los más comunes), pero también de 100 y 300 pares, y de ahí en adelante (hasta un máximo de 2200).

Los cables de par trenzado pueden dividirse en dos grupos:

- Los cables **sin blindaje** o **no apantallados**, conocidos por sus siglas UTP (*Unshielded Twisted Pair*), carecen de blindaje, por lo que son más propensos a las interferencias y en ellos las velocidades de transmisión son más bajas (véase la **Tabla 2.2**).
- Los cables **blindados** o **apantallados** poseen una envoltura metálica que aísla el cable frente a interferencias externas. Existen varios tipos de blindaje, que se resumen en la **Tabla 2.1**. La **Figura 2.10** muestra un esquema de la sección de dos de ellos, a modo de ilustración.

Tabla 2.1. Tipos de cable de par trenzado según su blindaje.

Denominación	Blindaje de par	Blindaje de cable
UTP	Ninguno	Ninguno
STP	Lámina metálica	Ninguno
FTP	Ninguno	Lámina metálica
F/STP	Lámina metálica	Lámina metálica
SFTP	Lámina metálica	Lámina metálica y malla de cobre

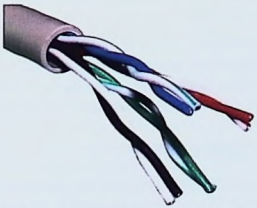


Figura 2.8. Cable de par trenzado no apantallado (UTP).

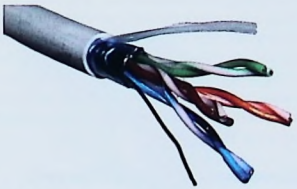


Figura 2.9. Cable FTP, en el que podemos observar la lámina metálica que recubre el conjunto de los pares trenzados.

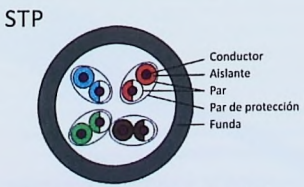


Figura 2.10. Sección esquemática de los cables STP y SFTP.

Tabla 2.2. Categorías de cable de par trenzado.

Nombre	Ancho de banda	Velocidad	Aplicaciones	Observaciones
Nivel 1	0.4 MHz		Líneas de teléfono y de módem.	No válido para sistemas modernos.
Nivel 2	4 MHz	4 Mbits/s	Terminales informáticos antiguos.	No válido para sistemas modernos.
Cat3	16 MHz	10 Mbits/s	10Base-T y 100Base-T4 Ethernet.	No válido para velocidades superiores a 16 Mbits/s. Hoy en día se usa principalmente en cables telefónicos.
Cat4	20 MHz	16 Mbits/s	Redes *Token Ring* de 16 Mbits/s.	No se emplea habitualmente.
Cat5	100 MHz	1 Gbit/s	100Base-TX y 1000Base-T Ethernet.	El más común hoy en día en la mayor parte de redes locales.
Cat5e	100 MHz	1 Gbit/s	100Base-TX y 1000Base-T Ethernet.	Categoría 5 mejorada.
Cat6	250 MHz	10 Gbit/s	10GBase-T Ethernet.	
Cat6a	500 MHz	10 Gbit/s	10GBase-T Ethernet.	
Clase F	600 MHz	10 Gbit/s	Teléfono, CCTV, 1000Base-TX en el mismo cable. 10GBaseT Ethernet.	Cable SFTP de cuatro pares.
Clase Fa	1000 MHz	100 Gbit/s	Teléfono, televisión por cable, 1000Base-TX en el mismo cable. 10Base-T Ethernet.	Cable SFTP de cuatro pares.

Debido a la diversidad de elementos que influyen en las características y el rendimiento (la velocidad de transmisión) de los cables de par trenzado, la EIA (*Electronic Industries Alliance*, Asociación de las Industrias Electrónicas) ha desarrollado una serie de estándares para el *cableado estructurado*. Como parte de estos estándares, se determinan una serie de *categorías* de cable que definen su calidad y sus prestaciones, se resumen en la **Tabla 2.2**.

Conectores para cable de par trenzado

Los conectores más utilizados para cable de par trenzado se denominan genéricamente *Registed Jack* o RJ. Los más habituales son los siguientes (véase la **Figura 2.12**):

- El **RJ45**, que emplea conectores modulares de 8 pines a los que se conectan cuatro pares de cables (8P8C); se emplea para redes de datos. El estándar que regula la forma de conexionado de los cables al conector, según su código de colores, es el TIA/EIA-568, de la Asociación de la Industria de las Telecomunicaciones (TIA, *Telecommunications Industry Association*). En realidad, este estándar define dos normas de conexionado diferentes, la **T568A** y la **T568B**. En la **Figura 2.11** se muestra la forma de conectar los cables al conector RJ45 según cada una de estas normas.
- El **RJ11** emplea conectores modulares de 8 pines a los que se conectan un par de cables (6P2C) o dos pares (6P4C) si la alimentación se efectúa mediante un par independiente; se emplea para redes telefónicas.

2.2.2. Cable coaxial

El cable coaxial está formado por dos conductores. Uno de ellos es un hilo rígido situado en el centro del cable; este hilo está recubierto por un material aislante que lo separa del otro conductor, una malla metálica. Esta malla sirve asimismo como blindaje frente a las interferencias electromagnéticas. En la parte exterior, una cubierta plástica aísla el cable de posibles contactos eléctricos y lo protege frente a la humedad o el polvo. Los cables de este tipo pueden transportar señales con rangos de frecuencia más elevados que los cables de par trenzado, pero la atenuación con la distancia que sufre la señal es mayor.

En la actualidad, el cable coaxial se emplea principalmente para transportar señales de televisión (CATV

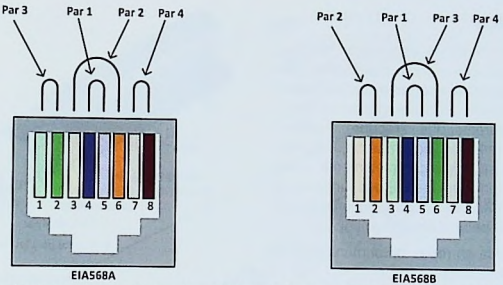


Figura 2.11. Conexión del cable de par trenzado a los conectores 8P8C según las normas T568A y T568B. Vista de la disposición de los cables en el conector con la patilla de este situada hacia abajo.



Figura 2.12. Conectores RJ45 y RJ11.

o televisión por cable). Las primeras redes Ethernet (10BASE2, 10BASE5) empleaban cable coaxial como medio de transmisión, pero hoy en día este ha quedado completamente obsoleto en las redes de datos.

Para la conexión del cable coaxial se suelen emplear unos conectores denominados BNC (*Bayonet Neill-Concellman*, por el nombre de sus inventores y la conexión rápida en forma de bayoneta; los conectores BNC macho y hembra se acoplan y se giran un cuarto de vuelta, quedando fijamente unidos). En otros casos se usan conectores con rosca, como TNC, SMA o SMC.



Figura 2.14. Conector BNC hembra.

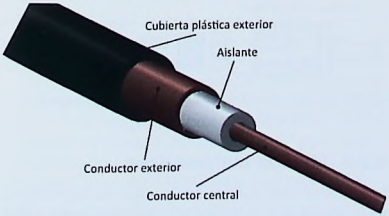


Figura 2.13. Esquema de los componentes de un cable coaxial.



Figura 2.15. Conectores SMA hembra y macho.

2.2.3. Fibra óptica

La fibra óptica es un medio de transmisión flexible y transparente, fabricado con vidrio o materiales plásticos, que se emplea para transportar ondas luminosas. El medio posee un material transparente en su interior y otro, también transparente, que lo recubre; el exterior posee un índice de reflexión algo más bajo, haciendo que el haz de luz se refleje completamente y quede confinado en el interior del medio, que funciona así como una *guía de ondas*. Las fibras tienen un grosor ligeramente superior al de un cabello humano.

El uso de la fibra óptica en redes de comunicaciones presenta una serie de ventajas:

- La señal que transmite la fibra óptica no sufre la influencia de campos electromagnéticos externos.
- La luz se propaga por la fibra con menor atenuación que a través de los cables conductores, lo que hace posible comunicaciones a larga distancia con un número reducido de repetidores.
- Las señales transmitidas a través de la fibra poseen un ancho de banda elevado, lo que permite velocidades de transmisión de entre 10 y 40 Gbps.
- Cada fibra puede transportar diversos canales (hasta ocho), cada uno de ellos mediante un haz de luz con una longitud de onda diferente.

La principal desventaja del cableado de fibra óptica es el elevado coste del medio de transmisión y del equipo necesario para su uso por parte del usuario final.

Existen dos tipos de cables de fibra óptica, en función de la forma en la que la luz viaja a través de ellos: multimodo y monomodo:

- Los cables **monomodo** son sumamente finos (su grosor es del orden de las micras, aproximadamente diez veces mayor que la longitud de onda del rayo luminoso), de modo que la luz viaja siguiendo una trayectoria prácticamente constante a lo largo del núcleo.
- Los cables **multimodo**, por el contrario, tienen un grosor superior a las 10 micras; en ellos, la luz experimenta reflexiones a lo largo de su camino, y puede seguir diversas trayectorias (véase la **Figura 2.16**).

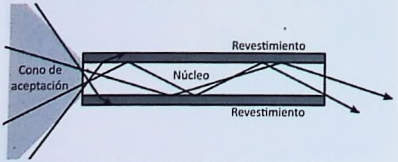


Figura 2.16. Sección longitudinal de una fibra óptica multimodo.



Figura 2.17. Estructura de un cable de fibra óptica.

Conectores para fibra óptica

Existen diversos tipos de conectores para los cables de fibra óptica. En la **Figura 2.18** se muestran algunos de ellos; los más comunes son los LC y los SC; y en la **Figura 2.19** podemos comprobar las piezas de las que constan.

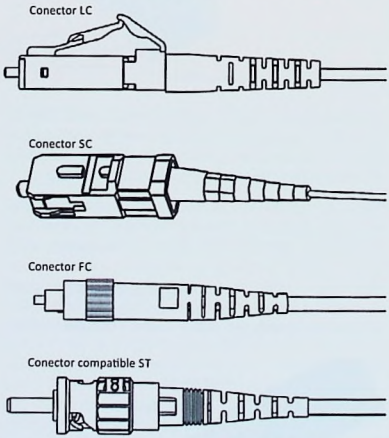


Figura 2.18. Tipos más comunes de conectores de fibra óptica. Cortesía de Corning Inc.

2.2.4. Medios inalámbricos

Los medios inalámbricos son medios no guiados que se basan en la transmisión de ondas electromagnéticas a través del aire o el espacio. Para la transmisión

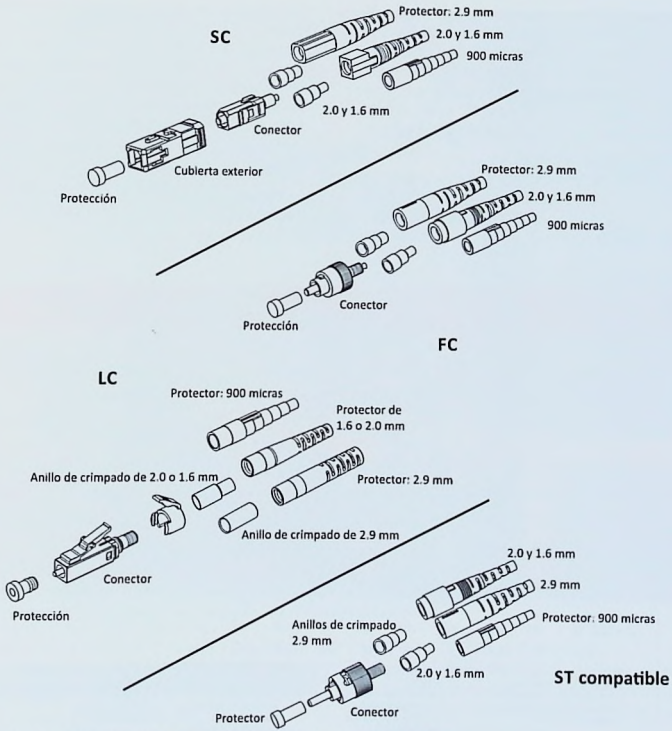


Figura 2.19. Despiece de los principales conectores de fibra óptica. Cortesía de Corning Inc.

de información se emplean ondas de diversas frecuencias, las más importantes de las cuales son:

- **Ondas de radio (radiofrecuencia)**. Este medio de transmisión presenta grandes ventajas frente a los medios guiados, como la movilidad, la facilidad de conexión a la red o la posibilidad de ampliar la red de modo sumamente sencillo. Sin embargo, el rango de radiofrecuencias presenta en la actualidad un grado muy elevado de utilización, lo que tiende a ocasionar problemas de interferencias en algunas bandas, como las empleadas por las redes Wi-Fi.
- **Microondas**. La elevada frecuencia de las microondas le proporciona a este tipo de ondas una gran capacidad de transmisión de información. Se emplea en comunicaciones vía satélite y comunicaciones con el espacio exterior o espacio profundo.
- **Infrarrojos**. Se emplean en comunicaciones de corto alcance, puesto que estas ondas no pueden atravesar paredes, por ejemplo, en las comunicaciones de los aparatos con control remoto.
- **Láser**. Se trata de ondas direccionales, que requieren que emisor y receptor estén perfectamente alineados y exista visión directa entre ellos.

La frecuencia de las ondas empleadas es importante por dos motivos:

1. Las emisiones de frecuencia elevada (láser y microondas) son *direccionales*; es decir, la onda se transmite principalmente en una dirección determinada, estos medios son preferibles en las transmisiones punto a punto. Sin embargo, cuando se requiere que la señal sea recibida por varios receptores, se suelen emplear ondas de radio, de frecuencia mucho más baja
2. La frecuencia determina también la forma en la que se propaga la onda electromagnética. Las ondas de frecuencia inferior a 2 MHz viajan por la superficie de la Tierra; las de frecuencia situada entre los 2 y los 30 MHz se transmiten hacia arriba y rebotan en la ionosfera —la parte superior de la atmósfera terrestre—, lográndose de este modo mayor alcance; las ondas de frecuencia superior a 30 MHz se transmiten en línea recta entre el emisor y el receptor, y es necesario que exista *visión directa* entre ambos, es decir, que no estén separados por ningún obstáculo. En función de su frecuencia, las ondas de radio se clasifican en *bandas*, la **Tabla 2.3** muestra las características y aplicaciones de cada una de ellas.

En la **Figura 2.20** podemos observar una clasificación de los medios de transmisión en función de la frecuencia a la que se transmite la señal.

Tabla 2.3. Bandas de radiofrecuencia.

Banda	Rango de frecuencias	Propagación	Aplicación
VLF (*Very Low Frecuency, Frecuencia Muy Baja*)	3–30 kHz	Tierra	Navegación de largo alcance
LF (Low Frequency, Baja Frecuencia)	30–300 kHz	Tierra	Localización de navegación
MF (*Middle Frequency*, Frecuencia Media)	300 kHz–3 MHz	Cielo	Radio AM
HF (*High Frequency*, Alta Frecuencia)	3–30 MHz	Cielo	Comunicación con aviones y barcos
VHF (*Very High Frequency*, Muy Alta Frecuencia)	30–300 MHz	Cielo y línea de vista	Radio FM y televisión VHF
UHF (*Ultra High Frequency*, Frecuencia Ultra Alta)	300 MHz–3 GHz	Línea de vista	Televisión UHF
SHF (*Super High Frequency*, Frecuencia Súper Alta)	3–30 GHz	Línea de vista	Comunicación vía satélite
EHF (*Extremely High Frequency*, Frecuencia Extremadamente Alta)	30–300 GHz	Línea de vista	Radar y satélite

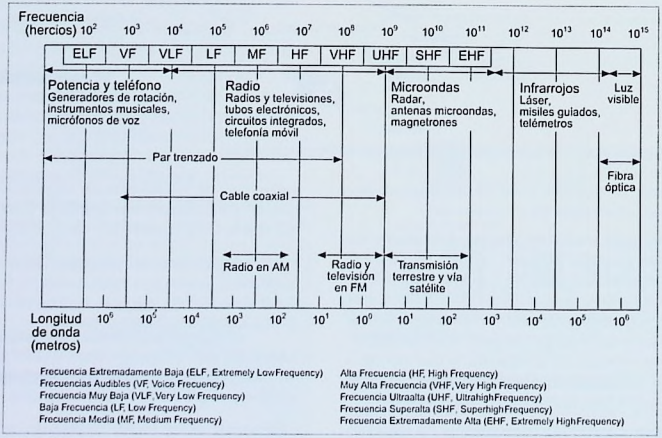


Figura 2.20. Clasificación de los medios de transmisión en función de la frecuencia empleada.



Figura 2.21. Diversos tipos de canalizaciones y puntos de acceso. Cortesía de Legrand.

Actividad propuesta 2.2

¿Por qué se emplean las ondas de mayor longitud de onda (menor frecuencia) para la navegación de largo alcance? ¿Es mayor el alcance de la radio AM o el de la FM? ¿Qué señales son capaces de transmitir mayor cantidad de información en la unidad de tiempo: las de mayor frecuencia o las de menor frecuencia?

2.3. Cableado en las redes de datos

Tal como estudiaremos enseguida en el Apartado 2.4.1, en una instalación de comunicaciones en una oficina, empresa, edificio o grupo de edificios se sigue una distribución *estructurada*, diseñada en forma lógica; el cableado se instala en el edificio mediante una serie de canalizaciones que permitan llevar los cables necesarios a todos los equipos de la red. Existen diversos tipos de canalizaciones, que varían según el local o edificio que se debe cablear y el tipo de instalación. Los tipos más comunes son:

- Suelo técnico.
- Techo técnico.
- Canaletas de superficie.

En las páginas siguientes estudiaremos en detalle cada uno de ellos.

2.3.1. Suelo técnico

El llamado *suelo técnico* es una estructura que se monta sobre el pavimento del local para sobre-elevar el piso y distribuir el cableado por debajo. Es muy útil en locales y oficinas en los que exista una gran cantidad de cables. En las **Figuras 2.22** y **2.23** se muestran los principales componentes de esta solución estructural.



Figura 2.22. Ejemplo de suelo técnico y elementos de los que consta. Cortesía de Legrand.



Figura 2.23. Aplicación del suelo técnico en una oficina. Se observan las conducciones diferenciadas para datos y electricidad. Cortesía de Legrand.

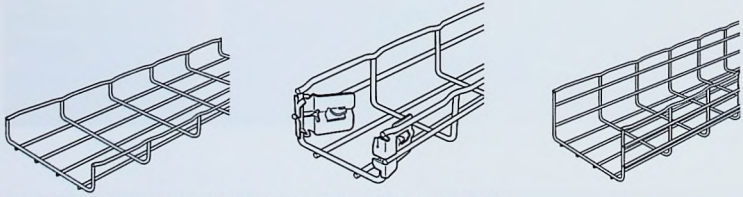


Figura 2.24. Rejillas para la colocación de cables en suelo técnico. Cortesía de Legrand.

2.3.2. Techo técnico

El *techo técnico* o *falso techo* está compuesto por una serie de elementos que se sitúan bajo el techo *real* de la planta que queremos cablear. En el falso techo se disponen conducciones de diversos tipos (eléctrica, datos, aire acondicionado, calefacción, megafonía, instalaciones de automatización, sensores, etcétera) y bajo las conducciones se sitúan unos paneles destinados a cubrir las canalizaciones y a proporcionar aislamiento térmico y acústico.

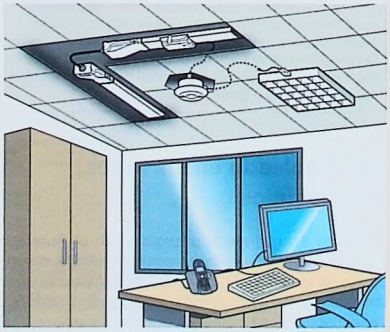


Figura 2.25. Ejemplo de techo técnico. Cortesía de Legrand.

2.3.3. Canaletas de superficie

Las *canaletas* están formadas por una serie de conductos plásticos que se sitúan sobreponiéndolos en las paredes del edificio u oficina que queremos cablear. Su instalación es mucho más sencilla que la de los

elementos anteriores (suelo y techo técnicos) y de los tubos empotrados. Existen diversos tipos de canaleta, de tamaño adaptado a la cantidad de cables que deben albergar, así como accesorios para las curvas y las derivaciones y cajas para instalar mecanismos o tomas de electricidad y datos.

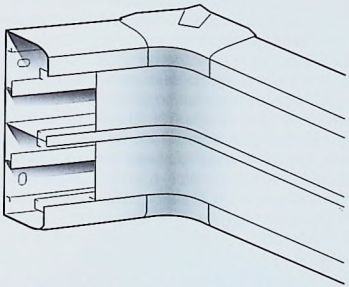


Figura 2.26. Detalle de canaleta de superficie con separación para cableado de energía y datos. Cortesía de Legrand.

2.3.4. Puntos de acceso

El *punto de acceso* o *toma ofimática* es la parte de la instalación destinada a dar servicio al usuario final, proporcionando las tomas para que los equipos se conecten a la red eléctrica y las redes de datos y telefonía. En el mercado existen muy diversas soluciones para este propósito, que elegiremos en función del espacio del que se trate y del tipo de instalación que se haya empleado. Entre ellas, citaremos las siguientes:

- Las **cajas de superficie** son fáciles de montar y constituyen una solución adecuada cuando se ha efectuado una instalación con canaletas y hay paredes en las que colocar las cajas junto a los lugares de trabajo donde están instalados los equipos a los que hay que dar servicio.
- En espacios diáfanos, en los que se ha efectuado una instalación en suelo técnico, se pueden emplear **cajas de suelo**, como las que muestran las **Figuras 2.28** y **2.29**.
- Otra opción para espacios abiertos son las **columnas** o **minicolumnas** (véase la **Figura 2.30**). Estas pueden conectarse al cableado del suelo técnico o del falso techo, según el modelo, y existen variantes con diversas alturas y con un número variable de tomas eléctricas y de datos.

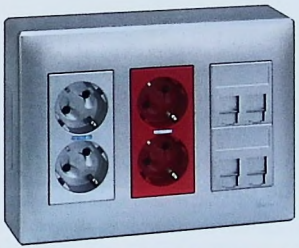


Figura 2.27. Caja para montaje en superficie con tomas de potencia tipo Schuko y adaptadores RJ45. Cortesía de Simon.

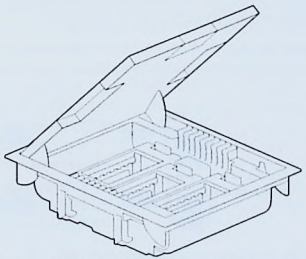


Figura 2.28. Caja de suelo de 12 módulos. Cortesía de Legrand.

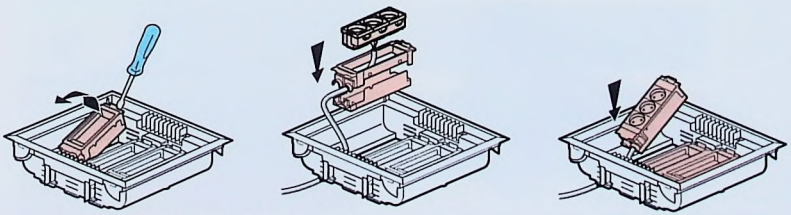


Figura 2.29. Secuencia de montaje para caja de suelo. Cortesía de Legrand.

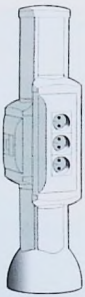


Figura 2.30. Minicolumna de aluminio con tomas de potencia y datos. Cortesía de Legrand.

2.4. Otros elementos de la red de datos

En este apartado estudiaremos los elementos necesarios para establecer una red local cableada tipo Ethernet, que, como hemos visto anteriormente, constituye la tecnología más común para LAN. Fijémonos en la **Figura 2.31**. Además del cableado propiamente dicho, los elementos empleados son los siguientes:

- **Roseta de red**. La roseta de red es un conector hembra para par trenzado que se acopla en la pared, ya sea empotrándolo en la pared o en una canaleta o atornillándola en superficie. En el interior de la roseta se efectúan las conexiones con el cableado de la red local, siguiendo las instrucciones que proporcione el fabricante.
- **Concentrador** (*hub*) y **conmutador** (*switch*). Ambos dispositivos permiten poner en comunicación los dispositivos de la red Ethernet. Se diferencian en su modo de funcionamiento: el *hub* simplemente difunde las señales que recibe por un puerto por todos los demás, funcionando de modo similar a un ladrón eléctrico; sus funciones se limitan, por tanto, a la capa física del modelo OSI. El *switch*, por el contrario, es un dispositivo dotado de cierta «inteligencia», que desempeña funciones correspondientes a la capa 2 (enlace de datos) o, en ocasiones, a capas superiores de la red. El *switch* descubre las direcciones MAC de cada una de las estaciones conectadas a sus puertos, y es capaz, de este modo, de enviar la trama de datos del puerto origen al puerto destino, en función de la dirección a la que vaya dirigida (de ahí el nombre de «conmutador»). Estos dispositivos cuentan, además, con una memoria intermedia o *buffer*, una por cada puerto, para almacenar temporalmente las tramas de datos. Todo ello hace que el *switch* se comporte de modo más eficiente que el *hub*, mejorando la velocidad de transmisión y reduciendo los tiempos de espera. Por esta razón, estos últimos han quedado desplazados por los conmutadores en la infraestructura de las redes Ethernet.

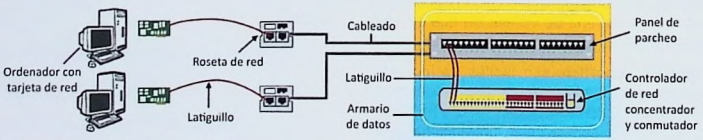


Figura 2.31. Elementos principales de una red local.

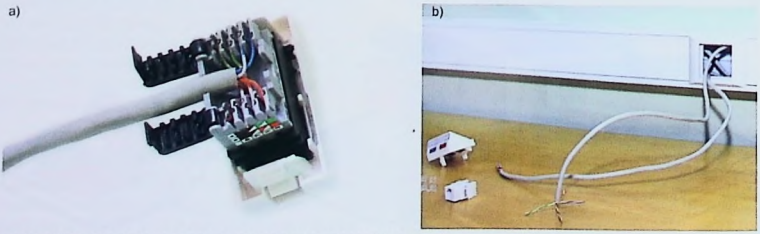


Figura 2.32. **a)** Vista interior de una roseta de red con sus conexiones. **b)** Instalación en una canaleta.

Universidad Tecnica del Norte
BIBLIOTECA
Ibarra Ecuador



Figura 2.33. Pequeño *switch* Ethernet de ocho puertos.

- **Adaptador de red Ethernet**. Para que un equipo pueda conectarse a una red de datos cableada necesita un *adaptador de red*. En particular, los dispositivos actuales cuentan con adaptadores de red Ethernet para conectarse a esta clase de redes locales. Muchos equipos de sobremesa llevan el adaptador integrado en la placa base; sin embargo, existen asimismo numerosas versiones en forma de tarjeta de expansión para ranuras PCI (véase la **Figura 2.34**).



Figura 2.34. Tarjeta de red Ethernet.

- **Panel de parcheo** o **panel de conexión**. Un panel de parcheo es un panel con un conjunto de conectores hembra RJ45, como si se tratase de varias rosetas de red una junto a otra. La **Figura 2.35** muestra la parte anterior y posterior de uno de estos paneles. Existen dos tipos de paneles de conexión: los que tienen las rosetas integradas en él y los que disponen de unos huecos para acoplar las rosetas individuales. Es importante tener en cuenta que el panel no sustituye al *switch*, sino que es un elemento destinado principalmente a *organizar* el cableado en instalaciones de tamaño medio o grande.

- **Armarios de distribución**. El armario de distribución es un punto clave en cualquier instalación de red. En el armario se centraliza todo el cableado de la instalación, colocando en su interior los paneles de conexión o los *switches* encargados de conectar los diversos equipos de la red. Podemos observar uno de estos armarios en la **Figura 2.36**.

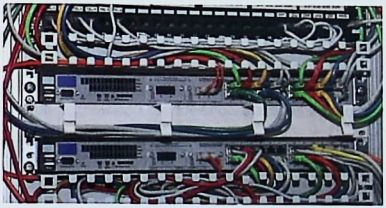


Figura 2.36. Armario de distribución en una red local.

2.4.1. Cableado estructurado

Hablamos de *cableado estructurado* para referirnos al cableado necesario para constituir un sistema de comunicaciones en un edificio o campus, compuesto de varios subsistemas estandarizados. Se trata de un cableado diseñado de forma lógica, para permitir la flexibilidad y la *escalabilidad* del sistema. En la configuración física del cableado se sigue una topología en estrella, que permite, sin embargo, la creación de diversas topologías *lógicas* sin más que cambiar las conexiones en los nodos centrales. El carácter *estructurado* del cableado permite configurar los puestos desde un nodo central hacia el exterior, sin modificar la configuración del resto, y facilita la localización de posibles averías.

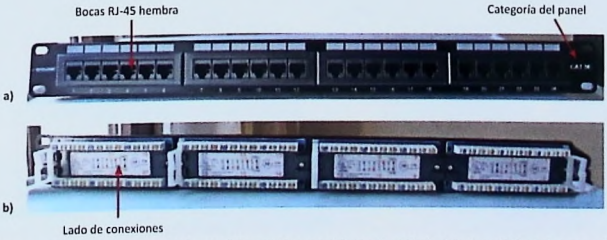
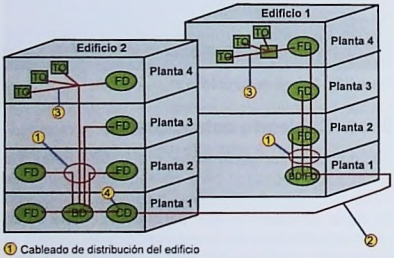


Figura 2.35. Panel de parcheo (también denominado panel de conexión o *patch panel*). **a)** Parte delantera. **b)** Parte trasera o de conexión.

Los elementos que componen la estructura son los siguientes (véase la **Figura 2.37**):

- Repartidor de campus (CD, *Campus Distributor*).
- Cableado de distribución o *backbone* de campus.
- Repartidor principal o repartidor del edificio (BD, *Building Distributor*).
- Cableado de distribución del edificio.
- Sub-repartidor de planta (FD, *Floor Distributor*).
- Cableado horizontal.
- Punto de transición (TP, *Transition Point*).
- Toma ofimática (TO).
- Punto de acceso o conexión.



① Cableado de distribución del edificio
② Cableado de distribución (Backbone) de campus
③ Cableado horizontal

Figura 2.37. Elementos de un sistema de cableado estructurado.

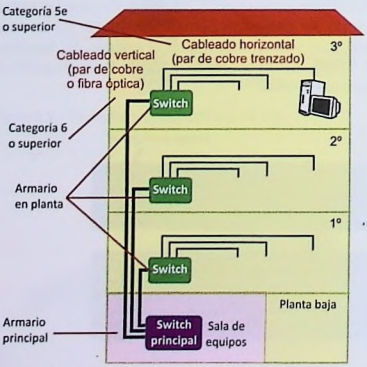


Figura 2.38. Esquema de cableado estructurado en un edificio.

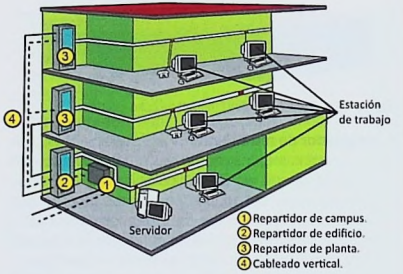


Figura 2.39. Esquema tridimensional de cableado estructurado en un edificio.

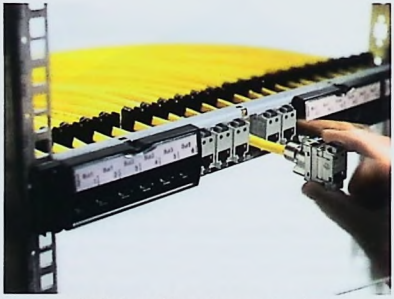


Figura 2.40. Detalle de panel de parcheo montado sobre rack. Cortesía de Legrand.

Actividad propuesta 2.3

Identifica todos los elementos del cableado estructurado implantado en tu centro educativo; localiza la ubicación de los mismos y dibújalos en un plano. Enumera las ventajas del uso del cableado estructurado en una red de datos.

2.5. Control de acceso al medio

¿Qué ocurre cuando dos ordenadores tratan de enviar simultáneamente información a través del mismo medio? Las redes que transmiten datos poseen una capacidad limitada, y en consecuencia puede circular cierto número de paquetes. El *control de acceso al medio* tiene como objeto evitar que se produzcan

colisiones en la información transmitida a través de la red y distribuir el medio de transmisión entre los equipos que lo comparten, evitando que uno solo acapare en exclusiva dicho medio.

Existen diversas formas de control de acceso al medio, que se pueden diferenciar siguiendo diversos criterios:

- Según *dónde* se efectúe el control de acceso, encontramos formas de carácter centralizado, en las que existe un dispositivo encargado de organizar el acceso, frente a otras distribuidas, en las que todos los equipos controlan el acceso basándose en una serie de reglas acordadas entre los participantes.
- Según *cómo* se efectúe el control, encontramos diversas formas o reglas de control; principalmente son la rotación circular, la reserva y la contienda. **(1)** En la *rotación circular*, cada uno de los equipos tiene asignado un turno para transmitir, que se va pasando de uno a otro secuencialmente. **(2)** En las técnicas de *reserva*, cuando un equipo desea transmitir, debe reservar un turno para hacerlo. **(3)** En la *contienda*, todos los equipos compiten por el uso del medio y tratan de transmitir a través de él. Si el medio está libre, se adueñan de él mientras dura su transmisión; si otro equipo está transmitiendo en ese momento, se detecta una *colisión*. Cuando eso ocurre, se ejecuta una secuencia de pasos para la que existen varias posibilidades, dando lugar a diversos protocolos de control de acceso. A modo de ejemplo citaremos dos:
  - Ethernet emplea un protocolo de control de acceso al medio denominado **CSMA/CD** (*Carrier Sense Multiple Access with Collision Detection*, Acceso Múltiple con Escucha de Portadora y Detección de Colisiones). Cuando un equipo detecta que el medio está libre, comienza a transmitir su trama de datos. Si en ese momento otro equipo había colocado sus datos en el medio, el primero detectará una colisión y esperará un lapso de tiempo aleatorio para tratar de transmitir de nuevo su trama.
  - Las redes inalámbricas suelen emplear un protocolo ligeramente distinto al anterior, denominado **CSMA/CA** (*Carrier sense multiple access with collision avoidance*, Acceso Múltiple con Escucha de Portadora y Evitación de Colisiones). En este caso, cuando un equipo desea transmitir «escucha» el medio y, si lo encuentra libre, espera un corto intervalo de tiempo aleatorio; si transcurrido ese intervalo el medio sigue libre, envía su trama de datos.

Actividad propuesta 2.4

¿Cuál es la función de los mecanismos de control de acceso al medio? ¿En qué capa de la red se implementan? Busca información sobre los mecanismos de control de acceso basados en la rotación circular. ¿En qué tecnologías de red se implementan? ¿En qué se diferencia la rotación circular de los protocolos CSMA?

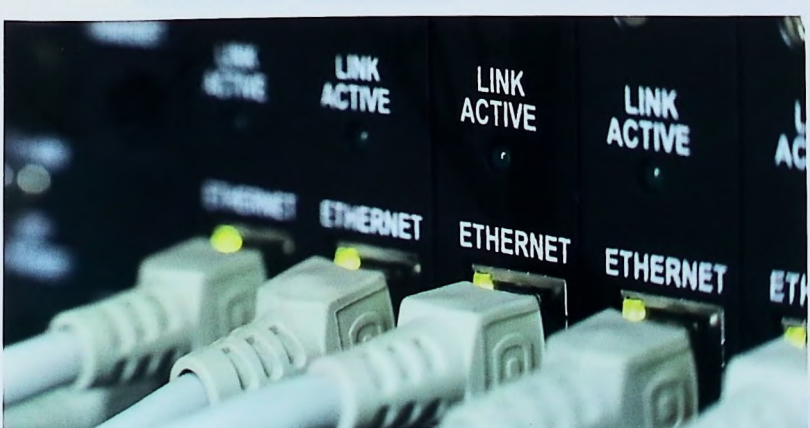
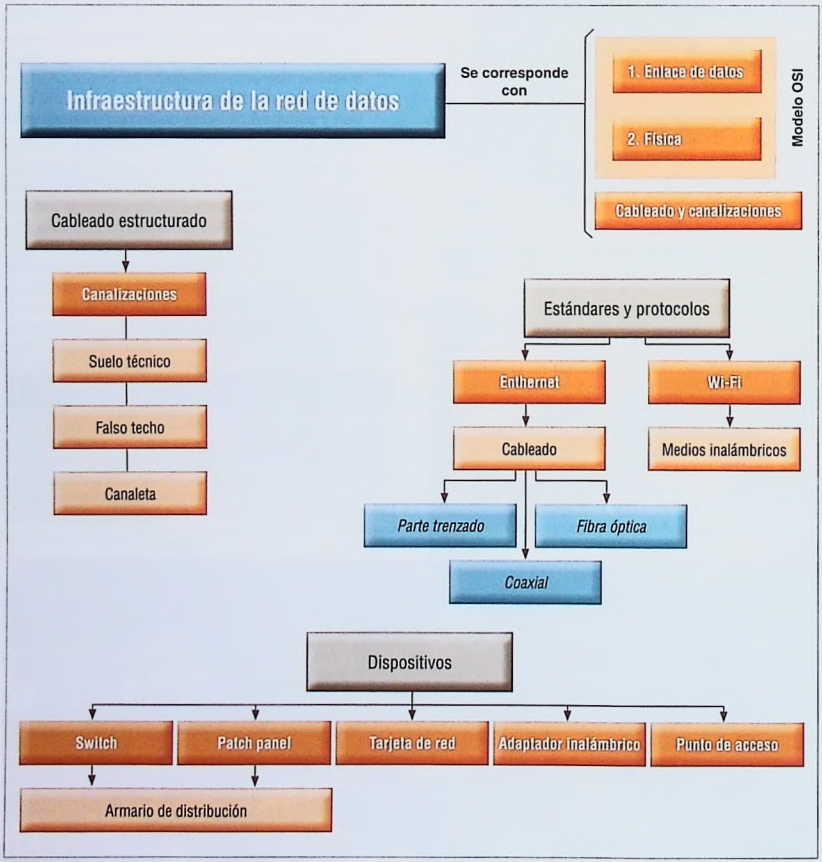


Figura 2.41. Detalle de las conexiones en un armario de distribución.

Mapa conceptual



Práctica profesional

2.1. Instalación de una canaleta de superficie para cableado de red

Por las razones que se expusieron en el Apartado 2.3.3, las canaletas de superficie son un elemento para la conducción del cableado muy habitual en las redes de transmisión de datos. La secuencia de operaciones para la instalación de estas canaletas es la siguiente:

1. En primer lugar, se elige el trayecto que deberá seguir la canaleta, a la altura más conveniente.
2. Se miden los tramos rectos que hay que instalar y se efectúan los cortes de las piezas. Estos cortes pueden efectuarse con una sierra manual o eléctrica. En ocasiones será preciso efectuar cortes en inglete (a 45°) para los giros, aunque en el mercado existen también accesorios para efectuarlos. Si empleamos la sierra manual, podemos utilizar una caja de ingletes para efectuar los cortes a 45°.
3. Se colocan o presentan los tramos cortados, retirando previamente su tapa y procurando que queden perfectamente horizontales o verticales (con ayuda del nivel), y se marcan los puntos en los que deberá perforarse la pared.
4. Se retira la canaleta y se efectúan los orificios por los puntos marcados.
5. Se introducen los tacos (con los de 6 mm de diámetro deberá ser suficiente) en los orificios.
6. Se atornilla la canaleta y se colocan los accesorios necesarios (piezas para giros, tapas, etcétera).

2.1.1. Tendido de los cables

Una vez instaladas las canaletas (u otros medios para la canalización del cableado como las bandejas para suelo técnico o falso techo), procederemos al tendido del cableado de red. En esta operación debemos seguir las normas que se detallan a continuación:

- En las esquinas y giros, el cable no debe quedar excesivamente doblado. Debe respetarse un radio mínimo de curvatura; suele recomendarse que el radio mínimo sea de cuatro veces el diámetro del cable.
- La proximidad de instalaciones y dispositivos eléctricos es una fuente de interferencias para la red de datos y puede dañar los equipos electrónicos conectados a ella. Por ello, nunca deben disponerse cables eléctricos y de red en la misma bandeja; si se instalan en canaleta, esta debe llevar un tabique de separación entre ellos. Como regla general, se dejará una distancia de 7,5 centímetros como mínimo entre ambos tipos de cable. Tampoco deben instalarse cerca de equipos eléctricos que, por sus características, son una fuente importante de ruido electromagnético, como tubos fluorescentes o motores eléctricos.
- Es importante que los cables queden holgados y no estén sometidos a esfuerzos de tracción. El fabricante del cableado indica en las especificaciones del cable el esfuerzo máximo de tracción admisible.
- Los cables deben cortarse dejando una longitud sobrante de medio metro en el extremo de la roseta de conexión y de cuatro metros en el extremo del armario de distribución.
- Los cables deben etiquetarse en ambos extremos para poder identificarlos y agruparse con bridas antes de colocarlos, para facilitar su instalación.

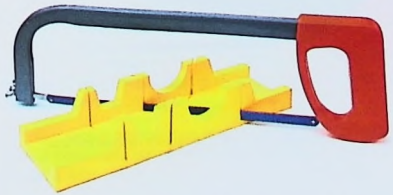


Figura 2.41. Caja de ingletes para el corte con la sierra manual.



Figura 2.42. Sierra ingletadora eléctrica.

Práctica profesional

2.2. Herramientas comunes en la instalación del cableado de red

La mayoría de las redes cableadas emplean en la actualidad el cable de par trenzado como medio de transmisión. En esta práctica describiremos las principales herramientas que se emplean para la colocación de conectores en esta clase de cables y para la comprobación del cableado.

Antes de colocar los conectores en un cable de red deberemos proceder a *pelar* el cable, es decir, a cortar su recubrimiento sin dañar el conductor interior. Para ello se emplean herramientas *pelacables* como la que podemos observar en la **Figura 2.43**.

La **crimpadora** (o las **pinzas de crimpar**) es una herramienta que se emplea para unir dos piezas mediante la deformación plástica de una de ellas o de ambas. Su uso más común es en la colocación de conectores RJ45 o RJ11, aunque también existen modelos para cable coaxial o para conectores de fibra óptica.

El **comprobador de cableado** o *tester* nos informa de si se han efectuado correctamente las conexiones del cableado. El *tester* comprueba la continuidad eléctrica en cada uno de los hilos del cable de red y, en algunos modelos superiores, nos informa también de si el cableado cumple con la categoría (5e, 6, etc.) de la instalación. En la **Práctica Profesional 2.6** profundizaremos en esta cuestión.

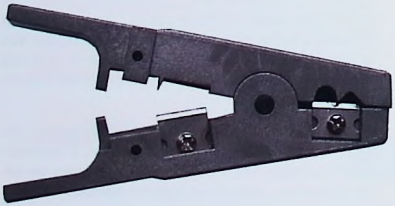


Figura 2.43. Herramienta para cortar y pelar cables.



Figura 2.45. Comprobador de cableado.

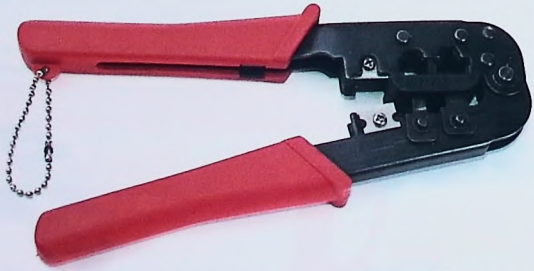
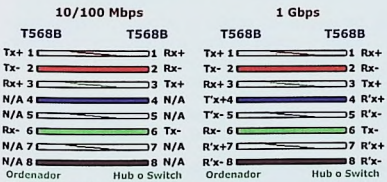


Figura 2.44. Herramienta crimpadora. Puede observarse que está adaptada para conectores RJ11 y RJ45 y que cuenta también con una cuchilla para pelar cable.

Práctica profesional

2.3. Colocación de un conector 8P8C (RJ45) en un cable de red

Cuando se desea confeccionar un cable de red para comunicar un equipo con un *switch* o un *patch panel*, se sigue el código de colores que observamos en la **Figura 2.46**. Los cables aparecen numerados del 1 al 8. En el conector 8P8C se colocan en ese orden situando la patilla del conector hacia abajo.



NA: No asignado.
Tx, T'x: transmisión.
Rx, R'x: Recepción.

Figura 2.46. Forma de colocación de los cables en el conector 8P8C (según la norma T568B) y función de cada uno de ellos.

En ciertas ocasiones, es posible que deseemos conectar directamente dos ordenadores a través de un cable de red, sin intermediación de un *switch*. En ese caso deberemos configurar un cable *cruzado*, disponiendo los cables en el conector en la forma que se indica en la **Figura 2.47**.

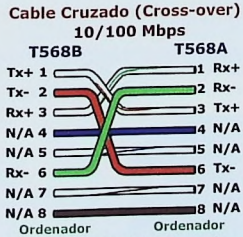


Figura 2.47. Forma de colocación de los hilos en el conector 8P8C para formar un cable cruzado.

El orden de las operaciones que debemos llevar a cabo para la colocación del conector es el siguiente (véase la **Figura 2.48**):

1. En primer lugar, pelamos con el pelacables uno de los extremos del cable, retirando el recubrimiento y dejando a la vista los ocho hilos de colores de los que está compuesto. Algunas crimpadoras (véase la **Figura 2.48b**) disponen de una cuchilla para pelar el cable de red.
2. Se desdoblan los pares de cables y se ordenan siguiendo la secuencia de colores correspondiente a la norma (T568A o T568B) que vayamos a utilizar. La **Figura 2.48c** muestra el orden de colores según la norma T568B.
3. Se cortan los cables con la cuchilla de la crimpadora situándola perpendicularmente al cable, para asegurar que tengan todos la misma longitud desde el borde cortado del recubrimiento. Se suele dejar una longitud de aproximadamente 12 mm, para que los hilos entren completamente en el conector.
4. Se coloca la patilla o clip del conector hacia abajo y se insertan los cables, asegurándonos de que llegan hasta el fondo del mismo y que mantienen el orden adecuado.
5. Se prensa o «crimpa» el conector mediante la herramienta crimpadora y se libera la presión sobre la herramienta, soltando el conector.
6. Se comprueba que los cables hayan quedado colocados correctamente y estén sujetos al conector RJ45.
7. Se repiten los pasos con el otro extremo del cable.

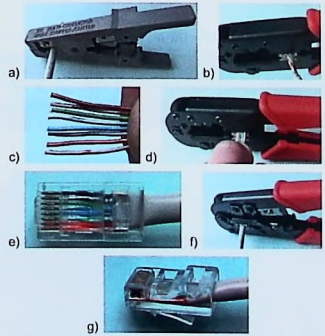


Figura 2.48. Secuencia de operaciones para la colocación de un conector 8P8C (RJ45). **(a)** Pelado del cable con el pelacables. **(b)** Pelado del cable con la crimpadora. **(c)** Disposición de los hilos del cable en el orden adecuado. **(d)** Corte perpendicular de los hilos para asegurar que todos tienen la misma longitud. **(e)** Inserción en el conector. **(f)** Crimpado del conector. **(g)** Conector una vez finalizado el proceso.

Práctica profesional

2.4. Instalación y cableado de los paneles de conexión

Antes de instalar y cablear los paneles dentro del armario de conexión, deberemos efectuar previamente un pequeño estudio de qué elementos tenemos que disponer dentro de él, para elegir correctamente el tamaño del armario y ubicarlos de manera óptima en su interior. Deberemos tener en cuenta las siguientes consideraciones:

- Las regletas para la alimentación eléctrica de los dispositivos del armario se sitúan en la parte inferior del mismo.
- Los equipos electrónicos deben situarse en la parte superior del armario, dejando un espacio libre por debajo de ellos para facilitar su ventilación.
- Los paneles para fibra óptica deben estar todos agrupados, siempre por debajo del *switch*.
- Los cables deben instalarse en las correspondientes guías para garantizar su sujeción y facilitar la circulación del aire dentro del armario.
- Si se instala un Sistema de Alimentación Ininterrumpida (SAI), este debe colocarse en la parte superior del armario.

Los pasos que se deben llevar a cabo para la instalación del armario y de los paneles de conexión son los siguientes:

1. Se monta la regleta de alimentación eléctrica en el armario, atornillándola en la parte inferior del mismo.
2. Se instalan las escuadras laterales en el *switch* y este se atornilla en la parte superior del *rack*, dejando un espacio libre por encima de él para asegurar su ventilación.
3. Se elige el modelo de panel de conexión que mejor se adapte a las necesidades de la instalación. En este caso emplearemos un panel con las rosetas integradas.
4. Se atornilla el panel al *rack*.
5. Se prepara el cable, pelando la cubierta exterior y dejando los hilos aproximadamente cuatro centímetros al descubierto.
6. Se colocan los cables en el lugar correspondiente según el código de color y se aplica la herramienta de inserción. La punta cortante de esta herramienta debe situarse siempre mirando hacia el exterior.
7. Se van conectando los cables desde la parte exterior del panel hacia su interior.
8. Por último, se colocan los cables en la guía de cables y se agrupan con bridas o, preferiblemente, con tiras de velcro.
9. En paneles de conexión apantallados, se conecta el panel al armazón del *rack* empleando los cables de conexión a masa correspondientes.

Si el panel de conexión está preparado para insertar en él rosetas de red individuales, procederemos de la forma que se representa en la **Figura 2.51**: en primer lugar, se conectan los cables a cada una de las rosetas de red, disponiendo los hilos en las ranuras que correspondan al código de color empleado. Una vez montada la roseta y colocada su cubierta (si dispone de ella), se atornilla el panel al *rack* y se insertan las rosetas en los orificios correspondientes, recogiendo finalmente los cables, del mismo modo que hicimos en el caso anterior.

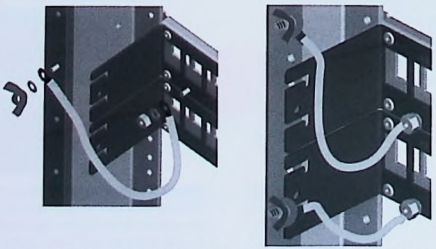


Figura 2.49. En paneles de conexión apantallados, se conecta el panel al armazón del armario empleando las conexiones preparadas a tal efecto. Cortesía de Belden Inc.

Práctica profesional

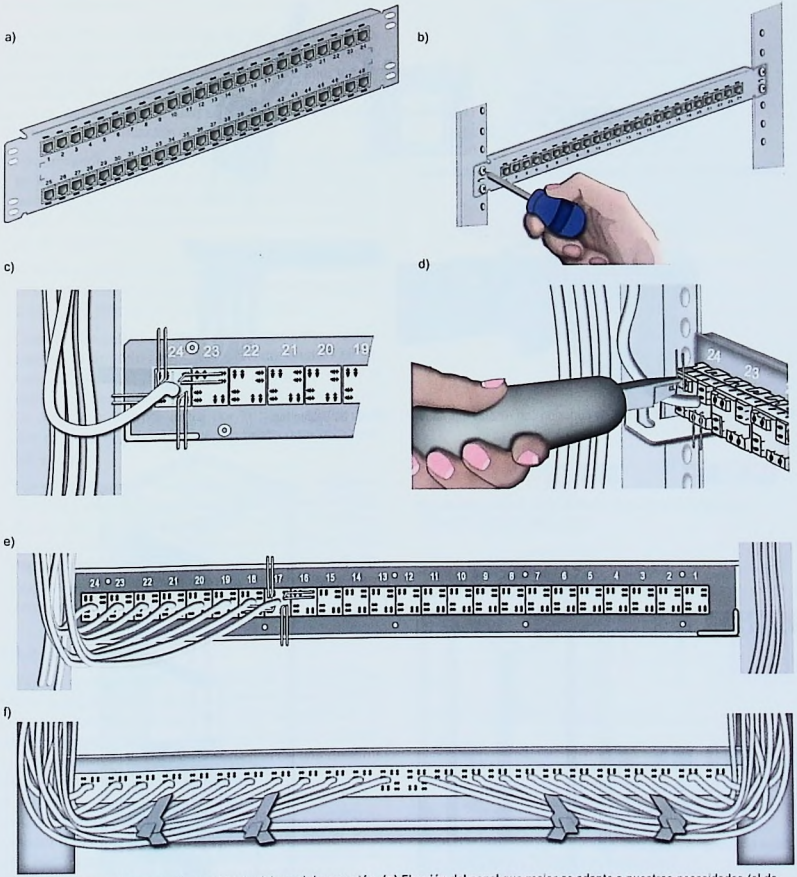


Figura 2.50. Pasos en la instalación y cableado del panel de conexión. **(a)** Elección del panel que mejor se adapte a nuestras necesidades (el de la figura, por ejemplo, es de 48 tomas o rosetas). **(b)** Fijación del panel al armario o rack mediante los tornillos de fijación. **(c)** Una vez pelado el cable, se introducen los hilos en los lugares correspondientes. **(d)** Se aplica la herramienta de inserción, cuidando de situar la punta de corte hacia el exterior. **(e)** Se conectan los cables del panel desde el exterior hacia el centro. **(f)** Se colocan los cables en las guías y se fijan con tiras de velcro. Cortesía de Belden Inc.

Continúa ›››

Práctica profesional

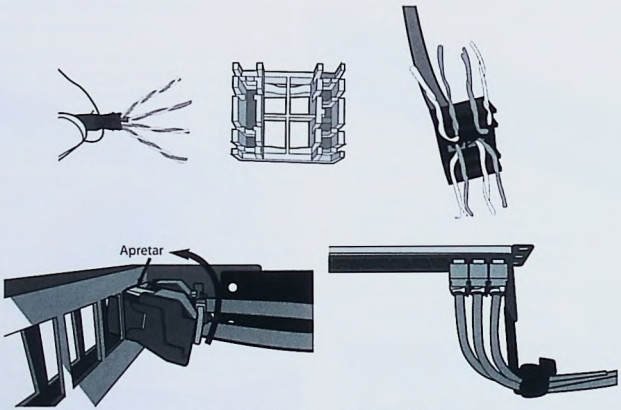


Figura 2.51. Montaje de un panel de conexión con rosetas individuales. Cortesía de Belden Inc.

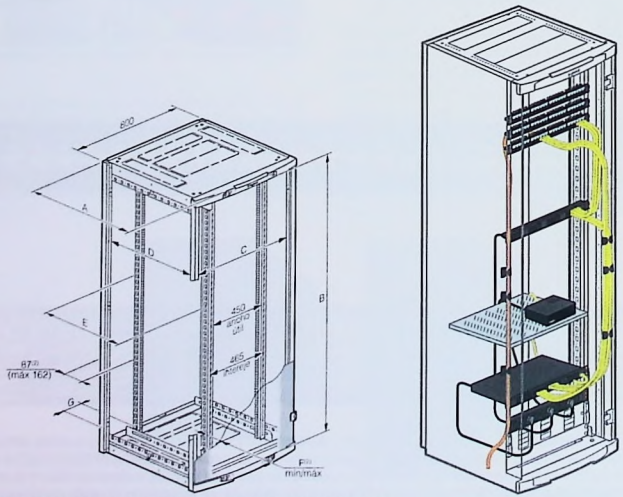


Figura 2.52. Armario para paneles de conexión (*patch panels*). Cortesía de Legrand.

Práctica profesional

2.4.1. Ventilación

Los componentes electrónicos de los paneles de conexión colocados en el interior de los armarios de distribución producen un calor considerable. Por ello, y para evitar daños a los equipos debido al aumento de la temperatura, deben seguirse una serie de reglas y consideraciones en la instalación de los armarios:

- Los armarios deben disponer de rejillas de ventilación en los laterales y en las caras superior e inferior. Para asegurar que por dichas rejillas circula el aire, debe dejarse una separación de unos 50 cm en cada lateral del armario.
- El cableado debe ordenarse y agruparse mediante bridas o tiras de velcro, evitando formar una maraña de cables que dificulte la circulación del aire.
- Cuando el número de dispositivos que se van a instalar en el armario no es muy elevado, bastan en general mecanismos de *ventilación pasiva*; es decir, el flujo ascendente de aire por los orificios del armario (el aire del ambiente entra por la parte inferior y el aire caliente sale por la superior) basta para refrigerar los equipos.
- Por el contrario, si el número de equipos instalados en el armario es muy elevado, se usan mecanismos de *ventilación activa* o *ventilación forzada*, instalándose en el techo del armario ventiladores como los de la **Figura 2.53**. Estos ventiladores son los que aseguran que se establezca un caudal de aire suficiente para refrigerar adecuadamente el interior del armario.

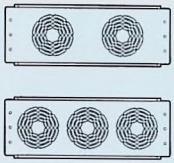


Figura 2.53. Ventiladores para armarios *rack*. Cortesía de Legrand.

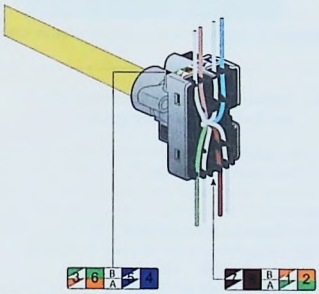


Figura 2.54. Conector de panel de conexión con el cableado conectado. Cortesía de Legrand.

2.4.2. Etiquetado

Identificar correctamente cada una de las rosetas del panel de conexión es una tarea fundamental para las operaciones de mantenimiento de la red e identificación de errores. El objetivo del etiquetado es identificar a qué equipo o dispositivo corresponde la conexión de una determinada roseta. En la etiqueta debe constar la ubicación y el número del equipo. Las etiquetas no deben escribirse a mano, sino elaborarse bien mediante una máquina rotuladora o bien mediante un procesador de textos. Para más información sobre el etiquetado de los paneles de conexión puede consultarse la norma EIA/TIA-606-A.

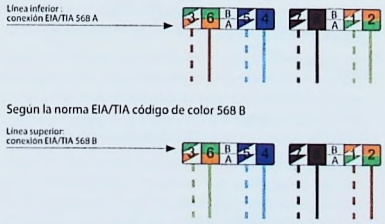


Figura 2.55. Conexión del cableado a la roseta de la Figura 2.54 según las normas T568A y T568B. Cortesía de Legrand.

Continúa >>>

Práctica profesional



Figura 2.56. Etiquetado de las conexiones del panel de conexión.

2.4.3. Conexión a la red eléctrica

La instalación eléctrica para la red de datos debe cumplir las especificaciones del Reglamento Electromagnético de Baja Tensión (REBT). Según el tamaño de la instalación, este Reglamento obliga a instalar o recomienda que los equipos de la red (tomas eléctricas de los armarios de distribución, sistemas de alimentación ininterrumpida y servidores de red) cuenten con una **Instalación Eléctrica Dedicada (IED)**, independiente de los demás circuitos del edificio. Esta IED debe contar con sus propios sistemas de protección (interruptor automático y diferencial).

2.5. Colocación de un conector SC en un cable de fibra óptica

En esta práctica aprenderemos a colocar un conector SC en un cable de fibra óptica. Puesto que se trata de un proceso laborioso y que requiere muchos pasos, lo dividiremos en tres «bloques» de operaciones: la preparación del cable; la preparación y colocación del conector SC; y el pulido y la terminación el conjunto.

2.5.1. Preparación del cable

Antes de la colocación de los conectores en el cable de fibra óptica, será necesario preparar el cable pelando sus fundas protectoras para desnudar la fibra, cuidando de respetar unas medidas que dependen del tipo de conector que vayamos a emplear.

1. Se coloca en el cable el protector del conector, introduciéndolo en el extremo del cable que debemos conectar.
2. Se marcan en el cable los puntos de pelado del cable y del conductor interior, empleando para ello la plantilla que corresponda al conector que vamos a emplear. En el paso 2 de la **Figura 2.57** se muestra la posición de ambos puntos para los tipos de conectores más habituales.
3. Se pela la funda protectora del cable con la herramienta pelacables por la marca más cercana al extremo del cable, siguiendo la guía mostrada en el paso 3 de la **Figura 2.57** y empleando el orificio de la herramienta que corresponda con el diámetro del cable. Se retira el trozo de cubierta pelado con la mano con cuidado para no romper la fibra.
4. Una vez pelado el cable, se corta el kevlar (aramida) sobrante con las tijeras, dejando al descubierto el protector interior de la fibra.
5. Se pela el cable por la segunda marca que efectuamos en el paso 2, dejando el kevlar al descubierto. Se introduce el anillo de crimpado y se doblan las fibras de kevlar hacia atrás.
6. Se marca el cable desde el extremo, siguiendo la referencia del paso 6 de la **Figura 2.57**. Empleando la herramienta especial para fibra, se pela el conductor interior por la marca dibujada y se deja al descubierto la fibra desnuda.
7. Se limpia la fibra con ayuda de un trapo limpio mojado en alcohol.

2.5.2. Preparación y colocación del conector

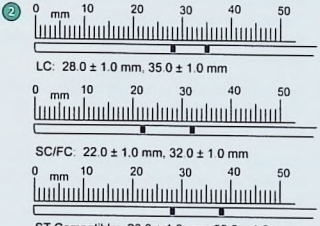
Una vez preparado el cable se prepara y coloca el conector. Este queda fijado al cable mediante un adhesivo de dos componentes; además, el conector va dotado de un anillo de crimpado que se prensará con la herramienta correspondiente para proporcionar resistencia mecánica al conjunto.

1. Se prepara una jeringuilla colocándole la aguja, se destapa el bote de adhesivo y se llena la jeringuilla con él, de la forma indicada en el paso 1 de la **Figura 2.58**.
2. Se inserta la aguja de la jeringuilla en el conector y se inyecta lentamente el adhesivo, limpiando posteriormente el sobrante de la parte superior con un trapo que no deje pelusa.
3. Se aplica el activador del adhesivo a toda la longitud de la fibra desnuda. Manteniéndola verticalmente se desliza el conector, girando la fibra ligeramente hasta que la parte inferior del conector asiente sobre el extremo del conductor interior. Deberán sobresalir unos cinco milímetros de fibra por encima del conector.

Práctica profesional



① Protector de 1,6 o 2,0 mm

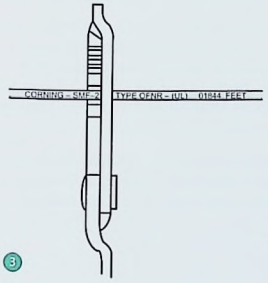


② 0 mm 10 20 30 40 50

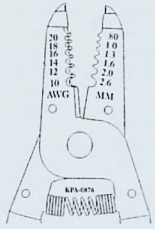
LC: 28.0 ± 1.0 mm, 35.0 ± 1.0 mm

SC/FC: 22.0 ± 1.0 mm, 32.0 ± 1.0 mm

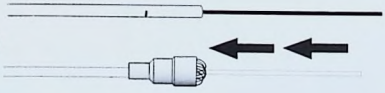
ST Compatible: 28.0 ± 1.0 mm, 38.0 ± 1.0 mm



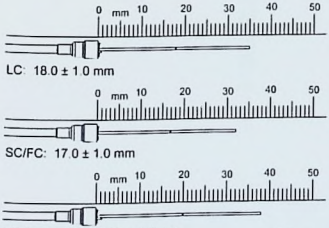
③



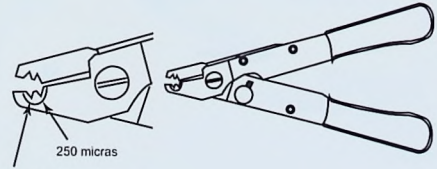
④



⑤



⑥



⑦

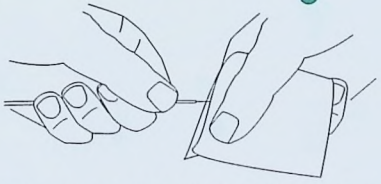


Figura 2.57. Pasos para la preparación de un cable de fibra óptica para la posterior colocación de un conector. Cortesía de Corning Inc. Los números de las ilustraciones corresponden a los pasos indicados en la práctica profesional.

Continúa >>>

Práctica profesional

En aproximadamente un minuto, el adhesivo habrá fraguado; durante ese tiempo deberemos asegurarnos de que la fibra permanece correctamente situada en él, sin moverse.

4. Con la herramienta de punta de diamante se corta la fibra sobrante, aplicando el corte al ras del extremo cerámico del conector.
5. Se retira hacia atrás el anillo de crimpado, liberando el kevlar que retuvimos con él en una de las operaciones anteriores. El kevlar deberá disponerse uniformemente cubriendo la parte trasera del conector SC. Posteriormente, se empuja el anillo de crimpado hacia el conector hasta que haga tope.
6. Se aplica la herramienta de crimpado en la posición que corresponda y se aprieta para fijar todo el conjunto. Finalmente, se desliza el protector hasta el extremo del conector.

2.5.3. Pulido y terminación del conector

Una vez colocado el conector, se deberá pulir la superficie del mismo para asegurar un contacto óptimo. Para ello se efectuarán las siguientes operaciones:

1. Se coloca el conector en el disco guía. Al inspeccionar el extremo del conector, probablemente se observará una pequeña cantidad de adhesivo en él.
2. Pulimos el conector sobre la lija de una micra, dibujando «ochos» con el disco guía. Seguidamente se limpia el conector con alcohol y se procede a efectuar la misma operación con la lija de 0,3 micras. Ambas lijas deben estar situadas sobre un soporte de goma para evitar que se muevan.
3. Una vez finalizado el pulido, se procede a la comprobación de la fibra mediante el microscopio. El núcleo de la fibra debe aparecer nítido, sin ranuras ni fisuras.

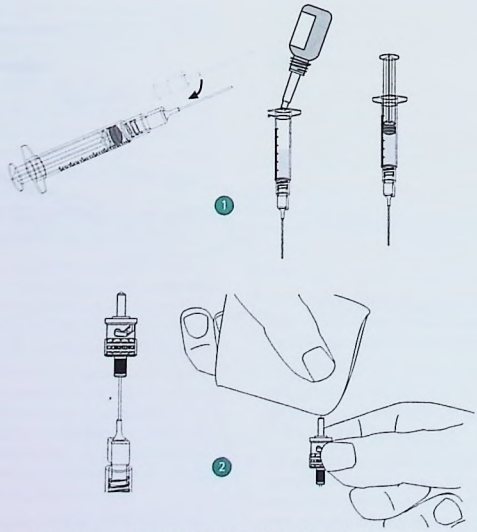
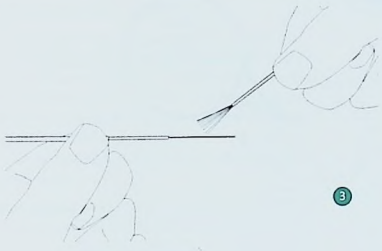
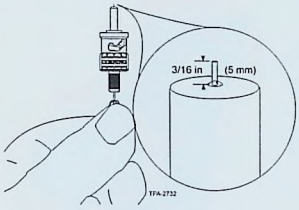
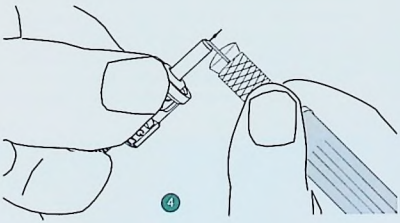


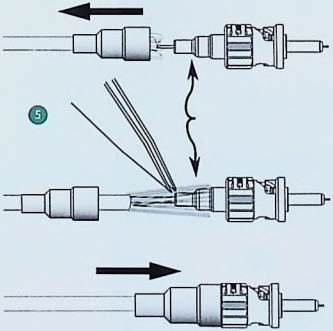
Figura 2.58. Pasos para la colocación de un conector SC en un cable de fibra óptica. Cortesía de Corning Inc. Los números de las ilustraciones corresponden a los pasos indicados en la práctica profesional.

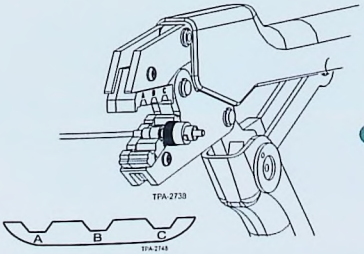
Práctica profesional











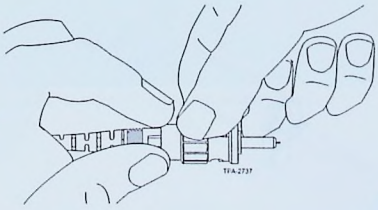


Figura 2.58. (*Continuación*).

Continua ›››

Práctica profesional

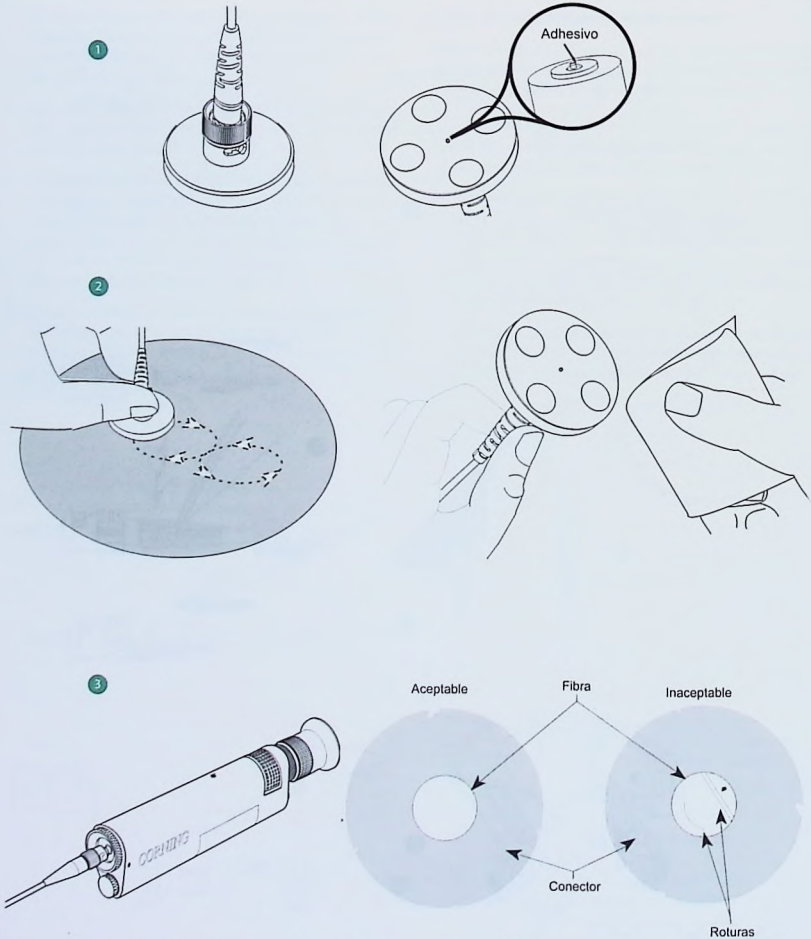


Figura 2.59. Pasos para el pulido y terminación del conector SC. Cortesía de Corning Inc. Los números de las ilustraciones corresponden a los pasos indicados en la práctica profesional.

Práctica profesional

Universidad Tecnica del Norte
BIBLIOTECA
Ibarra Ecuador

2.6. Comprobación del cableado

Una vez conformados los latiguillos de cable de red y efectuadas todas las conexiones en los paneles de conexión, será preciso comprobar el cableado de red. Para ello suelen emplearse unos comprobadores o *tester*. Estos dispositivos se componen de dos unidades, una principal y otra remota, que se sitúan en los extremos del cable que deseamos comprobar. Existen dos tipos de comprobadores:

- El **modelo básico** sirve para comprobar únicamente que todos los cables están bien conectados; para cada uno de los pines del conector, se comprueba si existe continuidad y si la unidad remota del comprobador recibe la señal transmitida por la unidad principal.
- El **certificador de cableado** nos informa no solo de la correcta conexión del cableado, sino que además permite comprobar si la red cumple con la categoría de cableado que se ha instalado; son dispositivos de precio más elevado que los anteriores y cuentan con una serie de funciones adicionales.



Figura 2.61. Certificador de red, con su unidad principal y su unidad remota.





Figura 2.60. Comprobadores de red, con su unidad principal (colocada a la izquierda de cada imagen) y su unidad remota (colocada a la derecha de cada imagen).

Práctica profesional

2.7. Comprobación de la dirección MAC del equipo (Windows XP o Windows 7)

Para saber la dirección MAC de las interfaces de red de nuestro equipo, seguiremos los pasos que se detallan a continuación:

1. Hacemos clic en el botón **Inicio** y en **Todos los programas** > **Accesorios** > **Símbolo del sistema**.

   Si disponemos de Windows 7, haremos clic en el botón **Inicio** y, en el cuadro **Buscar**, escribiremos la palabra **cmd** y pulsaremos Intro. Entre los resultados de búsqueda aparecerá el programa **cmd.exe**, sobre el que haremos clic para abrir el **Símbolo del sistema**.

2. En el *prompt* de Windows tecleamos el comando

   ```
   ipconfig /all
   ```

   que mostrará los datos de configuración relativos a todas las interfaces de red (véase la **Figura 2.62**). Entre ellas veremos las direcciones MAC de todas las interfaces de red de nuestro equipo. En el ejemplo de la figura, como podemos comprobar, existen en el equipo dos direcciones MAC, una de una interfaz Ethernet y otra de una interfaz Wi-Fi.

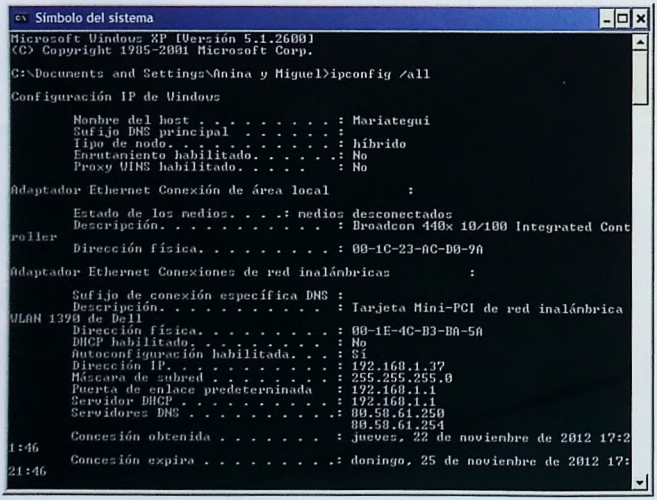


Figura 2.62. Direcciones MAC en las interfaces de red instaladas en el equipo.

Cuestiones

2.1. Ethernet es un estándar cuyas especificaciones se refieren a la:

a) Capa de aplicación de la red.

b) Capa de enlace de datos de la red.

c) Capa física de la red.

d) Capa física de la red y subcapa de control de acceso al medio (MAC).

2.2. Disponemos de una red Ethernet cuya especificación es 1.000 MBaseT. Indica cuál de las siguientes afirmaciones es falsa:

a) La tasa de transferencia de datos es de 1 Gbit/s.

b) La modulación se efectúa en banda base.

c) El medio de transmisión es fibra óptica multimodo.

d) Todas las afirmaciones son ciertas.

2.3. De un cable de red FTP podemos decir que:

a) No existen cables de red con esa denominación. FTP es un protocolo de la capa de aplicación para la transferencia de ficheros.

b) No tiene apantallamiento exterior.

c) Los hilos de cobre están protegidos con una lámina metálica.

d) Posee una malla exterior de cobre que protege el cable de la acción de las interferencias.

2.4. Los conectores que se emplean más habitualmente para cable coaxial son:

a) SC.

b) LC.

c) BNC.

d) SMA.

2.5. La topología física más habitual en una red Ethernet es:

a) Anillo.

b) Estrella.

c) Malla completa.

d) Bus.

2.6. ¿Qué diferencia hay entre un *switch*, un *hub* y un *patch panel*? Señala la afirmación correcta.

a) Cuando se instala un *patch panel* no es necesario instalar un *switch*, puesto que el primero desempeña las funciones del segundo.

b) El *hub* está dotado de una cierta «inteligencia», pero el *switch* no.

c) El *hub* conoce las direcciones físicas de los dispositivos conectados a él, mientras que el *switch* se limita a retransmitir por todos los puertos la señal que recibe por uno de ellos.

d) Todas las afirmaciones son ciertas.

2.7. El algoritmo de encriptación más seguro para una red Wi-Fi es:

a) WEP.

b) WPA.

c) WPA2.

d) SHA2.

2.8. El control de acceso al medio que se utiliza en una red Wi-Fi es:

a) CSMA/CD.

b) CSMA/CA.

c) WPS.

d) Ninguno de los anteriores.

2.9. El «cableado estructurado» significa:

a) Que el cableado se conduce mediante canaletas desde el armario de distribución hasta los puntos de acceso.

b) Que el cableado que se emplea en la instalación es fibra óptica multimodo.

c) Que se diseña el cableado de forma lógica, permitiendo la flexibilidad y escalabilidad del sistema.

d) Que se estructura el cableado siguiendo una topología en bus para dotar a la red de mayor tasa de transferencia de datos.

2.10. El código de colores que se utiliza con más frecuencia para conformar los latiguillos de red viene recogido en el estándar:

a) IEEE 802.11g.

b) TIA/EIA T568B.

c) TIA/EIA-606-A.

d) Ninguno de los anteriores.

Actividades de aplicación

2.11. Identifica el tipo de canalizaciones que se ha empleado en tu aula para conducir el cableado de datos desde el armario de distribución hasta los equipos de los usuarios finales.

2.12. ¿Qué tipo de canalizaciones emplearías en los siguientes casos?

- **a)** Un edificio de oficinas con salas de trabajo diáfanas.
- **b)** Un hospital.
- **c)** Un lugar de trabajo en el que no existe la posibilidad, por razones de presupuesto, de instalar suelo técnico ni falso techo.
- **d)** Elabora un listado con las herramientas y materiales que serán necesarios en cada caso para efectuar la instalación.

2.13. La nomenclatura de la red Ethernet de un edificio es 100BaseTX. Identifica toda la información sobre la red que te proporciona dicha nomenclatura.

2.14. Localiza el armario de distribución de tu aula y, si es posible, el de tu centro educativo. ¿De qué elementos está compuesto?

2.15. Señala las diferencias que existen entre un *switch* y un panel de conexión. El panel, ¿sustituye al *switch*? ¿Cuál es su función?

2.16. ¿En qué se diferencian los medios guiados y los no guiados? ¿Cuáles son las ventajas del uso de unos y otros en las redes de datos? ¿Qué medios de transmisión emplearías en cada uno de los siguientes casos?

- **a)** Red de datos de una pequeña oficina.
- **b)** Cableado de distribución para un campus universitario.
- **c)** Servicio de acceso a Internet en un aeropuerto, para que los pasajeros puedan navegar por la web o comprobar su correo electrónico.
- **d)** Conexión a Internet en una zona rural de difícil acceso.

2.17. Efectúa las siguientes prácticas siguiendo los procedimientos que se han detallado en la sección de **Práctica profesional** de la Unidad. Para cada una de ellas, indica la secuencia de pasos llevada a cabo y las herramientas necesarias para efectuar la práctica:

- **a)** Instalación de un conector RJ45 en un latiguillo UTP.
- **b)** Conexiones del cable de red a un panel de conexión con rosetas integradas.
- **c)** Etiquetado del *patch panel*.
- **d)** Instalación de un conector SC en un cable de fibra óptica.

2.18. ¿Por qué es tan importante la ventilación de los armarios de distribución? Indica todas las «buenas prácticas» que debes seguir en la instalación de uno de estos armarios para asegurar la correcta ventilación de los equipos.

2.19. ¿Qué es la dirección MAC en un adaptador de red? ¿Cómo se comprueba? ¿Para qué sirve?

2.20. Explica los problemas de seguridad que existen en una red Wi-Fi y los mecanismos que existen para hacer que la red sea más segura.

2.21. Comprueba el etiquetado de los elementos de la red de datos existente en tu centro educativo. ¿Qué información proporciona? ¿Te parece adecuado? ¿Introducirías alguna modificación o mejora en él?

2.22. Con el comprobador o certificador de red del que dispongas en tu centro educativo, efectúa una serie de pruebas con el cableado de par trenzado y las conexiones que hayas configurado en la Actividad de aplicación 2.17. Comprueba que exista continuidad en todas las conexiones. Si dispones de un certificador de red, asegúrate de que la red cumple con la categoría de cableado que hayas instalado.



3

Redes de telefonía

La telefonía es una tecnología con casi 140 años de antigüedad. Desde los primitivos teléfonos de manivela hasta los modernos sistemas de telefonía, esta tecnología ha experimentado una evolución espectacular. La red telefónica conmutada, cuyo funcionamiento estudiaremos en esta Unidad, ha constituido la médula espinal de la transmisión de información en nuestra sociedad. En la actualidad, comparte protagonismo con otras tecnologías, como la telefonía móvil, y el par de cobre tradicional cede parte de su importancia a favor de la fibra óptica. En los sistemas privados de telefonía, que actúan como una red conmutada en el interior de una empresa, ha irrumpido con fuerza un nuevo actor: los sistemas de voz sobre IP, que estudiaremos en detalle en la Unidad 5.

Contenidos

3.1. El circuito telefónico: historia y características
3.2. La red conmutada
3.3. Señalización y transmisión de voz en la red telefónica
3.4. La red de abonados y su infraestructura física
3.5. Telefonía analógica y digital
3.6. Redes de telefonía móvil
3.7. Sistemas privados de telefonía (PBX)
3.8. Medida del tráfico telefónico

Objetivos

- Conocer e identificar los elementos básicos que componen el circuito telefónico, el espectro de frecuencias en el que se transmite la voz en la telefonía convencional y el origen histórico de la telefonía.
- Comprender la necesidad de que en la red telefónica exista un elemento central de conmutación y la estructura jerárquica de dicho sistema, identificando los niveles de centrales que lo componen.
- Conocer las fases de las que consta una conversación telefónica, identificando el papel de las señales intercambiadas y la evolución que ha experimentado el sistema de señalización.
- Diferenciar las partes que componen la red de abonados en un sistema de telefonía, prestando especial atención a las Infraestructuras Comunes de Telecomunicaciones situadas en el interior de los edificios.
- Identificar las características diferenciadoras de la telefonía analógica y digital. Conocer en qué consiste la modulación digital (MIC) y la RDSI. Estudiar el funcionamiento de los sistemas de transmisión de datos mediante DSL.
- Comprender el funcionamiento de las redes de telefonía móvil, tanto para las transmisiones de voz como de datos.
- Conocer las características y funcionalidades de los sistemas privados de telefonía.
- Adquirir conceptos básicos acerca de la medida del tráfico telefónico en la red.

3.1. El circuito telefónico: historia y características

Para comprender el funcionamiento del circuito telefónico básico, supongamos que unimos dos teléfonos entre sí mediante un cable, un conductor eléctrico. Este circuito telefónico permitiría la comunicación de voz entre ambos terminales y estaría compuesto de los siguientes elementos:

- El **micrófono** convierte la información que deseamos transmitir (la voz) en señales eléctricas. La intensidad o energía de estas señales eléctricas varía proporcionalmente al volumen de la señal sonora.
- La **línea de transmisión** está formada por dos conductores eléctricos que conectan ambos terminales.
- Puesto que las características eléctricas del circuito del terminal telefónico y de la línea de transmisión son diferentes, se emplea entre ellos un **transformador**.
- La **batería** es la encargada de proporcionar la energía necesaria para la transmisión de la señal eléctrica entre ambos terminales.
- El **auricular receptor** convierte la señal eléctrica de nuevo en una señal sonora a un nivel audible por el receptor.

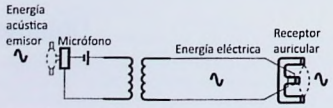


Figura 3.1. Circuito telefónico básico.

El circuito telefónico que acabamos de describir permite entender los fundamentos de la transmisión telefónica y, al mismo tiempo, ilustrar el funcionamiento del primer modelo de teléfono, patentado por Graham Bell en 1876. Veamos cómo surgió históricamente la telefonía.

3.1.1. Historia y evolución de los sistemas telefónicos

Desde comienzos del siglo XIX se desarrollaron sistemas de telecomunicaciones (o comunicaciones a distancia) basados en el *telégrafo eléctrico*. La telegrafía significa literalmente «escritura a distancia». Los primeros telégrafos empleaban varias líneas eléctricas para representar los caracteres del alfabeto, pero pronto se desarrollaron sistemas que codificaban la información que debía transmitirse: el sistema de codificación más empleado fue el desarrollado en 1837 por Samuel Morse y Alfred Vail. El telégrafo, en combinación con el *código Morse*, se convirtió en el principal sistema de telecomunicaciones durante buena parte del siglo XIX.

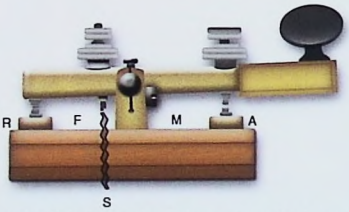


Figura 3.2. Pulsador para el envío de mensajes codificados en Morse a través del telégrafo.

Desde mediados del siglo XIX, sin embargo, se comenzó a experimentar con la transmisión de la voz a través de un circuito eléctrico. Como ocurre con otros inventos que han marcado época en la evolución de la tecnología, es difícil asociar su «invención» a una sola persona: figuras como los inventores italianos Innocenzo Manzetti y Antonio Meucci, o el estadounidense Thomas Edison efectuaron investigaciones y desarrollos al respecto de forma independiente. Pero fue el científico e ingeniero Alexander Graham Bell (1847-1922) quien logró construir el primer dispositivo capaz de transmitir la voz humana con calidad suficiente, obteniendo así (en 1876) la patente del nuevo invento: el teléfono.



Figura 3.3. Teléfono de comienzos del siglo XX, equipado con una manivela para accionar el timbre del interlocutor.



Figura 3.4. Teléfono de mediados del siglo xx, equipado con un disco de marcación.

El circuito telefónico ideado por Bell era similar al que hemos mostrado en la **Figura 3.1**, con la salvedad de que el micrófono del emisor y el altavoz del receptor eran idénticos y estaban formados por un simple diafragma metálico, con un núcleo de hierro y una bobina arrollada alrededor de él. Las ondas sonoras hacían vibrar la membrana, modificando con ello el flujo magnético de la bobina. Así se producían variaciones en la corriente eléctrica transmitida, que llegaban al dispositivo receptor, en el que se producía el proceso inverso.

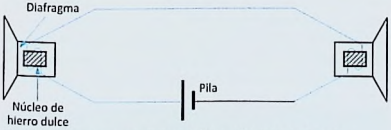


Figura 3.5. Esquema del circuito telefónico ideado por A. G. Bell.

El sistema construido por Bell presentaba, sin embargo, una limitación importante: ¿cómo podía el emisor indicar que quería iniciar una llamada telefónica? Le faltaba, en otras palabras, un mecanismo de *señalización* de la llamada. En los primeros teléfonos, este mecanismo lo proporcionaba la magneto, una espira acoplada a una manivela que, al ser girada, generaba una corriente alterna que hacía sonar un timbre en el lado del receptor. Por eso, en las películas ambientadas en la época, cuando una persona quiere iniciar una llamada hace girar la manivela del teléfono para comunicarse con la *central de conmutación*.

3.1.2. El sonido en la transmisión telefónica

Aunque en la actualidad los sistemas de telefonía se emplean para la transmisión de diversos tipos de informaciones, su cometido principal es la transmisión del sonido y, específicamente, de la voz humana. En este Apartado estudiaremos las cualidades principales de esta clase de sonidos.

Como sabemos, el sonido está formado por ondas senoidales que se transmiten a través de un medio físico, ya sea gaseoso (como el aire), líquido o sólido. El sonido puede ser complejo o puro: en el primer caso, está compuesto por varias frecuencias; en el segundo, por una sola. Si representamos las ondas sonoras en un diagrama Energía-Frecuencia, obtenemos las formas de la **Figura 3.6**.

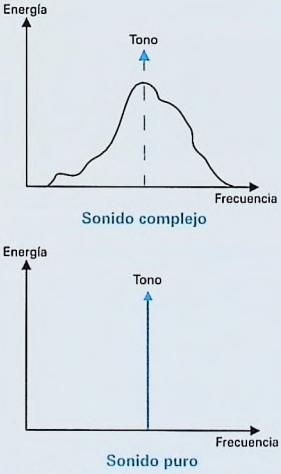


Figura 3.6. Diagrama Energía-Frecuencia para un sonido complejo y un sonido puro.

Las características principales de un sonido son su intensidad, su tono y su timbre. El área de la gráfica superior en la **Figura 3.6** corresponde a la *intensidad* del sonido; la frecuencia máxima es el *tono* del mismo, y la forma de la curva determina su *timbre*.

Las voces humanas presentan frecuencias comprendidas entre los 100 Hz y los 9500 Hz, aunque el espectro de audición del oído humano es mayor y se sitúa entre los 20 y los 20.000 Hz. (véase la **Figura 3.7**). Se ha comprobado experimentalmente que, para lograr una buena *inteligibilidad* en una conversación telefónica, es suficiente transmitirla a través del ancho de banda comprendido entre los 300 Hz y los 3400 Hz.

¿Sabías que...?

La percepción de nuestros sentidos no responde a los estímulos externos de manera lineal, sino *logarítmica*: cuando subimos ligeramente una persiana completamente cerrada y entra la luz del sol, experimentamos una variación muy grande en nuestra percepción de la luminosidad; en cambio, si la persiana ya está parcialmente subida y la abrimos más, la percepción de la variación de luminosidad de la habitación será mucho menor. Por esta razón la medición de la intensidad del sonido se efectúa sobre escalas logarítmicas; estas, además, hacen más sencillo trabajar con magnitudes de valores muy distintos, matemáticamente, las operaciones de producto, división y potencia se simplifican en gran medida.

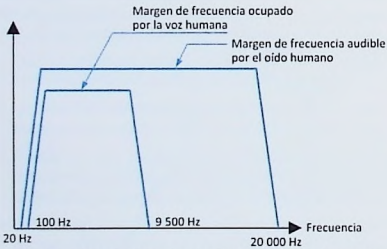


Figura 3.7. Espectro de frecuencias audible por el oído humano y ocupado por la voz.

3.2. La red conmutada

En los primeros modelos de teléfono, el emisor de la llamada elegía con quién deseaba comunicarse insertando una clavija en la posición correspondiente y luego accionando la manivela para hacer sonar el timbre en el otro extremo de la línea. En este modelo de red telefónica, todos los abonados estaban unidos entre sí, formando una estructura en forma de *malla completa* (recuerda las *topologías de red* que estudiamos en la Unidad 1), como la de la **Figura 3.8**.

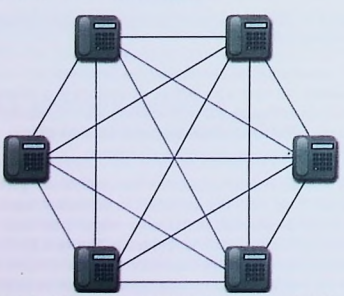


Figura 3.8. Red telefónica con una topología en forma de malla completa.

En una estructura como esta, cada enlace entre dispositivos tiene un canal propio, *dedicado*. El número de enlaces necesarios, sin embargo, sigue la siguiente ley matemática:

$$\text{Número de enlace} = \frac{N \times (N-1)}{2}$$

De este modo, el número de enlaces aumenta con el cuadrado del número de abonados o usuarios de la red telefónica (el número de terminales de la misma) y, por tanto, es inviable en la práctica (una red de 6 terminales requiere 15 enlaces; una de 10, 45 enlaces, y así sucesivamente).

Además de la complejidad y el coste de una red de este tipo, la estructura en malla completa es sumamente ineficaz. En el ejemplo de la red de 10 terminales, aunque todos los terminales telefónicos estén ocupados las 24 horas del día, habrá siempre libres 36 canales de los 45, es decir, un 80 % de la red estará desperdiciada.

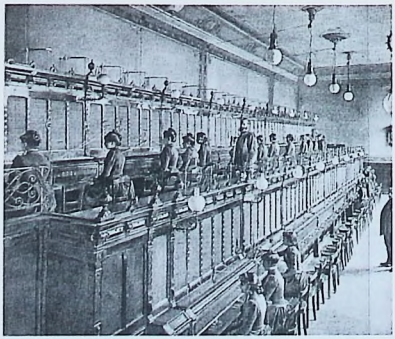


Figura 3.9. Central de conmutación manual de finales del siglo XIX.

¿Cómo se puede garantizar entonces que, en una red de teléfonos, se puedan comunicar entre sí dos terminales cualesquiera? La solución consiste en colocar en

la red un elemento central de *conmutación*, que ponga en contacto en cada momento a los usuarios que realmente desean comunicarse. Cada terminal de la red se conecta a dicha central de conmutación a través del *par de abonado* o la *línea de abonado*, denominada también en ocasiones *bucle de abonado*.

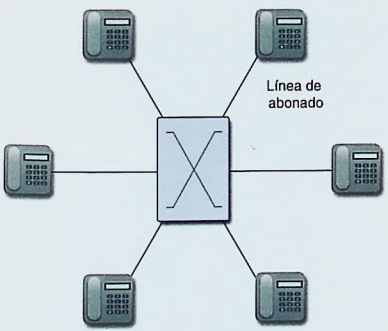


Figura 3.10. Red telefónica con un elemento central de conmutación.

El sistema de conmutación, en definitiva, se encarga de establecer un camino, dentro de la matriz de conmutación, entre la entrada y la salida. Existen dos clases de sistemas, que en las centrales reales se dan a menudo en combinación:

- **Conmutación espacial**. Consiste en el establecimiento de un camino físico entre la entrada y la salida, que se mantiene durante todo el tiempo que dura la conmutación. Es el tipo de sistema más adecuado para la conmutación de las señales analógicas.

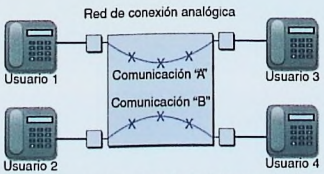


Figura 3.11. Esquema de funcionamiento de la conmutación espacial.

- **Conmutación temporal**. Este tipo de conmutación se emplea en la transmisión de señales digitales. Las señales analógicas se muestrean (volveremos sobre esta cuestión en el Apartado 3.5.2) y se envían en trozos de longitud fija, secuencialmente, a través del mismo canal físico de comunicaciones. En el extremo opuesto del canal se vuelven a separar las tramas y se dirigen a sus respectivos destinatarios.

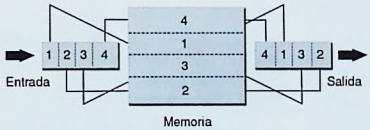


Figura 3.12. Esquema de la conmutación temporal.

> **¿Sabías que...?**
>
> En inglés, se suele hablar de *Space Division Multiplexing* para referirse a la conmutación espacial y de *Time Division Multiplexing* para referirse a la conmutación temporal.

3.2.1. Jerarquía y sistemas de conmutación

En la **Figura 3.9** se mostró el aspecto de una central de *conmutación manual*, en la que el contacto eléctrico entre el emisor y el receptor de la llamada se establece mediante la conexión de unas clavijas en los conectores correspondientes a ambos abonados. En este tipo de sistemas, cuando un abonado quería llamar a otro, primero tenía que ponerse en contacto con la central de conmutación e indicarle el número con el que quería contactar.

Los sistemas de conmutación manual fueron progresivamente reemplazados desde comienzos del siglo XX por sistemas de *conmutación electromecánica*. El disco de marcado del teléfono (como el de la **Figura 3.4**) generaba unos pulsos eléctricos proporcionales al número marcado, haciendo que el conmutador se desplazase, por medio de unos electroimanes, hasta efectuar el contacto con el bucle de abonado correspondiente. En un principio, las centrales de conmutación electromecánica se empleaban principalmente a nivel local; para la comunicación interprovincial e internacional se recurría a centrales de conmutación manuales.

En la actualidad, tanto la conmutación manual como la electromecánica están en desuso; en su lugar se emplea la *conmutación electrónica*. El contacto entre los bucles de abonado se emplea a través de

¿Sabías que...?

Uno de los sistemas de conmutación electromecánica más empleados fue el conmutador Strowger, cuyo funcionamiento se ilustra en la **Figura 3.13**: los impulsos eléctricos del número marcado provocan, a través de un electroimán, que el contacto móvil se mueva en el eje vertical hasta el nivel de contactos deseado. A continuación se moverá circularmente hasta un contacto en particular, correspondiente a una determinada línea telefónica.

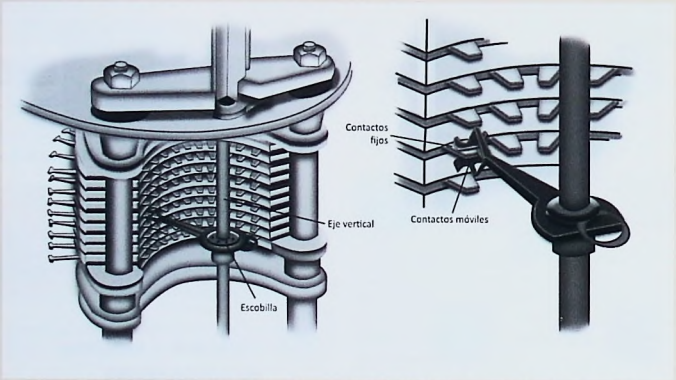


Figura 3.13. Funcionamiento del conmutador electromecánico Strowger. El contacto móvil se mueve en dirección vertical y circularmente hasta elegir el contacto fijo con el que se desea establecer la comunicación.



Figura 3.14. Banco de conmutadores electromecánicos Strowger. Cortesía del *Museum of Communications* (Seattle, Washington (EE.UU).

dispositivos electrónicos, mucho más fiables, rápidos y baratos.

La red telefónica es una red conmutada a nivel mundial y estructurada jerárquicamente, en la que —debido al elevadísimo número de abonados a redes distintas— existe una gran cantidad de centrales de conmutación conectadas entre sí por *niveles*: centrales locales, primarias, secundarias y terciarias.

¿Sabías que...?

En un principio, el desarrollo de la red telefónica estuvo impulsado por la iniciativa privada, pero pronto se convirtió en una red pública —en régimen de monopolio en la mayoría de los países—. Por eso se la denomina a veces Red Telefónica Pública Conmutada; también verás con frecuencia sus siglas en inglés, PSTN (*Public Switched Telehone Network*).

¿Sabías que...?

En España, en 1998 se establece el Plan Nacional de Numeración Telefónica actualmente en vigor. En él se establece que los números de abonado deben constar de nueve dígitos, siendo obligatorio incluir en el número de abonado el código identificador de la provincia. También se establece que los números de teléfonos móviles deben comenzar por un «6» o un «7» y se reservan los números de abonado que comiencen por «8» para *servicios vocales nómadas* (comunicaciones vocales a través de Internet, normalmente como segundas líneas).

Puedes consultar toda la información al respecto en la página web del Ministerio de Industria, Turismo y Comercio (http://www.minetur.gob.es).



Figura 3.15. Regletas de conexión en una central de conmutación telefónica.

- En el nivel inferior están situadas las **centrales locales**; su misión es la de interconectar a los abonados o usuarios finales de la red. En el interior de la central se sitúa el *equipo de conmutación*, que se encarga de encaminar las llamadas de los terminales desde su origen hasta su destino siguiendo diversos criterios.

  La *red de abonados* está formada por los elementos de conexión entre los equipos de abonado y la central local a la que pertenecen, recordemos que cada abonado tiene asignado un circuito único. La red formada por la central local, el cableado, las canalizaciones, las cajas de conexión y los terminales constituye la *red de abonados* o *red local*, y cubre un área denominada área local. Trataremos esta red más en detalle en el Apartado 3.4.

- Inmediatamente por encima encontramos las **centrales primarias**, que interconectan las centrales locales; un conjunto de centrales locales interconectadas por una central primaria forman un área de central primaria. Las centrales locales se conectan a las primarias a través de *secciones primarias*, formadas por un conjunto de enlaces constituidos por circuitos destinados a establecer una conmutación telefónica.

  El cometido fundamental de la central primaria es establecer llamadas entre abonados situados fuera de ella. A estas llamadas se las denomina *llamadas de tránsito*.

- Las **centrales secundarias** son las encargadas de conectar entre sí las centrales primarias a través de secciones secundarias; el conjunto de centrales primarias conectadas a través de una central secundaria forma una *red secundaria*. Esta red se encarga de cursar llamadas de tránsito.

- Las centrales secundarias se unen entre sí a través de secciones terciarias a **centrales terciarias** o nodales. Estas centrales se conectan directamente entre sí, formando una red en forma de malla. Las secciones cuaternarias, que forman esta malla, deben ser capaces de transportar miles de conversaciones simultáneamente, y por tanto requieren un elevado ancho de banda.

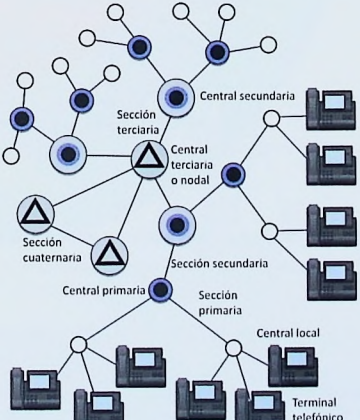


Figura 3.16. Estructura jerárquica de la red telefónica. Los terminales se conectan a las centrales locales; estas se conectan entre sí a las centrales primarias a través de secciones primarias; a su vez, las primarias se conectan a las secundarias y estas a las terciarias, que se unen a través de una estructura de malla.

Recuerda que...

La **sección** es un canal de comunicaciones que une entre sí dos centrales de conmutación. Las centrales locales se conectan a las primarias a través de la sección primaria; las primarias se conectan a las secundarias a través de la sección secundaria; las secundarias se conectan a las terciarias a través de la sección terciaria. Existen, por último, secciones cuaternarias que conectan entre sí las centrales terciarias.

Fijémonos en la **Figura 3.17**, imaginemos que es preciso conectar el terminal telefónico A con el terminal E. La llamada se establecerá siguiendo un *camino único* o *ruta final* a través de la estructura jerárquica de redes de conmutación, hasta llegar a su destino definitivo. En el caso de la comunicación A-E, deberá establecerse la siguiente ruta:

A-CL1-CP1-CS1-CT1-CS2-CP4-CL7-**E**

En el caso de que sea necesario conectar con un terminal ubicado en otra área de central terciaria, la ruta final deberá atravesar también una sección cuaternaria para que la llamada pueda dirigirse a la central terciaria que corresponda y llegar así a su destino.

En ocasiones, para mejorar la eficiencia de la red telefónica, se conectan entre sí mediante *secciones directas* centrales que, atendiendo a la estructura jerárquica de la red, no deberían estar unidas. Se constituye de ese modo la llamada *red complementaria*. El encaminamiento mediante rutas directas es más corto que el encaminamiento mediante rutas finales. Las secciones directas se pueden establecer entre centrales con el mismo rango en la jerarquía de la red o entre centrales con rango diferente, *siempre y cuando exista una diferencia no superior a un nivel en las centrales enlazadas*.

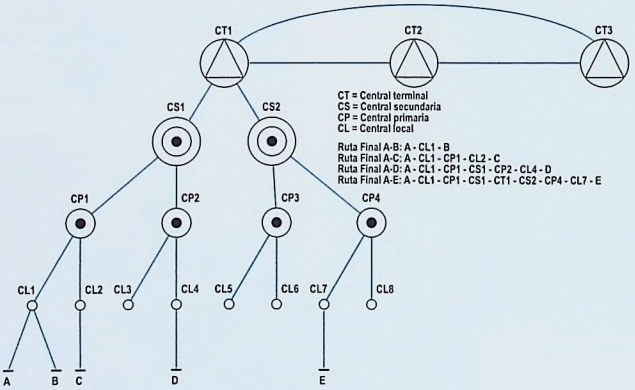


Figura 3.17. Arquitectura de la red telefónica y rutas entre los diversos abonados.

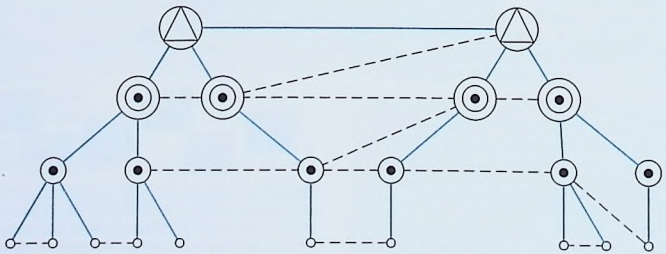


Figura 3.18. Ejemplos de secciones directas, que en la figura se representan mediante líneas de trazos.

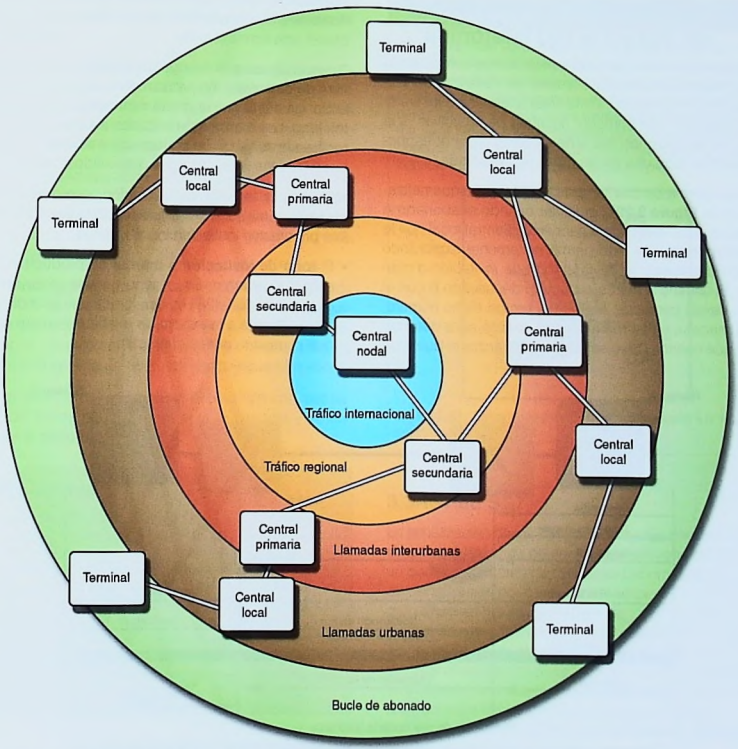


Figura 3.19. Jerarquía del sistema telefónico, estructurado en varios anillos a los que corresponden diversas categorías de centrales de conmutación.

¿Sabías que...?

Con la liberalización del mercado telefónico en España, los usuarios de la red telefónica pueden contratar los servicios de telefonía con diversas operadoras presentes en el mercado. En la mayoría de los casos, estas operadoras utilizan el bucle de abonado de Telefónica (o el operador dominante que corresponda en cada caso) en régimen de alquiler. En la central de conmutación, el operador suele instalar sus equipos en una sala del operador dominante habilitada a tal efecto. El uso de la red de distribución de Telefónica es la solución que más se ha extendido en España.

Los operadores privados también pueden disponer de su propia red de distribución. En los edificios de nueva planta, cada operador instala en el Registro Interior de Telecomunicaciones Inferior (RITI) unas regletas de entrada que se conectarán a los pares de abonado que contraten sus servicios de telefonía o acceso a Internet con dicho operador.

3.3. Señalización y transmisión de voz en la red telefónica

El proceso de una llamada telefónica se compone de dos fases diferenciadas: la fase de señalización y la fase de conversación. En la línea telefónica está siempre presente una corriente continua de 48 voltios, a la que se superponen las señales eléctricas correspondientes a cada una de las fases de la llamada.

La secuencia de una llamada telefónica (esquematizada en la **Figura 3.20**) comienza cuando el abonado A *descuelga* el teléfono. Al hacerlo, la central local que le corresponde, que está permanentemente explorando todas sus líneas, le envía el tono de *invitación a marcar*. El usuario A marca el número del usuario B con el que desea contactar. La central recibe dicho número, lo almacena en su memoria y lo analiza para determinar qué camino debe seguir para alcanzar el bucle de abonado. Una vez establecida la ruta, envía el tono de llamada a B, indicándole que un usuario quiere establecer una comunicación.

Cuando el usuario descuelga el teléfono, se inicia la fase de conversación propiamente dicha; esta fase se prolonga hasta que uno de los interlocutores cuelga el teléfono. Las centrales implicadas en la comunicación reciben la señal de fin de llamada y esta se libera: los equipos y las líneas quedan disponibles nuevamente.

Antes de la fase de conversación, como vemos, se transmiten una serie de *señales* o *tonos de información*. Los principales tonos son los siguientes:

- El **tono de invitación a marcar** se produce al descolgar el aparato. Es un tono continuo, de una frecuencia de 400-425 Hz, que indica que la central del abonado está a la espera de recibir el número con el que el usuario desea contactar.

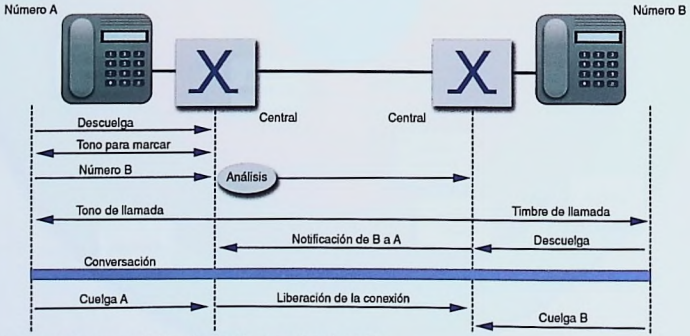


Figura 3.20. Procedimiento para el inicio y finalización de una llamada telefónica.

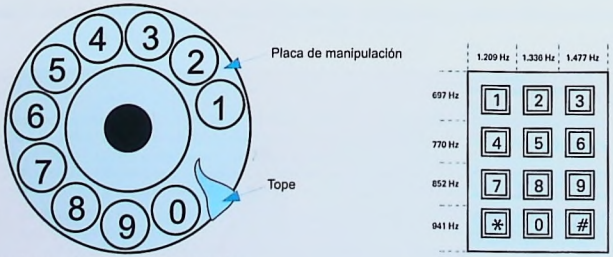


Figura 3.21. Disco de marcación y teclado multifrecuencia.

- Cuando el usuario A marca el número de abonado del usuario B, por la línea se envían los **impulsos de marcación**.

  Hasta hace unas décadas, los teléfonos estaban provistos de un *disco de marcación*. En su retorno, este disco provocaba aperturas y cierres de un bucle eléctrico, produciendo un número de impulsos (*impulsos decádicos*) proporcional al dígito marcado.

  En los *teclados multifrecuencia*, por el contrario, los impulsos de marcación se componen de dos señales de diferentes frecuencias. En este tipo de teclados, la marcación y la conmutación son mucho más rápidas.

- El **tono de llamada** es un conjunto o tren de tonos de 425 Hz, de un segundo de duración y espaciados cinco segundos, que indican que se ha establecido la conexión con el terminal del interlocutor y se está a la espera de que este descuelgue el teléfono.

- Si el terminal del usuario B está ocupado con otra llamada, no es posible establecer la llamada y se enviará el **tono de ocupado**.

¿Sabías que...?

Para la identificación de llamadas en la red telefónica se emplean diversos procedimientos. Uno de los más empleados en Europa sobre líneas analógicas es el denominado ETSI FSK, que envía la información de llamada mediante una trama con una modulación en frecuencia (*modulación FSK*) entre el primer y el segundo tono de la llamada; por eso en el terminal telefónico es necesario esperar para que se muestre el número que llama, siempre y cuando en el otro extremo de la comunicación no se haya restringido el envío de dicha información.

Actividad propuesta 3.1

Para comprobar las señales de la línea telefónica, se empleará una de las centralitas analógicas de las que dispongamos en nuestro centro educativo. Emplearemos un latiguillo telefónico con uno de sus extremos libres y conectaremos los hilos a una roseta, siguiendo el esquema de la **Figura 3.23**. Al conector RJ11 de la roseta se conecta un terminal telefónico y a los tornillos L1 y L2 se conectan los terminales de un osciloscopio.

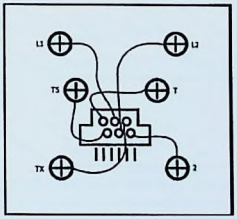


Figura 3.23. Conexiones del cableado de la centralita a la roseta telefónica.

3.3.1. Red SS7

La señalización de las llamadas ha evolucionado progresivamente, pasando de ser una simple serie de tonos a un completo sistema de mensajes denominado *Sistema de Señalización por canal común número 7* o *SS7* (*Common Channel Signalling System No 7*). En un primer momento, estas señales transmitían solamente el número de abonado del destinatario; hoy en día, pueden incluir muchas otras informaciones, como datos de usuario, de facturación, de enrutamiento de la llamada o de compatibilidad entre estructuras de abonado diferentes.

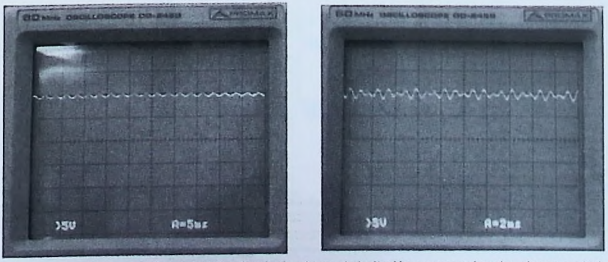


Figura 3.22. Dos ejemplos de señales en la línea telefónica: izquierda, el tono de invitación a marcar; derecha, el tono equivalente al número tres generado por un terminal equipado con un teclado multifrecuencia.

En 1976, AT&T introdujo un sistema de señalización en el que la información para el establecimiento y el fin de llamada estaba formada por mensajes en lugar de tonos. El mensaje permitía establecer un circuito virtual entre ambos terminales a través de la red. Además, los mensajes de señalización viajaban independientemente de la conversación telefónica. Este sistema evolucionó hacia el SS7, dotado de una estructura en capas, basado en tecnología digital y capaz de soportar tráfico de voz y datos.

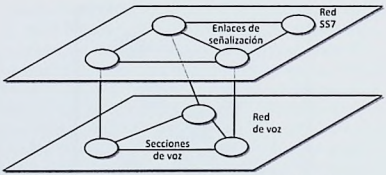


Figura 3.24. Red de señalización SS7, situada en una capa independiente de la red de voz.

La red SS7 es una red de paquetes compuesta por tres tipos de nodos de comunicación o señalización:

- Los **puntos de conmutación de servicio** (*Service Switching Points*) son los puntos en los que se origina la información que se transmite a través de la red de señalización.
- Los **puntos de transferencia de señal** (*Signal Transfer Points*) son las centrales de conmutación de la red SS7.
- Los **puntos de control de servicio** (*Service Control Points*) son las bases de datos de la red. En estos puntos de control se almacena la información de señalización y los mensajes transmitidos.

Entre estos puntos se establecen diversos tipos de enlaces (A, B, C, E y F), como observamos en la **Figura 3.25**. La red emplea canales distintos a los que se emplean para transmitir las llamadas, y los usuarios no tienen acceso a estos canales.

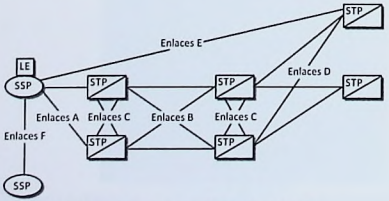


Figura 3.25. Estructura y componentes de la red SS7.

Actividad resuelta 3.2. ¿En qué consiste la *señalización* en la red telefónica?

Solución. La *señalización* es la información que se envía a través de la red sobre el estado de la misma, sobre la situación del interlocutor, la intención del que llama de entablar una conversación, etcétera. En definitiva, es la información que rodea la fase de conversación propiamente dicha. En los sistemas primitivos, consistía simplemente en la señal de llamada, generada mediante la magneto, accionada por la manivela. En la red telefónica pública moderna, existe todo un sistema paralelo destinado a la señalización, conocido como SS7.

3.4. La red de abonados y su infraestructura física

La *red de abonados* está formada por el conjunto de elementos que hacen posible la conexión eléctrica entre los equipos del abonado y la central local a la que pertenecen. Este tramo de la red es el más costoso de implantar y mantener, puesto que existen tantas líneas de abonado como abonados a la red telefónica.

La red de abonado se divide en varios tramos, desde el repartidor principal de la central hasta el terminal del usuario. Veamos las características principales de cada uno de ellos.

3.4.1. Repartidor de abonados

El repartidor de abonados garantiza la conexión entre la planta exterior de la central y el equipo de conmutación. Su función es posibilitar que cualquier par de la red exterior pueda ser conectado con los equipos de conmutación. Los cables llegan agrupados en una manguera de cables denominada *cable terminal* (véase la **Figura 3.26**). Los pares de este cable terminal se reparten en una serie de regletas verticales; cada regleta corresponde a un grupo de abonados. Desde estas regletas se tienden *hilos puente* a unas *regletas horizontales* conectadas directamente con la central de conmutación.

3.4.2. Cables de alimentación

Los cables de los repartidores de abonado se agrupan formando la *red de cables de alimentación*, que parten de la *galería de cables* hasta los *cables laterales*. Los cables de alimentación se distribuyen a través de canalizaciones visitables, para facilitar las reparaciones. Cada cierta distancia se preparan unas arquetas o locales subterráneos denominados *cámaras de registro*, donde se empalman los cables con los laterales y se instalan bobinas de carga para equilibrar las impedancias.

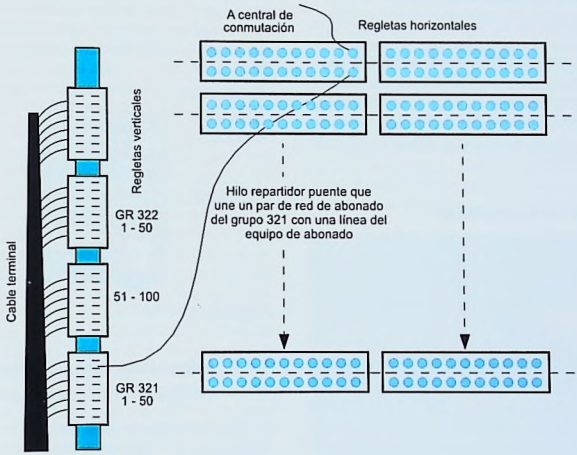


Figura 3.26. Repartidor principal de abonado y ejemplo de conexión de un abonado del grupo de abonados GR 321 (Regleta 1-50) con la central de conmutación a través de un hilo puente.

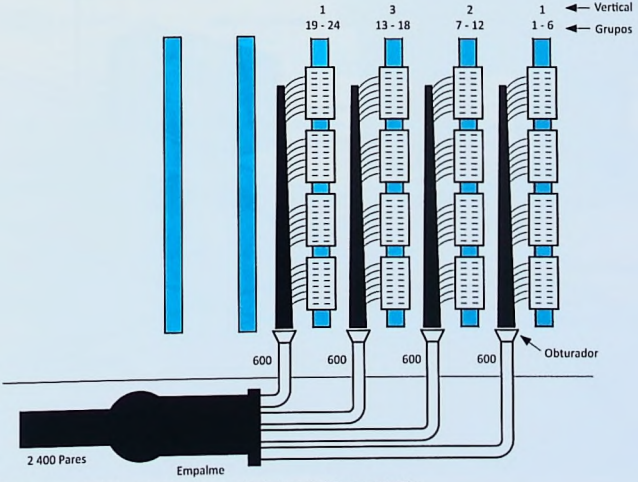


Figura 3.27. Repartidores principales y su empalme a partir de la central de conmutación.

3.4.3. Cables de distribución

La red de alimentación se ramifica mediante los cables laterales, que se distribuyen acoplados a las fachadas de los edificios, por el interior de los mismos o mediante postes (en zonas periurbanas y rurales). A este tramo de la red se le denomina *red de distribución*. Mediante *cajas terminales* o *cajas de conexión*, estos cables se ramifican en varias *líneas de acometida*, una por abonado.

3.4.4. Línea de acometida

La línea de acometida está formada por los cables que van desde la caja terminal o caja de conexión hasta el Punto de Terminación de Red (PTR), Punto de Conexión de Red (PCR) o Base de Acceso Terminal (BAT) del usuario.

3.4.5. Línea interior de abonado

La instalación de abonado está constituida por un par de hilos de cobre, de 0,5 mm de sección. En el PTR comienza la instalación interior de abonado, delimitando este elemento la parte de la instalación de la que es responsable la compañía telefónica y la parte que es responsabilidad del propio abonado. Por último, el elemento en el que se interconectan los equipos telefónicos en el domicilio del abonado se denomina *roseta*.

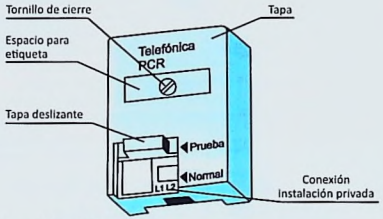


Figura 3.28. Modelo de PCR.

3.4.6. Infraestructuras Comunes de Telecomunicaciones

En 2011 se publica el Real Decreto que regula las Infraestructuras Comunes de Telecomunicaciones, con

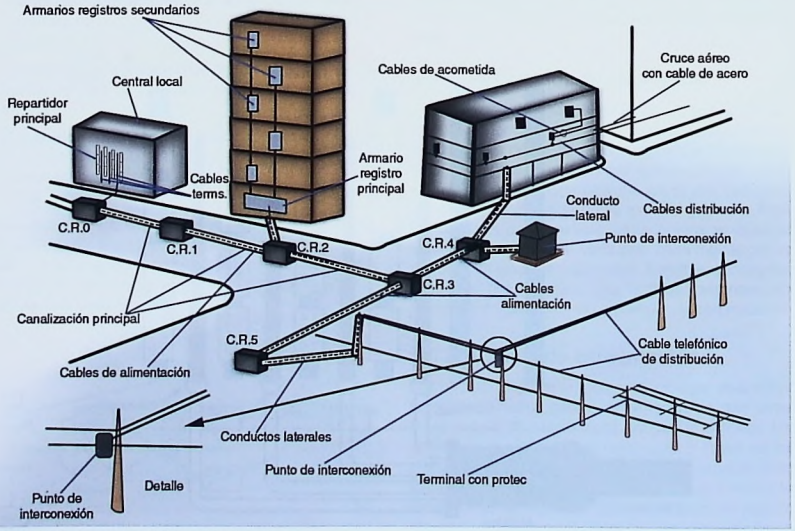


Figura 3.29. Esquema general de la red de abonados.

el objetivo de adaptar la normativa a la extensión de los servicios de telecomunicaciones y a los nuevos operadores presentes en el mercado, tras su liberalización. En él se define un nuevo concepto de acometida interior, sensiblemente distinto al que regía hasta entonces, que sigue estando presente en los edificios construidos antes de 1998 (año en el que se publicó el primer decreto que regulaba las ICT).

Las Infraestructuras Comunes de Telecomunicaciones (ICT) son las redes físicas, los elementos y los equipos de comunicaciones que permiten al abonado de un inmueble acceder a los servicios de telecomunicaciones que ofrecen diversas operadoras de telefonía. Los edificios destinados a viviendas y a locales comerciales u oficinas deben disponer de una canalización para las infraestructuras de telecomunicaciones totalmente independiente de la canalización destinada a la instalación eléctrica. En la **Figura 3.31**, a modo de ejemplo, vemos un esquema de la *canalización ICT* de un edificio de tres plantas y dos viviendas por planta. En la **Figura 3.32** se observa la planta de dicho edificio, sobre la que se han dibujado las instalaciones interiores de telecomunicaciones de ambas viviendas.

- La **canalización de enlace** transcurre desde la arqueta de entrada al edificio hasta el RITI (Registro Interior de Telecomunicaciones Inferior). Por ella transcurre la **red de alimentación**.
- La **canalización principal** está formada por varios tubos de 50 mm de diámetro que ascienden por el edificio, del RITI al RITS (Registro Interior de Telecomunicaciones Superior). Por la canalización principal transcurre la **red de distribución**.
- En el **Registro Interior de Telecomunicaciones Inferior** se alojan los dispositivos necesarios para la distribución de pares de telefonía. Dentro del RITI, el **punto de interconexión** forma el enlace de la red de alimentación de cada operador con la red de distribución del edificio.
- En el **Registro Interior de Telecomunicaciones Superior** se alojan normalmente los dispositivos para distribuir las señales de televisión y radio por el edificio, cuando estas se transmiten por el espacio radioeléctrico y son captadas por antenas ubicadas en el tejado del inmueble.
- En cada planta existen unos **registros secundarios** para efectuar las conexiones de la canalización principal con la canalización secundaria.
- La **canalización secundaria** está situada entre los registros secundarios y los registros de terminación de red. Por las canalizaciones secundarias transcurre la **red de dispersión**, que une la red de distribución con las redes interiores de cada una de las viviendas.
- Los **registros de terminación de red** se instalan dentro de la vivienda del usuario y delimitan la responsabilidad del mantenimiento de la red entre la comunidad y cada una de las viviendas del edificio.
- La **canalización interior de usuario** está formada por tubos (tantos como tomas de televisión, teléfono y tomas de reserva) que van desde el registro de terminación de red a las tomas propiamente dichas.

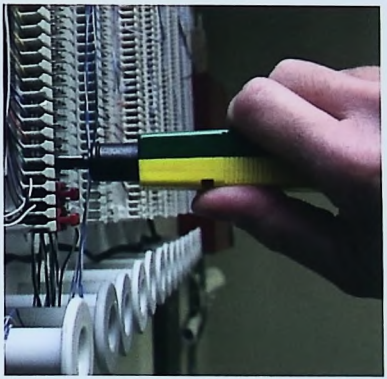


Figura 3.30. Instalación del punto de interconexión del RITI, haciendo uso de la herramienta de inserción.

¿Sabías que...?

La tecnología de comunicaciones FTTH (*Fiber To The Home*, Fibra Hasta el Hogar) se basa en el uso de cables de fibra óptica para la distribución de servicios de telefonía, conexión a Internet y Televisión hasta el hogar o las oficinas de abonado. Se diferencia de otras tecnologías de fibra óptica que llegan hasta la central del operador (FTTN, *Fiber To The Node*), hasta una cabina de telecomunicaciones cercana al usuario (FTTC, *Fiber To The Cabinet*) o hasta la acometida del edificio (FTTB, *Fiber To The Building*). Desde el punto donde termina la fibra al usuario final, en estos tres últimos casos, pueden emplearse diversos medios de transmisión, normalmente cable coaxial o par trenzado.

En España, la red FTTH se ha desplegado en la zona de los valles mineros asturianos, a través del Proyecto Asturcón, que emplean varios operadores para la distribución de sus servicios de telecomunicaciones.

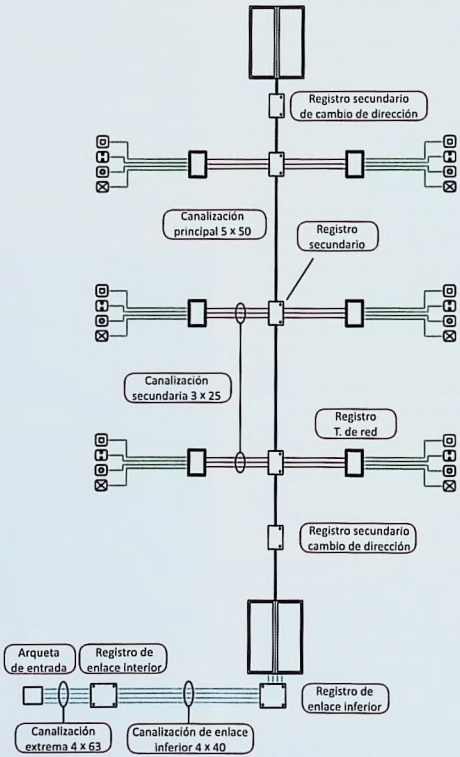


Figura 3.31. Plano de la canalización ICT para un edificio de tres plantas y dos viviendas por planta.

3.5. Telefonía analógica y digital

En la Unidad 1 de este libro mostramos las diferencias entre las señales analógicas y las señales digitales. Durante buena parte del siglo *xx*, la voz y la señalización en los sistemas de telefonía se transmitían directamente en su forma analógica, del modo descrito en el Apartado 3.1. A partir de la década de 1970, con el auge de los ordenadores y los sistemas digitales de procesamiento de la información, comienza un paulatino proceso de *digitalización* de los sistemas telefónicos, que se encuentra aún en curso.

La transmisión digital en telefonía presenta, en efecto, toda una serie de *ventajas*:

- La primera de ellas tiene que ver con el proceso de amplificación: los amplificadores analógicos simplemente toman la señal de entrada e incrementan su potencia. Al hacerlo, las distorsiones y los ruidos incorporados a la señal también se ven amplificados.

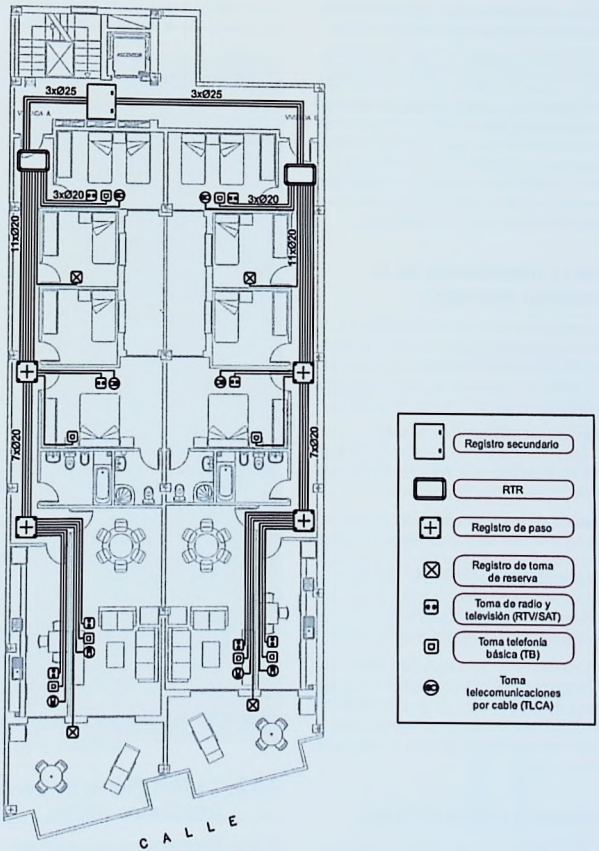


Figura 3.32. Canalización ICT de un edificio. Vista de planta.

Por el contrario, las señales digitales son recibidas y reconocidas por los dispositivos de retransmisión, que las vuelven a generar, evitando de este modo la propagación del ruido y las distorsiones.

- Las señales digitales son más fáciles de almacenar y procesar que las analógicas.
- Los protocolos de transmisión digital definen mecanismos de detección y corrección de errores, que hacen más fiable la transmisión de la información.
- Los equipos digitales consumen menos potencia y son más pequeños que sus equivalentes analógicos.

Sin embargo, el uso de señales digitales para la transmisión de voz presenta también algunos *inconvenientes*:

- Las señales digitales requieren un mayor ancho de banda para la transmisión que las señales analógicas.
- Antes de ser transmitida a través de la línea telefónica, la señal acústica (analógica) debe convertirse en digital; posteriormente, del lado del receptor, es preciso convertir de nuevo la señal digital en analógica. Estos procesos de conversión requieren dispositivos con capacidad para el procesamiento de datos e introducen inevitablemente retardos en la comunicación.

3.5.1. Errores y distorsiones en la transmisión analógica

Tal como hemos señalado anteriormente (Apartado 3.1.2), el espectro de frecuencias más adecuado para la transmisión de la voz humana está comprendido entre los 300 y los 3400 Hz. Existen, no obstante, algunos problemas característicos de esta transmisión de baja frecuencia:

- La **atenuación** es una distorsión de la señal proporcional a la longitud del cable; consiste en la pérdida de intensidad de la señal, que debe compensarse con bobinas de carga y otros dispositivos.
- La **desadaptación de impedancias** procede del hecho de que la impedancia de la línea telefónica no se mantiene constante, sino que varía con la frecuencia; las consecuencias pueden ser la pérdida de potencia, reflexiones de señal, ecos, inestabilidades en los amplificadores, etcétera. Todo ello puede llegar a distorsionar la señal haciendo imposible la comunicación.
- La **diafonía** consiste en el acoplamiento de las señales transmitidas por dos circuitos telefónicos cercanos. La señal de uno de los circuitos aparece en el otro, lo que hace que en una línea pueda llegar a escucharse la conversación telefónica que se está transmitiendo por otra.

3.5.2. Codificación digital de la voz

En la Unidad 1 estudiamos algunas de las técnicas básicas que se emplean para codificar digitalmente una señal analógica. El *muestreo* consiste en la medida del nivel de la señal a intervalos regulares y la conversión de este valor en un número binario.

La técnica de codificación empleada se denomina Modulación por Impulsos Codificados (MIC) o PCM (*Pulse-Code Modulation*). Las muestras de la señal se codifican mediante una secuencia o palabra de ocho bits, en el que el primero indica la polaridad (positiva o negativa) y con los otros siete se determina el valor de la misma. Con estos ocho bits se pueden codificar 256 posibles valores.

¿Sabías que...?

Dos de los códigos que se pueden emplear para la transmisión de los dígitos binarios son el RZ y el NRZ (véase la **Figura 3.33**). En el código NRZ (*Non-Return to Zero*, No Retorno a Cero), como podemos observar, la señal mantiene su valor cuando se transfiere una secuencia de varios ceros o varios unos; el problema de esta codificación es que, cuando la secuencia de ceros o unos consecutivos es larga, el receptor puede perder el sincronismo. Para evitar este problema puede emplearse la señal RZ (*Return to Zero*, Retorno a Cero). En ella, los unos binarios se transmiten mediante un pulso de señal que vuelve siempre al valor nulo.

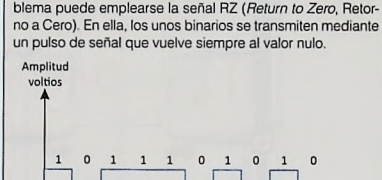


Figura 3.33. Señal NRZ.

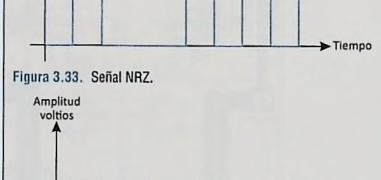


Figura 3.34. Señal RZ.

3.5.3. La Red Digital de Servicios Integrados (RDSI)

La Red Digital de Servicios Integrados (RDSI) o *Integrated Services Digital Network* (ISDN) es una red telefónica que proporciona conexión digital entre los terminales de la red. Se desarrolló en la década de 1980 con el objetivo de proporcionar conectividad no solo para servicios de voz, sino también para otros servicios como fax, acceso a Internet y videoconferencia. La transmisión se efectúa mediante canales de 64 Kbits/s.

RDSI se presentó en un primer momento como la alternativa de futuro para el sector de las telecomunicaciones.

En aquel momento, presentaba una serie de servicios de valor añadido, como la identificación de llamadas, la posibilidad de usar la llamada en espera o el desvío de llamadas. Sin embargo, la implantación de las tecnologías ADSL (de las que hablaremos más adelante) y la evolución de la propia red analógica y de los terminales han dejado atrás las prestaciones ofrecidas por la red RDSI, que nunca llegó a implantarse de forma masiva. Actualmente, algunas empresas la usan como soporte para servicios de datos y para videoconferencias.

¿Sabías que...?

Otra tecnología que experimentó un gran desarrollo durante la década de 1990 fue ATM (*Asynchronous Transfer Mode*, Modo de Transferencia Asíncrono). ATM estaba destinada a transmitir todo tipo de tráfico (tanto de voz como de datos y servicios multimedia), planteándose como una tecnología capaz de garantizar la convergencia de las telecomunicaciones. Emplea para el envío de los datos la multiplexación por división de tiempo asíncrona, codificando la información en pequeños paquetes de longitud fija denominados *celdas*. Esto lo diferencia de otros enfoques como el de *Internet Protocol* (IP, que estudiaremos en la siguiente Unidad), que emplean paquetes de datos de longitud variable. En la tecnología ATM, antes de efectuar la transferencia de datos, se establece un *circuito virtual* entre los dos extremos de la comunicación.

En la actualidad el uso de ATM y de otras tecnologías de *banda ancha* —aunque se sigue utilizando en las conexiones troncales de algunas redes— ha decaído sensiblemente, y la tendencia de las telecomunicaciones apunta hacia una red en la que, en efecto, converjan voz, datos y otros servicios, pero todos ellos transmitidos en forma de paquetes IP. Se habla, así, de que la *Red de la próxima generación* será una red *all-IP*.

3.5.4. Errores y distorsiones en la señal digital

Las señales digitales en la línea telefónica pueden sufrir diversas perturbaciones que producen errores en la transmisión. Las más importantes son las siguientes:

- El **ruido** afecta tanto a las señales analógicas como a las digitales. La ventaja de estas últimas es que el ruido puede eliminarse más fácilmente que en el caso de las señales analógicas. No obstante, el ruido puede provocar que la información transmitida por la señal digital se degrade y el receptor no sea capaz de interpretarla.
- Las señales que se trasmiten a través de las líneas telefónicas son senoidales. La forma cuadrada de la señal digital se obtiene mediante la combinación de cierto número de señales senoidales de diversas frecuencias.

La aproximación de la señal real a la señal teórica cuadrada será tanto mayor cuanto más elevado sea el ancho de banda del canal. Cuando el ancho de banda es limitado, el impulso transmitido se recibe con unas *colas* anterior y posterior. Este fenómeno, denominado **distorsión intersímbolos**, es uno de los factores limitantes de la velocidad de transmisión en los sistemas digitales.

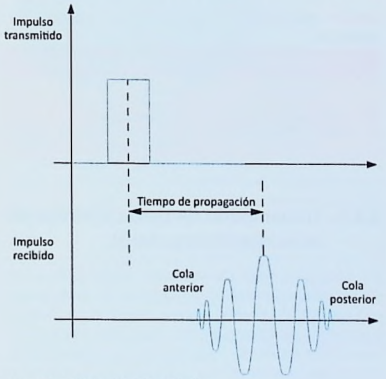


Figura 3.35. Distorsión intersímbolos.

- La **fluctuación de fase** o *jitter* es una variación de los frentes anterior y posterior del impulso con relación a la posición que deberían ocupar teóricamente en el mismo tiempo (véase la **Figura 3.35**).

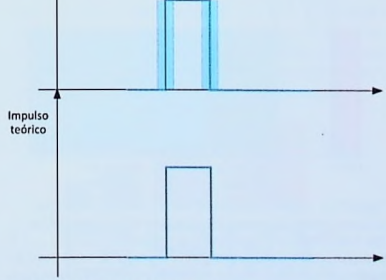


Figura 3.36. Distorsión de fase o *jitter*.

En la Unidad 5, dedicada a la telefonía IP, volveremos sobre estos y otros errores de la transmisión digital. La cantidad de errores que contiene una señal se cuantifica mediante la tasa de bits erróneos o BER (*Bit Error Rate*), como la fracción de bits erróneos del total de bits transmitidos. En función del BER se definen diversas *calidades de transmisión*:

Tabla 3.1. Relación entre la tasa de bits erróneos y la calidad de la transmisión.

Tasa de error	Calidad de la transmisión
BER ≤ 10^{-6}	Buena
10^{-3} > BER > 10^{-6}	Degradada
BER > 10^{-3}	Sistema averiado o cortado

3.5.5. Transmisión de datos a través de la red telefónica: ADSL

Se denomina *línea de abonado digital* (DSL, *Digital Subscriber Line*) a un conjunto de tecnologías que proporciona al abonado acceso a Internet mediante la transmisión de datos digitales a través del cable telefónico convencional. El bucle de abonado puede transmitir señales de frecuencia muy superior a la empleada por la voz, dependiendo del estado de la línea, pueden transmitirse señales del orden de las decenas de MHz. Recordemos que cuanto mayor es la frecuencia de la señal, más información puede transmitirse en la unidad de tiempo. Las tecnologías DSL emplean la banda de frecuencia superior, logrando de este modo una elevada tasa de transferencia de datos. Además de ello, el uso de dos bandas de frecuencia separadas permite que la voz y los datos puedan transmitirse simultáneamente, sin interferirse entre sí.

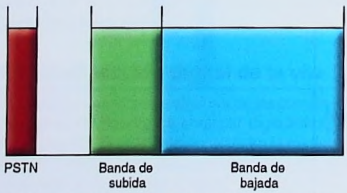


Figura 3.37. La tecnología ADSL emplea una banda de frecuencias situada por encima de la que emplea la línea de voz. Los transceptores DSL crean canales con una anchura de banda de 4312,5 Hz y posteriormente los combinan para formar una banda de subida y otra de bajada. Como podemos observar en la figura, el ancho de banda de bajada es superior al de subida; por eso decimos que la línea es *asimétrica*.

La tasa de transferencia de datos puede variar entre los 256 Kbps y los 40 Mbps, dependiendo de la tecnología empleada, las condiciones de la línea o la longitud del bucle de abonado (la proximidad de la central de conmutación al abonado).

En cada uno de los extremos de la línea DSL, un módem se encarga de codificar los datos digitales sobre la señal analógica. En el extremo del abonado, dicho módem suele estar integrado en un dispositivo que actúa asimismo como enrutador y como *switch*. En la central de conmutación del proveedor, existe un dispositivo, llamado DSLAM (*Digital Subscriber Line Access Multiplexer*, Multiplexor de Acceso a la Línea Digital de Abonado), que se encarga de conectar las líneas que llegan a la central a una línea de comunicaciones de datos de alta velocidad.

Recuerda que...

Para que la línea de voz funcione correctamente, debe instalarse entre la roseta y el terminal telefónico un filtro de paso bajo que elimine las frecuencias altas y deje pasar las situadas por debajo de 5 kHz. Los módems DSL llevan incorporado en su interior un filtro de paso alto que elimina las señales de baja frecuencia.



Figura 3.38. Filtro telefónico o *splitter*.

Se distinguen dos tipos de tecnologías DSL:

- Las *simétricas* (SDSL) proporcionan la misma tasa de transferencia de datos *de subida* (datos que parten del usuario) que *de bajada* (datos que llegan al usuario). Son menos frecuentes y se emplean, por ejemplo, en empresas que proporcionan alojamiento web.
- La mayoría de los abonados descargan muchos más datos a través de su conexión a Internet de los que necesitan *subir* a la red. La mayoría de empresas proveedoras de servicios de Internet (ISP) proporcionan, por ello, una línea de abonado digital *asimétrica* (ADSL), en la que el ancho de banda de bajada (y por tanto la tasa de transmisión de datos) es considerablemente superior al de subida.

¿Sabías que...?

Mediante el uso de frecuencias superiores para la transmisión de las señales a través del bucle de abonado se logran mejorar velocidades. Así, la tecnología ADSL2 presenta tasas de transferencia de 8 Mbps de bajada y 800 Kbps de subida mediante el uso de frecuencias de hasta 1,1 MHz. Por su parte, ADSL2+ presenta una tasa de transferencia máxima de 24 Mbps con el uso de frecuencias de hasta 2,2 MHz y la posibilidad adicional de sumar el ancho de banda de varios bucles de abonado que operen simultáneamente.

Actividad resuelta 3.3. ¿Para qué se emplea el filtro o *splitter* en las conexiones ADSL?

Solución. En la transmisión de datos a través de DSL se emplean unas bandas de subida y de bajada de frecuencias superiores (a partir de 25.875 kHz) a las que corresponden a la transmisión de voz a través de la línea telefónica (la transmisión de voz se produce en un rango de frecuencias entre 0 y 4 kHz). El receptor separa ambas señales mediante dos filtros: uno de paso bajo, que se instala entre la roseta y el terminal telefónico, y otro de paso alto, que viene normalmente incorporado en los propios dispositivos módem-router DSL.

3.6. Redes de telefonía móvil

Hasta aquí, los sistemas de telefonía que hemos estudiado pertenecen al ámbito de la *telefonía fija*: hemos asumido que la transmisión de la señal entre el terminal telefónico del abonado y la central de conmutación local se establece a través de un circuito eléctrico formado por un par de conductores de cobre. La telefonía móvil, sin embargo, emplea otro medio de transmisión, sobre el que ya hemos hablado en el Apartado 2.2.6 de este libro: las ondas electromagnéticas transmitidas a través del espacio libre.

La telefonía móvil es un sistema en el que las comunicaciones entre el abonado y la central de conmutación se establecen a través de una onda electromagnética, generalmente en un espectro de frecuencias situado entre los 900 y los 2100 MHz. Cuando el usuario está ubicado en el área de cobertura de su sistema de telefonía, entra en el área de conexión de una determinada *estación base*, que cubre una superficie denominada *celda*. Esta estación base será la encargada de establecer el contacto con el teléfono móvil del cliente; cuando este se desplaza, puede pasar de una celda a otra, cambiando entonces de estación base

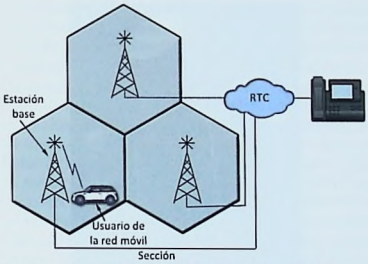


Figura 3.39. Estructura de celdas de una red de telefonía móvil.

En todo momento un teléfono móvil está situado en una celda determinada, bajo el control de la estación base de dicha celda. Cuando el teléfono abandona la celda, la estación detecta que la señal del teléfono cae por debajo de cierto umbral; entonces pregunta a todas las estaciones adyacentes con qué potencia reciben la señal de dicho teléfono. La estación base original transfiere la *propiedad* del teléfono a la estación adyacente que reciba su señal con mayor potencia. Este traspaso se denomina en inglés *handover* y se efectúa en un tiempo de unos 300 ms.

Para que un usuario pueda ser localizado bajo el área total de cobertura de un sistema de telefonía móvil, se precisa un sistema de seguimiento (*roaming*), que consiste en un registro actualizado de la celda en la que está situado el usuario.

3.6.1. GSM

Como ocurre con otras tecnologías, con el desarrollo inicial de la telefonía móvil surgieron en cada país sistemas tecnológicos diferentes e incompatibles entre sí. A comienzos de la década de 1980, la *Conférence européenne des administrations des postes et des télécommunications* (CEPT) creó un grupo de trabajo para desarrollar un estándar común para todo el territorio europeo, el *Groupe Spécial Mobile* (GSM).



Figura 3.40. Logo de GSM.



Figura 3.41. Antenas de telefonía móvil.

El estándar GSM se desarrolló para remplazar las redes de telefonía móvil analógica, de primera generación; definía una red conmutada *digital*, optimizada en un comienzo para las comunicaciones de voz, pero que pronto pasó a incluir comunicaciones de datos. Con el estándar GSM nacía la segunda generación (2G) de telefonía móvil o inalámbrica. La legislación de la Unión Europea convirtió GSM en un estándar de obligado cumplimiento. Si en 1995 el número de usuarios de telefonía GSM en todo el mundo era de 10 millones, en 1998 esa cifra se elevaba ya a 100 millones. En la actualidad, se calcula que el 80 % del mercado global de la telefonía móvil sigue este estándar. A partir de 2001 comienza a desarrollarse la red de telefonía móvil de tercera generación (3G), destinada a ofrecer servicios de datos de banda ancha.

¿Sabías que...?

Uno de los elementos del estándar GSM son los Módulos de Identificación de Abonado (SIM, *Subscriber Identification Module*), unas tarjetas que contienen la información de suscripción del usuario y, en muchos casos, su agenda telefónica. De este modo, el usuario puede cambiar de teléfono móvil manteniendo su información, o cambiar de proveedor del servicio de telefonía manteniendo su terminal telefónico.



Figura 3.43. Tarjetas SIM.

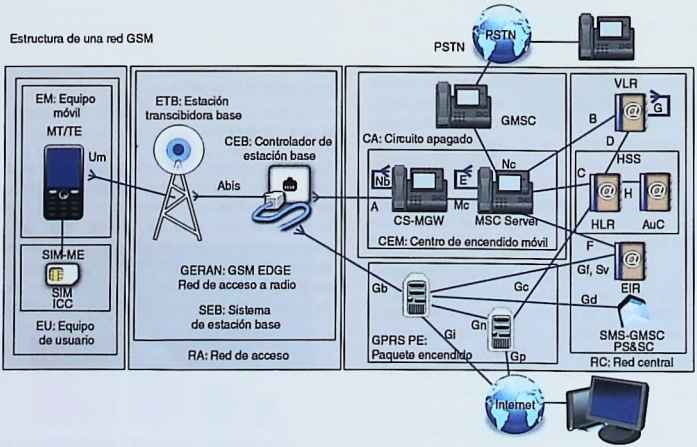


Figura 3.42. La red GSM está compuesta por varias sub-redes: (1) el subsistema de la estación base, formado por las estaciones base y sus controladores; (2) la red conmutada, similar a la red conmutada de la telefonía fija; (3) la red GRPS, que gestiona las conexiones a Internet mediante un sistema de conmutación de paquetes; (4) el sistema para el soporte de operaciones, destinado a las operaciones de mantenimiento de la red.

La red telefónica GSM sigue la estructura celular que se ha mencionado anteriormente. Se definen cinco áreas de celdas diferentes, en función del tamaño de la antena y del radio de cobertura de la señal, que puede oscilar entre unos cientos de metros y unas decenas de kilómetros.



Figura 3.44. Teléfonos móviles de tres generaciones diferentes.

La telefonía GSM de segunda generación opera en las bandas de 900 MHz y de 1800 MHz, mientras que la de tercera generación opera en la banda de frecuencias de los 2100 MHz.

3.6.2. Comunicaciones de datos en la telefonía móvil

La red móvil, aunque en un principio estuvo orientada principalmente a las comunicaciones de voz, soporta hoy en día la transmisión de todo tipo de datos y, en particular, proporciona el soporte para la conexión móvil a Internet. El servicio de transmisión de datos se denomina GPRS (*General Packet Radio Service*, Servicio General de Paquetes vía Radio). En la telefonía de segunda generación, GPRS proporciona tasas de transferencia de datos de entre 56 y 114 Kbps.

La telefonía móvil de tercera generación emplea un sistema denominado UMTS (*Universal Mobile Telecommunications System*, Sistema Universal de Telecomunicaciones Móviles). UMTS soporta tasas de transferencia de datos de hasta 42 Mbps mediante el uso del protocolo HSPA+.

3.7. Sistemas privados de telefonía (PBX)

En los apartados anteriores hemos considerado que a cada usuario llega una sola línea telefónica, capaz de transportar una conversación de voz y, a través de la tecnología DSL, una conexión de datos de banda ancha. Este tipo de conexión suele ser adecuada para entornos domésticos o de muy pequeñas empresas, pero en otros muchos escenarios (una empresa con cierto volumen de llamadas, una organización, una administración pública, etcétera) se revela claramente insuficiente. En estos casos se emplea un sistema de conmutación privado, cuyo cometido es similar al de una central de conmutación local: el sistema conecta las líneas privadas internas con las líneas externas; cuando un usuario que llama desde fuera del sistema, a través de la red telefónica pública, marca el número de extensión, la central conmuta de modo automático con la línea privada que corresponde a dicha extensión. A diferencia de las «centralitas» o sistemas multilínea (*key telephone system*) en las que un operador dirige manualmente las llamadas entrantes a la extensión o línea privada correspondiente —en las **Figuras 3.45** y **3.46** observamos dos ejemplos de estas centrales, pertenecientes a dos «generaciones» totalmente diferentes—, en los sistemas que estudiaremos en este apartado la conmutación se efectúa de modo automático.



Figura 3.45. Antigua «centralita» manual o sistema multilínea.



Figura 3.46. Centralita telefónica electrónica o sistema multilínea, un sistema híbrido que permite controlar manualmente la conmutación de las llamadas y soporta asimismo algunas funciones automáticas.

Los sistemas multilínea están limitados a un número reducido de líneas privadas. Por el contrario, las centrales privadas automáticas de conmutación o PBX (*Private Branch Exchange*) proporcionan funciones de conmutación a los usuarios conectados a ellas de modo automático, mediante un control por *software*. Además de las funciones de conmutación, las PBX proporcionan asimismo otros muchos servicios, como los mensajes de bienvenida, el contestador automático o el registro, grabación y control de las llamadas entrantes y salientes. En los casos necesarios (pensemos, por ejemplo, en los terminales telefónicos de las habitaciones de un hotel), la central PBX se encargará también de proporcionar información de tarificación de las llamadas salientes.

¿Sabías que...?

Las pasarelas GSM (*GSM gateways*) sirven para interconectar un sistema de telefonía privada cableado a una red GSM. Existen también pasarelas para la conexión con sistemas RDSI y para la conexión a redes VoIP (véase la Unidad 5). Estas pasarelas permiten efectuar llamadas directas desde la red privada a teléfonos móviles; muchos modelos permiten también el envío de mensajes SMS.

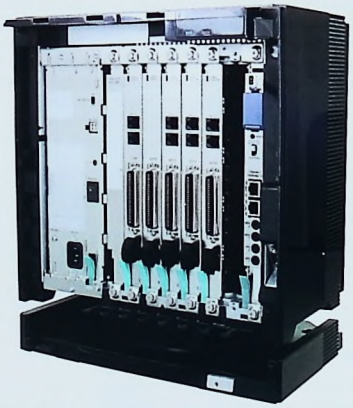


Figura 3.48. Sistema PBX. Vista posterior, en la que se observan las interfaces de conexión con las redes telefónicas pública y privada.

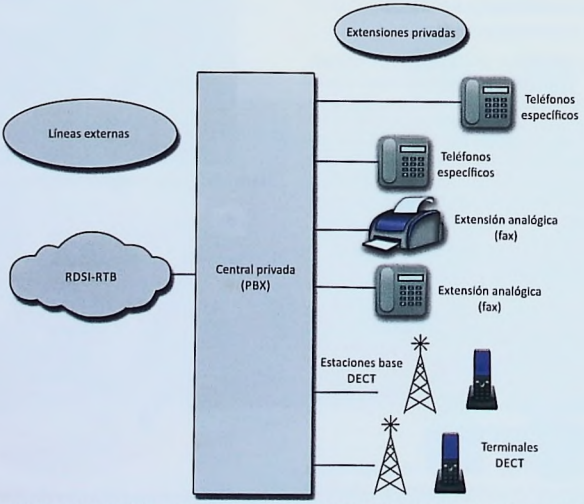


Figura 3.47. Funcionamiento de una central de conmutación privada. Como vemos, entre las extensiones privadas puede haber teléfonos fijos analógicos o digitales, faxes, teléfonos inalámbricos o buscapersonas. Se denominan *terminales específicos* o teléfonos a los terminales que se encuentran totalmente relacionados con el sistema.

¿Sabías que...?

Se emplea indistintamente el término de PBX y el de PABX (*Private Automatic Branch Exchange*); en los últimos años es más común el uso del término PBX, ya que se supone que todas las centrales privadas son automáticas.

Normalmente, se distinguen los siguientes componentes en un sistema PBX:

- La red de conmutación interna del PBX.
- El microcontrolador destinado al procesamiento de los datos.
- Las tarjetas telefónicas y los componentes de alimentación eléctrica.
- Las estaciones o terminales telefónicos (líneas).
- Las secciones que conectan la central PBX con la red pública conmutada.
- El tablero o consola de control de las llamadas entrantes.
- Un sistema de alimentación ininterrumpido.
- El cableado de conexión entre la central y los terminales.

Actividad propuesta 3.2

Consulta el manual de usuario de la centralita de la que dispongas para pruebas en el laboratorio de telefonía de tu centro educativo. ¿Qué funciones pueden realizarse con ella? ¿Cómo se configuran? ¿De qué conexiones dispone el sistema? ¿Para qué tipo de terminales? ¿Cuántas líneas externas y cuántas líneas internas permite conectar?

La comunicación entre los terminales conectados a la red privada se establece mediante la marcación de un número compuesto normalmente por dos o tres dígitos, dependiendo del *plan de marcación* establecido.

Para efectuar una llamada hacia el exterior de la red privada, normalmente se marca en primer lugar un dígito (por regla general el «0») y a continuación el número de abonado con el que se desea contactar.

3.8. Medida del tráfico telefónico

Aunque el tráfico telefónico se presenta de modo aleatorio, responde a ciertos patrones estadísticos; en la medida en que la red conmutada tiene muchos menos canales que terminales, se hace preciso un estudio, medida y previsión del tráfico para que la red sea capaz de cursar las llamadas correctamente, sin sobrecargas en las líneas. En otras palabras, el estudio del tráfico telefónico permitirá dimensionar la red para que el sistema resulte lo más eficiente posible.

Por una parte, se distinguen las variaciones de tráfico periódicas y, por otra, las variaciones aleatorias. Las variaciones aleatorias son impredecibles y se producen, por ejemplo, como resultado de una catástrofe natural:

- Las variaciones de tráfico diarias se presentan a lo largo de las horas del día; se producen picos de tráfico en las horas centrales de la jornada laboral y valles en las horas nocturnas, durante la hora de la comida, etcétera.
- Las variaciones de tráfico semanales se presentan a lo largo de los siete días de la semana; en esta escala de tiempo se registra un tráfico mayor en los días laborables que durante el sábado y el domingo.
- Al cabo del año también se producen ciertas variaciones en el tráfico telefónico, por ejemplo, las llamadas serán inferiores en los meses en los que hay más trabajadores disfrutando de sus vacaciones; a la inversa, existen picos de llamadas que se producen en ciertas épocas del año como la Navidad.

¿Sabías que...?

El sistema privado de telefonía puede dar servicio a un conjunto de teléfonos inalámbricos. En Europa, estos teléfonos emplean mayoritariamente el estándar de comunicación DECT (*Digital Enhanced Cordless Telecommunications*, Telecomunicaciones Inalámbricas Mejoradas Digitalmente).Estos sistemas actúan de modo similar a la red GSM, en el sentido de que cada estación base DECT tiene un área de cobertura y cuando el usuario del teléfono se desplaza, su terminal pasa a depender de una u otra celda. El control y la asignación se efectúan mediante una central privada (una central DECT de propósito específico), que actúa también como pasarela con la red privada de telefonía. Existen, por otra parte, módulos DECT que se integran en la central PBX y se configuran mediante el software de la misma.

Las estaciones base se conectan a los módulos o la central DECT mediante cables de par de cobre. Es importante planificar adecuadamente la ubicación de las centrales base en función de la densidad de tráfico en cada área de cobertura y de la propagación de las ondas de radio a través de paredes, pilares, puertas, etcétera.

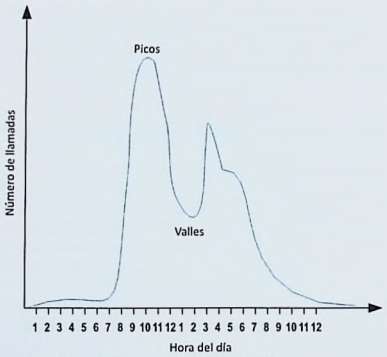


Figura 3.49. Variaciones diarias del tráfico telefónico.

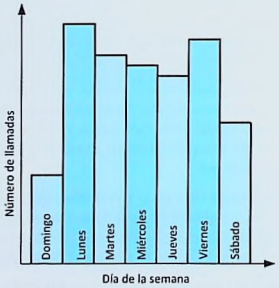


Figura 3.50. Variaciones semanales del tráfico telefónico.

En la medida del tráfico telefónico se distinguen dos magnitudes: por una parte, el *volumen* del tráfico y, por otra, la *intensidad* del tráfico telefónico.

El **volumen de tráfico** se expresa en unidades de tiempo y se obtiene de la expresión:

$$V_T = n \times d$$

donde n es el número de llamadas realizadas y d la duración media de las llamadas.

Otras unidades de medida del volumen de tráfico telefónico son la *llamada reducida* (LLR), que se define como la ocupación del equipo o enlace telefónico durante 120 segundos, y el *centum call centum* (CCS), tiempo de ocupación del equipo o enlace telefónico durante 100 segundos.

Actividad resuelta 3.4. Seis terminales telefónicos cursan al día 28 llamadas telefónicas con una duración media de 4 minutos y 20 segundos. Determina el tráfico telefónico en la red (en LLR y CCS).

Solución. Calculamos en primer lugar el volumen del tráfico telefónico en segundos, expresando en esta unidad la duración media de las llamadas y multiplicándola por el número de llamadas y de terminales.

$$V_T = 6 \times 28 \times [(4 \times 60) + 20] = 43.680 \text{ seg}$$

$$LLR = \frac{43.680 \text{ seg}}{2 \text{ min}} = \frac{43.680 \text{ seg}}{120 \text{ seg}} = 436{,}8 \; CCS$$

$$CCS = \frac{43.680 \text{ seg}}{100 \text{ seg}} = 436{,}8 \; CCS$$

La **intensidad de tráfico** es una medida de la ocupación que experimentan los circuitos o sistemas telefónicos. La intensidad viene dada como el cociente entre el volumen de tráfico cursado y el tiempo de observación:

$$I_T = \frac{V_T}{t_0}$$

La intensidad viene dada en una magnitud denominada *Erlang*.

¿Sabías que...?

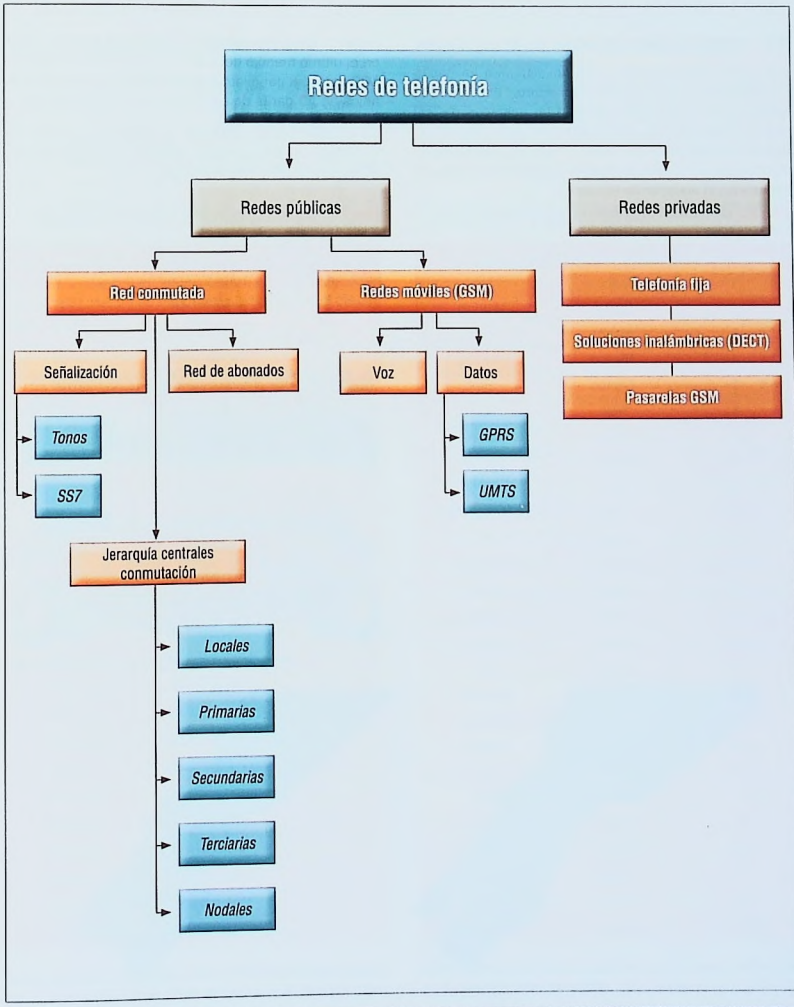
La unidad *Erlang* recibe el nombre del ingeniero danés Agner K. Erlang (1878–1929), especialista en teoría de colas y precursor del análisis del tráfico en la red telefónica.

Para dimensionar correctamente las centrales de conmutación y lograr que estas sean capaces de gestionar o cursar todo el tráfico telefónico, se toma habitualmente como referencia la intensidad media de tráfico producida en la hora del día de mayor tráfico. Este período de tiempo se conoce como *hora cargada*.

Actividad propuesta 3.2

Supongamos que un terminal telefónico cursa en un día 46 llamadas con una duración media de 3 minutos y 40 segundos. Expresa el volumen de tráfico en tiempo (horas, minutos y segundos) y en LLR y CCS.

Mapa conceptual



Práctica profesional

3.1. Cables de pares de cobre: código de colores

Los cables de hasta 25 pares se disponen en capas concéntricas. Si es necesario transportar un mayor número de pares, estos se agrupan en unidades de 25, atando cada una con una ligadura de color específico. Para la identificación de cada uno de los pares dentro de una misma unidad, se emplea el siguiente código de colores en el aislante de los pares:

Tabla 3.2. Identificación de los pares de cobre en función de su código de color.

Número de par	Color conductor 1	Color conductor 2
1	Blanco	Azul
2	Blanco	Naranja
3	Blanco	Verde
4	Blanco	Marrón
5	Blanco	Gris
6	Rojo	Azul
7	Rojo	Naranja
8	Rojo	Verde
9	Rojo	Marrón
10	Rojo	Gris
11	Negro	Azul
12	Negro	Naranja
13	Negro	Verde
14	Negro	Marrón
15	Negro	Gris
16	Amarillo	Azul
17	Amarillo	Naranja
18	Amarillo	Verde
19	Amarillo	Marrón
20	Amarillo	Gris
21	Violeta	Azul
22	Violeta	Naranja
23	Violeta	Verde
24	Violeta	Marrón
25	Violeta	Gris
Piloto	Negro	Blanco

Los pares piloto no se emplean para dar servicio, sino para efectuar pruebas. Los cables de dos, tres o cuatro manojos (50, 75 o 100 pares), llevan un solo par piloto en el último manojo del cable. En los cables de más de 100 pares, el par piloto está situado en los últimos manojos de 25 pares de cada grupo de cuatro manojos.

Con respecto a las unidades de varios pares, estas se identifican por el color de su ligadura, siguiendo el código que se detalla a continuación.

Tabla 3.3. Identificación de los manojos de cable en función del color de ligadura.

Número del par	Color de la ligadura	Numeración de los pares
1	Blanco-Azul	1-25
2	Blanco-Naranja	26-50
3	Blanco-Verde	51-75
4	Blanco-Marrón	76-100
5	Blanco-Gris	101-125
6	Rojo-Azul	126-150
7	Rojo-Naranja	151-175
8	Rojo-Verde	176-200
9	Rojo-Marrón	201-225
10	Rojo-Gris	226-250
11	Negro-Azul	251-275
12	Negro-Naranja	276-300
13	Negro-Verde	301-325
14	Negro-Marrón	326-350
15	Negro-Gris	351-375
16	Amarillo-Azul	376-400
17	Amarillo-Naranja	401-425
18	Amarillo-Verde	426-450
19	Amarillo-Marrón	451-475
20	Amarillo-Gris	476-500
21	Violeta-Azul	501-525
22	Violeta-Naranja	526-550
23	Violeta-Verde	551-575
24	Violeta-Marrón	576-600

Para los pares situados a partir del 601, se inicia nuevamente la secuencia de colores de las ligaduras.

Práctica profesional

3.2. Instalaciones de telefonía interior

En el RITI están situadas las regletas de distribución. En los registros secundarios, se emplean también una serie de regletas para realizar las conexiones de los pares para telefonía. A estas últimas regletas se las denomina *regleteros de telefonía* (véase la **Figura 3.51**) y suelen tener un tamaño de entre 5 y 10 pares. Las conexiones de los pares se efectúan insertando los cables en las ranuras del regletero, mediante la herramienta de inserción (véase la **Figura 3.52**). Al final de la ranura del regletero hay unas cuchillas que cortan el aislante del cable y entran en contacto con el cobre, asegurando de este modo la continuidad eléctrica de la conexión.

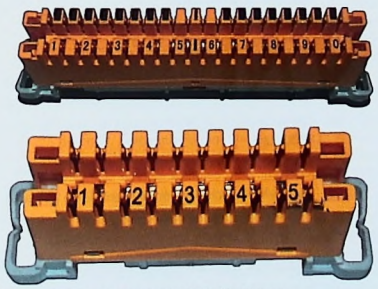


Figura 3.51. Regleteros de telefonía de 10 y 5 pares.

Recuerda que...

En una instalación de nueva planta, siempre debemos llevar como mínimo dos pares a cada vivienda, por si sus habitantes deciden contratar dos líneas telefónicas. En la instalación deben sobrar siempre pares de reserva para futuras ampliaciones.

En la Tabla 3.4 se muestran las medidas de las canalizaciones y los registros de las ICT:

Tabla 3.4. Medidas de canalización y registros en las ICT.

Elemento	Dimensiones
Arqueta de entrada	40 × 40 × 60 cm
Canalización externa	4 × Ø 63 mm
Canalización de enlace inferior	4 × Ø 40 mm
Canalización de enlace superior	4 × Ø 40 mm
Canalización principal	4 × Ø 50 mm
Canalización secundaria	3 × Ø 25 mm
RITI/RITS	100 × 200 × 50 cm
Registro de enlace inferior	45 × 45 × 12 cm
Registro de enlace superior	36 × 36 × 12 cm
Registro secundario	45 × 45 × 15 cm
Registro de terminación de red	30 × 50 × 6 cm
Registro de paso	10 × 16 × 4 cm
Registro de toma	6,4 × 6,4 × 4,2 cm

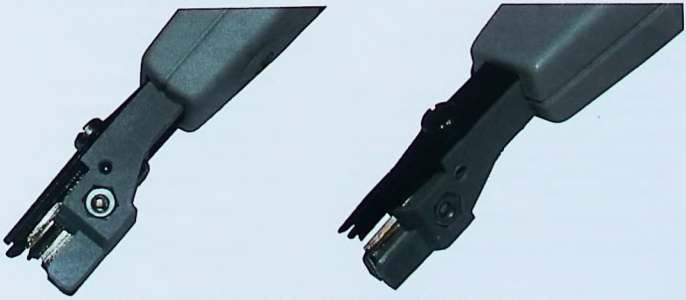


Figura 3.52. Detalle de la punta de la herramienta de inserción y mecanismo para el corte del cable sobrante.

Cuestiones

3.1. La tecnología DECT:

a) Es una tecnología para teléfonos inalámbricos.

b) Se basa en una estructura de celdas.

c) Puede integrarse en la red de telefonía privada de la empresa, ya sea mediante una central DECT o mediante módulos DECT que se instalan en la central PBX.

d) Todas las opciones son válidas.

3.2. En una red de telecomunicaciones con tecnología FTTB:

a) La fibra óptica llega hasta el hogar del usuario.

b) La fibra óptica llega hasta la central de conmutación de la empresa de telecomunicaciones.

c) La fibra óptica llega hasta la acometida del edificio.

d) Se emplea cable coaxial para conectar la central de conmutación y el registro de terminación de red.

3.3. Fíjate en la asociación de las tecnologías siguientes con sus correspondientes medios de transmisión. Indica cuál no es correcta:

a) FTTH: fibra óptica.

b) DECT: ondas de radio.

c) RBT: par de cobre.

d) ADSL: ondas electromagnéticas no guiadas.

3.4. En la red telefónica conmutada, las centrales nodales:

a) Conectan entre sí a los terminales telefónicos a escala local.

b) Están conectadas formando una topología en bus.

c) Sirven para conectar entre sí las centrales primarias.

d) Ninguna de las opciones es correcta.

3.5. La tecnología GSM:

a) Se basa en el uso de estaciones base, cada una de las cuales cubre un área denominada celda.

b) Permite que un usuario que se desplaza con su terminal móvil cambie de celda (*handover*) y sea localizado en las diversas celdas del área de cobertura del sistema (*roaming*).

c) Es una tecnología de transmisión analógica.

d) Permite la transmisión de voz y datos.

3.6. La red SS7:

a) Es una red de conmutación de paquetes.

b) Permite enviar mensajes con la señalización de las llamadas e información sobre el usuario, facturación, etcétera.

c) Está basada en tecnología digital.

d) Todas las opciones son correctas.

3.7. En las Infraestructuras Comunes de Telecomunicaciones, los registros secundarios:

a) Sirven para conectar las regletas de los operadores con los pares de abonado de cada una de las viviendas.

b) Contienen las conexiones entre la red de distribución y la red de dispersión.

c) Son el punto a partir del cual comienza la instalación interior del usuario.

d) Todas las opciones anteriores son falsas.

3.8. La transmisión de datos a través de ADSL:

a) Permite una tasa de transferencia de datos de subida y de bajada aproximadamente iguales.

b) Opera en el rango de frecuencias entre los 300 y los 6000 Hz.

c) Requiere que el usuario disponga de un módem.

d) Se ha visto desplazada en buena medida por la tecnología RDSI.

3.9. La red RDSI:

a) Está formada por canales de 64 Kbps.

b) Es una red plenamente digital.

c) Presenta una serie de servicios de valor añadido que, aunque novedosos en el momento de su introducción, han sido incorporados en gran medida a la Red Telefónica Básica.

d) Todas las opciones son correctas.

3.10. Los sistemas privados de telefonía:

a) Están basados en el intercambio de paquetes de datos (IP).

b) Solo disponen de interfaces digitales.

c) No pueden comunicarse con teléfonos móviles.

d) Actúan como un sistema de conmutación privado, semejante a una RTC a pequeña escala.

Actividades de aplicación

3.11. Supón que una pequeña empresa local de un polígono industrial cercano a tu cuidad, dedicada a la fabricación y venta de perfiles metálicos, desea contratar un sistema de telecomunicaciones que le facilite servicios de voz y de acceso a Internet. Valora las diversas opciones disponibles en el mercado, respondiendo a las siguientes cuestiones:

a) Consulta la oferta de acceso básico RDSI que ofrecen los operadores de telecomunicaciones. ¿Te parece una solución adecuada para esta empresa?

b) Consulta las ofertas de voz y DSL de diversos operadores y compáralas. ¿Qué velocidades de conexión ofrecen? ¿Qué tipo de conexión crees que es más adecuada para la empresa, ADSL o SDSL? ¿Estos operadores emplean su propia red o la del operador dominante?

c) ¿Existe alguna red que ofrezca servicios de voz y datos mediante una red de fibra óptica? ¿Qué velocidades de conexión ofrecen? ¿Hasta qué punto de la red de abonados llega la fibra óptica (FTTN, FTTC, FTTB, FTTH)? ¿Qué medio de transmisión se emplea desde ese punto hasta las instalaciones de la empresa?

3.12. ¿Existe alguna antena de telefonía móvil en las proximidades de tu domicilio o tu centro educativo? Ese tipo de antenas, ¿presenta algún problema para la salud? ¿Cuáles? Efectuad un debate en el aula respecto a los inconvenientes y las ventajas de la instalación de este tipo de dispositivos en zonas urbanas.

3.13. Se desea conectar en el hogar de un cliente que ha contratado una línea de voz analógica y acceso a Internet mediante ADSL una pequeña instalación de comunicaciones con dos equipos informáticos y tres terminales telefónicos. Dibuja la instalación a partir del PTR, incluyendo los elementos necesarios (filtro o *splitter*, *router*, rosetas, etcétera).

3.14. Identifica todos los tonos o señales presentes en una llamada entre dos abonados de la red telefónica conmutada. ¿Cuál es el significado de cada una de ellas?

3.15. En un cable de 100 pares telefónicos, indica en qué manojo están y qué colores tienen los siguientes pares: 3, 6, 9, 12, 21, 29, 32, 41, 53, 58, 63, 71, 77, 82, 91, 97 y 100.

3.16. ¿En qué consiste la modulación MIC o PCM? ¿Qué tipo de información obtienes al modular la señal de voz mediante MIC? ¿En qué tecnologías se emplea?

3.17. Efectúa un plano de las Instalaciones Comunes de Telecomunicaciones de un edificio de tres plantas y cuatro viviendas por planta. Indica cada una de las partes que componen la instalación. Emplea la simbología que se ha utilizado en la **Figura 3.32**. Efectúa la instalación en un tablero de pruebas de tamaño suficiente para albergarla.

3.18. Explica en qué se diferencia una línea telefónica analógica de otra digital.

3.19. ¿En qué consiste una central PBX? ¿Qué funciones tiene? ¿Cómo puedes integrar una solución inalámbrica en la red privada de una empresa? ¿Cómo puedes comunicarla con una red GSM?

3.20. Explica las partes de las que se compone la red de abonados y las funciones y características de cada una de sus partes. ¿Qué aspectos de la red «tradicional» han cambiado con la liberalización del mercado de las telecomunicaciones? ¿Cómo dan servicio los operadores de telecomunicaciones a los usuarios de la red?

3.21. ¿Cómo funciona un sistema de telefonía móvil? ¿De qué elementos consta? ¿Cómo se consigue que los abonados estén permanentemente conectados a la red a pesar de encontrarse en movimiento? ¿Cuál es la forma ideal de las celdas de la red de telefonía? ¿Qué es una tarjeta SIM?

3.22. ¿Qué son las «funciones de hotel» en una central telefónica privada? Busca información al respecto e identifica una central PBX del mercado que disponga de ellas, señalando su fabricante y su coste.

Lectura

Plan Nacional de Numeración Telefónica (RD 2296/2004, extractos)

Este Plan, que se aprueba mediante Real Decreto 2296/2004, de 10 de diciembre, es una adaptación al nuevo marco legal del plan de numeración que entró en vigor en España el 4 de abril de 1998. Se refiere exclusivamente a los números de teléfono y se define como un plan cerrado a 9 dígitos, lo que significa que los usuarios llamantes siempre deben marcar los 9 dígitos del número completo, independientemente del lugar donde se encuentren. Por ello, no son posibles las marcaciones locales abreviadas, como ocurría años atrás. El Plan adjudica los indicativos a las distintas provincias españolas y atribuye rangos de números a los servicios (por ejemplo, los servicios móviles disponen de los números que comienzan por el dígito 6, mientras que los indicativos provinciales comienzan por los dígitos 9 y 8).

Dado que una parte de los recursos públicos de numeración están sin atribuir ni adjudicar (aproximadamente el 50 %), el Plan se configura como un sistema flexible que permite la apertura de nuevos rangos por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información en función de las necesidades existentes en cada momento. Por su parte, la Comisión del Mercado de las Telecomunicaciones asigna los números del Plan a los operadores siguiendo el procedimiento establecido en el Capítulo V del Título IV del Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración, aprobado por Real Decreto 2296/2004, de 10 de diciembre.

El número nacional

El número nacional del Plan nacional de numeración telefónica consta de nueve dígitos representados por la secuencia alfabética NXYABMCDU, siendo N la cifra que se marca en primer lugar.

Los valores del dígito N están atribuidos a los siguientes servicios (se incluyen las atribuciones realizadas después de la aprobación del Plan):

Primer dígito	Servicios asignados
N = 0	Servicios de numeración corta (solo de interés social) y prefijo internacional.
N = 1	Servicios de numeración corta, servicios armonizados europeos (NX = 11), servicios internos (NX = 12) y prefijos.
N = 2	Servicios internos (NX = 22) y pendiente de atribución.
N = 3	Pendiente de atribución.
N = 4	Pendiente de atribución.
N = 5	Servicios de red privada virtual (X = 0), servicios vocales nómadas (X = 1), comunicaciones máquina a máquina (XY = 90) y pendiente de atribución.
N = 6	Servicios de comunicaciones móviles.
N = 7	Servicios de numeración personal (X = 0), servicios de comunicaciones móviles (X = 1,2,3,4) y reservado para comunicaciones interpersonales.
N = 8	Servicio telefónico fijo y servicios vocales nómadas ($X \neq 0, 9$), tarifas especiales (X = 0), y pendiente de atribución.
N = 9	Servicio telefónico fijo ($X \neq 0, 9$), tarifas especiales y acceso a Internet (X = 0), y pendiente de atribución.



4

Redes de transmisión de datos

En la Unidad 2 de este libro hemos estudiado extensamente cómo se monta y se configura la infraestructura de una red de comunicaciones: su cableado, sus interfaces de red y otros elementos físicos, así como la conexión y el acceso a la red de los equipos informáticos. En esta Unidad abordaremos las operaciones de configuración de la red de datos que pertenecen a las capas superiores del modelo OSI; concretamente, a las capas de red, transporte, sesión, presentación y aplicación. Introduciremos la arquitectura TCP/IP, conjunto de protocolos en los que se basa el funcionamiento de Internet, y aprenderemos a configurar los equipos de la red en diversos sistemas operativos.

Contenidos

4.1. La arquitectura TCP/IP

4.2. La capa de transporte

4.3. La capa de aplicación

Objetivos

- Conocer los aspectos básicos de la pila de protocolos TCP/IP, identificando a qué capa de dicha pila pertenecen los protocolos más comunes y relacionándolos con las correspondientes capas del modelo OSI que hemos estudiado en la Unidad 1.
- Comprender las diferencias entre los protocolos de la capa de Internet y la capa de transporte, identificando las funciones de unos y otros y las informaciones que contienen sus cabeceras.
- Conocer los protocolos de la capa de aplicación, sus funciones y los puertos que emplean para comunicarse con otros equipos.
- Configurar los equipos de la red (asignación de direcciones, nombres de equipo y recursos compartidos) en sistemas operativos Windows y GNU/Linux, así como configurar redes mixtas Windows-Linux.
- Ser capaces de modificar la configuración del router en aspectos como el servicio DHCP o la tabla NAT.

4.1. La arquitectura TCP/IP

En 1969, uno de los organismos del Departamento de Defensa de los Estados Unidos, denominado ARPA (*Advanced Research Project Agency*, Agencia de Proyectos de Investigación Avanzados), inició un proyecto de investigación para construir una red de ordenadores basada en el intercambio de paquetes de datos mediante enlaces dedicados. Esa red, denominada ARPANET, se convirtió en la base de lo que hoy en día conocemos como Internet.

En un comienzo, la red estaba montada sobre enlaces telefónicos alquilados, pero con el tiempo comenzaron a precisarse enlaces con otras redes empleando medios de transmisión no guiados. Los problemas de interconexión entre redes (*internetworking*) que aparecieron como resultado de ello dieron lugar al desarrollo de una familia de protocolos conocida como TCP/IP.

En realidad TCP/IP es la denominación genérica de un gran conjunto de protocolos, una *familia* de protocolos. Estos, con el paso del tiempo y debido a su flexibilidad y al propio crecimiento de Internet, se han convertido en estándares de «la Red». Al igual que el modelo OSI, la familia agrupa los protocolos en *capas*; cada una de ellas ofrece servicios a la situada en el nivel inmediatamente superior.

Las capas de la familia TCP/IP, de abajo hacia arriba, son las siguientes:

- **Acceso a la red**. En esta capa se definen las características físicas del medio de transmisión.
- **Internet**. Esta capa establece las herramientas necesarias para definir el camino seguido por los datos desde el dispositivo origen al dispositivo destino. En esta capa, el protocolo «estrella» es el denominado *Internet Protocol* (IP, Protocolo de Internet), que define el *mecanismo de transmisión* que emplean los protocolos de las capas superiores.

  El protocolo IP es un protocolo *no fiable* y *sin conexión*. ¿Qué significa esto? IP no proporciona ningún mecanismo de control de errores y de seguimiento de los datagramas. En otras palabras, IP *asume* que el medio de transmisión no es ni puede ser fiable, puesto que puede verse sujeto a todo tipo de contingencias, desde la presencia de interferencias hasta un corte en las líneas de transmisión provocado por una tormenta.

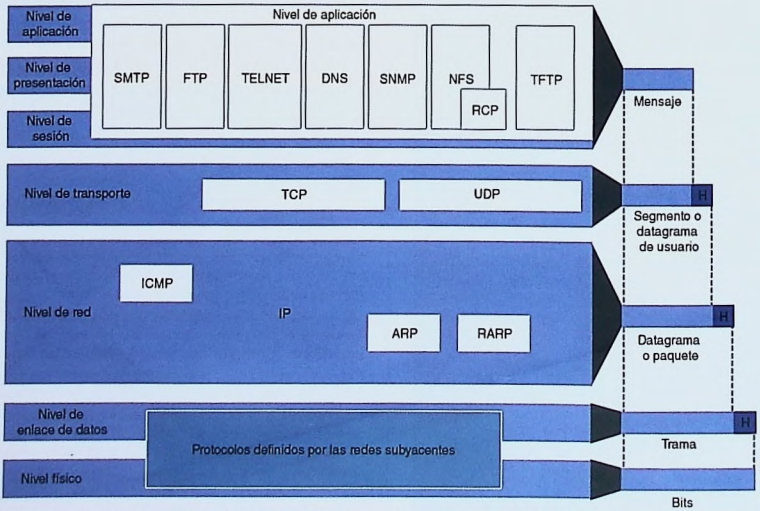


Figura 4.1. Capas y principales protocolos del modelo TCP/IP y su relación con las capas del modelo OSI.

El protocolo IP transmite los datos en paquetes denominados *datagramas*; cada datagrama se envía por separado, y cada uno de ellos puede seguir diversas rutas a través de Internet, de modo que pueden llegar a su destinatario desordenados, duplicados o incluso perderse o dañarse por el camino. El protocolo se preocupa *simplemente* de hacer llegar los datagramas a su destinatario, pero no proporciona mecanismos para reordenarlos y reconstruir el mensaje completo ni para comprobar si alguno de los datagramas se ha perdido. En otras palabras, no crea un «circuito virtual» entre remitente y destinatario, y por ello se dice que es un protocolo *no fiable* y *sin conexión*. Necesita, por tanto, de protocolos situados por encima de él que efectúen estas funciones de reordenación y control. El más importante de ellos es el Protocolo de Control de Transmisión (TCP, *Transmission Control Protocol*).

- **Transporte**. Los protocolos de este nivel proporcionan un servicio de transferencia entre sistemas finales, haciendo abstracción de los detalles y las especificidades de las redes subyacentes. El protocolo más importante que encontramos en esta capa es el *Protocolo de Control de Transmisión* (TCP, *Transmission Control Protocol*), un protocolo de transporte *fiable* de *puerto a puerto*. TCP es un protocolo *orientado a la conexión*, en el sentido de que crea una conexión entre dos ordenadores o, en otras palabras, establece un circuito virtual entre el remitente y el destinatario que permanecerá activo durante el tiempo que dure la transmisión.
- **Aplicación**. Permite la comunicación entre aplicaciones de equipos conectados a través de los protocolos de capas inferiores. La capa de aplicación se encarga de ofrecer mecanismos que permitan el intercambio de datos entre las aplicaciones; ejemplos de protocolos a este nivel son SMTP, POP e IMAP (empleados para los servicios de correo electrónico), Telnet y SSH (empleados para el uso remoto de sistemas operativos), FTP y SFTP (usados para la transferencia de ficheros entre equipos), HTTP y HTTPS (empleados para la transmisión de documentos web), etcétera.

La **Figura 4.1** muestra diversos protocolos presentes en cada capa de la familia TCP/IP, junto con su equivalencia según el modelo OSI. También muestra la *encapsulación* de los datos en las diversas capas del protocolo. La unidad de datos creada en la capa de aplicación se denomina *mensaje*. Los protocolos TCP y UDP crean una unidad de datos denominada *segmento* o *datagrama de usuario*. Aunque la transferencia del datagrama a través de Internet es responsabilidad del conjunto de protocolos TCP/IP, para poderse mover físicamente de una red a otra, el datagrama debe ser encapsulado en una *trama*, que se pasa a la capa de acceso a la red y que finalmente se transmite mediante las señales correspondientes a través del medio físico de transmisión.

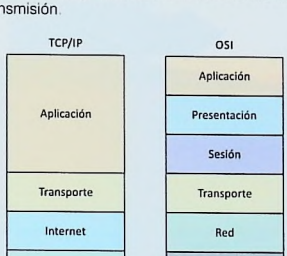


Figura 4.2. Comparación de las capas TCP/IP y OSI.

Para que los nodos de una red se comuniquen mediante TCP/IP, es preciso identificar cada uno de los nodos, tanto los situados en los extremos de la comunicación (el remitente y el destinatario del mensaje) como todos los dispositivos intermedios. El encargado de efectuar esta identificación es el Protocolo de Internet, como veremos a continuación, mediante las denominadas *direcciones IP*. Además de ello, se precisa otra identificación adicional, pues el dispositivo al que va dirigido el mensaje debe contar con algún mecanismo que le permita saber a qué aplicación o proceso debe entregarlo. Un mismo equipo puede recibir muchos mensajes diferentes a través de TCP/IP: un correo electrónico, un documento web, una petición o una respuesta para una transferencia de ficheros. El protocolo de transporte proporciona una forma de diferenciar todos estos mensajes mediante una dirección denominada *puerto*.

4.1.1. Paquetes de datos o datagramas

Los paquetes de la capa IP se denominan *paquetes de datos* o *datagramas*. Son grupos de información de longitud *variable*, de hasta 65.536 bytes. El paquete está dividido en una cabecera y un conjunto de datos. La cabecera contiene la información necesaria para el enrutamiento del mensaje y para asegurar que este se entregue al nodo de la red al que corresponde. El contenido de dicha cabecera se representa en la **Figura 4.3**.

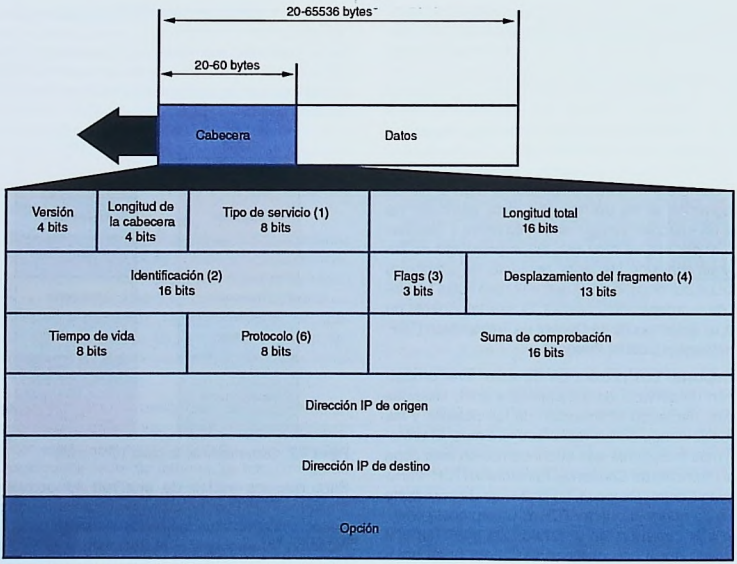


Figura 4.3. Datagrama IP y contenidos de la cabecera. **Notas: (1)** El **tipo de servicio** especifica, entre otros elementos, la *prioridad* del paquete. (2) Cuando un mensaje debe dividirse en varios paquetes, el campo de **identificación** contiene un número de orden que permite reconstruir el mensaje a partir de la secuencia de datagramas. (3) Las banderas o **flags** especifican si el paquete forma parte de un mensaje dividido o fragmentado y si dicho paquete está situado al comienzo, al final o en el medio de dicho mensaje. (4) Cuando el paquete es parte de una secuencia, el **Desplazamiento del fragmento** indica la distancia entre dicho fragmento al comienzo del mensaje. (5) El **tiempo de vida** es un parámetro destinado a evitar que los paquetes viajen indefinidamente a través de Internet. Es un valor entero que se reduce a medida que el mensaje viaja de nodo en nodo. Cuando llega a cero, el datagrama se descarta. (6) El protocolo especifica el protocolo del mensaje de la capa superior (TCP o UDP).

4.1.2. Direcciones IP

La dirección IP es una convención numérica para identificar unívocamente cada uno de los equipos conectados a la red. La dirección identifica al equipo *en su red*. En la definición inicial del protocolo (IPv4), las direcciones IP expresaban como una secuencia de cuatro dígitos, de 8 bits cada uno. Debido al enorme crecimiento de Internet, a partir de 1995 se desarrolló un nuevo protocolo, el IPv6, que permite definir un número mucho mayor de direcciones. Sin embargo, dicha versión del protocolo está aún en fase de implantación, por lo que en esta sección nos centraremos en la descripción de las direcciones IPv4.

Aunque, como toda la información digital, las direcciones IP se codifican y se transmiten en formato binario, para poder leerlas con más facilidad se suelen representar como cuatro dígitos decimales, con un valor situado entre 0 y 255 (véase la **Figura 4.4**).

> **Recuerda que...**
>
> El *nombre* indica lo que buscamos. La *dirección* indica dónde está. La *ruta* indica cómo llegar allí (definición del Protocolo de Internet de la IETF [*Internet Engineering Task Force*, Grupo de Ingeniería de Internet]).

Los dígitos de la izquierda de la dirección especifican la red a la que pertenece el equipo; los de la derecha identifican al equipo dentro de dicha red. Varios ordenadores conectados a una misma red (una red doméstica, una pequeña empresa, un gran edificio de

Universidad Tecnica del Norte
BIBLIOTECA
Ibarra Ecuador

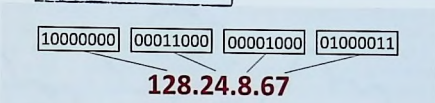


Figura 4.4. Dirección IP en notación binaria y decimal.

Tabla 4.1. Clases de direcciones IP.

Clase	Primeros bits de la dirección	Rango del primer dígito decimal	Dirección de la red	Dirección del equipo	Número de redes	Número de direcciones por red
A	0	0-127	a	b.c.d	$2^7 = 128$	$2^{24} = 16777216$
B	10	128-191	a.b	c.d	$2^{14} = 16384$	$2^{16} = 65536$
C	110	192-223	a.b.c	d	$2^{21} = 2097152$	$2^8 = 256$

oficinas o un campus universitario) comparten *algunos* dígitos de la dirección IP. En función de que la red sea más o menos amplia, se emplearán uno, dos o tres dígitos para identificar a cada uno de los equipos dentro de la red. Así, hablamos de tres *clases* de direcciones IP, que se enumeran en la **Tabla 4.1**.

La *máscara de red* es una dirección IP que permite determinar el ámbito de la red a la que pertenece un equipo. Dicha máscara permite dirigir o enrutar correctamente los paquetes. Por ejemplo, si uno de los dispositivos de la red tiene la dirección 192.168.0.1 y la máscara de red es:

11111111.11111111.11111111.00000000 = 255.255.255.0

El enrutador de dicha red entiende que todos los paquetes que se envíen a una dirección que comienza por 192.168.0 van dirigidos a la propia red local, y los que se envíen a cualquier otra van dirigidos hacia fuera de ella.

Actividad resuelta 4.1. Indica a qué clase pertenece cada una de las siguientes direcciones IP: (a) 122.56.1.60, (b) 193.20.47.35, (c) 142.23.49.50.

Solución. Podemos resolver este ejercicio fijándonos en la **Tabla 4.1**: (a) Clase A; (b) Clase C; (c) Clase B.

La **Figura 4.5** muestra un ejemplo sencillo de conexión de varios ordenadores en dos redes locales. Para comunicar entre sí las diversas redes se emplean dispositivos denominados encaminadores, enrutadores o *routers*; estos poseen dos o más direcciones IP, una por cada una de las redes a las que pertenecen. Fijémonos que, en la figura, el *router* posee las direcciones 192.168.1.1, 192.168.2.1 y la correspondiente «IP pública» asignada por el ISP para identificarla en Internet. Los encaminadores dirigen los paquetes IP a unas redes u otras en función de la dirección destino que esté indicada en su cabecera. Otro de los nodos actúa como pasarela de enlace predeterminada (*default gateway*), dispositivo al que se encaminan los paquetes que no van dirigidos a ninguno de los nodos de la red.

¿Sabías que...?

El desarrollo de Internet y el gran crecimiento de los dispositivos (no solo ordenadores de sobremesa, sino teléfonos inteligentes, tabletas, portátiles y mini-portátiles) que se conectan a la red ha provocado una creciente *sequía* de direcciones de Internet. Como respuesta a este reto surge el protocolo IPv6; las direcciones IPv6 están formadas por ocho grupos de cuatro dígitos hexadecimales. Así, por ejemplo, una dirección de este tipo tendría la forma:

```
2001:0db8:85a3:08d3:1319:8a2e:0370:7334
```

Frente a los poco más de cuatro mil millones de direcciones que soporta el protocolo de Internet versión 4 (IPv4), IPv6 admite 2^{128}, o sea, unos 340 sextillones de direcciones; con ese número se podrían asignar unos 670 mil billones de direcciones IP por cada milímetro cuadrado de superficie terrestre; con el desarrollo de este protocolo la sequía de IP queda definitivamente superada.

Direcciones IP fijas y dinámicas. En una red de datos (ya sea de ámbito local o la propia Internet), hay equipos que tienen una dirección IP asignada que no cambia con el tiempo. Por el contrario, hay otros cuya dirección es asignada dinámicamente por un servicio centralizado cuando el equipo se conecta a la red. Hablamos, así, de direcciones IP *fijas* y *dinámicas*.

En Internet, la mayor parte de los servidores que prestan servicios comerciales (servidores web, de correo, de archivos, etcétera) tienen asignada una IP fija, lo cual facilita la comunicación con ellos y la resolución

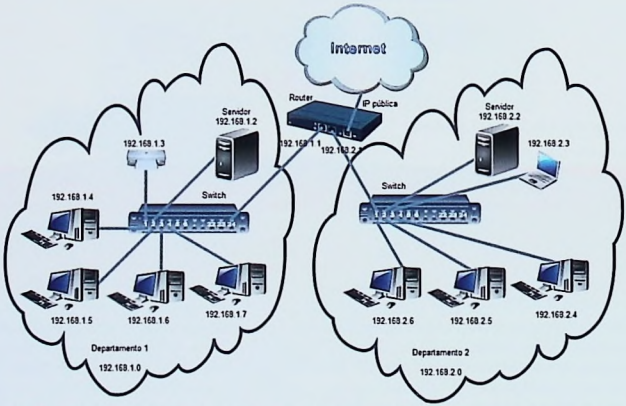


Figura 4.5. Dos redes de área local conectadas entre sí mediante un dispositivo enrutador. Cada equipo de la red, muestra la dirección IP asociada a él.

de sus nombres de dominio (cuestión que abordaremos enseguida). Sin embargo, debido a la «escasez» de direcciones IPv4, muchos proveedores de servicios de Internet (ISP) proporcionan a los usuarios domésticos y a algunas pequeñas empresas una IP dinámica, que puede cambiar cada vez que el equipo se conecta a la red. La asignación de una *IP fija* —que presenta ventajas para la conexión remota a los equipos de la red local o para el uso de la telefonía de voz sobre IP (VoIP)— conlleva normalmente un coste más elevado.



Figura 4.6. En las redes wi-fi públicas, la asignación centralizada de direcciones IP dinámicas permite que muchos equipos se conecten a la red simultáneamente sin que sea necesario otorgarles manualmente una IP y sin riesgo de que se presente una duplicidad de direcciones (es decir, que dos equipos tengan asignada la misma dirección IP).

En una red de área local podemos asignar a los equipos una dirección IP fija o dejar que sea un servidor central el que las asigne a través de un servicio denominado DHCP (*Dynamic Host Configuration Protocol*, Protocolo de Configuración Dinámica de Equipos). La ventaja de esta configuración en una red local es que ahorra el trabajo de asignación manual de las direcciones; sin embargo, es conveniente que ciertos equipos de la red local, como los servidores o las impresoras TCP/IP, tengan asignada una IP fija para facilitar la comunicación con ellos.

¿Sabías que...?

En las redes de tamaño pequeño, el servidor DHCP consiste en una aplicación *software* instalada en el propio *router*. En las Prácticas Profesionales veremos cómo configurarlo.

4.1.3. Resolución de direcciones IP

Además del protocolo IP, en la capa de Internet de TCP/IP existen dos protocolos que se emplean para traducir las direcciones IP a direcciones físicas y viceversa: son los denominados ARP (*Address Resolution Protocol*, Protocolo de Resolución de Direcciones) y RARP (*Reverse Address Resolution Protocol*, Protocolo de Resolución Inversa de Direcciones).

Siempre que un nodo necesita encontrar la dirección física de otro en su red, envía un paquete con una consulta ARP que incluye la dirección IP del nodo que está buscando. Todos los dispositivos de la red reciben y procesan el paquete, pero solo el destinatario reconoce la dirección IP como la suya propia y devuelve una respuesta indicando su dirección física.

A la inversa, el protocolo RARP permite a un dispositivo conocer su dirección IP enviando su dirección física. Se emplea, por ejemplo, cuando un ordenador se conecta por primera vez a la red. El ordenador enviará un paquete RARP con su dirección física a todos los nodos de la red, hasta que un servidor reconozca dicho paquete y envíe como respuesta la dirección IP que corresponde al ordenador recién conectado.

¿Sabías que...?

Además de los protocolos mencionados (IP, ARP y RARP), en la capa de Internet se define también el protocolo ICMP (*Internet Control Message Protocol*, Protocolo de Control de Mensajes de Internet); este se emplea como mecanismo para informar de errores en la entrega del datagrama. Si un nodo no es capaz de entregar un datagrama al destinatario (porque el enlace no funcione o el destinatario no responda), enviará un mensaje ICMP al remitente del datagrama informándole de ello.

Actividad propuesta 4.1

¿Qué es el protocolo IP? ¿Cuáles son sus principales funciones? ¿A qué capa del modelo OSI corresponde este protocolo? ¿En qué se diferencia una dirección IPv4 de una dirección IPv6?

4.2. La capa de transporte

Los protocolos de la capa de transporte proporcionan servicio de conexión a las aplicaciones de la capa superior. Se encargan de la transferencia de datos entre los nodos de la red que emiten y reciben información.

Los protocolos que se emplean en esta capa son TCP (*Transmission Control Protocol*, Protocolo de Control de Transmisión) y UDP (*User Datagram Protocol*, Protocolo de Datagrama de Usuario). En realidad, el primero de ellos es el más utilizado, pues proporciona los mecanismos necesarios para ordenar los paquetes o datagramas de la capa de Internet y comprobar que han sido recibidos correctamente. UDP, en cambio, no proporciona estos mecanismos, pero presenta la ventaja de su rapidez.

TCP es un protocolo *con conexión*. ¿Qué significa esto? El protocolo crea un *circuito virtual* entre ambos extremos de la comunicación, un circuito que permanece activo mientras dura la transmisión de los datos. Cuando se establece una conexión, se crea un canal de conexión bidireccional o *full-duplex* (concepto que hemos introducido en la Unidad 1 de este libro) en el que las aplicaciones de ambos nodos pueden enviar y recibir información. Una vez que la transmisión ha terminado, ambos extremos se ponen de acuerdo al respecto y la conexión se cierra.

Por el contrario, UDP es un protocolo *sin conexión*. Se usa en aplicaciones en las que la fiabilidad no es crítica y en las que esperar a que el destinatario de los segmentos envíe la confirmación de que ha recibido cada uno de ellos introduciría demasiados retardos en la transmisión de información.

Recuerda que...

TCP es un protocolo orientado a la conexión, que proporciona mecanismos para asegurarse de que el destinatario ha recibido correctamente los paquetes (segmentos) de información enviados. UDP es un protocolo sin conexión, pues envía los segmentos pero no incorpora mecanismos para asegurar que se han recibido correctamente; es menos fiable pero mucho más rápido que TCP.

Recordemos que IP es un protocolo *no fiable*. TCP sí lo es; su fiabilidad se basa en un sistema de reconocimiento de los mensajes o *segmentos* enviados. Por cada segmento que ha enviado, el remitente recibe una confirmación (ACK o *acknowledgement*); si esta no llega pasado cierto tiempo, se reenvía el segmento. Este mecanismo de envío y confirmación por segmentos se denomina *protocolo de ventana deslizante* (véase la **Figura 4.7**).

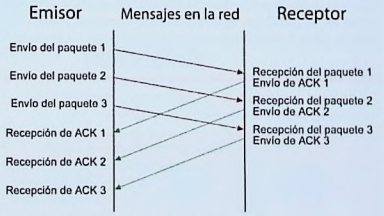


Figura 4.7. Protocolo de ventana deslizante.

Recuerda que...

A diferencia del protocolo IP, TCP es un protocolo fiable porque proporciona mecanismos para comprobar la integridad de los datos y su correcta recepción.

Tal como hemos visto anteriormente, la capa de Internet transmite los datagramas a través de la red entre el remitente y el destinatario identificándolos mediante sus *direcciones*. La capa de transporte añade un concepto adicional: el de *puerto*. Una misma máquina, definida por su dirección IP, puede recibir a través de la red paquetes de datos de muchas clases. El *puerto de comunicaciones* permite especificar diversos destinos dentro de un mismo equipo.

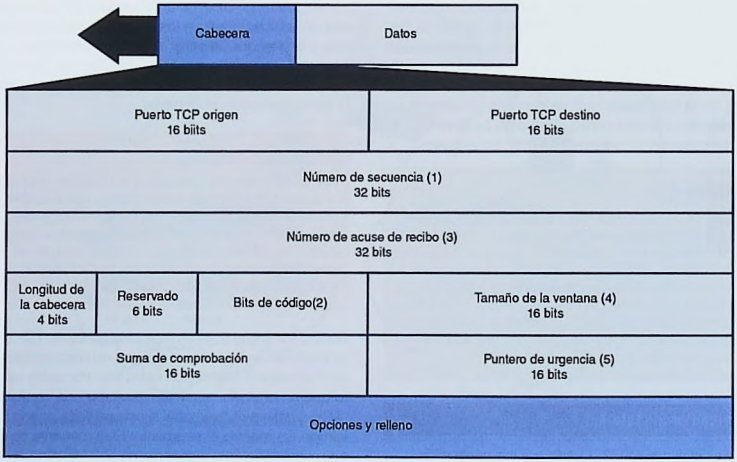


Figura 4.8. Formato del segmento de datos TCP. **Notas:** (1) Cuando la transmisión de datos se divide en varios segmentos, el **número de secuencia** permite reconstruir el mensaje original. (2) Los **bits de código** son seis bits que se emplean para definir el contenido y propósito del segmento (urgencia, acuse de recibo, reinicio de la conexión, etcétera). (3) El **número de acuse de recibo** indica el número del siguiente byte que el destinatario espera recibir; con ello se le indica al otro extremo de la comunicación que los bytes anteriores se han recibido correctamente. (4) El **tamaño de la ventana** define el tamaño de la ventana deslizante. (5) Si el segmento contiene datos urgentes, el **puntero de urgencia** indica su posición.

Actividad resuelta 4.2. ¿Cuáles son las ventajas y los inconvenientes del uso de TCP? ¿Y de UDP?

Solución. Como hemos estudiado en este apartado, el protocolo TCP es un protocolo fiable y con conexión; su cabecera es más extensa (contiene más datos) y el destinatario debe enviar un paquete de confirmación por cada segmento recibido. Estas características hacen de él un protocolo ideal para asegurar que la información llega a su destino íntegramente, pero a cambio las comunicaciones a través de TCP son lentas. Cuando deben transmitirse datos en tiempo real, minimizando los retardos (como ocurre en las comunicaciones de voz, que estudiaremos en la próxima Unidad), es habitual usar UDP, protocolo más sencillo y menos fiable, pero más rápido.

Actividad propuesta 4.2

¿En qué consisten los protocolos ARP y RARP? ¿A qué capa del modelo OSI corresponden? ¿Puede variar la dirección IP de un equipo con una determinada dirección física de red? ¿Cuál es la ventaja de la configuración de direcciones IP *dinámicas*?

4.3. La capa de aplicación

La capa de aplicación actúa como interfaz entre las aplicaciones de usuario instaladas en el equipo de la red y la capa de transporte. Por ejemplo:

- Cuando visualizamos una página web en nuestro navegador, la aplicación de usuario (Chrome, Firefox, Internet Explorer, etcétera) emplea los protocolos HTTP o HTTPS (en el caso de que se trate de una conexión *segura*) de la capa de aplicación.
- Cuando realizamos una transferencia de archivos a un servidor, la aplicación encargada de efectuar dicha transferencia (por ejemplo, FileZilla) emplea los protocolos FTP o SFTP de la capa de aplicación.
- Si descargamos el correo electrónico a través de un cliente de correo (Microsoft Outlook, Mozilla Thunderbird, etcétera) se emplean los protocolos POP o IMAP de dicha capa.
- Si efectuamos una conexión remota a otra máquina de la red local u otro equipo conectado a Internet, la aplicación de usuario puede emplear el protocolo SSH de dicha capa.

¿Sabías que...?

En los últimos tiempos se ha extendido enormemente el concepto de «informática en la nube» o *cloud computing*. Se usa para referirnos a ciertos recursos (como aplicaciones, almacenamiento de datos o entornos de desarrollo de programas) que se sirven a través de Internet, en lugar de estar ubicados en el equipo del propio usuario. Entre sus ventajas cabe citar el mayor aprovechamiento de los recursos y la posibilidad de acceder a ellos desde dispositivos muy diversos (ordenadores, tabletas, servidores, teléfonos, etcétera) y desde cualquier lugar del planeta que disponga de conexión a Internet.

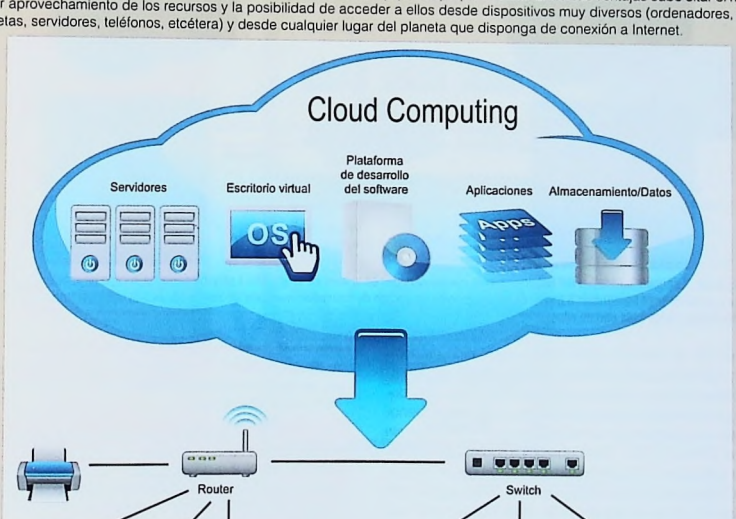


Figura 4.9. Esquema de funcionamiento del *cloud computing*.

Cada uno de estos protocolos emplea un puerto del equipo para enviar y recibir sus mensajes a través de la capa de transporte. La mayoría de las comunicaciones a través del protocolo TCP/IP se basan en el modelo *cliente-servidor*. Este último ofrece un servicio que los clientes solicitan a través de *peticiones*.

4.3.1. La resolución de nombres y los servidores DNS

Cuando se desea acceder a un determinado servicio de un equipo de la red, podemos identificarlo mediante su dirección IP y el puerto que está «escuchando» la aplicación que proporciona dicho servicio. Por ejemplo, podríamos visualizar el sitio web del Ministerio de Educación escribiendo en la barra de nuestro navegador la dirección: 193.147.0.112:80. Esta forma de comunicación, sin embargo, es engorrosa y poco práctica para los usuarios «humanos» de Internet; como sabemos, en lugar de direcciones IP, lo que solemos introducir en la barra de direcciones del navegador son *nombres de domino*.

¿Cómo sabe nuestro navegador de Internet a qué ordenador de la red debe efectuar la petición de la página web que hemos solicitado cuando introducimos en la barra de direcciones la URL **http://www.educacion.gob.es**? Existe

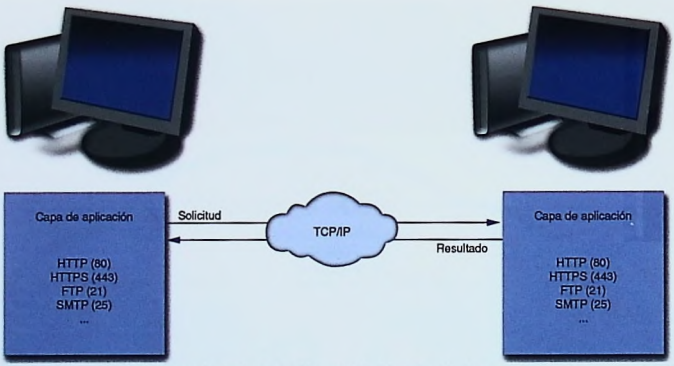


Figura 4.10. Esquema ilustrativo del funcionamiento cliente-servidor en el nivel de aplicación. Los protocolos de la capa de aplicación del cliente y el servidor se comunican a través de los protocolos de la capa de transporte mediante un puerto (se señala entre paréntesis el puerto predeterminado para cada uno de ellos).

un servicio de Internet, denominado *resolución de nombres*, que indica, para nombre de dominio, la dirección IP asociada a dicho nombre. En la red existen unos servidores que se dedican específicamente a esta tarea, denominados *servidores de nombres de dominio* o *Domain Name Servers* (DNS). Cada equipo conectado a Internet tiene asignados unos servidores de nombres a los que debe «preguntar», cada vez que introducimos un nombre de dominio en el navegador (o en otras aplicaciones que deban conectarse a Internet): ¿a qué dirección IP corresponde este nombre? Una vez que el servidor DNS responde a dicha solicitud, la capa de aplicación del equipo cliente puede ponerse en contacto con el equipo correspondiente empleando para ello su dirección IP.

¿Sabías que...?

La mayor parte de los servicios de la capa de aplicación emplean el protocolo TCP. Sin embargo, algunos, como el servicio para la resolución de nombres de dominio (DNS), envían sus datos a través de UDP.

¿Sabías que...?

Los proveedores de Internet proporcionan normalmente sus propios servidores de nombres, a los que se envían las solicitudes DNS de sus clientes. Existe también la posibilidad de emplear servicios de resolución de nombres *públicos*, como el que ofrece Google. Las direcciones IP de sus servidores DNS son 8.8.8.8 y 8.8.4.4.

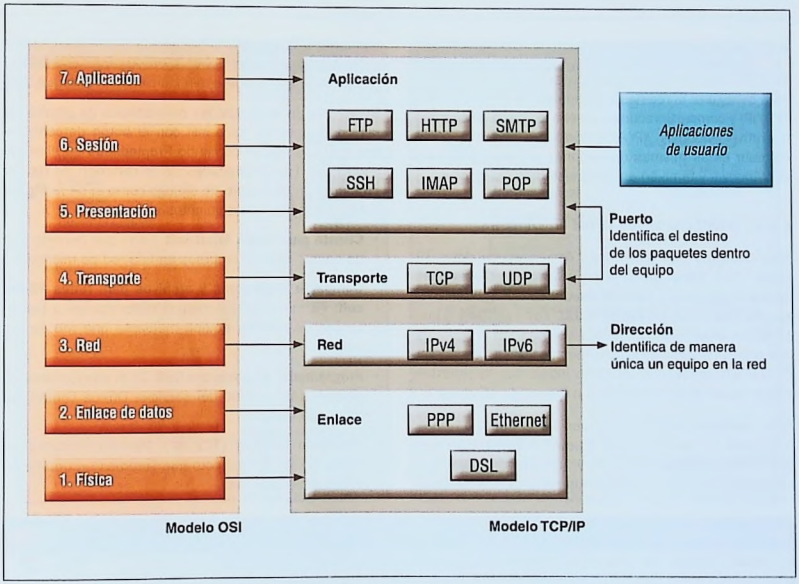
Actividad resuelta 4.3. ¿Qué protocolos se ponen en juego cuando accedemos a una página web? ¿A qué capa pertenece cada uno de ellos?

Solución. La «navegación» por la web conlleva una serie de procesos de intercambio de información bastante complejos que nos permiten ilustrar el modelo de capas. Imaginemos que accedemos a la página inicial de la Wikipedia escribiendo en la barra de direcciones de nuestro navegador:

http://www.wikipedia.org

En primer lugar, el cliente o agente de usuario (el navegador) efectúa una petición a la máquina identificada con el nombre de dominio wikipedia.org. Lo hace mediante un protocolo de la capa de aplicación, HTTP (*HyperText Transfer Protocol*, Protocolo de Transferencia de Hipertexto). El cliente establece una conexión en la capa de transporte a través del protocolo TCP con el servidor, concretamente con un puerto de él identificado por su número (generalmente el 80 para los documentos web). El paquete de datos se pasa a la capa de Internet, donde recibe la dirección (IP) de destino. El paquete viaja entonces a través de la capa física empleando diversos protocolos (Ethernet para redes LAN cableadas, PPP para módem telefónico o redes DSL). El paquete viaja a través de diversos routers de Internet hasta llegar a su dirección destino, donde emprende el camino opuesto hasta llegar a la capa de aplicación del servidor, que responderá a la petición HTTP enviando el código de aceptación y el texto en HTML de la página web solicitada.

Mapa conceptual



Práctica profesional

4.1. Windows XP

En esta práctica profesional analizaremos los métodos para configurar la red (las propiedades de los protocolos TCP/IP) y compartir recursos en ella mediante el sistema operativo Windows XP. Posteriormente veremos cómo efectuar estas mismas operaciones en otras versiones de Windows y también en otros sistemas operativos.

4.1.1. Configuración de la red en Windows

Para configurar las conexiones de red en Windows XP acudimos al **Panel de control** y a la opción **Conexiones de red**. Al hacerlo se abrirá el cuadro de diálogo **Conexiones de Red** (véase la **Figura 4.11**). Las conexiones que se hallan desactivadas o desconectadas (en la figura, la conexión de área local) están marcadas con un aspa roja. El candado amarillo en el icono indica que la conexión está empleando el cortafuegos o *firewall* de Windows.

Para visualizar las características de la conexión haremos doble clic sobre ella. En la pestaña **General** del cuadro de diálogo **Estado** visualizaremos sus características básicas. La pestaña **Soporte** nos mostrará, entre otros elementos, la dirección IP asignada al equipo *a través de dicha conexión*, así como la máscara de subred y la puerta de enlace predeterminada (véase la **Figura 4.12**).

Si se desean modificar las propiedades de alguna de las conexiones se hace clic con el botón derecho sobre ella y se elije el comando **Propiedades** en el menú contextual. Las propiedades de la conexión de red se muestran en un cuadro de diálogo como el de la **Figura 4.13**, que incluye los siguientes elementos:

- **Cliente para redes Microsoft**. Es el que permite que un equipo emplee recursos en una red de Microsoft.
- **Compartir impresoras y archivos para redes Microsoft**. Permite a otros equipos tener acceso a los recursos de nuestro equipo mediante una red de Microsoft.
- **Programador de paquetes QoS**. Es el programador de paquetes de calidad del servicio. Ofrece control del tráfico de la red.
- **Protocolo Internet (TCP/IP)**. Permite configurar el protocolo TCP/IP, aspecto que veremos en detalle en el siguiente apartado.

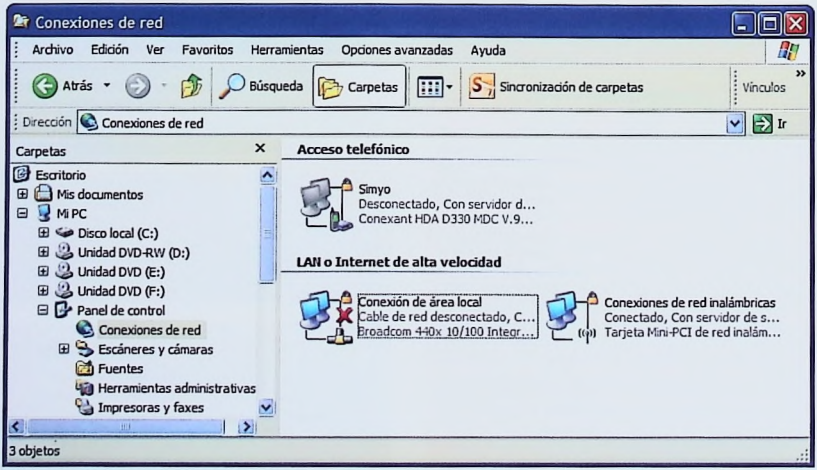


Figura 4.11. Conexiones de red en Windows XP.

Práctica profesional

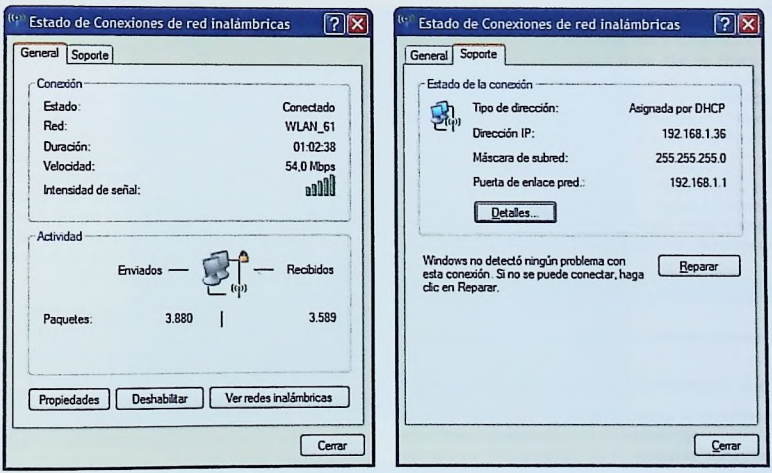


Figura 4.12. Estado de la conexión de red.

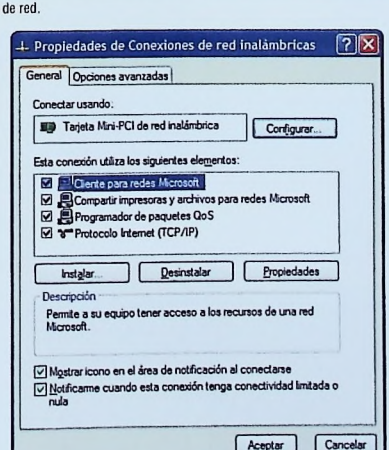


Figura 4.13. Propiedades de la conexión de red.

Práctica profesional

4.1.2. Configuración del protocolo TCP/IP

Para configurar el protocolo TCP/IP de una determinada conexión de red, se abren sus propiedades (tal como acabamos de ver), seleccionamos **Protocolo Internet (TCP/IP)** en el cuadro de diálogo **Propiedades de conexión** y hacemos clic en el botón **Propiedades**. Veremos entonces el cuadro de diálogo de la **Figura 4.14**.

Para visualizar información completa sobre las conexiones de red existentes y sus configuraciones actuales, podemos ejecutar el **Símbolo del sistema** de Windows (**Inicio** > **Todos los programas** > **Accesorios** > **Símbolo del sistema**). Una vez abierto, introducimos el comando:

```
ipconfig /all
```

El resultado de dicha acción se muestra en la **Figura 4.15**.

4.1.3. Comprobación de la respuesta de un equipo

El comando o utilidad **ping** se emplea para saber si un determinado equipo de la red responde y está listo para recibir paquetes IP. La comprobación se efectúa enviándole una solicitud a través del protocolo ICMP y esperando su respuesta. El proceso mide el tiempo que transcurre entre el envío de la solicitud y la recepción de la respuesta, y registra si se ha producido la pérdida de algún paquete.

En Windows XP se puede utilizar esta utilidad a través del **Símbolo del sistema**. Se puede «hacer ping» tanto a nodos de la red local como a equipos de Internet, identificados ya sea por su IP o bien por su nombre de dominio. En el caso de los equipos de la red local de Windows, los equipos se pueden identificar mediante su nombre. En la **Figura 4.16** se muestran tres ejemplos del uso de **ping**: a un equipo determinado por su nombre, a la puerta de enlace (definida por su dirección IP) y a un equipo de Internet definido por su nombre de dominio.

¿Sabías que...?

Si en el símbolo del sistema escribimos *ping localhost* o *ping 127.0.0.1*, estamos «haciendo ping» a nuestro propio equipo; pero, ¿qué interés puede tener saber si nuestro propio equipo está disponible? Si nuestro equipo no responde puede deberse a que la tarjeta de red esté estropeada o mal instalada, o a que Windows no sea capaz de comunicarse con ella.

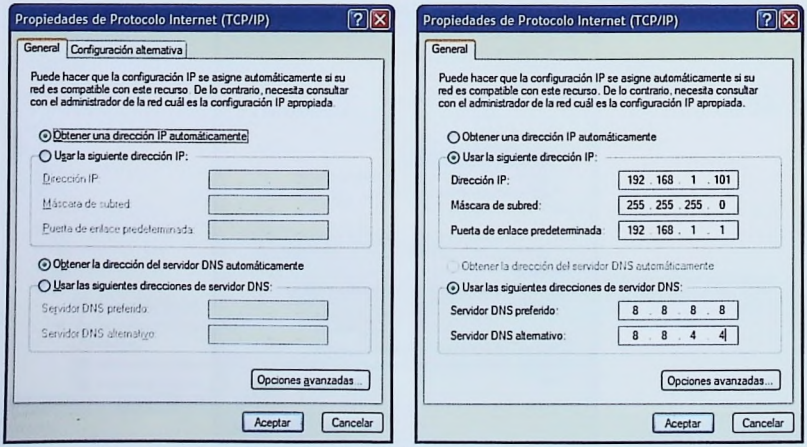


Figura 4.14. Configuración del protocolo TCP/IP. Configuración de IP dinámica e IP fija.

Práctica profesional

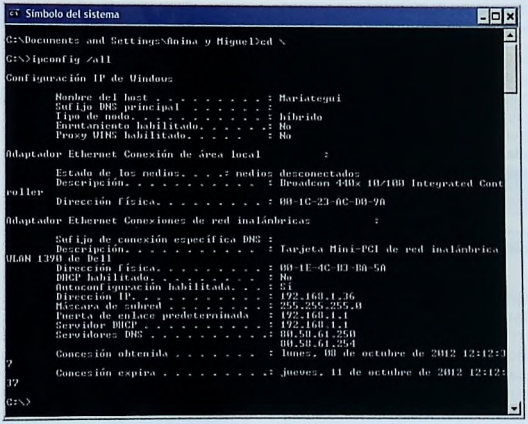


Figura 4.15. Visualización de las propiedades de la conexión de red a través del **Símbolo del sistema**.

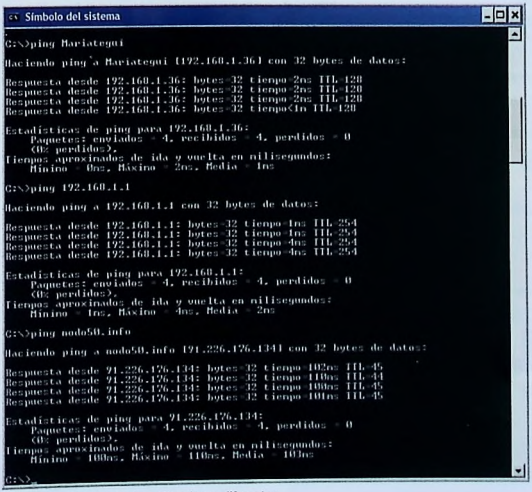


Figura 4.16. Respuestas del comando **ping** en tres situaciones diferentes.

Práctica profesional

Identificación del nombre del equipo y conexión a un grupo de trabajo

Windows emplea el concepto de **grupo de trabajo**, un conjunto de equipos en una red local que comparten diversos *recursos*. Cada equipo se identifica mediante un nombre. Para conocer el nombre del equipo en Windows XP y saber a qué grupo de trabajo pertenece podemos emplear las **Propiedades del sistema**. Podemos acceder a ellas de dos modos:

- Haciendo clic con el botón derecho del ratón sobre el icono **Mi PC**.
- Acudiendo al **Panel de control** y haciendo clic en **Sistema**.

En el cuadro de diálogo **Propiedades del sistema** (véase la **Figura 4.17**), haremos clic en la pestaña **Nombre de equipo**. En ella visualizamos el nombre del equipo y de la red. Para modificar su identificación, hacemos clic en el botón **Cambiar**. En el cuadro de diálogo **Cambios de nombre de equipo**, introduciremos el nuevo nombre del equipo y el del grupo de trabajo al que nos deseamos conectar. Para que los cambios tengan efecto debemos reiniciar nuestro ordenador.

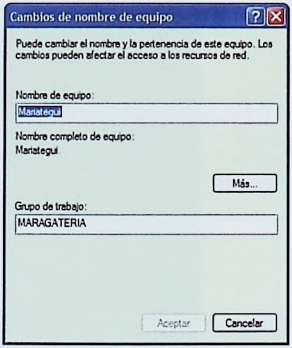
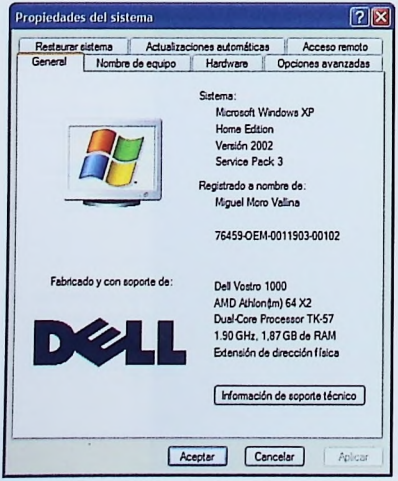


Figura 4.18. Cuadro de diálogo **Cambios de nombre de equipo**.

Examinar la red

Para examinar la red en Windows XP haremos clic en el icono **Mis sitios de red** del escritorio o emplearemos



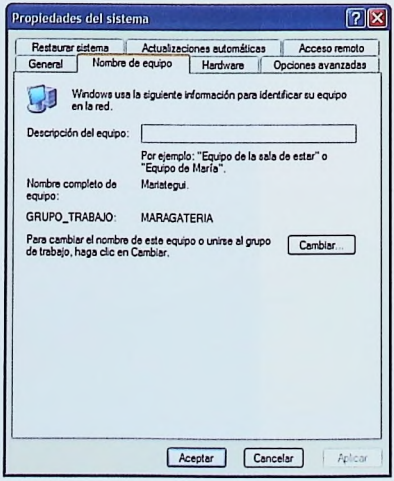


Figura 4.17. Cuadro de diálogo **Propiedades del sistema**. Pestañas **General** y **Nombre de equipo**.

Práctica profesional

el **Explorador de Windows**, haciendo clic a continuación en el elemento **Mis sitios de red**. En la columna izquierda de la ventana, hacemos clic en el enlace **Ver equipos del grupo de trabajo** (véase la **Figura 4.19**).

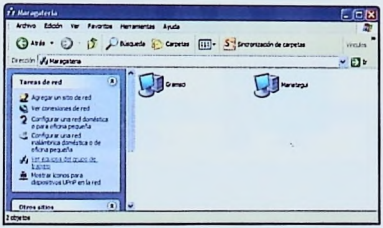


Figura 4.19. Visualización de los equipos del grupo de trabajo.

Al hacer doble clic en uno de los equipos de la red, visualizaremos sus recursos compartidos (carpetas o directorios, impresoras, unidades de disco, etcétera).

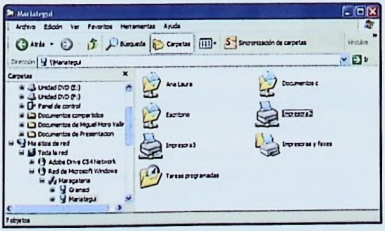


Figura 4.20. Recursos compartidos de uno de los equipos del grupo de trabajo.

4.1.4. Compartir recursos

Un equipo puede poner a disposición de su grupo de trabajo una carpeta de archivos, una unidad de disco o un periférico. A todos estos elementos los denominamos genéricamente *recursos*. Cuando se comparte un recurso, es posible especificar diversos niveles de permisos sobre él. Por ejemplo, los usuarios de la red pueden tener acceso de solo lectura a una carpeta o, por el contrario, pueden disponer de permisos para introducir en ella contenidos o para modificar o eliminar los archivos existentes.

Para compartir una carpeta en la red se accede a ella a través del **Explorador de Windows** y, haciendo clic con el botón derecho del ratón, se elige el comando **Compartir y seguridad** en el menú contextual. Se abre entonces un cuadro de diálogo como el de la **Figura 4.21**, en el que especificaremos el nombre del recurso en la red. Además, se podrá especificar el número máximo de usuarios que se podrán conectar simultáneamente a este recurso, así como los permisos sobre el recurso de cada uno de los usuarios de la red a través del botón **Permisos**.

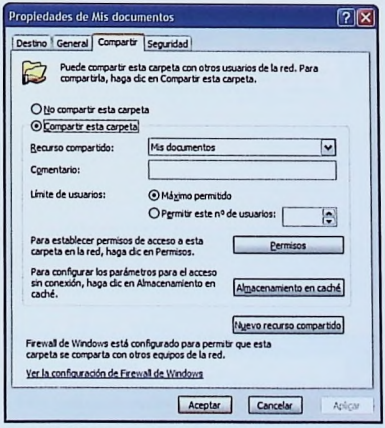


Figura 4.21. Pestaña **Compartir** del cuadro de diálogo **Propiedades del recurso**.

¿Sabías que...?

Para acceder a los recursos compartidos de un equipo, podemos hacer clic en el botón **Inicio**, comando **Ejecutar** y, a continuación, escribir el nombre del equipo precedido por dos barras invertidas, como muestra la **Figura 4.22**.

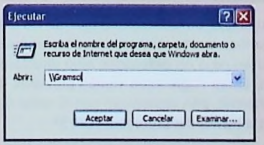


Figura 4.22. Acceso a los recursos compartidos de un equipo introduciendo su nombre en el cuadro **Ejecutar**.

Práctica profesional

Para compartir una impresora, accedemos a la lista de **Impresoras y faxes** a través del **Panel de control**, hacemos clic con el botón derecho sobre el icono de la impresora que deseemos compartir y, en el menú contextual, elegimos el comando **Compartir**. En el cuadro de diálogo de la **Figura 4.23**, elegimos la opción **Compartir esta impresora** y le asignamos el nombre con el que deberá mostrarse en la red este recurso.

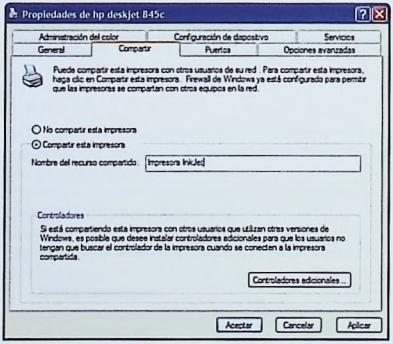


Figura 4.23. Compartir impresora en la red de Windows.

Por último, para compartir una unidad de disco externo, conectaremos dicha unidad a través del puerto USB y accederemos a **Mi PC**. Haciendo clic con el botón derecho del ratón sobre el icono del disco y eligiendo el comando **Compartir y seguridad**, aparecerá un cuadro de diálogo análogo al de la **Figura 4.21**. Previamente, es posible que Windows nos muestre un mensaje de advertencia recomendando que no se comparta la raíz de la unidad de disco duro.

4.1.5. Instalación de una impresora TCP/IP

En la actualidad, en las redes locales de los entornos de trabajo se han vuelto muy comunes las impresoras que se conectan no a un ordenador, sino directamente a la red local. Estas impresoras vienen provistas de una interfaz Ethernet, y se comunican con el resto de equipos de la red a través del protocolo TCP/IP.

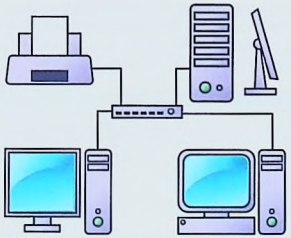


Figura 4.24. Las impresoras TCP/IP se pueden conectar directamente a la red local a través del *switch* o el concentrador (*hub*).

Para instalar en la red una impresora TCP/IP, es preciso conectarla e instalarla antes en un ordenador para poderla configurar. El proceso para hacerlo es el siguiente:

1. En primer lugar, conectamos la impresora al equipo y a la red eléctrica y la encendemos.
2. Accedemos al apartado **Impresoras y faxes** del **Panel de control**.
3. En el menú **Archivo**, elegimos el comando **Agregar impresora**. Con ello se abrirá el **Asistente para agregar impresoras** de Windows XP. Hacemos clic en el botón **Siguiente**.
4. En el apartado **Impresora local o de red**, seleccionamos la opción **Impresora local conectada a este equipo**. Hacemos clic en **Siguiente**.
5. En el apartado **Seleccionar un puerto de impresora** (véase la **Figura 4.25a**), seleccionamos la opción **Crear nuevo puerto** y, en el menú desplegable **Tipo de puerto**, elegimos la opción **Standard TCP/IP Port**.
6. Al pulsar el botón **Siguiente**, aparecerá un asistente para agregar un puerto de impresora TCP/IP. Tras pulsar de nuevo el botón **Siguiente**, deberemos especificar la dirección IP de la impresora mediante el cuadro de la **Figura 4.25b**. Dicha dirección puede obtenerse de la documentación técnica de la misma. En otros casos, aparece en la página de prueba que se imprime mediante una combinación de botones específica para cada impresora.
7. Es posible que, transcurridos unos segundos, Windows muestre el cuadro de diálogo **Se requiere información adicional sobre puertos**. En ese caso,

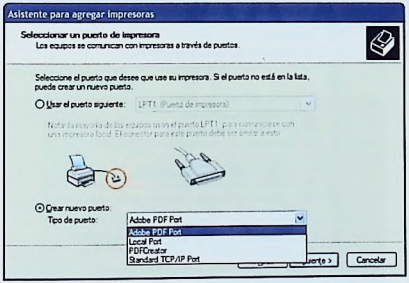
Práctica profesional

seleccionaremos la opción **Generic Network Card** y hacemos clic en **Siguiente**. Con ello finalizará el asistente para agregar el puerto TCP/IP.

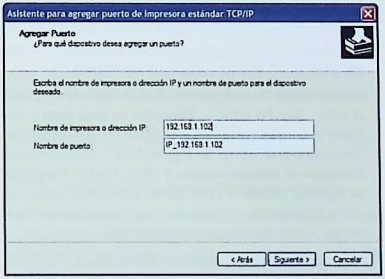
8. El siguiente paso consiste en instalar la impresora empleando sus drivers originales o seleccionándola de la lista de impresoras predefinidas en Windows.

9. Por último, se puede establecer la impresora como recurso compartido (aunque no es imprescindible hacerlo, puesto que nos comunicaremos con ella mediante TCP/IP) y se imprime (si lo deseamos) una página de prueba. Con ello finaliza el asistente.

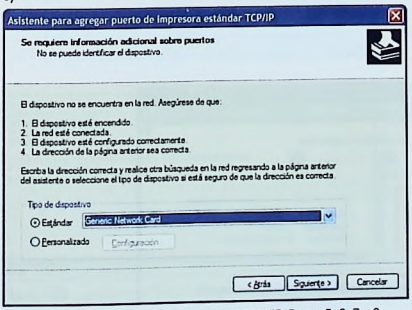
a)



b)



c)



d)

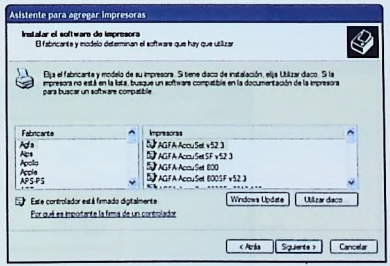


Figura 4.25. Instalación de una impresora TCP/IP. Pasos 5, 6, 7 y 8.

Práctica profesional

4.2. Windows 7

Las operaciones que hemos detallado para Windows XP son muy similares en la versión Windows 7. Mencionaremos brevemente cómo acceder a cada una de las configuraciones:

- Para la configuración de las conexiones de red, acudiremos al **Panel de control** y al **Centro de redes y recursos compartidos**. En esta ventana (véase la **Figura 4.26**) veremos las redes activas.
- Para modificar la configuración de la conexión de red se hace clic en el enlace **Cambiar configuración del adaptador**, en el panel izquierdo de la ventana.
- Para modificar la configuración TCP/IP hacemos clic con el botón derecho sobre la **Conexión de área local** y elegimos el comando **Propiedades**. En el cuadro de diálogo correspondiente (véase la **Figura 4.27**), seleccionamos **Protocolo de Internet versión 4 (TCP/IPv4)** o **Protocolo de Internet versión 6 (TCP/IPv6)** y hacemos clic en el botón **Propiedades**. El resto de la configuración se efectúa del mismo modo que en Windows XP.
- Para abrir la ventana **Símbolo del sistema**, hacemos clic en el botón **Inicio**. En el cuadro de búsqueda, escribimos **Símbolo del sistema** y, a continuación, en la lista de resultados, hacemos clic en **Símbolo del sistema**. En la ventana podemos ejecutar los mismos comandos que hemos estudiado para Windows XP.
- Para examinar la red y buscar los equipos conectados a ella hacemos doble clic en **Equipo** y entramos en el apartado **Red.**
- Para acceder a los recursos compartidos de un equipo determinado escribimos su nombre precedido de dos barras invertidas en el cuadro **Buscar programas y archivos** del menú **Inicio**.

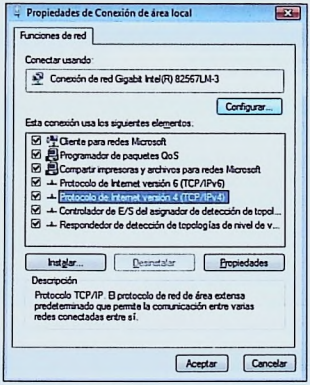


Figura 4.27. Propiedades de conexión de red en Windows 7.

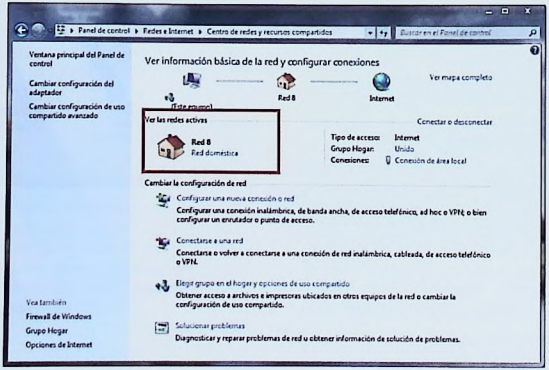


Figura 4.26. Centro de redes y recursos compartidos en Windows 7.

Práctica profesional

4.3. GNU/Linux

En esta práctica profesional abordaremos los métodos para la configuración de la red en Debian, una de las distribuciones más conocidas y extendidas de GNU/Linux.[1] Veremos cómo se configura la red en línea de comandos, un método de trabajo menos intuitivo pero más versátil que el de los entornos gráficos de usuario que encontramos en Microsoft Windows y en los gestores de ventanas de otros sistemas operativos. Es posible, además, que los equipos GNU/Linux que debamos configurar no tengan instalado ningún gestor de ventanas, o que debamos acceder a ellos remotamente, con lo cual el uso de la línea de comandos será imprescindible.

¿Sabías que...?

El proyecto GNU fue iniciado en 1984 por Richard Stallman para desarrollar un sistema operativo tipo UNIX compuesto enteramente por piezas de *software libre*. En la actualidad se distribuyen muchas de sus aplicaciones, bibliotecas y herramientas de desarrollo conjuntamente con el núcleo denominado *Linux* (obra de Linus Torvalds, que publicó su primera versión en 1991), formando así el sistema operativo *GNU/Linux*. La *Free Software Foundation* proporciona cobertura legal y económica al proyecto GNU (más información en **http://www.gnu.org**).

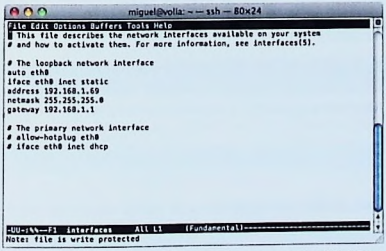


Figura 4.28. Edición de un fichero de texto en un servidor GNU/Linux con el editor emacs, a través de una conexión remota efectuada desde un sistema operativo Mac OS X mediante el protocolo SSH.

Para la configuración de la red en GNU/Linux será preciso editar varios archivos con privilegios de superusuario o administrador. Para hacerlo podemos emplear cualquiera de los editores de texto instalados en el sistema operativo, como **nano**, **vi** o **emacs**.

4.3.1. Cambio del nombre del equipo o *host*

El nombre de equipo en un sistema GNU/Linux se almacena en el archivo **/etc/hostname**. Para visualizarlo escribiremos en el *prompt* del sistema:

```
cat /etc/hostname
```

Para modificar el nombre del *host* editaremos el archivo **/etc/hostname** con privilegios de superusuario y ejecutaremos el siguiente *script* para que se haga efectivo:

```
/etc/init.d/hostname.sh
```

4.3.2. Identificación de las interfaces de red

Para ver todas las interfaces de red instaladas en el equipo y las características de cada una de ellas emplearemos el siguiente comando, cuya salida se muestra en la **Figura 4.29** (observa que se han adquirido privilegios de superusuario mediante el comando **su** antes de ejecutar **ifconfig**):

```
ifconfig -a
```

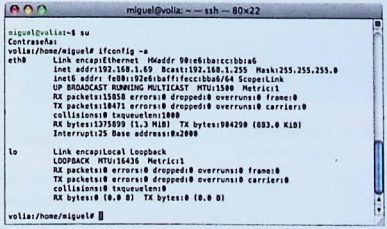


Figura 4.29. Interfaces de red en GNU/Linux.

4.3.3. Cambios en la configuración de red

Para modificar la configuración de red de nuestro equipo podemos emplear el propio comando **ifconfig**. Por ejemplo, el comando:

```
ifconfig eth0 10.0.0.100 netmask 255.255.255.0
```

[1] Ubuntu y Mint son, en la actualidad, las dos distribuciones de GNU/Linux más utilizadas. Ambas están basadas en Debian, con lo que los métodos de configuración que estudiaremos en este apartado también son válidos para ellas.

asigna la dirección IP (estática 10.0.0.100) a la interfaz de red denominada **eth0** y configura para ella la máscara de red 255.255.255.0. Para especificar la puerta de enlace predeterminada (dirección IP 10.0.0.1) de dicha interfaz de red, escribiremos:

```
route add default gw 10.0.0.1 eth0
```

Las modificaciones efectuadas mediante estos comandos son *temporales* y se pierden cuando se apaga o se reinicia el equipo. Para especificar la configuración de red de manera permanente deberemos editar el archivo **/etc/network/interfaces**. En él escribiremos la siguiente secuencia, dependiendo de si deseamos configurar una dirección IP fija o dinámica:

Dirección IP fija	Dirección IP dinámica
auto eth0	auto eth0
iface eth0 inet static	iface eth0 inetdhcp
address 192.168.1.69	
netmask 255.255.255.0	
gateway 192.168.1.1	

Para configurar los servidores DNS editaremos el archivo **/etc/resolv.conf**. En este archivo podemos obsevar, a modo de ejemplo, las siguientes líneas de texto:

```
nameserver 8.8.8.8
nameserver 8.8.4.4
```

4.3.4. Comprobación de la respuesta de un equipo

Al igual que hemos visto en el caso de Windows XP, desde el símbolo del sistema de GNU/Linux podemos emplear el comando **ping** para saber si un equipo está accesible a través de la red. El comando permanece «haciendo ping» indefinidamente al equipo que le hemos indicado; por tanto, pasado cierto tiempo de respuesta deberemos cancelar su ejecución mediante la combinación Ctrl + C. Su respuesta se muestra en la **Figura 4.30**. Para comprobar la dirección IP asociada a un determinado nombre de dominio podemos emplear también el comando **nslookup**, seguido del nombre de dominio que deseemos «resolver».

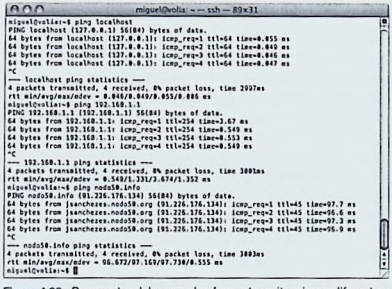


Figura 4.30. Respuestas del comando **ping** en tres situaciones diferentes: al propio equipo (localhost), a otro equipo de la red definido por su IP (en este caso, a la puerta de enlace predeterminada) y a un *host* definido por su nombre de dominio.

4.3.5. Configuración de un servidor SSH

El protocolo SSH permite controlar remotamente un equipo. Así, por ejemplo, un servidor de archivos de la red local no precisará más que la conexión a Internet, sin necesidad de periféricos de entrada ni salida. A través de cualquier ordenador de la red local (o de fuera de ella, como veremos más adelante) podremos acceder al equipo y administrarlo a través de la línea de comandos de GNU/Linux.

Para instalar un servidor SSH en nuestro sistema GNU/Linux debemos instalar el paquete **openssh-server**. Lo haremos ejecutando el siguiente comando:

```
apt-get install openssh-server
```

Para ajustar los parámetros de configuración del servidor editaremos el archivo **/etc/ssh/sshd_config.**

4.3.6. Configuración de un servidor FTP

El protocolo FTP es un protocolo de la capa de aplicación TCP/IP para la transferencia de ficheros entre ordenadores. Opera, al igual que otros protocolos de dicha capa, según un modelo *cliente-servidor*, con un componente en el servidor que está continuamente «escuchando» a través del puerto correspondiente, esperando posibles solicitudes de clientes.

Práctica profesional

Para instalar un servidor FTP en un sistema GNU/Linux podemos emplear el paquete **vsftpd**:

```
apt-get install vsftpd
```

En su configuración predeterminada, el paquete solamente permite las conexiones a través de FTP *anónimo*, es decir, que cualquier cliente se conecte al equipo y descargue los ficheros de un determinado directorio. Esta configuración es útil para determinados servidores públicos que ofrecen aplicaciones de código abierto, documentos de libre acceso o datos estadísticos. En otros casos, deberemos ajustar la configuración del servidor para permitir que solo determinados usuarios, a través de su nombre y contraseña, puedan acceder al equipo y descargar (o subir) archivos y carpetas a su directorio personal. Para ello debemos editar el archivo **/etc/vsftpd.conf** y «des-comentar» (eliminar el carácter # para habilitarlas) las siguientes líneas:

```
local_enable=YES
write_enable=YES
```

A continuación, deberemos reiniciar el servidor FTP para que los cambios tengan efecto, mediante el comando:

```
/etc/init.d/vsftpd restart
```

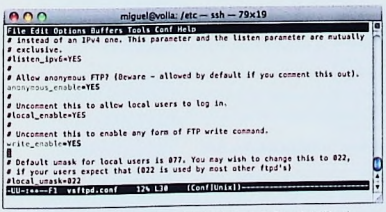


Figura 4.31. Edición del archivo **/etc/vsftpd.conf**. Para habilitar la opción **write_enable**, se elimina el símbolo de comentario (#) situado al comienzo de dicha línea de código.

4.3.7. Redes mixtas GNU/Linux-Windows

Es frecuente que en una red local existan equipos que trabajen con diversos sistemas operativos. De este modo se aprovechan las ventajas que proporciona cada uno de ellos. En este tipo de redes, se precisan mecanismos que aseguren la compatibilidad entre los distintos sistemas. Veremos cómo compartir un directorio de nuestro sistema GNU/Linux en un grupo de trabajo de Windows y viceversa, es decir, cómo trabajar desde Debian con recursos compartidos del grupo de trabajo de Windows.

En primer lugar, deberemos instalar el paquete *samba*:

```
apt-get install samba
```

En el proceso de instalación, es posible que una pantalla como la de la **Figura 4.32** nos pregunte con qué grupo de trabajo deseamos compartir archivos. Para configurar el servidor Samba, deberemos editar el archivo **/etc/samba/smb.conf**. En las primeras líneas del mismo veremos el nombre del grupo de trabajo que hemos indicado en la instalación de Samba:

workgroup = MARAGATERIA

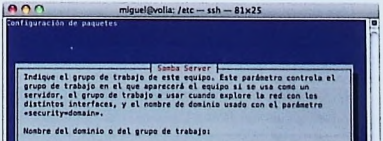


Figura 4.32. Pantalla de configuración de Samba para la especificación del nombre del grupo de trabajo.

En dicho archivo, para el recurso compartido se declaran su nombre y una serie de características. Lo ilustraremos con el siguiente ejemplo: para crear un recurso compartido denominado **compartido** en el grupo de trabajo, escribiremos al final del archivo:

```
[compartido]
comment = directorio compartido de Debian Linux
path = /home/compartido
browsable = yes
readonly = no
validusers = @users
```

Práctica profesional

A este recurso, el directorio **/home/compartido**, tendrán acceso todos los usuarios de Samba. Una vez que accedan a él, podrán explorarlo mediante el **Explorador de Windows (browsable=yes)** y tendrán permisos de escritura sobre él (**readonly=no**).

Además de añadir este bloque de instrucciones, en el archivo **/etc/samba/smb.conf** deberemos ajustar la configuración de seguridad des-comentando la línea:

```
security = user
```

en el caso de que esté comentada. Tras guardar el archivo, crearemos el directorio **/home/compartido** (en el caso de que no lo hubiéramos creado ya), especificaremos que su propietario es el usuario **nobody** y reiniciaremos Samba:

```
mkdir /home/compartido
chown nobody.nogroup /home/compartido
/etc/init.d/samba restart
```

Una vez efectuadas estas acciones, deberemos crear los usuarios de Samba que tendrán acceso al recurso compartido que hemos creado. Lo efectuaremos mediante el comando **smbpasswd**. Al ejecutarlo, el sistema nos pedirá que introduzcamos la nueva contraseña del usuario especificado:

```
smbpasswd -a miguel
```

Tras ello, desde cualquier equipo Windows conectado al grupo de trabajo especificado podremos conectarnos al recurso compartido introduciendo el nombre de usuario y la contraseña que hemos especificado mediante **smbpasswd** (véase la **Figura 4.33**).



Figura 4.33. Cuadro de diálogo para el acceso al recurso compartido del servidor Samba.

4.4. Configuración del *router*

Trataremos en este apartado algunos aspectos de la configuración del *router* relativos a las capas de red y de transporte. Lo haremos, a modo de ejemplo, con un *router* ADSL de la marca Zyxel. Cada fabricante proporciona unas interfaces específicas para el acceso a las funciones del *router*, aunque todas ellas tienen bastantes similitudes. Para configurar un modelo determinado, conviene siempre remitirse al manual de instrucciones del fabricante.

4.4.1. Configuración DHCP

La **Figura 4.34** muestra la configuración básica del servidor DHCP del *router*. Para detener el servicio DHCP seleccionaríamos el valor **None** en la lista desplegable **DHCP**. También podemos indicar el valor de la IP a partir de la cual se asignarán direcciones y los servidores DNS del *router*; estos servidores serán los que emplearán los equipos conectados a la red local si no se les especifican otros explícitamente. Notemos también que en este apartado podremos modificar la dirección IP del *router* y la máscara de subred de nuestra LAN.

La **Figura 4.35** muestra las direcciones IP que ha asignado el *router* a los equipos de la red que han solicitado una IP dinámica, junto con su nombre y su dirección física.

4.4.2. Configuración NAT

NAT (*Network Address Translation*, Traducción de Direcciones de Red) es un proceso para dirigir los paquetes que atraviesan un *router* a uno de los equipos de la red local. Típicamente, un *router* está conectado a la red local y a Internet, y posee una dirección IP en el espacio de direcciones de la LAN y otra IP asignada por el ISP que permite identificarlo en Internet. Cuando los equipos de la LAN efectúan peticiones a un equipo conectado a Internet, el *router* debe saber cuál de los equipos de la LAN ha efectuado dicha petición para poder encaminar el paquete de respuesta a dicho equipo.

Práctica profesional

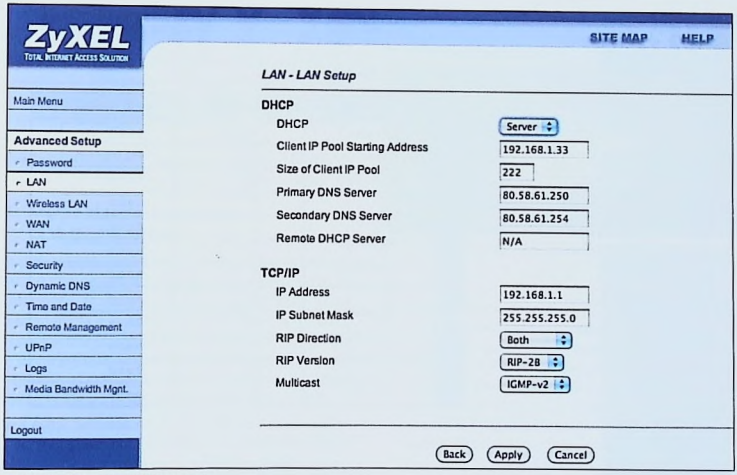


Figura 4.34. Configuración DHCP del *router*.

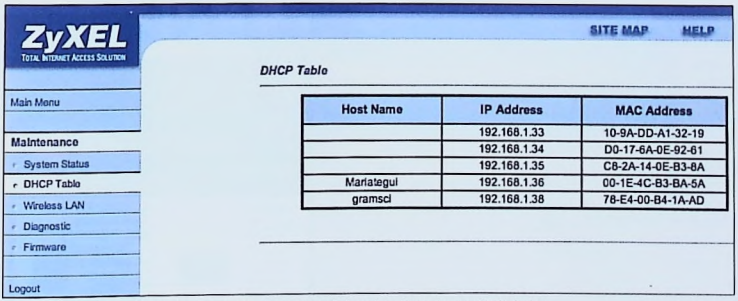


Figura 4.35. Tabla de asignación de direcciones IP a los equipos de la red configurados con IP dinámica.

Imaginemos una red local de diez ordenadores; entre ellos, hay un equipo configurado como servidor web y servidor FTP; deseamos que este equipo (con IP 192.168.1.69, por ejemplo) esté accesible desde fuera de la red local. En Internet, para acceder a dicha LAN debemos emplear la IP pública del *router* (por ejemplo, 80.120.34.3). A través de la configuración NAT, le indicaremos a este que encamine los paquetes dirigidos a los puertos 21 (FTP) y 80 (HTTP) de la dirección 80.120.34.3 al equipo de la LAN con dirección 192.168.1.69; en el *router* que estamos configurando a modo de ejemplo, esta asignación se efectuaría del modo indicado por la **Figura 4.36**.

Práctica profesional

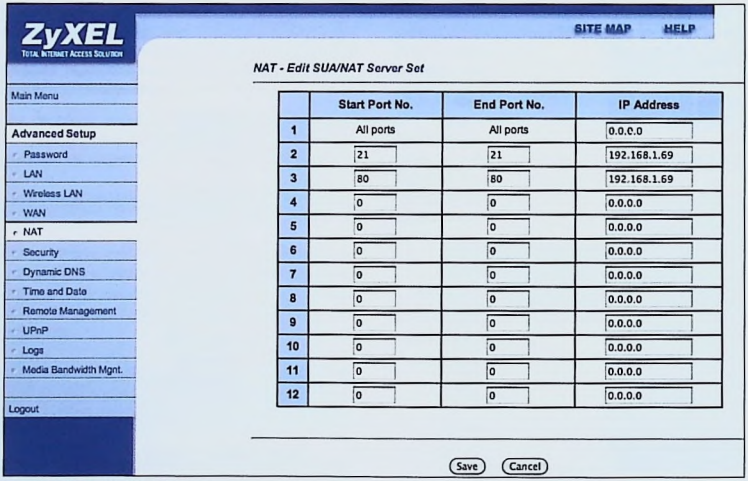


Figura 4.36. Configuración NAT del *router*.

¿Sabías que...?

Los servicios DNS dinámicos son una forma de asignar en tiempo real un nombre de dominio fijo a una dirección IP dinámica de Internet. Uno de estos servicios, No-IP, es gratuito para uso personal; el servicio nos permite asignar a nuestro equipo un nombre de dominio propio o un nombre del tipo **equipo.no-ip.org**. Para su configuración deberemos instalar una aplicación en nuestro equipo que le indique en cada momento al servicio cuál es la IP pública de nuestro ordenador (en el caso de que se conecte directamente a Internet) o de nuestro *router*.

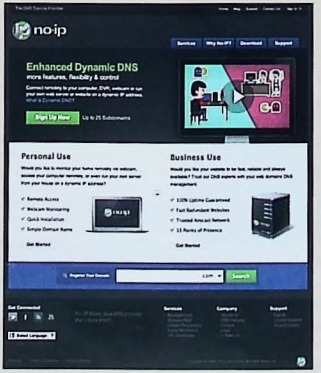


Figura 4.37. Página de inicio de No-IP.

Práctica profesional

4.5. Configuración de una red inalámbrica

En la Unidad 2 de este libro introdujimos las redes inalámbricas y estudiamos algunas de sus características y aplicaciones. En esta práctica aprenderemos a configurar el *punto de acceso inalámbrico*. La función de este dispositivo es la conexión de los equipos Wi-Fi y su integración con el resto de la red local. En las redes domésticas o de muy pequeño tamaño, es frecuente que el punto de acceso se halle integrado en el propio modem-router.

4.5.1. Acceso al router y activación de la red inalámbrica

1. En primer lugar, accedemos a la interfaz web del *router* o punto de acceso introduciendo en la barra de direcciones de nuestro navegador la dirección IP correspondiente a la *puerta de enlace predeterminada*. La página nos solicitará la introducción de un nombre de usuario y una contraseña; para obtenerlas nos remitiremos al manual del fabricante. En nuestro caso (véase la **Figura 4.38**), ambos datos son «1234».
2. Para evitar accesos no autorizados al *router* inalámbrico, es conveniente modificar la contraseña predeterminada y sustituirla por una más segura. En nuestro ejemplo, lo haremos mediante el menú **Access control > Passwords** (véase la **Figura 4.39**).

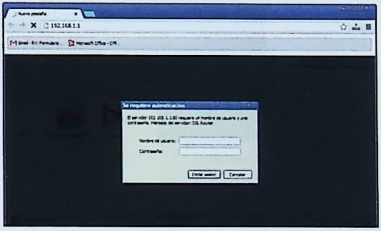


Figura 4.38. Acceso al router inalámbrico.

3. Para activar o desactivar la red inalámbrica acudiremos al menú correspondiente del punto de acceso; en nuestro caso, la operación se efectúa en el menú **Wireless > Basic** (véase la **Figura 4.40**). En este apartado también podemos visualizar el identificador (*Service Set Identifier* o SSID) de la red inalámbrica y el BSSID, que corresponde a la dirección MAC del punto de acceso. El primero, como podemos observar en la **Figura 4.40**, puede modificarse libremente, mientras que el segundo ha sido establecido por el fabricante.

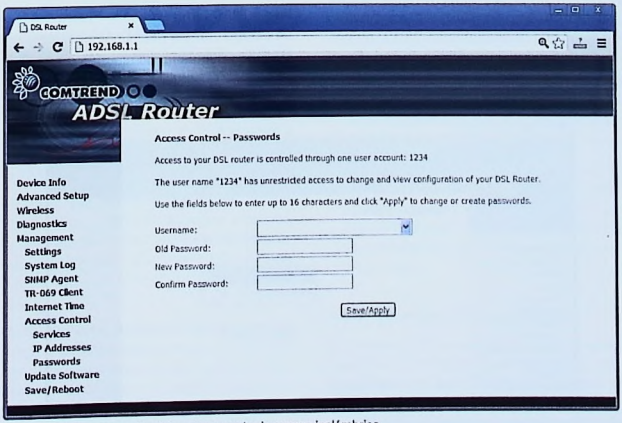


Figura 4.39. Modificación de la contraseña del router o punto de acceso inalámbrico.

Práctica profesional

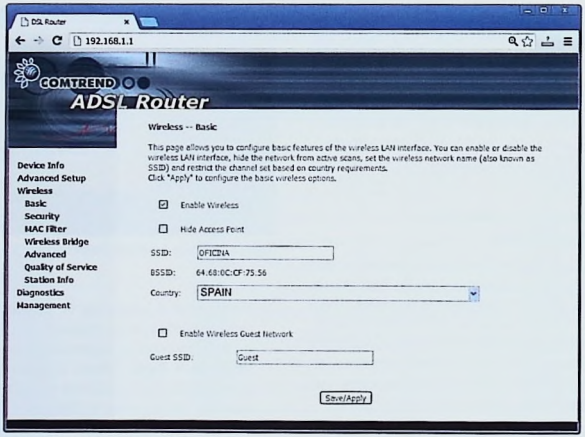


Figura 4.40. Configuración básica de la red inalámbrica.

4.5.2. Configuración del filtrado por MAC

Como hemos comentado en la Unidad 2, no se trata de un método infalible para garantizar la seguridad de nuestra red inalámbrica, pero constituye un mecanismo que, en combinación con la encriptación WPA2, proporciona un nivel de seguridad *razonable* a la red. En el punto de acceso que estamos configurando a modo de ejemplo, introduciremos las direcciones MAC que deseamos *permitir* en nuestra red mediante el menú **Wireless > MAC Filter** (véase la **Figura 4.41**). Aquí veremos un listado con las direcciones actualmente habilitadas, pudiendo asimismo eliminarlas o añadir otras nuevas.



Figura 4.41. Seguridad en la red inalámbrica. Filtrado por MAC.

Práctica profesional

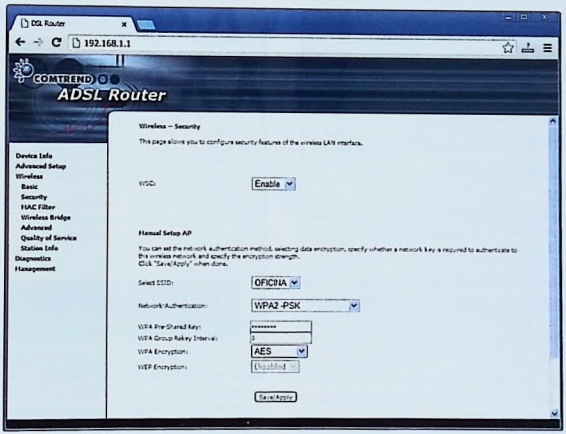


Figura 4.42. Configuración de seguridad en el punto de acceso.

4.5.3. Seguridad en la red inalámbrica

En la Unidad 2 (Apartado 2.1.2) insistimos en la importancia de establecer un nivel de seguridad adecuado en nuestra red inalámbrica. En nuestro caso, configuraremos la red con un nivel de seguridad WPA2 en el apartado **Wireless > Security** (véase la **Figura 4.42**). Los elementos que se pueden configurar en este apartado son los siguientes:

- WPS (*Wi-Fi Protected Setup*) o WSC (*Wi-Fi Simple Config*) es un estándar que facilita la puesta en marcha de la red inalámbrica, especialmente en entornos domésticos. Se han publicado una serie de vulnerabilidades de este método, por lo que hay quienes desaconsejan su uso para la configuración de redes inalámbricas.
- En el apartado **Network Authentification** (Autentificación de red) especificaremos el tipo o modo de seguridad que deseamos emplear. En nuestro caso, se elige el modo «WPA2-PSK» (o «WPA2-Personal»), diseñado para el uso doméstico o en pequeñas empresas.
- La clave o **Pre-Shared Key** es la clave que usarán los equipos para conectarse a la red. Se entiende que dicha clave será proporcionada a los usuarios a través de un medio seguro; el algoritmo WPA2 encriptará dicha clave para crear otra de 256 bits. A pesar de la robustez del algoritmo de encriptación, la seguridad de la red depende poderosamente de la elección de una contraseña segura, que cuente con números, letras y símbolos.
- En el apartado **WPA Encryption** (Encriptación WPA) especificamos cómo se codifica la clave encriptada. En este apartado existen varias opciones (AES, TKIP y AES+TKIP); AES aporta más seguridad que TKIP y la combinación de AES+TKIP es la opción más segura de las tres.

4.5.4. Conexión del equipo a la red

En Windows XP, si disponemos de un adaptador de red operativo y correctamente instalado, en el apartado **Conexiones de red** del **Panel de control** observaremos (véase la **Figura 4.43**) el icono de la (o las) conexiones de red Wi-Fi que tengamos habilitadas.

Prácticas profesionales



Figura 4.43. Conexiones de red de Windows y presencia entre ellas de una conexión de red inalámbrica.

Cuando se instala un adaptador de red, este normalmente añade al equipo su propio *software* para la gestión del adaptador y la conexión a redes inalámbricas. Al acceder a él (en el área de notificación de Windows dispondremos de un icono a tal efecto), podremos conectarnos a una de las redes disponibles (véase la **Figura 4.44**) o comprobar el estado del enlace (véase la **Figura 4.45**), entre otras operaciones.

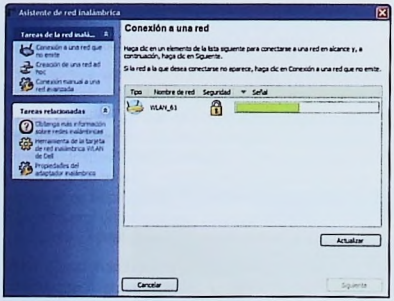


Figura 4.44. Conexión del equipo a una red inalámbrica disponible. La presencia del candado indica que dispone de un mecanismo de encriptación (o, en el argot, que está «cerrada»); también podemos comprobar la potencia de la señal de la red.

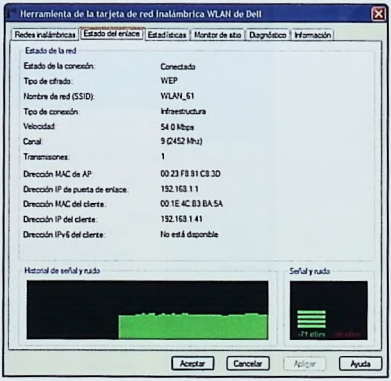


Figura 4.45 Herramienta de gestión del adaptador de red inalámbrico. Comprobación de las características de la red y la potencia del enlace.

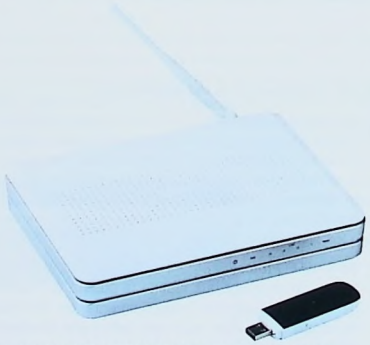


Figura 4.46. Punto de acceso inalámbrico y adaptador USB.

Cuestiones

4.1. La dirección IP 65.70.98.50, ¿a qué clase pertenece?

a) A la clase A.

b) A la clase B.

c) A la clase C.

d) Con la información de la dirección IP no podemos deducir la clase de dicha dirección.

4.2. La información sobre el puerto de comunicaciones forma parte de la cabecera de los paquetes:

a) IP.

b) TCP.

c) UDP.

d) TCP y UDP.

4.3. La capa de aplicación del modelo OSI, ¿a qué capa de la arquitectura IP corresponde?

a) A la capa de Internet.

b) A la capa de acceso a la red.

c) A la capa de transporte.

d) A la capa de aplicación.

4.4. La dirección 2001:0db8:85a3:08d3:1319:8a2e:0370:7334:

a) Corresponde a la dirección física de un equipo.

b) Corresponde a una máscara de subred.

c) Corresponde a una dirección IPv6.

d) Corresponde a una dirección IPv4.

4.5. La unidad de datos en la capa de transporte de TCP/IP se denomina:

a) Segmento.

b) Paquete.

c) Mensaje.

d) Datagrama.

4.6. La unidad de datos en la capa de Internet de TCP/IP se denomina:

a) Segmento.

b) Mensaje.

c) Paquete o datagrama.

d) Trama de datos.

4.7. El servicio DHCP:

a) Permite a los servidores de nombres conocer la dirección IP del servidor a partir de su nombre de dominio.

b) Sirve para traducir la dirección IP de un equipo a su dirección física.

c) Permite asignar direcciones IP dinámicas a los equipos conectados a una red local.

d) Todas las respuestas anteriores son falsas.

4.8. ¿Cuál de los protocolos de la capa de transporte se considera propiamente *fiable*?

a) TCP.

b) UDP.

c) FTP.

d) ICMP.

4.9. El/la _____ permite identificar a un equipo de Internet de manera única y fácil de recordar.

a) Dirección IP.

b) Dirección MAC.

c) Nombre de dominio.

d) Todas las anteriores.

4.10. ¿Cuál de las siguientes direcciones IP es de clase B?

a) 230.0.0.0.

b) 130.4.5.6.

c) 230.4.5.9.

d) 30.4.5.6.

Actividades de aplicación

4.11. Explica con tus palabras en qué consiste el protocolo ICMP.

4.12. ¿Qué es una dirección IP dinámica? ¿Cómo se configura en Windows XP? ¿Y en GNU/Linux? ¿Quién es el encargado de asignar las direcciones IP en una red de área local?

4.13. ¿Has oído hablar del protocolo Telnet? ¿A qué capa de la pila TCP/IP corresponde? ¿Se emplea actualmente? ¿Cuáles son sus problemas? Investiga en Internet o en la bibliografía si es necesario al respecto.

4.14. Explica por qué un *router* suele tener asignadas, como mínimo, dos direcciones IP.

4.15. ¿Cómo es posible que consideremos TCP un protocolo *fiable* si se basa en IP, un protocolo que no lo es?

4.16. Explica en qué consiste el modelo cliente-servidor. ¿Es lo mismo que el *cloud computing*?

4.17. ¿En qué consiste el proceso de *resolución de nombres*? ¿Qué servicio lo lleva a cabo? Dicho servicio, ¿qué protocolo de la capa de transporte emplea habitualmente? ¿Qué son los *servidores de nombres*?

4.18. Si dispones de un equipo con una instalación de Windows, efectúa las siguientes operaciones de configuración de la red:

- **a)** Cambia el nombre del equipo asignándole tu primer apellido. Si existen varios en el aula, añádele un número (por ejemplo: «GARCIA1», «GARCIA2») para evitar duplicidades de nombres en la red.
- **b)** Conéctalo a un grupo de trabajo que tendrá como nombre la palabra «AULA» y el número de tu aula, que habrá sido creado previamente por el profesor o profesora.
- **c)** Asígnale una dirección IP estática (ponte de acuerdo con tus compañeros para evitar duplicidades de direcciones en la red) y los servidores DNS de Google.
- **d)** Comparte en el grupo de trabajo una de las carpetas de tu equipo.
- **e)** «Haz ping» a otros equipos de la red para comprobar que responden.

4.19. Si dispones de un equipo con una instalación GNU/Linux, efectúa con él las siguientes operaciones de configuración de la red:

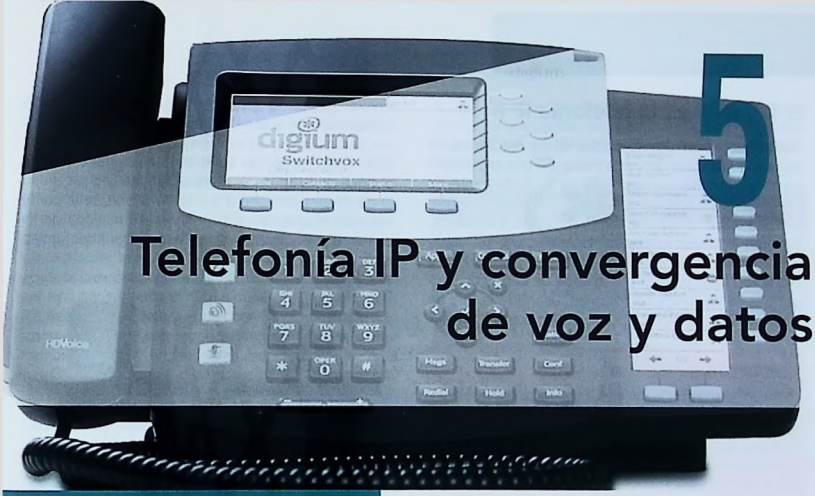
- **a)** Cambia el nombre del equipo de la red y asígnale tus dos apellidos, sin espacio de separación entre ellos.
- **b)** Asigna al equipo una dirección IP estática (ponte de acuerdo con tus compañeros para evitar duplicidades de direcciones en la red) y los servidores DNS de Google.
- **c)** «Haz ping» a varios equipos de la red y a un nombre de dominio de Internet.
- **d)** Crea un servidor FTP en el equipo, configúralo para que los usuarios puedan acceder a sus carpetas remotamente con permisos de escritura y prueba a conectarte a él desde otros *hosts* de la red local.
- **e)** Instala Samba y comparte en el grupo de trabajo de Windows la carpeta **/home/share**. Configúrala para que los usuarios de Samba puedan escribir en ella. Prueba dicha configuración en los equipos Windows del grupo de trabajo.

4.20. Explica en qué consiste la tabla NAT. ¿Cómo deberíamos configurarla para poder conectarnos desde cualquier equipo de Internet al ordenador con IP 192.168.1.75 de la red local?

4.21. Cita todos los protocolos de la pila TCP/IP que se emplean en los siguientes casos. Especifica las funciones de cada uno de ellos e indica a qué capa de la pila pertenecen:

- **a)** Conexión mediante SSH a un servidor de la red local.
- **b)** Descarga del correo mediante POP a través de un cliente de correo.
- **c)** Visualización de una página web en nuestro navegador.

4.22. Mediante un punto de acceso inalámbrico o un router-modem inalámbrico, configura una red Wi-Fi asignándole filtrado por MAC y estableciendo el nivel de encriptación más seguro que permita el dispositivo. Añade las direcciones MAC de algunos dispositivos con interfaz Wi-Fi y comprueba que se conectan correctamente al punto de acceso.



5

Telefonía IP y convergencia de voz y datos

La telefonía IP, o la «voz sobre IP (VoIP)», es una tecnología para transmitir las comunicaciones de voz a través de una red TCP/IP, en el entorno de una red local o a través de Internet. De este modo, los servicios de telefonía ya no se transmiten a través de una red específica, sino que tienden a confluir con la red de datos, creando una única red de telecomunicaciones. En esta Unidad estudiaremos cómo funciona una red VoIP, sus componentes y protocolos, y aprenderemos a instalar Asterisk, un completo sistema de comunicaciones que nos permitirá crear un servidor PBX con un sinfín de funcionalidades a partir de un simple ordenador personal.

Contenidos

5.1. ¿Qué es la telefonía IP?
5.2. Componentes de un sistema VoIP
5.3. Protocolos de la red
5.4. Asterisk
5.5. Convergencia de voz y datos

Objetivos

- Conocer los fundamentos de la telefonía IP y la tecnología VoIP y sus ventajas sobre la telefonía tradicional.
- Identificar los componentes de un sistema VoIP, estableciendo sus semejanzas y diferencias con los de una red telefónica convencional.
- Comprender la importancia de los protocolos para el funcionamiento de una red VoIP y distinguir en qué capa o capas de la pila TCP/IP están definidos. Conocer y valorar la importancia de la *calidad del servicio* (QoS, *Quality of Service*) en una red VoIP, así como las principales fuentes de ruido y retardos en los sistemas de telefonía IP.
- Conocer el funcionamiento y las partes de Asterisk, valorando su carácter modular y el interés que presenta este sistema para la implantación de sistemas de telefonía sobre la red TCP/IP.
- Valorar hasta qué punto las redes de voz y datos están dejando de ser sistemas independientes, para integrarse progresivamente en una única red de comunicaciones, tendencia que presenta múltiples ventajas pero también exige el mantenimiento de estándares elevados de calidad del servicio.

5.1. ¿Qué es la telefonía IP?

VoIP (*Voice over IP*, Voz sobre IP) es una forma de transmitir llamadas de voz a través de una red TCP/IP como las que hemos estudiado en la Unidad anterior. Con ello se proporcionan servicios de telefonía sobre una red única, en la que confluyen la voz y los datos. Esta red IP puede emplearse para efectuar las llamadas internas de la propia empresa (empleando para ello la red local privada o dedicada de la que disponga) o para las llamadas externas, usando Internet en lugar de la red telefónica pública conmutada.

> **Recuerda que...**
>
> Aunque en muchas ocasiones empleamos los términos *VoIP* y *telefonía IP* como sinónimos, en realidad hay diferencias entre ambos: la telefonía IP se refiere a la utilización de una red TCP/IP (ya sea pública o privada) para las comunicaciones de voz. Por su parte, VoIP es la tecnología empleada para el funcionamiento de la telefonía IP.

Los pasos para efectuar una comunicación a través de una red TCP/IP se representan en la **Figura 5.2**: conversión de la señal de voz analógica a digital, compresión de la señal y empaquetamiento de la misma para su envío a través de la red TCP/IP, y transmisión. En la recepción se efectúa el proceso inverso, aunque en la figura se representan las flechas de flujo de información con doble cabeza porque la comunicación telefónica es, en la inmensa mayoría de los casos, bidireccional, siendo ambos extremos emisores y receptores.

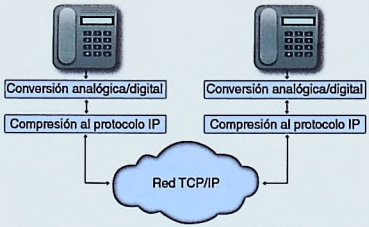


Figura 5.2. Diagrama de bloques de una comunicación telefónica a través de VoIP.

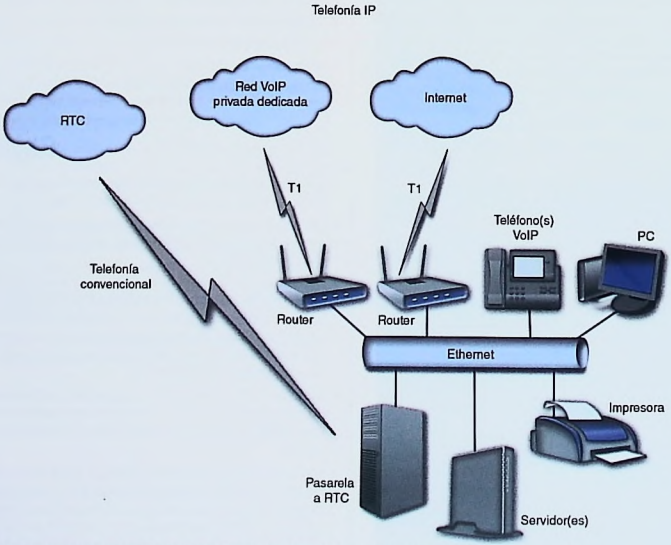


Figura 5.1. Componentes de una red de telefonía IP con una pasarela (*gateway*) hacia la red telefónica conmutada.

5.1.1. Ventajas (e inconvenientes) de la telefonía IP

¿Cuáles son las ventajas de la telefonía IP sobre la el servicio de telefonía convencional? En una llamada telefónica convencional, se establece una conexión permanente entre ambos interlocutores. El sistema funciona muy bien en escenarios en los que la densidad de llamadas telefónicas es relativamente baja. Pero, ¿qué ocurre cuando varios interlocutores quieren utilizar simultáneamente el mismo canal? En la telefonía IP, los paquetes de datos —que contienen la señal de voz, además de sus correspondientes cabeceras, como hemos estudiado en la Unidad precedente— viajan a través de una única red de datos hasta la dirección IP del destinatario.

Las capacidades de la telefonía convencional (ya sea a través de la red pública conmutada o a través de una red privada, como hemos estudiado en el caso de las centrales PBX en el Apartado 3.7 de la Unidad 3) son proporcionales a la infraestructura física de la red: cuanto mayor sea el número de abonados y llamadas, mayor debe ser la infraestructura de comunicaciones necesaria para soportarlo. Sin embargo, cuando se efectúa una llamada telefónica, el canal (el circuito dedicado que se crea temporalmente entre ambos abonados) proporciona una capacidad (un ancho de banda) que solo se usa parcialmente. Por el contrario, en una red TCP/IP la capacidad está más ligada a la eficiencia del *software* empleado que a las capacidades físicas de la red.

En conclusión, algunas de las razones mas importantes para el uso de la telefonía IP son las siguientes:

- Una de las principales ventajas de la telefonía IP es la infraestructura física. La implantación de un sistema PBX requiere una importante infraestructura de cableado para crear los bucles entre los terminales telefónicos y la centralita. Sin embargo, la implantación de un sistema VoIP no requiere más que una red TCP/IP, una infraestructura que hoy en día está presente en cualquier empresa u oficina.
- En lugar de tener que mantener dos redes de comunicaciones, la de voz y la de datos, la administración del sistema se simplifica, puesto que *solo* es necesario mantener una red, la red TCP/IP.

Sin embargo, también existen algunas desventajas de la telefonía IP: el elevado coste de los terminales telefónicos IP, en comparación con los tradicionales, y la dependencia de la red de datos para todas las comunicaciones de la empresa, ya sea la red local (si un enlace de datos falla o se produce un fallo software en el equipo, la red de voz se inhabilita) o la red pública (si se produce un fallo en la conexión a Internet perdemos también la posibilidad de realizar llamadas telefónicas).

Actividad propuesta 5.1

Asocia los siguientes términos a la red telefónica convencional o a la red VoIP: (a) Conmutación de paquetes; (b) Codificación y compresión de la señal de voz; (c) Conmutación de circuitos; (d) Versatilidad; (e) Coste elevado de los terminales telefónicos; (f) Pasarelas o *gateways* a la red telefónica conmutada.

Recuerda que...

Cada vez más se usan las redes de datos para transmitir información en tiempo real, como llamadas de voz o vídeo; a este proceso se lo denomina *convergencia de voz y datos*.

5.1.2. Las capas de una red VoIP

Al igual que ocurre con cualquier otra red de comunicaciones, la red VoIP puede representarse mediante el modelo OSI, tal como hemos estudiado en la Unidad anterior con respecto a la red de datos.

- La **capa física** es la que proporciona la infraestructura eléctrica, mecánica, radiante u óptica necesaria para la transmisión de información a través de la red. Dos problemas muy importantes que aparecen en esta capa son la atenuación y la degradación o distorsión de la señal. La infraestructura mínima necesaria para soportar una red VoIP es Ethernet 100BaseT y cableado de par trenzado de categoría 5.
- La **capa de enlace de datos** proporciona, entre otros, mecanismos para la detección y/o corrección de los errores que se presentan en la capa física. En realidad, los protocolos VoIP prácticamente no presentan especificaciones sobre la capa física ni sobre la capa de enlace de datos; solo las funciones QoS (que estudiaremos más adelante en esta Unidad) interactúan con esta capa.
- La **capa de red** proporciona la lógica necesaria para la existencia de una única red a través de muchas conexiones físicas distintas; entre sus funciones están el proporcionar un esquema de *rutas* o *caminos* para que los paquetes puedan viajar hasta los diversos equipos de la red y un mecanismo de direccionamiento. Normalmente, la definición de los protocolos VoIP *comienza en esta capa*; es decir, aquellos *hacen*

abstracción del funcionamiento de las capas inferiores. Cada dispositivo (por ejemplo, cada terminal telefónico) conectado a la red VoIP cuenta con una dirección IP, como si se tratase de un ordenador o de un *router*. Todo lo que hemos estudiado en la Unidad 4 sobre direcciones IPv4 e IPv6, máscaras de subred y paquetes IP se aplica también aquí. Recordemos que IP es un protocolo *no fiable* y *sin conexión*.

- La **capa de transporte** introduce mecanismos para garantizar la fiabilidad de la transmisión de datos. En el modelo TCP/IP se emplean dos protocolos en esta capa: TCP y UDP. El primero es más fiable pero introduce más sobrecarga y retardos en la transmisión; el segundo es más rápido y sencillo, pero menos fiable. Las redes VoIP emplean mayoritariamente el protocolo UDP. ¿Por qué? En una red VoIP, en la que se envían entre 30 y 50 datagramas por segundo, verificar que cada uno de los paquetes se ha entregado correctamente al destinatario introduciría retardos inasumibles en una conversación de voz. Sin embargo, el protocolo TCP sí se emplea para transmitir las señales de llamada, es decir, la información que se emplea para iniciar, controlar y finalizar la conversación telefónica.
- Las **capas superiores (sesión, presentación y aplicación)** proporcionan la interfaz de usuario necesaria para efectuar la comunicación en una red VoIP. En dichas capas, que constituyen el objeto principal de esta Unidad, hablaremos de teléfonos IP, teléfonos *software*, servidores VoIP, mensajes de voz, contestadores automáticos, etcétera. Más adelante veremos con detalle cuáles son los protocolos que emplea la telefonía IP en estas capas de la red.

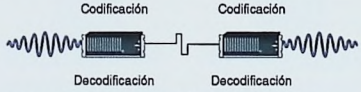


Figura 5.4. Para efectuar la transmisión de las llamadas de voz a través de la red de datos, es necesario convertir las señales analógicas a digitales (emisión) y luego convertirlas de nuevo de digitales a analógicas (recepción). Esta operación la llevan a cabo los codecs (codificadores/decodificadores).

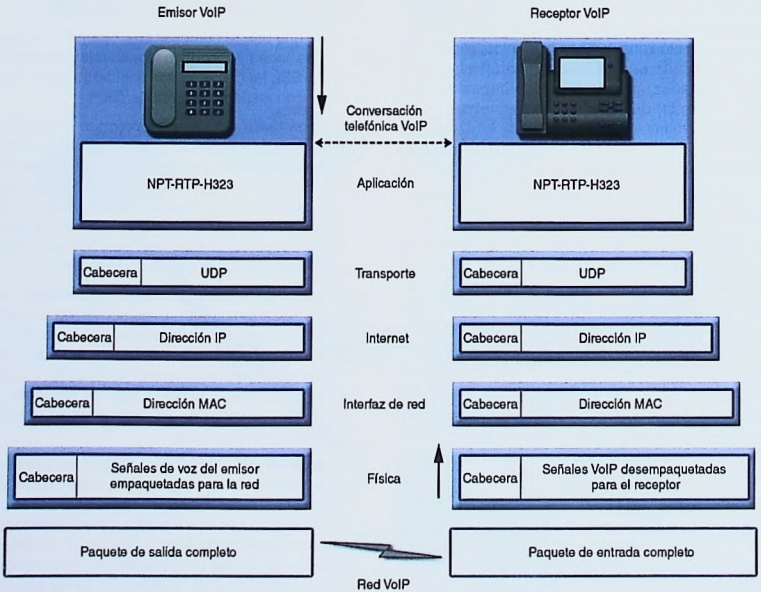


Figura 5.3. La telefonía IP vista según el modelo OSI.

Universidad Tecnica del Norte
BIBLIOTECA
Ibarra Ecuador

¿Sabías que...?

Los retardos tienen una gran importancia en la calidad de una red VoIP, por lo que resultan inasumibles cuando su valor es superior a 300 ms. Por ello es sumamente importante la elección de códecs que no introduzcan retardos excesivos en el empaquetado.

Codecs

Los codecs son los encargados de convertir la señal de sonido analógica en información digital (en dígitos binarios o bits), que se envían a una velocidad predeterminada. A menudo, el códec se encarga también de comprimir la información, con el objetivo de ahorrar ancho de banda.

Existen multitud de codecs disponibles; algunos de ellos, junto con sus características básicas, se resumen en la **Tabla 5.1,** que veremos a continuación. El nombre del códec indica el estándar de la ITU-T (la sección de estándares de telecomunicaciones de la *International Telecommunications Union*, a la que ya nos hemos referido en la Unidad 1) que describe su operación. Como podemos observar en la **Tabla 5.1**, hay codecs que ofrecen diversos grados de calidad en su operación de codificación de los datos digitales. Obviamente, mayor calidad implica mayor ancho de banda; en la elección del códec empleado en la red de telefonía IP se deberá buscar siempre un compromiso entre estos dos factores.

En la **Tabla 5.1** se incluyen, junto con los nombres de los codecs, el ancho de banda empleado (las velocidades de transmisión que ofrecen los diferentes codecs) y el retardo en el empaquetado, es decir, el retardo que introducen dichos codecs en la fase de conversión de analógico a digital y viceversa. Un mayor retardo en el empaquetado afecta negativamente a la calidad del servicio (QoS), como veremos en el Apartado 5.3.1.

Recuerda que...

En la codificación de una señal de audio analógica en digital, se produce un muestreo de la señal: se mide el valor de la misma a intervalos regulares y dicho valor se codifica en forma de ceros y unos (bits).

5.2. Componentes de un sistema VoIP

El componente más importante de una red de telefonía IP es el servidor o los servidores VoIP. Junto con ellos, es imprescindible que la red disponga de una serie de terminales telefónicos; normalmente estos son teléfonos IP, pero también podemos encontrar en la red teléfonos software y terminales telefónicos convencionales, que se conectan a la red IP mediante un adaptador telefónico analógico.

5.2.1. Servidores VoIP

Los servidores VoIP son dispositivos con un software instalado que permite gestionar las conversaciones de voz, facilitando las llamadas y otras aplicaciones VoIP. Entre otras, las funciones de un servidor VoIP son las siguientes:

- Conmutación de llamadas y gestión de las conexiones, como en el caso de una central PBX.
- Registro de llamadas y contestadores automáticos, como en un sistema de telefonía de voz tradicional.
- Interfaces de acceso para que los dispositivos de telefonía convencional (teléfonos analógicos, PBX) puedan participar en la red de telefonía IP.
- Traducción de las codificaciones de audio en tiempo real, para posibilitar las llamadas entre terminales analógicos y digitales o entre teléfonos convencionales y teléfonos IP.

En una red VoIP pueden existir pasarelas, puertas de enlace o *gateways* que conecten la red de voz con la red telefónica conmutada o con otras redes, como ilustra la **Figura 5.1**. Otro elemento que encontramos en las redes VoIP son las *gatekeepers*, componentes del protocolo H.323 que proporcionan servicios de resolución de direcciones y control de acceso a la red, además de gestionar el ancho de banda y registrar y controlar las llamadas efectuadas.

5.2.2. Terminales telefónicos

Los *teléfonos IP* son terminales que se conectan directamente a una red TCP/IP. Su apariencia es similar

Tabla 5.1. Codecs empleados en VoIP.

Tipo de códec	Ancho de banda empleado	Retardo en el empaquetado	Calidad ofrecida
G711u-a	56-64 kbit/s	1 ms	Muy buena
G.726-32	32 kbit/s	1 ms	Muy buena
G.729	8 kbit/a	25 ms	Buena
G723.1 MPMLQ	6,3 kbit/s	67,5 ms	Buena
G.723.1 ACELP	5,3 kbit/s	67,5 ms	Media

a la de un teléfono comercial, pero en lugar de contar con un adaptador RJ11 para conectarse al bucle de abonado, disponen (normalmente) de una interfaz RJ45 para la conexión a la red Ethernet mediante un cable de par trenzado. Las aplicaciones de voz que se ejecutan en un terminal de este tipo proporcionan funciones similares a las de un terminal convencional, aunque los mecanismos de transmisión de voz y señalización de llamadas operan de modo completamente distinto.



Figura 5.5. Teléfono IP de la empresa Digium. Cortesía de Digium.

También es posible emplear terminales convencionales para conectarse a la red VoIP por medio de un *adaptador telefónico analógico* (véase la **Figura 5.6**). El dispositivo efectúa la codificación de la señal analógica y participa en la red VoIP empleando los estándares de la misma (véase más adelante). En general, el uso de adaptadores es una opción más limitada que el uso de teléfonos IP pero de menor coste.

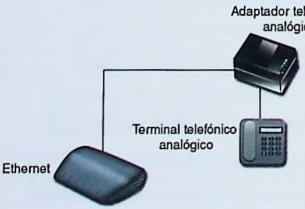


Figura 5.6. Uso de un terminal telefónico convencional en una red de telefonía IP por medio de un adaptador telefónico analógico.

Las redes IP inalámbricas aún no soportan la Calidad del servicio que proporciona la telefonía IP cableada. Una alternativa es emplear teléfonos inalámbricos IP, que operan como un inalámbrico convencional, pero su base se conecta a la red VoIP mediante un cable de par trenzado.



Figura 5.7. Adaptador telefónico analógico Cisco ATA 187. Cortesía de Cisco.

5.2.3. Teléfonos *software* o *softphones* (*software phones*)

Un *softphone* es una aplicación software que proporciona las funcionalidades de un teléfono en un dispositivo no telefónico, como un PC o una tableta. Se trata de un concepto que evoluciona rápidamente, puesto que aplicaciones como Skype, Instant Messanger de Microsoft o Google Video, de uso extendido y creciente, constituyen en realidad un tipo específico de *softphone*.

En la **Práctica profesional 5.2** aprenderemos a instalar uno de los múltiples *softphones* libres disponibles en Internet para su descarga y a usarlo para efectuar llamadas directas entre dos o más equipos conectados a la red local.



Figura 5.8. Página de inicio de Skype.

Actividad propuesta 5.2

¿Usas algún sistema de comunicaciones de voz a través de Internet? ¿Cuál? ¿Qué funcionalidades proporciona? Investiga qué protocolos emplea. ¿Podríamos usarlo para la implantación de un sistema de telefonía IP en una empresa?

¿Sabías que...?

Skype, a diferencia de otras aplicaciones de voz sobre Internet, emplea un protocolo propietario cuyas especificaciones no están a disposición pública. Por ello, Skype no es compatible con la mayoría de aplicaciones VoIP, sino solamente con aquellas que cuenten con la licencia correspondiente.

5.2.4. Conexión a la red telefónica conmutada

VoIP puede emplearse para conectar los teléfonos de la red a la red telefónica pública conmutada, siguiendo un esquema que se muestra (de forma simplificada) en la **Figura 5.9**. En ella, el servidor VoIP actúa como puerta de enlace para los teléfonos de la red TCP/IP hacia la red telefónica convencional.

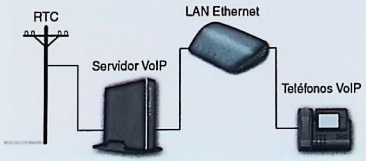


Figura 5.9. Servidor VoIP actuando como puerta de enlace con la red telefónica conmutada.

Para la conexión de un servidor VoIP a terminales o líneas telefónicas convencionales, se emplean tarjetas de interfaz telefónica. En muchas ocasiones, se trata de simples tarjetas de expansión que se conectan a una de las ranuras PCI de la placa base del servidor y que cuentan con una serie de interfaces o puertos telefónicos RJ11.

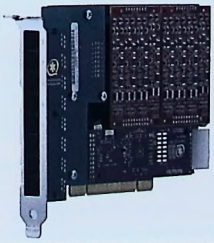


Figura 5.10. Tarjeta telefónica analógica de 8 puertos. Cortesía de Digium.

5.3. Protocolos de la red

Como hemos observado anteriormente en la **Figura 5.3**, los protocolos VoIP están situados en la capa de aplicación de la pila TCP/IP. La realización de una llamada telefónica VoIP conlleva dos fases diferenciadas: una *fase de establecimiento de llamada* y una *fase de conversación*. En la *fase de establecimiento* se efectúan las operaciones de: producción de un tono de invitación a marcar, marcado del número de teléfono, señal de llamada (o de teléfono ocupado) y contestación del extremo opuesto de la línea; cuando el interlocutor contesta, se pasa a la *fase de conversación*. Las características y los requisitos en términos de calidad del servicio de ambas fases son diferentes, y los protocolos utilizados en ellas también lo son.

Los principales protocolos que se emplean en la fase de establecimiento son SIP (*Session Initiation Protocol*, Protocolo de Iniciación de Sesión, desarrollado por la *Internet Engineering Task Force*, una organización destinada al desarrollo de estándares para las comunicaciones a través de Internet) y H.323, desarrollado por la ITU-T; existen otros muchos, como muestra la **Figura 5.11**, normalmente desarrollados por empresas privadas para sus servidores, adaptadores y terminales telefónicos VoIP.

Los principales protocolos empleados en la transmisión de voz (*fase de conversación*) son RTP y RTCP. El protocolo RTP (*Real-Time Protocol*, Protocolo en Tiempo Real) se emplea para aplicaciones de transmisión de audio y vídeo a una dirección; el protocolo no incluye reconocimiento de la recepción de los paquetes recibidos, lo cual evita la sobrecarga de la red, redundando en una mayor calidad del servicio. El protocolo incluye una información con la fecha y la hora (*timestamp*) en la que se ha enviado el paquete, además de un número de secuencia; la aplicación que lo recibe puede reconstruir el mensaje original y comprobar si se ha perdido alguno de los paquetes enviados. Este protocolo se complementa con el protocolo RTCP (*Real-Time Control Protocol*, Protocolo de Control en Tiempo Real), que controla la calidad del servicio de la comunicación y permite obtener información acerca de los participantes en la conversación.

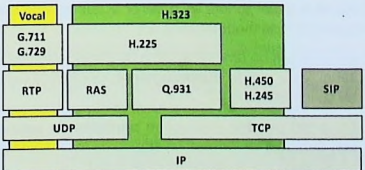


Figura 5.11. Protocolos de VoIP. Fuente: José Manuel Huidobro Moya y Rafael Conesa Pastor, *Sistemas de telefonía. Paraninfo, 2006.*

Actividad resuelta 5.1. Explica brevemente las fases de una conversación telefónica sobre VoIP y el protocolo o los protocolos que se emplean en ella.

Solución. La llamada telefónica VoIP presenta dos fases diferentes: la fase de establecimiento de llamada y la fase de conversación. Los principales protocolos en la fase de establecimiento de llamada son el SIP y el H.323; en la fase de conversación se emplean el RTP y el RTPC, el primero para el envío de los paquetes de voz y el segundo para el control de la calidad del servicio.

5.3.1. Calidad del servicio (QoS)

En la telefonía convencional, como sabemos, cuando se establece una conversación entre dos extremos, se crea un canal dedicado a la comunicación. La calidad de la conversación queda garantizada por la disponibilidad permanente de un ancho de banda dedicado. Por el contrario, en la telefonía IP, cuando el ancho de banda es limitado, a medida que aumenta el número de paquetes enviados a la red, el envío de información se ralentiza. Algunas aplicaciones toleran esta ralentización mejor que otras; el envío de voz (y vídeo) sobre una red de datos es especialmente sensible ante los retardos en la transmisión de la información.

Los factores que degradan la calidad de la transmisión de información entre dos o más interlocutores se conocen genéricamente como *ruido*. En la telefonía IP pueden existir distintas fuentes de ruido, se resumen en la **Figura 5.12**, organizadas según los niveles de la red en los que se producen:

- El **ruido de fondo** es una fuente de ruido común a la telefonía convencional y a la telefonía IP. Cuando en un ambiente ruidoso colocamos nuestra mano alrededor del micrófono del teléfono, estamos efectuando un método para la *atenuación del ruido*. Existen también métodos electrónicos para hacerlo, que suelen ser comunes a la telefonía convencional y a la telefonía IP.
- La **saturación** de la señal se produce cuando el nivel de la señal sonora es superior al que la onda portadora puede modular.
- En las fases de amplificación o de codificación de la señal, esta puede **distorsionarse**, perdiendo parte de su información.
- En la red pueden producirse **pérdidas de paquetes**, debido a los errores en alguno de los medios de transmisión o a la congestión de la red.
- La **latencia** son los huecos o *gaps* que aparecen en la conversación como consecuencia de los retardos introducidos en cada una de las fases de la transmisión de una conversación VoIP (codificación, procesamiento) y por la congestión de la red. Según ponen de manifiesto diversas investigaciones empíricas, una latencia inferior a 150 ms no es perceptible —al menos de modo inmediato—, pero a partir de ese valor comienza a afectar negativamente a la conversación; un valor de 300 ms se hace intolerable en una conversación de voz.
- El ***jitter*** es el efecto que se produce debido a un retardo o latencia variable entre los paquetes. Ello hace que los paquetes no lleguen en orden, dejando huecos en la secuencia de tramas de la conversación.
- En la capa física, las **interferencias** procedentes de diversas fuentes electromagnéticas son una importante causa de ruido.

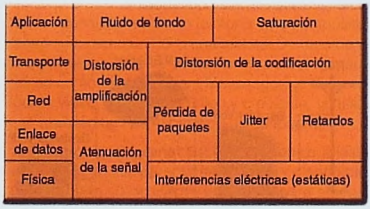


Figura 5.12. Fuentes de ruido o distorsión de la señal en las diversas capas de la red.

La *calidad del servicio* (*Quality of Service* o QoS) es un concepto con dos acepciones: por un lado, es un enfoque para el diseño de redes robustas, con un ancho de banda adecuado y con prioridad para el tráfico de aplicaciones *críticas*; por otro, es un conjunto de estándares para la reserva de ancho de banda en la red y el orden de prioridad de los paquetes. En la **Tabla 5.2** se citan el nombre y el ámbito de aplicación de los estándares más relevantes.

Tabla 5.2. Estándares QoS.

Nombre	Aplicación
802.1p	Ethernet con un solo segmento
802.1p VLAN	Redes Ethernet privadas
DiffServ	Redes compuestas de varios segmentos
RSVP	Redes compuestas de varios segmentos con un ancho de banda limitado
MPLS	Redes de alto rendimiento

En la elección de nuestro estándar QoS podemos seguir algunas reglas como las siguientes:

- Si el tráfico de red es principalmente de datos, y solo se transmite un 30 % de voz o menos, puede usarse un sistema de priorización de paquetes como 802.1p.
- Para redes extensas (centenares de nodos de voz) y con un tráfico medio, puede usarse DiffServ.
- Para redes muy extensas (miles de nodos de voz) o con una gran densidad de tráfico, es preferible emplear RSVP.

5.4. Asterisk

Asterisk es una aplicación desarrollada por la empresa Digium para la implementación servidores VoIP. Se distribuye bajo licencia de software libre, de modo que se puede descargar e instalar gratuitamente. Se trata de un sistema muy robusto y potente, que soporta gran cantidad de protocolos de comunicación VoIP, lo que permite usarlo con cualquier teléfono IP. En la **Figura 5.14** se muestran las funciones que puede desempeñar un servidor Asterisk.



Figura 5.13. Logotipo de Asterisk.

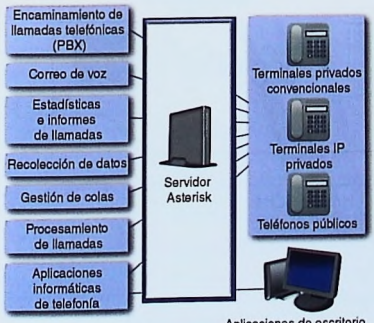


Figura 5.14. Funciones de un servidor Asterisk.

Asterisk puede ser ejecutado en varios sistemas operativos, como FreeBSD, Solaris, Mac OS X o Microsoft Windows, pero está especialmente diseñado para ejecutarse con GNU/Linux. En las prácticas profesionales de esta Unidad veremos cómo instalarlo. Una de las ventajas que presenta el sistema es que puede ser usado en ordenadores con recursos relativamente limitados: un microprocesador Intel Pentium III o equivalente, con 256 MB de RAM y una tarjeta de red Ethernet, es suficiente para configurar un sistema básico.

Más que una aplicación de telefonía, Asterisk es un *servidor de comunicaciones*. Del mismo modo que un servidor web, en el que se almacenan las páginas web que los *clientes* (los navegadores de Internet) solicitan y visualizan, Asterisk ejecuta unos programas (*scripts*) de mayor o menor complejidad que efectúan ciertas tareas, como descolgar el teléfono, grabar una conversación, redirigir la llamada o poner en funcionamiento un contestador automático. Del mismo modo que las páginas almacenadas en un servidor web están escritas (entre otros posibles lenguajes) en HTML, las aplicaciones Asterisk emplean un lenguaje propio denominado *Dialplan*; los *scripts* de *Dialplan* se almacenan en el servidor Asterisk en ficheros de texto plano. Lo ilustraremos con un ejemplo: en la columna de la izquierda vemos la secuencia de etiquetas HTML necesarias para imprimir en la ventana de nuestro navegador la frase «Hola mundo»; en la de la derecha el equivalente aproximado escrito mediante una sencilla secuencia de comandos Dialplan:

```
<html>                          exten=>(100,1),Answer()
  <head>                        exten=>(100,n),Wait(1)
  <title>Hola mundo</title>     exten=>(100,1),PlayBack(Hola)
  </head>                       exten=>(100,1),Hangup()
  <body>
     <h1>Hola mundo</h1>
  </body>
</html>
```

El *script* de Dialplan contesta el teléfono en la extensión 100, espera un segundo y reproduce la palabra «Hola»; tras ello, cuelga el teléfono.

Cuando el servidor Asterisk se encuentra activo, está ejecutándose continuamente en segundo plano, «escuchando» en el puerto o puertos predeterminados, del mismo modo que hace un servidor web o un servidor FTP. Se trata de una aplicación «multi-hilo», es decir, capaz de ejecutar varias tareas al mismo tiempo: el sistema puede, por ejemplo, conmutar una llamada y, al mismo tiempo, ejecutar un sistema de contestador automático o procesar una cola de mensajes.

El funcionamiento y las partes o *módulos* de un sistema Asterisk se ilustra esquemáticamente en la **Figura 5.15**. Asterisk se conecta a los dispositivos telefónicos empleando unos *drivers* de canal modulares; estos se encargan de gestionar las señalizaciones y de la gestión

de voz de los diversos protocolos que soporta Asterisk. De este modo, con Asterisk es posible conectar dispositivos y sistemas de telefonía que empleen protocolos diferentes. En la parte superior de la figura se muestran algunos de los protocolos que soporta el sistema:

- **SIP**, el más extendido en redes VoIP, es el que se emplea mayoritariamente para la comunicación con teléfonos IP o con los servicios telefónicos de otros proveedores que empleen este protocolo.
- Cuando se emplea un sistema con varios servidores Asterisk distribuidos, para la comunicación entre ellos se utiliza el protocolo **IAX2** (*Inter-Asterisk eXchange*, Protocolo de Comunicación entre Asterisks).
- Asterisk soporta otros muchos protocolos para la comunicación de voz, como **H.323**, **SCCP**, **MGCP** o **XMPP**, entre otros. XMPP (*Extensible Messaging and Presence Protocol*, Protocolo Extensible de Mensajería y Presencia), por ejemplo, se emplea para la comunicación con las aplicaciones de Google para las comunicaciones de voz y vídeoconferencia.
- **DADHi** es un *driver* de canal para la comunicación con las tarjetas de interfaz telefónica, que permiten conectar el sistema Asterisk con terminales o sistemas telefónicos convencionales, o directamente con la red telefónica conmutada.

En la parte inferior de la figura se observan algunos módulos adicionales de Asterisk:

- **CDR** (*Call Detail Records*, Registro de Información de Llamada) es un módulo que registra todo tipo de información sobre las llamadas gestionadas por el sistema.
- Los **Codecs** son los módulos encargados de la codificación, decodificación y traducción entre codificaciones del sistema Asterisk. Una de las virtudes de Asterisk es que permite conectar entre sí dispositivos que empleen algoritmos de codificación diferentes.
- Los módulos de **Formato** son los encargados de leer y escribir los archivos multimedia (grabación de llamadas entrantes, contestadores automáticos, mensajes de voz) empleados en el sistema de telefonía IP.
- Los módulos de **Configuración** proporcionan la información y los parámetros necesarios para el funcionamiento del sistema Asterisk.

Para la comunicación con el sistema se puede emplear la interfaz de línea de comandos (**LdC**), un mecanismo similar al del **Símbolo del sistema** de Windows o la *consola* de GNU/Linux para la configuración y el control de Asterisk.

Asterisk contiene cientos de funciones y aplicaciones, escritas en el lenguaje Dialplan, desde algunas muy sencillas, como los contestadores automáticos, hasta otras mucho más complejas, como los sistemas de mensajería de voz. Estas funciones y aplicaciones constituyen el núcleo del sistema Asterisk y le proporcionan una gran versatilidad al sistema, encargándose de las siguientes tareas: control de llamadas (establecimiento,

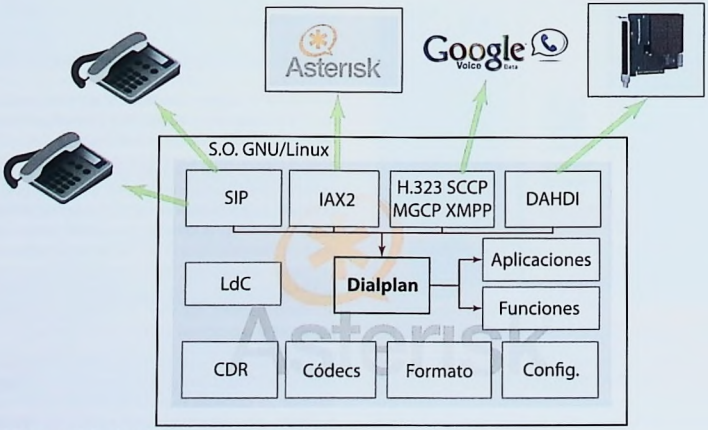


Figura 5.15. Esquema de funcionamiento y módulos de un sistema Asterisk.

desconexión y redirección), reproducción y grabación de voz o vídeo, registro de la información introducida por el usuario (mediante el marcado de números o el reconocimiento de voz), registro de los datos de la llamada, control de flujo, emisión de tonos, etcétera.

El proceso que se lleva a cabo cuando se produce una llamada se ilustra mediante las flechas de color rojo de la figura. Dialplan gestiona las llamadas (procedentes de terminales IP, de la red telefónica convencional o de otros sistemas de voz sobre datos) basándose en el número de extensión al que van dirigidas. Una vez identificado, Asterisk ejecuta el conjunto de instrucciones vinculado a ese número; también es posible que existan instrucciones para un rango de números o para aquellos números de extensión que concuerden con un determinado patrón.

Actividad propuesta 5.3

Enumera las características y ventajas de Asterisk que te parezcan más relevantes. ¿Qué ventajas crees que ofrece la posibilidad de programar las funciones del servidor PBX mediante Dialplan?

¿Sabías que...?

El desarrollo inicial de Asterisk se debe a Mark Spencer, ingeniero informático de la empresa Digium. La característica que más diferencia Asterisk de otras soluciones VoIP es su licencia abierta, que permite que cualquiera pueda estudiar su código e introducir mejoras. La enorme *comunidad Asterisk*, formada por más de 86.000 usuarios y desarrolladores en todo el mundo, es la responsable de su mantenimiento y de la introducción de mejoras y aplicaciones específicas.

5.5. Convergencia de voz y datos

«Convergencia» significa que todo el tráfico de datos, voz, vídeo, servicios multimedia y otros servicios que requieran la comunicación entre dispositivos se efectúa a través de una única red, en nuestro caso una red TCP/IP. En las **Figuras 5.16** y **5.17** se ilustra la diferencia entre dos redes separadas para telefonía y para datos y una única red en la que convergen ambos servicios, y en la que existe un enlace a la red telefónica convencional a través de una línea dedicada.

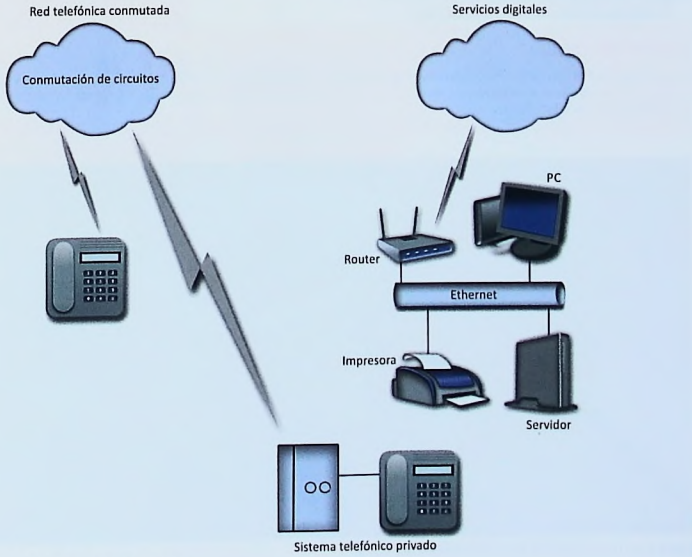


Figura 5.16. Redes de telefonía y datos separadas.

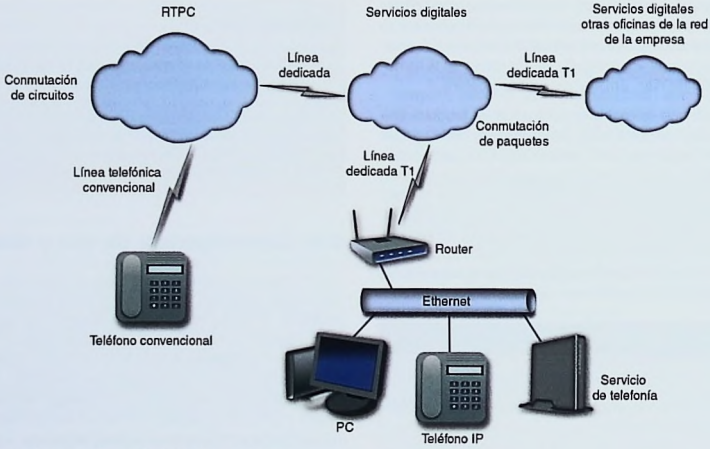


Figura 5.17. Convergencia entre las redes de voz y datos.

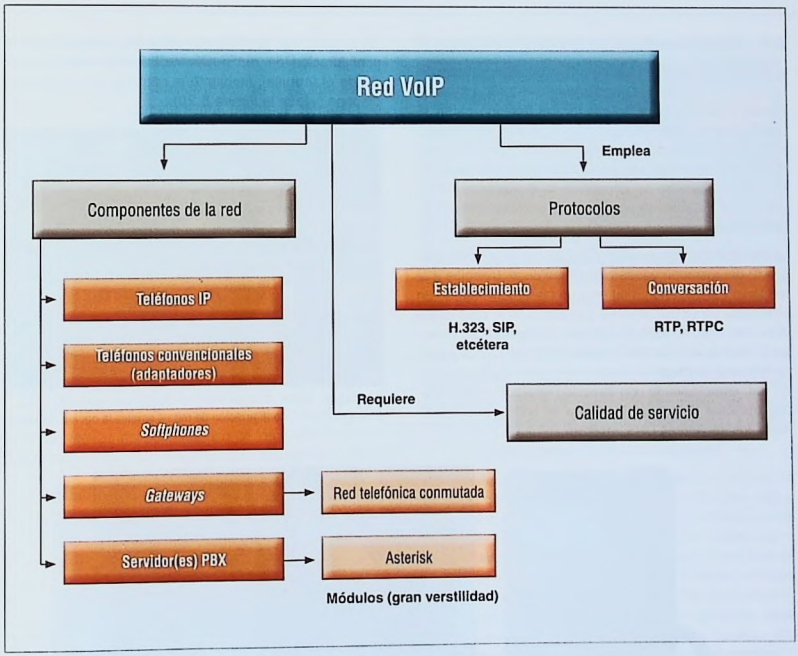
Recuerda que...

La versatilidad de las redes TCP/IP ha provocado que hoy en día el intercambio de información, tanto de datos como de voz, se efectúe cada vez más a través de estas redes, en forma de paquetes o datagramas IP. A esta tendencia se la denomina *convergencia de voz y datos*.



Figura 5.18. Convergencia de voz y datos sobre la red TCP/IP.

Mapa conceptual



Práctica profesional

5.1. Configuración de un terminal telefónico IP

A modo de ejemplo, estudiaremos la configuración de un terminal telefónico Grandstream GPX2200 (véase la **Figura 5.18**). En la parte inferior del teléfono están situadas las diversas interfaces de conexión del teléfono (LAN, USB, Tarjeta SD Flash, etcétera). El terminal cuenta con una pantalla táctil y el sistema operativo Android. Cuando el teléfono se conecta a la corriente eléctrica y se inicia su sistema operativo, la pantalla muestra la dirección IP que tiene asignada.

La configuración de la mayor parte de terminales telefónicos IP del mercado puede efectuarse conectándolos a la red local y accediendo mediante un navegador web de un ordenador conectado a la red a la dirección IP asignada a dicho terminal. A modo de ejemplo, la **Figura 5.19** muestra la interfaz web del Grandstream GPX2200. En la pestaña **Network Settings** se pueden configurar las direcciones de red, estableciendo una dirección estática o dinámica, una máscara de subred, la puerta de enlace predeterminada, los servidores DNS, etcétera.

En el caso del terminal que estamos configurando, la configuración de red puede modificarse directamente desde el terminal, mediante la pantalla táctil de la que dispone (véase la **Figura 5.20**).



Figura 5.20. Menú de la pantalla táctil del Grandstream GPX 2200. Para modificar la configuración de red se emplea la opción **Settings**.



Figura 5.18. Terminal telefónico IP Grandstream GPX 2200 y pantalla de inicio. Cortesía de Grandstream Networks.

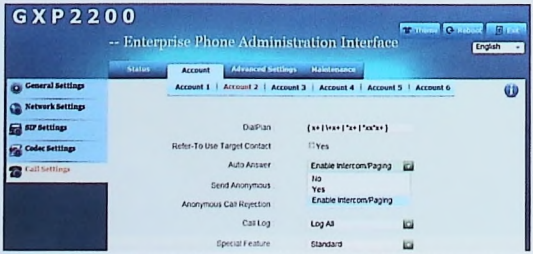


Figura 5.19. Interfaz web para la configuración del terminal Grandstream GPX 2200. Cortesía de Grandstream Networks.

Práctica profesional

5.1.1. Llamada entre dos terminales mediante su dirección IP

Para probar que los teléfonos IP con las direcciones asignadas funcionan correctamente, podemos efectuar una llamada directamente desde un terminal a otro. Para efectuar una llamada IP con el Grandstream GPX 2200, simplemente descolgamos el auricular y, en la pantalla que se activa en ese momento (véase la **Figura 5.21**), elegiremos la opción **IP Call** en el recuadro **Mode Select**. A continuación introduciremos la dirección IP y el número de puerto. Por ejemplo, si deseamos llamar a la dirección 192.168.1.60 y puerto 5062, introduciremos:

```
192*168*1*60#5062
```



Figura 5.21. Pantalla de llamada en el terminal Grandstream GPX 2200.

5.2. Instalación de un *softphone* en nuestro PC

En esta práctica instalaremos uno de los múltiples teléfonos software que podemos descargar gratuitamente en Internet. Se trata de SJPhone, de la empresa SJ Labs. Para descargar el archivo de instalación ejecutable que corresponda a nuestro sistema operativo accederemos a la URL:

http://www.sjlabs.com/sjp.html

Al hacer doble clic en el archivo ejecutable, se iniciará el Asistente que nos guiará en la instalación de esta aplicación. Tras aceptar el acuerdo de licencia, SJPhone se instalará. Tras hacer clic en el botón **Finish** (en el último paso de la instalación), podremos ejecutar la aplicación. Esta se nos mostrará en nuestro escritorio de Windows con una apariencia similar a la de la **Figura 5.23**. Para efectuar una llamada a una dirección IP dentro de nuestra red local, simplemente teclearemos dicha dirección y haremos clic en el botón de la esquina inferior derecha (**Dial number**).

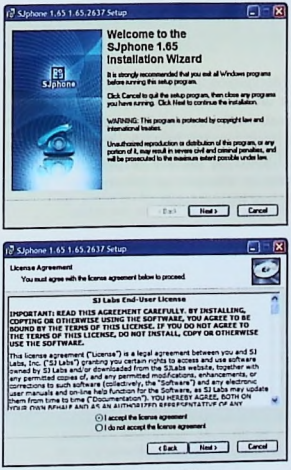


Figura 5.22. Instalación de la aplicación SJPhone.
Paso 1: Inicio del Asistente (arriba). **Paso 2**: Aceptación del acuerdo de licencia (abajo).



Figura 5.23. Interfaz de SJPhone.

Práctica profesional

5.3. Comprobación de la capacidad de la red

En esta práctica comprobaremos la *calidad del servicio* que nos proporciona nuestro proveedor de servicio de Internet o nuestra red local. Para ello emplearemos una utilidad de red de Windows denominada **tracert**[1]; esta utilidad devuelve una traza completa de la ruta que efectúan los paquetes de datos hasta alcanzar un equipo (*host*) determinado. También registra información de cada nodo intermedio en dicha ruta y nos proporciona los tiempos de latencia de tres paquetes ICMP La diferencia entre dichos tiempos de latencia puede ser una buena indicación de la presencia de *jitter* en un nodo determinado. Veamos, a modo de ejemplo, los datos que nos devuelve el comando:

```
1   0.470 ms    22.056 ms    22.132 ms    192.168.1.1 (192.168.1.1)
2   41.074 ms   42.988 ms    44.935 ms    192.168.153.1 (192.168.153.1)
3   100.079 ms  100.534 ms   101.007 ms   226.Red-80-58-114.staticIP.rima-tde.net (80.58.114.226)
4   62.854 ms   64.921 ms    66.843 ms    So6-0-0-0-grtmadde2.red.telefonica.wholesale.net (84.16.8.117)
5   96.130 ms   97.818 ms    95.083 ms    Xe7-1-0-0-grtparix1.red.telefonica-wholesale.net (213.140.43.218)
6   191.903 ms  154.826 ms   171.968 ms   Xe3-0-8-0-grtwaseq2.red.telefonica-wholesale.net (94.142.116.197)
7   168.240 ms  183.865 ms   183.415 ms   Xe7-2-0-0-grtwaseq4.red.telefonica-wholesale.net (94.142.118.162)
8   175.258 ms  182.856 ms   181.653 ms   xe-7-3-0.edge3.Washington4.Level3.net (4.53.112.41)
9   186.360 ms  194.024 ms   185.016 ms   vlan80.csw3.Washington1.Level3.net (4.69.149.190)
10  181.335 ms  187.462 ms   186.646 ms   ae-82-82.ebr2.Washington1.Level3.net (4.69.134.153)
11  197.485 ms  198.408 ms   157.293 ms   ae-3-3.ebr1.NewYork2.Level3.net (4.69.132.90)
12  175.061 ms  282.889 ms   158.791 ms   ae-4-4.ebr1.NewYork1.Level3.net (4.69.141.17)
13  177.095 ms  179.512 ms   178.970 ms   ae-7-7.car2.Detroit1.Level3.net (4.69.133.249)
14  186.332 ms  185.809 ms   194.481 ms   WAVEFORM-TE.car2.Detroit1.Level3.net (4.53.74.174)
15  209.124 ms  215.514 ms   227.992 ms   g2-0.core1.troy2.waveform.net (208.92.220.173)
16  193.911 ms  196.731 ms   197.783 ms   g4-1.agr1.troy2.waveform.net (208.92.220.198)
17  232.515 ms  567.035 ms   *            tlf-try-rtr-01.net.thelinuxfix.com (208.79.213.34)
18  174.072 ms  175.998 ms   175.462 ms   208.92.217.139 (208.92.217.139)
```

Fijémonos que en algunos de los nodos intermedios, en lugar del tiempo de respuesta del paquete encontramos un asterisco (*). Ello ocurre cuando el *router* no responde al paquete ICMP después de 4,0 segundos[2].

De modo similar a **tracert**, el comando **pathping** de Windows proporciona estadísticas respecto a todos los nodos intermedios que atraviesan los paquetes IP hasta alcanzar un *host* determinado; la ventaja es que cada uno de los nodos es estudiado durante un período de tiempo relativamente dilatado. Además, **pathping** proporciona tasas de pérdida de paquetes. En las líneas siguientes se muestra un resumen de la información devuelva por esta utilidad.

```
Traza a www.macvoip.com[208.92.217.139] sobre caminos de 30 saltos como máximo:
0 Aaron.hsd1.mn.comcast.net. [192.168.11.3]
1 air.setup [192.168.11.1]
2 73.127.68.1
3 ge-1-38-ur01.minnetonka.mn.minn.comcast.net [68.86.234.41]
4 68.86.232.37
5 68.86.232.33
Procesamiento de estadísticas durante 450 segundos...
Salto RTT Perdido/Enviado = Pct Perdido/Enviado = Pct Dirección
...
```

Continúa >>>

[1] En los sistemas GNU/Linux podemos obtener los mismos resultados mediante el comando traceroute.

[2] La utilidad **traceroute**, el equivalente de tracert en GNU/Linux, establece un tiempo de espera máximo de 5,0 segundos. La salida de esta utilidad es muy similar a la de **tracert**, aunque además de los tiempos de latencia devuelve algunas informaciones adicionales, como «!X», que indica que el administrador del sistema ha prohibido la comunicación con el *router* a través de **traceroute**.

Práctica profesional

```
...
4 9ms 0/ 10 = 0%        0/ 10 = 0% 68.86.232.37
                        0/ 10 = 0% |
5 8ms 0/ 10 = 0%        0/ 10 = 0% 68.86.232.33
                        0/ 10 = 0% |
6 12ms 0/ 10 = 0%       0/ 10 = 0% 68.86.232.5
                        0/ 10 = 0% |
7 8ms 0/ 10 = 0%        0/ 10 = 0% 68.86.232.1
                        0/ 10 = 0% |
8 20ms 0/ 10 = 0%       0/ 10 = 0% 12.116.99.41
                        0/ 10 = 0% |
9 --- 10/ 10 =100%      10/ 10 =100% tbr2.cgcil.ip.att.net [12.122.99.70]
                        0/ 10 = 0% |
10 --- 10/ 10 =100%     10/ 10 =100% ggr2.cgcil.ip.att.net [12.123.6.69]
                        0/ 10 = 0% |
```

5.4. Instalación de Asterisk en GNU/Linux

Al igual que hicimos en la Unidad anterior, emplearemos la distribución Debian de GNU/Linux para estudiar cómo se instala un servidor Asterisk. Con privilegios de superusuario, ejecutaremos en línea de comandos la instrucción:

```
apt-get install asterisk
```

El sistema solicitará probablemente una confirmación para descargar el conjunto de paquetes necesarios para configurar el servidor (véase la **Figura 5.24**) y tras ello comenzará la descarga y la instalación del sistema. En la configuración de los paquetes aparecerá una pantalla como la de la **Figura 5.25**, en la que deberemos introducir el código telefónico de nuestro país. Una vez efectuado, finalizará la instalación del servidor y este se iniciará automáticamente (véase la **Figura 5.26**).

```
  automake1.9 libtool flex bison gdb gcc-doc gcc-4.4-multilib
  libmudflap0-4.4-dev gcc-4.4-locales libgcc1-dbg libgomp1-dbg libmudflap0-dbg
  libcloog-ppl0 libppl-c2 libppl7 uw-mailutils glibc-doc libsox-fmt-all
  libstdc++6-4.4-doc vpb-utils make-doc libmail-box-perl libmyodbc
  odbc-postgresql tdsodbc unixodbc-bin
Se instalarán los siguientes paquetes NUEVOS:
  asterisk asterisk-config asterisk-core-sounds-en-gsm binutils
  build-essential dahdi dahdi-linux debhelper dpkg-dev fakeroot freetds-common
  fxload g++ g++-4.4 gcc gcc-4.4 html2text intltool-debian
  libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl
  libc-client2007e libc-dev-bin libc6-dev libcorosync4 libcurl3 libdpkg-perl
  libgmime-2.0-2a libiksemel3 liblua5.1-0 libmail-sendmail-perl libopenais3
  libopencore-amrnb0 libopencore-amrwb0 libopenr2-3 libpq5 libpri1.4
  libradiusclient-ng2 libresample1 libsox-fmt-alsa libsox-fmt-base libsox1b
  libspandsp2 libspeexdsp1 libsqlite0 libss7-1 libssh2-1 libstdc++6-4.4-dev
  libsybdb5 libsys-hostname-long-perl libtonezone2.0 libvpb0 linux-libc-dev
  make manpages-dev mlock module-assistant odbcinst odbcinst1debian2
  po-debconf sox unixodbc vpb-driver-source
Se actualizarán los siguientes paquetes:
  libc-bin libc6
2 actualizados, 63 se instalarán, 0 para eliminar y 103 no actualizados.
Necesito descargar 38,3 MB de archivos.
Se utilizarán 95,2 MB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]?
```

Figura 5.24. Instalación de un sistema Asterisk sobre GNU/Linux. Confirmación de descarga.

Práctica profesional



Figura 5.25. Configuración de Asterisk. Introducción del código telefónico de país.

Para conectarse a la línea de comandos del servidor Asterisk ejecutaremos desde el *shell* de Debian el comando:

```
asterisk -r
```

Con ello accederemos a una interfaz como la de la **Figura 5.27**; desde la línea de comandos podremos controlar completamente nuestro sistema Asterisk. En los próximos párrafos estudiaremos algunos comandos básicos para ello.

```
Configurando libsox-fmt-base (14.3.1-1+b1) ...
Configurando manpages-dev (3.27-1) ...
Configurando module-assistant (0.11.3) ...
Configurando sox (14.3.1-1+b1) ...
Configurando vpb-driver-source (4.2.52-2) ...
Configurando libstdc++6-4.4-dev (4.4.5-8) ...
Configurando odbcinst (2.2.14p2-1) ...
Configurando g++-4.4 (4.4.5-8) ...
Configurando g++ (4:4.4.5-1) ...
update-alternatives: utilizando /usr/bin/g++ para proveer /usr/bin/c++ (c++) en
modo automático.
Configurando build-essential (11.5) ...
Configurando odbcinst1debian2 (2.2.14p2-1) ...
Configurando unixodbc (2.2.14p2-1) ...
Configurando asterisk (1:1.6.2.9-2+squeeze8) ...
Adding system user for Asterisk
Añadiendo al usuario `asterisk' al grupo `dialout' ...
Añadiendo al usuario asterisk al grupo dialout
Hecho.
Añadiendo al usuario `asterisk' al grupo `audio' ...
Añadiendo al usuario asterisk al grupo audio
Hecho.
Starting Asterisk PBX: asterisk.
miguel@volia:~$
```

Figura 5.26. Una vez finalizada la configuración de los paquetes de Asterisk, se inicia automáticamente el servidor PBX.

```
volia:/home/miguel# asterisk -r
Asterisk 1.6.2.9-2+squeeze8, Copyright (C) 1999 - 2010 Digium, Inc. and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for detail
s.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=========================================================================
Connected to Asterisk 1.6.2.9-2+squeeze8 currently running on volia (pid = 5832)
volia*CLI>
```

Figura 5.27. Acceso a la interfaz de línea de comandos de Asterisk.

Práctica profesional

5.5. Instalación de AsteriskNOW en una máquina virtual

AsteriskNOW es una distribución de GNU/Linux con un sistema Asterisk completo instalado en ella. Está montado sobre CentOS, una distribución de Linux orientada al mundo de la empresa. Puede descargarse gratuitamente en **http://www.asterisk.org/downloads/asteriskNOW** e instalarse en un equipo con una o varias particiones de disco dedicadas a dicho sistema. A efectos de realizar pruebas con el sistema, en este apartado estudiaremos cómo instalar AsteriskNOW en una máquina virtual sobre Microsoft Windows.

5.5.1. Virtualización

Se denomina *virtualización* a la instalación y uso de un sistema operativo A sobre otro sistema B. En el sistema B se instala una aplicación específica —denomina *máquina virtual*— que permite la ejecución del sistema A sin abandonar el sistema B. Ello es muy útil para generar entornos de desarrollo y pruebas de software o para emplear sistemas diseñados para una arquitectura específica sobre otra distinta. En el lado negativo, los sistemas A y B deben compartir los recursos del equipo, lo cual ralentiza el funcionamiento de ambos.

Una de las aplicaciones para la creación de máquinas virtuales es VM VirtualBox, de la empresa Oracle. Se trata de una aplicación de software libre, desarrollada bajo licencia GPL y que está disponible para su descarga gratuita a través de Internet (véase la **Figura 5.28**) en:

https://www.virtualbox.org/wiki/Downloads

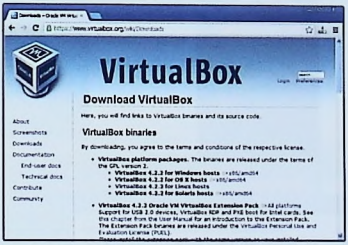


Figura 5.28. Página web para la descarga de VM VirtualBox.

Una vez descargado el archivo correspondiente a nuestro sistema operativo, lo ejecutaremos y seguiremos los pasos que observamos en las pantallas de la **Figura 5.29**. Una vez instalada la aplicación, al ejecutarla se mostrará una ventana como la de la **Figura 5.30**.

Una vez instalada la aplicación, procederemos a la creación de una máquina virtual sobre la que posteriormente instalaremos AsteriskNOW. El proceso consiste en asig-

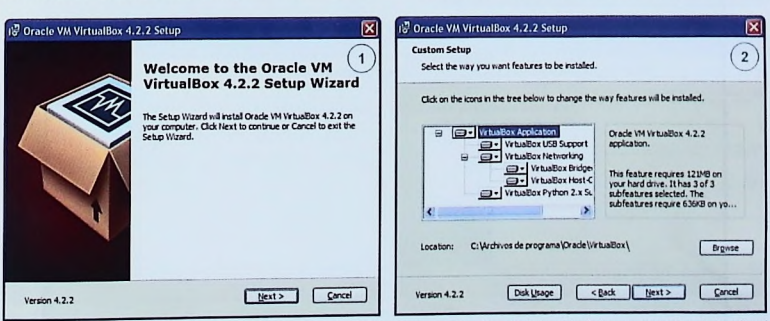


Figura 5.29. Pasos para la instalación de VM VirtualBox. **Paso 1.** Pantalla de bienvenida. **Paso 2.** Selección de los componentes de la aplicación que se instalarán. **Paso 3.** El programa de instalación nos avisa de que las conexiones de red se deshabilitarán momentáneamente durante la instalación de VM VirtualBox. **Paso 4.** Posiblemente Windows nos avisará de que algunos de los componentes de la aplicación no han superado la prueba de compatibilidad con Windows XP. Aun así, haremos clic en el botón **Continuar** para seguir con la instalación.

Práctica profesional

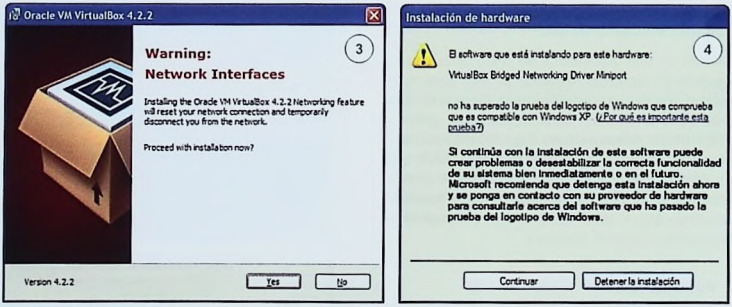


Figura 5.29. *(Continuación).*

nar a la máquina un nombre y una serie de recursos (memoria RAM y espacio en disco) del equipo. En las pantallas de la **Figura 5.31** se resume la secuencia de pasos que debemos llevar a cabo. Tras la creación de la máquina virtual, la ventana de VM VirtualBox mostrará sus características (véase la **Figura 5.32**), como el nombre, los recursos asignados y los permisos de acceso a los componentes de hardware que posee dicha máquina.

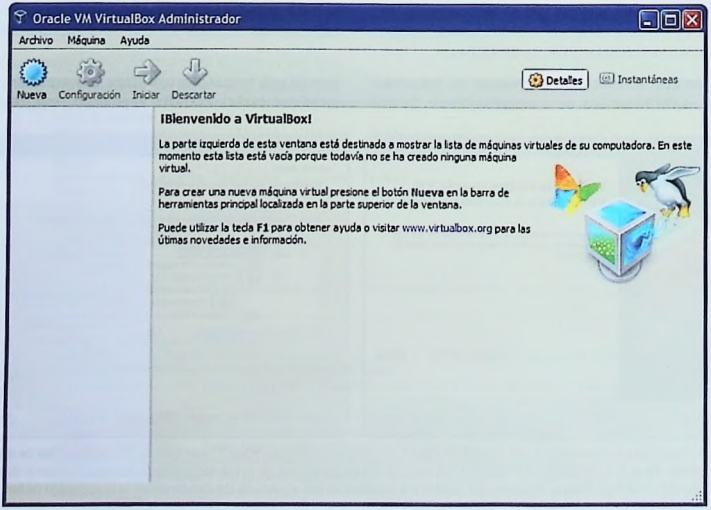


Figura 5.30. Ventana de inicio de VM VirtualBox.

Práctica profesional

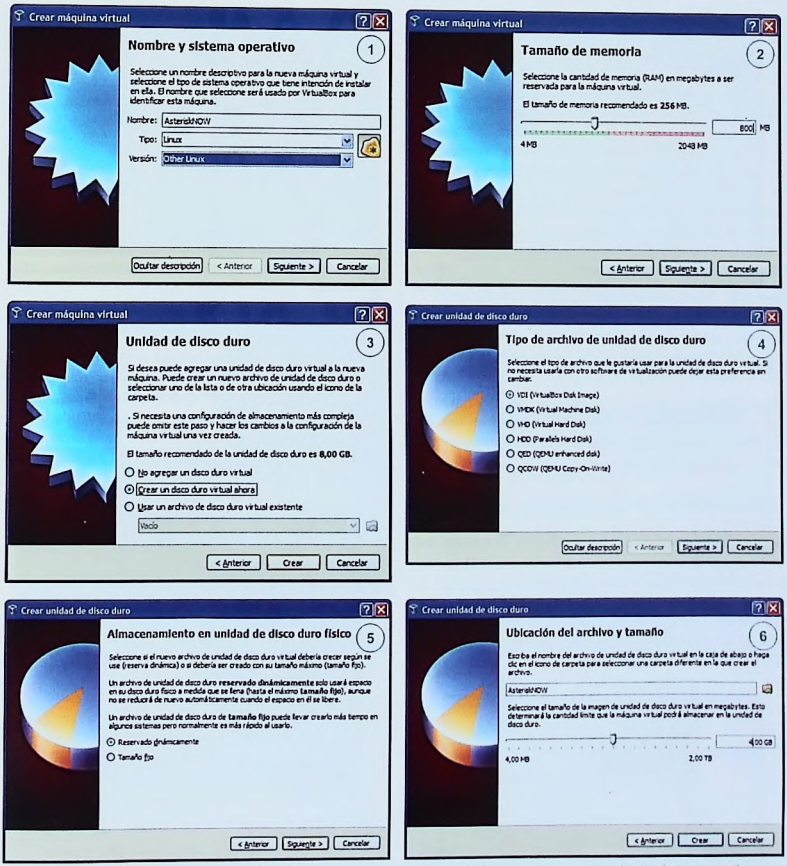


Figura 5.31. Proceso de creación de una máquina virtual para AsteriskNOW. **Paso 1.** Asignación de un nombre y tipo de sistema operativo a VirtualBox. **Paso 2.** Asignación de memoria reservada para la máquina virtual. **Paso 3.** Creación de un disco virtual, que en Windows se comportará como un archivo más con el tamaño que se le asigne. **Paso 4.** Selección del tipo de disco virtual (podemos dejar el valor predeterminado sin modificar). **Paso 5.** Dejaremos que el espacio del disco sea dinámico, es decir, que el archivo crezca según las necesidades de la máquina virtual hasta un tamaño máximo. **Paso 6.** En este último paso determinaremos el tamaño máximo asignado al disco virtual.

Práctica profesional



Figura 5.32. Una vez creada la máquina virtual, la ventana de VM VirtualBox muestra sus características y recursos asignados.

5.5.2. AsteriskNOW sobre VirtualBox

Procederemos ahora a la instalación de AsteriskNOW sobre la máquina virtual que hemos creado en VM VirtualBox. En primer lugar, deberemos descargar la imagen de disco desde la URL:

http://www.asterisk.org/downloads/asterisknow

Elegiremos la imagen de 32 o de 64 bits en función del ancho de palabra de nuestro microprocesador. Una vez descargado el archivo **.Iso**, procederemos a montar la imagen en VM VirtualBox como disco DVD virtual. Para ello haremos clic en el botón **Configuración** y, en la pestaña **Almacenamiento**, en el botón **Agregar dispositivo CD/DVD** (véase la **Figura 5.33**).

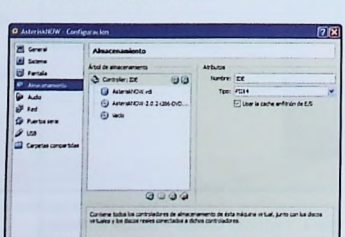


Figura 5.33. Procedimiento para añadir un CD/DVD virtual a partir de una imagen de disco (Paso 1).

El sistema mostrará entonces un aviso como el de la **Figura 5.34**. Haremos clic en el botón **Seleccionar disco** y elegiremos la imagen **.Iso** de AsteriskNOW que hemos grabado anteriormente.

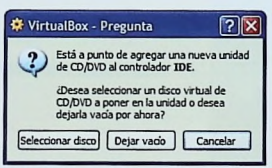


Figura 5.34. Procedimiento para añadir un CD/DVD virtual a partir de una imagen de disco (Paso 2).

Una vez efectuada esta operación, podemos iniciar la máquina virtual para instalar nuestro sistema operativo AsteriskNOW. Al hacer clic en el botón **Iniciar** de la ventana principal de VirtualBox, veremos una pantalla como la de la **Figura 5.35**[1]. Una vez iniciada, deberemos pulsar la tecla F12 para iniciar el disco DVD de instalación virtual que hemos asignado en el paso anterior. Ello dará paso a un menú de inicio (véase la **Figura 5.36**) en el que seleccionaremos la opción **(c)**.



Figura 5.35. Inicio de la máquina virtual AsteriskNOW que hemos creado en el Apartado 5.5.1.

[1] El sistema nos avisará con una serie de cuadros de diálogo de la «captura» del teclado y el ratón: cuando la máquina virtual esté activa; todas las pulsaciones de teclado (incluida la combinación Alt-Tab para cambiar de ventana) se enviarán a dicha máquina, no estando disponibles para el resto de aplicaciones de Windows. Para dejar de capturar el teclado, deberemos pulsar la tecla Ctrl Derecha.

Práctica profesional

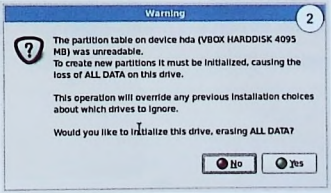


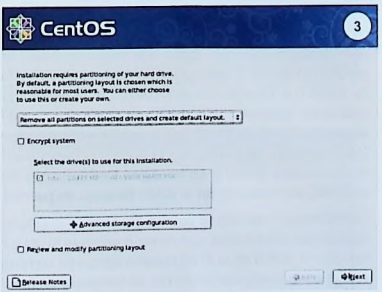
Figura 5.36. Selección del dispositivo de inicio para la máquina virtual.

Los pasos para la instalación se resumen en la **Figura 5.37**. Tras la pantalla de inicio (**Paso 1**), en la que pulsaremos la tecla Enter para iniciar el programa de instalación con su configuración predeterminada, el sistema nos mostrará un aviso para inicializar la unidad de disco virtual, paso previo necesario para su particionado y formateo (**Paso 2**). Se iniciará entonces el proceso de particionado de la unidad de disco (**Paso 3**), en el que podemos elegir la opción que se muestra en la figura y hacer clic sobre el botón **Next**. El sistema pedirá confirmación de la selección efectuada y pasaremos al paso siguiente, en el que deberemos elegir nuestra configuración horaria (**Paso 4**). A continuación el programa de instalación nos solicitará (**Paso 5**) que introduzcamos (dos veces) la contraseña de superusuario (usuario **root**).

El sistema comenzará a instalarse (**Paso 6**) y nos mostrará, si la instalación finaliza correctamente, una pantalla informándonos de ello y solicitando reiniciar el sistema (**Paso 7**); al hacer clic en el botón **Reboot**, la má-







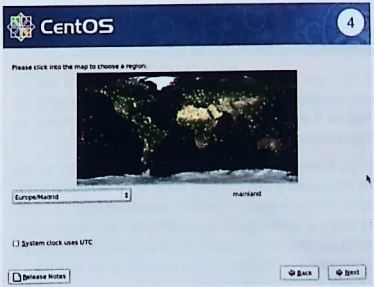


Figura 5.37. Pasos para la instalación de AsteriskNOW sobre VirtualBox. **Paso 1**. Menú de inicio. **Paso 2**. Aviso para confirmar la inicialización del disco virtual. **Paso 3**. Particionado de la unidad de disco. **Paso 4**. Elección de la zona horaria. **Paso 5**. Introducción de la contraseña de superusuario. **Paso 6**. Comienzo de la instalación del sistema. **Paso 7**. Finalización de la instalación y solicitud para reiniciar el equipo (en nuestro caso, la máquina virtual).

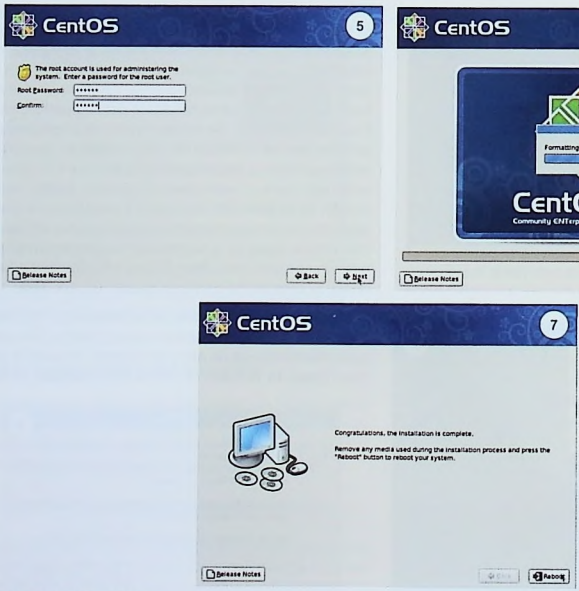


Figura 5.37. *(Continuación).*

quina virtual se reiniciará, iniciándose por primera vez nuestro sistema AsteriskNOW recién instalado.

Una vez que se reinicia el sistema por primera vez, el programa de configuración nos mostrará la pantalla de la **Figura 5.38**; a través de ella podremos modificar la configuración de nuestra instalación.

Una vez finalizada la configuración de la instalación, el sistema dará paso a una pantalla como la de la **Figura 5.39**. Introduciremos la palabra **root** tras **localhost login**, pulsaremos Intro y a continuación el sistema nos solicitará la contraseña que hemos introducido en el proceso de instalación (la contraseña no hace eco en la pantalla al ser escrita).

Notemos que en la segunda línea de esta pantalla, el sistema nos informa de que «Para configurar AsteriskNOW con FreePBX, introduzca en su navegador web la dirección 10.0.2.1». (puede que en nuestra instalación aparezca otra dirección IP diferente). Puesto que estamos ejecutando el sistema operativo sobre una máquina virtual, será preciso configurar la redirección de puertos en VirtualBox, de modo que cuando nos conectemos a un determinado puerto del sistema anfitrión (Microsoft Windows), redirija al puerto 80 de la IP 10.0.2.1 en el sistema huésped (AsteriskNOW). Para hacerlo acudimos a la **Configuración** de la máquina virtual y, en la página **Red** (véase la **Figura 5.40**), hacemos clic en el botón **Reenvío de puertos**.

La redirección o reenvío de puertos consiste en lo siguiente: cuando nos conectemos a un determinado puerto (en nuestro caso el 8080) de la IP de nuestro equipo (la comprobaremos en la configuración de red de Windows; en nuestro caso es 192.168.1.36), VirtualBox reenviará los segmentos TCP o UDP al puerto 80 de la IP del sistema invitado (nuestro sistema Asterisk; en nuestro caso, 10.0.2.15). Estableceremos la regla que se indica en la **Figura 5.41**.

Práctica profesional

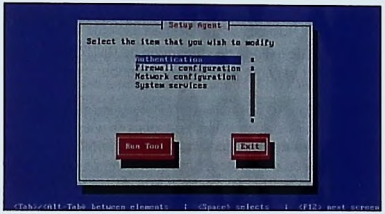


Figura 5.38. Programa de configuración durante el inicio del sistema.



Figura 5.39. Login de AsteriskNOW.

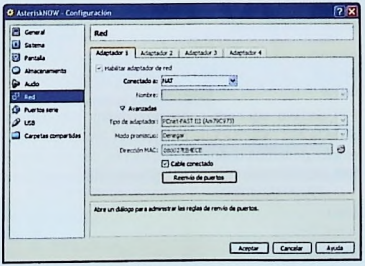


Figura 5.40. Página **Red** de la configuración de nuestra máquina virtual.

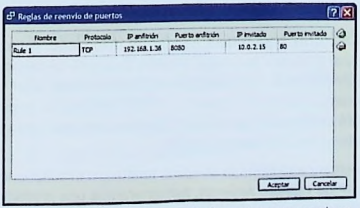


Figura 5.41. Configuración del reenvío de puertos para acceder a Asterisk mediante la interfaz web (FreePBX).

Efectuada esta operación, abriremos un navegador del propio equipo o de otro sistema conectado a la red local e introduciremos en la barra de direcciones la URL:

http://192.168.1.36:8080

o la que corresponda a nuestro caso. De este modo accederemos a una interfaz web como la de la **Figura 5.42**. Para acceder a PBXFree haremos clic en el enlace correspondiente y nos validaremos introduciendo la palabra **admin** en el nombre de usuario y la contraseña (véase la **Figura 5.43**). Al hacer clic en el botón **Login** se abre el panel web de FreePBX, una interfaz gráfica de usuario (GUI) para el control y la gestión de Asterisk.



Figura 5.42. Al introducir en nuestro navegador la URL http://192.168.1.36:8080 accedemos a una página web como esta.



Figura 5.43. Página de acceso a FreePBX.

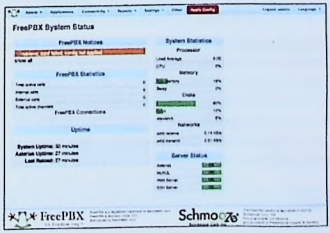


Figura 5.44. Panel principal de FreePBX, la interfaz web para el control de Asterisk.

5.6. Comunicación de un teléfono IP con Asterisk

Para efectuar esta práctica, debemos asegurarnos de que el módulo SIP de Asterisk está funcionando, para que el servidor pueda atender las llamadas telefónicas efectuadas mediante este protocolo. Por defecto, el módulo SIP de Asterisk escucha el puerto UDP 5060. Para comprobar que dicho módulo está activo, simplemente introduciremos en nuestro teléfono IP o *softphone* la dirección del servidor y comprobaremos si responde.

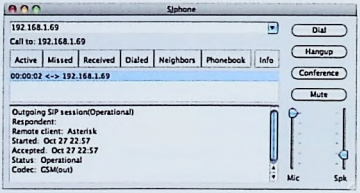


Figura 5.45. Llamada al servidor Asterisk desde un *softphone*. La respuesta del servidor indica que el módulo SIP está activo.

La comunicación de Asterisk con dispositivos SIP se define en el fichero **/etc/asterisk/sip.conf**. Si editamos este extenso archivo, veremos una sección que contiene las siguientes líneas:

```
[general]
context=default                 ;Default context for inco-
ming calls
;allowguest=no                  ;Allow or reject guest
calls (default is yes)
```

La directriz **allowguest** permite que los teléfonos IP «invitados» (es decir, aquellos dispositivos que no se hayan definido explícitamente en el archivo **sip.conf** puedan efectuar llamadas al (o a través del) servidor PBX.

Para modificar este comportamiento haremos lo siguiente: editaremos el archivo **sip.conf** y eliminaremos el carácter de comentario (;) al comienzo de la línea **allowguest=no**. Cuando efectuamos una modificación en algunos de los archivos de configuración de Asterisk, es necesario pedirle al servidor que vuelva a cargar dichos archivos. Para hacerlo, accederemos a la línea de comandos de Asterisk escribiendo:

```
asterisk -r
```

Y una vez que accedemos a la interfaz de nuestro PBX emplearemos el comando **reload**:

```
volia*CLI> reload
```

O bien, desde la línea de comandos de GNU/Linux, reiniciaremos el servidor Asterisk escribiendo:

```
/etc/init.d/asterisk restart
```

Tras ello, usaremos el comando **quit** para salir de la interfaz de línea de comandos. Si ahora tratamos de efectuar la llamada a través del teléfono IP o del *softphone*, esta se verá rechazada (véase la **Figura 5.46**), pues hemos prohibido las llamadas de invitados (*guests*) y aún no hemos definido el dispositivo en nuestro archivo **sip.conf**.

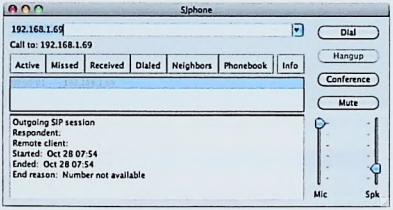


Figura 5.46. Llamada rechazada por el servidor Asterisk como resultado de la directiva **allowguest=no**.

En el archivo **sip.conf** podremos definir los dispositivos de la red Asterisk que emplean el protocolo SIP. Por ejemplo, podemos definir un dispositivo con la extensión **1000** añadiendo al archivo el siguiente bloque de líneas:

```
[1000]
type=friend
context=default
username=1000
fromuser=SIP Phone
callerid=1000
host=192.168.1.35
```

La directriz **type=friend** permite al dispositivo definido enviar y recibir llamadas. Hemos asignado al teléfono la IP 192.168.1.35 mediante la directriz **host**; aquí deberemos escribir la dirección IP del terminal, o, si este está configurado con una IP dinámica, en esta línea se deberá escribir **host=dynamic**.

Al efectuar la llamada desde el teléfono o el *softphone* a la IP de nuestro Asterisk, escucharemos una grabación en inglés indicando que hemos instalado y ejecutado correctamente el servidor Asterisk PBX.

Cuestiones

5.1. ¿Qué segmentos de la pila TCP/IP se emplean para la comunicación VoIP?

a) Se emplean siempre segmentos UDP.

b) Se emplean siempre segmentos TCP.

c) No se emplean segmentos TCP ni UDP.

d) Suelen emplearse segmentos TCP para la señalización de llamadas (fase de establecimiento) y segmentos UDP para la fase de conversación.

5.2. El protocolo SIP:

a) Es el protocolo más extendido en los dispositivos telefónicos IP.

b) Fue desarrollado por la *Internet Engineering Task Force*.

c) Se emplea en la fase de establecimiento de llamadas VoIP.

d) Todas las opciones anteriores son correctas.

5.3. El *jitter* es:

a) El retardo de los paquetes al atravesar un nodo de la red.

b) La distorsión introducida como consecuencia de las interferencias eléctricas en el cableado de red.

c) La saturación que se produce en los dispositivos de captación de la señal auditiva, cuando no están correctamente configurados.

d) El efecto que se produce como resultado de las diferencias en la latencia de los paquetes.

5.4. Para acceder a la interfaz de línea de comandos de Asterisk debemos introducir el siguiente comando:

a) ifconfig

b) asterisk –r

c) /etc/init.d/asterisk restart

d) Ninguno de los anteriores.

5.5. La telefonía VoIP:

a) Permite utilizar una única red para todas las comunicaciones de la empresa.

b) Proporciona menos flexibilidad que una red telefónica convencional.

c) Requiere el uso de costosas centralitas PBX.

d) Todas las opciones son falsas.

5.6. Una máquina virtual:

a) Es una aplicación para clonar discos duros.

b) Es una aplicación que simula mediante software un equipo *real*, permitiendo, por ejemplo, ejecutar un sistema operativo A sobre otro B.

c) Es de gran utilidad para probar sistemas operativos o instalarlos en plataformas diferentes a aquellas para las que han sido diseñadas.

d) Las opciones *b* y *c* son correctas.

5.7. La utilidad **pathping** de Windows:

a) Permite conocer las direcciones IP de los nodos o *routers* intermedios hasta alcanzar un *host* determinado.

b) Proporciona información sobre la pérdida de paquetes.

c) Nos informa de los tiempos de latencia en cada uno de los nodos intermedios.

d) Todas las opciones son verdaderas.

5.8. En Asterisk, el módulo DADHi se emplea para:

a) La conexión con Google Voice.

b) La conexión con los teléfonos IP.

c) La conexión entre varios servidores PBX en un sistema descentralizado.

d) La conexión con los dispositivos y las redes telefónicas convencionales.

5.9. El protocolo RTP:

a) Se emplea para la señalización de las llamadas VoIP.

b) Es un protocolo de control.

c) Está basado sobre segmentos TCP.

d) Todas las opciones son falsas.

5.10. La asignación de la dirección IP en un terminal telefónico VoIP puede efectuarse:

a) Mediante DHCP, si está definida dinámicamente.

b) Mediante los menús del propio teléfono.

c) Mediante una interfaz web.

d) Todas las opciones son válidas.

Actividades de aplicación

5.11. Explica en qué consiste la Calidad del Servicio (QoS) en una red VoIP.

5.12. Si dispones de terminales telefónicos IP, prueba a configurarlos, remitiéndote al manual del fabricante si es necesario:

a) A través de su sistema de menús y de la pantalla del propio teléfono.

b) A través de su interfaz web.

Asigna a los teléfonos IP las direcciones estáticas y la máscara de subred necesarias para integrarlos en la red local de tu centro educativo. Asígnales también una puerta de enlace predeterminada para que puedan comunicarse con otras redes a través de Internet.

5.13. Una vez configurados los dispositivos telefónicos, prueba a efectuar llamadas entre ellos para comprobar que funcionan correctamente.

5.14. Instala SJPhone u otro *softphone* en tu ordenador. Comprueba su configuración. ¿Qué protocolo emplea? ¿A través de qué puerto se comunica? Prueba a hacer llamadas con tus compañeros entre los *softphones* instalados y entre *softphones* y teléfonos IP.

5.15. Con los ejercicios desarrollados hasta ahora, hemos creado una sencilla red telefónica IP. Analiza sus posibles limitaciones. ¿Qué componente faltaría para completarla?

5.16. Si dispones de un ordenador con GNU/Linux, prueba a instalar Asterisk en él. Anota los pasos necesarios, los mensajes de aviso relevantes de la instalación y los posibles errores del proceso.

5.17. En una red telefónica VoIP en producción, normalmente el equipo que actúe como servidor PBX será un ordenador dedicado exclusivamente a esa función; en redes de tamaño pequeño, quizá actúe también como servidor de archivos o desempeñe otras funciones de red. En estos casos es habitual que el equipo carezca de terminales de entrada (teclado o ratón) y salida (monitor). Será necesario comunicarse con él de modo remoto a través de otro equipo de la red.

a) En el equipo en el que has instalado el servidor Asterisk, instala un servidor SSH. (Puedes remitirte a la Unidad 4 para recordar cómo hacerlo.)

b) Descarga e instala en un equipo Windows la aplicación PuTTY, que emplearás como cliente SSH en la red. Puedes hacerlo en la página oficinal del proyecto, **http://www.putty.org.**

c) Configura PuTTY para comunicarse con el equipo en el que has instalado el servidor PBX.

5.18. Accede a la interfaz de línea de comandos de Asterisk y prueba a ejecutar los siguientes comandos: **help**, **restart now**, **restart when convenient**, **voicemail show users**, **quit**. Indica qué función desempeña cada uno de estos comandos.

5.19. Edita el archivo **/etc/asterisk/sip.conf** y configura los dispositivos SIP de los ejercicios 2 y 4, de modo análogo a como has efectuado en la **Práctica Profesional 5.6.** Accede a la interfaz de línea de comandos de Asterisk, reinicia el servidor y comprueba que se han cargado correctamente con el comando **sip show peers**. Prueba a efectuar una llamada desde cualquiera de estos dispositivos al servidor.

5.20. Descarga e instala la aplicación VM Virtual Machine en tu equipo. Crea una máquina virtual y configúrala para usar 800 MB de memoria RAM y un espacio en disco de 4 GB, si el equipo dispone de este espacio libre. Descarga AsteriskNOW e instálalo en la máquina virtual que has creado. Anota los pasos de la instalación, así como los avisos relevantes y los posibles errores con los que te encuentres en el proceso.

5.21. Enumera las ventajas que presenta el uso de sistemas de código abierto frente a sistemas propietarios. ¿Crees que estos sistemas de código abierto proporcionan suficiente calidad para su implantación en el entorno de una empresa? El que su código fuente esté disponible, ¿crees que favorece que se puedan explotar las debilidades en la seguridad del sistema?

5.22. Explica en qué consiste el carácter modular de Asterisk. ¿Cuáles son los principales módulos de los que consta el sistema? Indica la función de cada uno de ellos. ¿Es posible integrar nuevos módulos en Asterisk?

ELECTRICIDAD - ELECTRÓNICA

Instalaciones de Telecomunicaciones

Infraestructuras de redes de datos y sistemas de telefonía

Este libro desarrolla los contenidos del módulo profesional de Infraestructuras de Redes de Datos y Sistemas de Telefonía que cursan los alumnos del Ciclo Formativo de grado medio de Instalaciones de Telecomunicaciones, perteneciente a la familia profesional de Electricidad y Electrónica.

El enorme crecimiento que han experimentado las redes para el intercambio de información en las últimas dos décadas, estrechamente vinculado al desarrollo de Internet, justifica el estudio en detalle de los mecanismos y los fundamentos de la transmisión de voz y de datos. El currículo de este módulo aborda principalmente la infraestructura de las redes o, con un lenguaje más preciso, de sus capas inferiores.

Para cubrir el contenido de las infraestructuras de redes, se conjugan la teoría y la práctica: las explicaciones generales sobre estándares, protocolos y medios de transmisión, con el modelo OSI como referencia permanente, se combinan con un amplio contenido práctico en el que se detallan los procedimientos que el futuro técnico deberá seguir en su trabajo. Todo ello, a través de un lenguaje asequible, sencillo y directo que no merma en absoluto el rigor y la profundidad del discurso.

Además, las Unidades del libro se acompañan de Prácticas Profesionales en las que se exponen pormenorizadamente muchas de las operaciones que habrá de aplicar el alumno en su futuro trabajo, lo que contribuye a que desarrolle su propio criterio profesional. Del mismo modo, las cuestiones y las actividades de aplicación, situadas al final de cada unidad le permitirán comprobar y ampliar sus conocimientos.

Asimismo, el libro incluye un amplísimo material gráfico (fotografías, ilustraciones, diagramas, planos...) orientado a enriquecer y complementar la teoría y la práctica, y a presentar de modo visual los conceptos introducidos, la estructura, los materiales y los dispositivos que componen las redes de datos y telefonía y los procedimientos que habrán de llevarse a cabo en su instalación.

En suma, con este manual el alumno logrará afianzar su formación en el ámbito de las infraestructuras de redes de transmisión de datos y telefonía, y adquirir los conocimientos imprescindibles para el desempeño de su futura actividad profesional.

El autor, ingeniero industrial de formación, actualmente desarrolla su actividad profesional como docente, programador web y consultor tecnológico, y cuenta con una amplia experiencia en el ámbito de la informática y de las redes de comunicaciones. Asimismo, ha publicado gran número de obras relacionadas con la formación en el campo de la informática, las comunicaciones domóticas y la energía.

ISBN: 978-84-9732-874-6

Paraninfo
ciclos formativos

www.paraninfo.es