CERTIFICADO DE PROFESIONALIDAD

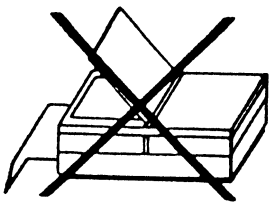
DISEÑO DE REDES TELEMÁTICAS

MF0228_3

MANUEL SANTOS GONZÁLEZ

Ra-Ma®

www.ra-ma.es/cp



La ley prohíbe
Copiar o Imprimir este libro

DISEÑO DE REDES TELEMÁTICAS
© Manuel Santos González

© De la Edición Original en papel publicada por Editorial RA-MA
ISBN de Edición en Papel: 978-84-9964-261-1

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

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

ISBN: 978-84-9964-405-9

E-Book desarrollado en España en septiembre de 2014

DISEÑO DE REDES TELEMÁTICAS

MANUEL SANTOS GONZÁLEZ

Ra-Ma®

A mi familia.

Índice

Introducción

Los **certificados de profesionalidad** son titulaciones oficiales válidas que acreditan la capacitación para el desarrollo de una actividad laboral. Para su obtención es necesario superar todos los módulos formativos que integran dichos certificados.

La presente obra se ha tratado de ajustar en lo posible a los contenidos oficiales del módulo formativo de 200 horas de duración llamado "**Diseño de redes telemáticas**", incluido en los certificados de profesionalidad "**Administración y diseño de redes departamentales**" (IFCT0410) y "**Gestión de redes de voz y datos**" (IFCM0310), ambos de nivel 3, el nivel más alto que se otorga a una cualificación profesional.

Dicho módulo trata de ofrecer una visión general de las redes telemáticas, incluyendo los principios generales sobre la transmisión de datos, los diferentes medios de transmisión, así como las principales características de los sistemas de cableado estructurado.

En la segunda parte se hace un amplio repaso a las tecnologías, protocolos y dispositivos utilizados en el diseño e implantación de las redes telemáticas, incluyendo un capítulo con las principales pautas de cómo afrontar un proyecto de diseño de una red telemática. El último capítulo está dedicado a un elemento clave en el desarrollo de cualquier servicio o producto actual y que cualquier técnico debe conocer: el *sistema de gestión de la calidad* en una empresa.

El autor mantiene un blog sobre las redes telemáticas donde el lector puede ampliar información:

redestelematicas.com

1 Introducción a las comunicaciones y redes de computadoras

1.1 ¿QUÉ ES UNA RED TELEMÁTICA?

De una manera general, una **red telemática** (o red de datos) se podría definir como la infraestructura que posibilita que varios dispositivos intercambien datos entre sí, conectados para ello a algún medio físico que permita la transmisión de dichos datos. Los dispositivos que forman parte de la red también reciben el nombre de nodos. En cuanto a los medios físicos a través de los cuales viajan los datos, estos pueden ser medios guiados (como el clásico cable de cobre o la fibra óptica), o se pueden utilizar ondas electromagnéticas transmitidas a través del aire.

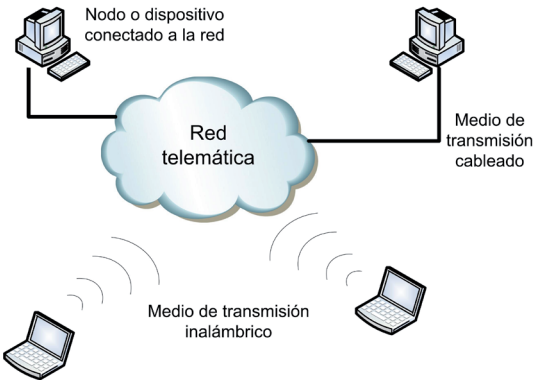


Figura 1.1. *Varios dispositivos conectados a una red telemática*

En las primeras redes telemáticas, los nodos que formaban parte de las mismas eran en su gran mayoría ordenadores de sobremesa, grandes servidores o impresoras. En la actualidad, sin embargo, el abanico de dispositivos que pueden conectarse a las redes telemáticas es más amplio, incluyendo ordenadores portátiles, *smartphones*, *tablet* PC, NAS (almacenamiento accesible por red), videoconsolas, escáneres, etc.

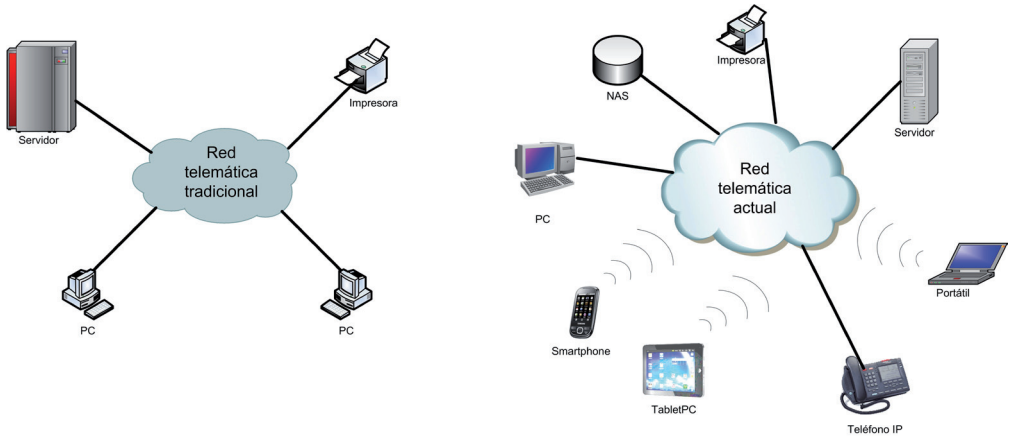


Figura 1.2. *Aumento del tipo de dispositivos que se pueden conectar a las redes telemáticas actualmente*

Y después de la definición, la siguiente pregunta es ¿para qué sirven las redes telemáticas? En un principio, las redes telemáticas se comenzaron a desarrollar con el objetivo de compartir recursos y de acceder a información a distancia. Derivados de estos primeros objetivos han surgido multitud de servicios telemáticos que actualmente han adquirido una gran importancia, como puede ser el correo electrónico, el acceso a páginas web, videoconferencia, compartición de recursos como impresoras y unidades de almacenamiento, etc. A dichos servicios, derivados directamente de la aparición de las redes de datos, hay que añadir los servicios de telecomunicación clásicos como la telefonía, radio o televisión, ya que, en la actualidad, dichos servicios pueden ser proporcionados por las actuales redes telemáticas.

Ya tenemos, a grandes rasgos, la definición y los objetivos de las redes telemáticas. Ahora se podrían plantear algunas dudas al intentar aplicar estos conceptos a nuestra realidad diaria. Por ejemplo, "si yo me conecto en casa o en mi trabajo a Internet, ¿me estoy conectando a una red telemática?", "¿es Internet una red telemática?", "¿cuando un establecimiento público, como un restaurante, ofrece conexión Wi-Fi gratuita, significa que tienen algún tipo de red telemática?". Bueno, la respuesta a todas esas preguntas es sí.

La primera cuestión que conviene aclarar es que **Internet** sí es una red telemática, de hecho es la mayor y más importante red telemática del mundo. Aunque lo cierto es que es una gran red telemática pero un poco especial, porque la principal función de Internet no es permitir conectar dispositivos, sino permitir conectar redes telemáticas. Internet posibilita la interconexión de millones de redes telemáticas esparcidas por todo el mundo. Internet es la red telemática que une el resto de redes telemáticas del mundo. Por ello es conocida como la Red de redes.

En sus inicios, Internet era una red telemática que se ajustaba a la definición ofrecida en este apartado, es decir, conectaba dispositivos generalmente alejados geográficamente, incluso hasta en miles de kilómetros. El desarrollo tecnológico en las telecomunicaciones y la aparición de las redes de área local han producido un cambio de su "función" a la interconexión de redes.

Por tanto hay que tener claro que cuando nos conectamos a Internet en casa, o en el trabajo, o en un restaurante, realmente nos estamos conectando a una red telemática que a su vez estará conectada al resto de las redes que forman Internet.

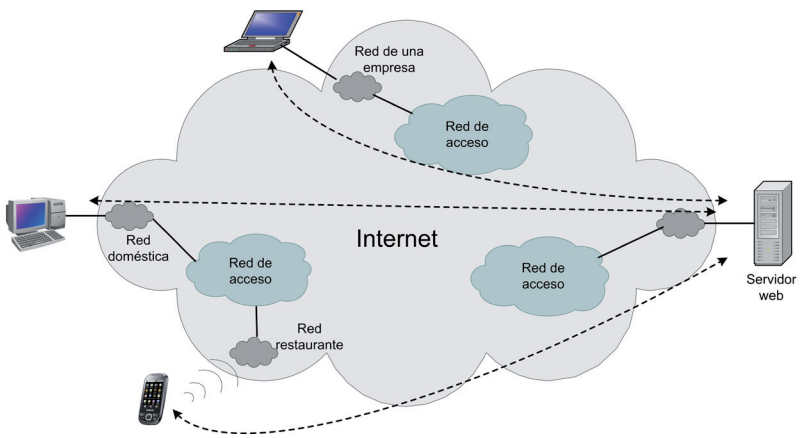


Figura 1.3. *Interconexión de redes temáticas formando Internet*

Es importante no perder la perspectiva de lo que realmente ocurre cuando "nos conectamos" a Internet. Para la gran mayoría de personas, "entrar" en Internet es abrir en el ordenador un navegador web (Internet Explorer, Firefox, Chrome…) y acceder a alguna página web. Precisamente en ese punto se produce la comunicación entre dos dispositivos que forman parte de la red telemática. Un dispositivo es mi ordenador y el otro dispositivo es un servidor (también un ordenador pero con mucha potencia y prestaciones) ubicado en algún lugar del mundo. Esta perspectiva se puede visualizar en la figura 1.3.

1.2 ¿QUÉ SERVICIOS NOS OFRECEN LAS REDES TELEMÁTICAS?

O dicho de otra manera, ¿qué podemos hacer cuando nos conectamos a una red telemática? Principalmente, los servicios ofrecidos por las redes telemáticas se pueden clasificar en función del ámbito de la red:

Servicios telemáticos ofrecidos en redes privadas

El escenario de este tipo de servicios es una red telemática que conecta los ordenadores de una empresa dentro de un ámbito geográfico limitado, por ejemplo, un edificio. En este caso, los servicios telemáticos principales son:

- Compartir información (archivos).
- Compartir recursos hardware (impresoras, escáneres, fotocopiadoras…).
- Acceso al servicio web de la empresa (lo que se conoce como *intranet*) o a aplicaciones corporativas (de gestión, bases de datos, etc.).
- Servicio de directorio para la gestión de recursos de red y nombres de usuario.
- Acceso a otras redes, típicamente Internet.

Es decir, desde el ordenador del empleado de una empresa, que tenga su propia red telemática, éste podrá acceder a archivos ubicados en otros ordenadores de la empresa, podrá enviar trabajos de impresión a las impresoras de la empresa o podrá acceder tanto a la intranet de la empresa como a Internet.

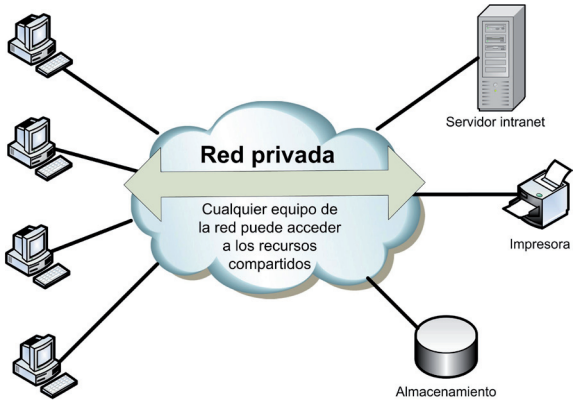


Figura 1.4. *Esquema general de una red privada*

IMPORTANTE

El término **intranet** se aplica habitualmente al servicio de páginas web proporcionado por una empresa de forma interna. Para acceder a la intranet de una empresa se utiliza un navegador web. Normalmente el acceso a una intranet solo es posible desde un equipo ubicado dentro de la propia empresa.

Servicios telemáticos ofrecidos a través de Internet (red pública)

Actualmente la mayor parte de los servicios que se proporcionan en Internet se hacen mediante el servicio web, es decir, el acceso a los servicios se hace utilizando un navegador web. Algunos ejemplos son:

- Acceso a páginas web.
- Servicio de correo electrónico.
- Servicio de mensajería instantánea (chat).
- Servicios multimedia como la visualización de programas de televisión, radio, películas o música.
- Comercio electrónico.
- Acceso a las denominadas redes sociales.

Aunque lo más extendido sigue siendo el uso de un PC (de sobremesa, portátil o *notebook*) para conectarnos a las redes telemáticas, cada vez es más común el uso de otros dispositivos como teléfonos móviles de última generación (*smartphones*), *tablets* PC o televisiones.

En este apartado no se han mencionado todos los servicios telemáticos que pueden proporcionar las redes telemáticas, pero sí los más representativos.

1.3 CLASIFICACIÓN DE LAS REDES

La principal clasificación que se hace actualmente de las redes telemáticas es en función del ámbito o alcance geográfico de la red. Y en función de este factor podemos distinguir entre tres tipos de redes: LAN, MAN y WAN.

1.3.1 REDES LAN

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

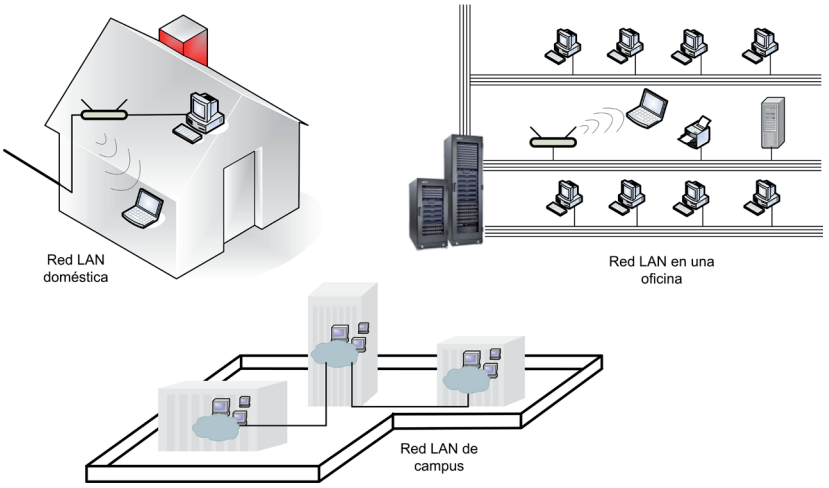


Figura 1.5. *Diferentes ejemplos de redes LAN*

Se han desarrollado tecnologías específicas para implementar este tipo de redes, por ello, otro criterio habitual de identificación de una red LAN es el uso de una tecnología específica para redes LAN. Los estándares actuales de redes LAN son Ethernet y Wi-Fi, que se estudiarán con detalle más adelante.

Lo cierto es que la aparición de diferentes estándares de Ethernet sobre fibra óptica ha facilitado que Ethernet extienda su uso no solo a redes LAN, sino también a redes MAN

1.3.2 REDES MAN

El término **MAN** (*Metropolitan Area Network* o red de área metropolitana) se aplica a redes que unen redes LAN o dispositivos dispersos en varias ubicaciones dentro de un núcleo de población, o de varios núcleos cercanos entre sí. Por lo general, estas diferentes ubicaciones pertenecen, al igual que el caso anterior, a la misma unidad organizativa, por ejemplo, la misma empresa.

Las redes MAN suelen ser puestas en funcionamiento por los operadores de telecomunicaciones que operan en la zona de cobertura de la red MAN. En grandes núcleos urbanos lo habitual es que cada operador tenga su propia red MAN, aunque en ocasiones es posible que una misma infraestructura física esté compartida por más de un operador.

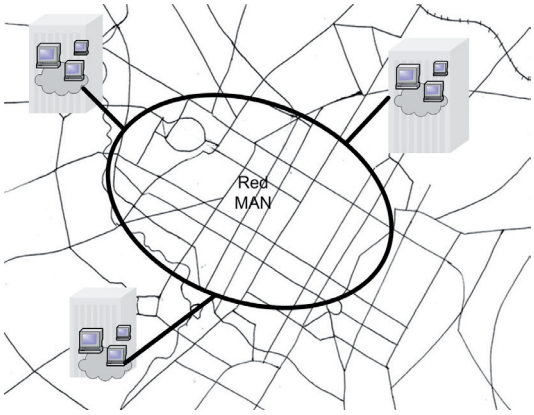


Figura 1.6. *Red MAN en un núcleo urbano*

1.3.3 REDES WAN

El término **WAN** (*Wide Area Network* o red de área extensa) se aplica realmente a la infraestructura que permite la conexión de redes o dispositivos ubicados en diferentes zonas geográficas con una distancia lo suficientemente grande como para no considerarse una red MAN. Generalmente, las redes WAN las ponen en servicio las grandes operadoras de telecomunicación para ofrecer conectividad entre ubicaciones alejadas desde cientos a miles de kilómetros. En teoría, las redes WAN no tienen un límite de distancia cubierta. De forma que la comunicación entre dos puntos alejados miles de kilómetros se hará utilizando la infraestructura una o varias redes WAN. Internet se podría considerar una gran red WAN formada por la interconexión de muchas otras redes WAN de ámbito regional.

En las redes WAN se pueden distinguir dos partes, la red de acceso y la red de transporte. La red de acceso se refiere a la infraestructura necesaria para que los clientes de una operadora accedan a la red WAN. La red de transporte es la infraestructura de la red WAN propiamente dicha, aunque en muchas ocasiones se considera red WAN tanto a la red de acceso como a la red de transporte.

Veamos los dos principales ejemplos del uso de redes WAN: la conexión de una LAN a Internet y la conexión privada de dos o más LAN. En el primer caso, se desea conectar una red doméstica con la red de un **ISP**. Esta conexión necesita utilizar infraestructuras de algún operador de telecomunicaciones, que podría ser la misma empresa que proporciona el acceso a Internet.

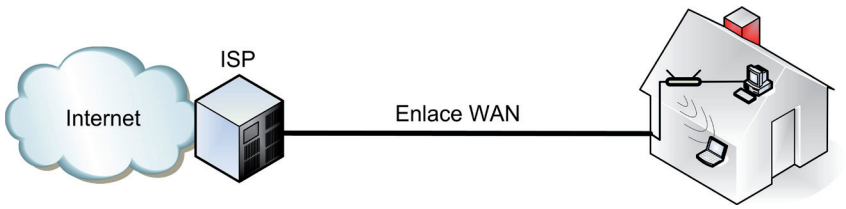


Figura 1.7. *Ejemplo de red WAN para conectar una red LAN a Internet*

IMPORTANTE

ISP: *Internet Service Provider*. Empresa que proporciona el servicio de conexión a Internet, por ejemplo, Telefónica, Jazztel, Ono...

En el segundo caso, se utilizan las infraestructuras de redes WAN para unir diferentes sedes de una empresa ubicadas en distintas ciudades.

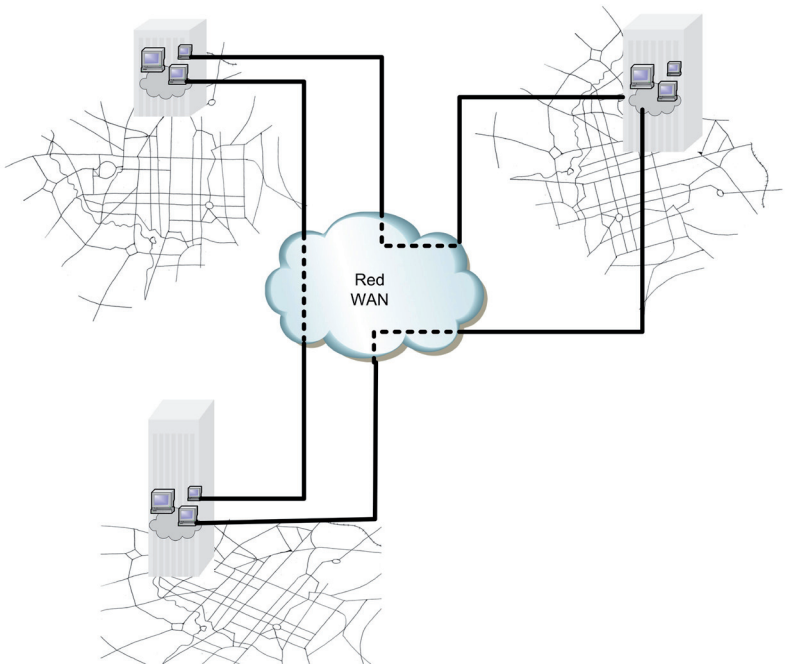


Figura 1.8. *Conexión de varias sedes ubicadas en diferentes núcleos urbanos mediante una red WAN*

La tendencia actual es la de utilizar las mismas infraestructuras, tecnologías y protocolos para redes MAN y redes WAN, por lo que la única diferencia entre ellas es el ámbito geográfico.

1.4 MODELOS DE RED Y ARQUITECTURA DE PROTOCOLOS

1.4.1 JUSTIFICACIÓN DEL USO DE UN MODELO BASADO EN NIVELES

Antes de empezar a profundizar en las tecnologías, técnicas y procedimientos que forman parte de las redes telemáticas, hay que tener en cuenta una idea importante: el proceso de comunicación llevado a cabo en las redes de datos es **complejo**.

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

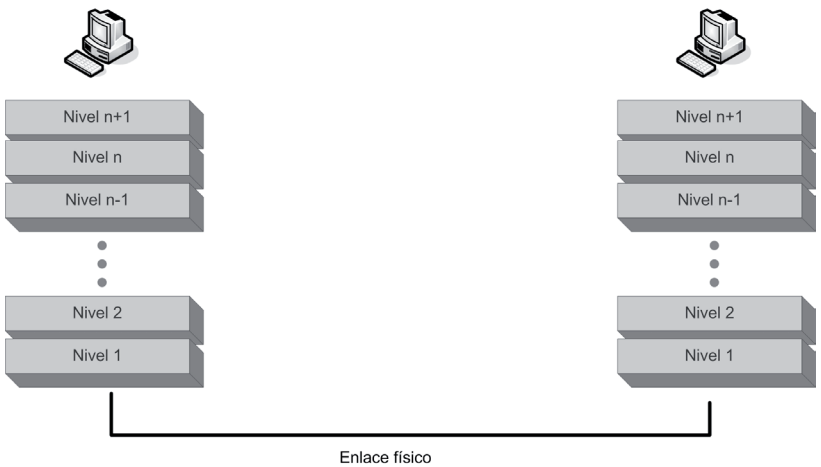


Figura 1.9. *Arquitectura de red por niveles*

RECUERDA

El proceso de comunicación en las redes de datos es complejo. Una posible estrategia para afrontar esta complejidad es agrupar todas las funciones de la comunicación en capas o niveles.

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

- Cada nivel lleva a cabo una serie de funciones de la comunicación. Estas funciones deben estar claramente definidas.
- El número de niveles y su función puede ser diferente en cada arquitectura de red. El número de niveles debe ser suficiente para separar las funciones de forma eficiente, pero un número demasiado alto de niveles complicaría en exceso el diseño.

- Cada nivel *n* conoce la existencia de los niveles adyacentes, es decir, el nivel superior *n*+1 y el nivel inferior *n*-1.
- La comunicación entre niveles adyacentes se lleva a cabo por medio de servicios. Se dice, por tanto, que cada nivel ofrece servicios al nivel superior y utiliza servicios del nivel inferior.
- Una interfaz define básicamente qué información y servicios ofrece un nivel determinado al nivel superior. Es muy importante que las interfaces estén muy bien definidas. Cuando esto ocurre, la implementación específica de las funciones de un nivel puede ser modificada o reemplazada sin realizar ningún cambio en los niveles adyacentes, característica que se conoce como modularidad. Unas interfaces bien definidas proporcionan modularidad a la arquitectura de red.
- El diseño de las interfaces debe hacerse de forma que se minimice el flujo de información entre los niveles, en definitiva, las interfaces deben ser lo más sencillas posible.

A lo largo del tiempo, ha habido dos modelos de arquitectura de red que se han convertido en referencia dentro de las redes de datos y que debemos conocer y entender: uno teórico, el modelo OSI, y otro práctico, el modelo TCP/IP. Más adelante en este capítulo, se proporcionarán algunas nociones básicas del modelo OSI, y en el capítulo 5 se abordará con mayor detalle el modelo que siguen prácticamente todas las redes en la actualidad, el modelo TCP/IP.

1.4.2 TRANSFERENCIA DE INFORMACIÓN EN UN MODELO BASADO EN NIVELES

El fin último de cualquier modelo de red es transferir datos de un sistema a otro. En el caso de un modelo basado en niveles, el flujo de información se lleva a cabo según lo mostrado en la figura 1.10. Cuando un nivel tiene que transferir datos, estos deben pasar obligatoriamente por todos los niveles inferiores hasta alcanzar el destino de la comunicación, donde la información transmitida deberá pasar igualmente por los niveles inferiores hasta alcanzar el nivel de destino.

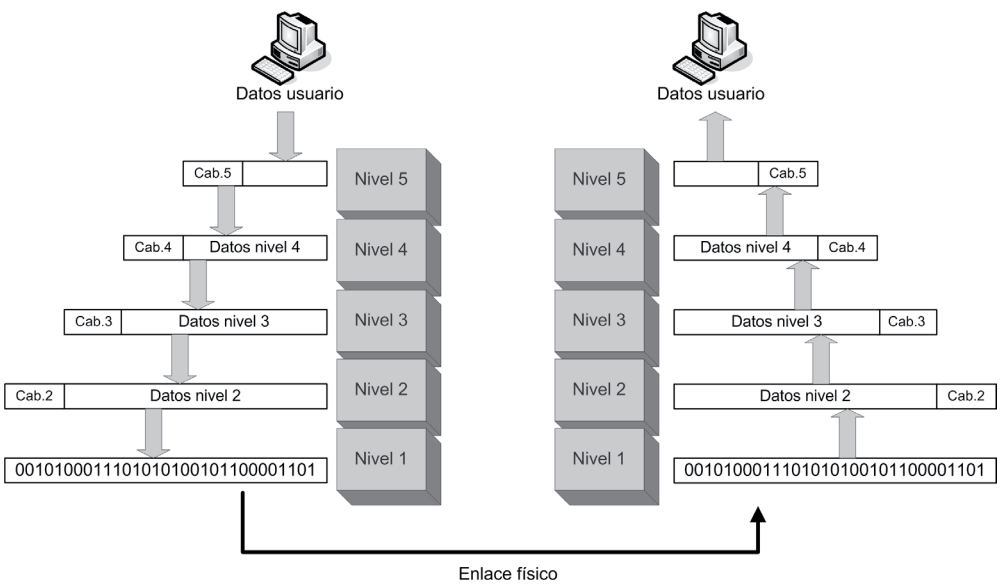


Figura 1.10. *Transferencia de datos en un modelo basado en niveles*

Cada uno de los niveles tiene asignadas una serie de funciones, y algunas de esas funciones necesitan el envío de cierta información de control. Esta información de control se añade al comienzo del bloque de datos y se conoce como **cabecera**. Es fácil deducir que debe haber cierta correspondencia en lo que se hace en el nivel *n* del emisor y el nivel *n* del receptor, a los que se conoce como **niveles homónimos**. Es decir, los niveles homónimos deben "entenderse" para que la comunicación sea efectiva. De hecho, la información de control que contiene la cabecera de un determinado nivel de la comunicación será tratada por el nivel inferior como datos sin ningún significado especial y solo el nivel homónimo en el receptor será capaz de interpretarlos.

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

El mecanismo que permite el "entendimiento" entre dos niveles homónimos de la comunicación se denomina protocolo y es uno de los conceptos clave en la implementación de las redes telemáticas. Un **protocolo** se puede definir como un conjunto de reglas que se establecen para llevar a cabo una comunicación. Muy importante, hay que tener en cuenta que estas reglas se establecen siempre entre niveles homónimos. Así, si dos dispositivos que desean comunicarse mediante una red de datos utilizan diferentes protocolos en un determinado nivel, la comunicación, simplemente, no será posible. A la lista de protocolos empleados en un sistema, con un protocolo por nivel, se le denomina **pila de protocolos**.

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

RECUERDA

Los protocolos son reglas que se establecen para llevar a cabo la comunicación en los niveles homónimos. Este término suele emplearse para referirse a la comunicación en los niveles superiores de los modelos de red.

1.4.3 MODELO OSI

El modelo **OSI** (*Open System Interconnection*, interconexión de sistemas abiertos) fue publicado en 1983 por el organismo de estandarización ISO. Este modelo aparece en la ISO como ISO 7498 y también forma parte de las recomendaciones de la ITU-T como recomendación X.200 (más adelante, en el apartado 1.5 se habla sobre los organismos de estandarización).

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

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

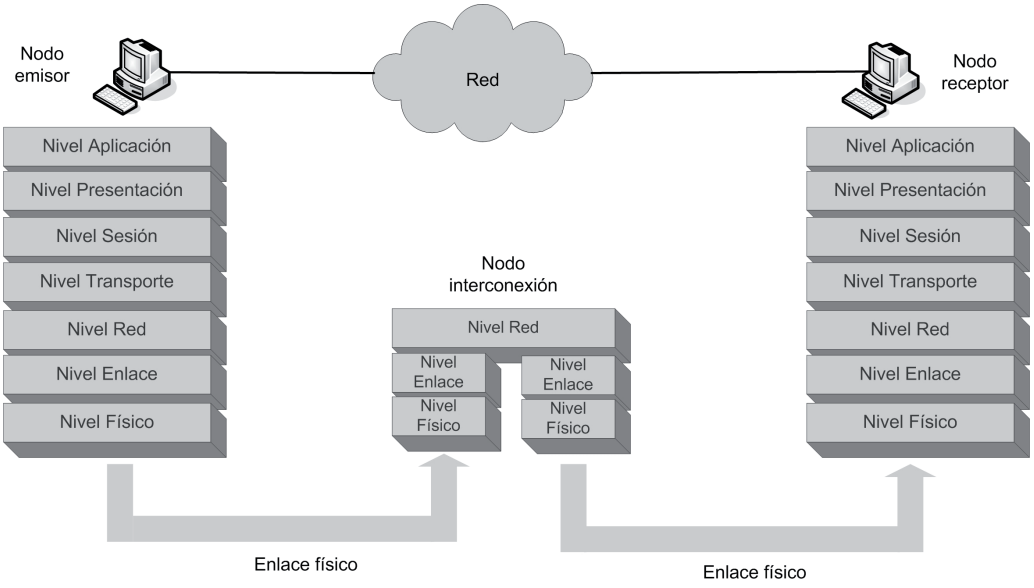


Figura 1.11. *Modelo OSI*

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

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

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

1.4.3.1 Nivel 7. Aplicación

El nivel de aplicación es el nivel de la comunicación en el que un usuario interactúa con la red. Éste es el nivel más alto del modelo y por tanto es el nivel donde se generan los datos que luego viajarán por las redes. En este nivel se define lo que se conoce como **servicios de red**. Cuando un usuario quiere transferir un archivo de un equipo a otro, utiliza un servicio de red de compartición de archivos (por ejemplo, el servicio proporcionado por Windows para compartir archivos). Si desea acceder a la información que una empresa proporciona en su página web, utiliza el servicio web para acceder a dicha información. Tanto la compartición de archivos en red como el acceso a páginas web son ejemplos de servicios proporcionados por el nivel de aplicación.

1.4.3.2 Nivel 6. Presentación

El nivel de presentación se encarga básicamente de aislar las capas inferiores del formato de los datos del nivel de aplicación. Este nivel implementa características que tienen que ver con la sintaxis y la semántica de la información que se intercambia entre un emisor y un receptor.

Para ello, las principales funciones que se llevan a cabo son:

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

1.4.3.3 Nivel 5. Sesión

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

- **Gestión de sesiones**. Para ello implementa las funciones necesarias para crear, mantener y finalizar sesiones de comunicación.
- **Sincronización**. Funciona con el nivel de aplicación para proporcionar conjuntos de datos sencillos llamados puntos de sincronización, que permitirá a una aplicación conocer cómo está progresando la transmisión y recepción de datos. En caso de pérdida de transmisión o de errores es capaz de resincronizar el flujo de información.

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

1.4.3.4 Nivel 4. Transporte

El nivel de transporte se encarga de realizar la entrega completa y sin errores del mensaje desde el origen hasta el destino. Para ello debe desarrollar las siguientes funciones:

- **Control de la conexión**. El nivel de transporte puede proporcionar servicios orientados a la conexión. En este caso, el envío de los datos del emisor al receptor se lleva a cabo en tres pasos: establecimiento de la conexión, transferencia de los datos y finalización de la conexión. Este tipo de servicios proporciona fiabilidad a la comunicación, ya que antes de enviar los datos se comprueba que el receptor está preparado para recibirlos. Un ejemplo de protocolo del nivel de transporte orientado a conexión es TCP. Por el contrario, en los protocolos no orientados a conexión esta función no se lleva a cabo. Un ejemplo de protocolo del nivel de transporte no orientado a conexión es UDP.
- **Control de flujo**. En una transmisión puede ocurrir que el receptor no sea capaz de procesar la información a la velocidad a la que la recibe y por tanto hay que implementar un mecanismo para que el emisor envíe datos solo cuando el receptor los pueda procesar. El nivel de transporte se encarga de llevar a cabo la función de control de flujo de extremo a extremo de la comunicación.

- **Control de errores**. Otra función importante del nivel de transporte es proporcionar mecanismos para detectar y corregir los errores que se produzcan en la comunicación de extremo a extremo. La información en este nivel se envía fragmentada en paquetes y el nivel de transporte se encarga de que los paquetes enviados lleguen sin errores, sin pérdidas y sin duplicados.
- **Direccionamiento**. Un equipo conectado a una red puede tener varios procesos, normalmente en la capa de aplicación, que llevan a cabo comunicación de datos a través de la red. Por ello, es necesario distinguir qué procesos dentro de cada equipo emisor y receptor están intercambiando información. Este direccionamiento se lleva a cabo en el nivel de transporte a través de la llamada dirección de **punto de servicio o dirección de puerto**.

1.4.3.5 Nivel 3. Red

El nivel de red se encarga de todas las funciones necesarias para encaminar la información a través de varias redes. Sus funciones son necesarias cuando el emisor y el receptor están en redes diferentes. Este nivel recibe un paquete de datos del nivel superior y se encarga de que llegue a su destino, siendo necesario llevar a cabo mecanismos de enrutamiento. Las funciones básicas que realiza son:

- **Enrutamiento** de los paquetes. El nivel de red proporciona los mecanismos para la identificación de la ruta que deben llevar los paquetes de datos hasta alcanzar su destino.

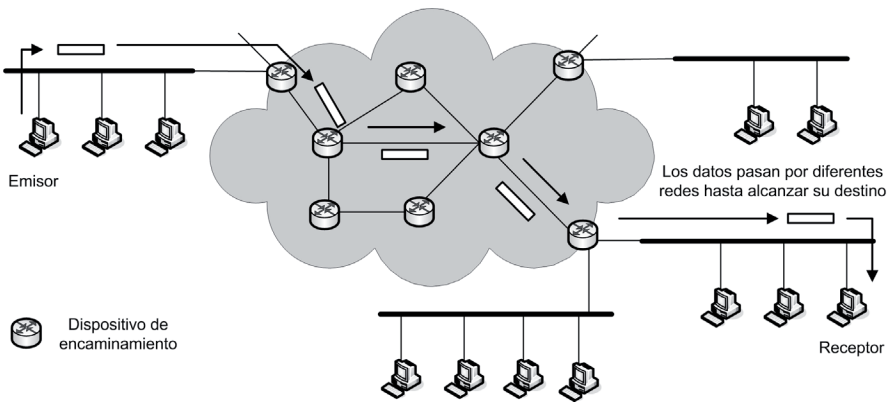


Figura 1.12. *Enrutamiento en el nivel de red*

- Proporcionar un **direccionamiento lógico**. Es necesario establecer un mecanismo de direccionamiento utilizado para identificar cada dispositivo en la red. Además, este direccionamiento debe ser jerárquico, incluyendo información de la red a la que está conectado dicho dispositivo. Por tanto, cada equipo debe identificarse a través de una dirección lógica.
- **Control de la congestión**. La congestión se produce en las redes cuando los dispositivos de enrutamiento no son capaces de manejar el volumen de tráfico presente en la red. El control de la congestión podría confundirse con el control de flujo. La diferencia es que el control de la congestión se implementa para asegurar que la red es capaz de transportar el tráfico ofrecido, mientras que el control de flujo está referido solo a la conexión entre dos dispositivos concretos.

1.4.3.6 Nivel 2. Enlace

La transmisión de los datos se lleva a cabo en el nivel físico, aunque dicho nivel no proporciona ningún mecanismo para asegurar que los datos (bits) que se envían llegarán libres de errores al receptor. El objetivo del nivel físico es llevar a cabo la transmisión de los datos con la mayor fiabilidad posible pero sin llevar a cabo ningún control de errores, función de la que se encarga el nivel de enlace. La principal función del nivel de enlace es, por tanto, proporcionar fiabilidad a la transmisión entre dos dispositivos unidos mediante un enlace. Además, el nivel de enlace lleva a cabo las siguientes funciones:

- **Encapsulación de datos**: **tramado**. Para llevar a cabo las funciones del nivel de enlace se hace necesario dividir el flujo de datos que llega del nivel superior en bloques de datos llamados tramas, a las cuales se añade la cabecera con información de control del nivel de enlace. Una de las informaciones de control más importante que se añade es un código de comprobación de errores. Este código no se incluye en la cabecera, sino que suele ir al final de la trama.
- Proporcionar un **direccionamiento físico**. Esto es necesario en los enlaces multipunto donde hay varios dispositivos conectados a una red y cualquiera de ellos puede ser el receptor de los datos. En este caso es necesario proporcionar un mecanismo de identificación del receptor. De hecho, tanto la dirección física del emisor como del receptor es una información incluida en la cabecera que se añade a los datos en el nivel de enlace.
- **Control de acceso al medio**. Esta función no es siempre necesaria, solo cuando el enlace es compartido por varios dispositivos. En este caso, es el nivel de enlace el encargado de determinar qué dispositivo puede acceder al medio para transmitir.
- **Control de flujo**. El control de flujo llevado a cabo en este nivel se refiere al control del flujo de información en un enlace. El objetivo de esta función es que el emisor envíe información a través del enlace solo cuando el receptor pueda procesarla.
- **Control de errores**. Como ya se ha apuntado, ésta es la principal función del nivel de enlace: detectar y corregir los errores de transmisión producidos en un enlace. Esta función incluye la capacidad de detectar y retransmitir tramas con error y tramas perdidas, así como detectar tramas duplicadas.

Es importante diferenciar las funciones de control de flujo y de errores llevadas a cabo en el nivel de enlace y en el nivel de transporte. El nivel de enlace lleva a cabo estas funciones en un enlace y el nivel de transporte lo hace pero para la comunicación de extremo a extremo.

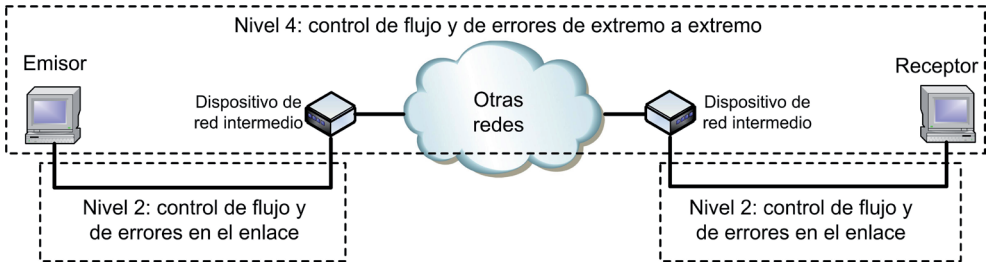


Figura 1.13. *El control de flujo y de errores se aplica en dos niveles*

Se puede observar que existen 3 niveles en los que se llevan a cabo funciones de direccionamiento, aunque en cada nivel la función de la dirección es diferente. En el nivel de enlace, la dirección (llamada dirección física) sirve para identificar un dispositivo en un enlace donde puede haber varios dispositivos conectados. En el nivel de red, la dirección (llamada dirección lógica) se utiliza para identificar un dispositivo de forma única en un conjunto de redes. En el nivel de transporte, la dirección (llamada dirección de puerto) sirve para identificar dentro de un dispositivo a qué aplicación van dirigidos los datos. Todas las direcciones son transmitidas en sus correspondientes cabeceras.

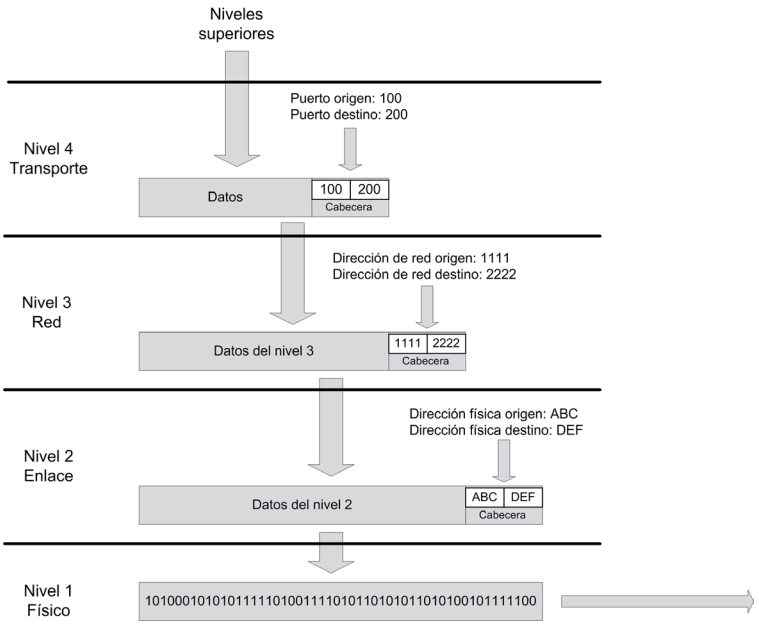


Figura 1.14. *Direccionamiento en los distintos niveles del modelo OSI*

1.4.3.7 Nivel 1. físico

El nivel físico se encarga de la transmisión de la información a través de un medio físico, es decir, el nivel físico debe ser capaz de enviar datos (bits) a través de un canal de comunicaciones (cable de cobre, fibra óptica, aire) procurando que esos datos no sufran alteraciones y puedan ser correctamente interpretados en el receptor. Para lograr este propósito se llevan a cabo las siguientes funciones:

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

- **Configuración de la línea**. Que está referido a la forma en la que se conectan los dispositivos al medio. Puede ser punto a punto o multipunto.
- **Topología física**. La topología se refiere a la forma en la que están conectados entre sí los dispositivos de una red telemática.
- **Modo de transmisión**: que puede ser símplex, half-dúplex, full-dúplex.
- **Velocidad de transmisión**. Con todas las características anteriores se establece la velocidad a la que se pueden transmitir los datos, es decir, la tasa de bits de la comunicación.

La mayor parte de las funciones que aparecen en la lista anterior serán ampliadas en los próximos capítulos. Los principales organismos dedicados a estandarizar las distintas implementaciones del nivel físico han sido la EIA y la ITU-T.

1.4.4 EL MODELO OSI FRENTE A TCP/IP

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

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

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

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

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

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

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

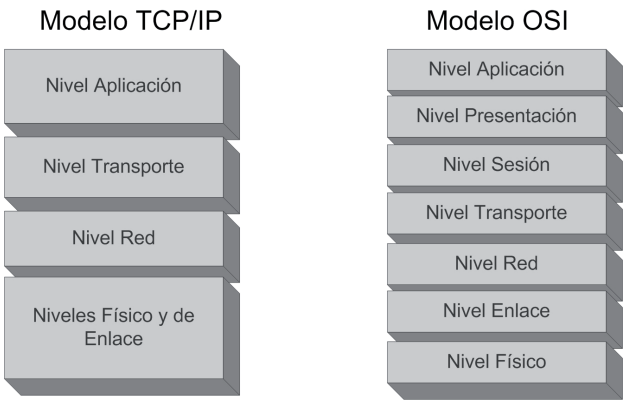


Figura 1.15. *El modelo TCP/IP frente al modelo OSI*

1.5 ESTÁNDARES Y ORGANISMOS DE ESTANDARIZACIÓN

Un **estándar** en el ámbito tecnológico es un modelo o norma que se utiliza como referencia para el desarrollo de un producto o servicio. Los estándares son normalmente desarrollados por **organismos oficiales de estandarización**. Los organismos de estandarización son instituciones formadas normalmente por empresas del sector o comités técnicos de los países que desean participar en la elaboración de estándares. Actualmente juegan un papel fundamental en la implantación de nuevas tecnologías.

La existencia de un estándar, sin embargo, no siempre está ligada a un organismo oficial de estandarización. En algunas ocasiones, hay un desarrollo tecnológico proporcionado inicialmente por una organización u organismo no oficial y se convierte en estándar debido a la extensión de su uso. Es el llamado estándar de facto. En función de esta característica, los estándares se pueden clasificar en dos grupos:

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

En muchos casos, la existencia de estándares abiertos ha favorecido la implantación masiva de muchas tecnologías. Este tipo de estándares proporciona un modelo de desarrollo abierto que hace que un producto funcione adecuadamente con otros, sin tener en cuenta el fabricante. Los estándares abiertos son esenciales para crear y mantener un mercado abierto y competitivo.

Gracias a los estándares abiertos podemos, por ejemplo, adquirir un ordenador portátil de la marca que nos parezca más conveniente y no preocuparnos de si será capaz de reproducir música, películas, leer correctamente información en soportes extraíbles como DVD o *pendrives*, conectarse a nuestra red doméstica, ya sea por cable o de

forma inalámbrica. No nos preocupamos de estos aspectos precisamente porque existen estándares que permiten que los fabricantes y empresas involucradas en todos los aspectos mencionados anteriormente tengan una guía común que haga que sus productos sean compatibles.

Veamos algunos ejemplos de estándares relacionados con las tecnologías:

DVD	Disco óptico de almacenamiento de datos. Realmente, esta denominación genérica engloba muchos estándares como DVD-Video, DVD-ROM, DVD-R, DVD+R, etc.	
Wi-Fi	Nombre comercial para los productos que operan en redes locales inalámbricas utilizando el estándar IEEE 802.11.	
GSM	Sistema digital de comunicaciones móviles usado en teléfonos móviles.	
HTML	Lenguaje de marcas utilizado para elaborar páginas web.	

Existen a nivel mundial varias organizaciones encargadas de proponer y desarrollar los estándares utilizados en las redes telemáticas:

- **ISO** es la Organización Internacional de Estandarización (en inglés, *International Organization for Standardization*). Creada en 1947 y formada actualmente por 162 países. Este organismo elabora estándares en muchos ámbitos, como por ejemplo las medidas del papel (ISO A4), lenguaje de programación C (ISO 9899), sistema de codificación de audio y video MPEG-2 (ISO/IEC 13818), sistemas de gestión de calidad (ISO 9000). Una de las principales aportaciones de la ISO a las redes telemáticas es el modelo OSI (ISO 7498).
- **ITU** (*International Telecommunications Union*, Unión Internacional de Telecomunicaciones). Es un organismo internacional dependiente de las Naciones Unidas encargado de coordinar los servicios y las redes globales de telecomunicación. Está dividido en tres sectores:
  - ITU-R desarrolla estándares para las radiocomunicaciones.
  - ITU-T se encarga del desarrollo de estándares de telecomunicaciones.
  - ITU-D encargado del desarrollo en concreto de proyectos e iniciativas dentro del sector.
- **ETSI** (*European Telecommunications Standards Institute*, Instituto Europeo de Estándares de Telecomunicaciones). Es una organización constituida para el desarrollo de estándares especialmente de ámbito europeo. Está formado por 655 miembros de 59 países diferentes tanto de Europa como de fuera de Europa.
- **IEEE** (*Institute of Electrical and Electronics Engineers*, Instituto de Ingenieros Eléctricos y Electrónicos). Organismo formado por profesionales de las nuevas tecnologías, electricidad, electrónica y comunicaciones. Una de sus principales labores es la de la estandarización. Uno de sus más destacados trabajos está desarrollado por un comité conocido como Proyecto 802 dedicado a estandarizar sistemas de red.

- **IETF** (*Internet Engineering Task Force*, Grupo de Trabajo de Ingeniería de Internet). Es un organismo internacional dedicado a tareas de normalización sobre aspectos relacionados con la evolución de la arquitectura de Internet. Los estándares propuestos por este organismo se publican como documentos públicos conocidos como **RFC** (siglas de *Request For Comment*).
- **ANSI** (*American National Standards Institute*, Instituto Nacional Americano de Estándares). Es el equivalente americano del ETSI. Su dilatada historia (nació en 1919) ha hecho que muchos de los estándares publicados por ANSI se hayan adoptado a nivel mundial.
- **EIA** (*Electronics Industries Alliance*, Alianza de Industrias Electrónicas). Otro organismo de estandarización norteamericano formado principalmente por empresas del sector tecnológico y enfocado a proporcionar estándares para el mercado americano, como por ejemplo el famoso interfaz serie EIA-232, antes conocido como RS-232. La EIA también se ha encargado de desarrollar las normas de cableado estructurado que luego se han aplicado a nivel mundial.

1.6 REDES DE COMUNICACIONES

1.6.1 TOPOLOGÍAS DE RED

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

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

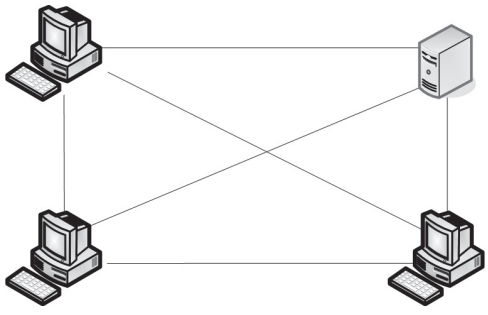


Figura 1.16. *Topología en malla*

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

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

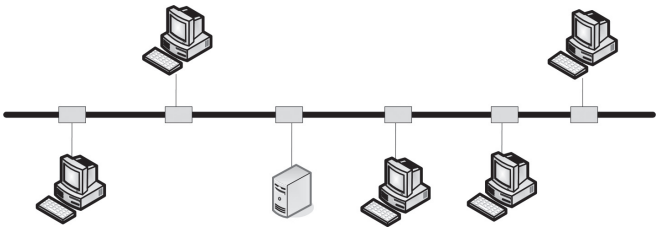


Figura 1.17. *Topología en bus*

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

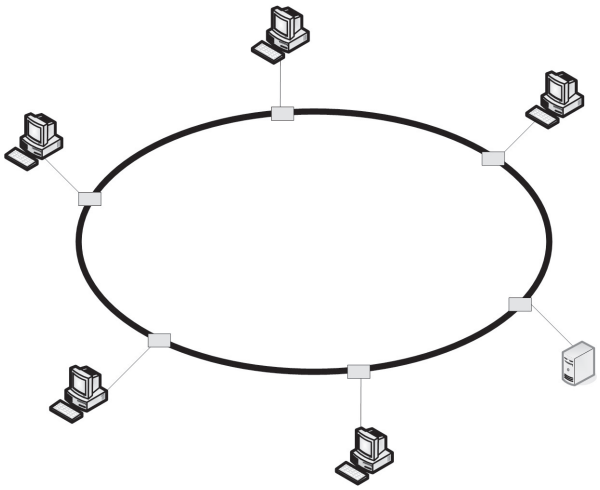


Figura 1.18. *Topología en anillo*

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

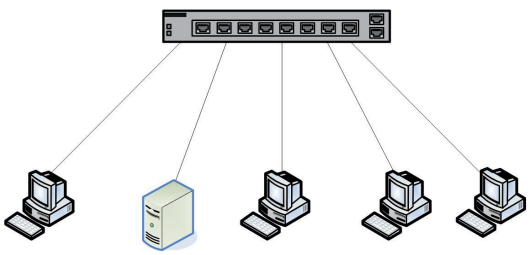


Figura 1.19. *Topología en estrella*

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

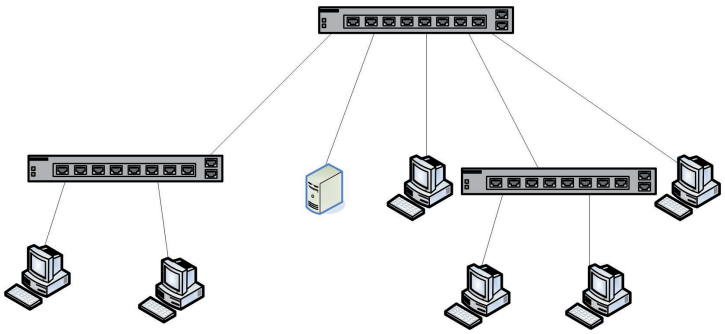


Figura 1.20. *Topología en árbol*

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

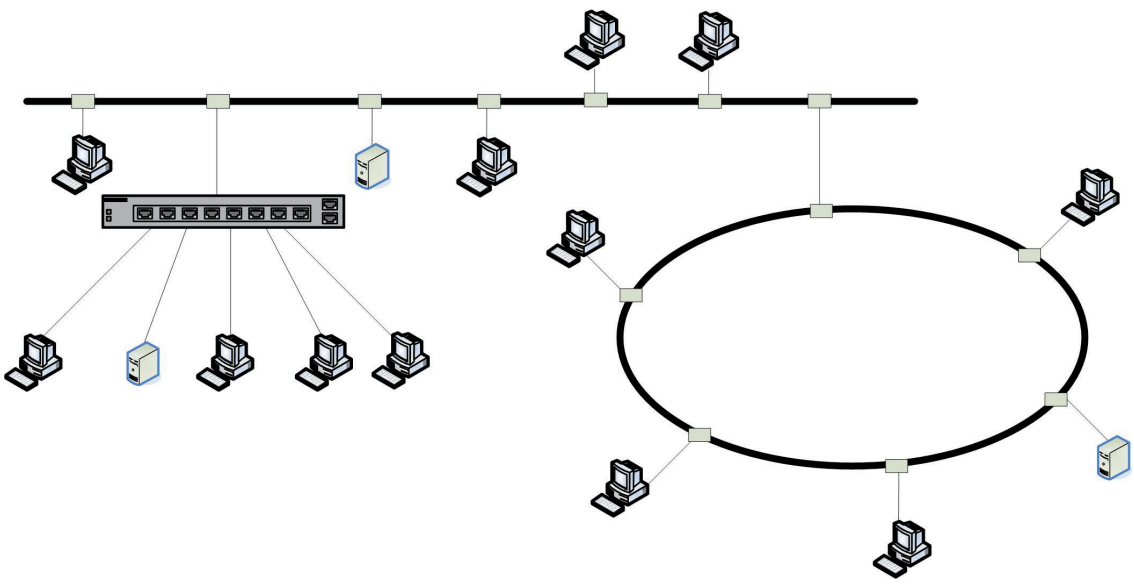


Figura 1.21. *Topología híbrida*

1.6.2 TECNOLOGÍAS UTILIZADAS EN LAS REDES DE COMUNICACIONES

Como hemos visto, existen tres tipos de redes de comunicaciones: las redes LAN, MAN y WAN. En este apartado se ofrecerá una visión general de las diferentes tecnologías empleadas en cada tipo.

1.6.2.1 Redes LAN

En la actualidad existen solo dos tecnologías que dominan las redes LAN y que serán estudiadas con detalle en los próximos capítulos:

- **Ethernet**. La mayor parte de las redes LAN cableadas actuales utilizan esta tecnología debido a su facilidad de uso y su alta fiabilidad. Dicha tecnología, además, es altamente escalable, es decir, se utiliza tanto en pequeñas redes domésticas como en grandes redes corporativas. Las redes Ethernet actuales utilizan una topología en estrella o en árbol, siendo el *switch* el principal dispositivo de interconexión.
- **Wi-Fi**. Al igual que Ethernet, la tecnología Wi-Fi es el estándar actual utilizado en redes LAN inalámbricas, teniendo especial éxito en el ámbito doméstico. Al igual que en Ethernet, en Wi-Fi se utiliza una topología en estrella en la cual un dispositivo conocido como punto de acceso inalámbrico es el dispositivo de interconexión utilizado, que además sirve para la conexión de la red inalámbrica con una red cableada.

1.6.2.2 Redes MAN y WAN

Las grandes redes de comunicación están englobadas dentro los términos MAN y WAN y permiten la conectividad entre equipos cubriendo distancias más grandes de las que se pueden cubrir con redes LAN. Habitualmente las redes MAN y especialmente las redes WAN son implementadas por empresas de telecomunicaciones específicas. Antes de dar un repaso a las tecnologías utilizadas hay que tener en cuenta que la arquitectura global de la mayor parte de las redes de estos tipos se puede dividir en dos partes:

- **Red de acceso**. Utilizada como punto de conexión de los usuarios de la red. Para implementarla se utilizan tecnologías específicas. Los usuarios que acceden a la red de acceso, en muchos casos, especialmente en redes MAN son empresas que necesitan interconectar diferentes redes LAN.
- **Red de transporte**. También conocido como *core network* o simplemente *core*, es la infraestructura de comunicaciones que lleva a cabo la comunicación de los diferentes clientes de la red. Lo habitual es utilizar la fibra óptica como medio de transmisión, y la tecnología utilizada permite la transmisión de datos a muy altas velocidades.

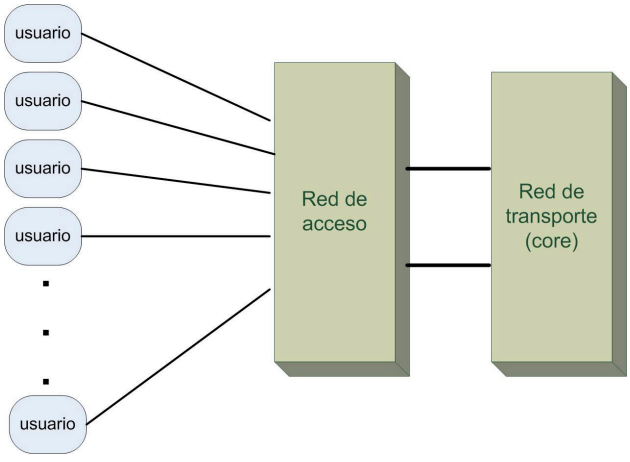


Figura 1.22. *Arquitectura de las redes MAN y WAN*

Las tecnologías empleadas en redes MAN y WAN:

- **Frame Relay** (retransmisión de tramas). Tecnología utilizada especialmente en redes WAN tanto en la red de acceso como en la red de transporte. Está basada en la conmutación de paquetes y cubre las funciones de los dos primeros niveles del modelo OSI, el nivel físico y el nivel de enlace. Se empezó a utilizar a principios de los años 90 y actualmente su uso es residual. Uno de sus inconvenientes es que no es muy eficiente para manejar tráfico de datos de audio o video.
- **ATM** (*Asynchronous Transfer Mode*, modo de transferencia asíncrona). Tecnología basada en la conmutación de paquetes, al igual que Frame Relay, pero que ofrece prestaciones superiores tanto en velocidad como en el tratamiento de diferentes tipos de tráfico, es decir, gestiona eficazmente la transmisión tanto de datos como de audio y video. Actualmente ATM se utiliza en la red de transporte de las redes MAN y WAN, y cubre las funciones del nivel físico y del nivel de enlace del modelo OSI.

El concepto de conmutación de paquetes es una técnica utilizada en las redes de comunicación para optimizar las infraestructuras. Se pueden ver más detalles sobre la conmutación en el próximo capítulo

- **xDSL**. Conjunto de tecnologías utilizadas principalmente en la red de acceso de las redes WAN que permiten una conexión de datos de alta velocidad a través de un par de cable telefónico. Diseñada para aprovechar las infraestructuras de acceso del sistema telefónico. Uno de los tipos más utilizados en España es ADSL.
- **3G**. Conjunto de tecnologías inalámbricas que utilizan la red de acceso de la telefonía móvil para el acceso a una red WAN. Utilizada por los operadores de telefonía móvil para proporcionar acceso a Internet a sus clientes.
- **WiMAX**. Tecnología inalámbrica utilizada habitualmente en la red de acceso a redes MAN o WAN. Puede cubrir áreas de varios kilómetros, por lo que es una opción muy interesante para proporcionar acceso a redes en zonas donde no hay infraestructuras cableadas.
- **Metro Ethernet**. Actualmente se está imponiendo como la tecnología dominante en redes MAN. Los últimos desarrollos Ethernet sobre fibra permiten velocidades de hasta 10 Gbps, cubriendo distancias de varias decenas de kilómetros. La gran ventaja del uso de Metro Ethernet es que apenas requiere conversión de formatos para la comunicación de redes LAN y para la interconexión entre la red de acceso y la red de transporte, ya que todas las partes de la comunicación utilizan Ethernet como tecnología base.

IMPORTANTE

En la lista anterior aparecen las principales tecnologías utilizadas en la actualidad, pero a lo largo de los años han surgido otras muchas tecnologías que, o bien se han ido abandonando, o bien su uso es ya muy minoritario:

- Redes LAN cableadas: Token Ring, Token Bus.
- Redes LAN inalámbricas: HiperLAN, HiSWAN.
- Redes MAN: FDDI, DQDB, SMDS.
- Redes WAN: X.25.

EJERCICIOS PROPUESTOS

1. Elabora una lista de los estándares que conozcas relacionados con las redes telemáticas y averigua si son estándares abiertos o cerrados. En el caso de estándares abiertos, obtén el organismo encargado de su desarrollo. Para los estándares cerrados, averigua qué empresa u organismo lo ha desarrollado.

2. Aplica los conceptos que aparecen en la jerarquía por niveles del modelo OSI a una empresa de logística que envía paquetes de todo tipo a cualquier lugar del mundo. Para ello define primero las funciones, los niveles y asigna cada función en uno de los niveles definidos. Aplica en alguno de los niveles definidos el concepto de interfaz y de protocolo. A continuación se sugieren algunos aspectos que se deben tener en cuenta en la definición de las funciones:

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

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

TEST DE CONOCIMIENTOS

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

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

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

4 Para que haya comunicación entre dos niveles homónimos en el modelo OSI es necesario que utilicen:
- **a)** El mismo protocolo.
- **b)** La misma interfaz.
- **c)** El mismo lenguaje de programación.
- **d)** El mismo sistema operativo.

5 La información contenida en una cabecera la procesa:
- **a)** El nivel superior.
- **b)** El nivel inferior.
- **c)** El nivel homónimo.
- **d)** El nivel más alto.

6 El nivel que asegura la transmisión fiable de datos en un enlace simple es:
- **a)** El nivel físico.
- **b)** El nivel de enlace.
- **c)** El nivel de transporte.
- **d)** El nivel de aplicación.

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

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

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

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

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

2 Principios de transmisión de datos

En el capítulo anterior planteamos que, para afrontar la complejidad de las redes de datos, era necesario aplicar un modelo de capas que permitiera agrupar en niveles menos complejos las múltiples funciones que es necesario resolver. Utilizando el modelo OSI como referencia, el único nivel en el que se produce el "movimiento" real de la información es en el nivel físico. Vamos a dedicar un par de capítulos a revisar conceptos relacionados con la transmisión de los datos propiamente dicha. En este capítulo repasaremos los fundamentos sobre señales eléctricas y las principales técnicas utilizadas para la transmisión de los datos, tales como la codificación, multiplexación y conmutación. En el próximo capítulo se repasarán los medios de comunicación utilizados en las redes telemáticas para transportar los datos. Una vez más, recuerdo que todos estos conceptos están englobados dentro del nivel 1, del nivel físico.

2.1 CONCEPTOS DE TRANSMISIÓN DE DATOS

2.1.1 MODOS DE TRANSMISIÓN: SÍMPLEX, SEMI-DÚPLEX Y DÚPLEX

En la mayor parte de las ocasiones tendremos dos dispositivos que se intercambian datos conectados mediante un medio de transmisión. Este intercambio de datos se puede hacer de varias formas en función de la dirección del flujo de las señales enviadas entre los dos dispositivos enlazados, lo que se conoce como **modos de transmisión**:

- **Símplex**, cuando se establece una comunicación unidireccional entre los dos dispositivos. Un dispositivo solo recibe y el otro solo envía. Un ejemplo de comunicación símplex podría ser la radio o la televisión.
- **Half-dúplex o semi-dúplex**, cada dispositivo puede enviar y recibir datos pero no al mismo tiempo. Cuando un dispositivo envía, el otro solo puede recibir y viceversa. Un ejemplo de este tipo de comunicación son los *walkie talkies*.
- **Full-dúplex o dúplex**, cuando los dos dispositivos que llevan a cabo la comunicación pueden enviar y recibir de forma simultánea. Para ello debe haber dos caminos físicos diferentes o se tiene que dividir la capacidad del enlace en dos canales. Un ejemplo de comunicación dúplex es la que se lleva a cabo en un ordenador conectado a una LAN.

2.1.2 TRANSMISIÓN DE DATOS EN SERIE Y EN PARALELO

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

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

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

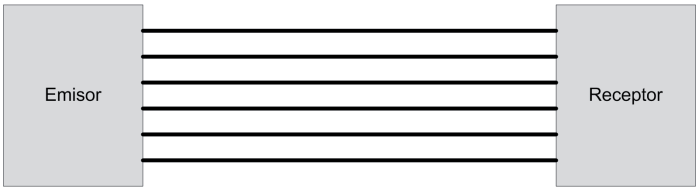


Figura 2.1. *Transmisión de datos en paralelo*

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

Figura 2.2. *Transmisión de datos en serie*

En la actualidad, prácticamente todas las comunicaciones se llevan a cabo transmitiendo los datos en serie.

2.1.3 CONFIGURACIÓN DE LÍNEA: PUNTO A PUNTO Y MULTIPUNTO

Existen dos formas de conectar los dispositivos de una red a un enlace. El enlace es el medio físico por el que se transfieren los datos. A este concepto se le conoce como **configuración de línea**.

- **Punto a punto**. La conexión recibe este nombre cuando existe un enlace dedicado entre dos dispositivos. Toda la capacidad del enlace se reserva para la transmisión entre ambos dispositivos. También se conoce como conexión dedicada. Esta configuración es la más habitual en las redes cableadas actuales.

Figura 2.3. *Configuración punto a punto*

- **Multipunto**. La conexión recibe este nombre cuando varios dispositivos comparten el mismo enlace. En esta configuración, la capacidad del enlace está compartida en el espacio o en el tiempo. Esta configuración se puede utilizar sobre todo en redes inalámbricas. La tecnología de redes LAN cableadas conocida como Ethernet, que se estudiará en el capítulo 6, hace uso de la configuración multipunto en sus primeras versiones. Hoy en día prácticamente está en desuso.

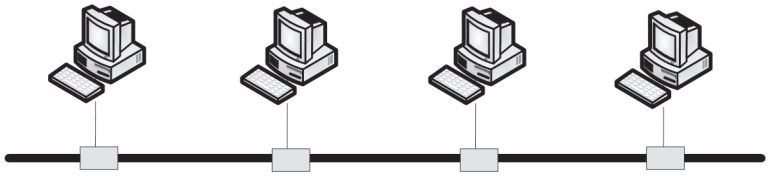


Figura 2.4. *Configuración multipunto*

2.2 TRANSMISIÓN ANALÓGICA Y DIGITAL

La práctica totalidad de los dispositivos que están conectados a redes telemáticas son dispositivos digitales, es decir, todos los datos con los que trabajan son datos digitales. Los datos digitales habitualmente están constituidos solo por dos estados, representados como 0 y 1. Por tanto, cualquier información digital del tipo que sea (audio, vídeo, texto, imágenes…) se puede representar como una larga sucesión de unos y ceros. Estos datos, en última instancia y para ser transmitidos, deben transformarse en señales eléctricas (o señales electromagnéticas para el caso de utilizar como medio de transmisión el aire). Por tanto, la transmisión de datos se basa en el envío de señales eléctricas o señales electromagnéticas a través de un medio de transmisión.

Existen dos tipos de señales eléctricas que se pueden utilizar para transmitir información: **señales analógicas y señales digitales**. Parece que lo más lógico es que, si tenemos que transmitir información digital, utilicemos señales digitales, pero no siempre será posible, debido fundamentalmente a la naturaleza del medio de transmisión que utilicemos. Así pues, para transmitir información digital a través de un medio de transmisión podremos utilizar tanto señales analógicas como digitales. Vamos a hacer un repaso a sus principales características.

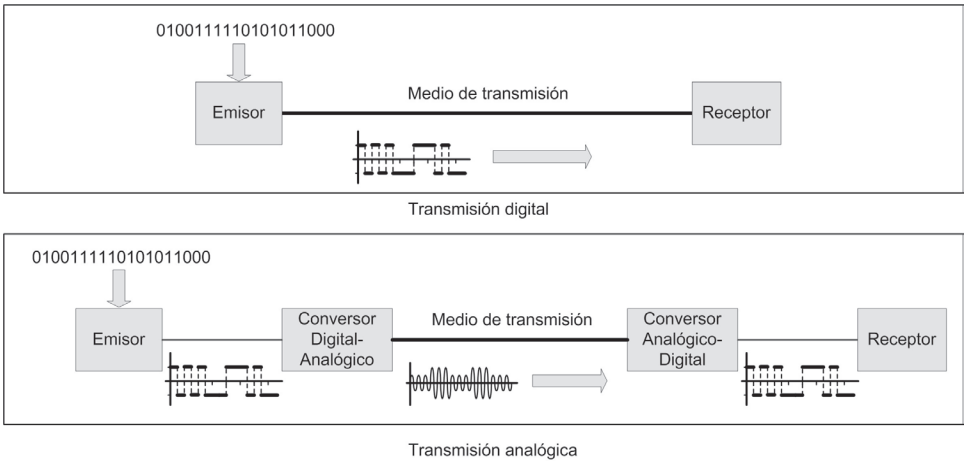


Figura 2.5. *Esquema básico de transmisión con señales analógicas y digitales*

RECUERDA

Los datos en las redes telemáticas se pueden transmitir utilizando tanto señales analógicas como digitales.

2.2.1 SEÑALES ANALÓGICAS Y DIGITALES

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

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

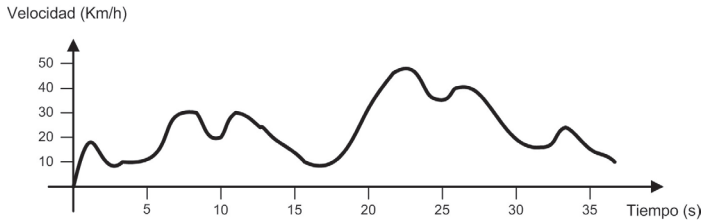


Figura 2.6. *Representación de la variación de la velocidad de un vehículo como ejemplo de una magnitud analógica*

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

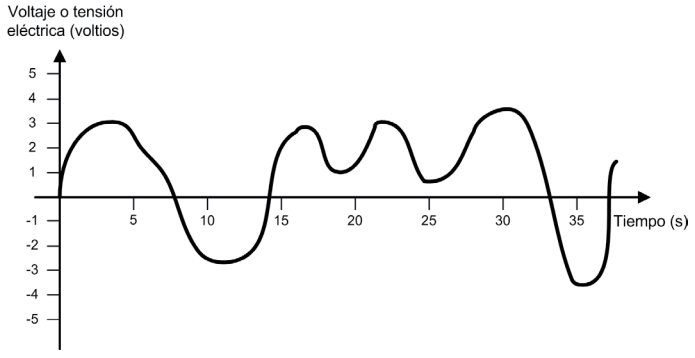


Figura 2.7. *Representación de una señal analógica*

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

la velocidad es una magnitud analógica, la medición de la misma es digital. El velocímetro pasará de 10 a 20 km/h, pero la velocidad realmente aumentará de forma continua, pasando por todas las posibles velocidades entre 10 y 20.

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

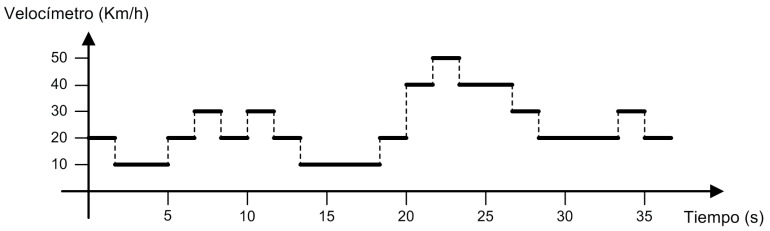


Figura 2.8. *Representación de una magnitud digital*

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

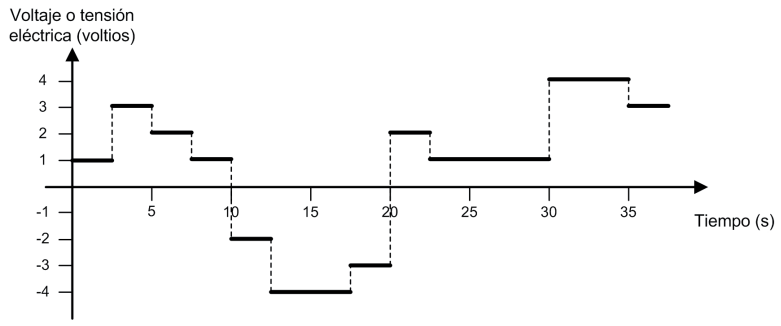


Figura 2.9. *Representación de una señal digital*

La señal de la figura anterior puede tomar hasta ocho valores diferentes en el rango de entre -4 v y + 4 v. Sin embargo, una de las señales digitales más comunes son aquellas que solo pueden tomar dos valores. A estas señales se les denomina **señales digitales binarias**. En la siguiente figura se representa una señal digital binaria que puede tomar solo dos valores, +5 v y -5 v.

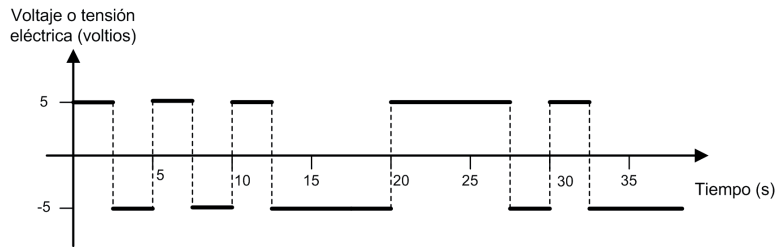


Figura 2.10. *Ejemplo de la representación de una señal digital binaria*

RECUERDA

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

2.2.2 SEÑALES PERIÓDICAS Y APERIÓDICAS

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

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

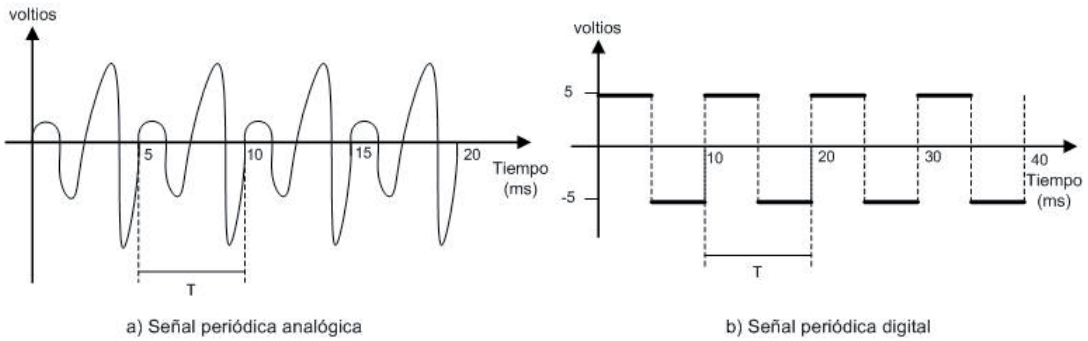


Figura 2.11. *Ejemplos de señales periódicas*

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

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

Las señales aperiódicas son aquellas que no presentan ningún patrón de repetición en el tiempo. Las figuras 2.7 y 2.9 son ejemplos de señales aperiódicas, la primera analógica y la segunda digital.

2.2.3 SEÑALES ANALÓGICAS SIMPLES

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

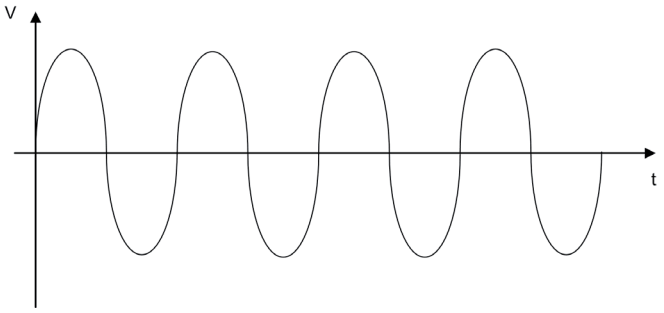


Figura 2.12. *Señal sinusoidal*

La expresión matemática que define la función seno es:

$V(t) = A_0 \text{ sen } (wt + \varphi)$

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

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

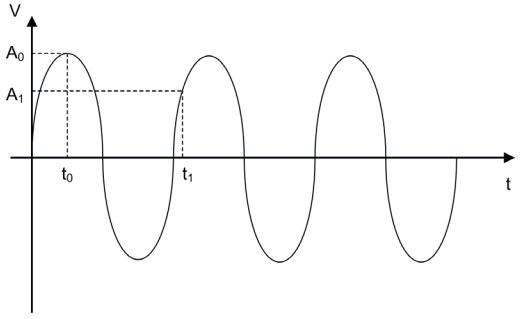


Figura 2.13. *La amplitud en las señales sinusoidales*

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

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

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

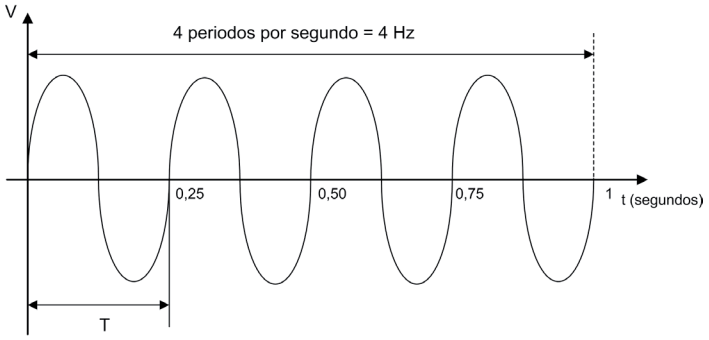


Figura 2.14. *La frecuencia en una señal sinusoidal*

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

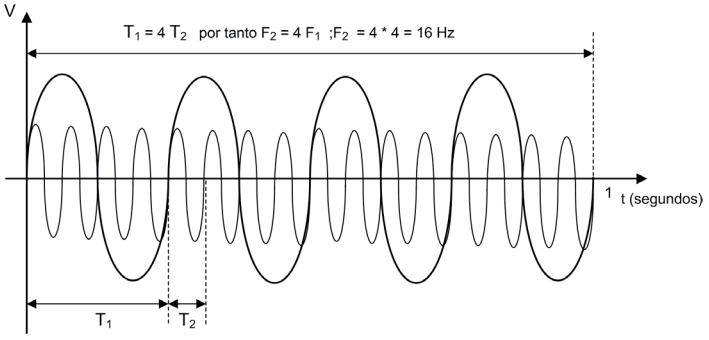


Figura 2.15. *Comparación de dos señales con distinta frecuencia*

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

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

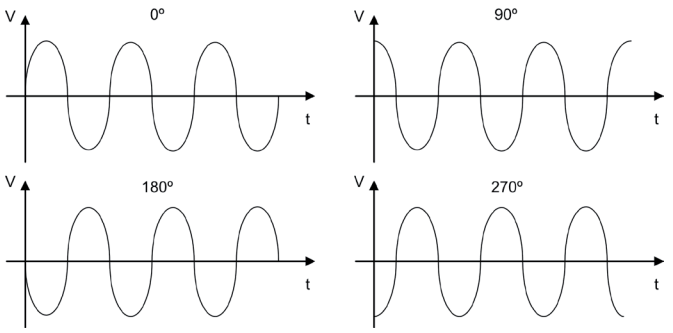


Figura 2.16. *Comparación de señales con diferentes fases*

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

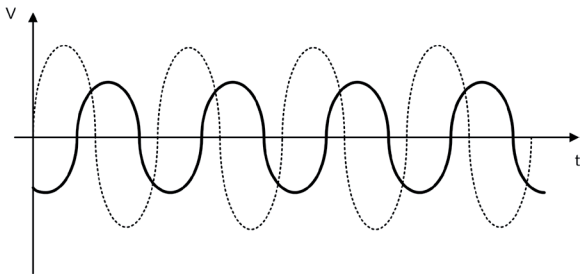


Figura 2.17. *Fase de una señal respecto a otra señal de referencia*

2.2.4 SEÑALES ANALÓGICAS COMPUESTAS

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

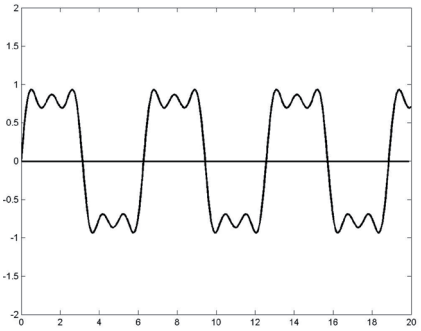


Figura 2.18. *Ejemplo de señal periódica compuesta*

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

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

$V(t) = A_0 + A_1 \text{sen}\,(wt+\theta_1) + A_2 \text{sen}\,(2wt+\theta_2) + A_3 \text{sen}\,(3wt+\theta_3) + \ldots + A_n \text{sen}\,(nwt+\theta_n)$

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

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

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

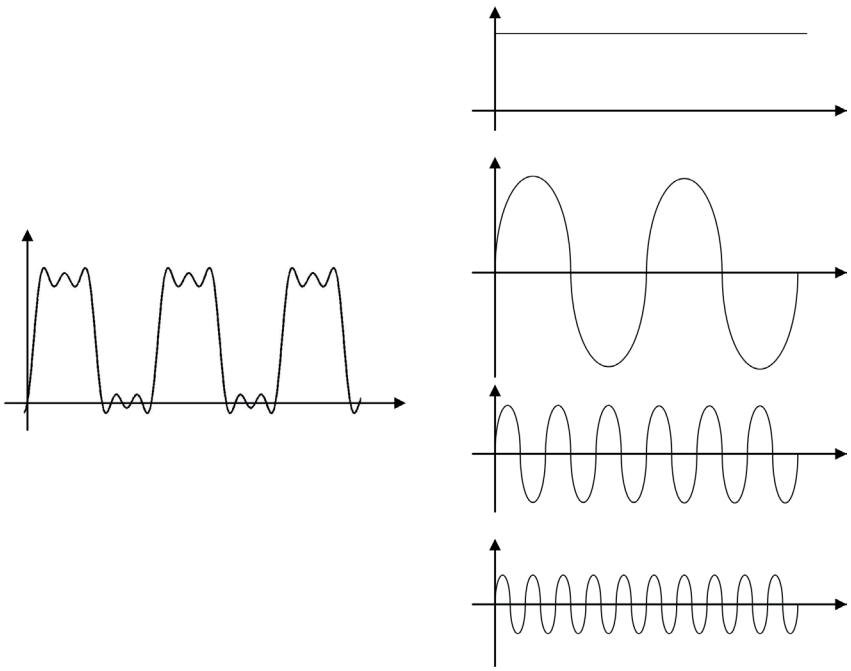


Figura 2.19. *Señal periódica formada por cuatro componentes sinusoidales*

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

2.2.5 DOMINIO DE LA FRECUENCIA: ESPECTRO Y ANCHO DE BANDA

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

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

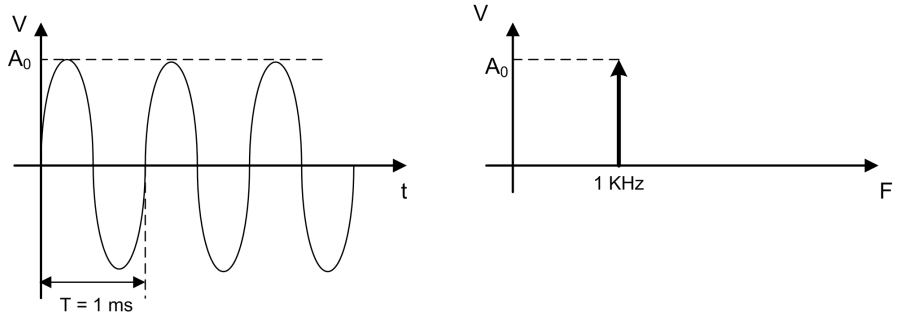


Figura 2.20. *Representación de una señal sinusoidal en el dominio de la frecuencia*

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

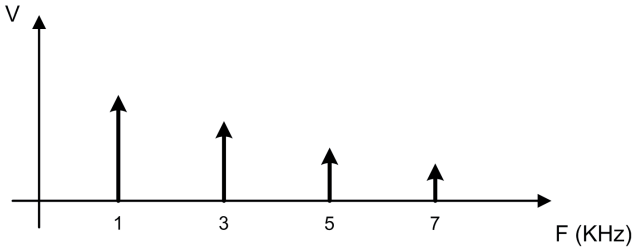


Figura 2.21. *Representación en el dominio de la frecuencia de una señal periódica compuesta*

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

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

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

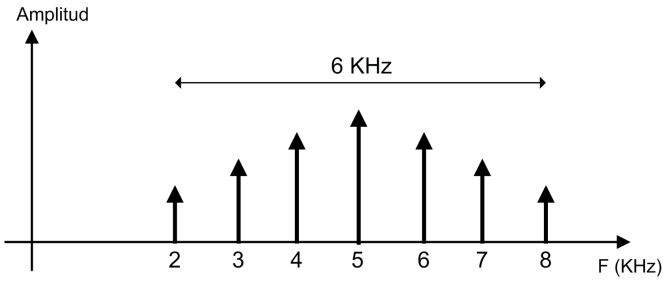


Figura 2.22. *Ancho de banda*

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

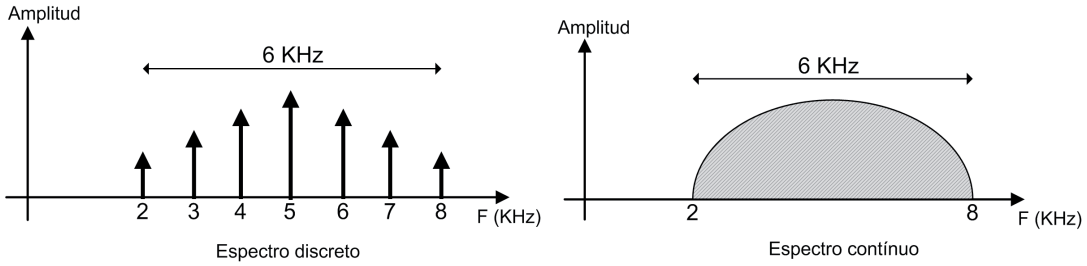


Figura 2.23. *Espectro discreto vs. continuo*

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

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

Por último, es interesante apuntar que existe una relación entre las series y la transformada de Fourier: la transformada de Fourier de una señal aperiódica es la envolvente de las series de Fourier para esa misma señal convertida en periódica.

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

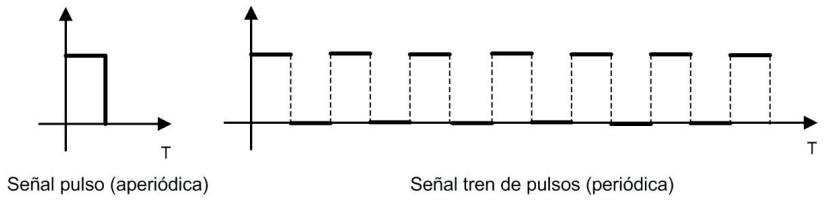


Figura 2.24. *Representación de las señales pulso y tren de pulsos*

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

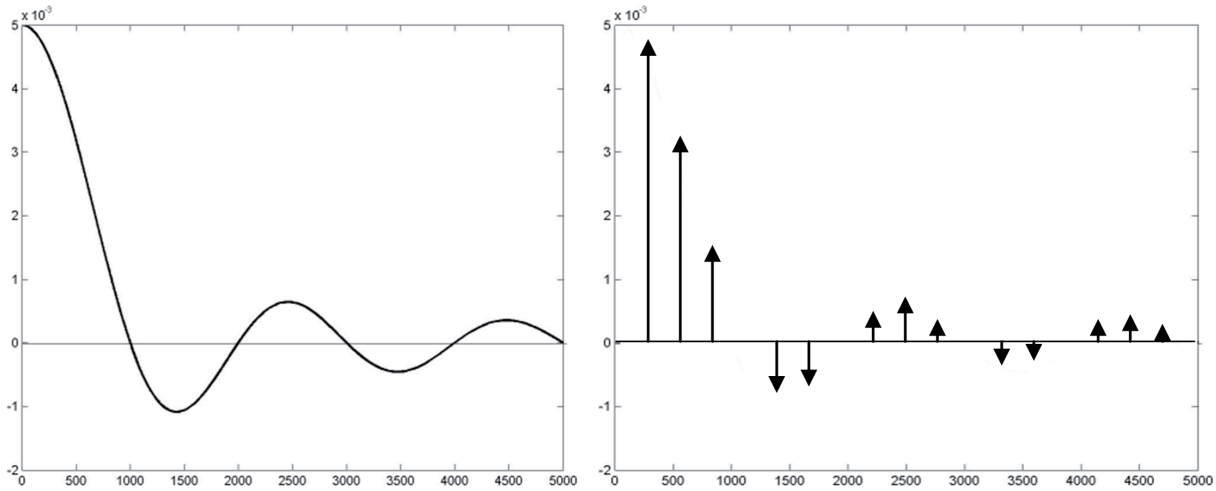


Figura 2.25. *Señales pulso y tren de pulsos en el dominio de la frecuencia*

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

RECUERDA

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

2.2.6 SEÑALES DIGITALES

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

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

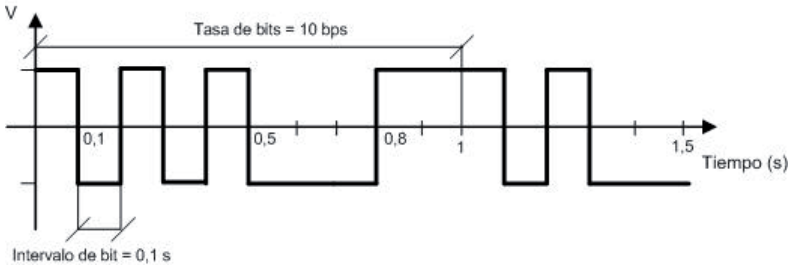


Figura 2.26. *Señal digital con sus parámetros característicos*

En la siguiente figura se representan dos señales digitales, la primera periódica y la segunda aperiódica.

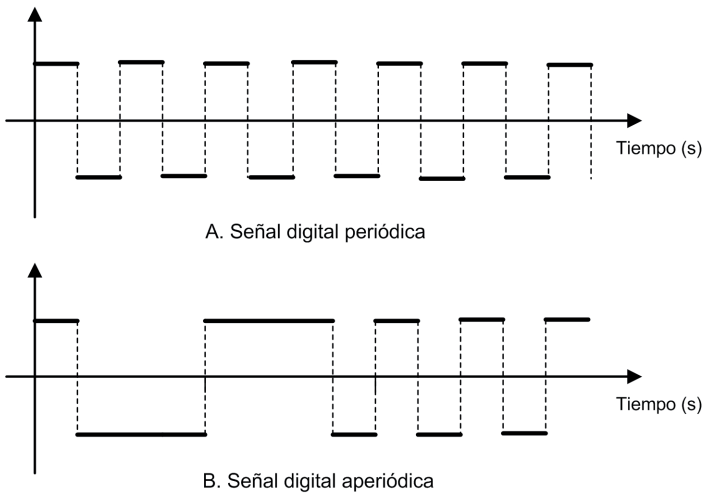


Figura 2.27. *Comparación señal digital periódica y aperiódica*

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

En el apartado anterior se apuntó una idea importante y que afecta directamente a las señales digitales: **si una señal cambia su valor de forma instantánea**, **su frecuencia es infinito**. Como se puede observar en la siguiente figura, en cada discontinuidad de la señal se produce precisamente este hecho, su valor cambia de forma instantánea. Es decir, para transmitir una señal digital de forma exacta sería necesario un ancho de banda infinito. Lógicamente, en la práctica esto es imposible, por lo que habrá que establecer qué ancho de banda es necesario para transmitir señales digitales sin que se pierda la información que representa.

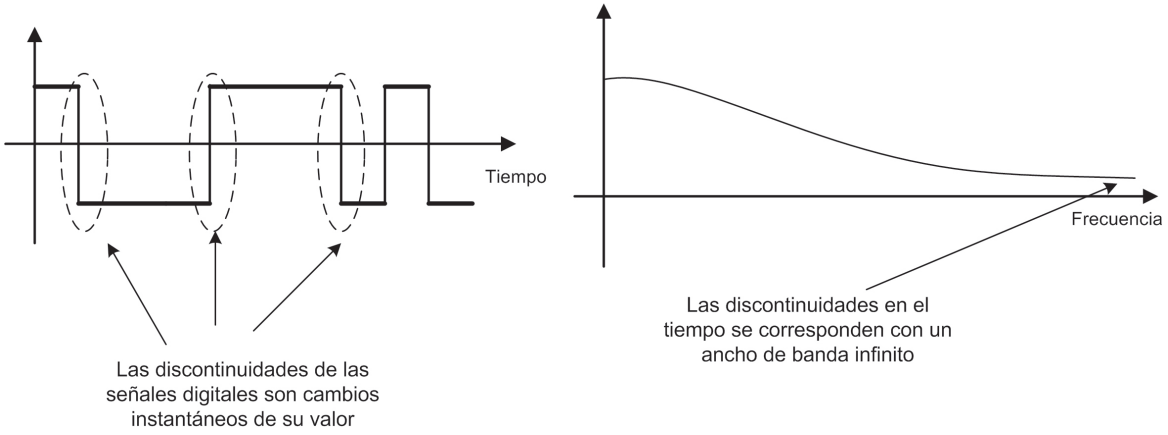


Figura 2.28. *Discontinuidad de las señales digitales*

RECUERDA

Las señales digitales tienen un ancho de banda idealmente infinito. En la práctica se debe establecer algún criterio para limitar dicho ancho de banda.

Pero ¿se puede recortar el ancho de banda de una señal? Esto supone eliminar componentes de frecuencia de la señal, con lo cual estaríamos alterando la señal original. ¿Y eso es posible? La respuesta es sí. En ocasiones es posible eliminar componentes de frecuencia de la señal sin que ésta pierda su información esencial.

Esto es lo que ocurre con la transmisión en el sistema telefónico. La señal eléctrica generada en el micrófono del terminal telefónico puede llegar hasta los 9 ó 10 kHz de ancho de banda y, sin embargo, se le aplica un recorte para adaptar el ancho de banda de la señal a las condiciones de diseño de toda la red del sistema telefónico. El ancho de banda se queda reducido a 3.400 Hz. Las consecuencias son que la voz que oímos en el sistema telefónico tiene un cierto grado de distorsión debido a este recorte de frecuencias de la señal original.

Lo mismo ocurre con las señales digitales en las redes telemáticas, se recorta el ancho de banda y la señal sufre un cierto deterioro respecto a la señal ideal. Lo importante en este caso es que la señal digital siga reflejando la información digital que se transmite, es decir, que los niveles digitales estén claros. En la siguiente figura se puede apreciar la forma de onda de señales digitales "reales" donde se ha recortado el ancho de banda.

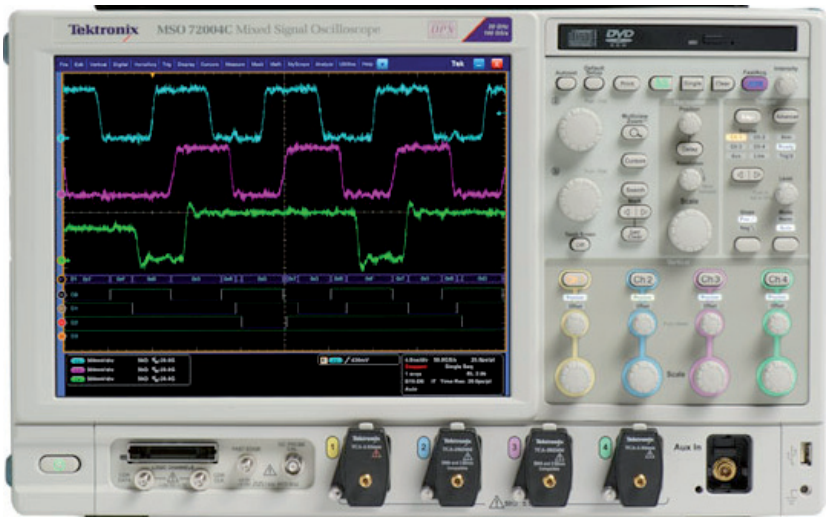


Figura 2.29. *Señales digitales reales vistas en un oscilospio*

2.3 PERTURBACIONES EN LA TRANSMISIÓN

En transmisión de datos, el término **perturbación** se refiere al conjunto de actuaciones externas e internas sobre el sistema de transmisión que hacen que la señal recibida no sea exactamente igual a la emitida por el emisor. Las perturbaciones pueden tener diferente origen y producir diferentes tipos de efectos sobre la señal que contiene la información. Algunos tipos de perturbaciones se producen solo en presencia de señal, mientras que otros tipos existen siempre con independencia de la señal. Además, algunos tipos de perturbaciones tienen carácter aleatorio, mientras que otros dependen de alguno o varios de los elementos de la transmisión. A continuación repasaremos los principales tipos de perturbaciones.

2.3.1 ATENUACIÓN

En todos los canales de transmisión se produce una pérdida de potencia durante el proceso de propagación de la señal por el propio medio. A esta pérdida de potencia se la conoce como atenuación.

El principal factor que influye en el valor de la atenuación es el propio medio de transmisión y la forma en la que se propaga la información. Normalmente la atenuación suele representarse como una relación entre la potencia de la señal en el emisor y la potencia de la señal en el receptor utilizando unidades logarítmicas.

En el caso de medios de transmisión guiados, la atenuación es un parámetro que se suele proporcionar en función de la distancia, es decir, los fabricantes facilitan la atenuación del medio por una unidad de distancia.

2.3.2 RUIDO

El ruido es una señal no deseada que se superpone a la señal transmitida. El nombre de ruido tiene su origen en los sistemas telefónicos, donde este tipo de señales producían un efecto de un sonido no deseado, es decir, un ruido. Este tipo de perturbación tiene una naturaleza aleatoria. Hay varios tipos de ruido dependiendo de su origen.

- **Ruido térmico**. Producido por los propios componentes electrónicos como consecuencia del aumento de temperatura de los mismos. En los sistemas digitales este tipo de ruido suele tener poca importancia.
- **Ruido de intermodulación**. Es debido a las características no lineales de los diferentes circuitos electrónicos como amplificadores, moduladores…
- **Ruido impulsivo**. Este tipo de ruido consiste en impulsos irregulares o picos de ruido de corta duración y amplitudes relativamente grandes. La aparición del ruido impulsivo puede ser debido a chispas producidas por aparatos eléctricos, automóviles, trenes eléctricos, taladradoras, interruptores. Su importancia es alta en los sistemas digitales, ya que suele producir lo que se llama *errores en ráfaga*, es decir, un grupo contiguo de bits se ven afectados por este fenómeno, llegando con errores al receptor.
- **Interferencias**. Este término se utiliza normalmente para señales no deseadas en los sistemas radioeléctricos, es decir, en los sistemas que transmiten la información mediante ondas electromagnéticas propagadas por el aire. Se podrían incluir aquí las perturbaciones producidas por fenómenos atmosféricos.

Para mejorar las transmisiones, frente a los tipos de perturbaciones descritas, lo más habitual es tratar de mejorar lo que se conoce como la **relación señal-ruido**, es decir, se intenta que la relación entre la potencia de la señal y la potencia del ruido sea lo más alta posible para que el ruido tenga una menor repercusión.

Debido a la atenuación de propgagación, con la distancia puede reducirse drásticamente la relación señal-ruido. Para solucionarlo se recurre al uso de los dispositivos llamados **repetidores**, que se utilizan para aumentar la potencia de la señal y mejorar así la relación señal-ruido.

2.3.3 DIAFONÍA

La diafonía o cruce es una transferencia indeseada de la potencia de la señal de un circuito llamado perturbador a otro llamado perturbado. Este tipo de perturbación es propia de los sistemas cableados donde existen varios canales muy próximos entre sí transmitiendo información digital. En los cables fabricados específicamente para redes de datos se han definido un conjunto de parámetros que miden diferentes tipos de diafonía.

Los más importantes son:

- **NEXT**: *Near End Crosstalk* o diafonía de extremo cercano. Es la medida de la perturbación producida en el extremo de un canal debido a la existencia de otro canal cercano. La perturbación se produce en el extremo de otro canal cercano muchas veces debido a malas terminaciones en los conectores. Para reducir este tipo de inducciones se usan pares trenzados. Este parámetro se representa en decibelios.
- **FEXT**: *Far End Crosstalk* o diafonía de extremo lejano. Es la medida de la perturbación en el extremo contrario al de la medición, producida por la existencia de un canal adyacente. La perturbación se origina en el extremo contrario y viaja por el medio de transmisión junto con la señal original y sufre la atenuación debida a la distancia. Por ello esta medida depende de la distancia y no es una referencia útil.
- **PSNEXT**: *Power Sum Near Crosstalk* o suma de potencias de la diafonía de extremo cercano. Actualmente existen transmisiones de datos que utilizan varios pares, como es el caso de las transmisiones a 1 Gbps sobre el llamado UTP de categoría 6 (ver el próximo capítulo). Este parámetro mide el efecto de la diafonía de extremo cercano (NEXT) en un canal producido por el efecto de todos los canales cercanos.
- **ELFEXT**: *Equal Level Far End Crosstalk* o FEXT normalizado. Como se ha indicado, el parámetro FEXT no resulta una referencia fiable, ya que depende de la distancia. Para el cálculo del parámetro ELFEXT se elimina el componente de atenuación, por lo que se consigue independizar dicho parámetro de la distancia.

	Margen de Peor Caso		Valor de Peor Valor	
PASA	MAIN	SR	MAIN	SR
Peor Par	36-45	36-78	36-45	36-45
NEXT (dB)	3.7	2.6	3.7	3.2
Frec. (MHz)	473.0	70.3	473.0	489.0
Límite (dB)	27.4	44.3	27.4	27.0
Peor Par	36	36	36	36
PS NEXT (dB)	4.8	4.4	4.8	4.5
Frec. (MHz)	473.0	431.0	473.0	489.0
Límite (dB)	24.6	26.0	24.6	24.1

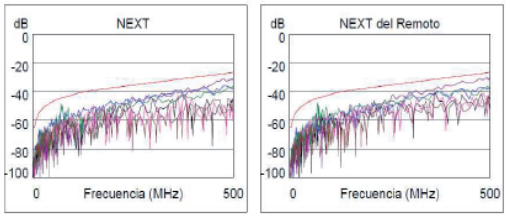


Figura 2.30. *Medición de los parámetros NEXT y PSNEXT en un cable de par trenzado*

2.3.4 DISTORSIÓN

La distorsión es un elemento perturbador de una señal producido por los sistemas electrónicos por los que pasa la señal. La distorsión se produce como consecuencia del tratamiento de la señal por los sistemas electrónicos debido a la no linealidad de los mismos. Los tipos más comunes de distorsión son:

- **Distorsión de amplitud**. Se produce debido a que la respuesta en frecuencia de los sistemas electrónicos no es lineal y atenúa más unas frecuencias que otras.
- **Distorsión de fase o de retardo**. Se produce cuando las diferentes componentes de frecuencia viajan por el medio de transmisión con diferentes velocidades de propagación debido a las propias características del medio.
- **Distorsión armónica**. Es debida a que algunos circuitos producen armónicos que no existen en la señal original.

2.4 UNIDADES LOGARÍTMICAS: EL DECIBELIO

Una de las magnitudes más utilizadas en los sistemas electrónicos, incluyendo los equipos de transmisión de datos, es la potencia. Las unidades de potencia son los vatios (W), sin embargo, en muchas ocasiones, dicha potencia viene expresada en una unidad logarítmica conocida como **decibelio** (**dB**).

Los decibelios son unidades utilizadas para representar la relación entre dos magnitudes, una de ellas se puede utilizar como una magnitud de referencia. Estas unidades también se utilizan en otros campos, como en acústica, para representar intensidades de sonido o niveles de presión sonora. La fórmula general para calcular una magnitud, por ejemplo la potencia, en decibelios es:

$$P(dB) = 10 \cdot \log \frac{P_1(W)}{P_2(W)}$$

Como se observa en la expresión anterior, la potencia en decibelios siempre representa la relación entre dos valores de potencia. También es útil conocer la expresión inversa para obtener la relación de potencias en W a partir de su valor en dB:

$$\frac{P_1(W)}{P_2(W)} = 10^{\frac{P(dB)}{10}}$$

En el campo de las telecomunicaciones el decibelio se puede utilizar en dos casos:

- Para expresar **la potencia de una señal respecto a una referencia**. Una de las referencias más utilizadas es la potencia de 1 mW. En este caso, la unidad recibe el nombre de **dBm**.

$$P(dBm) = 10 \cdot \log \frac{P(W)}{1mW}$$

En la expresión anterior se puede representar la potencia en mW:

$$P(dBm) = 10 \cdot \log P(mW)$$

Para obtener la potencia en mW a partir de su valor de dBm se utiliza la expresión:

$$P(mW) = 10^{\frac{P(dBm)}{10}}$$

- Para expresar **la ganancia o atenuación de un sistema**. En este caso, el cálculo de la unidad logarítmica se hace utilizando la potencia a la entrada del sistema y la potencia a la salida.

$$P(dB) = 10 \cdot \log \frac{P_{salida}(W)}{P_{entrada}(W)}$$

En el caso de que el sistema amplifique la señal, es decir, la potencia a la salida sea mayor que la potencia a la entrada, el resultado será un valor en decibelios mayor que cero. En el caso de que un sistema produzca una atenuación de la señal, la unidad logarítmica será un valor negativo.

La principal razón de utilizar las unidades logarítmicas es la facilidad de uso para realizar operaciones relacionadas con la potencia donde estén involucrados varios sistemas. Además, las unidades logarítmicas permiten un mejor manejo de unidades muy grandes o muy pequeñas. Vamos a ver a continuación algunos ejemplos:

Una potencia de 25 mW se puede representar en dBm como:

$$P(dBm) = 10 \cdot \log 25\,mW = 13{,}98\,dBm$$

Una potencia de 32 µW se puede expresar en dBm como:

$$P(dBm) = 10 \cdot \log 0{,}32\,mW = -4{,}95\,dBm$$

Se puede observar que los valores positivos se corresponden con potencias superiores a 1 mW y los valores negativos se corresponden con valores inferiores a 1 mW. El valor de 0 dBm se corresponde con una potencia justamente de 1 mW.

Un sistema amplificador se representa habitualmente como la ganancia entre la potencia de entrada y la potencia de salida. Esta relación se puede representar con unidades logarítmicas. En un sistema que tenga una ganancia de 20, es decir, la señal de salida es 20 veces superior a la de entrada, dicha ganancia se puede expresar en decibelios:

$$G(dB) = 10 \cdot \log 20 = 13\,dB$$

Un sistema atenuador se representa habitualmente como la atenuación de la señal de salida respecto a la señal de entrada. De igual forma esta relación se puede expresar con unidades logarítmicas, en este caso, el valor resultante siempre será negativo. En un sistema que produzca una atenuación de la potencia de la señal de entrada a la mitad tendrá un factor de 0,5, dicha atenuación en decibelios será:

$$A(dB) = 10 \cdot \log\ 0{,}5 = -3\,dB$$

2.5 VELOCIDAD DE TRANSMISIÓN, ANCHO DE BANDA Y CAPACIDAD DE UN CANAL

Qué duda cabe de que uno de los parámetros críticos que define en muchas ocasiones las prestaciones de las redes telemáticas es la velocidad de transmisión (o tasa de bits) expresada como el número de bits transmitidos por segundo (bps).

Se ha hablado en este capítulo de un parámetro llamado **ancho de banda**. En el apartado 2.2.5 se definía el ancho de banda como la anchura del espectro de una señal, es decir, el rango de frecuencias en las que una señal tiene componentes significativos. Hay que recordar también que el ancho de banda de una señal digital "perfecta" es infinito, por lo que es necesario establecer unos criterios más realistas para determinar su ancho de banda efectivo, es decir, es necesario recortar el ancho de banda de la señal sin que se pierda la información digital que contiene. De una manera general, se puede establecer una relación entre el ancho de banda de una señal digital y la tasa de bits de esa señal. Para la transmisión de una señal digital en **banda base**, esta relación es la siguiente:

$$Ancho\ de\ banda = \frac{tasa\ de\ bits}{2}$$

Es decir, cuanto más alta sea la tasa de bits de la señal digital, mayor será su ancho de banda. Así, el ancho de banda mínimo de una señal digital de 1 Mbps es de 500 kHz. Cuanto más ancho de banda se utilice para transmitir una señal digital, más se parecerá a la señal ideal. La relación anterior marca el ancho de banda mínimo por debajo del cual el deterioro de la señal sería tal que se perdería la información digital que contiene.

Se denomina **banda base** al conjunto de señales que son transmitidas en su frecuencia original a la salida de la fuente que las origina, es decir, no sufren ningún proceso de modulación. Como contraposición, si una señal se transmite variando las frecuencias originales, se dice que la señal ha sido modulada.
La transmisión de señales digitales en banda base se utiliza para distancias relativamente cortas y cuando el medio de transmisión lo permita.

Por otra parte, el término **ancho de banda** también se puede aplicar a un medio de transmisión y se definirá como el rango de frecuencias que dicho medio es capaz de transmitir. Así, si tenemos un medio de transmisión con un ancho de banda de 100 MHz, significa que por ese medio podremos transmitir señales que tengan un ancho de banda de hasta 100 MHz. Por lo tanto, cuanto mayor sea el ancho de banda de un medio de transmisión, mayor podrá ser la tasa de bits de la señal que transporte.

Obviamente las señales que se transmiten por un determinado medio no tienen por qué tener un ancho de banda igual al del propio canal, pueden tener anchos de banda menores, aunque esto supone un desaprovechamiento de las posibilidades de transmisión del canal. En el caso de medios de transmisión con anchos de banda enormes como la fibra

óptica, que puede ser de varios Gbps, se utilizan técnicas para poder transmitir varias señales simultáneamente y así poder aprovechar todo su ancho de banda. Más adelante en este capítulo se repasará la **multiplexación** como la técnica utilizada para poder transmitir varias señales por un mismo canal de transmisión, aprovechando así todo su ancho de banda. En el próximo capítulo se hará un repaso de los medios de transmisión utilizados en las redes de comunicaciones.

Existe una regla que nos proporciona la máxima velocidad alcanzable en un medio de transmisión para un ancho de banda dado. A esta velocidad máxima se la conoce como **capacidad del canal**:

$$C = 2 \cdot Ancho\ de\ banda$$

Es decir, la capacidad de un canal de comunicación es dos veces el ancho de banda de dicho canal en condiciones ideales en las que no haya ningún tipo de perturbación de la señal. Esta capacidad, que al fin y al cabo es una velocidad de transmisión, se mide en bits por segundo (bps). Lógicamente, la capacidad real del canal se verá reducida por las perturbaciones y atenuaciones que puede sufrir la señal.

La expresión anterior se aplica cuando se utilizan señales digitales binarias, es decir, con solo dos niveles. Si se tienen señales digitales de más de dos niveles, es decir que cada elemento de la señal representa más de un bit, la expresión anterior se transforma en la siguiente:

$$C = 2 \cdot Ancho\ de\ banda \cdot \log_2 M$$

donde M es la cantidad de niveles.

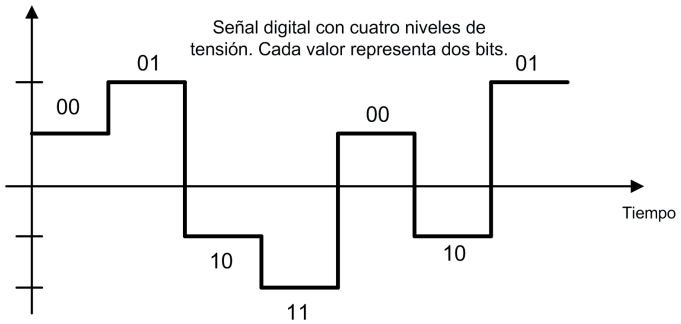


Figura 2.31. *Señal digital con cuatro niveles*

Una vez más, esta expresión establece la capacidad máxima teórica, sin ruido, con la que se puede transmitir una señal digital a través de un canal con un ancho de banda dado.

RECUERDA

El concepto de ancho de banda se puede aplicar a una señal, refiriéndose en este caso al rango de frecuencias que componen la señal. También se puede aplicar a un medio de transmisión, siendo, en este caso, el rango de frecuencias que dicho medio permite transmitir.

Ejemplo: disponemos de un cable de cobre que por sus características físicas, diámetro, longitud, atenuación, etc., tiene un ancho de banda de 200 MHz. Esto significa que podremos transmitir señales eléctricas con un ancho de banda de 200 MHz. En el caso de que queramos transmitir señales digitales, cuyo ancho de banda ideal es infinito, podemos recortar su ancho de banda dependiendo de la velocidad de transmisión o tasa de bits de la señal digital. El límite máximo en condiciones ideales para una señal digital de dos niveles sería de 400 Mbps (según la regla de la capacidad de un canal).

En la práctica, el ancho de banda de un canal de comunicación depende tanto del ancho de banda del medio de transmisión como de las tecnologías empleadas para transmitir la información. El ejemplo más claro es la transmisión de datos a través del par de cable telefónico del bucle de abonado. Las primeras tecnologías de transmisión que hicieron uso de dicho medio de transmisión, los llamados módems analógicos, alcanzaron su techo en 56 kbps. Para aumentar la velocidad utilizando el mismo par de cobre telefónico se desarrolló la tecnología ADSL, que en ciertas condiciones consigue velocidades de 10-12 Mbps.

2.6 CODIFICACIÓN

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

El ejemplo más básico de codificación se conoce como codificación unipolar. Para codificar información digital (ceros y unos) mediante esta técnica, se asigna a cada nivel lógico un nivel de voltaje usando únicamente una polaridad. Por ejemplo, los "unos" se codifican con un valor de voltaje positivo y los "ceros" se codifican con el valor de voltaje cero.

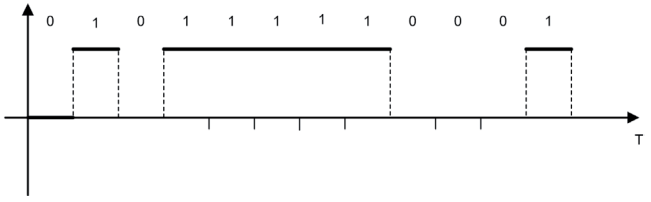


Figura 2.32. *Codificación unipolar*

Esta codificación, aunque extremadamente sencilla, no se utiliza en la práctica debido a dos problemas que presenta. El primero es la posible pérdida de sincronismo de la señal cuando se envían secuencias largas de "ceros" o de "unos". En las transmisiones digitales de tipo serie es muy importante que tanto el emisor como el receptor estén sincronizados, es decir, sepan en qué momento exacto empieza cada bit que se transmite. La manera más sencilla que tienen de sincronizarse es cuando se produce algún cambio en la señal, pero si durante un intervalo de tiempo grande no hay ningún cambio, es posible que debido a diferencias entre las temporizaciones de los circuitos del emisor y receptor se produzcan dichos problemas de sincronismo.

El otro problema es debido a lo que se conoce como componente continua. En las señales digitales la componente continua sería algo así como el valor medio de la señal. Por cuestiones de eficiencia, interesa que dicha componente continua sea lo más baja posible, idealmente cero. Sin embargo, esta característica no se cumple en la codificación unipolar.

A continuación se exponen algunos ejemplos de codificación que sí se utilizan en los sistemas de transmisión.

2.6.1 CODIFICACIÓN NRZ-I

Es un tipo de codificación polar que utiliza dos niveles de voltaje, con la misma amplitud pero con polaridades diferentes, es decir, un nivel con polaridad positiva y el otro con polaridad negativa. Con esta característica se consigue reducir la componente continua.

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

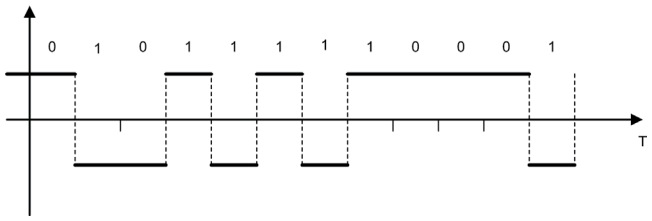


Figura 2.33. *Codificación NRZ-I*

Como se observa en la figura anterior, además de reducir el valor de la componente continua, característica común en todas las codificaciones polares, se consigue reducir el problema de sincronismo, ya que éste solo afecta a las secuencias largas de ceros.

2.6.2 CODIFICACIÓN MANCHESTER

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

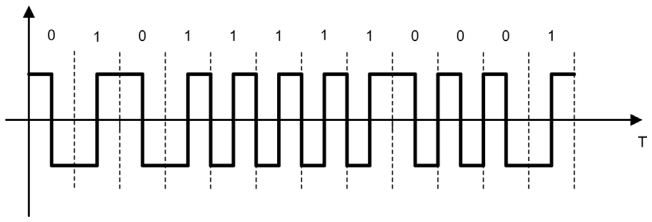


Figura 2.34. *Codificación Manchester*

La codificación Manchester representa un tipo de codificación bastante eficiente, ya que se consigue anular completamente la componente continua y además proporciona una sincronización en cada bit, por lo que no presenta problemas de sincronismo.

2.6.3 CODIFICACIÓN AMI

La codificación AMI es un tipo de codificación bipolar, en la que se utilizan tres niveles de voltaje: positivo, negativo y cero. El nivel cero se utiliza para codificar el 0 lógico y el 1 lógico se representa alternando polaridad positiva y negativa.

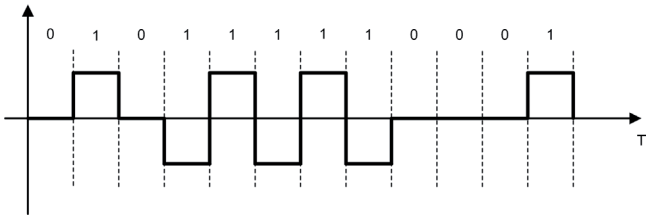


Figura 2.35. *Codificación AMI*

Con esta codificación se elimina prácticamente la componente continua y solo habría problemas de sincronismo con secuencias largas de ceros.

2.6.4 CODIFICACIÓN HDB3

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

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

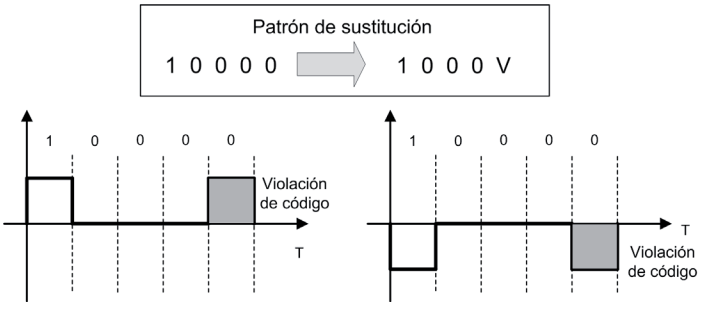


Figura 2.36. *Patrón de sustitución impar para la codificación HDB3*

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

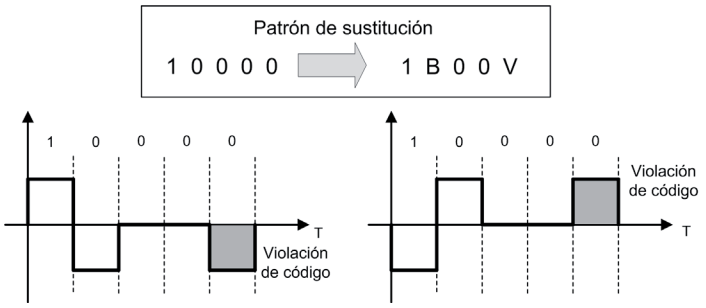


Figura 2.37. *Patrón de sustitución par para la codificación HDB3*

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

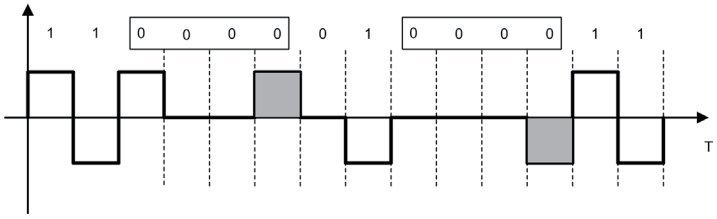


Figura 2.38. *Ejemplo de codificación HDB3*

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

2.7 CONMUTACIÓN

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

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

2.7.1 CONMUTACIÓN DE CIRCUITOS

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

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

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

Existen dos técnicas de conmutación de circuitos:

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

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

2.7.2 CONMUTACIÓN DE PAQUETES

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

Hay dos tipos de conmutación de paquetes:

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

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

2.7.3 CONMUTACIÓN DE MENSAJES

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

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

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

2.8 MULTIPLEXACIÓN

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

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

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

2.8.1 FDM. MULTIPLEXACIÓN POR DIVISIÓN DE FRECUENCIA

La multiplexación por división de frecuencia o **FDM** (*Frequency Division Multiplexing*) es una técnica empleada cuando se quiere transmitir varias señales analógicas a través de un medio de transmisión con un ancho de banda mayor que el de las señales que hay que transmitir.

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

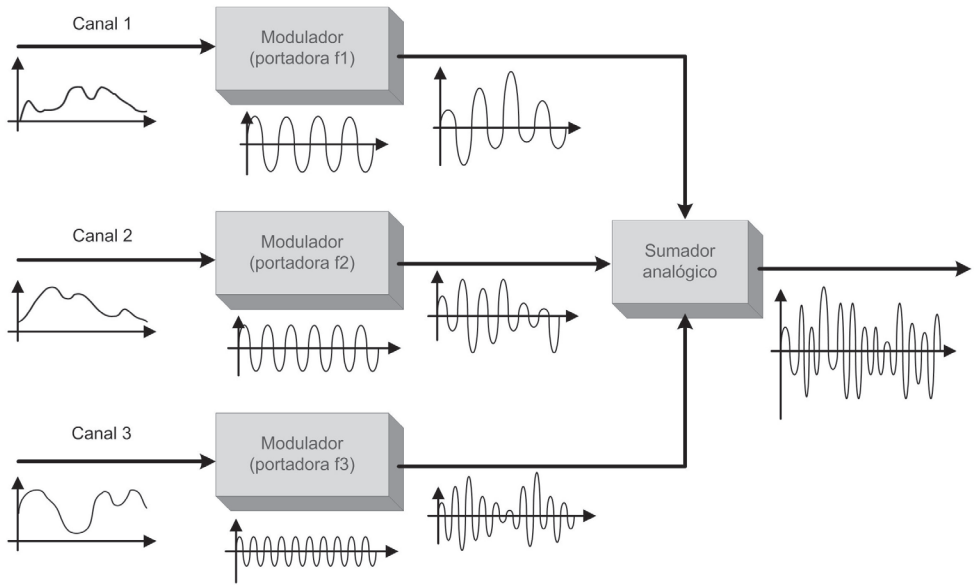


Figura 2.39. *Proceso de multiplexación FDM en el tiempo*

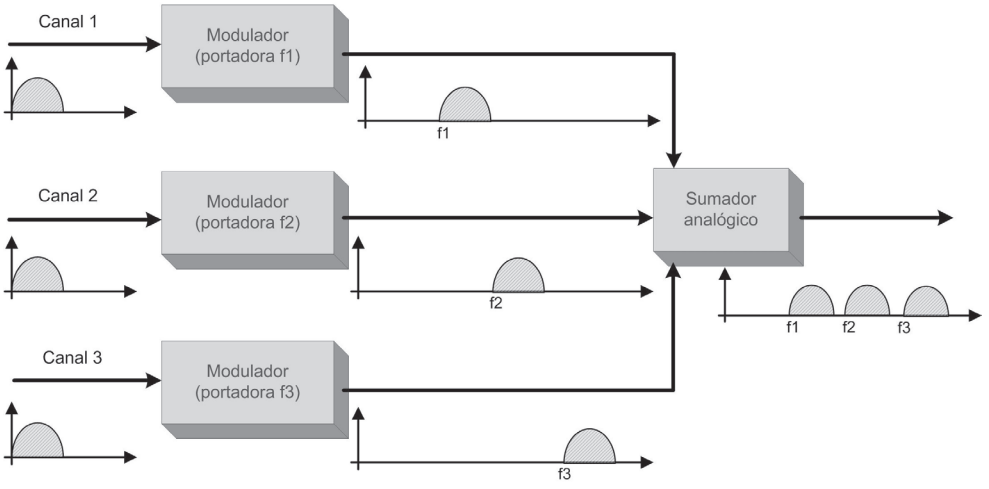


Figura 2.40. *Proceso de multiplexación FDM en la frecuencia*

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

FDM se aplica para multiplexar señales analógicas, por lo que se deberá utilizar cualquier técnica de modulación de señales analógicas, por ejemplo, AM o FM. El problema es que tanto en AM como en FM la señal modulada tiene

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

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

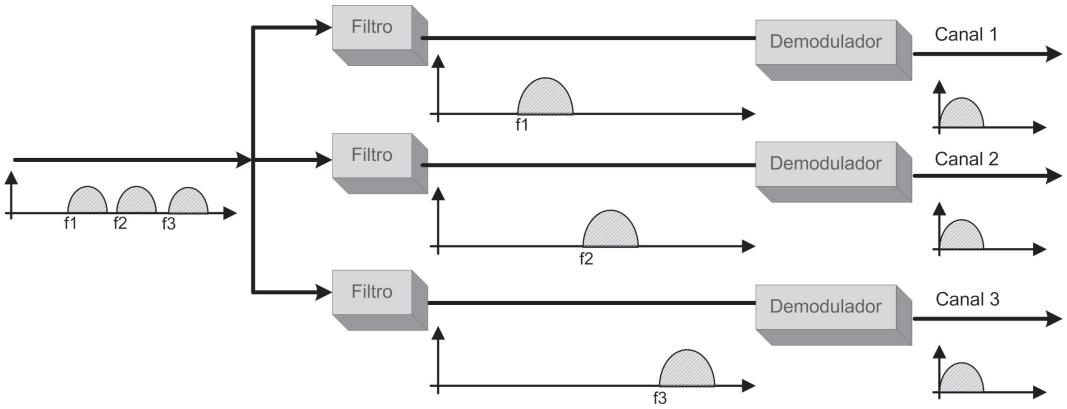


Figura 2.41. *Proceso de demultiplexación FDM en la frecuencia*

2.8.2 TDM SÍNCRONA. MULTIPLEXACIÓN POR DIVISIÓN EN EL TIEMPO SÍNCRONA

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

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

Existen dos tipos de TDM: **síncrona** y **asíncrona**. El término "síncrono" no tiene el mismo significado que el que se vio en la transmisión serie de datos. En este caso, síncrono se refiere a que, en la multiplexación, a cada canal que se desea transmitir se le asigna exactamente la misma porción de tiempo, independientemente de si en el canal hay datos para transmitir. Digamos que se asignan turnos de transmisión fijos e iguales a cada canal. Si tenemos cuatro canales, a cada canal se le asigna un turno de transmisión. Si a un canal le toca transmitir y no tiene nada, durante ese turno no se transmitirán datos.

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

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

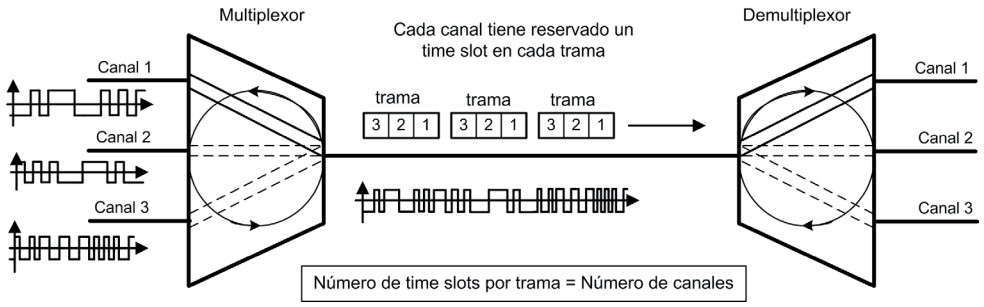


Figura 2.42. *TDM síncrona*

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

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

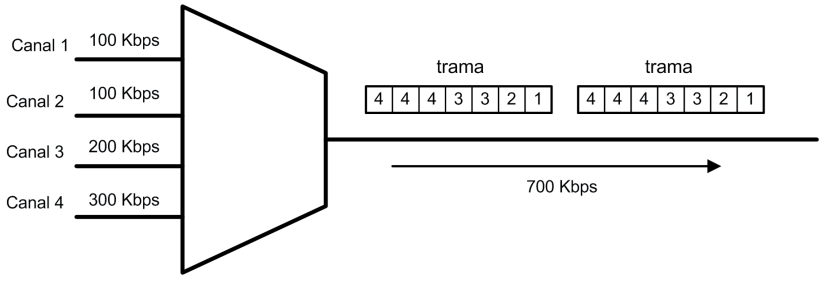


Figura 2.43. *TDM síncrona con canales a diferente velocidad*

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

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

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

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

2.8.3 TDM ASÍNCRONA O ESTADÍSTICA

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

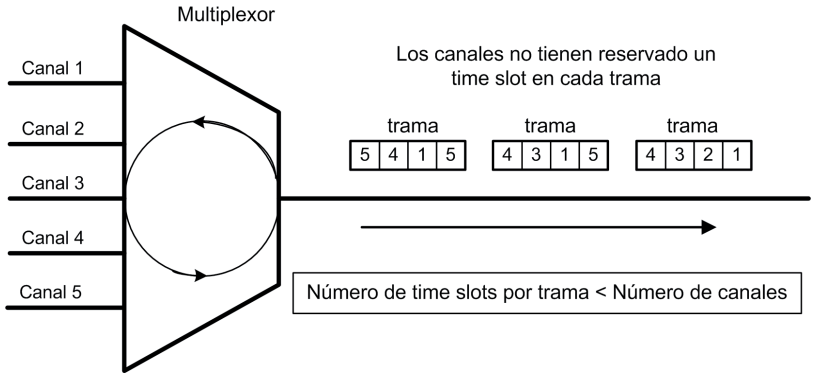


Figura 2.44. *TDM asíncrona*

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

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

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

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

2.8.4 WDM. MULTIPLEXACIÓN POR DIVISIÓN DE LONGITUD DE ONDA

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

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

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

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

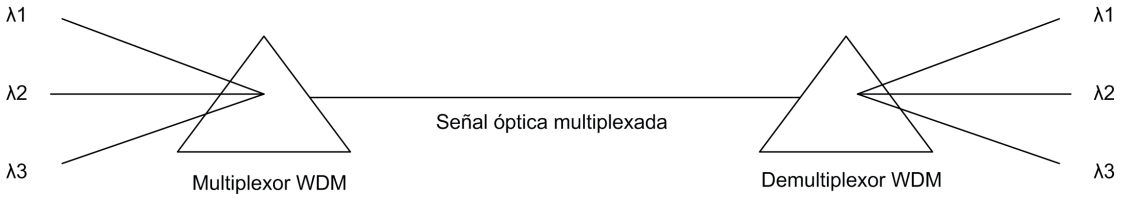


Figura 2.45. *WDM*

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

EJERCICIOS PROPUESTOS

1. Realiza los siguientes cambios de unidades:

- 56.500 Hz en kHz.
- 2.248 kHz en MHz.
- 36 GHz en kHz.
- 4.876.246 Hz en MHz.
- 0,0045 segundos en milisegundos.
- 0,0619 milisegundos en microsegundos.
- 0,000000728 segundos en picosegundos.
- 0,0000854 segundos en nanosegundos.

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

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

- Señal A: amplitud 20 v, frecuencia 1 kHz, fase 0º.
- Señal B: amplitud 10 v, frecuencia 10 kHz, fase 90º.
- Representa las señales anteriores en el dominio de la frecuencia.

4. Obtén la velocidad de transmisión (tasa de bits) para cada una de las siguientes señales:

- Una señal en la cual un bit dura 0,005 segundos.
- Una señal en la cual un bit dura 8 milisegundos.
- Una señal en la cual 5 bits duran 60 microsegundos.
- Una señal en la cual 2.000 bits duran 100 picosegundos.

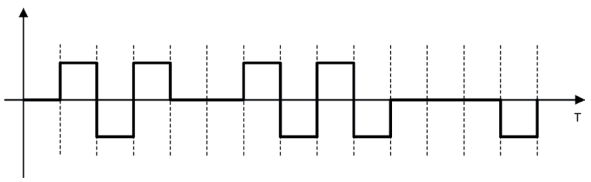
5. ¿Cuál es la duración de un bit para cada una de las señales siguientes?

- Una señal con una velocidad de transmisión de 500 bps.
- Una señal con una velocidad de transmisión de 200 kbps.
- Una señal con una velocidad de transmisión de 2 Mbps.
- Una señal con una velocidad de transmisión de 4 Gbps.

6. Codifica la secuencia de bits 0111110100000011 en las siguientes codificaciones:

- NRZ-L.
- Manchester.
- HDB3.

7. Obtén la información digital de la siguiente señal codificada utilizando HDB3:



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

9. Se multiplexan en TDM cuatro canales de 1 kbps. Si en la ranura de tiempo (*time slot*) del multiplexor se envía 1 bit, halla:

- La duración de un bit antes de la multiplexación.
- Tasa de bits de la transmisión.
- Duración de una trama.
- Duración del *time slot*.

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

TEST DE CONOCIMIENTOS

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

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

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

4 La capacidad de un canal (medio de transmisión) para transmitir señales digitales en banda base depende:
- **a)** Solo del ancho de banda del canal.
- **b)** Del ancho de banda y del número de niveles de la señal digital.
- **c)** Del ancho de banda y de la técnica de modulación empleada.
- **d)** No se pueden transmitir señales digitales en banda base.

5 El ancho de banda es una característica que se puede aplicar:
- **a)** Solo para señales.
- **b)** Solo para los medios de transmisión.
- **c)** Tanto en señales como en medios de transmisión.
- **d)** Tanto en señales como en medios de transmisión y en dispositivos de interconexión.

6 Para transmitir una señal digital y debido a que su ancho de banda es infinito:
- **a)** Es necesario recortar su ancho de banda.
- **b)** Es necesario convertirla a analógica.
- **c)** Solo se puede transmitir utilizando fibra óptica.
- **d)** No es cierto que el ancho de banda sea infinito.

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

8 En la codificación HDB3 un patrón de sustitución se utiliza:
- **a)** Para distinguir el tipo de codificación.
- **b)** Para evitar la pérdida de sincronismo en la transmisión de muchos ceros seguidos.
- **c)** Para detectar códigos erróneos.
- **d)** Para minimizar el efecto de la componente continua en secuencias largas de unos.

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

10 El ancho de banda de una señal FDM es:

a) Mayor o igual a la suma de los anchos de banda de las señales multiplexadas.

b) Menor o igual a la suma de los anchos de banda de las señales multiplexadas.

c) Siempre igual a la suma de los anchos de banda de las señales multiplexadas.

d) Depende de si los canales son analógicos o digitales.

11 En TDM asíncrono, si un canal tiene datos que enviar, los datos van dentro de la trama en:

a) El siguiente *time slot* disponible.

b) Un *time slot* preasignado.

c) El primer *time slot*.

d) Ninguna de las anteriores es correcta.

12 La técnica utilizada en FDM para transportar el espectro de las señales al rango adecuado es:

a) Codificación.

b) Digitalización.

c) Conmutación.

d) Modulación.

3 Medios de transmisión y sistemas de cableado estructurado

3.1 TIPOS DE MEDIOS DE TRANSMISIÓN

Los medios de transmisión son el elemento por el que viajan los datos en las redes telemáticas. La función proporcionada por los medios de transmisión está englobada en el nivel 1 (nivel físico) del modelo OSI, y conocer las características, propiedades y comportamiento de los medios de transmisión disponibles es fundamental para entender el funcionamiento de las redes telemáticas.

Como ya se mencionó en el capítulo 1, existen dos tipos de medios de transmisión: medios guiados y medios no guiados.

- En los **medios guiados** los datos son transportados a través de un material que canaliza la señal que transporta. Es lo que se conoce habitualmente como medios cableados o simplemente cables. Cuando conectamos dos dispositivos mediante un cable, la información viaja de un dispositivo a otro canalizada en dicho cable. Existen dos tipos de señales que se pueden utilizar para transportar datos a través de un medio guiado: las señales eléctricas y las señales ópticas. Cada uno de estos tipos de señales utiliza un material diferente:
  - **Medios guiados de cobre**. El cobre es el material que se emplea para transportar señales eléctricas. Sin ninguna duda, es el medio actualmente más utilizado en las redes telemáticas y, en general, en cualquier sistema que necesite transportar señales eléctricas. Sus principales propiedades son:
    - Conductividad. El cobre es el mejor conductor de la corriente eléctrica que se conoce.
    - Ductilidad o capacidad para dividirse en finos hilos sin romperse.
    - Maleabilidad o facilidad para darle forma.

    En las redes telemáticas se utilizan dos tipos de cableado de cobre: el cable de par trenzado y el cable coaxial.
  - **Medios guiados de fibra óptica**. La fibra óptica es el medio que se emplea para transportar señales ópticas. La fibra óptica es el medio más utilizado en la transmisión de datos a larga distancia. Su funcionamiento está basado en el envío de luz a través de una fina canalización de fibra de vidrio o algún material plástico de similares características.
- En los **medios no guiados** los datos viajan en forma de ondas electromagnéticas utilizando el aire como medio de transmisión. En este caso, los datos se propagan sin estar sujetos a ninguna canalización que guíe la señal. También reciben el nombre de **medios inalámbricos**. El uso de medios inalámbricos está muy extendido en las telecomunicaciones, ya que los principales servicios ofrecidos, como la televisión, radio o telefonía móvil usan medios inalámbricos.

3.2 PAR TRENZADO

El cable de par trenzado es un tipo de cable de cobre utilizado en los sistemas telefónicos y en la gran mayoría de redes de datos de área local. El elemento básico de un cable de par trenzado es el llamado par, formado por dos hilos o cables de cobre. El par es el elemento necesario para transmitir una señal eléctrica. Los pares están trenzados para proporcionar protección frente a una fuente de interferencias llamada diafonía generada por pares adyacentes.

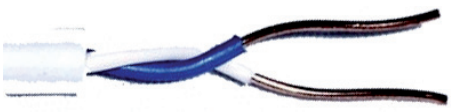


Figura 3.1. *Cable de par trenzado*

Un cable de par trenzado puede estar formado por uno o varios pares. Por ejemplo, para telefonía se emplea cable de par trenzado con un solo par o con dos pares (dos o cuatro hilos de cobre). El cable de par trenzado más utilizado en redes de área local (LAN) tiene cuatro pares, es decir, ocho hilos de cobre. Existen dos tipos de cable de par trenzado, conocidos por sus siglas en inglés: UTP y STP.

3.2.1 CABLE UTP

El **cable UTP** (*Unshielded Twisted-Pair*) o cable de par trenzado sin apantallar es el medio de transmisión más empleado en redes de área local. La razón principal de su extenso uso es que es el medio cableado más barato para transmitir datos. Es flexible y por tanto sencillo de instalar (otros tipos de cables son más rígidos y por tanto más difíciles de manipular), el conector utilizado en este tipo de cable es también barato, es relativamente ligero y de poco diámetro y las velocidades soportadas se ajustan a las necesidades de la mayor parte de las redes.

El cable UTP está formado por cuatro pares trenzados (ocho hilos de cobre), cada uno de los hilos está cubierto por una funda protectora de un color determinado para identificar su función. Además, todo el conjunto está cubierto por otra funda plástica exterior.

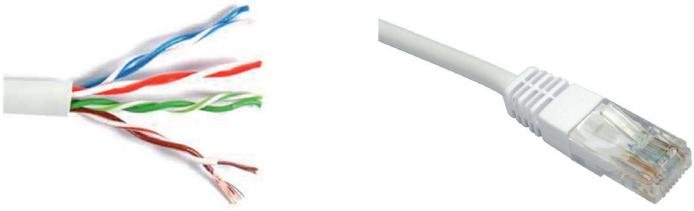


Figura 3.2. *Cable UTP formado por cuatro pares trenzados y conector RJ-45*

El conector utilizado en redes de datos con cable UTP se conoce como RJ-45.

Por otra parte, el cable UTP presenta dos desventajas, primero que no incorpora ningún elemento para protegerse del ruido eléctrico y las interferencias (como ocurre con otros tipos de cable de cobre como el STP o el cable coaxial), y segundo, que no permite las transmisión de datos para distancias largas (la mayor parte de los estándares que utilizan cable UTP limitan su longitud máxima a 100 metros).

RECUERDA

El cable UTP o par trenzado sin apantallar es el medio de transmisión dominante actualmente en las redes de área local, aunque la longitud máxima que se puede cubrir con este tipo de cable es de 100 metros.

Debido al aumento de las prestaciones de las redes de datos a lo largo de los últimos años, la industria de cableado ha tenido que desarrollar cables UTP que ofrecieran cada vez mejores características. Por ello, existen varios tipos de cable UTP conocidos como **categorías**. Se han ido desarrollando nuevas categorías de cable UTP donde el principal objetivo era proporcionar mayor ancho de banda y, consecuentemente, mayor velocidad de transmisión. Las primeras categorías de cable UTP, conocidas como categoría 1 (CAT 1) y categoría 2 (CAT 2), se consideran extinguidas. En la siguiente tabla aparecen las categorías existentes en la actualidad.

Nombre	Ancho de banda	Velocidad de transmisión	Estado
CAT 3	16 MHz	16 Mbps	Utilizado en las primeras redes locales Ethernet a 10 Mbps. Actualmente ya no se utiliza en redes de datos.
CAT 5	100 MHz	100 Mbps	Utilizado en muchas redes locales Ethernet, aunque actualmente ha sido desplazado por la categoría CAT 5e.
CAT 5e	100 MHz	1.000 Mbps	Utilizado en redes Ethernet tanto a 100 Mbps como a 1 Gbps.
CAT 6	250 MHz	1.000 Mbps	Utilizado principalmente para redes Ethernet a 1 Gbps. Existe una mejora llamada CAT 6e que admite velocidades de 10 Gbps con 500 MHz de ancho de banda.
CAT 7	600 MHz	10 Gbps	Realmente es cable de par trenzado apantallado.

Cuidado con confundir el cable de par trenzado con uso exclusivo para voz. Suele ser un cable con uno o dos pares y el conector es del tipo RJ-11 con solo cuatro pines (y no ocho como el RJ-45) y lógicamente más estrecho que el RJ-45.

Figura 3.3. *Comparación entre los conectores RJ-11 y RJ-45*

3.2.2 CABLE STP

El **cable STP** (S*hielded Twisted-Pair)* o cable de par trenzado apantallado es otro tipo de cable de cobre utilizado en redes telemáticas, aunque su uso en la actualidad es más bien escaso. Al igual que el cable UTP, está formado por cuatro pares trenzados y cada par está recubierto de una malla metálica o pantalla cuya función es reducir el efecto de las interferencias. Además, todo el conjunto lleva otra malla o lámina metálica para aumentar su inmunidad frente al ruido eléctrico y las interferencias. Existe además un tipo de cable STP que solo lleva la lámina metálica exterior, es decir, los pares no van apantallados.

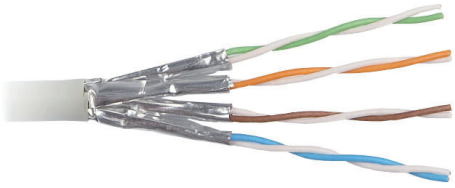


Figura 3.4. *Cable STP*

La inmunidad que presenta este tipo de cable mejora sus prestaciones pero, por el contrario, proporciona algunos inconvenientes, como mayor coste y mayor dificultad de instalación. Hay que tener en cuenta que el blindaje metálico debe estar conectado a tierra, y si esto no se hace correctamente, el efecto puede ser justo el contrario, ya que los blindajes metálicos sin conexión a tierra son muy sensibles a las interferencias.

En la práctica, solo es justificable utilizar cable STP en instalaciones con fuerte nivel de interferencias y lo cierto es que en la actualidad muy pocas instalaciones están preparadas para el uso de cables STP y éste apenas se utiliza.

Una **conexión a tierra** o una toma de tierra es un elemento que aparece en prácticamente en todas las instalaciones eléctricas y cuyo principal uso es la protección de los usuarios de los dispositivos eléctricos y electrónicos ante voltajes eléctricos no deseados. La descripción formal de la tierra en una instalación eléctrica es:

Una conexión conductora, ya sea intencional o accidental, por medio de la cual un circuito eléctrico o equipo se conecta a la tierra o a algún cuerpo conductor de dimensiones relativamente grandes que cumpla la función de la tierra.

En la práctica, una conexión a tierra es simplemente una pieza metálica enterrada en el suelo y conectada al llamado cable de tierra. También se puede conectar a las partes metálicas de la estructura del edificio.

Además de esta función de protección, la conexión a tierra también proporciona una trayectoria alternativa a las corrientes inducidas y por tanto minimiza el ruido eléctrico en los cables, que es el efecto que se busca en los cables STP.

3.3 CABLE COAXIAL

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

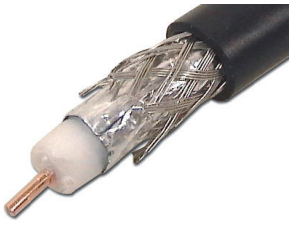


Figura 3.5. *Cable coaxial*

La figura anterior muestra la estructura de un cable coaxial. La velocidad de transmisión de este cable depende de su longitud y en cables de 1 km se pueden obtener velocidades entre 1 y 2 Gbps. Los cables coaxiales solían utilizarse en los troncales del sistema telefónico, pero ahora se les ha reemplazado por fibra óptica. También se utilizó ampliamente para las primeras implementaciones de redes Ethernet. Actualmente, el cable coaxial todavía se utiliza para la televisión por cable y para los tramos locales de algunos tipos de líneas de datos. Los proveedores de acceso a Internet por cable utilizan este tipo de cable para la conexión de sus clientes a la red.

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

- RG-8, conocido como coaxial grueso, con alrededor de 1 cm de diámetro y 50 Ω de impedancia. Este tipo se ha utilizado ampliamente en las redes de área local, aunque actualmente no se usa.
- RG-58, conocido como coaxial fino, con un diámetro de 0,5 cm y 50 Ω de impedancia. Al igual que el anterior, se han utilizado para redes de área local, aunque actualmente no se usa.
- RG-59, este tipo de unos 0,6 cm de diámetro y 75 Ω de impedancia se utiliza actualmente en las redes de transmisión de señales de televisión por cable.
- RG-6, es un cable de 0,69 cm de grosor y 75 Ω de impedancia. Es el más utilizado actualmente para la conexión a los proveedores de acceso a Internet por cable.

El conector que se utiliza para el cableado coaxial se conoce como conector BNC.

Figura 3.6. *Conector BNC*

Fuera del ámbito de las redes telemáticas podemos encontrar cable coaxial en aplicaciones relacionadas con el video, tomas de antena de TV y de satélites.

En la actualidad, un uso típico del cable coaxial es en la red de acceso a los proveedores de servicios de televisión y datos por cable, como, por ejemplo, Ono, R, Euskaltel, Telecable. En estos casos, el cable que une el punto de acceso a la red del operador con la red interna del usuario (normalmente un *router* o módem de cable) suele ser cable coaxial.

IMPORTANTE

Uno de los parámetros que podemos encontrar dentro de las características de los cables de cobre es el diámetro del hilo de cobre. Este diámetro se suele especificar utilizando el sistema americano conocido como **AWG** (*American Wire Gauge*, medición americana de cable). Para indicar el diámetro de un tipo de cable utiliza una numeración relacionada con el diámetro en pulgadas. Los cables de cobre más habituales van desde el tipo AWG 14 (1,6 mm de diámetro) hasta el AWG 24 (0,51 mm de diámetro). Los cables más utilizados en redes de datos suelen estar entre AWG 23 y AWG 24.

3.4 FIBRA ÓPTICA

A diferencia de los anteriores medios de transmisión guiados, la fibra óptica utiliza rayos de luz en lugar de señales eléctricas para el envío de datos. Para ello se utiliza en uno de los extremos de la transmisión un elemento que genere luz, con la longitud de onda adecuada, a partir de la información digital que se quiere transmitir. La luz generada en el emisor se canaliza por un cable formado por un material adecuado para guiarla, normalmente fibra de vidrio. En el otro extremo del sistema de transmisión existirá un elemento que convierte la luz en impulsos eléctricos. Por tanto, un sistema de transmisión por fibra óptica está formado por tres elementos: transmisor, cable de fibra óptica y receptor.

El cable de fibra óptica está cuidadosamente diseñado para transportar señales de luz. Se trata de un cilindro de pequeña sección flexible, conocido como **núcleo**, con un diámetro del orden de 8 a 125 μm (como comparación, el diámetro del cabello humano es del orden de 50 μm) por el que se transmite la luz. El núcleo está recubierto de un material similar al del propio núcleo, pero con un índice de refracción menor a fin de mantener toda la luz en el interior de él. Recibe el nombre de **revestimiento**. A continuación viene una cubierta plástica (normalmente PVC) para proteger el revestimiento e impedir que cualquier rayo de luz del exterior penetre en la fibra.

Figura 3.7. *Cable de fibra óptica*

Entre el revestimiento y la cubierta exterior suele existir otra capa constituida por un material en forma de hilos llamado Kevlar, cuya función es dar consistencia y protección contra las sobretensiones.. Dependiendo de las condiciones de uso de la fibra, se pueden añadir cubiertas exteriores para proporcionar rigidez y protección extra al cable de fibra.

Normalmente, por un cable de fibra se puede enviar información en un solo sentido, es decir, es una transmisión símplex. Para obtener una transmisión full-dúplex es necesario utilizar dos cables de fibra óptica. Esta configuración se utiliza mucho en las redes LAN.

Figura 3.8. *Cable de fibra óptica dúplex*

IMPORTANTE

Algunos datos sobre el elemento transmisor en la fibra óptica: la luz

La luz es un tipo de energía electromagnética que puede desplazarse en forma de onda a través de diferentes medios, como el aire, el vacío o el vidrio. La principal propiedad de la luz (y en general de cualquier tipo de onda) es su longitud de onda. La **longitud de onda** se puede definir como la distancia lineal entre dos puntos equivalentes de ondas sucesivas. Se mide en metros y se suele representar con la letra griega λ (lambda).

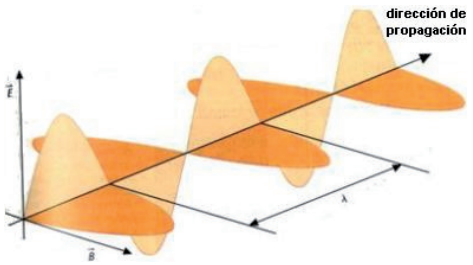


Figura 3.9. *Longitud de onda*

Dependiendo del rango de la longitud de onda de la luz, ésta recibe diferentes nombres. Por ejemplo, la luz visible son ondas electromagnéticas con una longitud de onda entre unos 400 nm y 700 nm (1 nm equivale a 0,000000001 m o 10^{-9} m). La luz utilizada en las transmisiones con fibra óptica está fuera del alcance de la luz visible. Pertenece al rango denominado **luz infrarroja**. Las longitudes de onda, dentro del rango de la luz infrarroja, que tienen un mejor comportamiento para su transmisión con fibra óptica son tres: 850 nm, 1.310 nm y 1.550 nm.

También existen en el mercado cables que contienen varios haces de fibra óptica, protegidos por una cubierta exterior común, utilizados sobre todo en las redes WAN.

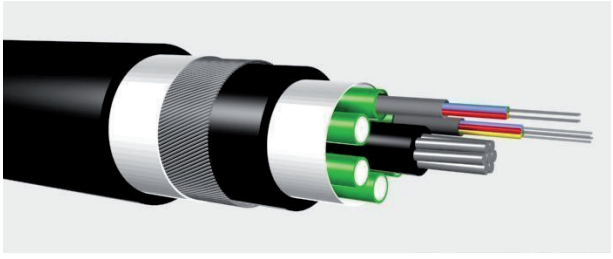


Figura 3.10. *Cable de fibra con varios haces*

Los cables de fibra óptica utilizados en las redes telemáticas pueden transmitir la luz de dos formas diferentes:

- **Fibra monomodo**: la luz se propaga en el interior del núcleo siguiendo un solo camino (modo). Para conseguir esta característica es necesario construir el núcleo de un diámetro muy pequeño. En las fibras monomodo el núcleo tiene un diámetro que oscila entre 8 y 10 micras, aunque el valor más habitual es de 9 micras. En estos casos, el diámetro del revestimiento suele ser de 125 micras. En el etiquetado de la fibra suelen aparecer estos dos valores, el diámetro del núcleo y del revestimiento. En el caso de fibras monomodo lo habitual es que estén etiquetadas como 9 µ/125 µ.
- **Fibra multimodo**: la luz se propaga en el interior del núcleo siguiendo varios caminos o modos. Esto se debe a que el diámetro en este tipo de fibras es sensiblemente mayor. Los valores más utilizados son de 50 o 62,5 micras. Para compensar el desfase que se produce en el receptor entre los diferentes modos se utiliza un tipo de vidrio llamado fibra de vidrio de índice gradual, cuyo índice de refracción va disminuyendo gradualmente desde el núcleo hasta la parte más exterior. El revestimiento en este tipo de fibra también suele ser de 125 micras, por lo que los tipos más habituales de fibras multimodo se suelen etiquetar como 62,5 µ / 125 µ o 50 µ / 125 µ.

La fibra óptica es el medio de transmisión que más se utiliza en transmisiones en largas distancia o en transmisiones que requieran un gran flujo de información. Las principales características de la fibra óptica como medio de transmisión son:

- Es el medio de transmisión con **mayor ancho de banda**, por lo que es el medio que más información puede transportar.
- **Inmunidad frente a perturbaciones electromagnéticas**. Las señales ópticas no se ven afectadas por este tipo de perturbaciones.
- **Menor atenuación**. Gracias a que la atenuación de la señal óptica es menor que la atenuación de las señales eléctricas por medios de cobre, se pueden cubrir distancias mayores sin utilizar repetidores o regeneradores de señal.
- Es el medio de transmisión **más adecuado para grandes distancias**, ya que en este caso es más barato que el cobre, es más ligero y resiste mejor elementos medioambientales como el agua.

3.4.1 EMISORES Y RECEPTORES

En la actualidad, lo habitual es que el cableado que conecta los dispositivos de los usuarios finales a una red telemática sea cable de cobre. Sin embargo, en algunas ocasiones, esta infraestructura de cableado de cobre debe conectarse a la infraestructura formada por fibra óptica, como puede ser en los troncales de las grandes redes LAN o en los enlaces WAN. Por tanto, son necesarios elementos que transformen las señales eléctricas que viajan por el cable de cobre en señales ópticas que viajan por la fibra óptica.

El emisor en un sistema de transmisión de fibra óptica es el elemento encargado de convertir una señal de datos eléctrica a una señal de datos óptica equivalente, apta para ser transmitida por la fibra de vidrio. Existen dos tipos de transmisores:

- **Emisores LED** (*Light Emitting Diodes*, diodos electroluminescentes). Este tipo de transmisor genera luz infrarroja con longitudes de onda de 850 ó 1.310 nm y por tanto se utiliza en la fibra multimodo instalada habitualmente en las redes LAN. Son emisores relativamente baratos.

- **Emisores láser**. Este tipo de transmisor genera luz infrarroja con longitudes de onda de 1.310 ó 1.550 nm y, por tanto, se utiliza para fibra monomodo. Además, el láser puede recorrer distancias más largas que la luz generada por los emisores LED; por tanto, es el tipo de transmisor utilizado en los enlaces WAN. Este tipo de conectores son mucho más costosos que los emisores LED.

Por otra parte, los receptores son los elementos encargados de convertir la señal óptica transmitida por la fibra en una señal eléctrica. Para ello se utilizan los llamados **fotodiodos**, que son dispositivos electrónicos sensibles a una longitud de onda concreta y que produce corriente eléctrica cuando llega un pulso de luz.

Tanto los emisores como los receptores de fibra óptica pueden estar incluidos en los dispositivos utilizados dentro de las redes telemáticas como *switches* o *routers*. A continuación se presenta una tabla resumen de las características de los dos tipos de cables de fibra óptica.

Tipo	Diámetro núcleo/ revestimiento	Longitud de onda	Tipo de luz	Distancia máxima de cable	Uso
Fibra monomodo	9 µ/125 µ	1.310 nm 1.550 nm	Láser	Más de 10 km	Redes WAN y troncal de redes LAN
Fibra multimodo	50 µ/125 µ 62,5 µ/125 µ	850 nm 1.310 nm	LED	Unos 2 km	Redes LAN

3.4.2 CONECTORES

Existen varios tipos de conectores utilizados para conectar el cable de fibra óptica a los equipos. Los más utilizados en las redes telemáticas son:

- **Conector ST**. Uno de los conectores de fibra óptica más utilizados en redes LAN, aunque en la actualidad se tiende a su sustitución por los conectores SC. Tiene un mecanismo de acople de tipo bayoneta similar a algunos conectores de cable coaxial.

Figura 3.11. *Conector ST*

- **Conector SC**. Este tipo de conector se ha ido imponiendo al conector ST debido a sus mejores prestaciones y facilidad de conexión. Es fácil de identificar por su perfil cuadrado en lugar del perfil circular del ST. Existe una variedad dúplex con dos conectores SC unidos.

Figura 3.12. *Conector SC*

Se puede encontrar una lista completa de conectores usados en fibra óptica en el siguiente enlace: www.*fibraoptica.com/informacion-tecnica/identificacion-de-conectores*

3.5 MEDIOS INALÁMBRICOS

Las redes telemáticas también pueden utilizar medios inalámbricos para transmitir información. Realmente, cuando hablamos de medios inalámbricos nos referimos al aire (aunque también se considera un medio inalámbrico el vacío). En este caso, la información se propaga mediante ondas electromagnéticas sin estar confinadas en ninguna canalización, por ello también se conocen como medios no guiados.

Los medios de transmisión inalámbricos han sido utilizados tradicionalmente en las telecomunicaciones para ofrecer diferentes servicios como televisión, radio, telefonía móvil, etc. En los últimos años se ha producido un auge del uso de este medio para las redes telemáticas debido a su versatilidad y su bajo coste de instalación en comparación con las redes cableadas.

Al igual que en los rayos de luz, en la fibra óptica, el principal parámetro que define las ondas electromagnéticas propagadas por el aire es su **longitud de onda** (λ). Aunque en este caso, también se emplea como parámetro característico la **frecuencia (f)**. La relación entre frecuencia y longitud de onda viene expresada por la siguiente ecuación:

$$v = \lambda \cdot f$$

Donde v es la velocidad de propagación de la onda electromagnética. Es muy frecuente utilizar como referencia de velocidad de propagación la velocidad de la luz en el vacío: $3 \cdot 10^8$ m/s.

El conjunto de todas las posibles longitudes de onda (o frecuencias) constituye el llamado **espectro electromagnético**. Este espectro se divide en bandas en función de la frecuencia. El rango de frecuencias utilizadas en telecomunicaciones va desde los 3 kHz hasta alrededor de los 300 GHz. A este rango se le conoce como **espectro de radiofrecuencia** y abarca las siguientes bandas:

- **Ondas de radio**. Son fáciles de generar, pueden viajar largas distancias, penetran en los edificios sin problemas y viajan en todas direcciones desde la fuente emisora. El rango de frecuencias que cubre va desde las frecuencias más bajas, alrededor de los 10 kHz, hasta frecuencias en torno a los 300 MHz. Existen dos tipos de ondas de radio:
  - **Ondas de radio de baja frecuencia**: se caracterizan por que en su recorrido siguen la curvatura de la Tierra y pueden atravesar con facilidad los edificios. Sin embargo, su ancho de banda solo permite velocidades de transmisión bajas.
  - **Ondas de radio de alta frecuencia**: estas ondas tienden a ser absorbidas por la Tierra, por lo que deben ser enviadas a la ionosfera, donde son reflejadas y devueltas de nuevo, con lo que se consigue transmitir a largas distancias.
- **Microondas**. Además de su aplicación en hornos, las microondas permiten transmisiones tanto terrestres como con satélites. Sus frecuencias están comprendidas entre 300 MHz y 300 Ghz. A diferencia de las ondas de radio, las microondas no atraviesan bien los obstáculos, de forma que es necesario situar antenas repetidoras cuando queremos realizar comunicaciones a largas distancias. En el caso de las comunicaciones por satélite, hay que tener en cuenta que siempre existe un pequeño retardo en las transmisiones debido a que la señal tarda aproximadamente 0,3 segundos en llegar y volver. Para algunas aplicaciones de envío y recepción de datos, este tiempo de espera puede resultar inaceptable.
- **Ondas infrarrojas**. Este tipo de ondas se utiliza para la comunicación de corto alcance, en controles remotos de televisores, y en general de dispositivos electrónicos. También es posible encontrar un puerto de comunicación infrarroja en los ordenadores portátiles. Estos controles son relativamente direccionales, baratos y fáciles de construir, pero tienen un inconveniente importante: no atraviesan los objetos sólidos. Este inconveniente también resulta a veces una ventaja en el sentido de que ofrecen más seguridad, precisamente porque la comunicación no atraviesa las paredes de un edificio. Además, el uso de frecuencias en la banda de los infrarrojos no está regulado por las administraciones como ocurre con otras bandas de frecuencia.

La mayor parte de las comunicaciones en redes telemáticas inalámbricas se llevan a cabo en la banda de las microondas.

El uso del espacio radioeléctrico está regulado por las administraciones de los diferentes países. En la página web del Ministerio de Industria, Turismo y Comercio se puede obtener la asignación de frecuencias del espectro radioeléctrico en España:
www.mityc.es/telecomunicaciones/Espectro/Paginas/CNAF.aspx

3.6 USO DE LOS MEDIOS DE TRANSMISIÓN EN LAS REDES TELEMÁTICAS

En los apartados anteriores se ha dado un repaso a los diferentes medios de comunicación existentes. En este apartado se ofrece una síntesis de cómo y dónde se usan estos medios de transmisión dentro de las redes telemáticas más comunes en la actualidad. Recordemos que podemos establecer dos grandes tipos de redes telemáticas, las redes LAN y las redes WAN.

Empecemos con las redes LAN. En este ámbito, la gran mayoría de redes están constituidas por alguno de estos medios de comunicación:

- **Cable de par trenzado**. La inmensa mayoría de las redes LAN cableadas actuales utilizan cable UTP. La tendencia es utilizar cable UTP de categoría 5e o 6, aunque podemos encontrar aún muchas redes funcionando con cables UTP de categoría 5. La categoría 3 prácticamente ha desaparecido y la categoría 7 aún no está muy extendida.
- **Fibra óptica**. La fibra óptica se encuentra con frecuencia en las redes LAN formando parte de lo que se conoce como el troncal de la red, que es la parte de la red local que soporta mayor volumen de información. Además, es necesario utilizar fibra cuando la distancia es mayor de 100 metros. Habitualmente se utiliza fibra multimodo, ya que las distancias que hay que cubrir no son excesivamente grandes y este tipo de fibra es más barata que la fibra monomodo.
- **Medio inalámbrico utilizando señales electromagnéticas en el rango de las microondas**. El estándar actual para establecer redes LAN inalámbricas es Wi-Fi, cada vez más utilizado tanto en entornos domésticos como profesionales. Su punto fuerte es la flexibilidad y facilidad de instalación, ya que no requiere cableado. Las desventajas son la potencial falta de seguridad respecto a las redes cableadas y unas menores prestaciones respecto a éstas.

El uso de cable STP o cable coaxial en las redes LAN hoy en día es prácticamente inexistente.

Para redes WAN sin duda el medio estrella en la actualidad es la **fibra óptica**, aunque, como veremos más adelante, en una de las partes de las redes WAN, que es la conexión del usuario final a la red WAN (que se suele denominar red de acceso), se utilizan otras opciones:

- **Par trenzado telefónico**. Usado por los proveedores de acceso a Internet a través del par telefónico. Habitualmente usando tecnologías de banda ancha xDSL.
- **Cable coaxial**. Usado para proporcionar acceso a Internet por los operadores de cable.
- **Enlaces inalámbricos WiMAX**. Proporciona una conexión inalámbrica entre un abonado y un proveedor de servicio de datos.
- **Satélite**. También basado en el uso de tecnologías inalámbricas, habitualmente en el rango de las microondas.
- **Telefonía móvil**. La mayor parte de los operadores de telefonía móvil también proporcionan acceso a Internet mediante las redes inalámbricas de telefonía móvil utilizando GSM o 3G.

3.7 SISTEMAS DE CABLEADO ESTRUCTURADO

3.7.1 ESTÁNDARES DE CABLEADO ESTRUCTURADO

Cuando el número de equipos que se quieren conectar en una red es alto y estos equipos están ubicados en edificios de oficinas con varias plantas y/o estancias, es necesario estructurar adecuadamente la instalación del cableado que formará la red de área local. Afortunadamente existen estándares que proporcionan las pautas e indicaciones adecuadas y que facilitan enormemente la instalación y el mantenimiento de las redes locales, estos estándares se conocen como **estándares de cableado estructurado**.

El principal estándar de cableado estructurado lo ha desarrollado el organismo de estandarización norteamericano llamado **TIA** (Telecommunication Industry Association) y, por tanto, su ámbito de aplicación es en la región de Norteamérica. Dicho estándar es el **TIA/EIA-568-A** y fue publicado en 1995. Posteriormente, en 2001, se llevó a cabo una revisión del mismo, publicada como **TIA/EIA-568-B**. Este estándar se conoce como **norma de cableado de telecomunicaciones para edificios comerciales** (*commercial building telecommunication cabling standard*).

Debido al éxito de este estándar, otros organismos de estandarización lo han adoptado prácticamente sin cambios. Así, el equivalente estándar utilizado en Europa es el **EN 50173**, publicado por el CENELEC, organismo de estandarización europeo. Así mismo, y con un ámbito de aplicación mundial, se publicó el estándar **ISO/IEC 11801**, publicado por el ISO.

IMPORTANTE

AENOR ha publicado el equivalente a la norma europea EN 50173 con el código **UNE-EN 50173**. Esta norma es de obligado cumplimiento para la instalación de redes de datos en la mayor parte de las administraciones públicas.

Existen algunas pequeñas diferencias entre los estándares TIA/EIA e ISO/IEC, aunque se pueden considerar compatibles. Habitualmente se utiliza como referencia por parte de la industria (fabricantes, instaladores…) el estándar TIA/EIA-568-B por ser el más restrictivo.

Un estándar de cableado estructurado contiene un conjunto de normas para el diseño y la implementación de la infraestructura de cableado de forma que facilite el uso de la mayor cantidad posible de servicios de telecomunicaciones. El objetivo del estándar es proporcionar una infraestructura de telecomunicaciones altamente adaptable a los cambios, es decir, escalable.

Los sistemas de cableado estructurado definen aspectos que forman parte del nivel físico del modelo OSI, como son tipos de medios de transmisión, conectores, distancias, topología, etc. Lógicamente, su principal uso es como infraestructura para redes locales de datos.

3.7.2 PRINCIPALES CARACTERÍSTICAS

El estándar original EIA/TIA-568 se diseñó para proporcionar una infraestructura válida para instalaciones de hasta 3 km de longitud máxima, 1.000.000 m^2 de superficie de trabajo y hasta 50.000 usuarios. Por lo tanto, las normas de cableado estructurado cubren un amplio abanico de diferentes requisitos, ya que también se pueden utilizar de forma eficiente para redes más pequeñas con unos pocos de cientos de usuarios.

Otro de los aspectos que se persigue en la norma es que la infraestructura de cableado que siga el estándar sea válida un período mínimo de 10 años. Esto significa que el sistema de cableado estructurado debería ser capaz de soportar todos los servicios de comunicaciones necesarios durante ese período de tiempo y además puede afrontar de forma sencilla posibles ampliaciones del número de usuarios.

El sistema de cableado estructurado está ideado para que sea independiente de la aplicación, es decir, que dé soporte a cualquier tipo de comunicación de datos, por tanto, no solo se puede utilizar para redes locales, sino que dicha infaestructura es válida para cualquier sistema que requiera la transmisión de datos, como pueden ser sistemas de telecontrol y de televigilancia.

Por último, hay que destacar que una de las principales ventajas de los sistemas de cableado estructurado es su gran flexibilidad, ya que permite una gran movilidad de los puestos de trabajo sin apenas esfuerzo. Esto supone un importante ahorro en los costes de mantenimiento de las redes.

3.7.3 ARQUITECTURA Y SUBSISTEMAS

Para proporcionar un alto índice de flexibilidad, los sistemas de cableado estructurado están basados en el desarrollo de una estructura jerárquica formada por niveles de jerarquía conocidos como subsistemas. Se puede encontrar hasta tres niveles jerárquicos o subsistemas, subsistemas de campus, subsistema vertical y subsistema horizontal. En la siguiente figura se puede observar la estructura física del sistema de cableado y la ubicación de cada uno de los subsistemas.

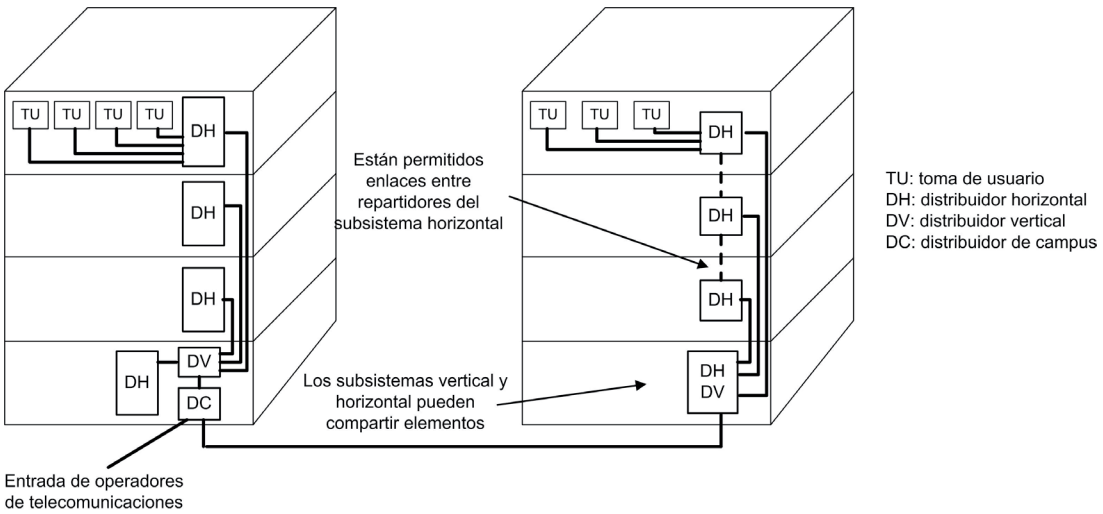


Figura 3.13. *Distribución de un sistema de cableado estructurado*

Los elementos que pueden existir en un sistema de cableado estructurado son los siguientes:

- **Repartidor o distribuidor de campus**. Es el elemento del sistema desde donde se distribuye el cableado que forma parte del subsistema de campus. Solo puede haber uno.
- **Cableado troncal de campus o backbone de campus**. Como su nombre indica, es el cableado que forma parte del subsistema de campus. Se utiliza para unir los diferentes edificios que forman parte de la infraestructura.
- **Distribuidor vertical o de edificio**. Es el elemento del sistema desde donde se distribuye el cableado que forma parte del subsistema vertical. Habrá un distribuidor vertical por cada edificio que forma parte del sistema.
- **Cableado troncal de edificio, vertical o backbone de edificio**. Es el cableado que forma parte del subsistema vertical. Su función es interconectar los diferentes subsistemas horizontales.
- **Distribuidor horizontal o de planta**. Es el elemento del sistema desde donde se distribuye el cableado que forma parte del subsistema horizontal. Habrá un distribuidor horizontal por cada planta del edificio.
- **Cableado horizontal**. Es el cableado que forma parte del subsistema horizontal y se encarga de conectar los puestos de trabajo al sistema de cableado.
- **Toma de usuario**, **toma de telecomunicaciones o toma de área de trabajo**. Es el punto de unión del equipo de usuario con el sistema de cableado estructurado. Se ubican en las áreas de trabajo.
- **Punto de transición (opcional)**. Punto de interconexión intermedio utilizado en alguna conexión horizontal que debe cubrir demasiada longitud. No es muy frecuente su uso.

Otros elementos:

- **Punto de demarcación (demarc) o acometida exterior**. Es el punto del sistema donde se conectan las líneas externas a la infraestructura de cableado y que proporcionan las comunicaciones con el exterior.
- **Sala de equipos o sala de telecomunicaciones**. Es el espacio donde se encuentran los equipos de interconexión que forman parte del sistema de cableado, así como otros equipos que formen parte de la infraestructura de comunicaciones, como *routers*, servidores, etc.

En la siguiente figura se puede observar la estructura lógica de un sistema de cableado estructurado donde se puede apreciar como sigue una estructura jerárquica en estrella.

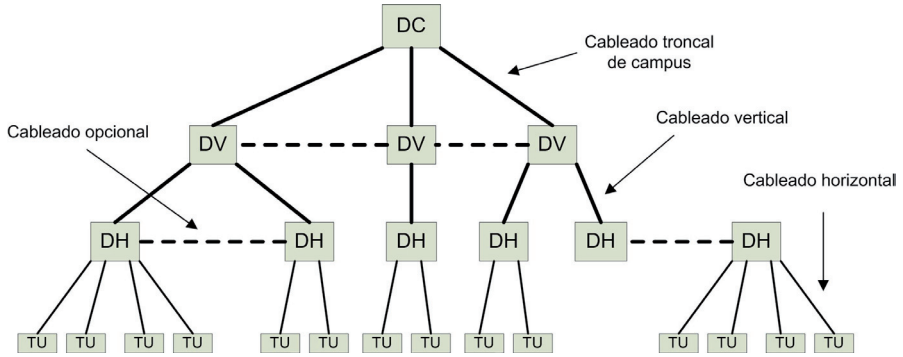


Figura 3.14. *Estructura lógica de un sistema de cableado estructurado*

3.7.3.1 Subsistema de distribución de campus

El subsistema de distribución de campus es la parte del sistema de cableado estructurado utilizado en la unión de diferentes edificios. Normalmente es el subsistema que cubre mayores distancias. Los medios de transmisión utilizados son la fibra óptica y los radioenlaces. Está formado por el distribuidor de campus, que estará situado en uno de los edificios, y el cableado troncal de campus. Lógicamente, este subsistema solo se implementará en los sistemas que necesiten conectar más de un edificio.

3.7.3.2 Subsistema de distribución vertical

El subsistema de distribución vertical, también conocido como *backbone*, se encarga de suministrar la interconexión entre los diferentes subsistemas horizontales. Habitualmente el cableado que forma parte del subsistema vertical recorre el edificio en sentido vertical, de ahí su nombre. Está formado por el distribuidor vertical y el cableado vertical. Sus principales características son:

- ✓ Como medio de transmisión se utiliza fibra óptica o cable de par trenzado.
- ✓ Se permiten conexiones entre dos subsistemas horizontales directamente. Dichas conexiones se considera que forman parte del cableado vertical.
- ✓ La distancia máxima entre el distribuidor de campus y el distribuidor vertical es de 2.000 metros.
- ✓ La distancia máxima entre el distribuidor vertical y el horizontal es de 500 metros.

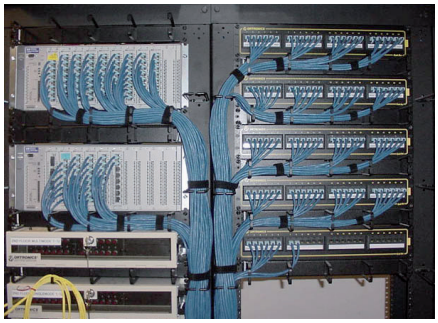


Figura 3.15. *Distribuidor de cableado*

3.7.3.3 Subsistema de distribución horizontal

El subsistema de distribución horizontal es la parte del sistema de cableado estructurado que suministra la conectividad a los puestos de trabajo en las diferentes áreas de trabajo que cubre dicho sistema. Frecuentemente, el área cubierta por un subsistema de distribución horizontal es una planta del edificio donde está ubicada la instalación. Todo el cableado que forma parte de este subsistema está en una misma planta de la instalación, de ahí su nombre. Los elementos que forman parte del subsistema son:

- **Cableado horizontal**. El cableado que forma parte de este subsistema es el cableado que va desde el distribuidor horizontal hasta la toma de usuario en el área de trabajo. Normalmente, el tendido de este cable se hace por falsos suelos y techos o por canaletas.

- **Latiguillos**. Además del cableado horizontal propiamente dicho, hay que incluir un cable de unión entre el distribuidor horizontal y la electrónica de red, y otro cable de unión entre la toma de usuario y el equipo. Estos cables de unión se conocen como latiguillos. Un latiguillo es un cable UTP con un conector RJ-45 en cada uno de sus extremos.

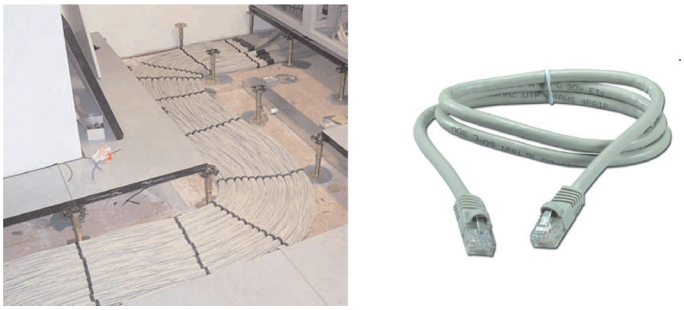


Figura 3.16. *Tendido de cableado horizontal por un falso suelo y latiguillo de red*

- **Rosetas**. Con este nombre se conoce al elemento que hace las funciones de toma de usuario. Una roseta es un conector hembra RJ-45 y, por tanto, en una roseta se conectará un latiguillo para unir el equipo del usuario a la red.

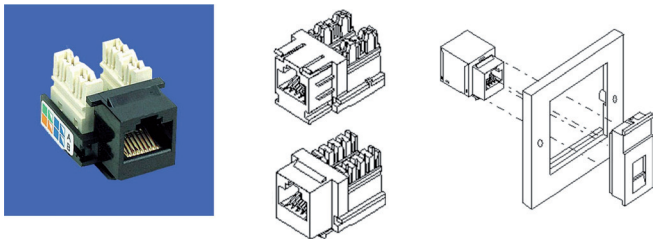


Figura 3.17. *Roseta*

- **Patch panel**. Son los elementos que hacen la función de distribuidor horizontal, ya que es donde va conectado el cableado horizontal que llega de cada uno de los puestos de trabajo. Los *patch panel* (o paneles de parcheo) van montados en armarios de comunicaciones especialmente diseñados para alojar este tipo de elementos junto con otros auxiliares.

Figura 3.18. *Patch panel*

- **Electrónica de red**. Son los dispositivos electrónicos que proporcionan las funciones de red propiamente dichas. Actualmente esta función la proporcionan los dispositivos conocidos como *switches*. Dichos dispositivos no forman parte del sistema de cableado propiamente dicho.

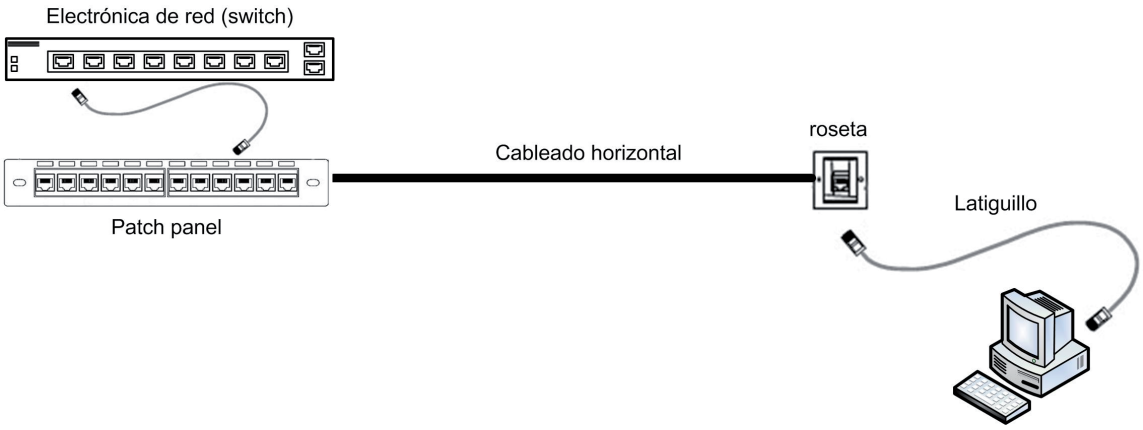


Figura 3.19. *Conexión del sistema de cableado a la electrónica de red*

Las características más destacadas de este subsistema son:

- ✓ La distancia máxima que pude cubrir el cableado horizontal es de 90 metros.
- ✓ La suma de las longitudes de los latiguillos de cada punto de interconexión no debe ser superior a 10 metros.
- ✓ El tipo de cable de cobre utilizado es UTP de categoría 5e o 6. La norma también permite utilizar cable STP si las condiciones lo requieren.
- ✓ Cada puesto de trabajo debe tener dos tomas de usuario para prevenir ampliaciones del sistema y futuros nuevos servicios.

3.7.4 INSTALACIÓN Y CERTIFICACIÓN

La instalación de un sistema de cableado estructurado requiere de una adecuada planificación y el conocimiento de los espacios físicos donde se va a ubicar. En este apartado se ofrecen algunas nociones básicas referidas sobre todo a la parte del subsistema horizontal que es la parte del sistema de cableado estructurado que mejor conviene conocer.

En el apartado anterior ya se hablaba sobre los armarios de comunicaciones, que son los espacios donde estará ubicado el distribuidor horizontal junto con la electrónica de red. Existen en el mercado multitud de modelos de armarios de comunicaciones, los más usados son los armarios de 19" de cuerpo entero y los armarios murales de 19" utilizados en pequeñas instalaciones o en instalaciones auxiliares.

Figura 3.20. *Armarios de comunicaciones*

Las herramientas más utilizadas en la instalación del sistema de cableado estructurado son:

- **Crimpadora**. También se puede encontrar bibliografía que la denomina *grimpadora*. Esta herramienta se utiliza para unir un conector RJ-45 con un cable UTP.
- **Herramienta de impacto o de inserción**. Utilizada para conectar el cableado UTP al *patch panel* por la parte posterior del mismo.

Figura 3.21. *Herramienta de impacto y crimpadora*

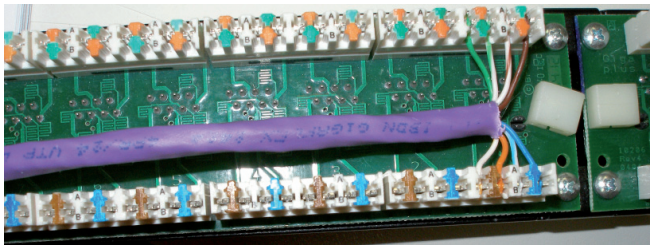


Figura 3.22. *Conexión de un cable de red a un patch panel*

- **Téster de red**. Dispositivo formado por dos unidades que se utiliza para comprobar que no haya ningún par del cableado que no tenga conectividad. Una unidad se conecta en un extremo del cable y la otra unidad al otro extremo. Normalmente la comprobación se hace mediante algún sencillo sistema de luces.

Figura 3.23. *Téster de red*

Hay fabricantes de dispositivos electrónicos que han desarrollado herramientas para comprobar que una instalación cumple con los parámetros exigidos en las normas de cableado estructurado. Estas herramientas se conocen como **certificadores de cableado** y lo cierto es que en la actualidad son dispositivos electrónicos con funciones muy potentes. Una instalación de cableado que ha sido comprobada por un dispositivo de este tipo se dice que es una instalación certificada, esto significa que se ha comprobado que la conexión de todas las tomas de usuario al sistema de cableado cumple los requisitos exigidos por las normas de cableado estructurado.

Figura 3.24. *Certificador de cableado*

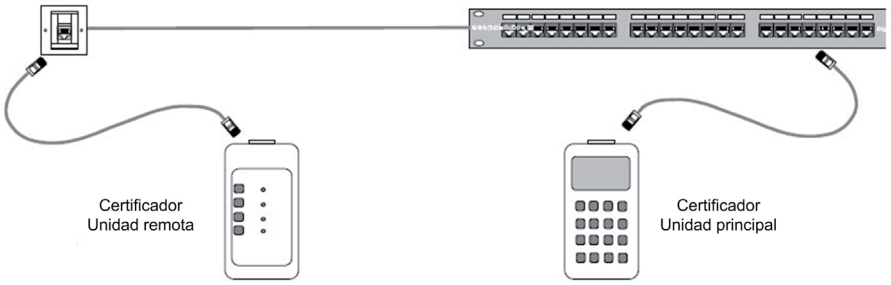


Figura 3.25. *Conexión del certificador al sistema de cableado*

EJERCICIOS PROPUESTOS

1. Busca información sobre los medios de transmisión utilizados por las tecnologías LAN y WAN utilizadas en la actualidad.

2. Busca en catálogos y páginas web de fabricantes de cableado las principales características de cableado comercial, tanto de cobre como de fibra óptica. Obtén información de los precios.

3. Busca información en catálogos y páginas web de fabricantes sobre los diferentes elementos relacionados con las instalaciones de cableado estructurado vistos en esta unidad, como *patch panel*, armarios de comunicaciones, canaletas, bandejas… Así mismo, obtén información sobre el precio de estos elementos.

TEST DE CONOCIMIENTOS

1 La mayor parte de las comunicaciones inalámbricas en los sistemas telemáticos utilizan:
- **a)** Ondas de radio de baja frecuencia.
- **b)** Ondas de radio de alta frecuencia.
- **c)** Microondas.
- **d)** Ondas infrarrojas.

2 La principal diferencia entre las categorías de cable de cobre existentes es:
- **a)** El tipo de conector utilizado: RJ-11, RJ-45…
- **b)** La distancia máxima que pueden cubrir.
- **c)** El tipo de red en el que se pueden utilizar.
- **d)** El ancho de banda y, por tanto, la velocidad de transmisión.

3 El tipo de medio de transmisión más empleado en las redes LAN es:
- **a)** Exclusivamente cable de par trenzado UTP.
- **b)** Principalmente cable de par trenzado UTP y cable coaxial para la parte troncal.
- **c)** Cable de par trenzado, tanto UTP como STP.
- **d)** Principalmente cable de par trenzado UTP, aunque también es posible utilizar fibra óptica.

4 ¿Qué elemento se utiliza en la fibra óptica monomodo para transmitir?
- **a)** Emisores LED.
- **b)** Emisores láser.
- **c)** Fotodiodos.
- **d)** Fotorresistencias.

5 El cable de cobre UTP utilizado en redes locales está formado por:

a) Un par.
b) Dos pares.
c) Tres pares.
d) Cuatro pares.

6 Los medios no guiados se utilizan especialmente:

a) En redes LAN.
b) En la red de acceso de las redes WAN.
c) En la red de transporte de las redes WAN.
d) Tanto en redes LAN como en la red de acceso de las redes WAN.

7 La principal diferencia entre cable categoría 5 y categoría 6 es:

a) El ancho de banda.
b) La resistencia a la humedad y corrosión.
c) El tipo de datos que se pueden transmitir.
d) Todas las respuestas anteriores son correctas.

8 La ventaja del uso de cable de fibra óptica respecto al cable de cobre es:

a) La fibra óptica tiene mayor ancho de banda.
b) La fibra óptica tiene mayor inmunidad frente a perturbaciones.
c) Las señales ópticas sufren una menor atenuación que las señales eléctricas.
d) Todas las respuestas anteriores son correctas.

9 El subsistema del cableado estructurado que proporciona conectividad a los puestos de trabajo de los usuarios es:

a) El subsistema horizontal.
b) El subsistema vertical.
c) El subsistema de campus.
d) Cualquier subsistema puede hacer esa función.

10 El tipo de cableado más común utilizado en el subsistema horizontal es:

a) Fibra óptica multimodo.
b) Fibra óptica monomodo.
c) Cable UTP categoría 3 ó 5.
d) Cable UTP categoría 5e o 6.

4 Control de enlace de datos

4.1 FUNCIONES DEL CONTROL DE ENLACE DE DATOS

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

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

Estas tres funciones están englobadas en el nivel de enlace, por tanto, el estudio de las técnicas para llevar a cabo las funciones citadas es, en el fondo, el estudio del propio nivel de enlace.

4.2 CONTROL DE ACCESO AL MEDIO

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

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

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

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

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

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

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

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

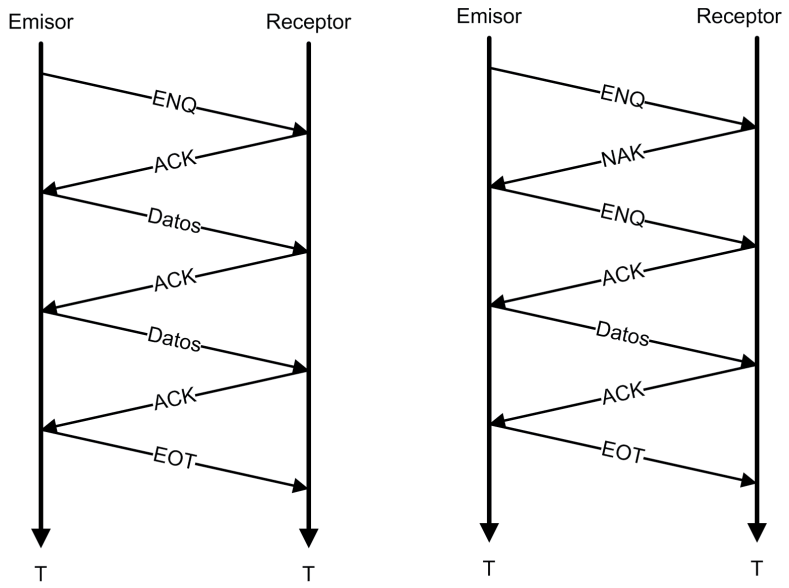


Figura 4.1. *Ejemplos de representación del envío de datos con la técnica de solicitud y reconocimiento*

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

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

4.2.1 SONDEO Y SELECCIÓN

La técnica de sondeo y selección se utiliza en enlaces multipunto, es decir, donde el medio está compartido por varios dispositivos, con configuraciones centralizadas, donde uno de los dispositivos ejerce de estación primaria o maestro, y el resto de dispositivos ejercen de estaciones secundarias o esclavos. En este caso, el dispositivo maestro controla el enlace y todas las comunicaciones se llevan a cabo a través del mismo, incluso las comunicaciones entre dos dispositivos esclavos. Los dispositivos esclavos siguen las instrucciones del maestro.

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

- **Comunicación desde el maestro a un esclavo**. Se lleva a cabo mediante el **modo selección** en el que el dispositivo maestro envía una trama de selección, para verificar que el dispositivo destino está preparado para recibir los datos. Dicha trama debe contener la dirección del dispositivo esclavo al que se va a enviar los datos. Esta trama irá pasando por los diferentes dispositivos del enlace, cada uno de los cuales comprobará la dirección incluida en la trama hasta llegar al dispositivo destino, que responderá con una trama ACK si está preparado para aceptar los datos.
- **Comunicación entre un esclavo y el maestro**. En este caso se utiliza el **modo sondeo** en el que el dispositivo primario envía una trama de sondeo a cada dispositivo secundario. Esta trama se utiliza para preguntar a cada dispositivo secundario si tiene algo que enviar. En caso negativo el dispositivo secundario envía una trama NAK y, en caso afirmativo, el dispositivo envía los datos que necesita enviar. La estación primaria responderá con una trama ACK para indicar que ha recibido los datos.

Un dispositivo secundario no puede iniciar una comunicación, sino que tiene que esperar a que el dispositivo primario le envíe una trama de sondeo para poder enviar sus datos. Si el destino de los datos es otro dispositivo secundario, los datos son enviados al primario, que es el que se encarga de dirigirlos al secundario correspondiente.

4.2.2 CONTIENDA

El método de **contienda** se utiliza en enlaces multipunto distribuidos en los que existen varios equipos conectados al mismo enlace y en los que no existen dispositivos que actúan como maestros. En este caso, se trata de establecer un mecanismo de arbitraje para resolver el conflicto ocasionado cuando dos equipos quieren acceder al mismo tiempo al medio de transmisión. Existen varias técnicas de contienda que se presentan a continuación:

ALOHA

Inicialmente desarrollado para radiotransmisiones, aunque aplicable a cualquier sistema en el que dispositivos no coordinados compiten por el uso de un solo canal compartido. En esta técnica, los dispositivos transmiten cuando tengan algo que transmitir. El problema se produce si dos (o más) dispositivos intentan transmitir sus datos al mismo tiempo. Cuando esto ocurre, el resultado es la alteración de las señales eléctricas originales y la consiguiente pérdida de la información. Esta situación se denomina colisión.

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

Para solucionar el problema de las colisiones, cuando un dispositivo transmite una trama debe escuchar el canal para comprobar si ha habido colisión. Básicamente esto consiste en comprobar que los niveles de tensión de las señales que se han propagado por el medio no han variado como consecuencia de una colisión. Si se comprueba que ha habido una colisión, el dispositivo espera un tiempo aleatorio y vuelve a transmitir la trama. Es fundamental que el tiempo de espera sea aleatorio para asegurar que las transmisiones no vuelvan a coincidir y vuelvan a producir una colisión.

ALOHA ranurado (slotted Aloha)

Esta técnica es una mejora de la ALOHA original. Su funcionamiento es igual que en ALOHA, excepto que, en este caso, se divide el tiempo en intervalos discretos correspondientes al tiempo de retransmisión de una trama, de forma que solo se puede comenzar a transmitir una trama en el comienzo de un intervalo o ranura de tiempo. Si se produce colisión, se espera un número aleatorio de intervalos de tiempo discretos o ranuras para realizar la retransmisión.

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

CSMA persistente (*Carrier Sense Multiple Access*, acceso múltiple por detección de portadora)

En esta técnica, cuando una estación quiere transmitir primero escucha, es decir, comprueba si hay datos propagándose por el medio. Si detecta que se están transmitiendo datos, es decir, que el canal está ocupado, espera a que se libere y entonces comienza su transmisión. Si se produce una colisión, espera un tiempo aleatorio y vuelve a comenzar el proceso. De nuevo, la aplicación de esta técnica mejora el rendimiento respecto a ALOHA ranurado.

CSMA no persistente

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

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

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

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

Por tanto, una vez que se detecta y finaliza la transmisión de la trama en curso, el dispositivo espera un tiempo aleatorio e intenta de nuevo la transmisión. A continuación se presentan las principales características de CSMA/CD:

- ✓ Si el medio está libre, la estación transmite su trama.
- ✓ Si el medio está ocupado, la estación espera hasta que quede libre y transmite su trama.
- ✓ Mientras se transmite la trama se comprueba si se produce colisión.
- ✓ Si se detecta una colisión se deja de transmitir inmediatamente, se espera un tiempo aleatorio y se intenta transmitir de nuevo.
- ✓ Solamente se comprueba si hay colisión mientras se transmite la trama, por lo que es importante que los sistemas que utilicen CSMA/CD estén correctamente diseñados para que no se produzcan colisiones después de que el transmisor deje de transmitir.

El principal campo de aplicación de CSMA/CD han sido las redes de área local (LAN) cableadas.

MACA (*Multiple Access with Collision Avoidance*, acceso múltiple con prevención de colisiones)

Este método se utiliza en redes inalámbricas donde el método CSMA/CD no resulta adecuado, ya que no se puede asegurar la detección de colisiones en todas las estaciones que forman parte de la red debido a la naturaleza de las señales utilizadas en la transmisión, las señales radioeléctricas.

La técnica consiste en que cuando un dispositivo quiere enviar datos, primero envía una pequeña trama de solicitud (trama RTS). El dispositivo receptor contesta a esta trama con otra trama de respuesta (trama CTS). Tanto la trama RTS como CTS contienen el número de bytes que se transmitirán en la trama de datos. Por tanto, cualquier dispositivo que reciba las tramas RTS o CTS sabrá que se va a iniciar una comunicación y sabrá además cuánto va a durar la transmisión de los datos. Cuando finalice dicha transmisión, podrá enviar su trama de solicitud RTS.

La única posibilidad de producirse una colisión es cuando dos dispositivos envían tramas RTS simultáneamente. En este caso, se espera un tiempo aleatorio y se retransmite la trama de solicitud.

Se añadieron algunas mejoras a la técnica original MACA y al resultado se le denominó MACAW.

4.2.3 PASO DE TESTIGO

Al igual que en el tipo anterior, se utiliza en enlaces multipunto distribuidos. Este método está basado en el uso de una trama de control llamada **testigo** (o *token*). Solo la estación que tenga el testigo puede transmitir datos a través del enlace. Cuando finaliza su transmisión cede el testigo a la siguiente estación siguiendo un orden determinado.

4.3 CONTROL DE FLUJO

El segundo aspecto que se necesita controlar en la gestión de un enlace de comunicación es el control de flujo, el cual es necesario para poder adaptar la velocidad de envío de datos con la velocidad de procesamiento de los datos en el receptor. El control de flujo es un conjunto de mecanismos que permiten saber al emisor cuándo puede transmitir.

Hay que tener en cuenta que, en muchas ocasiones, la velocidad de transmisión no está determinada por el ancho de banda de la línea de transmisión, es decir, la velocidad a la que el medio puede transmitir datos, sino que depende de la velocidad a la que los datos pueden ser procesados por el receptor. De esta forma, si los datos le llegan al receptor más rápido de lo que puede procesarlos, inevitablemente los datos se perderán. Podría pensarse en una solución basada en un *buffer* o memoria intermedia donde almacenar los datos hasta que el receptor los puede procesar. Pero esta solución solo retrasaría el problema de la pérdida de información, ya que los *buffers* tienen una capacidad limitada. Por ello se debe establecer un mecanismo para que el receptor pueda notificar al emisor cuándo puede enviar datos. Existen básicamente dos métodos: parada y espera, y ventana deslizante.

4.3.1 PARADA Y ESPERA

En este método de control de flujo, el emisor envía una trama y espera el reconocimiento de la misma antes de enviar la siguiente, dicho reconocimiento se envía mediante una trama ACK. Este proceso se repite hasta que el emisor no tiene más datos y envía una trama EOT para indicar el final de la transmisión. Debido a que el método lleva implícita una alternancia en el flujo de los datos, se puede utilizar tanto en transmisiones half-dúplex como full-dúplex.

Este método tiene como principal ventaja su extremada sencillez, pero tiene un gran inconveniente, que es su lentitud.

4.3.2 VENTANA DESLIZANTE

En el método de ventana deslizante, a diferencia del de parada y espera, el emisor puede enviar varias tramas consecutivas antes de esperar por la confirmación de las mismas. Así mismo, el receptor puede enviar una sola confirmación para varias tramas de datos. Para implementar esta técnica es necesaria la existencia de *buffers* tanto en el emisor como en el receptor. Cada trama se numera con un número de secuencia.

El nombre completo de esta técnica sería "ventana deslizante de módulo n". El valor de *n* está directamente relacionado con el tamaño máximo de las ventanas de transmisión. Por ejemplo, la más común es la técnica de ventana deslizante de módulo 8. Las tramas se numeran de 0 a n-1, y el tamaño máximo de la ventana es n-1. Para el ejemplo de ventana deslizante módulo 8, las tramas se numerarían de 0 a 7 y el tamaño máximo de la ventana es de siete tramas, uno menos del módulo. Esto es debido a que se pueden producir situaciones de ambigüedades que se resuelven reduciendo el tamaño máximo de la ventana.

Funcionamiento en el emisor

- En todo momento el emisor mantiene un grupo de números de secuencia que corresponde a las tramas que tiene permitido enviar. Ésta es la ventana de emisión.
- Inicialmente llenamos el *buffer* con todas las tramas que quepan, es decir, el tamaño máximo de la ventana. El tamaño máximo de la ventana se corresponde con el máximo número de tramas que pueden ser enviadas sin ser confirmadas. Si utilizamos ventana deslizante módulo 8, el tamaño máximo de la ventana será de 7. La ventana de emisión contendrá siete tramas y éstas se almacenan en el *buffer*.
- Cada vez que se envía una trama, la ventana de emisión se reduce "por la izquierda" una posición.
- Cada vez que llegue un asentimiento, la ventana de emisión se expande "por la derecha" tantas posiciones como tramas se confirmen en el asentimiento.
- El *buffer* contiene en todo momento las tramas que se pueden transmitir y las que están pendientes de confirmarse.

Funcionamiento en el receptor

- Ventana de recepción: grupo de tramas que el receptor tiene permitido aceptar. Toda trama que se reciba con un número de secuencia fuera de la ventana será descartada.
- Cuando se recibe una trama, se reduce "por la izquierda" una posición la ventana del receptor.
- Cuando se envía una confirmación, se expande "por la derecha" la ventana del receptor tantas posiciones como tramas se confirmen.
- Las confirmaciones (ACK) se envían numeradas con la siguiente trama que se desea recibir. Un solo ACK puede confirmar varias tramas simultáneamente. Por ejemplo, si se envía una trama ACK 3, significa que el receptor confirma la recepción correcta de todas las tramas hasta la 2 inclusive.

RECUERDA

Cuidado, la ventana del receptor no representa el número de tramas recibidas, sino las que todavía se pueden recibir antes de enviar una confirmación.

En la siguiente figura se puede ver un ejemplo:

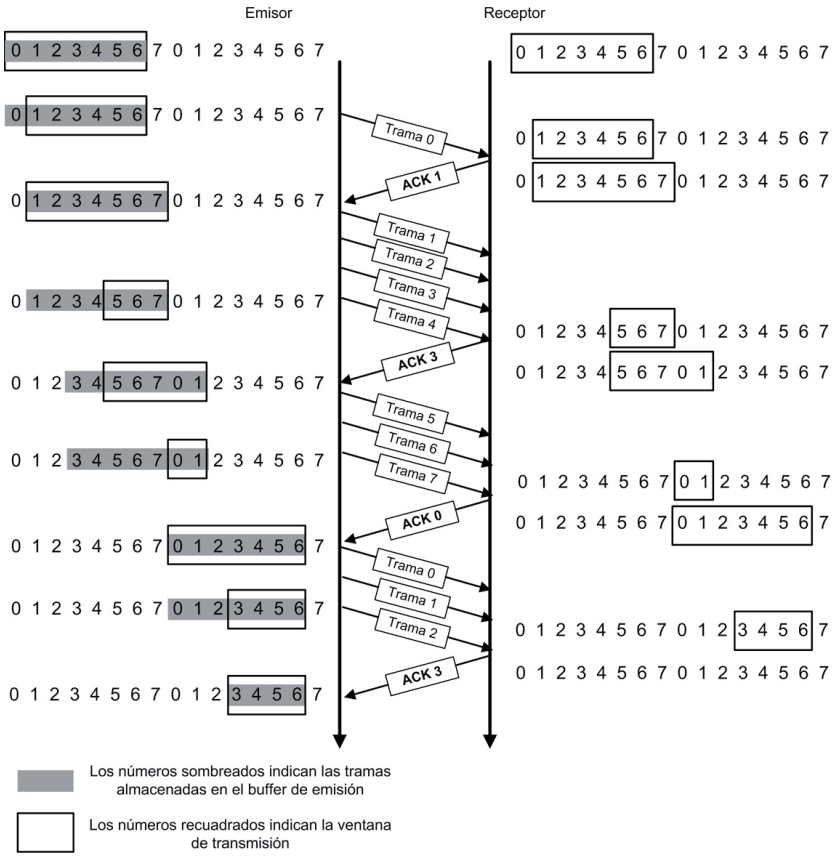


Figura 4.2. *Ejemplo de control de flujo mediante ventana deslizante*

El método de ventana deslizante es útil sobre todo para transmisiones full-dúplex en las que las tramas de confirmación se pueden enviar junto con los datos que se envían en el otro sentido de la transmisión, lo cual es más eficiente que enviar tramas separadas de control. Efectivamente, al llegar una trama de datos, en lugar de enviar inmediatamente una trama de confirmación, el receptor espera a que se tengan datos que transmitir. Cuando esto ocurre, aprovecha la trama de datos para incluir en su cabecera la confirmación a la trama recibida. La mayor parte de las veces es mucho más eficiente enviar las confirmaciones dentro de una trama de datos (en la cabecera de la trama) que utilizar una trama específica solo para enviar la confirmación, ya que ésta debe incluir una cabecera propia y un campo de comprobación de errores. Por ejemplo, en el protocolo HDLC se utiliza un solo bit para enviar una confirmación dentro de una trama de datos. Está claro que esta opción es mucho más eficiente. Esta técnica de retardar el envío de la confirmación para poder anexarlo a la siguiente trama de datos de salida se conoce como *piggybacking* (incorporación).

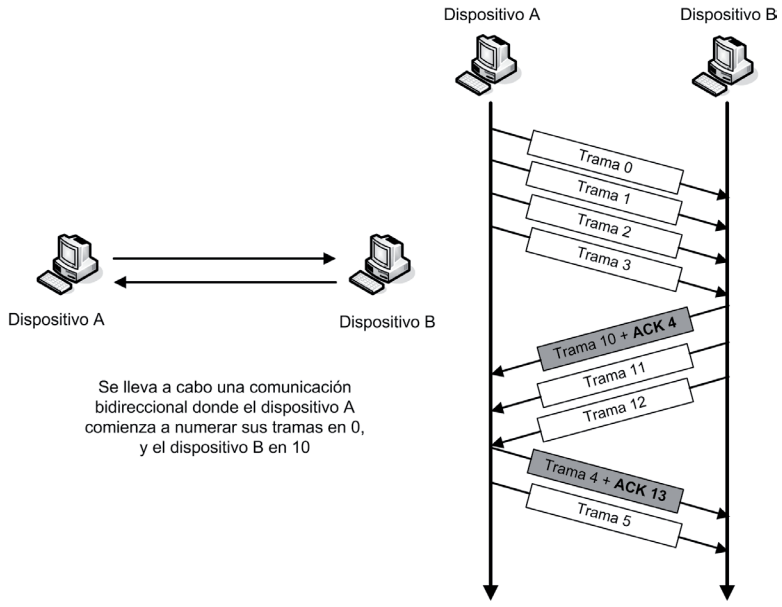


Figura 4.3. *Funcionamiento de la técnica piggybacking*

La técnica de ventana deslizante es especialmente útil en transmisiones full-dúplex, ya que se pueden aprovechar las tramas de datos para enviar confirmaciones.

Hay algunas implementaciones de ventana deslizante donde la ventana del transmisor y receptor no tienen el mismo tamaño. En algunos protocolos las ventanas pueden disminuir y aumentar a medida que se envían y reciben tramas.

4.4 CONTROL DE ERRORES

El control de errores es una de las principales funciones del nivel de enlace. Se trata de detectar y corregir todos los errores que se produzcan en el medio de transmisión.

El método más ampliamente utilizado para llevar a cabo la corrección de los errores detectados en el receptor se llama **petición de repetición automática o ARQ (*Automatic Repeat Request*)** y está basado en la retransmisión de las tramas en tres situaciones diferentes de error: tramas dañadas, tramas perdidas y reconocimiento perdido.

En la práctica, el control de errores con ARQ se implementa en el nivel de enlace como parte del control de flujo. De esta forma existe parada y espera con ARQ y ventana deslizante con ARQ.

4.4.1 PARADA Y ESPERA CON ARQ

Este método es básicamente utilizar como control de flujo parada y espera pero añadiendo la funcionalidad de la retransmisión de tramas perdidas o dañadas. Para ello se añaden cuatro características al mecanismo básico de control de flujo:

- ✓ Se mantiene en el emisor una copia de la trama enviada hasta que se recibe su reconocimiento. Esto es necesario para el caso en el que haya que retransmitir la trama con algún error o pérdida.
- ✓ Para permitir la identificación de las tramas de datos en el caso de que haya una transmisión duplicada, se numeran las tramas de datos y las tramas ACK alternativamente con 0 y 1.
- ✓ Cuando se detecta un error en el receptor, se envía una trama NAK sin numeración. Esta trama le indica al emisor que debe retransmitir la última trama enviada.
- ✓ Se utiliza un temporizador en el emisor. Si el reconocimiento a la trama de datos no se recibe en un tiempo determinado, se asume que la trama se perdió y se retransmite.

Cuando se detecta en el receptor una trama con error se envía una trama NAK y el emisor retransmite la trama.

La detección de tramas perdidas se realiza con el temporizador implementado en el emisor. Cada vez que se envía una trama se inicializa el temporizador, y si el mismo vence sin haber recibido asentimiento (positivo o negativo) se retransmite la trama de datos.

El tratamiento de reconocimientos perdidos (tramas ACK o NAK) se basa también en la retransmisión de las tramas de datos. Si la trama perdida fue un NAK, el receptor acepta la nueva copia recibida y devuelve un ACK. Si se perdió en ACK, el receptor detecta que la trama es duplicada, ya que las tramas se envían numeradas y por tanto descarta la misma y envía una trama ACK.

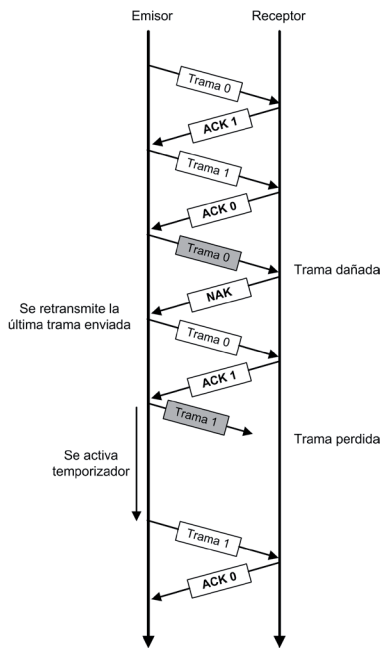


Figura 4.4. *Ejemplo de transmisión usando parada y espera con ARQ*

4.4.2 VENTANA DESLIZANTE VUELTA ATRÁS CON ARQ

En este caso se utiliza el método de ventana deslizante para llevar a cabo el control de flujo pero añadiendo las características de ARQ para el control de errores. Para ello se añaden las siguientes funcionalidades al método de ventana deslizante original:

- Si en el receptor se detecta que la trama llega con error, se envía una trama NAK para indicar al emisor que debe retransmitir la trama con error. La trama NAK debe incluir el número de la trama en la que se ha producido el error. Una trama NAK, además, confirma la recepción de todas las tramas pendientes de confirmación anteriores a la trama con error.
- Cuando el emisor recibe una trama NAK con un número de secuencia determinado, retransmite la trama con ese número de secuencia y todas las tramas que se hubiesen enviado después de la trama con error.
- Se implementa un temporizador en el emisor para solucionar el problema de las tramas de datos perdidas o los asentimientos perdidos. Cuando se envían todas las tramas posibles (tamaño de ventana 0) se activa el temporizador en el emisor. Cuando éste vence, se retransmiten todas las tramas pendientes de confirmación.
- Si se recibe una trama con un número de secuencia diferente del esperado, se considera una trama con error y se envía una trama NAK. Esta situación se suele producir cuando se pierde una trama de datos.

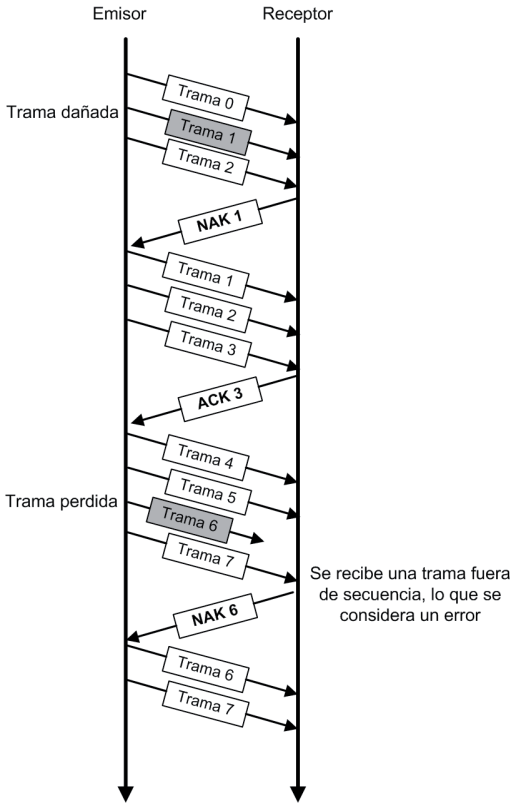


Figura 4.5. *Ejemplo de transmisión usando ventana deslizante vuelta atrás con ARQ*

4.4.3 VENTANA DESLIZANTE RECHAZO SELECTIVO CON ARQ

La técnica de rechazo selectivo utiliza también ventana deslizante como control de flujo y ARQ como control de errores. Por tanto, es muy similar al método de vuelta atrás, aunque presenta algunas diferencias. La principal diferencia es que cuando llega una NAK solo se retransmite la trama cuyo número de secuencia indica la trama NAK, es decir, la trama que llegó con error. Sus características son:

- ✓ Al igual que en vuelta atrás, cuando el receptor detecta que la trama llega con error se envía una trama NAK para indicar al emisor que debe retransmitir la trama con error. La trama NAK debe incluir el número de la trama en la que se ha producido el error.
- ✓ Cuando el emisor recibe una trama NAK con un número de secuencia determinado, retransmite solo la trama con ese número de secuencia. Esta característica hace que puedan llegar al receptor tramas desordenadas, por lo que hay que implementar en el receptor un método de ordenación de tramas. Ésta es la principal diferencia con el método de vuelta atrás.
- ✓ A diferencia del método de ventana deslizante, los números de secuencia enviados en las tramas ACK se refieren a la trama recibida, no a la siguiente esperada.
- ✓ Se utiliza un tamaño máximo de la ventana más pequeño que en el método general de ventana deslizante. Para la implementación de ventana deslizante de módulo n con rechazo selectivo se utiliza un tamaño de ventana de $(n + 1)/2$. En vuelta atrás se utilizaría el tamaño del método genérico: $n - 1$.
- ✓ Al igual que en vuelta atrás, se implementa un temporizador en el emisor para solucionar el problema de las tramas de datos perdidas o los asentimientos perdidos. Cuando éste vence, se retransmiten todas las tramas pendientes de confirmación.

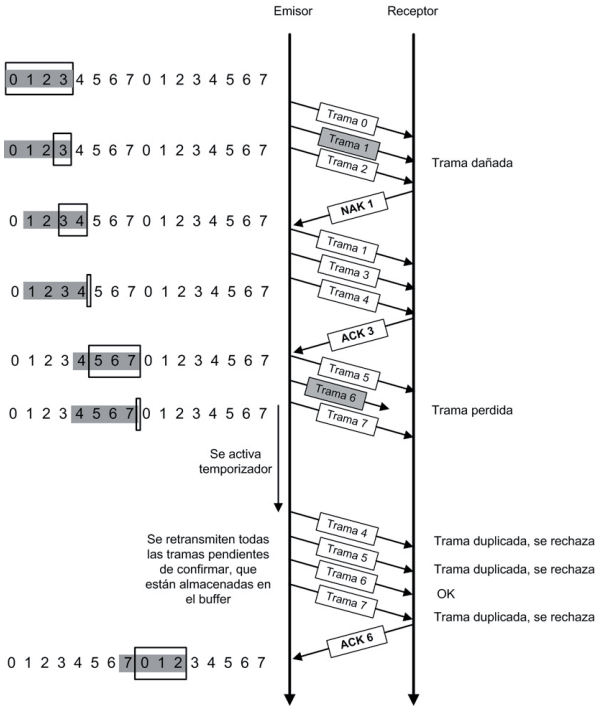


Figura 4.6. *Ejemplo de transmisión usando ventana deslizante rechazo selectivo con ARQ*

4.4.4 TÉCNICA DE DETECCIÓN DE ERRORES: CRC

La técnica ARQ se utiliza en el nivel de enlace, en combinación con el control de flujo para la corrección de los errores de transmisión. Este método se basa en la detección de los errores de transmisión en la recepción, por lo cual es necesario implementar en el nivel de enlace un mecanismo de detección de los errores.

Existen diferentes técnicas para verificar que un bloque de datos se transfiere de un sistema a otro sin errores, aunque el más utilizado en el nivel de enlace se conoce como **CRC (*Cyclic Redundancy Code*, código de redundancia cíclica)**.

Esta técnica se basa en añadir al bloque de datos una secuencia de bits, llamada CRC, obtenida a partir de la información contenida en el propio bloque de datos. Esta secuencia de bits es calculada por el emisor y transmitida junto con los datos. El receptor, cuando recibe los datos realiza el mismo cálculo. Si el CRC calculado por el receptor coincide con el recibido es que los datos no han sido alterados en la transmisión, es decir, no ha habido errores y por tanto la trama se acepta. Cuando el CRC calculado no coincide con el recibido es que ha habido errores en la transmisión, con lo cual la trama se rechaza.

La secuencia de bits o CRC se calcula realizando la operación división binaria de los datos entre un divisor predeterminado. A este divisor se le conoce como **polinomio generador**. El resto obtenido de la división es el CRC. Se conoce como polinomio generador porque la secuencia de bits del divisor se expresa como un polinomio. Por ejemplo, el número binario 1100101 se puede expresar de forma polinomial como:

$$1X^6 + 1X^5 + 0X^4 + 0X^3 + 1X^2 + 0X^1 + 1X^0$$

o lo que es lo mismo, suprimiendo los términos cuyo coeficiente es 0: $X^6 + X^5 + X^2 + 1$

El exponente más alto se conoce como orden, de forma que, en el ejemplo anterior, se dice que es un polinomio de orden 6. Los pasos que se siguen para el cálculo del CRC son:

1. Llamamos *n* al orden del polinomio generador.
2. A los datos para los que se quiera obtener su CRC se añaden a la derecha *n* ceros.
3. Se lleva a cabo la división binaria entre los datos (con los ceros añadidos) y el polinomio generador.
4. El resto que se obtiene en la división es el CRC que tendrá *n* bits.

En el siguiente ejemplo se quiere calcular el CRC para el bloque de bits 10110010. En este ejemplo utilizamos un bloque de datos de solo 8 bits, pero el proceso es el mismo para bloques de datos más grandes.

En el ejemplo se va a utilizar el siguiente polinomio generador de orden 3: $X^3 + X^2 + 1$, que expresado como número binario queda 1101. Como el polinomio generador es de orden 3 se añaden tres ceros a la derecha de los datos y se efectúa la división binaria.

Como se puede observar, la división binaria utiliza las mismas reglas que la división aritmética. La obtención de los cocientes parciales es sencilla:

- Si el bit más significativo del dividendo parcial es 1, el cociente parcial es 1.
- Si el bit más significativo del dividendo parcial es 0, el cociente parcial es 0.

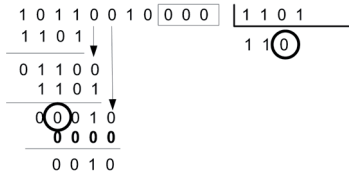
Por ejemplo, para el primer cociente parcial. El dividendo parcial es 1011, por tanto, el cociente parcial es 1. Se pasa el divisor para restarse al dividendo parcial:

La resta binaria también es sencilla:

0 – 0 = 0
0 – 1 = 1
1 – 0 = 1
1 – 1 = 0

Después de cada resta se toma el siguiente bit del dividendo y se descarta el que está más a la izquierda, que siempre va a ser un 0.

Si el cociente parcial es 0, se ponen todos los bits a cero:



Para el cálculo del CRC se descarta el cero de la izquierda del resto. Para el ejemplo queda como resto 100 que, por tanto, será el CRC obtenido.

4.5 TIPOS DE PROTOCOLOS

Los protocolos del nivel de enlace son los que implementan las funciones de dicho nivel y para ello hacen uso de las técnicas estudiadas en el apartado anterior. Dichos protocolos cubren básicamente las funciones de control de flujo y control de errores. Además, todos los protocolos del nivel de enlace especifican el formato de trama utilizado para la transmisión de los datos, incluyendo la información que se incluye en la cabecera. Si es necesario, los protocolos también incluyen mecanismos de direccionamiento físico.

Para enlaces multipunto compartidos, donde es necesario llevar a cabo un control de acceso al medio, se suelen utilizar protocolos diferentes a los protocolos que cubren las funciones de control de errores y control de flujo. Incluso se utilizan subniveles diferentes, como ocurre en redes de área local IEEE donde el nivel de enlace se divide en dos subniveles: MAC y LLC. MAC se ocupa del control de acceso al medio y LLC se ocupa del control de flujo y control de errores. Los protocolos desarrollados en el nivel de enlace se pueden dividir en dos grupos: asíncronos y síncronos.

4.5.1 ASÍNCRONOS

Los protocolos asíncronos son los primeros protocolos implementados en el nivel de enlace y se utilizaron sobre todo en las transmisiones de ficheros por módem. Su principal ventaja es que son fáciles (y, por tanto, baratos) de implementar. Su principal desventaja es su lentitud. De hecho, actualmente apenas se utilizan y han sido sustituidos por protocolos síncronos, más rápidos. Algunos ejemplos de los viejos protocolos asíncronos son XMODEM, YMODEM y ZMODEM.

4.5.2 SÍNCRONOS

Son protocolos más eficientes que los asíncronos. A su vez pueden ser orientados a carácter u orientados a bits. Actualmente casi todos los protocolos en el nivel de enlace utilizados en las principales arquitecturas y tecnologías de red son orientados a bits, fundamentalmente por una razón: la eficiencia.

El protocolo orientado a carácter más importante es **BSC (*Binary Synchronuos Communication*, comunicación síncrona binaria)**, desarrollado por IBM en los años 60. Este protocolo se puede utilizar tanto en comunicaciones punto a punto como en multipunto, y utiliza la técnica de parada y espera con ARQ para el control de flujo y errores.

La mayor parte de los protocolos utilizados en el nivel de enlace en las diferentes arquitecturas y tecnologías de red se basan en el estándar propuesto por la ISO, llamado HDLC. Originalmente se desarrollaron varias recomendaciones para completar el protocolo, pero actualmente están todos los aspectos del mismo agrupados en la recomendación ISO 13239.

HDLC (High-level Data Link Control, control de enlace de datos de alto nivel) es un protocolo del nivel de enlace orientado a bits que se puede utilizar para comunicaciones half-dúplex o full-dúplex y en configuraciones punto a punto o multipunto.

A su vez, la ITU-T modificó HDLC para crear su familia de protocolos **LAP** (*Link Access Procedure*) a partir de la cual se especificaron varios protocolos:

- **LAPB** (*Link Access Procedure Balanced*) como protocolo del nivel de enlace para redes X.25.
- **LAPD** (*Link Access Procedure – Channel D*) como protocolo del nivel de enlace de RDSI.
- **LAPM** (*Link Access Procedure for Modems*), protocolo incluido en la norma V.42bis como protocolo de corrección de errores para módems.
- **LAPF** (*Link Access Procedure – Frame*), protocolo de nivel de enlace para Frame Relay.

La organización IEEE también utilizó HDLC para crear su estándar IEEE 802.2, también conocido como **LLC (*Logical Link Control*)**. El organismo IETF (*Internet Engineering Task Force*) desarrolló el protocolo **PPP (*Point to Point Protocol*)**, cómo no, utilizando como base el protocolo HDLC.

EJERCICIOS PROPUESTOS

1. Calcula el CRC de la secuencia de bits 1111000011 a partir del polinomio generador X3 + X1 + 1.

2. Dibuja el esquema de transmisión y la ventana del emisor para un sistema que usa ventana deslizante módulo 8, vuelta atrás (rechazo simple) con ARQ a partir de la siguiente secuencia de operaciones:

- Trama 0 enviada, trama 0 reconocida.
- Tramas 1 y 2 enviadas, tramas 1 y 2 reconocidas.
- Tramas 3, 4 y 5 enviadas, recibido NAK 4.
- Tramas 4, 5, 6 y 7 enviadas, tramas 4 a 7 reconocidas.

3. Dibuja el esquema de transmisión y la ventana del emisor para la siguiente secuencia de operaciones:

- Trama 0 enviada.
- Trama 1 enviada.
- Trama 2 enviada.
- Trama 3 enviada.
- Trama 4 enviada.
- Recibido ACK 3.
- Trama 5 enviada.
- Recibido NAK 3.
- Enviadas tramas 3, 4 y 5.
- Recibido ACK 6.

4. Asume tamaño de la ventana 7. ¿Qué técnica de ventana deslizante se está utilizando?

TEST DE CONOCIMIENTOS

1 La técnica de solicitud y reconocimiento se utiliza:
- **a)** En enlaces multipunto half-dúplex.
- **b)** En enlaces multipunto full-dúplex.
- **c)** Exclusivamente en enlaces punto a punto full-dúplex.
- **d)** En enlaces punto a punto, tanto half-dúplex como full-dúplex.

2 En enlaces multipunto donde se utiliza una configuración centralizada en la que una estación tiene la función de estación primaria y el resto son estaciones secundarias se utiliza como método de acceso al medio:
- **a)** Sondeo y selección.
- **b)** Cualquiera de los métodos de contienda.
- **c)** Paso de testigo.
- **d)** Las dos últimas son correctas.

3 La mejora que introduce CSMA/CD respecto a otras técnicas de contienda es que:
- **a)** Primero escucha el medio antes de transmitir.
- **b)** Si detecta una colisión realiza la retransmisión de la trama.
- **c)** Si detecta una colisión deja de transmitir y espera un tiempo aleatorio antes de retransmitir.
- **d)** Divide el tiempo en intervalos discretos y solo puede transmitir al comienzo de cada intervalo.

4 El principal problema de la técnica de parada y espera es:
- **a)** Que es muy compleja de implementar.
- **b)** Que es lenta.
- **c)** Que solo sirve para comunicaciones full-dúplex.
- **d)** Que las tramas de datos tienen que tener una longitud fija.

5 En la técnica de ventana deslizante, la ventana de emisión contiene en todo momento:
- **a)** Todas las tramas que se tienen que enviar.
- **b)** Los números de secuencia de las tramas pendientes de enviar.
- **c)** Los números de secuencia de las tramas que pueden ser enviadas.
- **d)** Los números de secuencia de las tramas pendientes de confirmación.

6 En ventana deslizante vuelta atrás con ARQ, si se recibe un NAK con un número de secuencia:
- **a)** Se debe retransmitir la trama con ese número de secuencia.
- **b)** Se debe retransmitir la trama anterior a ese número de secuencia.
- **c)** Se debe retransmitir la trama con ese número de secuencia y todas las anteriores sin confirmar.
- **d)** No se utilizan tramas NAK.

5 Protocolos

5.1 ARQUITECTURA TCP/IP

En la arquitectura TCP/IP realmente no existe un modelo de red dividido en niveles, fundamentalmente porque su diseño se enfocó a implementar protocolos que solucionasen los requisitos de interconexión que se plantearon en su desarrollo inicial, y para ello no se partió de ningún modelo concreto. Así pues, el modelo en niveles de la arquitectura TCP/IP es un intento de acercamiento al modelo OSI y se puede considerar solo como una descripción de los protocolos existentes.

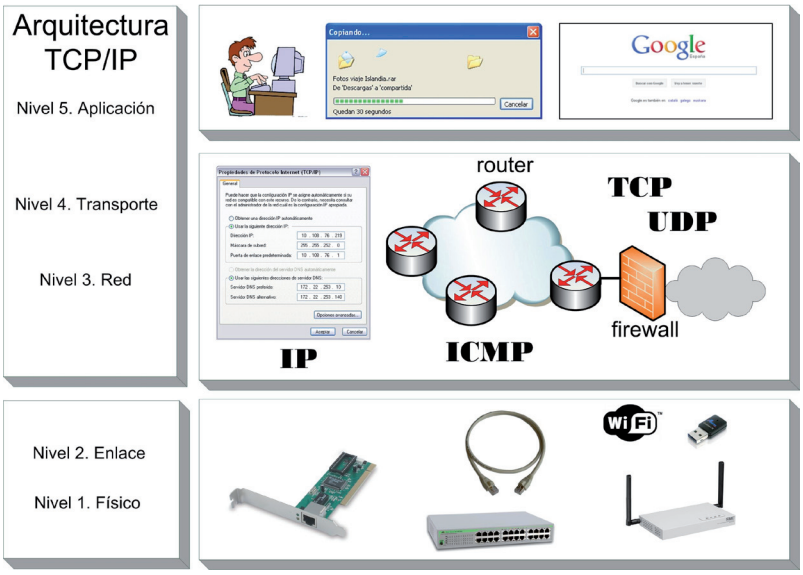


Figura 5.1. *Niveles en la arquitectura TCP/IP*

Aunque en el capítulo 1 se hizo una comparación en la que los modelos OSI y TCP/IP parecían muy similares, la siguiente figura se acerca más a la realidad.

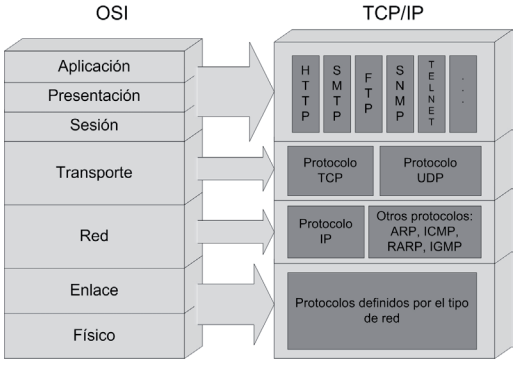


Figura 5.2. *Comparativa de niveles entre el modelo OSI y la arquitectura TCP/IP*

El modelo TCP/IP no diferencia los niveles físico y de enlace. Los protocolos TCP/IP propiamente dichos comienzan en el nivel 3, de forma que se puede utilizar cualquier protocolo y cualquier tecnología en estos niveles inferiores. Posiblemente éste sea uno de los factores que más ha ayudado a la expansión de la arquitectura TCP/IP.

Como se observa, el grueso de la arquitectura se encuentra en los equivalentes a los niveles de red y de transporte, los cuales curiosamente cubren prácticamente las mismas funciones que sus homónimos en el modelo OSI. A partir de ahí, todo pertenece al nivel de aplicación.

También se puede establecer un cierto paralelismo con el modelo OSI, en la forma en la que se pasan los datos entre los diferentes niveles en la arquitectura TCP/IP. Como ocurre en el modelo OSI, los dispositivos de interconexión solo implementan funciones hasta el nivel de red. Por tanto, dichos dispositivos de interconexión no necesitan implementar la complejidad del protocolo de transporte, encargado de proporcionar fiabilidad a la comunicación. Esto tiene una importante consecuencia, las comunicaciones intermedias entre nodos de la red (normalmente llevadas a cabo por los llamados encaminadores o *routers*) son relativamente fáciles de hacer, y esto proporciona eficacia y rapidez a las operaciones de enrutamiento de datos, algo que también ha sido crucial en el desarrollo de esta arquitectura.

IMPORTANTE

Los actuales dispositivos de interconexión, es decir, los *routers*, también necesitan acceder a la estructura de datos del nivel 4 (transporte), ya que aquí se encuentran los llamados **puertos de la comunicación**, un parámetro utilizado para algunas funciones relacionadas fundamentalmente con la seguridad.

5.2 PROTOCOLO DE RED IP

El principal protocolo que utiliza la arquitectura TCP/IP en el nivel de red es el **protocolo IP** (*Internet Protocol*). IP es un protocolo del nivel de red no orientado a conexión, basado en datagramas y no fiable.

- Se dice que un protocolo está **basado en datagramas** cuando la información que debe transmitir se divide en fragmentos. Por tanto, a cada uno de los paquetes o fragmentos de información que transporta IP se le denomina datagrama.
- IP es un protocolo **no orientado a conexión**, es decir, no se establece un camino previamente, con lo cual cada datagrama viaja de forma independiente, pudiendo llegar al destino fuera de secuencia o duplicado. No se crean circuitos virtuales.
- Y, además, es un protocolo **no fiable**, es decir, no ofrece comprobaciones ni seguimientos. IP intenta que los datos lleguen a su destino lo mejor que puede pero sin ofrecer garantías.

La unidad básica de información en el nivel 2 o nivel de enlace se denomina **trama**. La unidad básica de información en el nivel 3 o nivel de red es el **datagrama**.

Se puede comparar IP con el servicio de correo postal, donde, al igual que en IP, no se realiza ningún seguimiento de que una carta se reciba correctamente. Deben ser el remitente o el destinatario los que estén pendientes de que el envío llegue correctamente.

Si se necesita llevar a cabo una comunicación fiable utilizando IP, es necesario añadir otro protocolo que le dé fiabilidad a la transmisión; este protocolo es TCP en la arquitectura TCP/IP. Del mismo modo, para dar más fiabilidad a la entrega del correo postal, se puede utilizar el envío postal con acuse de recibo. En esta modalidad, cuando la carta llega a su destino, se envía un acuse de recibo al remitente. Si no se recibe acuse de recibo, el remitente puede suponer que la carta no llegó correctamente y volver a enviarla.

Aunque pueda parecer que IP es un protocolo con carencias, realmente no es así. Este funcionamiento permite gran flexibilidad para implementar los servicios en los niveles superiores.

La versión actualmente implantada en la mayor parte de los sistemas es la versión 4, conocida como IPv4. Sin embargo, algunas limitaciones de la versión 4 llevaron al desarrollo de la versión 6 (hay una versión 5 experimental no utilizada de forma comercial). La versión 6 de IP, conocida como **IPv6** (en sus inicios también fue conocida como **IPng** de *IP Next Generation*), fue adoptada por el organismo encargado de la publicación de los estándares en Internet llamado **IETF** (*Internet Engineering Task Force*) en 1994.

Hasta ahora el nuevo protocolo IPv6 apenas ha sido utilizado, aunque el agotamiento de las direcciones IPv4 está obligando a empezar a utilizarlo de forma cada vez más masiva. Más adelante en este tema se expondrán las principales características de esta nueva versión del protocolo IP.

5.2.1 DATAGRAMA IPV4

La transmisión de los datos en el nivel de red utilizando el protocolo IP se realiza en unidades de información llamadas **datagramas**. Como es de suponer, un datagrama consta de dos partes, una cabecera y los datos. La longitud de un datagrama es variable, pudiendo alcanzar un tamaño máximo de 65.535 bytes. A continuación se muestra la estructura de un datagrama IP. Los números mostrados en la parte inferior de la figura son los tamaños de los campos de la cabecera expresados en bits.

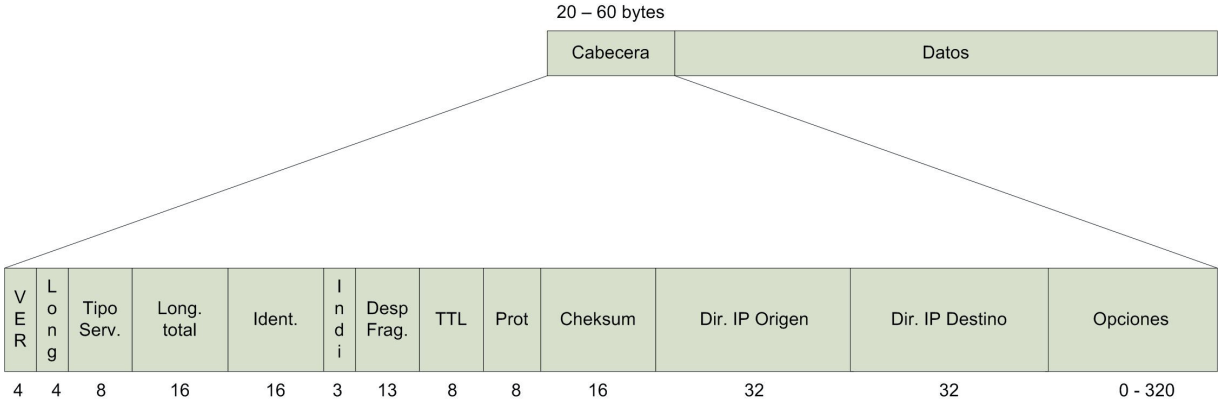


Figura 5.3. *Datagrama IP*

La descripción de cada uno de los campos es la siguiente:

- **Versión**. Se incluye la versión del protocolo IP. Actualmente la mayor parte de las redes utiliza la versión 4, por tanto este campo contiene el valor 4 en binario: 0100.
- **Longitud de la cabecera**. La cabecera de un datagrama IP no tiene un tamaño fijo. Su longitud puede estar entre 20 y 60 bytes. En este campo se define la longitud de la cabecera en un valor múltiplo de 4, es decir, el valor almacenado en este campo se multiplica por 4 para obtener el número total de bytes de la cabecera.
- **Tipo de servicio (actualmente ECN)**. En la especificación original de IP este campo se utilizaba para incluir información sobre el nivel de retardo, fiabilidad y prestaciones, en función del tipo de servicio que se estuviera utilizando. En la práctica este campo apenas ha sido utilizado, de forma que el IETF redefinió su uso como **ECN** (*Explicit Congestion Notification*), utilizado para enviar información sobre congestión de la red (RFC 3168 publicado en 2001).
- **Longitud total**. Almacena la longitud total del datagrama IP incluyendo la cabecera y los datos. Es un campo de 16 bits, por lo que puede almacenar hasta una longitud de 65.535 bytes.

IMPORTANTE

Aunque la longitud máxima que admite el protocolo IP es de 65.535 bytes, en la práctica el tamaño del datagrama IP utilizado en las redes suele ser bastante inferior y depende de la tecnología de red empleada en los niveles inferiores. Esto es así para evitar la fragmentación de los datagramas, lo que ocasionaría una importante pérdida de rendimiento.
El tamaño máximo en bytes de la unidad de datos que un protocolo puede procesar se conoce como **MTU** (*Maximum Transfer Unit*). El tamaño máximo del datagrama IP suele adaptarse a la MTU del nivel de enlace. Así, en redes Ethernet donde el tamaño máximo de la trama es de 1.518 bytes se establece el tamaño máximo del datagrama IP en 1.500 bytes.

- **Identificación**. Este campo se utiliza para enumerar los datagramas fragmentados. La fragmentación de un datagrama IP se produce cuando la MTU de una red es menor que la de la red en la que originó el datagrama. Por las características propias de IP, los datagramas fragmentados pueden llegar con un orden diferente con el que se enviaron, por lo que esta numeración es necesaria.
- **Indicadores**. Campo formado por tres bits:
  - El primer bit es de uso reservado y debe ser 0.
  - El segundo bit se llama **DF** (*Don't Fragment*) y se activa a valor 1 para indicar que el datagrama no puede fragmentarse. En caso contrario su valor será 0.
  - El último bit se llama **MF** (*More Fragments*) y su valor debe ser 1 para indicar que el datagrama está fragmentado y aún faltan más fragmentos por enviarse. Cuando su valor es 0 indica que es el último fragmento. En el caso de que sea un datagrama sin fragmentación su valor es también 0.

- **Desplazamiento del fragmento**. Este campo se utiliza para indicar el desplazamiento de los datos incluidos en el datagrama fragmentado respecto al datagrama original.
- **TTL** (*Time To Live*, tiempo de vida). Este campo es un número que indica el número de saltos que el datagrama puede realizar antes de ser descartado. Cuando se crea el datagrama se asigna a este campo un valor inicial (normalmente 127). Un salto se produce cuando el datagrama cambia de red, esto lo lleva a cabo un *router*. El *router* es el que decrementa el valor de este campo en una unidad. Si el valor del campo llega a cero, el datagrama se descarta. Este funcionamiento se utiliza para evitar que los datagramas permanezcan de forma indefinida en la red.
- **Protocolo**. Este campo es un identificador del protocolo de nivel superior utilizado. Los valores más comunes son TCP (6), UDP (17) o ICMP (1).
- **Cheksum o suma de comprobación**. Este campo se utiliza para la detección de errores en la cabecera. Para su cálculo no se tienen en cuenta los datos. Los errores de los datos deben ser detectados por los niveles superiores.

El código *checksum* se calcula de forma más sencilla que el CRC. Simplemente se efectúa la suma aritmética de los datos ajustando el resultado para representarlo con 16 bits.

- **Dirección lógica de origen**. Este campo identifica el dispositivo de red del que parte el datagrama. El formato de la dirección lógica utilizado en IP se especifica en el siguiente apartado.
- **Dirección lógica de destino**. Este campo identifica el dispositivo de red al que va dirigido el datagrama.
- **Opciones**. Este campo se puede utilizar para enviar información adicional en la cabecera del datagrama, aunque se utiliza con poca frecuencia.

5.2.2 DIRECCIONAMIENTO IPV4

Una de las principales funciones del nivel de red es el llamado direccionamiento lógico. Este direccionamiento lógico se utiliza para definir un identificador para cada dispositivo de la red, pero teniendo en cuenta la jerarquía necesaria en la arquitectura de las redes.

Por tanto, en el protocolo IP, cada dispositivo debe tener asignada una dirección lógica conocida también como **dirección de red** o **dirección IP**. Dicha dirección IP está formada por 32 bits (4 bytes) y consta de tres campos de longitud variable, dependiendo del tipo de red a la que pertenezca la dirección. Estos campos son la clase, el identificador de red y el identificador de *host*.

En terminología de redes, la palabra **host** se refiere a cualquier dispositivo conectado a una red y que es capaz de transmitir datos a través de dicha red. En el protocolo IP, un *host* es un dispositivo conectado a la red y que tiene asignada una dirección IP. Un *host* podría ser un equipo final como un PC de sobremesa, un portátil conectado por Wi-Fi, un *smartphone*, una impresora en red; o un equipo de interconexión, como un *router*.
Los casos un tanto especiales son los *switches* configurables y los puntos de acceso inalámbricos. Estos dispositivos operan habitualmente en los niveles físicos y de enlace, por lo que no se les puede considerar un dispositivo final que envía y recibe datos. Sin embargo, en operaciones de configuración de dichos dispositivos, estos se comportan como dispositivos finales (es decir, como *host*), ya que implementan un servicio web para el cual se necesita la asignación de una dirección IP.

Debido a la incomodidad que supone trabajar con direcciones IP en formato binario utilizando 32 bits, se ha definido una notación más práctica para representar dichas direcciones y que se conoce como **notación punto-decimal**. La representación en dicha notación simplemente consiste en agrupar los bits en grupos de ocho y representar cada grupo en notación decimal en lugar de binaria. Se utiliza el punto (.) para separar cada grupo.

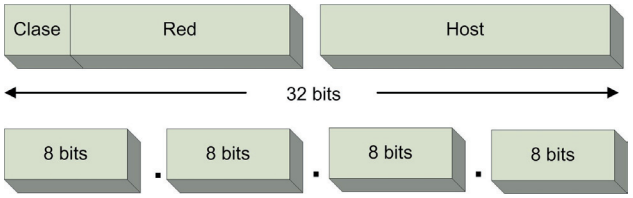


Figura 5.4. *Dirección IP jerárquica y notación punto-decimal*

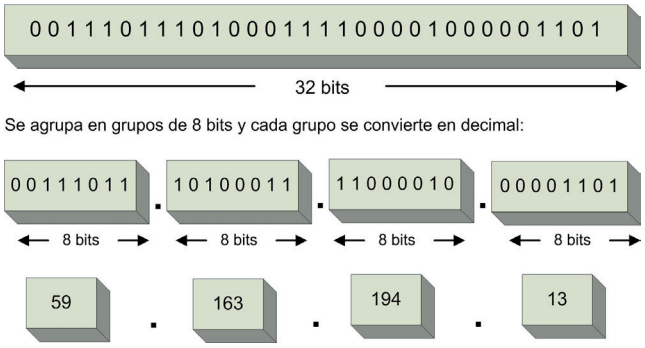


Figura 5.5. *Ejemplo de dirección IP en formato punto-decimal*

Como se observa, cada número decimal de una dirección IP realmente representa un número binario de 8 bits, por lo tanto, el rango válido de números que pueden aparecer en una dirección IP es del 0 al 255. A cada uno de estos números decimales que forman una dirección de red le denominaremos **octeto**.

La principal diferencia del direccionamiento lógico respecto al direccionamiento físico es que el primero es un direccionamiento jerárquico, donde una parte de la numeración se utiliza para identificar la red y otra parte para identificar el *host* dentro de la red.

Además de la jerarquía utilizada en las direcciones IP para identificar la red y los *hosts* dentro de cada red, fue necesario definir otro concepto conocido como clase. Las **clases** se definieron en el protocolo IP para optimizar el uso del enrutamiento de los datagramas, ya que no usar clases hubiera supuesto que los *routers* deberían almacenar una gran cantidad de información en sus tablas de enrutamiento, lo cual hubiera sido negativo para el funcionamiento de las redes. Se establecieron varios tipos de redes, es decir, de clases, para cubrir las necesidades de los diferentes tipos de organizaciones, ya que cada clase permite un máximo de direcciones IP en cada red que pertenezca a dicha clase.

Las clases que se definieron en el protocolo IP son:

- **Clase A**. En esta clase, el bit más significativo de la dirección IP vale siempre 0. Se utilizan 7 bits para identificar la red y el resto de bits, es decir, 24, se utilizan para identificar un *host* dentro de la red.
- **Clase B**. En este caso, el valor de los dos primeros bits de la dirección es siempre 10. Se utilizan 14 bits para identificar la red y 16 bits para identificar un *host* dentro de la red.
- **Clase C**. En este caso, el valor que se utiliza en los tres primeros bits para asignar la clase C es el 110. Se utilizan 21 bits para identificar la red y 8 bits para identificar un *host* dentro de la red.
- **Clase D**. Esta clase se identifica por contener en los cuatro primeros bits el valor 1110 y se utiliza para establecer direcciones de multienvío.
- **Clase E**. Identificada por sus primeros 4 bits tiene el valor 1111. Estas direcciones están reservadas inicialmente para usos futuros, aunque en la práctica nunca se ha llegado a definir ningún uso para estas direcciones.

El resumen del direccionamiento se puede ver en la siguiente figura:

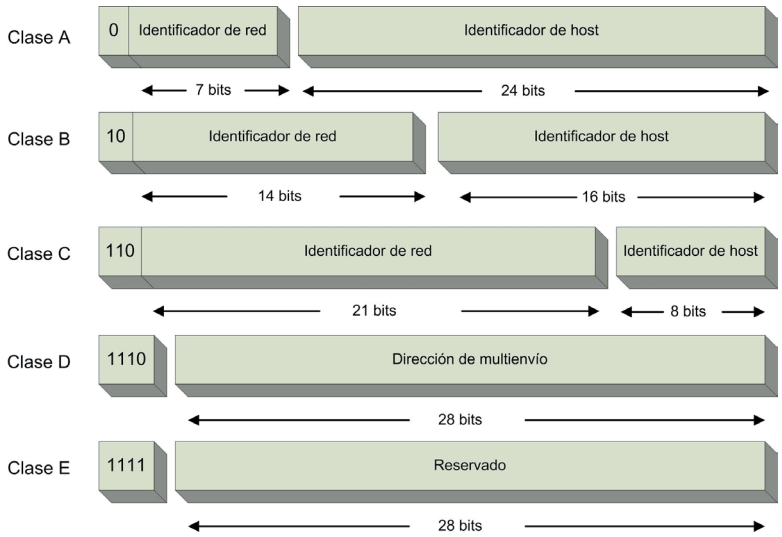


Figura 5.6. *Las clases en el direccionamiento IP*

Según la definición de las clases, un *host* dentro de una red tendrá asignada una dirección IP que pertenecerá a alguna de las tres primeras clases, es decir, las clases A, B y C. Es decir, para llevar a cabo la asignación de direcciones IP en una red, dicha red debe pertenecer a alguna de estas tres clases.

La figura anterior muestra de qué manera se identifica cada una de las clases basándose en el formato binario, pero en la práctica las direcciones IP se representan utilizando la notación punto-decimal. Por ejemplo, a continuación se indican tres direcciones IP representadas, lógicamente, en notación punto-decimal:

64.54.126.45 188.12.3.4 215.63.10.15

Con la información que tenemos sobre las clases no podemos deducir de forma inmediata a qué clase pertenece cada una de estas direcciones. Habría que pasar al menos el primer octeto a formato binario para conocer el valor de los primeros bits. Sin embargo, es mucho más práctico conocer los valores de ese primer octeto en notación decimal para cada una de las clases.

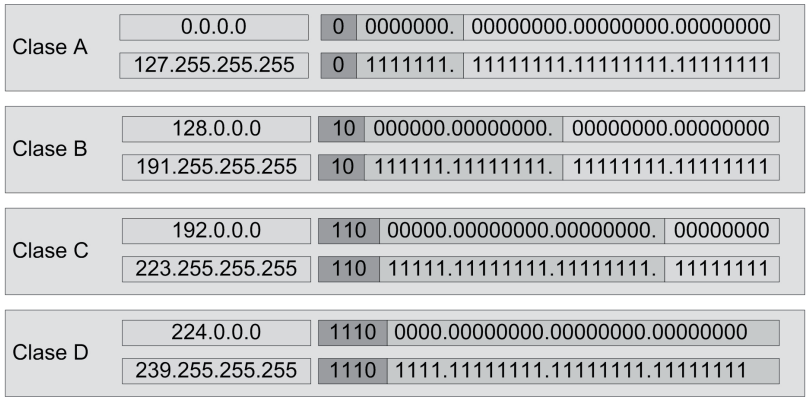


Figura 5.7. *Los rangos de las clases*

En definitiva, para identificar a qué clase pertenece una dirección IP solo es necesario fijarse en el primer octeto de la dirección IP. Con la tabla anterior ya sí es inmediato identificar a qué clase pertenece cada una de las direcciones anteriores. La primera pertenece a una red de clase A, ya que el primer octeto es el 64. La segunda es de clase B, ya que su primer octeto es el 188. Y la tercera pertenece a una red de clase C, ya que el primer octeto de la dirección es el 215.

También es conveniente conocer las capacidades teóricas de cada una de las clases:

- Puede haber un máximo de 128 (2^7) redes de clase A. Cada red de clase A puede contener un máximo de 16.777.216 (2^{24}) *hosts*.
- Puede haber un máximo de 16.384 (2^{14}) redes de clase B. Cada red de clase B puede contener un máximo de 65.536 (2^{16}) *hosts*.
- Puede haber un máximo de 2.097.152 (2^{21}) redes de clase C. Cada red de clase C puede contener un máximo de 256 (2^8) *hosts*.

Lógicamente, los diseñadores del protocolo IP nunca esperaron el espectacular desarrollo de su tecnología y, aunque en el momento de su desarrollo este esquema de direccionamiento parecía más que suficiente para proporcionar direcciones lógicas a todos los dispositivos, cuando empezó el crecimiento de Internet pronto se dieron cuenta de que dicho esquema de direccionamiento era poco eficiente.

Por último, es importante destacar que el protocolo define una serie de **direcciones IP reservadas** para otras funciones y que no se pueden utilizar como direcciones para *hosts*. La siguiente tabla muestra dichas direcciones:

X. 0. 0. 0	Dirección de red de una red de clase A.
X. X. 0. 0	Dirección de red de una red de clase B.
X. X. X. 0	Dirección de red de una red de clase C.
X.255.255.255	Dirección de difusión de una red de clase A.
X. X.255.255	Dirección de difusión de una red de clase B.
X. X. X.255	Dirección de difusión de una red de clase C.
0. 0. 0. 0	Dirección utilizada para referirse al propio equipo en las tablas de enrutamiento internas de los equipos.
127. 0. 0. 1	Dirección de *loopback* o de bucle local. Utilizada habitualmente para hacer pruebas de protocolos superiores.

En la especificación de la dirección en la tabla anterior, el símbolo X representa un valor cualquiera entre 0 y 255, que es el rango válido en la notación punto-decimal.

Las **direcciones de difusión**, también llamadas de **broadcast**, se utilizan para llevar a cabo envíos simultáneos a todos los dispositivos de una red. Las direcciones de difusión solo se pueden utilizar como direcciones destino en un datagrama IP.

La dirección de red se utiliza, especialmente, en los *routers* para identificar una red. Se podría decir que esa dirección reservada sirve para nombrar la red. Por ejemplo, la dirección IP 188.12.3.4 estaría asignada a un *hosts* que pertenece a la red 188.12.0.0, que es una red de clase B.

RECUERDA

Cuando en una dirección IP todos los bits reservados para identificar los equipos de una red están a cero, esa dirección no se refiere a ningún equipo, sino que es la **dirección de la red**. Y cuando están a uno, esa dirección es la **dirección de broadcast** o de difusión de la red.

5.2.3 SUBREDES

Como hemos visto, las direcciones IP incluyen dos niveles jerárquicos, por lo que cada dirección de red utiliza una parte para identificar la red y otra parte para identificar un equipo o *host* dentro de la red.

El protocolo IP permite, además, la utilización de un tercer nivel de jerarquía entre los dos niveles jerárquicos definidos por defecto, es el **nivel de subred**. Esta característica se utiliza cuando una organización, que tiene asignado un rango de direcciones IP (públicas o privadas), necesita organizar de forma interna el uso de dichas direcciones.

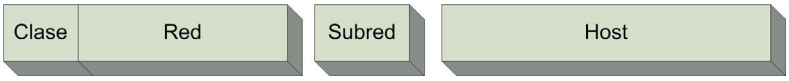


Figura 5.8. *Jerarquía de una dirección IP con subredes*

Para ello, se aplica una técnica llamada **enmascaramiento**, que es el proceso por el cual se puede obtener la dirección de red o de subred de una dirección IP dada. El enmascaramiento se puede aplicar tanto en redes que utilicen subredes como en redes que no las utilicen. De hecho, actualmente, y para ofrecer un método homogéneo del tratamiento de las direcciones de red, se aplica el enmascaramiento siempre.

Para utilizar esta técnica se define un parámetro llamado **máscara de subred** o simplemente **máscara**. La máscara es un número de 32 bits que define qué bits de una dirección IP se utilizan para identificar la red o subred y qué bits se utilizan para identificar el *host*. Lógicamente el valor de la máscara estará condicionado por la clase a la que pertenezca la dirección de red. Los bits que identifican la red o subred toman el valor 1 en la máscara. Los bits que identifican el equipo toman el valor 0 en la máscara.

Las máscaras utilizadas para redes que no utilizan subredes están acordes con las características de las clases utilizadas.

Clase	Máscara	Máscara en binario
Clase A	255.0.0.0	11111111.00000000.00000000.00000000
Clase B	255.255.0.0	11111111.11111111.00000000.00000000
Clase C	255.255.255.0	11111111.11111111.11111111.00000000

Cuando se utilizan subredes, la máscara especifica cuántos bits de la dirección IP se utilizan para la red y la subred. Por ejemplo, una empresa tiene reservada para su uso la dirección de clase B 180.30.0.0. Esto le permite utilizar hasta 65.534 direcciones de *hosts* diferentes. Al ser un número elevado de direcciones y por razones de organización, puede crear subredes. El número máximo de subredes que se pueden crear depende de la máscara elegida y debe ser potencia de dos, es decir, 2, 4, 8, 16, 32…

Si se decide utilizar una máscara que permita crear hasta ocho subredes, se deben añadir tres *unos* a la máscara original sin subredes para clase B. Para la clase B, la máscara es 255.255.0.0. Para llevar a cabo este proceso es más sencillo utilizar la notación binaria:

Máscara para una red de clase B: 11111111.11111111.00000000.00000000

Para el uso de ocho subredes se añaden tres *unos* a la máscara y se pasa de nuevo a notación punto-decimal.

Máscara en formato binario: 11111111.11111111.**111**00000.00000000

Máscara en notación punto-decimal: 255.255.224.0

Las direcciones de las subredes definidas en el ejemplo serían:

Dirección de subred	Dirección de red	Subred	Hosts
180.30.0.0	10110100.00011110.	000	00000.00000000
180.30.32.0	10110100.00011110.	001	00000.00000000
180.30.64.0	10110100.00011110.	010	00000.00000000
180.30.96.0	10110100.00011110.	011	00000.00000000
180.30.128.0	10110100.00011110.	100	00000.00000000
180.30.160.0	10110100.00011110.	101	00000.00000000
180.30.192.0	10110100.00011110.	110	00000.00000000
180.30.224.0	10110100.00011110.	111	00000.00000000

Para obtener la dirección de subred a partir de una dirección de red y una máscara se sigue el siguiente procedimiento:

- Los bytes de la dirección IP que se correspondan con el número 255 en la máscara se repiten en la dirección de la subred.
- Los bytes de la dirección IP que se correspondan con 0 en la máscara se cambian por un 0 en la dirección de la subred.
- Para números diferentes a 0 y 255 se aplica el operador AND entre el byte de la dirección IP y el byte de la máscara.

En los siguientes ejemplos se obtienen las direcciones de subred y de red de una dirección IP y su máscara:

Ejemplo 1

```
Dirección IP:          79.199.217.111
Máscara de subred:  255.255.   0.    0
```

La dirección IP pertenece a una red de clase A con subredes

Dirección de subred: 79.199.0.0

Dirección de red: 79.0.0.0

Se pueden definir hasta 256 subredes con 65534 host cada subred

Ejemplo 2

```
Dirección IP:          133.210. 51.  8
Máscara de subred:  255.255.255. 0
```

La dirección IP pertenece a una red de clase B con subredes

Dirección de subred: 133.210.51.0

Dirección de red: 133.210.0.0

Se pueden definir hasta 256 subredes con 254 host cada subred

La dirección IP pertenece a una red de clase C con subredes

```
Cálculo del cuarto octeto de la dirección de subred
77      01001101
192     11000000     AND
-------------------
64      01000000
```

Dirección de subred: 200.45.67.64

Dirección de red: 200.45.67.0

Se pueden definir hasta 4 subredes con 62 host cada subred

Algunas correspondencias útiles entre valores binarios y decimales:

- 10000000 128
- 11000000 192
- 11100000 224
- 11110000 240
- 11111000 248
- 11111100 252
- 11111110 254

5.2.4 ÁMBITOS EN EL USO DE DIRECCIONES IP: PÚBLICAS Y PRIVADAS

Durante los primeros años de funcionamiento del protocolo IP todos los dispositivos conectados en las redes que formaban Internet utilizaban direcciones IP dentro del espacio de direcciones conocido como **direcciones públicas**. Cuando una empresa o institución quería conectar su red a Internet solicitaba un bloque de direcciones. Esta asignación se hacía mediante las clases, es decir, cuando alguna entidad solicitaba direcciones públicas, se le asignaba un rango completo de una de las clases (A, B o C). Un organismo llamado **IANA** (Internet Assigned Numbers Authority) se encargaba de la asignación de las mismas.

Sin embargo, el rápido crecimiento de Internet hizo que esa política de asignación de direcciones IP no fuese viable. Fue necesario poner en marcha mecanismos para optimizar el uso de las cada vez más escasas direcciones IP públicas. Uno de esos mecanismos fue el uso de **direcciones privadas**, dichas direcciones son válidas en una red privada y no se pueden utilizar para la conexión a otras redes. En la siguiente tabla se muestran todos los rangos de direcciones IP que se pueden utilizar como direcciones privadas.

Rangos de direcciones IP privadas		Total rangos	Descripción
Primer rango	Último rango		
10.0.0.0		1	Dirección de red privada de clase A
172.16.0.0	172.31.0.0	16	Rangos de direcciones privadas de clase B
192.168.0.0	192.168.255.0	256	Rangos de direcciones privadas de clase C

Los mecanismos de enrutamiento desarrollados sobre el protocolo IP no permiten encaminar fuera de las redes privadas datagramas que utilicen este tipo de direccionamiento, por ello también reciben el nombre de **direcciones no enrutables**.

Para poder proporcionar conectividad en Internet a redes que utilizasen direcciones privadas se utilizó una variante de una técnica llamada **NAT** (*Network Address Traslation*). Dicha variante, conocida como **NAPT** (*Network*

Address Port Traslation) permite compartir una sola dirección IP pública entre varios dispositivos dentro de la misma red. En la actualidad, lo más frecuente es encontrar redes locales que utilizan direccionamiento privado dentro de la propia red y solo los *routers* tienen direccionamiento público. Para ello es necesario que los *routers* implementen NAT. Éste es el escenario más habitual en muchos tipos de redes, incluyendo las redes residenciales.

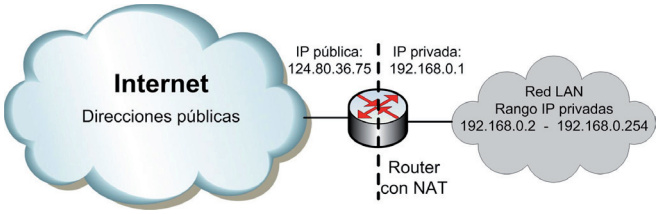


Figura 5.9. *Conexión de redes privadas con Internet mediante un router con NAT*

En función de lo expuesto, podemos distinguir por tanto dos tipos de direcciones IP, las direcciones IP públicas y las direcciones IP privadas. En los dos próximos apartados se expondrá de qué modo se lleva a cabo la asignación de cada tipo.

Aunque la técnica utilizada en la mayor parte de las redes privadas para acceder a Internet es NAPT, se suele emplear el término genérico de NAT para referirse a dicha técnica de traducción de direcciones.

Un *router* es un dispositivo de interconexión que permite unir dos o más redes diferentes. Es el dispositivo utilizado habitualmente para unir una red LAN con una red WAN como se observa en la figura 5.9. Más adelante en este capítulo se expondrán algunas nociones sobre los mecanismos de enrutamiento y en el capítulo 7 se hablará algo más de los *routers*.

5.2.5 ASIGNACIÓN DE DIRECCIONES IP PRIVADAS

Las direcciones IP privadas se suelen utilizar en las redes locales, de forma que todos los dispositivos conectados en una red local necesitan una dirección IP para intercambiar datos con el resto de dispositivos. Sin embargo, para que un equipo funcione correctamente en una red local necesita estar configurado para disponer tanto de conectividad física como lógica.

- **Conectividad física**. Hablaremos de conectividad física entre dispositivos cuando exista una infraestructura física que haga posible la comunicación de dichos dispositivos, por ejemplo, una red local. Todos los dispositivos conectados a dicha infraestructura tendrán conectividad física, es decir, existirá un camino físico por el que los dispositivos podrán intercambiar datos.

- **Conectividad lógica**. Por otra parte, hablaremos de conectividad lógica entre dispositivos cuando los parámetros de configuración del nivel de red (y superiores) permitan el intercambio de información entre dichos dispositivos. Lógicamente, para que haya un intercambio real de información entre los dispositivos debe haber tanto conectividad física como lógica.

Por tanto, para que un equipo conectado en una red local se pueda conectar con otros equipos, además de estar conectado físicamente a la red (ya sea por Ethernet o por Wi-Fi), deberá tener correctamente configurado su direccionamiento IP, es decir, su dirección IP y su máscara de subred. Lo más habitual es utilizar alguno de los rangos privados disponibles y su correspondiente máscara.

Primer rango	Último rango	Máscara de subred
10.0.0.0		255.0.0.0
172.16.0.0	172.31.0.0	255.255.0.0
192.168.0.0	192.168.255.0	255.255.255.0

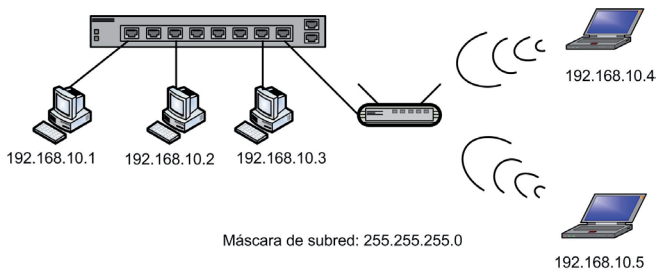


Figura 5.10. *Configuración de direcciones IP en una red privada*

En algunos casos además se podrá organizar el direccionamiento de la red en subredes. El uso de subredes se conoce con el término *subnetting*. El **subnetting** se utiliza principalmente para separar el tráfico de red generado en diferentes áreas de la organización donde está implementada la red.

Si se configuran diferentes subredes en una red local no habrá "visibilidad" entre los equipos de diferentes subredes, aunque sí haya conectividad física entre ellos.

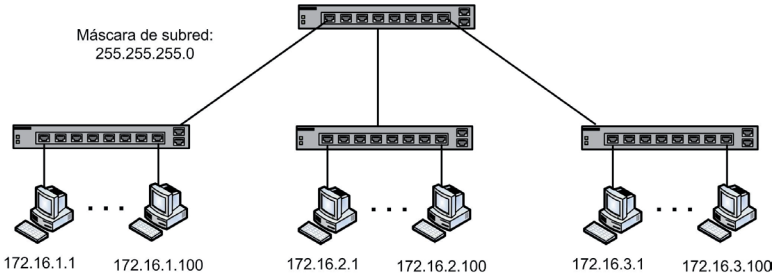


Figura 5.11. *Subredes IP sin conectividad lógica*

Para proporcionar conectividad lógica entre dispositivos de diferentes subredes será necesario el uso de *routers*.

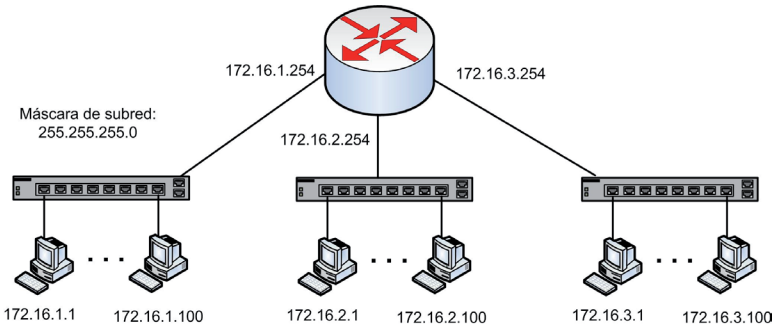


Figura 5.12. *Subredes IP con conectividad lógica proporcionada por un router*

IMPORTANTE

Se puede utilizar el formato de asignación CIDR en direcciones privadas. Por ejemplo, la dirección de red 192.168.0.0, que sería una dirección de clase C, equivale al rango CIDR 192.168.0.0 / 24.
Se puede utilizar la notación CIDR también para definir subredes. En este caso la técnica se conoce como VLSM (*Variable-Length Subnet Masking*, máscara de subred de longitud variable).

5.2.6 EL NUEVO PROTOCOLO IPV6

IPv6, que originalmente se llamó **IPng** (*IP Next Generation*), fue desarrollado por el organismo **IETF** (*Internet Engineering Task Force*) en 1994 sobre todo para solventar uno de los principales problemas que apareció en IPv4, que es la falta de direcciones IP. Además de solucionar este problema se añadieron características adicionales para mejorar el funcionamiento de IP. Por tanto, las principales características de IPv6 son:

- ✓ **Espacio de direcciones ampliado**. Éste es el principal objetivo de IPv6. Se define un nuevo tipo de dirección IP de 128 bits, en lugar de los 32 bits de una dirección IPv4, lo que conlleva un espacio de direccionamiento prácticamente inagotable.
- ✓ **Mecanismo de opciones mejorado**. Las opciones de IPv6 se encuentran en cabeceras separadas opcionales situadas entre la cabecera IPv6 y la cabecera de la capa de transporte. La mayoría de estas cabeceras opcionales no se examinan ni procesan por ningún dispositivo de enrutamiento en la trayectoria del paquete. Esto simplifica y acelera el procesamiento que realiza un dispositivo de enrutamiento sobre los datagramas IPv6 en comparación con los datagramas IPv4, y hace que sea más fácil incorporar opciones adicionales.
- ✓ **Direcciones de autoconfiguración**. Esta capacidad proporciona una asignación dinámica de direcciones IPv6, siendo por tanto innecesario el uso de DHCP.

- ✓ **Aumento de la flexibilidad en el direccionamiento**. IPv6 incluye el uso mejorado de direcciones *multicast* (envío de un datagrama a un grupo de receptores) incluyendo direccionamiento *anycast* (envío de un datagrama a un receptor dentro de un grupo).
- ✓ **Facilidad para la asignación de recursos**. IPv6 habilita el etiquetado de los paquetes como pertenecientes a un flujo de tráfico particular para el cual el emisor solicita un tratamiento especial. Esto ayuda al tratamiento del tráfico especializado, como puede ser el video o la voz en tiempo real.
- ✓ Las **características de seguridad**, **conocidas como IPsec**, **son intrínsecas al núcleo** del protocolo. En IPv4 se puede utilizar IPsec pero es opcional.
- ✓ **Enrutamiento y procesamiento de los datagramas en los routers es más eficiente** gracias a la jerarquía de direccionamiento de IPv6 y a que no haya fragmentación, ya que, de ser necesaria, ésta se aplica solo en el nodo origen.
- ✓ **Características para permitir la movilidad**.

5.2.7 DIRECCIONAMIENTO IPV6

El principal objetivo por el que se desarrolló la versión 6 de IP fue la ampliación del espacio de direcciones, que se había quedado corto con IPv4 después del gran desarrollo que experimentó Internet. Una dirección IPv4 es un número de 32 bits representados en formato punto decimal, es decir, agrupando los bits de ocho en ocho y pasando cada cifra a decimal. El nuevo protocolo IPv6 utiliza direcciones de 128 bits, es decir, cuatro veces más bits que una dirección IPv4. Con ello, el espacio de direcciones en IPv6 es de 2^{128}, un número enorme y prácticamente inagotable.

Además de ampliarse el número de bits de las direcciones IPv6 también se ha cambiado la forma de representar dichas direcciones. Se utiliza la numeración hexadecimal y se forman grupos de 16 bits, es decir, de 4 dígitos hexadecimales. Por tanto, una dirección IPv6 estará formada por 8 grupos de 4 dígitos hexadecimales. El carácter separador de cada grupo son los dos puntos (:). La siguiente dirección es un ejemplo de dirección IPv6:

2001:0bd8:0000:0000:0012:ac43:0000:65d3

La escritura de las direcciones IPv6 admite además varias simplificaciones:

- Dentro de cada bloque de 4 dígitos hexadecimales se pueden quitar los ceros a la izquierda. Aplicando esta regla, la dirección anterior quedaría:

  2001:**bd8**:0000:0000:**12**:ac43:0000:65d3

- Un bloque donde todos los dígitos sean cero se puede representar con un solo cero. Siguiendo con el ejemplo anterior:

  2001:bd8:**0**:**0**:12:ac43:**0**:65d3

- Se pueden sustituir varios bloques consecutivos con el valor cero por la abreviatura "::". Esto solo se puede aplicar una vez. Aplicando esta regla en el ejemplo:

  2001:bd8**::**12:ac43:0:65d3

En el siguiente ejemplo se muestra otra dirección donde existen bloques consecutivos a cero en dos partes de la dirección. Solo se aplica la regla anterior en la primera aparición:

Dirección sin simplificaciones: 2001:006b**:0000**:**0000:**cd41:**0000**:**0000**:923a

Dirección con simplificaciones: 2001:6b**::**cd41:**0:0**:923a

Para especificar bloques de direcciones IPv6 se utiliza la notación CIDR, donde se indica la dirección base del rango, con el valor correspondiente de su prefijo, y un número que indica el número de bits del prefijo.
Por ejemplo, el rango 2001:bd8:: / 32 indica que los 32 primeros bits de la dirección forman el prefijo del rango. El resto de bits de la dirección base están a valor cero. La primera dirección válida en este rango sería:
• 2001:bd8:0:0:0:0:0:1 o con la simplificación 2001:bd8::1
La última dirección IP del rango sería:
• 2001:bd8:ffff:ffff:ffff:ffff:ffff:ffff

5.2.8 TIPOS DE DIRECCIONES IPV6

Se han definido tres tipos de direcciones IPv6:

- **Unicast**. Dirección utilizada para identificar una interfaz de red única. Es equivalente a las direcciones IPv4 actuales. Hay varios tipos de direcciones Unicast que se pueden asignar a una interfaz de red. Las más comunes son las siguientes:
  - **Direcciones unicast globales**. Utilizadas como direcciones públicas. Actualmente el rango que se está utilizando para la asignación de direcciones *unicast* globales es **2000::/3**.
  - **Direcciones unicast de enlace local (local-link)**. Son direcciones utilizadas con propósitos de autoconfiguración y como dirección IP en redes donde no hay *router* que asigne una dirección *unicast* global, por tanto, este direccionamiento se aplica en el ámbito de redes locales. Son direcciones IP que no se pueden enrutar a otras redes. Se utiliza el rango **fe80::/10**.
- **Anycast**. Dirección utilizada para identificar un grupo de interfaces, normalmente asociadas a diferentes dispositivos. Un datagrama enviado a una dirección *anycast* se entrega solo a uno de los dispositivos del grupo de dispositivos asociados a la dirección *anycast*. Dicho dispositivo será el más cercano en términos de la distancia al nodo origen determinada por el algoritmo de enrutamiento que se esté utilizando. Este tipo de direcciones es útil para poder implementar varios servidores de un mismo servicio distribuidos geográficamente. Se utiliza una única dirección IP *anycast* y los dispositivos cliente que soliciten el servicio serán atendidos por el servidor "más cercano". Las direcciones *anycast* utilizan los mismos rangos que las direcciones *unicast* globales.

- **Multicast**. Dirección utilizada para identificar un grupo de interfaces, normalmente asociadas a diferentes dispositivos. A diferencia de una dirección *anycast*, un datagrama enviado a una dirección *multicast* se entrega a todos los dispositivos del grupo. Este tipo de direcciones se utiliza para aplicaciones de difusión donde se desea que una sola transmisión llegue a varios dispositivos. El rango utilizado para direcciones *multicast* es **ff00:: /8**. En IPv6 no hay direcciones de *broadcast*, en su lugar se utilizan las direcciones *multicast*.

Existen un par de direcciones IPv6 reservadas, que son las siguientes:

- **Dirección no especificada**. Utilizada en tablas de enrutamiento y otros mecanismos de configuración para indicar que no existe una dirección IPv6 específica.

  Dirección completa 0:0:0:0:0:0:0:0 Dirección abreviada **::**

- **Dirección de bucle local (*loopback*)**. Tiene el mismo significado que en IPv4. Es la dirección IP de una interfaz lógica de bucle utilizada para hacer pruebas internas de servicios de red.

  Dirección completa: 0:0:0:0:0:0:0:1 Dirección abreviada **::1**

Cada interfaz de red tendrá al menos una dirección *unicast* de enlace local. Dicha dirección se establece de forma automática en la interfaz de red. Para ello se utiliza el prefijo de red para direcciones de enlace local fe80:: / 64 y para establecer los últimos 64 bits de la dirección se utiliza el denominado identificador global de 64 bits (EUI-64), que se forma utilizando la dirección MAC de la interfaz de red como se muestra en el ejemplo.

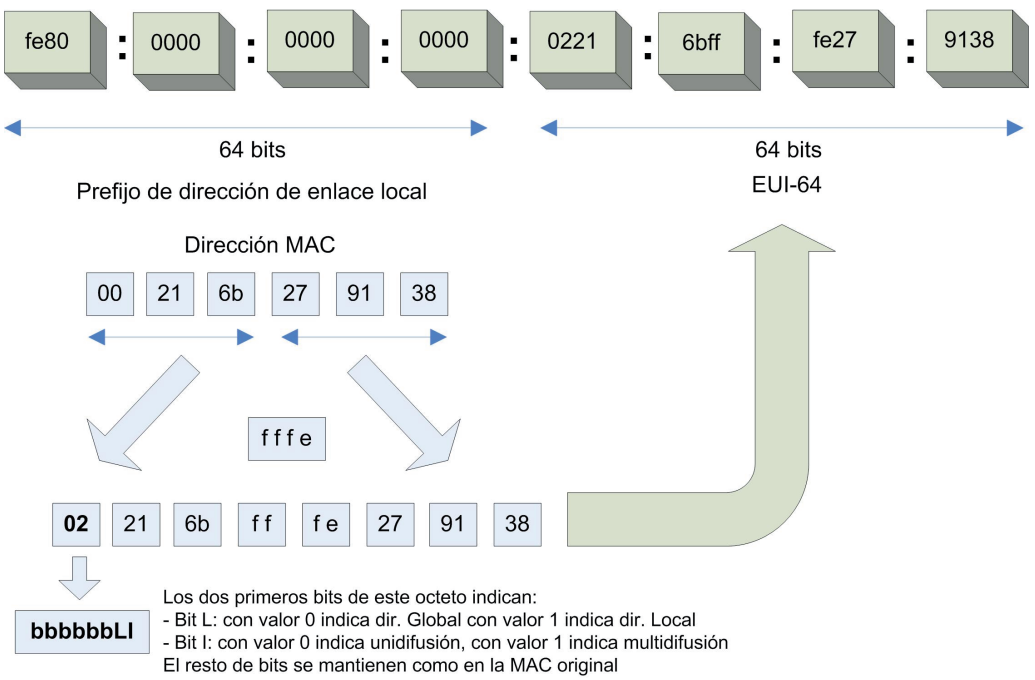


Figura 5.13. *Establecimiento de la dirección de enlace local en IPv6*

5.3 ENRUTAMIENTO

Una de las principales funciones del nivel 3 en las redes es la de encaminar o enrutar la información entre las diferentes redes hasta llegar a su destino. Dicha función es realizada por un dispositivo conocido como *router*. Los *routers* tienen una doble función en las redes. Por una parte se utilizan para unir redes, para ello retransmiten la información entre las redes a las que están conectados, adaptando, si es necesario, dicha información (tramas) entre diferentes tecnologías de red. Además de la función de interconectar redes, los *routers* implementan funciones de enrutamiento de paquetes. De hecho, los *routers* utilizados en los *backbones* de las grandes redes están especializados en esta función.

Cuando un *router* está conectado a dos redes sin otros *routers* adyacentes, el mecanismo de enrutamiento es bastante simple. Éste es el caso de un *router* de conexión a Internet (como se muestra en la figura 5.14) proporcionado por un ISP a sus clientes. El *router* conecta la red del ISP con la red local del usuario. Los paquetes de la red local con una dirección de destino que no pertenezcan a la red son encaminados a la red del ISP.

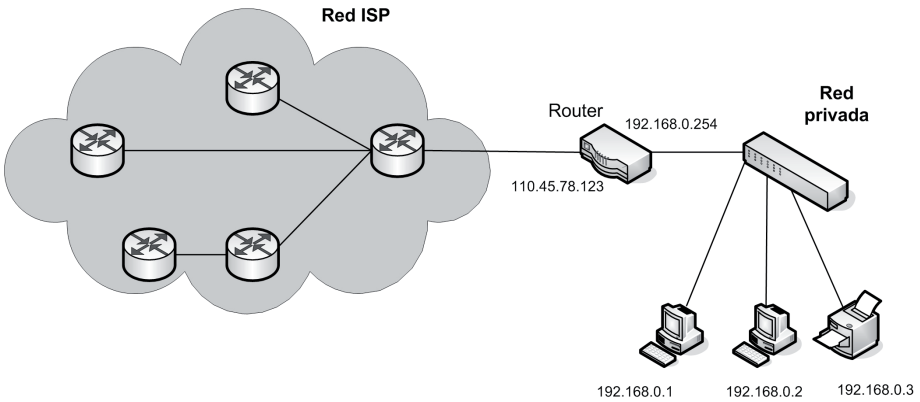


Figura 5.14. *Router para unir una red local con la red de un ISP*

Sin embargo, el enrutamiento se vuelve una tarea fundamental cuando un *router* tiene más de dos interfaces de red, es decir, está conectado a más de dos redes, o en las redes a las que está conectado existen otros *routers*. En este caso, los *routers* deben almacenar información que le permita decidir la interfaz de red por la que tiene que redirigir un paquete. Esta información se almacena en la llamada **tabla de enrutamiento**. Además, los *routers* deben implementar algún mecanismo que obtenga y actualice periódicamente la información de dicha tabla. Estos mecanismos son los llamados **algoritmos de enrutamiento**. La topología de interconexión en las grandes redes que habitualmente es de tipo mallada (como se observa en la figura 5.15) hace que la elección de un algoritmo de enrutamiento eficiente sea fundamental para el rendimiento de las propias redes.

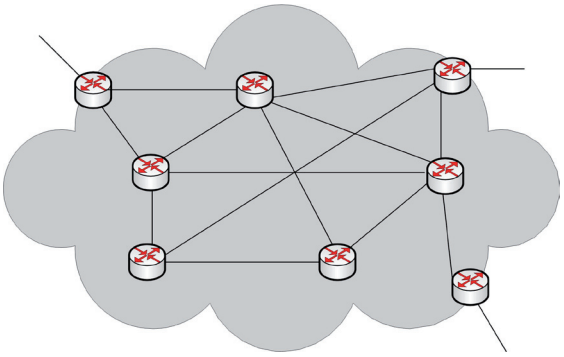


Figura 5.15. *Topología parcialmente mallada presente en las grandes redes*

Es importante destacar que cada *router* elige, en función de su tabla de enrutamiento, la ruta por la que debe enviar un datagrama, envía el datagrama al *router* correspondiente y se olvida de dicho datagrama. Es decir, un *router* simplemente encamina los datagramas al siguiente *router*, pero no lleva a cabo ninguna comprobación ni seguimiento de que la ruta sea la adecuada. Esta característica permite a los *routers* minimizar las operaciones de enrutamiento y con ello ganar en rendimiento.

Sin embargo, este procedimiento tiene asociado un inconveniente. Cuando las tablas de enrutamiento no están convenientemente actualizadas y sincronizadas puede ocurrir que un datagrama no consiga alcanzar su destino, quedándose en una especie de bucle de forma indefinida. Para evitar esta situación se utiliza el campo TTL del datagrama IP. Cada paso por un *router* decrementa este campo una unidad. Cuando llega a 0 el paquete es descartado.

RECUERDA

Las funciones principales de un *router* son:
- Unir redes.
- Encaminar los datos.

Otra característica interesante de los *routers* es que no propagan los envíos de difusión, por lo que se dice que cada red a la que está conectado un *router* forma un dominio de difusión.

El enrutamiento de los paquetes en un *router* se basa en la información de la tabla de enrutamiento. Dicha información puede ser de dos tipos:

- **Rutas estáticas**: son las reglas de enrutamiento configuradas manualmente por los administradores de la red.
- **Rutas dinámicas**: son las reglas de enrutamiento proporcionadas por los algoritmos de enrutamiento. Estos algoritmos se basan en el envío de la información de enrutamiento entre los *routers* de forma periódica, por ello se llaman rutas dinámicas. La compleja estructura actual de Internet se mantiene en gran parte gracias a las rutas dinámicas.

La tabla de enrutamiento está formada al menos por los campos:

- **Identificador de red**, donde se almacena la dirección IP de la red de destino.
- **Siguiente salto**, este campo contiene la dirección del próximo *router* al que tiene que dirigirse el paquete para alcanzar una red de destino dada.
- **Interfaz**, en este campo se especifica la interfaz de red hacia donde se tiene que enviar el paquete.
- **Coste**, contiene un valor que pretende cuantificar en función de algún criterio el coste que supone alcanzar dicha red. Un valor bajo indicará una ruta rápida y un valor alto indicará una ruta lenta.

La tabla de enrutamiento inicial solo incluye información de las redes a las que el *router* está conectado. Posteriormente se irá recibiendo información de los *routers* adyacentes (también llamados "vecinos") y se irá completando dicha tabla de enrutamiento. Existen dos tipos de algoritmos de enrutamiento:

- **Enrutamiento basado en el vector distancia**. En este tipo de enrutamiento se asume el coste de una unidad por cada enlace. Por tanto, el coste de una ruta determinada es la suma de los costes de cada enlace. En este caso la ruta óptima se considera a aquella que necesita menos retransmisiones o saltos. La eficiencia de la transmisión, por tanto, es función solo del número de enlaces requeridos para alcanzar el destino.
- **Enrutamiento basado en el estado del enlace**. En este caso, el coste no se refiere al número de saltos hasta la red de destino, sino que es un valor con peso basado en una variedad de factores como el tráfico, estado del enlace... Por tanto, el coste asociado a una ruta representa una valoración de la eficacia de la misma.

El enrutamiento basado en el vector distancia es más sencillo de implementar y más rápido, pero el coste no refleja a veces las situaciones de tráfico reales. Esta situación está mejor reflejada en el enrutamiento basado en el estado del enlace, pero por el contrario es más complejo de implementar.

5.3.1 PROTOCOLOS DE ENRUTAMIENTO

A efectos de enrutamiento de información se define un **sistema autónomo** como una colección de redes que están bajo el control administrativo de una única organización y que comparten una misma estrategia de enrutamiento. Ejemplos de sistemas autónomos: redes de empresas, proveedores de servicio, organismos oficiales, universidades. En función de donde se lleve a cabo el enrutamiento existen dos tipos de protocolos de enrutamiento:

- **Protocolos de pasarela interior**: protocolos de enrutamiento que operan dentro de un sistema autónomo. Los principales protocolos de pasarela interior son:
  - **RIP** (*Routing Information Protocol*), tipo vector distancia y de los primeros utilizados. Muy extendido. Para solucionar algunas limitaciones de RIP se implementó RIP2.
  - **IGRP** (*Interior Gateway Routing Protocol*), tipo vector distancia, más robusto que RIP. Desarrollado por CISCO y por tanto es propietario.
  - **EIGRP**, mejora de IGRP, se considera un protocolo híbrido.
  - **OSPF** (*Open Shortest Path First*), estándar abierto basado en el estado del enlace.

- **Protocolos de pasarela exterior**: se ejecutan en los *routers* situados en los extremos de los sistemas autónomos y que intercambian información con otros sistemas autónomos. Los protocolos de pasarela interior más comunes son:
  - **BGP** (*Border Gateway Protocol*). Estándar actual (de facto). Hace posible el crecimiento y la propia existencia de Internet. Soporta el direccionamiento CIDR, lo que hace posible un uso más eficiente de las tablas de enrutamiento. Actualmente se utiliza la versión 4.
  - **EGP** (*Exterior Gateway Protocol*). Antiguo protocolo de pasarela exterior que ha sido sustituido por BGP. En extinción.

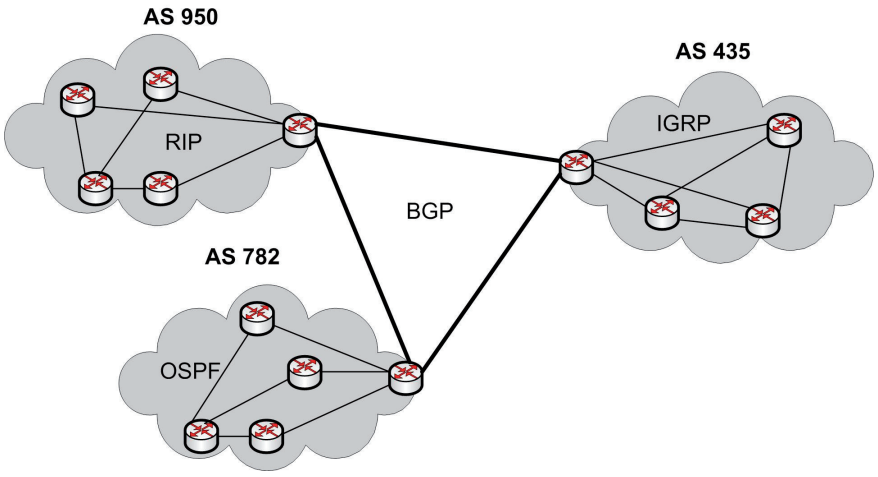


Figura 5.16. *Conexión de sistemas autónomos*

5.4 PROTOCOLOS DE TRANSPORTE: TCP Y UDP

El nivel de transporte está implementado en la arquitectura TCP/IP por dos protocolos, TCP y UDP. El protocolo TCP lleva a cabo las principales funciones del nivel de transporte del modelo OSI que se vieron en el capítulo 1, es decir, proporciona la entrega fiable de mensajes completos desde un origen a un destino. UDP es un protocolo más sencillo que proporciona la entrega de mensaje de origen a destino, pero no ofrece la fiabilidad de TCP, por lo que cuando se usa UDP deben ser los protocolos del nivel de aplicación los que se encarguen del control de errores.

Una de las funciones importantes implementadas en el nivel de transporte es la definición de **los puertos del protocolo**, llamados simplemente **puertos**, que ofrecen un mecanismo para identificar la comunicación de un proceso individual dentro de un *host*. En la arquitectura TCP/IP los puertos son números de 16 bits, es decir, el rango de puertos válidos es de 0 a 65.535.

5.4.1 PROTOCOLO UDP

El protocolo **UDP** (*User Datagram Protocol*, protocolo de datagramas de usuario) es un protocolo del nivel de transporte en la arquitectura TCP/IP no orientado a conexión, que proporciona las funciones básicas necesarias para la entrega de datos de un origen a un destino. No se lleva a cabo control de flujo ni de errores, además UDP no proporciona funciones de secuenciamiento ni de reordenación de paquetes. No puede especificar el paquete dañado cuando se produce un error ni detecta paquetes perdidos.

Como se puede ver, las funciones de UDP son muy limitadas. Realmente, la principal función de UDP es proporcionar el direccionamiento de los puntos de acceso a los diferentes protocolos del nivel de aplicación, es decir, los puertos. Por tanto, los protocolos del nivel de aplicación que utilicen UDP deben implementar mecanismos de control de flujo y de errores para llevar a cabo una comunicación fiable.

El formato del paquete UDP es el siguiente:

Figura 5.17. *Formato del paquete UDP*

- **Dirección del puerto origen**. Identificador del puerto del proceso origen.
- **Dirección del puerto destino**. Identificador del puerto del proceso destino.
- **Longitud total**. Es el tamaño en bytes del datagrama UDP incluida la cabecera.
- **Checksum**. Suma de comprobación utilizada para la detección de errores.

5.4.2 PROTOCOLO TCP

El protocolo **TCP** (*Transmission Control Protocol*, protocolo de control de transmisión) proporciona todas las funciones de un protocolo de nivel de transporte, es decir, es un protocolo orientado a conexión que permite la comunicación fiable de datos de un origen a un destino. Implementa funciones de control de flujo y control de errores.

Las unidades de datos en el protocolo TCP se conocen como segmentos. La estructura de un segmento TCP es la siguiente:

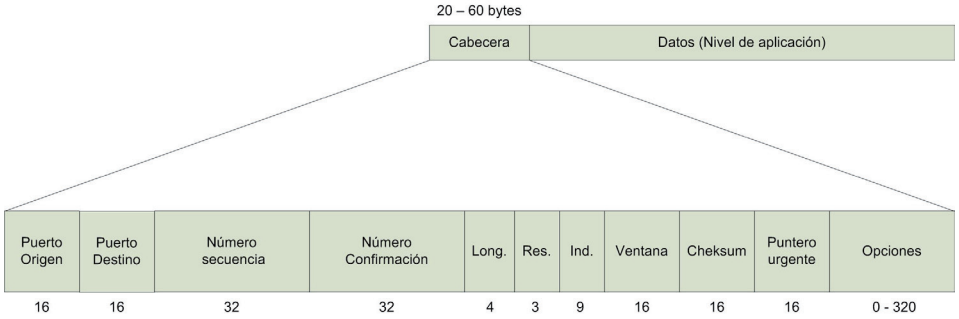


Figura 5.18. *Formato del paquete TCP*

- **Puerto origen**. Dirección del puerto en el proceso origen.
- **Puerto destino**. Dirección del puerto en el proceso destino.
- **Número de secuencia**. Cada uno de los segmentos en los que se dividen los datos en una comunicación por medio de TCP se numera. En este campo se envía el número asignado a cada paquete TCP.
- **Número confirmación**. Si el indicador ACK está activo, este campo confirma la recepción correcta y sin errores de todos los segmentos con un número de secuencia menor o igual al indicado en este campo y que estuvieran pendientes de confirmación.
- **Longitud**. Este campo contiene el tamaño de la cabecera del segmento TCP expresado en grupos de 4 bytes, es decir, para un valor de 5 en este campo, la longitud de la cabecera sería 20 bytes.
- **Reservado**. Campo reservado de 3 bits.
- **Indicadores**. Este campo contiene los siguientes *flags* o indicadores:
  - **NS** (*Nonce Sum*). Indicador utilizado para llevar a cabo funciones de control de la congestión.
  - **CWR** (*Congestion Window Reduced*). Indicador utilizado para llevar a cabo funciones de control de la congestión.
  - **ECE** (*ECN-Echo*). Indicador que se activa para indicar la existencia de información sobre congestión en el campo ECN del datagrama IP.
  - **URG**, indica que hay datos urgentes. El campo *Puntero urgente* indica la cantidad de datos urgentes en el segmento.
  - **ACK**, bit utilizado para validar segmentos recibidos.
  - **PSH**, indica al receptor que entregue al nivel superior todos los datos que tenga disponibles en el *buffer* de recepción.
  - **RST**, indica que se necesita reiniciar la comunicación.
  - **SYN**, bit utilizado para sincronizar los números de secuencia.
  - **FIN**, bit utilizado para indicar el fin de la comunicación.
- **Tamaño de ventana**. Parámetro que tiene relación con la función del control de flujo. Se utiliza una técnica conocida como *ventana deslizante* y este campo indica el tamaño de dicha ventana. El tamaño de la ventana está relacionado con el número de paquetes consecutivos que pueden enviarse sin recibir una confirmación de que han llegado. Dicho tamaño depende de las condiciones de transmisión. Si las condiciones de transmisión son buenas, se puede aumentar el tamaño de la ventana, y si son malas se debe disminuir.
- **Checksum**. Campo utilizado para la comprobación de errores en la información tanto de la cabecera como de los datos del paquete TCP.
- **Puntero urgente**. Este campo contiene un puntero al final de los datos urgentes, por lo que, a partir de la posición indicada en este campo, comienzan los datos con prioridad normal.
- **Opciones**. Es un campo opcional utilizado para enviar diferentes tipos de información adicional. Su longitud es variable se obtiene del campo *Longitud* de la propia cabecera TCP.

Uno de los usos del campo *Opciones* es el envío de un parámetro llamado **MSS** (*Maximun Segment Size*, tamaño máximo del segmento). Este parámetro se utiliza para definir cuál es el tamaño del segmento más grande que se puede enviar. Lo más óptimo es que este tamaño sea el adecuado para evitar la fragmentación de datagramas IP. Se suele enviar en el proceso de establecimiento de la conexión TCP.

Como hemos visto, TCP es un protocolo orientado a conexión y por lo tanto implementa mecanismos para establecer y finalizar conexiones. Además, para llevar a cabo el control de flujo de los datos se emplea la técnica de ventana deslizante.

El procedimiento para establecer una conexión se lleva a cabo en tres pasos. El origen de la conexión (normalmente un cliente de un servicio de red) envía un segmento TCP con un número de secuencia inicial N y el indicador SYN activo. El destinatario de la conexión (normalmente un servidor de un servicio de red) responde enviando un segmento TCP con otro número de secuencia M, el indicador SYN activo y el ACK activo con un número de confirmación N+1. En el último paso, el origen de la conexión envía otro segmento TCP con el número de secuencia N+1 y con el indicador de ACK activo y el número de confirmación M+1. La siguiente figura resume el proceso de establecimiento de una conexión TCP.

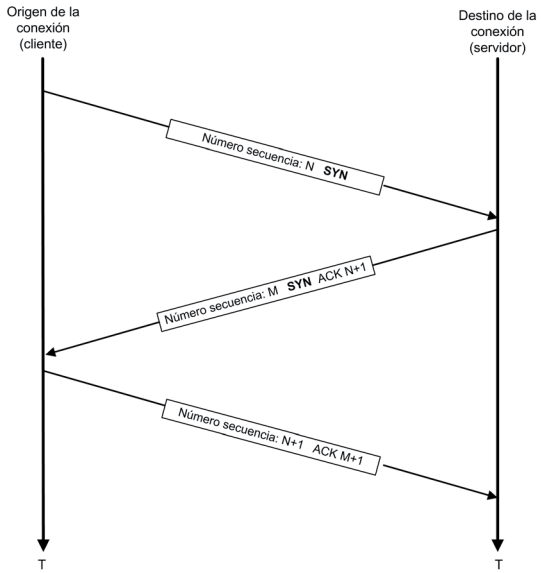


Figura 5.19. *Establecimiento de una conexión TCP*

Para finalizar una conexión TCP se establece un mecanismo de cuatro pasos. El proceso que desea finalizar la conexión envía un segmento TCP con el indicador FIN activo y un número de secuencia inicial N. El proceso en el otro extremo de la conexión envía entonces un segmento TCP con un número de secuencia inicial M y el indicador ACK activo, con el número de confirmación N+1. A continuación, este último proceso envía otro segmento TCP, esta vez con

el indicador FIN activo y número de secuencia M+1. El primer proceso, cuando recibe los segmentos anteriores, genera un segmento TCP con número de secuencia N+1 y el indicador ACK activo con el número de confirmación M+2. En la siguiente figura se puede ver un ejemplo de finalización:

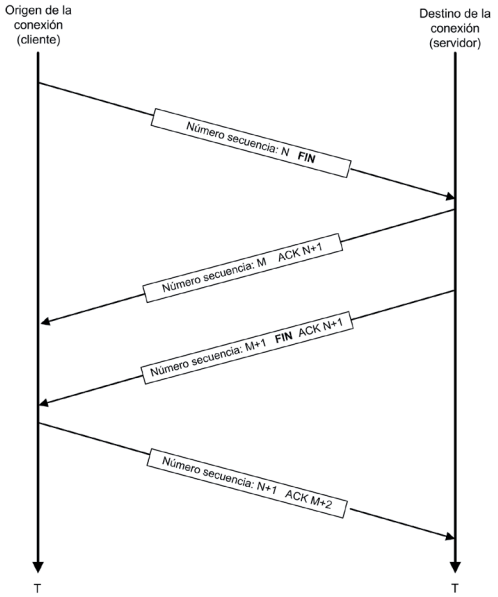


Figura 5.20. *Finalización de una conexión TCP*

Las conexiones TCP pueden encontrarse en varios estados que definen su comportamiento inmediato. Estos estados se muestran en la siguiente tabla:

Estado	Descripción
CLOSED	No hay conexión.
LISTEN	Un proceso servidor espera las peticiones de procesos clientes.
SYN-SENT	Se ha enviado una petición de conexión. En espera del reconocimiento.
SYN-RCVD	Se ha recibido una petición de conexión.
ESTABLISHED	Conexión establecida.
FIN-WAIT-1	Se ha solicitado el cierre de la conexión.
FIN-WAIT-2	El equipo remoto ha aceptado el cierre de la conexión.
TIME-WAIT	Esperando la retransmisión de segmentos.
CLOSE-WAIT	Un proceso servidor espera el cierre del proceso cliente.
LAST-ACK	El proceso servidor espera el último reconocimiento.

5.5 SEGURIDAD EN REDES

5.5.1 CRIPTOGRAFÍA

La criptografía es el estudio de técnicas y mecanismos para transformar un mensaje inteligible en un mensaje no inteligible y su posterior transformación en el mensaje inteligible original. El proceso de transformación del mensaje inteligible a no inteligible se conoce como **cifrado**. Al mensaje transformado en no inteligible se le conoce como **mensaje cifrado**.

Para llevar a cabo el cifrado de un mensaje se utilizan dos elementos:

- **Clave**: información conocida solo por el emisor y el receptor y utilizada en el proceso de cifrado.
- **Algoritmo de cifrado**: mecanismo que convierte el mensaje sin cifrar en mensaje cifrado.

La criptografía además proporciona una segunda funcionalidad que es la **autenticación**, es decir, la comprobación de la identidad del emisor del mensaje. Existen dos tipos de criptografías:

- **Criptografía simétrica**, también conocida como *criptografía de clave privada*. Las dos partes de la comunicación acuerdan y comparten una clave secreta única. Los datos se encriptan y desencriptan utilizando la misma clave y el mismo algoritmo.

  Para garantizar la seguridad de los datos transmitidos, debe protegerse la clave y solo debe ser conocida por aquellos que participan de la comunicación.

  Este sistema de cifrado es rápido y eficaz, hablando en términos computacionales. Actualmente existen diversos algoritmos muy robustos y potentes para llevarlo a cabo. Las claves utilizadas no son muy largas, aunque el grado de protección de la información es directamente proporcional a la longitud de la clave secreta.

  El mayor inconveniente de este sistema se presenta en la distribución de la clave entre las partes a comunicarse. La distribución de la clave debe ser por medios seguros, ya que de otra forma podría ser interceptada y verse comprometida la privacidad de las transmisiones.

  Actualmente, los algoritmos de clave privada más usados son DES, 3DES, AES, RC4, RC2.

- **Criptografía asimétrica**, también conocida como *criptografía de clave pública*. En este caso se utilizan dos claves, llamadas **clave pública** y **clave privada**. La base de la criptografía asimétrica es que la información que se cifra usando una de las claves solo se puede descifrar usando la otra. Lo normal es que se utilice la clave pública para cifrar y la clave privada para descifrar.

  En un proceso de comunicación cifrada, el receptor debe generar el par de claves pública/privada. La clave pública puede ser distribuida a todos los posibles remitentes de información, sin embargo la clave privada nunca debe ser facilitada (tampoco es necesario). Cuando un dispositivo quiera enviar información al receptor, utilizará la clave pública para cifrar dicha información, la cual solo podrá descifrarse utilizando la clave privada que solo conoce el receptor.

Por tanto, la clave pública puede ser distribuida libremente, pero la clave privada no es necesario distribuirla y solo el receptor necesita conocerla. Ésta es la principal ventaja de este tipo de cifrado, ya que proporciona un alto nivel de seguridad.

La principal desventaja es que el proceso de encriptación es bastante más lento que en el caso de la criptografía simétrica. Por ello, en algunos casos se utiliza la criptografía asimétrica solo para transmitir una clave secreta que luego se utilizará para cifrar los datos con criptografía simétrica.

Las claves en el caso de la criptografía asimétrica son más largas que en la criptografía simétrica.

Los algoritmos de criptografía asimétrica más utilizados son RSA, PGP y Diffie-Hellman.

RECUERDA

En la criptografía asimétrica o de clave pública:
- Se utilizan siempre dos claves, una pública y otra privada.
- Solo el dispositivo que conozca la clave privada podrá descifrar la información cifrada con la clave pública.
- La clave pública se puede distribuir sin problema, la clave privada nunca.

La criptografía se utiliza en varios protocolos y tecnologías de las redes de datos. Se puede encontrar en las redes Wi-Fi, en la tecnología VPN para crear túneles, en los protocolos SSL/TLS (usado por ejemplo en HTTPS) o en IPsec.

5.5.2 AUTENTICACIÓN

Como ya se ha mencionado en el apartado anterior, la **autenticación** es la comprobación de la identidad del emisor del mensaje y la integridad de los datos del mismo. Los principales métodos de autenticación, como son las firmas digitales y los certificados digitales, se basan en la utilización de la criptografía asimétrica.

Firmas digitales

En las firmas digitales, el emisor de un mensaje firma el mismo cifrando la información con su clave privada y esa "firma" es única, ya que solo él dispone de dicha clave privada. El receptor puede verificar esa firma utilizando la clave pública correspondiente emitida por el emisor del mensaje. Con este proceso se proporciona autenticación para el mensaje enviado, pero no seguridad mediante cifrado porque cualquiera puede disponer de la clave pública correspondiente y recuperar el mensaje original.

Certificados

Un certificado es un documento digital que acredita que la clave pública que contiene es de quien dice ser. Para avalar tal afirmación, este documento es respaldado por una **autoridad de certificación** (**CA**, *Certification Authority*) mediante su firma digital.

Las entidades de certificación son organismos seguros e independientes que emiten certificados de autenticidad de claves públicas.

Un certificado consta de la clave pública que certifica, el nombre del propietario, un período de validez, el nombre de la autoridad de certificación y un número de serie. Este certificado viene firmado digitalmente por el emisor.

Los navegadores web contienen una lista de las principales entidades de certificación, por lo que si establecemos una comunicación segura con alguna entidad (banco, comercio electrónico) que haya certificado su clave pública con alguna de éstas, la comunicación se realizará de forma segura y transparente al usuario. Si la entidad de certificación no está reconocida por el navegador web, es el usuario el que debe aceptar o no la comunicación.

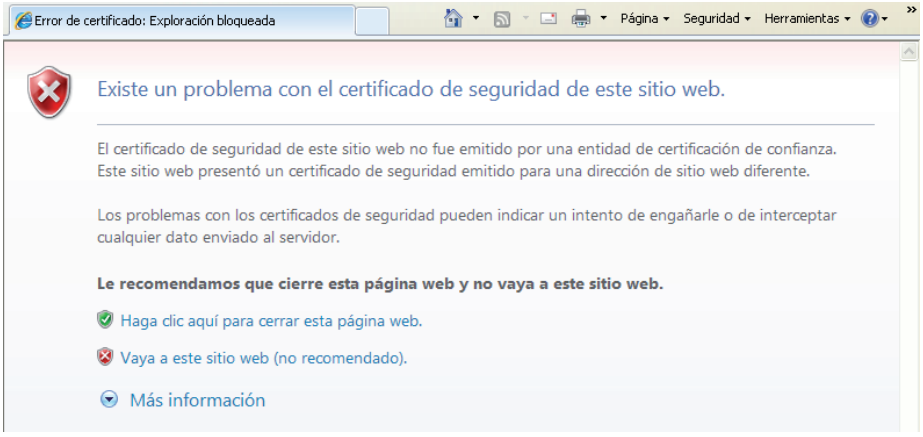


Figura 5.21. *Mensaje de advertencia de un navegador web ante una entidad de certificación no reconocida*

5.5.3 IPSEC

El término **IPsec** se refiere al conjunto de protocolos implementados para proporcionar seguridad a las comunicaciones a través de redes IP. Inicialmente IPsec fue diseñado para IPv6, pero debido a las fuertes necesidades de seguridad actuales se ha adaptado para poder utilizarlo sobre IPv4.

IPsec proporciona servicios de seguridad, incluyendo control de acceso, integridad en las comunicaciones sin conexión, autenticación del origen de los datos, protección contra ataques de repetición, confidencialidad mediante encriptado… Estos servicios son proporcionados en el nivel IP (nivel 3) y ofrece protección para éste y los niveles superiores.

Para ofrecer tales servicios, IPsec utiliza dos protocolos de seguridad, **AH (*Authentication Header*)** y **ESP (*Encapsulating Security Payload*)**, además del uso de protocolos y procedimientos de administración de claves criptográficas. El protocolo de administración automática de claves por defecto es **IKE (*Internet Key Exchange*)**. IKE es usado para establecer una política de seguridad compartida y claves autenticadas para servicios que los requieran (como IPsec). Antes del envío de tráfico IPsec, cada *router/firewall/host* debe ser capaz de verificar la identidad de su par.

Los mecanismos utilizados por IPsec están diseñados para ser independientes de los algoritmos empleados. Esta modularidad permite la selección de diferentes conjuntos de algoritmos sin afectar al resto del sistema.

El protocolo AH proporciona autenticación, integridad y antirreproducción para todo el paquete. AH firma el paquete entero pero no cifra la información, por lo que no proporciona confidencialidad. La información es legible, pero está protegida contra modificaciones. Utiliza algoritmos *hash* con claves que se denominan **HMAC (códigos hash de autenticación de mensajes)**, para firmar el paquete.

El protocolo ESP proporciona confidencialidad (además de autenticación, integridad y antirreproducción) para los datos de un datagrama IP. No firma, normalmente, el paquete entero (a no ser que se esté realizando un túnel), ya que solo protege la información, y no el encabezado *IP*. Puede utilizarse por sí solo o en combinación con *AH*.

Existen dos modos de utilización de IPsec:

- **Modo túnel**, se utiliza para comunicaciones red a red, red a *host* o *host* a *host* a través de Internet. El encabezado IP interno (encapsulado) es encriptado ocultando la identidad del destinatario y el origen del tráfico.
- **Modo transporte**, utilizado para comunicaciones de extremo a extremo, es decir, de *host* a *host*. Solo se cifran los datos. La cabecera no va encriptada pero sí puede ir firmada, por lo que no se puede modificar.

Todo el proceso de encapsulación, encaminamiento y desencapsulación se denomina túnel.

5.5.4 CORTAFUEGOS (*FIREWALL*)

El concepto de ***firewall*** o **cortafuegos** apareció en el ámbito de las redes de datos para describir los diferentes mecanismos de seguridad destinados a bloquear la transferencia de datos que no cumplan unos criterios de seguridad determinados. Está considerado en la actualidad como un mecanismo de seguridad necesario pero no suficiente para proteger las redes y los equipos conectados a las mismas. Se puede aplicar en dos ámbitos:

- ***Firewall* de red**. Este ámbito se aplica a dispositivos de interconexión, es decir, *routers*. Un *firewall* de red proporciona los mecanismos de control en los datos intercambiados entre las redes a las que se conecta el *router* o cualquier dispositivo que haga funciones de enrutamiento.

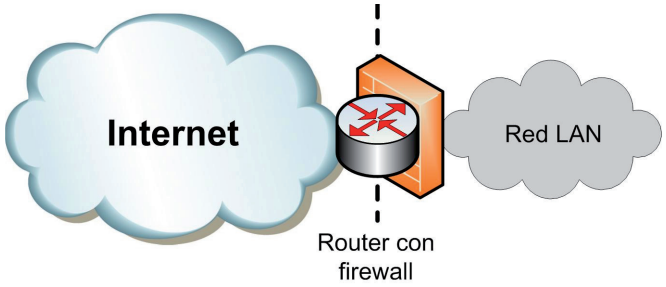


Figura 5.22. *Firewall de red implementado en un router*

- ***Firewall* de equipo**. Este ámbito está referido a la función de *firewall* implementada en un ordenador y que tiene como finalidad aplicar los mecanismos de control en los datos intercambiados entre el equipo y la red.

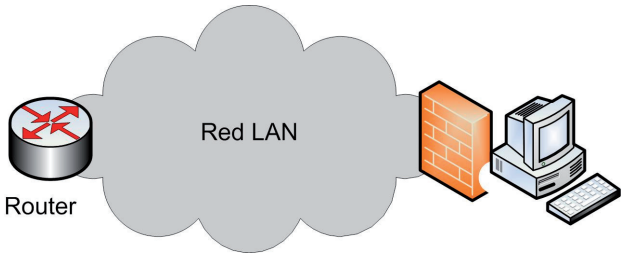


Figura 5.23. *Firewall de equipo*

Las funciones básicas de un *firewall* consisten en inspeccionar todo el tráfico intercambiado entre dos entidades (entre dos redes o entre un equipo y una red) y comprobar que cumplen ciertas reglas de seguridad permitiendo o denegando dicho tráfico en función de que se cumplan o no dichas reglas. El tipo más habitual de reglas se basa en el criterio de selección de puertos. De esta manera se establecen una serie de reglas para permitir el paso de datos dirigidos a una serie de puertos determinados, denegando el acceso al resto de los puertos.

A este proceso de inspección de paquetes intercambiados entre dos entidades para permitir o denegar el propio intercambio se le denomina generalmente **filtrado**.

5.6 CONFIGURACIÓN DE PARÁMETROS DE RED

En los próximos apartados se mostrarán los mecanismos de configuración de los parámetros de red en los principales sistemas operativos utilizados en la actualidad como son Windows XP, Windows 7 y Ubuntu.

Los elementos de configuración relacionados con TCP/IP que se tendrán que configurar son los siguientes:

- **Dirección IP**. Dirección IP asignada al equipo.
- **Máscara de subred**. Máscara de subred asignada al equipo.
- **Puerta de enlace**. Este parámetro se utiliza para indicar la dirección IP del *router* donde el equipo deberá dirigir los datagramas que deban enviarse fuera de la red (por ejemplo, a Internet).
- **Servidores DNS**. Este parámetro se utiliza para indicar las direcciones IP de los servidores DNS que se encargan de proporcionar las direcciones IP a partir de los nombres de dominio utilizados en la mayor parte de los servicios de Internet. En el apartado correspondiente se explica con más detalle.

Actualmente existen dos métodos para establecer los parámetros de red en un equipo:

- **Configuración manual**. Si se utiliza esta opción, el usuario del equipo o un técnico de administración debe especificar manualmente el valor de dichos parámetros. Esto requiere tener conocimientos sobre el direccionamiento utilizado en la red local para saber qué dirección IP se puede utilizar, si existen subredes en

dicha red para establecer el valor adecuado de máscara de subred y cuál es la puerta de enlace del *router* de la red.

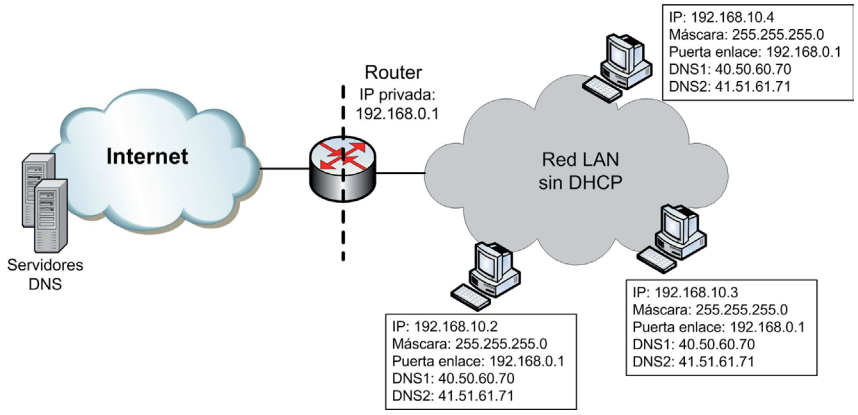


Figura 5.24. *Configuración manual de los parámetros de red*

- **Configuración automática**. Este método es el que está configurado por defecto en la mayor parte de los equipos. En este caso no es necesario configurar ningún parámetro de red en el equipo, ya que se utiliza un procedimiento para obtener los parámetros de red de forma automática. Para ello se utiliza un protocolo llamado DHCP y es imprescindible que en la red exista lo que se conoce como un servidor DHCP que sea el que proporciona al resto de equipos los parámetros de configuración adecuados.

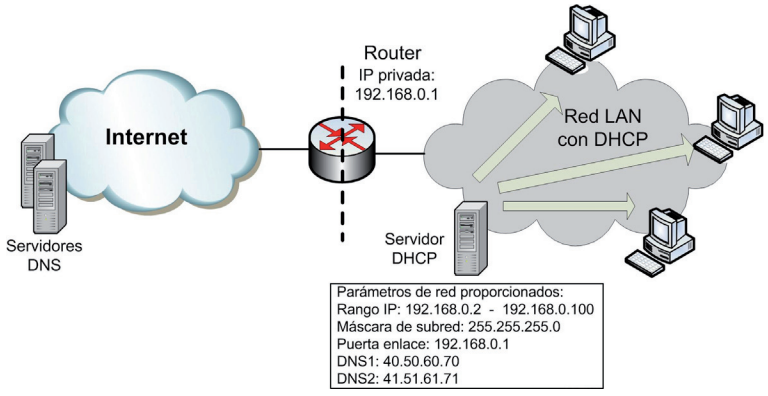


Figura 5.25. *Configuración automática proporcionada por un servidor DHCP*

Actualmente el uso de servidores DHCP está muy extendido. La mayoría de los ISP utilizan un servidor DHCP para asignar las direcciones públicas a sus clientes. Y la mayor parte de los *routers* actuales también implementan un servidor DHCP para la asignación de direcciones privadas en una red de área local. Los sistemas operativos de tipo servidor como Windows 2003/2008 Server o Linux incluyen también servidores DHCP. También es habitual que los puntos de acceso inalámbrico incluyan el servicio DHCP.

5.6.1 ASIGNACIÓN AUTOMÁTICA DE PARÁMETROS IP: SERVICIO DHCP

DHCP (*Dynamic Host Configuration Protocol*, protocolo de configuración dinámica de estación) es un protocolo cliente-servidor utilizado en redes TCP/IP para proporcionar la configuración de los parámetros de red a un equipo, es decir, una dirección IP, una máscara de red, la dirección IP de la puerta de enlace y la dirección IP de un servidor DNS.

Para utilizar este servicio debe existir un equipo que funcione como servidor DHCP y en el que se configuran los parámetros de red que se proporcionarán a todos los equipos que lo soliciten, que se consideran clientes del servicio.

DHCP utiliza el protocolo UDP en el nivel de transporte. El servidor lleva a cabo sus comunicaciones por el puerto 67 y los clientes utilizan el puerto 68. Para solicitar una configuración de red a un servidor DHCP se envía una solicitud utilizando la dirección IP de *broadcast* genérica 255.255.255.255 o la dirección de *broadcast* de la subred.

La asignación de los parámetros de red es dinámica. Esto implica que las asignaciones son temporales, es decir, se asigna un tiempo de validez y transcurrido el mismo se deben renegociar los parámetros de red.

RECUERDA

En la mayor parte de las ocasiones no se utiliza un equipo exclusivamente como servidor DCHP. En redes profesionales suele ser un equipo que proporciona servicios de red entre los que se encuentra el servicio DHCP. En pequeñas redes se suele utilizar el servidor DHCP incluido en la mayor parte de los *routers* proporcionados por el proveedor de conexión a Internet. La mayor parte de los puntos de acceso inalámbricos también implementan un servidor DHCP.

5.6.2 OBTENCIÓN DE DIRECCIONES IP DE DOMINIOS: SERVICIO DNS

DNS (*Domain Name System*, sistema de nombres de dominio) es el protocolo utilizado para poder asociar a una dirección IP un nombre. DNS utiliza el modelo cliente-servidor. Dichos nombres, conocidos como **nombres de dominio**, se almacenan, junto con sus direcciones IP, en una base de datos jerárquica y distribuida.

La asignación de un nombre de dominio es el método utilizado para asociar un nombre a un recurso dentro de Internet. Un nombre de dominio está formado por una sucesión de nombres (dominios) separados por puntos y siguiendo una determinada jerarquía. El dominio de nivel superior (también conocido como **TLD** (*Top Level Domain*) es el que aparece en última posición. Por ejemplo, para el nombre **www.redestelematicas.es**, el domino de nivel superior es 'es'.

Los dominios de nivel superior más frecuentes son 'com', 'org', 'edu', 'net' o los nombres de dominios asignados por países, como 'es' para España, 'ar' para Argentina, 'br' para Brasil, 'de' para Alemania, 'nl' para Holanda…

Muchos servicios del nivel de aplicación utilizan nombres para referirse a equipos, sin embargo, para llevar a cabo una comunicación con ese equipo es necesario conocer su dirección IP. Para ello se genera una petición DNS que se envía a un servidor DNS. La información que se mantiene en el sistema DNS es distribuida, y si dicho servidor no es capaz de resolver la petición, puede redirigirla a otro servidor. Los servidores que gestionan los dominios de nivel superior o TLD se conocen como **root servers**, que se pueden considerar como los nodos primarios del sistema DNS.

El envío de la información DNS, tanto de las peticiones como de las respuestas, se lleva a través del puerto 53 y se utiliza tanto UDP como TCP.

5.6.3 CONFIGURACIÓN DE PARÁMETROS IP EN WINDOWS

Para el caso de la configuración de un equipo en red que utilice Windows como sistema operativo vamos a presentar dos posibilidades: Windows XP y Windows 7.

El acceso a la configuración de los parámetros de red en Windows XP se puede hacer desde diferentes opciones. Por ejemplo, accediendo al **Panel de Control** de Windows y seleccionando la opción **Conexiones de red**. En esta ventana aparecerán todas las interfaces de red existentes en el equipo. Cada una de ellas tendrá su propia configuración de red. Para acceder a la configuración de red se selecciona la opción **Propiedades** del menú contextual.

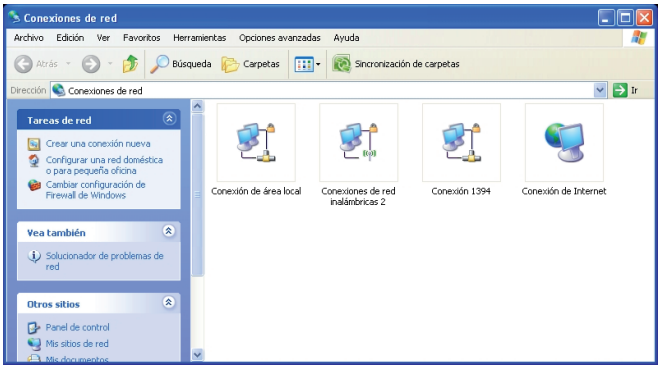


Figura 5.26. *Ventana de Conexiones de red en Windows XP*

En la ventana de propiedades aparece una lista de protocolos y servicios de red asociados a esa interfaz y uno de ellos será **Protocolo Internet (TCP/IP)**. Hay que seleccionar esa opción haciendo doble clic o pulsando el botón **Propiedades**.

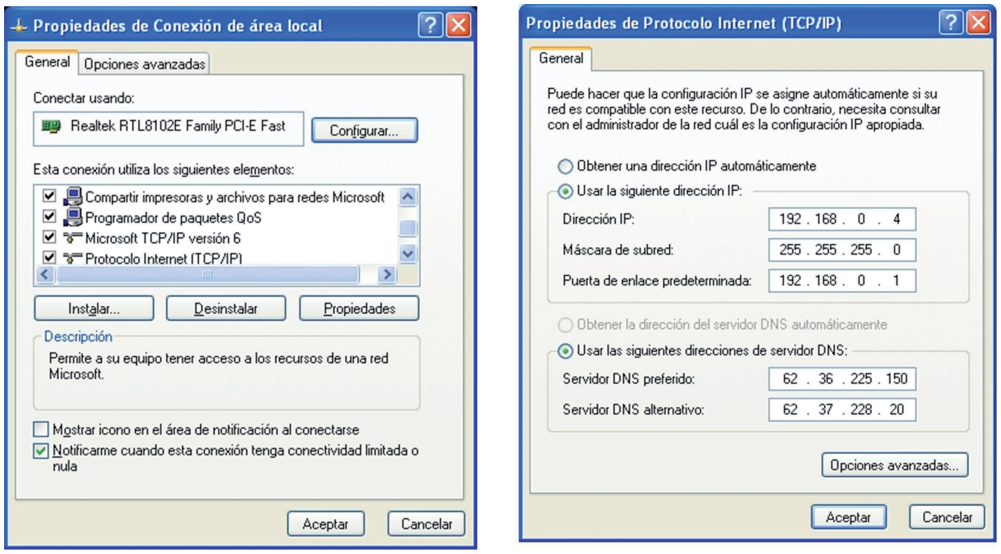


Figura 5.27. *Ventanas de configuración de red en Windows XP*

En la ventana de configuración de la figura se puede seleccionar la opción **Obtener una dirección IP automáticamente** y **Obtener la dirección del servidor DNS automáticamente** para seleccionar el modo automático. O seleccionar las opciones **Usar la siguiente dirección IP** y **Usar las siguientes direcciones de servidor DNS** para seleccionar el modo manual. En este último caso habrá que introducir los valores adecuados en los campos *Dirección IP, Máscara de subred, Puerta de enlace predeterminada, Servidor DNS preferido y Servidor DNS alternativo.*

Puede aparecer una interfaz de red llamada **Conexión 1394**. Esta interfaz de red se utiliza para proporcionar conectividad IP a dispositivos que utilicen el estándar IEEE 1394 (también conocido como **Firewire**). Este estándar se utiliza en dispositivos digitales tales como cámaras de vídeo. La aparición de esta interfaz en la ventana de conexión de red depende de la implementación del *bus* IEEE 1394 en la placa base del equipo.

Utilizando el botón **Opciones avanzadas** se puede configurar más de una dirección IP y más de una puerta de enlace para una determinada interfaz de red.

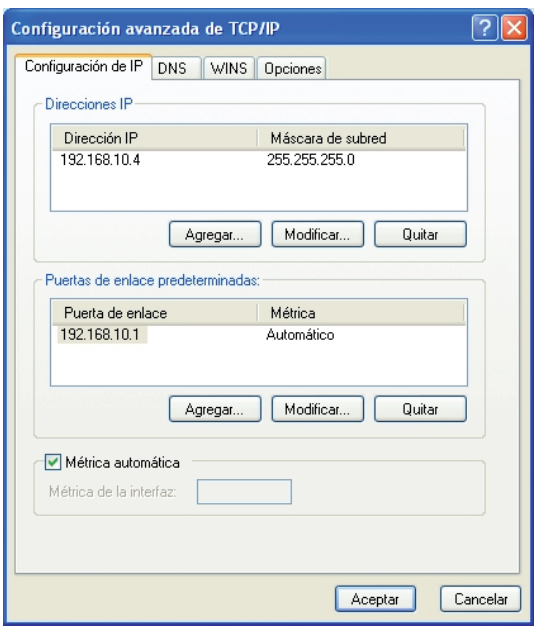


Figura 5.28. *Ventanas de configuración avanzada de la configuración TCP/IP*

La configuración de los parámetros de red en equipos con Windows 7 se lleva a cabo desde la ventana de **Centro de redes y recursos compartidos**, a la que se puede acceder desde el menú de *Propiedades* en la opción de *Red* del menú principal de Windows 7, o bien desde el **Panel de control**, seleccionando la opción **Redes e Internet**.

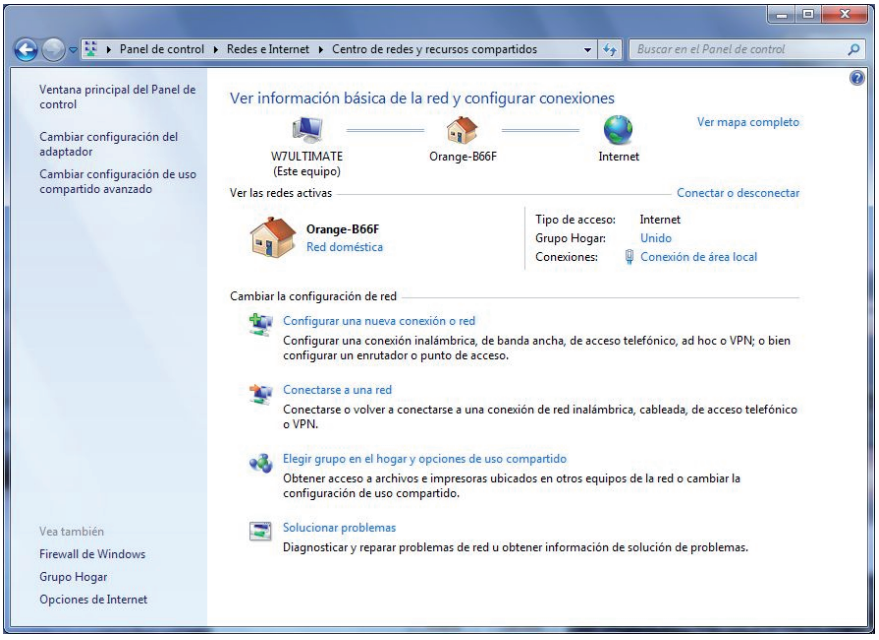


Figura 5.29. *Ventana Centro de redes y recursos compartidos de Windows 7*

Desde aquí se puede seleccionar la opción de **Conexión de área local** y con el botón **Propiedades** se puede acceder a la ventana de configuración de los parámetros de red.

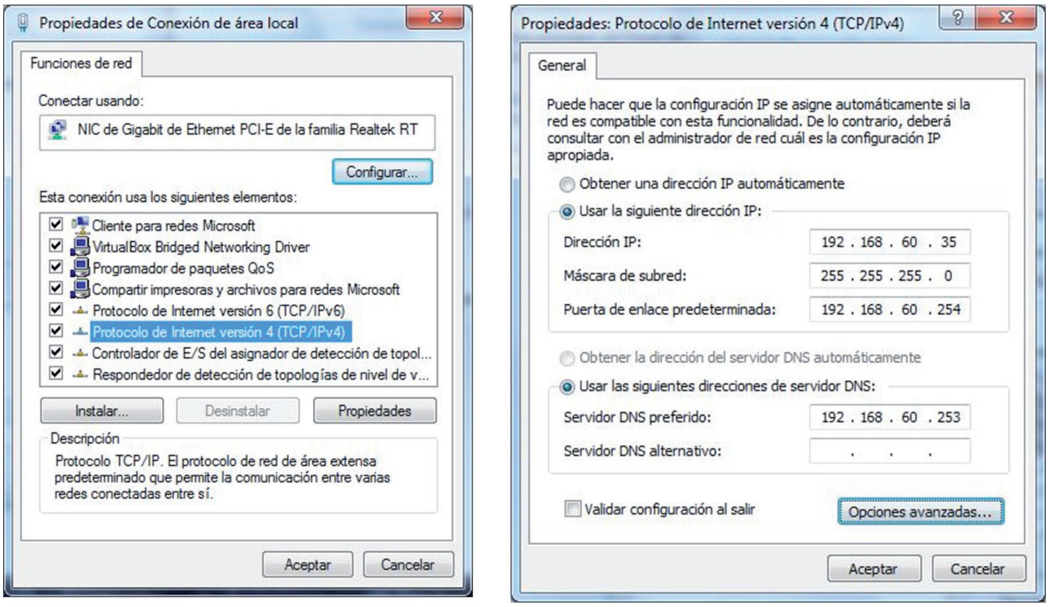


Figura 5.30. *Ventanas para la configuración de red en Windows 7*

RECUERDA

- Para que el modo de configuración automática funcione, debe haber en la red local un servidor DHCP en funcionamiento.
- Los *routers* proporcionados por los proveedores de conexión a Internet incluyen un servidor DHCP integrado en el propio *router* y que suele estar activado por defecto. Por ello, en este tipo de redes funciona por defecto el modo de configuración automática.
- Podemos encontrar servidores DHCP en sistemas Windows 2003/2008 Server, en sistemas servidores bajo Linux, en *routers* y en puntos de acceso inalámbricos.

5.6.4 CONFIGURACIÓN DE PARÁMETROS IP EN UBUNTU

Ubuntu es sin duda una de las distribuciones de Linux más utilizadas en la actualidad. Por ello se utilizará como distribución de referencia. La configuración de red utilizando la versión 11.10 de Ubuntu se puede realizar directamente desde la barra superior, desplegando el icono de red.

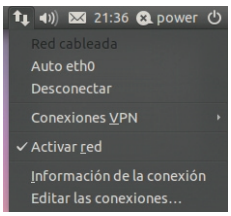


Figura 5.31. *Acceso a la configuración de red desde la barra principal de Ubuntu*

Desde este menú se puede activar o desactivar la red y se puede acceder a los parámetros de configuración desde la opción **Editar conexiones**.

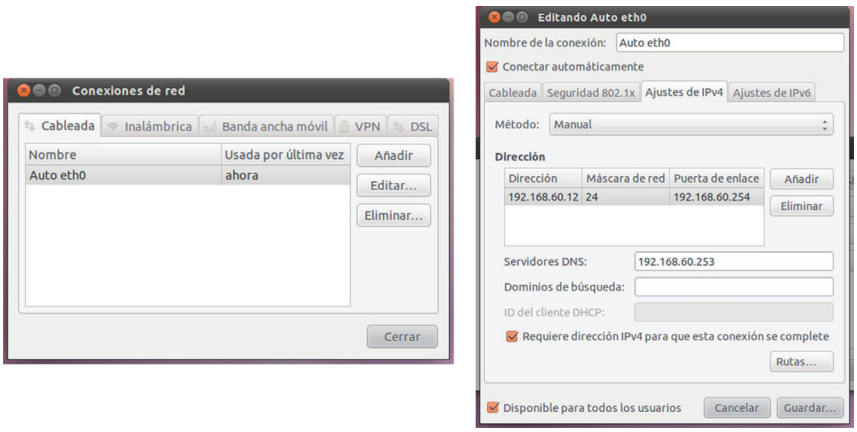


Figura 5.32. *Ventanas de configuración de red en Ubuntu*

Tradicionalmente Linux, y por extensión Ubuntu, ha permitido la configuración de los parámetros de red editando los archivos de configuración correspondientes. Sin embargo, en las últimas versiones de Ubuntu Desktop se aconseja la configuración de red siempre desde el modo gráfico. La versión Ubuntu Server sí mantiene la posibilidad de configurar la red editando directamente los archivos de configuración.

5.6.5 CONFIGURACIÓN DEL *FIREWALL*

En este apartado se tratarán aspectos de configuración de las funciones de *firewall* en equipos con Windows. Para acceder a las funciones del *firewall* en sistemas que utilicen Windows XP se accede al **Panel de Control** y se selecciona la herramienta **Centro de seguridad**.

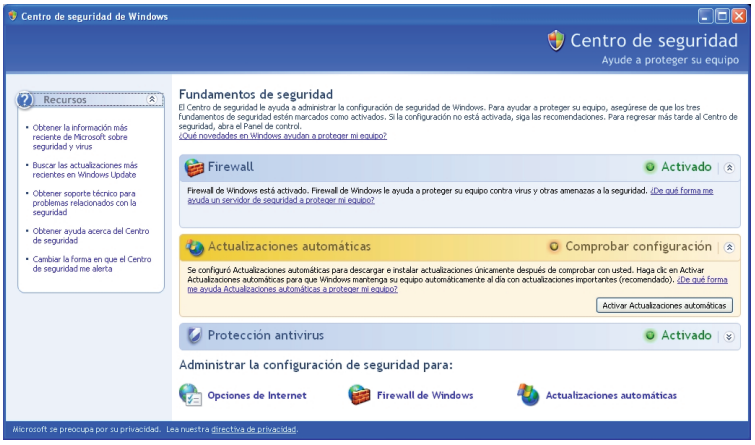


Figura 5.33. *Ventana Centro de seguridad desde donde se puede acceder al firewall de Windows XP*

También es posible acceder al *firewall* desde la ventana de **Conexiones de red** de la figura 5.26. En ambos casos la ventana principal de configuración permite activarlo o desactivarlo, lo cual no está recomendado.

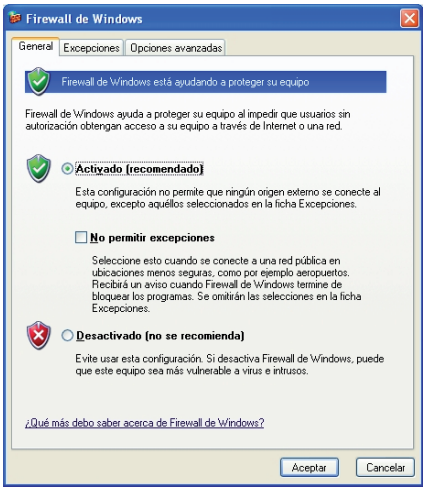


Figura 5.34. *Ventana de configuración del firewall de Windows XP*

Con el *firewall* activo no se permitirá el tráfico entrante de red a ningún puerto, salvo los especificados en la pestaña **Excepciones**.

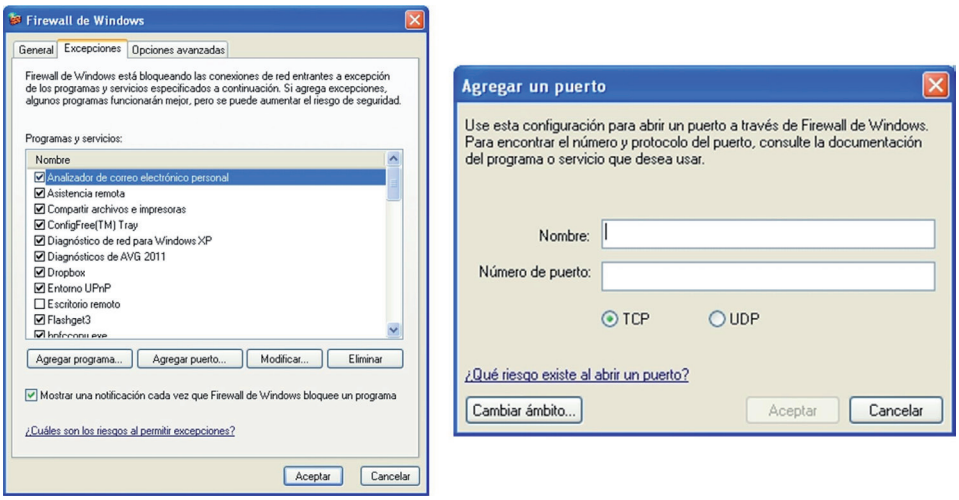


Figura 5.35. *Ventana de excepciones del firewall y para agregar un puerto a las excepciones*

En Windows 7 se puede acceder a las características y configuración del *firewall* desde la ventana de **Centro de redes y recursos compartidos**.

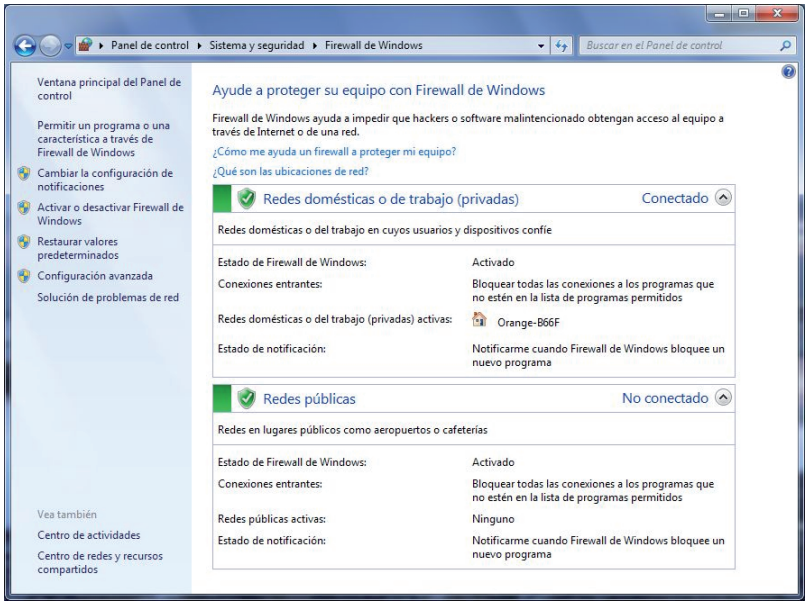


Figura 5.36. *Ventana principal de configuración del firewall de Windows 7*

5.7 PROTOCOLOS DEL NIVEL DE APLICACIÓN

El nivel de aplicación es el nivel más alto del modelo TCP/IP y su funcionalidad está asociada generalmente a cubrir las necesidades del usuario final. La implementación de las funcionalidades del nivel de aplicación se lleva a cabo, como en el resto de niveles, a través de protocolos. La mayor parte de los protocolos del nivel de aplicación en TCP/IP siguen un modelo cliente-servidor. Uno de los extremos de la comunicación será el que solicita datos (cliente) y el otro extremo de la comunicación se encarga de proporcionar dichos datos (servidor).

En este contexto, la funcionalidad aportada por una aplicación que utiliza alguno de los protocolos del nivel de aplicación se conoce como **servicio**. De esta forma, una aplicación cliente se ejecuta en un equipo para solicitar un servicio (envío de datos) a una aplicación servidor que estará en ejecución en otro equipo atendiendo cualquier petición de servicio que reciba.

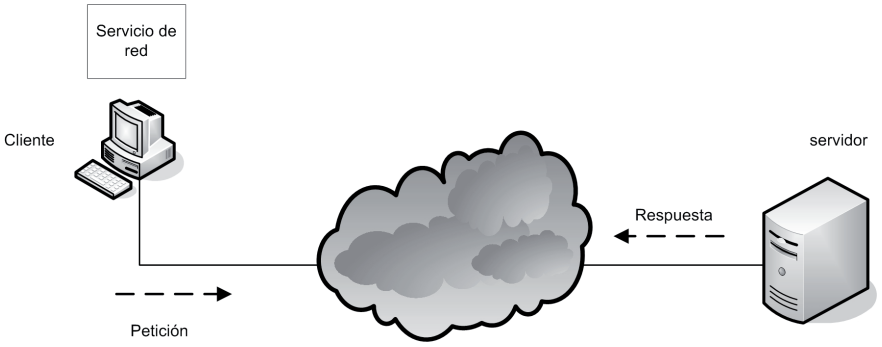


Figura 5.37. *Modelo cliente-servidor en los servicios de red*

En los próximos apartados se describirán brevemente los principales protocolos utilizados en TCP/IP en el nivel de aplicación.

5.7.1 SERVICIO DE ACCESO A PÁGINAS WEB

El acceso al sistema **World Wide Web**, o simplemente **web**, es sin duda el servicio más utilizado en Internet en la actualidad. Para acceder a este servicio se utiliza el protocolo **HTTP** (*Hypertext Transfer Protocol*, protocolo de transferencia de hipertexto). Este protocolo permite la transferencia tanto de texto sin formato como de texto con formato, hipertexto (permite saltos rápidos entre documentos), imágenes, sonido y video. La comunicación a través del protocolo HTTP se lleva por defecto por el puerto 80.

Es un protocolo cliente-servidor en el cual el cliente HTTP (normalmente un navegador web) envía mensajes, llamados peticiones, a un servidor HTTP. El servidor responde enviando una respuesta al cliente, esta respuesta contiene normalmente la página web solicitada por el cliente en la petición. Dicha página web en realidad es un archivo.

Para el acceso a los recursos proporcionados por el servicio web se utiliza un parámetro conocido como localizador uniforme de recursos o **URL** (*Uniform Resource Locator*). Dicho parámetro sigue un formato estándar para nombrar y localizar cualquier tipo de información en Internet. Un URL está formado por cuatro elementos:

- **Método**: protocolo utilizado para obtener el recurso. Es opcional y si no se especifica se utiliza el valor *http*.
- **Servidor**: equipo donde se encuentra la información a la que se quiere acceder. El servidor se puede especificar mediante su dirección IP o (más habitual) por su nombre de dominio.
- **Puerto**: es opcional y contiene el número de puerto del servidor. Por defecto se utiliza el puerto 80.
- **Ruta**: camino para llegar al recurso al que se quiere acceder. Se utiliza el carácter / para separar los nombres de los directorios.

El formato general de un URL es el siguiente:

Método :// Servidor : puerto / ruta

Algunos ejemplos:

- ✓ *http://www.google.es*
- ✓ *http://www.uc3m.es/depar/operativos/index.html*
- ✓ *http://www.servidor.com:3500/ejemplo/graficos.html*

En función de lo anterior se podría decir que *World Wide Web* (www) o simplemente *web* es un servicio cliente-servidor distribuido que utiliza principalmente el protocolo HTTP para su funcionamiento. La web es un repositorio de información mundial y enlazada entre sí. Los documentos contenidos en la web pueden ser de tres tipos:

- **Páginas web estáticas**: son páginas de contenido fijo que se crean y se almacenan en un servidor. El cliente obtiene bajo petición una copia de las mismas para visualizarlas en el navegador web. El lenguaje estándar utilizado para crear páginas web estáticas es **HTML**. Este lenguaje permite especificar etiquetas para dar formato al texto. Estas etiquetas son leídas e interpretadas por los navegadores web para establecer el formato de visualización de la página.
- **Páginas web dinámicas**: una página dinámica se crea en el servidor cuando un cliente lo solicita. Cuando llega la petición, el servidor web ejecuta un programa que crea el documento y le envía el resultado al cliente. El contenido del documento dinámico puede variar de una petición a otra.

  CGI es la tecnología utilizada para crear y gestionar páginas dinámicas. CGI no es un lenguaje, es un conjunto de estándares que definen cómo escribir una página dinámica, cómo proporcionar la entrada al programa y cómo se debería utilizar el resultado de salida. Un programa CGI puede estar escrito en cualquier lenguaje de programación.
- **Páginas web activas**: las páginas activas son realmente programas que necesitan ejecutarse en el cliente. Cuando un navegador solicita una página activa, el servidor envía una copia de la página en formato binario y ésta es ejecutada en el cliente.

  El lenguaje de programación más utilizado para crear páginas activas es **Java**. Los programas escritos en Java y ejecutados a través de un navegador web se conocen como **applets**.

5.7.2 SERVICIO DE TRANSFERENCIA DE CORREO ELECTRÓNICO: SMTP

SMTP (*Simple Mail Transfer Protocol*, protocolo simple de transferencia de correo) es un protocolo cliente-servidor que sirve para el envío de mensajes de correo electrónico de un usuario a otro o de un usuario a un servidor SMTP. El envío de correo entre un cliente y un servidor se lleva a cabo a través del puerto 25 de una conexión TCP.

Para el envío de correo se utiliza un sistema de direccionamiento con el siguiente formato:

Parte local @ nombre de dominio

SMTP solo se puede utilizar para enviar texto ASCII. Debido a esta limitación se desarrolló **MIME** (*Multipurpose Internet Mail Extensions*) como una extensión a SMTP para permitir el envío de datos no ASCII.

Otro protocolo asociado al servicio de correo electrónico es **POP3** (*Post Office Protocol*, protocolo de oficina de correos versión 3) que es un protocolo cliente-servidor utilizado para descargar mensajes de correo electrónico desde un servidor (normalmente SMTP). POP3 lleva a cabo la comunicación mediante conexiones TCP utilizando el puerto 110.

En el modelo OSI existía otro protocolo que implementaba el servicio de correo electrónico llamado X.400, pero actualmente apenas se utiliza debido a la gran aceptación de SMTP.

5.7.3 SERVICIO DE TRANSFERENCIA DE ARCHIVOS: FTP

FTP (*File Transfer Protocol*, protocolo de transferencia de ficheros) es uno de los primeros protocolos del nivel de aplicación desarrollados en redes TCP/IP. Es un protocolo cliente-servidor utilizado para el intercambio de ficheros, que es una de las tareas más habituales realizadas en un entorno de red. Se utilizan dos conexiones TCP para realizar las transferencias, una para los datos que utiliza el puerto 20 y otra para información de control que utiliza el puerto 21.

El servicio de transferencia de ficheros es proporcionado por un servidor FTP, que es un proceso ejecutándose en un equipo y que escucha las peticiones recibidas a través del puerto 21. Este protocolo utiliza la validación de la conexión mediante la introducción de un nombre de usuario y una contraseña, aunque la mayor parte de los servidores FTP admiten la posibilidad de activar lo que se conoce como **usuario anónimo** (*anonymous*) para permitir el acceso anónimo a un servidor FTP, normalmente con acceso restringido.

Las primeras implementaciones de clientes FTP se usaban sobre líneas de comandos. Este tipo de clientes todavía están disponibles en los sistemas Windows o en Linux, a través del **comando ftp**. Actualmente existen clientes FTP que se ejecutan en los avanzados entornos gráficos y que son mucho más sencillos de utilizar. Incluso los navegadores web implementan la funcionalidad del protocolo FTP.

Una de las principales carencias del protocolo FTP es que todos los datos intercambiados, incluidos los datos de validación (nombre de usuario y contraseña), se transfieren sin ningún tipo de encriptación. Actualmente se han desarrollado otros protocolos de transferencia de ficheros en modo seguro, con encriptación de los datos, como FTP sobre SSH (conocido como **Secure FTP**), **FTPS** (FTP/SSL) o **SCP** (*Secure Copy Protocol*).

5.7.4 SERVICIO DE TERMINAL REMOTO: TELNET Y SSH

Telnet (*Terminal Network*, terminal de red) es un protocolo cliente-servidor que permite la conexión a un equipo remoto a través de un terminal desde el cual se pueden ejecutar comandos y aplicaciones como si se ejecutasen de forma local. El protocolo Telnet envía los caracteres tecleados en el equipo local (cliente) al equipo remoto (servidor), el cual los interpreta como si se hubiesen tecleado en un terminal de comandos local. La salida producida en el equipo remoto se envía al equipo local donde se visualiza. Telnet utiliza el puerto 23.

Es uno de los primeros protocolos implementados en redes TCP/IP. En los sistemas Unix ha sido ampliamente utilizado para llevar a cabo la administración de equipos de forma remota.

Al igual que el protocolo FTP, uno de sus principales problemas es la seguridad, ya que ni siquiera el nombre de usuario y la contraseña de validación se envían encriptados. Por ello, se ha desarrollado el protocolo **SSH** (*Secure Shell*) con la misma funcionalidad que Telnet pero llevando a cabo la encriptación de todos los datos que se transmiten. SSH utiliza el puerto 23 y se utiliza ampliamente en los sistemas Linux.

5.7.5 SERVICIO DE GESTIÓN DE RED: SNMP

SNMP (*Simple Network Management Protocol*, protocolo simple de gestión de red) es un protocolo para gestionar dispositivos de red a través del protocolo TCP/IP. Está basado en el concepto de gestor y agente. Un gestor es normalmente un equipo que controla y monitoriza un conjunto de agentes, normalmente *routers*. Como este protocolo está definido en el nivel de aplicación, puede gestionar redes con características y tecnologías diferentes.

Los equipos gestores ejecutan un cliente SNMP. Los dispositivos gestionados o agentes ejecutan un servidor SNMP. El protocolo SNMP proporciona un mecanismo útil y eficaz para monitorizar redes. Sin embargo, el intercambio de información entre gestores y agentes hace que el tráfico de red aumente.

La transferencia de los datos del protocolo SNMP se lleva a cabo mediante UDP a través de los puertos 161 (agente) y 162 (gestor).

5.8 INTERNET Y SUS ORGANIZACIONES

En una obra dedicada a exponer conocimientos sobre redes telemáticas es inevitable no hacer una mención a la gran red telemática mundial, es decir, **Internet**. No hay un consenso claro de en qué momento nace Internet. Algunos autores sitúan este momento en el nacimiento de **ARPANET** en 1969. Este hecho se puede considerar el embrión de Internet por ser el primer intento de unir ordenadores situados en distintos lugares, pero no se puede considerar Internet todavía. La definición más extendida de Internet es la de *red de redes*. ARPANET no es una red de redes sino unas cuantas computadoras unidas entre sí mediante conexiones telefónicas (los primeros enlaces WAN).

Sería más correcto señalar como el nacimiento de Internet a la puesta en servicio de la red **NSFNET**, una red que ya utiliza los protocolos TCP/IP y cuya misión es la de ser troncal para la conexión de redes. Este hecho se produce en 1986 aún cuando ARPANET sigue en servicio. Es por ello que NSFNET se considera una evolución o continuación de ARPANET cuando realmente su objetivo es ya claramente la interconexión de redes, eso sí, utilizando todos los desarrollos tecnológicos de ARPANET.

La red NSFNET la crea en Estados Unidos una fundación llamada NSF (***National Science Foundation***, **Fundación Nacional de Ciencia)**, que es algo así como una agencia de investigación científica financiada por el propio Gobierno de Estados Unidos. Por tanto, NSF se puede considerar el organismo responsable de los primeros pasos de Internet. De hecho, este organismo ya había participado en el desarrollo de ARPANET.

En 1990 se desmantela definitivamente ARPANET (aunque continúa operativa la rama militar MILNET), quedando NSFNET como único troncal de la Red. Sin embargo, el gran desarrollo de Internet comienza cuando algunas empresas empiezan a implementar sus propias redes y a ofrecer servicios de conexión de Internet a través de ellas.

En paralelo a estos acontecimientos, se produce otro hecho fundamental en la evolución de Internet. En 1989, Tim Berners-Lee, un licenciado en Física que trabajaba en el **Laboratorio Europeo de Física de Partículas** (CERN, Organisation Européenne pour la Recherche Nucléaire), propuso un proyecto para la creación de un sistema de gestión de la información. Tres años más tarde, en 1992, empezaban a funcionar los primeros servicios para compartir información a través de la Red, era el nacimiento del **World Wide Web** (www) o simplemente Web. El éxito de este sistema fue inmediato, ya que permitía la publicación de documentos en Internet con la posibilidad de incluir enlaces a otros documentos alojados en otros servidores (hipertexto). El impulso definitivo del servicio web se produjo cuando apareció el primer navegador con capacidades gráficas llamado **Mosaic**, en 1993.

Mientras tanto, la NSF decide ceder el control del *backbone* de Internet a las empresas proveedoras de los servicios de conexión. Esta decisión implica que el control de Internet dejaba de estar en manos de un país (la NSF estaba financiada con dinero de Estados Unidos) para ser una red descentralizada. Esta característica ha sido fundamental en el desarrollo posterior de la Red.

En 1995, la NSF transfiere el control de Internet de forma provisional a cuatro operadoras norteamericanas: **MFS Datanet**, **Sprint**, **Ameritech** y **Pacific Bell**. Estas empresas constituyen los llamados **NAP** (*Network Access Point*) o puntos de acceso a la red, que proporcionan conectividad al resto de empresas que ofrecen servicios de conexión a Internet, los llamados **ISP (*Internet Service Provider*)**. Sin embargo, durante los siguientes años el proceso de descentralización de la Red sigue avanzando y desaparecen estos primeros NAP para establecerse la arquitectura definitiva y que se mantiene en la actualidad a través de los llamados **IXP (*Internet eXchange Points*)**. Un IXP es una infraestructura física que permite la interconexión de varios ISP para intercambiar tráfico entre ellos y con otros IXP.

Como veíamos, a pesar de que Internet ofrecía casi desde sus inicios diferentes servicios basados todos en la arquitectura TCP/IP, como correo electrónico, transferencia de ficheros, búsqueda de información, etc., fue el servicio web el que hizo explotar definitivamente el potencial de la Red a nivel comercial. El primer navegador que se ejecutó en un entorno gráfico (concretamente en entornos X de sistemas Unix) fue **Mosaic** y tuvo una gran aceptación debido sobre todo a que era gratuito.

Unos años más tarde, Microsoft desarrolla su propio navegador web, llamado **Internet Explorer**, también gratuito, y Mosaic se convierte en **Netscape**, estableciéndose una dura competencia entre ellos. Actualmente Microsoft sigue ofreciendo su navegador web incluido en los sistemas operativos Windows, mientras que Netscape evolucionó a **Mozilla Firefox**. El servicio web es, con diferencia, el servicio más utilizado en Internet debido sobre todo a los grandes avances técnicos conseguidos en la tecnología de navegación, que permite a su vez la visualización o ejecución de numerosos formatos multimedia y es capaz de proporcionar a los documentos web un alto grado de dinamismo.

Aunque en sus inicios Internet dependía del Gobierno de Estados Unidos, en los años 90 se produjo un proceso de desvinculación y actualmente los organismos que gestionan Internet de manera global son bastante independientes. Los principales son:

- **ISOC** (*Internet Society*). La ISOC es una organización no gubernamental dedicada al desarrollo a nivel global de Internet, formada por instituciones comerciales, gubernamentales y educativas. Su objetivo principal es ser un centro de cooperación y coordinación global para el desarrollo de protocolos y estándares compatibles para Internet. La ISOC proporciona la infraestructura corporativa, así como el financiamiento, apoyo jurídico y fiscal del resto de organizaciones que gestionan Internet.

- **IAB** (*Internet Architecture Board*). Comisión creada para gestionar los protocolos usados en la red. Creada inicialmente por DARPA en 1979 como Internet Configuration Control Board, y en donde estaban representados DARPA, NASA, Dep. Energía, NSF. Presidida por Vinton G. Cerf, uno de los desarrolladores de los protocolos TCP/IP junto a Robert E. Kahn. A partir de 1992, depende de la ISOC. Entre otras funciones el IAB es responsable de la publicación de los RFC y de la supervisión de los trabajos del IETF.

  Los **RFC** (*Request For Comments*) son los documentos donde se publican todos los estándares que forman parte de Internet. Se determinan mediante equipos de trabajo que operan de manera abierta y democrática para asegurar la evolución transparente de Internet. Por ejemplo, la arquitectura TCP/IP está publicada bajo documentos RFC. Los documentos RFC están publicados en ficheros con formato ASCII y en inglés en la página web oficial *www.rfc-editor.org*. Existe además una página donde algunos de los más importantes RFC han sido traducidos al español: *www.rfc-es.org*.

- **IETF** (*Internet Engineering Task Force*). La IETF es una organización formada por grupos de trabajo encargados de diversos aspectos relacionados con la evolución de la arquitectura de Internet. Los grupos de trabajo se constituyen para llevar a cabo estudios de las diferentes tecnologías utilizadas en Internet. Los trabajos de la IETF son supervisados por la IAB. Anualmente ISOC aporta a la IEFT alrededor de un millón de dólares para la elaboración de los RFC.

- **IRTF** (*Internet Research Task Force*). Al igual que la anterior, es una organización formada por grupos de trabajo dedicados a tareas de investigación de las nuevas tecnologías que se pueden aplicar a Internet.

- **ICANN** (*Internet Corporation for Assigned Names and Numbers*). Es una organización sin fines de lucro que opera a nivel internacional, responsable de asignar espacio de direcciones numéricas del protocolo IP, identificadores de protocolo y de las funciones de gestión (o administración) del sistema de nombres de dominio de primer nivel genéricos y de códigos de países, así como de la administración del sistema de servidores raíz. La gestión del direccionamiento global y los dominios raíz se lleva a cabo desde otro organismo llamado **IANA** (*Internet Assigned Numbers Authority* o Agencia de Asignación de Números en Internet). Inicialmente la IANA pertenecía al Gobierno de Estados Unidos, pero a partir del año 2000 IANA pasa a depender de ICANN como organización independiente.

  Como asociación privada-pública, ICANN está dedicada a preservar la estabilidad operacional de Internet, promover la competencia, lograr una amplia representación de las comunidades mundiales de Internet y desarrollar las normativas adecuadas a su misión por medio de procesos “de abajo hacia arriba” basados en el consenso.

EJERCICIOS PROPUESTOS

1. Indica la clase y la dirección de red de las siguientes direcciones IP:

- 203.56.125.12
- 238.56.112.78
- 109.235.1.90
- 129.157.221.2
- 191.1.23.44

2. ¿Cuál es el máximo número de subredes en una red de clase A utilizando las siguientes máscaras?

- 255.192.0.0
- 255.255.128.0
- 255.255.255.0
- 255.255.248.0

3. ¿Cuál es el máximo número de subredes en una red de clase B utilizando las siguientes máscaras?

- 255.255.255.0
- 255.255.252.0
- 255.255.255.128
- 255.255.192.0

4. ¿Cuál es el máximo número de subredes en una red de clase C utilizando las siguientes máscaras?

- 255.255.255.248
- 255.255.255.192
- 255.255.255.252
- 255.255.255.224

5. Indica la dirección de subred de cada una de las siguientes direcciones IP:

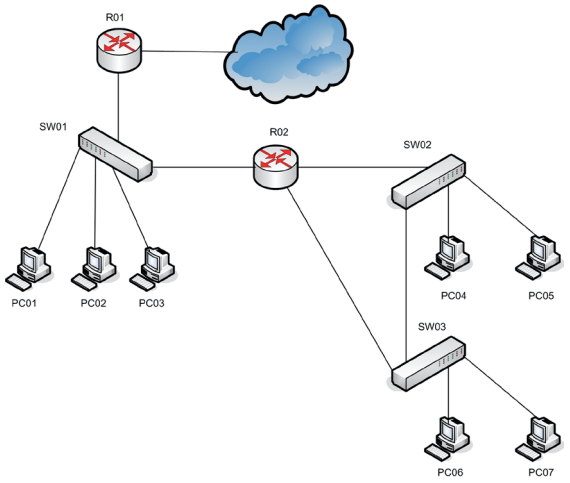
- IP: 121.63.120.56 Máscara: 255.255.0.0
- IP: 98.231.126.198 Máscara: 255.255.128.0
- IP: 168.50.121.5 Máscara: 255.255.224.0
- IP: 180.4.30.101 Máscara: 255.255.192.0
- IP: 205.78.44.153 Máscara: 255.255.255.240

6. Establece el direccionamiento para obtener seis subredes a partir del rango 193.105.10.0/24:

Dir. Subred	Rango de direcciones	Máscara	Dir. Broadcast

7. A partir del esquema de la figura se desea configurar tres subredes. La subred 1, formada por los equipos PC01, PC02 y PC03. La subred 2, formada por los equipos PC04 y PC06. La subred 3, formada por los equipos PC05 y PC07. La capacidad máxima de cada subred debe ser de 60 equipos.

- Dirección de red: 204.34.56.0/24



8. Especifica la configuración de red (dirección IP, máscara y puerta de enlace) de todos los PC, así como las direcciones IP y máscaras de las interfaces de red de los *routers*.

- ¿Los datagramas enviados de PC06 a PC07 serán procesados por el *router* R02? Justifica la respuesta.
- ¿Los datagramas enviados de PC04 a PC06 serán procesados por el *router* R02? Justifica la respuesta.
- Para pasar el equipo PC03 a la subred 2, ¿sería necesario algún cambio en la configuración física de la red? Justifica la respuesta.
- Para pasar el equipo 5 a la subred 2, ¿sería necesario algún cambio en la configuración física de la red? Justifica la respuesta.

TEST DE CONOCIMIENTOS

1 El modelo de niveles de la arquitectura TCP/IP:

a) Es prácticamente igual al modelo OSI.
b) Solo están definidos los niveles de red y de transporte.
c) No se hace distinción entre los niveles físico y de enlace.
d) Las funcionalidades del nivel de sesión se incluyen en el nivel de red.

2 IP es un protocolo:

a) Orientado a conexión.
b) Basado en datagramas.
c) Del nivel de transporte.
d) Todas las respuestas anteriores son correctas.

3 Una de las principales funciones de IP es:
- **a)** Llevar a cabo el control de flujo de la comunicación.
- **b)** Evitar las congestiones en las redes.
- **c)** Identificar errores en la transmisión.
- **d)** Proporcionar un direccionamiento lógico.

4 Una dirección de difusión (*broadcast*) en IP:
- **a)** Tiene todos los bits a 1.
- **b)** Tiene a 1 todos los bits que identifican la red.
- **c)** Tiene a 1 todos los bits que identifican los equipos en una red.
- **d)** No existe la dirección de difusión en IP solo en Ethernet.

5 Cuando se utiliza criptografía asimétrica para proporcionar confidencialidad a los datos:
- **a)** Se utiliza una sola clave privada.
- **b)** Se utiliza una sola clave pública.
- **c)** Se utiliza una clave pública para encriptar y una clave privada para desencriptar.
- **d)** Se utiliza una clave privada para encriptar y una clave pública para desencriptar.

6 De las cinco clases de direcciones IP definidas se utilizan para asignación a redes:
- **a)** Todas las clases.
- **b)** Solo las clases A, B y C.
- **c)** Solo las clases A, B, C y D.
- **d)** Solo las clases A y B. La clase C es solo para subredes.

7 El enmascaramiento se utiliza:
- **a)** Solo en redes que utilicen subredes.
- **b)** Solo en redes de clase C.
- **c)** Tanto en redes con subredes como en redes sin subredes.
- **d)** Solo en los *routers*.

8 Para llevar a cabo la función de un *firewall* se inspeccionan:
- **a)** Todos los paquetes intercambiados entre dos redes.
- **b)** Solo los paquetes salientes.
- **c)** Solo los paquetes entrantes.
- **d)** Solo los paquetes entrantes provenientes de Internet.

9 Cuando un datagrama IP llega a un *router*:
- **a)** El *router* decrementa el campo TTL una unidad.
- **b)** El *router* cambia la dirección de destino.
- **c)** El *router* cambia la dirección origen.
- **d)** El *router* reenvía el datagrama a todas sus interfaces.

10 La nueva versión IPv6:
- **a)** Mantiene el formato del datagrama respecto a IPv4.
- **b)** Mantiene el formato de dirección lógica respecto a IPv4.
- **c)** Sustituye las direcciones de *broadcast* por las de *multicast*.
- **d)** Elimina la dirección de bucle local o *loopback*.

11 Para que un equipo obtenga los parámetros de configuración de red de forma automática es necesario que en la red haya:
- **a)** Un servidor HTTP.
- **b)** Un servidor DHCP.
- **c)** Un servidor DNS.
- **d)** Un servidor SNMP.

12 El localizador uniforme de recursos o URL se suele utilizar para acceder a recursos del servicio:
- **a)** SMTP.
- **b)** SSH.
- **c)** Web.
- **d)** DHCP.

6 Redes de área local

Como vimos en el primer capítulo, existen principalmente dos tipos de redes telemáticas, conocidas como LAN y WAN. La principal diferencia entre ellas es que los dispositivos conectados a una LAN se encuentran ubicados en un área geográfica limitada, mientras que las redes WAN no tienen esa limitación.

Si tenemos en cuenta que el nivel físico en una red telemática se encarga precisamente de la transmisión de los datos, la distancia que tienen que recorrer estos datos es un factor de diseño decisivo. Precisamente es en los dos primeros niveles, el físico y el de enlace, donde se establecen las principales diferencias entre los dos tipos de redes. Salvo alguna excepción, el diseño de las diferentes arquitecturas LAN se ha centrado en la definición de las funciones de estos dos niveles.

Este capítulo estará centrado en **Ethernet**, que es la tecnología utilizada en las redes LAN cableadas y que cubre las funciones del nivel físico y del nivel de enlace. Así mismo, se estudiarán los dispositivos de interconexión utilizados en las redes locales, principalmente los **switches**.

Sin ninguna duda se puede afirmar que Ethernet es una de las tecnologías más importantes en el ámbito de las redes telemáticas. Actualmente es la tecnología dominante en las redes LAN cableadas. Ethernet tuvo que competir a mediados de los años 80 con otras tecnologías LAN como **Token Ring**y **Token Bus**, pero salió claro ganador y hoy en día el porcentaje de utilización de Ethernet en redes LAN cableadas debe estar muy cerca del 100%. El éxito de Ethernet está basado fundamentalmente en su simplicidad, bajo coste y su alta capacidad de adaptación. En su primera versión Ethernet proporcionaba una velocidad de apenas 3 Mbps y en la actualidad existen especificaciones de Ethernet para trabajar a 10 Gbps. Desde luego, toda una evolución.

6.1 INTRODUCCIÓN

Ethernet es una tecnología desarrollada para ser utilizada en redes LAN, en las cuales cubre las funciones de los niveles físico y de enlace del modelo de referencia OSI. Recordemos que las redes LAN proporcionan conexión a dispositivos en un ámbito geográfico limitado, lo cual es una de las condiciones de diseño. Además, para desarrollar Ethernet se tuvieron en cuenta otras necesidades importantes de las redes LAN, como son alcanzar altas velocidades de transferencia de datos con una baja tasa de errores y que la instalación y mantenimiento sean lo más sencillos posible.

Actualmente, nadie pone en duda las ventajas que se generan al interconectar equipos próximos entre sí o que pertenezcan a una misma unidad organizativa en un edificio (o varios próximos entre sí), es decir, al implementar una LAN. Desde pequeñas oficinas, naves o talleres hasta grandes empresas con cientos o miles de empleados, se utilizan las tecnologías de las redes LAN para interconectar sus equipos y aprovecharse de todas las ventajas que ello supone, principalmente el uso compartido de archivos, impresoras y otros periféricos, así como el acceso compartido a Internet, el acceso a aplicaciones corporativas... Incluso cada vez son más frecuentes los hogares donde montan sus redes LAN a pequeña escala, con dos o tres ordenadores, una impresora y un *router* de acceso a Internet.

La tecnología Ethernet fue desarrollada inicialmente por la empresa **Xerox** en 1973 y funcionaba a una velocidad de 2,94 Mbps. Posteriormente la colaboración entre las empresas Xerox, Intel y Digital (conocida como DIX) dio lugar a su primera versión oficial, que fue publicada en 1980, donde ya se especificaba una velocidad de 10 Mbps.

Ethernet no fue un desarrollo cerrado, Xerox permitió el uso de esta tecnología mediante el pago de una pequeña cuota, de forma que cualquier empresa pudo utilizarlo, propiciando su rápida difusión. En 1982 se publicó la segunda versión de Ethernet, conocida como **Ethernet II**. Esta versión fue la última especificada por DIX y de hecho ese mismo año Xerox liberó la marca registrada sobre el nombre Ethernet.

La organización IEEE utilizó las características de Ethernet como base para desarrollar su estándar IEEE 802.3. Actualmente se utiliza la denominación Ethernet para referirse tanto a la especificación original como a la especificación IEEE 802.3.

Ethernet fue un éxito desde su comienzo, y el éxito ha continuado gracias a su gran capacidad de evolución. Durante algunos años se trabajó con redes Ethernet a 10 Mbps pero en 1995 se publicó una nueva extensión de la norma para velocidades de 100 Mbps, conocida como Fast Ethernet. Pocos años más tarde, en 1998, se publicó la extensión de la norma Ethernet, llamada Gigabit Ethernet, para velocidades de 1 Gbps sobre fibra óptica, y en 1999 para cable UTP. Desde el año 2002 se han ido publicando varias ampliaciones de la norma Ethernet para velocidades de 10 Gbps.

6.2 ETHERNET, IEEE 802.3 Y EL MODELO OSI

Como se ha mencionado en el apartado anterior, el organismo IEEE decidió crear un comité (conocido como Comité 802) para estandarizar las redes telemáticas. Fruto de este trabajo, en 1985 se publicó la norma IEEE 802.3, que definía una tecnología abierta (cualquier fabricante podía adoptarla) para redes de área local. El comité del IEEE utilizó la tecnología Ethernet como referencia para desarrollar la norma IEEE 802.3, pero a su vez intentó encajar esta tecnología en el modelo de referencia OSI (publicado solo un par de años antes, en 1983). Debido a ello, la norma IEEE 802.3 presentaba algunas pequeñas diferencias respecto a Ethernet, aunque se consideraron tecnologías compatibles.

Además del estándar IEEE 802.3, fueron publicados otros estándares de redes locales como el IEEE 802.4, conocido como Token Bus, y el IEEE 802.5, desarrollado a partir de la tecnología de redes locales usada en esa época por IBM y llamada Token Ring. Durante unos años estas tecnologías de redes locales convivieron hasta que se impuso el estándar basado en Ethernet.

El organismo IEEE ha seguido desarrollando estándares relacionados con las redes telemáticas, muchos de ellos basados en transmisiones inalámbricas como IEEE 802.11 (Wi-Fi), IEEE 802.15.1 (Bluetooth) o IEEE 802.16 (WiMAX). Así mismo, el IEEE ha seguido publicando revisiones y actualizaciones del estándar IEEE 802.3 para adaptarlo a las nuevas exigencias de prestaciones de las redes locales.

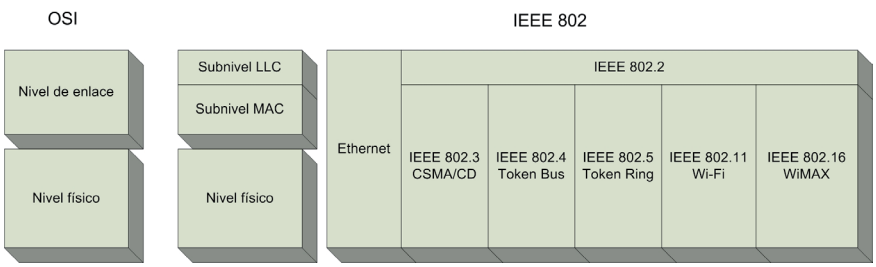


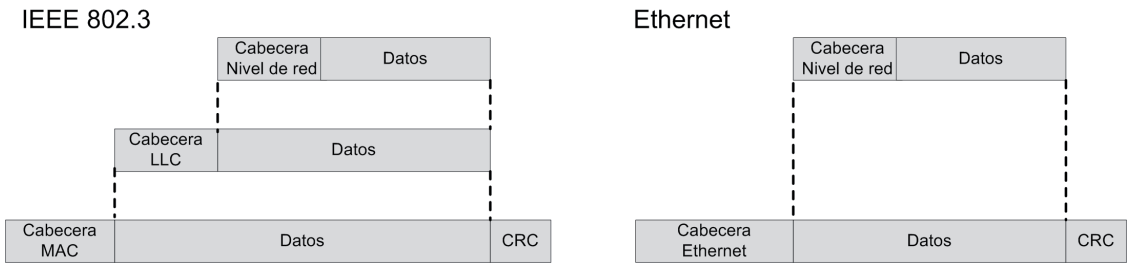
Figura 6.1. *Estándares para redes del IEEE*

Como se observa, el nivel de enlace en las redes LAN definidas por el proyecto IEEE 802 se subdivide de dos niveles, uno superior y común a todas las implementaciones LAN, llamado **LLC** (*Logical Link Control* o control de enlace lógico), y otro inferior llamado **MAC** (*Medium Access Control* o control de acceso al medio), que depende de cada implementación.

IMPORTANTE

Control de enlace lógico (LLC): 802.2

El subnivel **LLC** (control de enlace lógico) está definido dentro del estándar **IEEE 802.2**. Es el subnivel superior del nivel de enlace en todas las tecnologías de red definidas por el IEEE. Es decir, este subnivel no depende de ninguna implementación de red concreta y es común a todas ellas.
La principal función de este subnivel es proporcionar un formato único de datos y una interfaz común al nivel superior, es decir, al nivel de red. De esta forma se esconden al nivel de red las diferencias de formatos en los diferentes tipos de redes. Para ello, este nivel implementa una encapsulación de datos añadiendo una cabecera.



Las funciones que proporciona Ethernet son las funciones que cubren los niveles físico y de enlace del modelo de referencia OSI. Por una parte, Ethernet especifica todos los aspectos relacionados con el nivel físico, como puede ser el tipo de cableado, conectores, velocidad, codificación de los datos, etc. Pero además especifica funciones del nivel de enlace como métodos de acceso al medio, direccionamiento físico, tramado o control de errores.

La evolución de Ethernet ha supuesto desarrollar nuevas especificaciones, sobre todo en las funciones del nivel 1 (físico). Sin embargo, algunas de las funciones del nivel 2 (enlace) han permanecido sin variaciones desde las primeras versiones. Después de dedicar un apartado sobre el primer contacto práctico con una red basada en Ethernet, dedicaremos los siguientes a estudiar todas las funciones que proporciona Ethernet.

6.3 UN PRIMER CONTACTO PRÁCTICO CON ETHERNET

Antes de profundizar en los aspectos técnicos relacionados con Ethernet, se ofrecerá en este apartado una visión más práctica de lo que nos vamos a encontrar cuando estemos delante de una red que utilice Ethernet.

En muchas ocasiones se utiliza la expresión **red Ethernet** para referirse a una red LAN que utiliza la tecnología Ethernet, que, por otra parte, son la gran mayoría de las redes. Emplearemos esta expresión en la presente obra.

La primera característica importante a tener en cuenta sobre las redes Ethernet es su topología, es decir, cómo están conectados los elementos que forman parte de la red. Actualmente Ethernet utiliza una **topología en estrella**, y dado que admite un cierto nivel de anidamiento es frecuente encontrar redes Ethernet siguiendo topologías en árbol o estrella anidada.

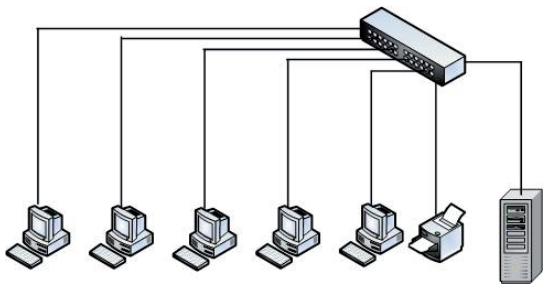


Figura 6.2. *Topología en estrella de las redes Ethernet actuales*

Es prácticamente seguro que cuando estemos en algún lugar que tenga una red local en funcionamiento, ésta utilice Ethernet. ¿Cuáles son los elementos visuales que nos encontraremos en una red Ethernet?

- **Cableado y su infraestructura de distribución**. Si nos encontramos en un lugar donde existe una instalación de cableado de datos, dicha instalación contará con unos puntos de conexión llamados **rosetas** o tomas murales, situadas en cada área de trabajo.

Figura 6.3. *Roseta en una red Ethernet*

Desde este punto de conexión existirá un cable que conectará dicho punto al ordenador. Este cable habitualmente es de tipo UTP de 4 pares y se conoce como **latiguillo de red**. Los latiguillos de red se identifican porque tienen en cada extremo un conector RJ-45.

Figura 6.4. *Latiguillo de red*

Los puntos de conexión o rosetas a su vez estarán unidos a la infraestructura de comunicaciones mediante el cableado distribuido por canaletas, bandejas, falsos suelos o techos. Todo el cableado de distribución acaba en los armarios de comunicaciones donde se conectan a los dispositivos de interconexión, típicamente *switches*.

Figura 6.5. *Cableado de red distribuido por un falso suelo*

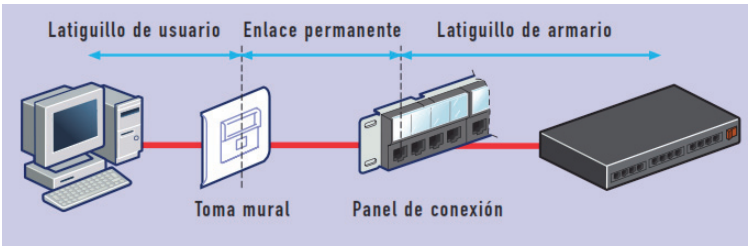


Figura 6.6. *Enlace completo en una instalación de red Ethernet*

El uso del cable UTP en redes LAN basadas en Ethernet está tan extendido que es frecuente escuchar el término **cable Ethernet** para referirse a un cable UTP de cuatro pares.

- **Tarjetas de red**. El punto de entrada de la red a los equipos es la tarjeta de red. Podemos encontrar tarjetas de red que se instalan en los *slots* PCI de la placa del equipo, aunque la mayor parte de las tarjetas de red están incluidas en la propia placa base del equipo. El único elemento identificativo en este caso es el conector de red, que para cable UTP es de tipo RJ-45. En el próximo apartado se dan algunos detalles más sobre las tarjetas de red.
- **Dispositivo de interconexión**. Habitualmente, el dispositivo de interconexión utilizado para formar redes LAN se conoce como ***switch*** o **conmutador**. En la mayor parte de las redes, el *switch* (o los *switches*) suele estar ubicado en un espacio reservado o una sala técnica hasta donde llega todo el cableado. Más adelante en este capítulo se darán más detalles del funcionamiento de los *switches*.

Figura 6.7. *Dos switches en funcionamiento en una red local Ethernet*

En las pequeñas instalaciones domésticas no existe una infraestructura de cableado. El *router* de acceso a Internet proporcionado por el proveedor de acceso a Internet suele integrar la funcionalidad de un *switch* de cuatro puertos, por lo que dicho *router* hace las funciones de dispositivo de interconexión. La conexión de los puertos Ethernet del *router* a los equipos se hace directamente con un latiguillo de red.

Figura 6.8. *Router ADSL con cuatro puertos Ethernet formando una red local de cuatro equipos*

6.4 TARJETAS DE RED

Las tarjetas de red, también conocidas por sus siglas en inglés **NIC** (*Network Interface Card*), son elementos electrónicos que posibilitan la conexión de un equipo a una red local. Las primeras tarjetas de red se conectaban en un equipo a través de un *slot* de expansión en la placa base del equipo.

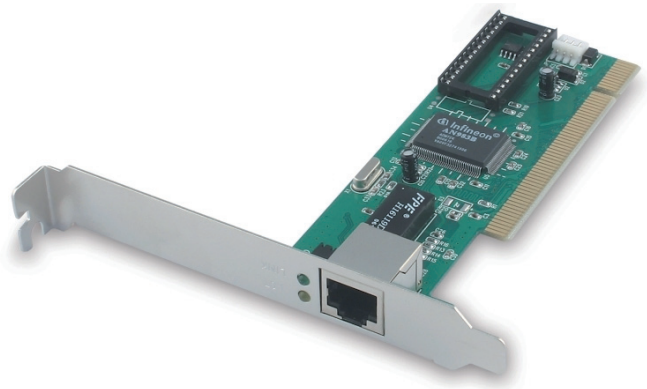


Figura 6.9. *Tarjeta de red para conectar en un slot PCI*

En la actualidad, todas las placas base incluyen ya la circuitería relativa a la interfaz de red, es decir, de la tarjeta de red, por lo que no es necesario conectar al equipo ninguna tarjeta de red a menos que la tarjeta de red incluida en la placa base se estropee o necesitemos una tarjeta de red con características especiales.

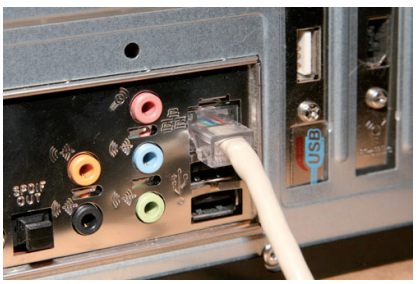


Figura 6.10. *Tarjeta de red incluida en la placa base de un equipo*

El diseño y las funciones implementadas en una tarjeta de red dependen de la tecnología para la que se va a utilizar. Actualmente la tecnología dominante es Ethernet, por lo tanto, todas las tarjetas de red que se pueden encontrar son tarjetas Ethernet. La mayor parte de ellas utilizan cable UTP y, por tanto, el conector que llevan incorporado es de tipo RJ-45. Sin embargo, existen especificaciones Ethernet que utilizan fibra óptica, por lo que también existen en el mercado tarjetas de red Ethernet con un conector para fibra óptica.

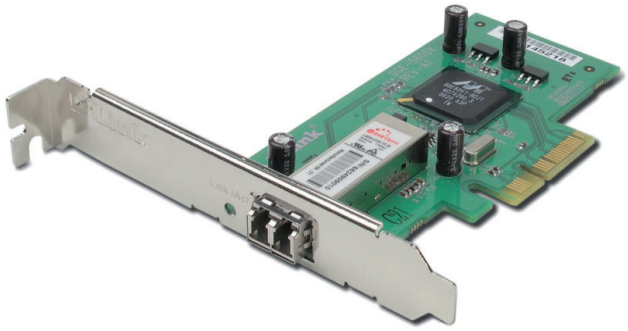


Figura 6.11. *Tarjeta Gigabit Ethernet (DLink DGE-560SX) que utiliza fibra óptica en lugar de cable UTP*

En cualquier caso, tanto si tenemos un equipo con tarjeta de red como si ésta está integrada en la placa base, lo más habitual es el uso de cable UTP y, por tanto, en la parte trasera de dicho equipo encontraremos un conector hembra RJ-45 utilizado para conectar el equipo a la red.

Las tarjetas de red llevan a cabo todo el procesamiento de las funciones 1 y 2 del modelo de referencia OSI en el equipo. Muchas de las funciones que veremos en los próximos apartados se llevan a cabo precisamente en las tarjetas de red.

Para que una tarjeta de red funcione adecuadamente en un equipo con el sistema operativo Windows o Linux es necesario que exista un **controlador** o ***driver***. Dicho controlador posibilita que el sistema operativo pueda intercambiar información con la tarjeta, es decir, permite la comunicación entre el sistema operativo y la propia tarjeta de red. Los sistemas operativos contienen internamente controladores para muchos modelos diferentes de tarjetas de red pero en algunas ocasiones será necesario instalar dicho controlador, que deberá ser suministrado por el fabricante de la tarjeta de red.

Una vez instalado correctamente el controlador, es posible acceder a algunos parámetros de configuración avanzados de la tarjeta de red. En la siguiente figura se puede observar la ventana de configuración en Windows XP:

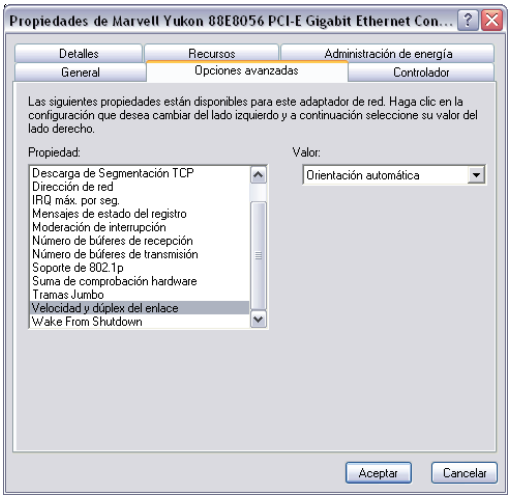


Figura 6.12. *Ventana de configuración de la tarjeta de red en Windows*

6.5 ESPECIFICACIONES DEL NIVEL 2 EN ETHERNET

Algunas de las especificaciones sobre funciones del nivel 2 del modelo de referencia OSI desarrolladas para las primeras versiones de Ethernet se han mantenido a lo largo del tiempo y siguen siendo válidas en la actualidad. Éstas son el direccionamiento físico, el formato de la trama y el control de errores. Sin embargo, la función de control del enlace utilizado en las redes Ethernet tradicionales hoy en día está prácticamente en desuso, aunque se ha mantenido en las especificaciones por motivos de compatibilidad.

6.5.1 DIRECCIONAMIENTO

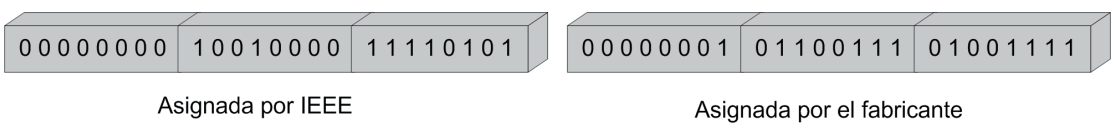
En los próximos apartados se repasará la forma en que se implementan las principales funciones del nivel 2 del modelo OSI en Ethernet. Empecemos con el **direccionamiento físico**, que consiste en proporcionar un mecanismo para identificar cada equipo conectado a la red.

La dirección física en las redes Ethernet es un número binario formado por 48 bits (6 bytes) y almacenado en la propia tarjeta de red. La dirección física también se conoce como **dirección MAC**.

Esta dirección debe ser única para toda la red, y para conseguir esto cada tarjeta de interfaz de red se configura de fábrica con una dirección física diferente. De esta forma se asegura de que no va a haber dos tarjetas conectadas en la misma red con la misma dirección física. Los 24 bits de mayor peso los asigna el IEEE e identifica a la empresa fabricante de la tarjeta de red. Este número de 24 bits se conoce como **OUI** *(Organizationally Unique Identifier)*. Los 24 bits de menor peso los asigna el fabricante a cada tarjeta durante el proceso de fabricación.

La asignación de los 24 primeros bits a fabricantes se puede encontrar en la siguiente página: *http://standards.ieee.org/regauth/oui/oui.txt*.

Un ejemplo de dirección física podría ser el siguiente:



La notación binaria utilizada en el ejemplo anterior es incómoda de manejar, por lo que normalmente se utiliza la notación hexadecimal. En dicha notación se utilizan guiones (-) o dos puntos (:) como separadores de cada dos dígitos hexadecimales. El ejemplo anterior se representaría en formato hexadecimal de la siguiente forma:

00-90-F5-01-67-4F o bien utilizando el carácter "dos puntos" como separador: **00:90:F5:01:67:4F**

Se ha definido una dirección especial llamada **dirección de broadcast o de difusión** utilizada para enviar una trama a todos los dispositivos de una red. Es la dirección FF:FF:FF:FF:FF:FF, es decir, todos los bits a valor 1.

Todos los equipos conectados a una red Ethernet deben tener asignada una dirección MAC. Incluso puede darse el caso de equipos que tienen más de una tarjeta de red. En este caso, cada tarjeta de red tendrá su dirección MAC. Para equipos que utilizan como sistema operativo Windows 7 (o XP) se puede consultar la dirección MAC con el comando **ipconfig /all** ejecutado mediante la herramienta *Símbolo del sistema*.

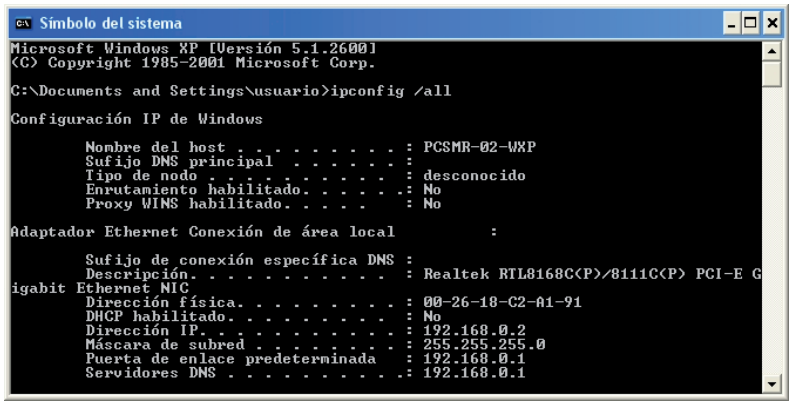


Figura 6.13. *Ejecución del comando ipconfig para ver la dirección MAC*

En sistemas Linux se puede consultar la dirección MAC mediante el comando **ifconfig** ejecutado desde un terminal de comandos.

La dirección física asignada por el fabricante a una tarjeta de red en el proceso de fabricación no puede ser cambiada. Sin embargo, en la actualidad existen mecanismos que permiten llevar a cabo un cambio ficticio de la dirección física por software, normalmente a través de los sistemas operativos más actuales como Windows XP, Windows 7 o Linux. En este caso, la dirección física de la tarjeta no se altera pero los servicios de red del sistema operativo proporcionan una dirección física ficticia, es decir, enmascaran la verdadera dirección.

En la siguiente figura se puede observar la ventana de configuración de la tarjeta de red de un equipo y el parámetro con el que se puede modificar la dirección física de dicho equipo.

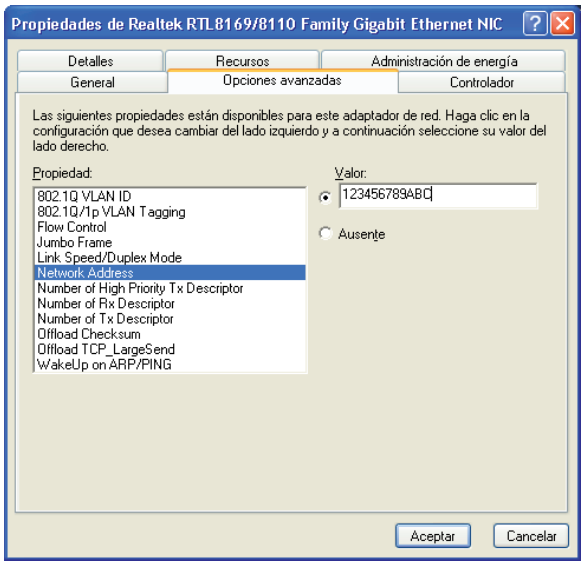


Figura 6.14. *Enmascaramiento de la MAC de una NIC desde Windows XP*

6.5.2 FORMATO DE TRAMA

Una de las funciones cubiertas en el nivel de enlace es el tramado de la información que se quiere transmitir. El tramado consiste en dividir dicha información en fragmentos denominados tramas y añadir a cada fragmento información de control en lo que se conoce como cabecera. Veamos primero cómo es el formato de la trama especificada en el estándar IEEE 802.3.

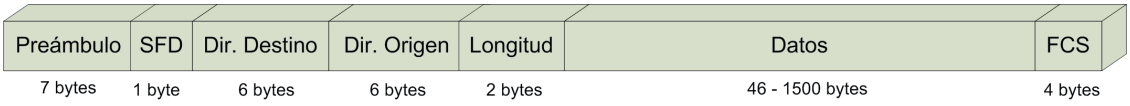


Figura 6.15. *Formato de la trama IEEE 802.3*

La trama IEEE 802.3 se divide en campos o bloques de información. La información real que se quiere transmitir y que proviene del nivel superior se incluye en el campo **Datos**, el resto es información de control. A continuación se describe la función de cada campo:

- **Preámbulo**. Está formado por 7 bytes (56 bits) con valores 0 y 1 alternados. Es decir, cada byte contiene los bits 10101010. Este campo se utiliza para realizar la sincronización entre el emisor y el receptor.
- **SFD** (*Start Frame Delimiter*) o delimitador del comienzo de trama. Es 1 byte con el valor 10101011. Este campo indica el inicio de la trama.

- **Dirección de destino**. Campo con un tamaño de 6 bytes que contiene la dirección física (dirección MAC) del dispositivo de destino.
- **Dirección fuente u origen**. Campo con un tamaño de 6 bytes que contiene la dirección física (dirección MAC) del dispositivo que envía la trama.
- **Longitud**. Este campo está formado por 2 bytes que indican la longitud de los datos. El valor mínimo es 0 y el máximo es 1.500.
- **Datos**. Este campo tiene un tamaño variable entre 46 y 1.500 bytes dependiendo lógicamente de la información recibida del nivel superior. El tamaño mínimo de este campo debe ser de 46 bytes, por lo tanto, si el número de bytes para enviar es inferior, se envían bytes de relleno hasta completar este tamaño mínimo. Esto se debe a que el tamaño mínimo total de la trama debe ser de 64 bytes por cuestiones relacionadas con la temporización en el uso del medio de transmisión.
- **FCS** (*Frame Check Sequence*) o secuencia de verificación de trama. Este campo contiene un valor de 4 bytes (32 bits) conocido como **CRC** o código de redundancia cíclica y que es utilizado para la detección de errores en la transmisión. El campo FCS no se considera parte de la cabecera, ya que se añade al final de la trama, sin embargo, sí forma parte de la información de control.

Veamos ahora cúal es el formato de la trama Ethernet II:

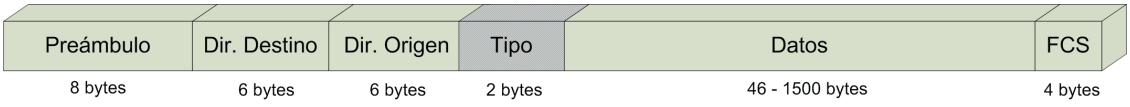


Figura 6.16. *Formato de la trama Ethernet II*

Se puede observar que hay pocas diferencias entre las tramas IEEE 802.3 y Ethernet II. Por una parte, el campo SFD de IEEE 802.3 está incluido en el preámbulo en Ethernet II, pero su contenido es el mismo. Por otra parte, el campo **Longitud** en IEEE 802.3 se ha convertido en el campo **Tipo** en Ethernet II. El campo **Tipo** es un código de 2 bytes que indica el protocolo de nivel superior (nivel de red).

Los protocolos de nivel de red más utilizados en redes LAN basadas en TCP/IP son IP y ARP. Además, para IP existen dos versiones, la actual IPv4 y la futura IPv6. Los códigos en valor hexadecimal utilizados en el campo *Tipo* para estos protocolos son:

- IPv4 0800
- IPv6 86DD
- ARP 0806

Además, hay que tener en cuenta que en la trama IEEE 802.3 el campo *Datos* contiene la información del nivel superior, que en este caso es el subnivel LLC. Este subnivel, como se ha comentado anteriormente, añade una cabecera de 3 bytes. En el caso del formato Ethernet II, el campo *Datos* contiene información que proviene directamente del nivel de red, ya que en este caso no se utiliza el subnivel LLC.

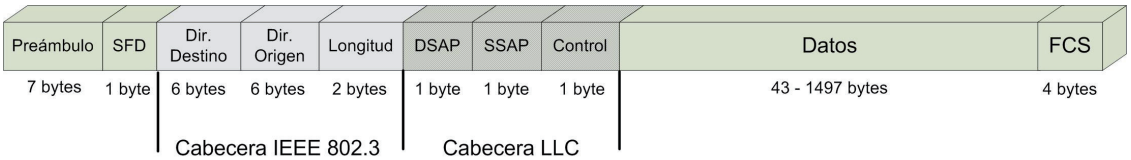


Figura 6.17. *Formato de la trama IEEE 802.3 incluyendo la cabecera LLC*

Estos dos formatos de trama han coexistido en las redes Ethernet hasta que en 1997 el IEEE incluyó el formato Ethernet II en el estándar IEEE 802.3, por lo que desde entonces ambos formatos de trama forman parte del estándar, pasándose a denominar el campo que marcaba la diferencia como *Longitud / Tipo*. En cualquier caso, la mayor parte de los dispositivos de red en la actualidad utilizan el formato Ethernet II.

La forma en la que las tarjetas de red manejan los dos tipos de tramas es simplemente analizando los dos siguiente bytes de la dirección origen. Si es un número igual o inferior a 1.500 es una trama IEEE 802.3 y este campo indica la longitud de la trama, y si es un número superior a 1.500 (05DC en hexadecimal) es una trama Ethernet II y este campo indica el tipo de protocolo de nivel superior.

Los campos *preámbulo* y *SFD* son campos utilizados para sincronización y realmente no forman parte de la trama. De hecho, las últimas versiones no necesitan estos mecanismos de sincronización y estos campos no son necesarios, aunque se mantienen en el estándar por motivos de compatibilidad.

6.5.3 CONTROL DE ACCESO AL MEDIO: CSMA/CD

Las primeras versiones de Ethernet utilizaron enlaces multipunto en los que varios dispositivos estaban conectados en el mismo enlace (por ejemplo, en la implementación 10BASE-T), por ello fue necesario establecer un mecanismo de arbitraje para resolver el conflicto ocasionado cuando dos equipos quieren acceder al mismo tiempo al medio de transmisión.

Las técnicas utilizadas para esta función se denominan técnicas de **contienda** y se han desarrollado varias a lo largo de la historia. Todas ellas se basan en el tratamiento de un estado que se puede producir en el medio de transmisión llamado colisión. Una **colisión** se produce cuando dos dispositivos transmiten datos simultáneamente. Las señales enviadas por cada dispositivo se mezclan y se pierde la información que contienen.

La técnica de contienda utilizada en Ethernet es **CSMA/CD** (*Carrier Sense Multiple Access with Collision Detection*, acceso múltiple por detección de portadora y con detección de colisiones) y sus principios de funcionamiento son los siguientes:

- ✓ Cuando un equipo quiere transmitir una trama comprueba si el medio de transmisión está libre, es decir, no hay otro dispositivo enviando información. Por lo tanto, si el medio está libre, dicho equipo comienza la transmisión de su trama.
- ✓ Si el medio está ocupado, el equipo espera hasta que quede libre y transmite su trama.
- ✓ Mientras se transmite la trama el equipo comprueba continuamente si se produce alguna colisión.

- ✓ Si se detecta una colisión se deja de transmitir inmediatamente, se espera un tiempo aleatorio y se intenta la transmisión de nuevo.

Solamente se comprueba si hay colisión mientras se transmite la trama, por lo que es importante que los sistemas que utilicen CSMA/CD estén correctamente diseñados para que no se produzcan colisiones después de que el transmisor deje de transmitir. En el caso de Ethernet, esta situación puede ocurrir para la transmisión de tramas muy cortas, por esta razón las tramas Ethernet necesitan un número mínimo de bytes, concretamente 64 bytes, ya que con tramas más pequeñas no se garantizaría la detección correcta de colisiones.

El uso de medios de transmisión compartidos donde es necesario utilizar **CSMA/CD convierte a Ethernet en una tecnología half-dúplex**, ya que solo puede haber una trama simultáneamente en el medio de transmisión.

6.5.4 CONTROL DE ERRORES EN ETHERNET

En las redes Ethernet pueden aparecer diferentes tipos de errores, algunos de ellos relacionados con las colisiones (colisiones atrasadas) y otros relacionados con tamaños incorrectos de trama. Estos errores aparecen de forma esporádica.

Como se ha visto anteriormente, en la trama Ethernet existe un campo llamado FCS utilizado para el control de errores. Los errores detectados con este campo se refieren a errores de transmisión en los datos y normalmente son producidos por tarjetas de red defectuosas, controladores defectuosos o cableado en malas condiciones.

La técnica utilizada para la detección de errores FCS se basa en obtener a partir de un bloque de datos una secuencia de bits, llamada **CRC** (*Cyclic Redundancy Code*, o código de redundancia cíclica). En este caso, el bloque de datos es la propia trama Ethernet, incluida la información de control. Esta secuencia de bits es calculada por el emisor siguiendo un algoritmo determinado y transmitida en el campo FCS de la trama Ethernet. El receptor, cuando recibe los datos, realiza el mismo cálculo. Si el CRC calculado por el receptor coincide con el recibido es que los datos no han sido alterados en la transmisión, es decir, no ha habido errores y por tanto la trama se acepta. Cuando el CRC calculado no coincide con el recibido es que ha habido errores en la transmisión, con lo cual la trama se descarta.

6.6 PRIMERAS ESPECIFICACIONES DEL NIVEL 1 EN ETHERNET

Ya hemos visto como la implementación de muchas de las funciones del nivel 2 desarrolladas en Ethernet se han mantenido a lo largo del tiempo. No ha ocurrido lo mismo con la implementación de las funciones del nivel 1. Es en las funciones del nivel 1, en el que se definen aspectos como tipo de cableado, conectores, velocidad de transmisión y longitud máxima de los cables, etc., donde se ha llevado a cabo la evolución de Ethernet para conseguir adaptarse a las nuevas exigencias de prestaciones de las redes actuales.

Veremos en este apartado un repaso rápido de las primeras especificaciones del nivel físico englobadas todas bajo el nombre genérico de Ethernet. Todas ellas trabajan a una velocidad máxima de 10 Mbps y actualmente se pueden considerar prácticamente obsoletas. A pesar de ello y para tener una perspectiva histórica de las redes Ethernet se expondrán sus principales características.

IMPORTANTE

El nombre de la implementación se descompone en tres partes. La primera indica la velocidad máxima (10 indica 10 Mbps). La segunda parte indica el tipo de transmisión (BASE indica banda base). Y la tercera parte indica la longitud máxima de un segmento (5 indica 500 metros) para las primeras implementaciones o un código referido al tipo de medio de transmisión en las más recientes.

6.6.1 10BASE5 (THICK ETHERNET): ETHERNET DE CABLE GRUESO

Esta implementación física fue la primera utilizada en redes Ethernet y se incluyó en el estándar IEEE 802.3 en 1983, aunque hoy en día no se encuentran redes de este tipo. Sus principales características se detallan a continuación:

- ✓ Utiliza una topología en *bus* físico, es decir, un cable como medio de interconexión común a todos los dispositivos que forman la red.

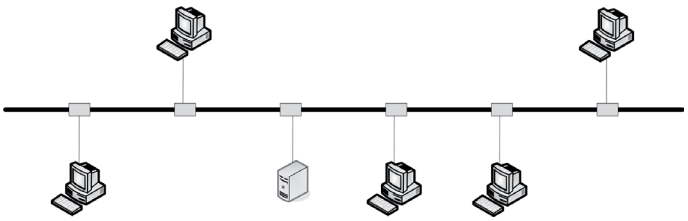


Figura 6.18. *Topología en bus de Ethernet 10BASE5*

- ✓ Se utiliza cable coaxial grueso tipo RG-8 (diámetro externo de 10,2 mm) para implementar el *bus* físico. Aunque la norma no obliga a ello, este cable suele ser de color amarillo.
- ✓ Codificación Manchester en banda base con valores de tensión de +/- 0'85 v.
- ✓ Velocidad de transmisión de 10 Mbps.
- ✓ La longitud máxima permitida de un segmento único de cable coaxial es de 500 metros.
- ✓ La longitud máxima total de una red 10BASE5 es de 2.500 metros. Es decir, un máximo de 5 segmentos de 500 metros de longitud.
- ✓ La separación mínima entre los equipos conectados al *bus* es de 2,5 metros. De hecho, el cable utilizado solía incluir marcas cada 2,5 metros para indicar esta característica. Con esta limitación se pueden conectar en un segmento un máximo de 200 equipos. En una red 10BASE5 puede haber un máximo total de 1.000 equipos.
- ✓ Para la conexión de un equipo a la red se utilizan los llamados transceptores o también **MAU** (*Medium Attachment Unit*, unidad de conexión al medio). Estos dispositivos incluían conectores de tipo vampiro para su conexión con el cable coaxial. El conector vampiro estaba diseñado para atravesar la funda protectora del cable coaxial y establecer contacto eléctrico con el cable propiamente dicho.

✓ Para la conexión del transceptor al equipo se utiliza el llamado cable **AUI** (*Attachment Unit Interface*, interfaz de unidad de conexión). Dicho cable está formado de 15 hilos con conectores DB-15 y puede tener una longitud máxima de 50 metros. Por tanto, las tarjetas de red 10BASE5 incluyen un conector de 15 pines.

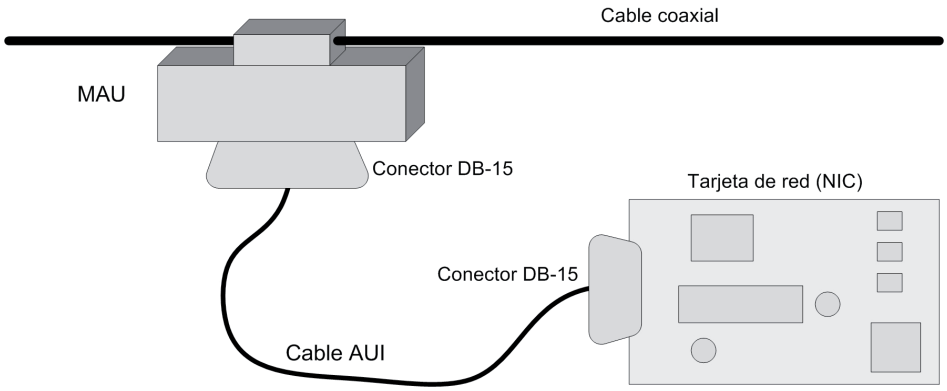


Figura 6.19. *Conexión MAU en redes 10BASE5*

Existen algunas implementaciones más, como por ejemplo **10BROAD36**, **1BASE5** o **10BASE-F**, que tuvieron muy poca repercusión.

6.6.2 10BASE2 (THIN ETHERNET): ETHERNET DE CABLE FINO

Esta segunda implementación de redes Ethernet, publicada por el IEEE en 1985, se desarrolló para ofrecer una alternativa a menor coste que 10BASE5. Actualmente está prácticamente en desuso. En este caso, como indica su nombre, se mantiene la velocidad y el tipo de transmisión, pero se ve reducida la longitud máxima de un segmento a 200 metros (realmente se hace un redondeo para acortar el nombre, pero la longitud exacta es de 185 metros). Sus principales características son:

✓ Utiliza una topología en *bus* físico al igual que 10BASE5.

✓ Utiliza cable coaxial fino de tipo RG-58 (diámetro externo de 5 mm) para implementar el *bus* físico.

✓ Al igual que en 10BASE5 la velocidad de transmisión es de 10 Mbps y se utiliza codificación Manchester en banda base con valores de tensión de +/- 0,85 v.

✓ La longitud máxima de un segmento es de 185 metros, con un máximo de 30 equipos por segmento de cable.

✓ No se utilizan transceptores. Se conecta el equipo directamente al *bus* utilizando un conector BNC-T, que es un conector con forma de T y con tres puertos: uno para la tarjeta de red y los otros dos para la entrada y salida del cable de red. Por tanto, las tarjetas de red 10BASE2 incluyen un conector BNC.

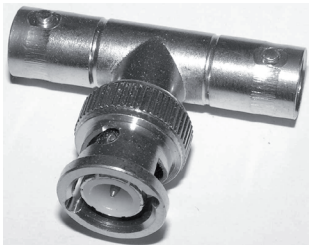


Figura 6.20. *Conector BNC-T utilizado en las redes 10BASE2*

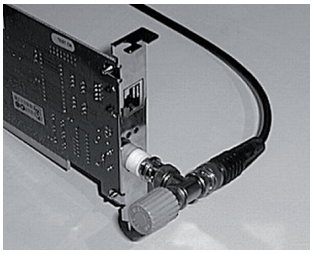


Figura 6.21. *Conexión de una tarjeta de red 10BASE2*

6.6.3 10BASE-T: ETHERNET DE PAR TRENZADO

Las implementaciones Ethernet anteriores tenían varios inconvenientes. Además de que su implantación requería una alta inversión inicial, el mantenimiento posterior también suponía una fuente de problemas. En este tipo de redes, las roturas de cables o malas derivaciones eran difíciles de detectar y afectaban al rendimiento de la red entera.

En este escenario el IEEE publicó en 1990 la implementación 10BASE-T (la letra T es de *twisted*, trenzado), basada en un elemento central donde se implementa un *bus* lógico, pero utilizando una topología física en estrella. Las uniones entre cada equipo y el elemento central se realizan utilizando cable de par trenzado de categoría 3. Muchos edificios disponían de una infraestructura con este tipo de cable para dar servicio telefónico, por lo que se podía aprovechar para implementar las redes 10BASE-T. La topología en estrella favoreció su mantenimiento, ya que los problemas en una sección de cable solo afectarían al equipo al que daba servicio. En definitiva, esta implementación Ethernet era la más barata y la más fácil de mantener, por lo que se convirtió rápidamente en la más popular.

Paralelamente al desarrollo de los estándares para redes locales se desarrollaron normativas de cableado de telecomunicaciones para edificios comerciales que permiten constituir lo que se conoce como **cableado estructurado**. Las primeras normas de cableado estructurado fueron publicadas como **EIA/TIA 568** en 1991. Esta circunstancia propició aún más el despliegue de redes 10BASE-T. Actualmente las dos normativas más utilizadas en cableado estructurado son la EIA/TIA 568-A y la ISO/IEC 11801, publicadas en 1995. A continuación se enumeran las principales características de 10BASE-T:

✓ La topología física es en estrella física, aunque a nivel lógico se sigue comportando como un *bus*.

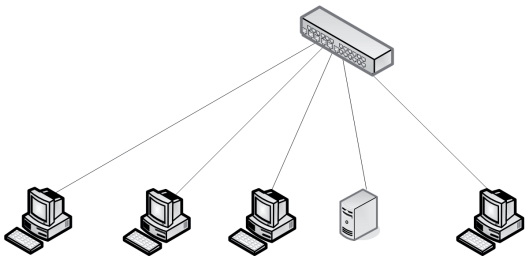


Figura 6.22. *Topología en estrella física en 10BASE-T*

- ✓ Se utiliza cable de par trenzado sin apantallar (UTP) de categoría 3 o superior. Las categorías de cables están definidas en la norma EIA/TIA 568.
- ✓ Los cables UTP utilizados son de cuatro pares (ocho conductores) con conectores RJ-45 en ambos extremos. De estos cuatro pares solo se utilizan dos.

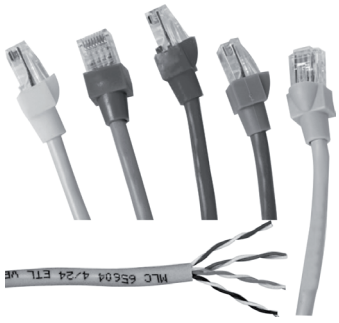


Figura 6.23. *Cable UTP con conectores RJ-45*

- ✓ La velocidad de transmisión es de 10 Mbps.
- ✓ La codificación utilizada es Manchester en banda base con valores de tensión de +/- 5 v.
- ✓ Todas las operaciones de red se sitúan en un dispositivo de red llamado **concentrador** o **hub**, el cual tiene un puerto de entrada de tipo RJ-45 por cada equipo. Todos los equipos de la red se conectan al *hub*. En el interior del *hub* se implementa un *bus* lógico.

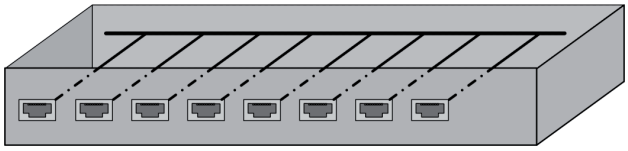


Figura 6.24. *Implementación de un bus lógico en un hub*

- ✓ La longitud máxima del cable entre un equipo y el *hub* es de 100 metros. Esta limitación viene impuesta por las características físicas del cable de par trenzado, de calidad inferior al cable coaxial.
- ✓ El *hub* retransmite todas las tramas recibidas a los equipos que están conectados al mismo. Cada tarjeta de red comprueba si la trama le pertenece comprobando la dirección de destino. Si no coincide con la dirección física la trama se desecha. Con este modo de operación la topología lógica sigue siendo en *bus*, ya que cualquier trama enviada por un equipo se propagará por el resto de equipos. Lógicamente se seguirán produciendo colisiones.

El *hub* o concentrador es el elemento central de las redes 10BASE-T. Retransmite la trama recibida por un puerto al resto de los puertos.

6.7 EL ESTÁNDAR MÁS CONSOLIDADO: FAST ETHERNET

El rápido crecimiento y utilización de las redes Ethernet produjo a su vez un aumento de los requerimientos de velocidad. Las redes Ethernet estaban formadas cada vez por más equipos y las transferencias de información a través de las mismas también iban en aumento.

La solución adoptada por el IEEE fue **Fast Ethernet**, publicada en 1995 como **IEEE 802.3u**. Su principal característica es el aumento de la velocidad de transmisión de 10 a 100 Mbps.

Fast Ethernet utiliza la especificación 10BASE-T como referencia, de forma que se intenta mantener las características de ésta. Por ejemplo, se mantiene la topología en estrella física y lógica en *bus*, se sigue utilizando CSMA/CD como método de acceso al medio y se mantiene el formato de la trama.

Para dar diferentes alternativas en función de los medios de transmisión disponibles, el IEEE publicó tres alternativas de redes Fast Ethernet que se verán a continuación.

6.7.1 100BASE-TX

Esta versión de Fast Ethernet es la que se ha impuesto y actualmente es uno de los tipos de redes más utilizados.

Uno de los cambios necesarios en esta implementación es el tipo de cable. Se utiliza cable de cobre de par trenzado sin blindaje (UTP) de categoría 5. La principal diferencia entre categoría 3 y categoría 5 es la frecuencia máxima, que lógicamente debe ser mayor en categoría 5. Se utilizan dos pares, uno para transmisión y otro para recepción, de forma que este tipo de redes admite operaciones full-dúplex (esta característica se verá en el próximo apartado). La distancia máxima entre un equipo y el *hub*, al igual que en 10BASE-T, es de 100 metros.

Se utilizan las codificaciones 4B/5B y MLT-3. La **codificación MLT-3** (*Multilevel Transmit-Three Levels*, transmisión multinivel-tres niveles) es parecida a NRZ-I, pero utilizando tres niveles diferentes en lugar de dos: positivo, negativo y cero. Un valor 0 lógico se codifica sin cambio de nivel y un valor 1 lógico con cambio de nivel. Esta codificación tiene el mismo problema que NRZ-I, puede producir pérdidas de sincronismo ante secuencias largas de ceros. Para solucionarlo se utiliza la **codificación 4B/5B** aplicada antes de la codificación MLT-3. En 4B/5B cada grupo de 4 bits se convierte a un código de 5 bits especialmente preparado para que no se produzcan combinaciones largas de ceros. De hecho, una secuencia de datos codificados en 4B/5B no contiene nunca secuencias de más de tres ceros. Además, algunas de las combinaciones sobrantes se utilizan para funciones de control.

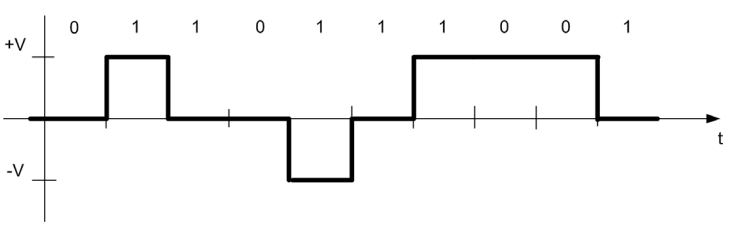


Figura 6.25. *Ejemplo de codificación MLT-3*

Binario	4B/5B	Binario	4B/5B
0000	11110	1000	10010
0001	01001	1001	10011
0010	10100	1010	10110
0011	10101	1011	10111
0100	01010	1100	11010
0101	01011	1101	11011
0110	01110	1110	11100
0111	01111	1111	11101

Resumen de características de 100BASE-TX:

- ✓ Velocidad de transmisión 100 Mbps.
- ✓ Topología física en estrella y lógica en *bus* con modo de transmisión half-dúplex.
- ✓ Necesidad de un elemento de interconexión central (*hub*).
- ✓ Cableado UTP de categoría 5, cada enlace puede tener una distancia máxima de 100 metros.
- ✓ Conectores RJ-45.
- ✓ Codificación 4B/5B y codificación de línea MLT-3.

El uso de la codificación 4B/5B hace que por el cable de red viajen los datos realmente a 125 Mbps.

6.7.2 100BASE-FX

Esta versión de Ethernet, al igual que la siguiente, no ha tenido mucha repercusión y actualmente no hay muchas redes que la utilicen. Sus principales características son:

- ✓ Utiliza como medio de transmisión fibra óptica multimodo.
- ✓ Utiliza conectores SC o ST.
- ✓ La codificación utilizada es 4B/5B y NRZ-I. Elegida por compatibilidad con las redes FDDI.
- ✓ La Distancia máxima entre el concentrador y un equipo es de 2.000 metros en modo full-dúplex.

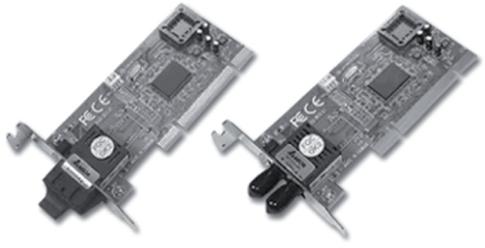


Figura 6.26. *Tarjetas de red 100BASE-FX*

6.7.3 100BASE-T4

Esta versión de Fast Ethernet se especificó para dar la opción de aprovechar cableado instalado de categoría 3. Aunque, al igual que la anterior, no tuvo mucha penetración en el mercado.

- ✓ Utiliza cables de par trenzado categoría 3. Sin embargo, utiliza cuatro pares en lugar de dos para repartir el flujo de datos a 100 Mbps en tres de 33,3 Mbps. Dos de los pares utilizados se utilizan en modo half-dúplex, por lo que este tipo de redes no admite operaciones full-dúplex.
- ✓ La distancia máxima entre un equipo y el *hub*, al igual que en 100BASE-TX, es de 100 metros.
- ✓ Utiliza codificaciones 8B/6T y NRZ-I. La codificación 8B/6T sustituye un grupo de 8 bits en seis símbolos ternarios, es decir, se utilizan tres niveles de tensión diferentes en lugar de dos.

6.8 MEJORANDO ETHERNET: ETHERNET CONMUTADA Y FULL-DÚPLEX

Las redes Ethernet conmutadas se basan en la utilización como elemento central de la topología física en estrella un *switch* o conmutador en lugar de un *hub*.

Un ***switch*** o **conmutador** es un dispositivo de interconexión que posee varios puertos de entrada, normalmente de tipo RJ-45. Externamente es parecido a un *hub*, sin embargo, y a diferencia de éste, un *switch* es capaz de leer las tramas Ethernet que recibe por cualquiera de sus puertos, analizar la dirección física de destino y reenviar la trama solo al puerto donde esté conectado el equipo con dicha dirección. Es decir, no hace una simple difusión de las señales eléctricas al resto de puertos. De esta forma se reduce drásticamente el número de colisiones. En un apartado posterior, en el capítulo 7 se verán en detalle las características más importantes de los *switches*.

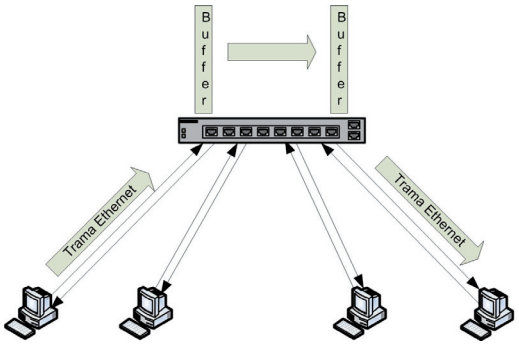


Figura 6.27. *En la Ethernet conmutada no se produce difusión de las tramas en el switch*

La otra característica interesante que añaden los *switches* es que permiten comunicación full-dúplex. Para que este funcionamiento sea posible tanto la tarjeta de red (NIC) como el *switch* deben estar diseñados para ello. En el modo de funcionamiento full-dúplex no se utiliza el método de acceso al medio CSMA/CD por ser innecesario, ya que la conexión de cada NIC al *switch* utiliza un canal dedicado por cada sentido de la comunicación.

RECUERDA

En modo full-dúplex no es necesario utilizar el método CSMA/CD de acceso al medio, ya que cada conexión equipo-*switch* se comporta como una línea punto a punto.

El modo de funcionamiento full-dúplex está definido dentro del estándar IEEE en la especificación **IEEE 802.3x** (publicada en el año 1997), donde además se incluye un método de **control de flujo**. Esto es necesario, ya que es posible que un dispositivo transmita tramas más rápido de lo que el receptor puede procesarlas, lo que provocaría pérdidas de información. Este control de flujo se implementa mediante el envío de una trama de control llamada **trama PAUSE** desde el receptor, donde le indica al emisor el tiempo que debe permanecer sin enviar datos. Durante el tiempo de inactividad el receptor puede volver a enviar *tramas PAUSE* para prolongar, reducir o suprimir la pausa inicial. Las *tramas PAUSE* se identifican porque contienen el valor 8808 (hexadecimal) en el campo *Tipo*.

El buen funcionamiento de esta operación depende sobre todo de lo rápido que se identifiquen las tramas de control de flujo. El Comité IEEE comprobó que el formato Ethernet original era el más adecuado para este propósito, ya que permitía identificar las tramas de control de flujo mediante el campo *Tipo*, mientras que en el formato IEEE esta información debe incluirse en la trama LLC. Por tanto, IEEE decidió estandarizar el formato de trama Ethernet. Este formato forma parte del estándar desde 1997 utilizando el campo *Tipo*/*Longitud* para distinguir el tipo de trama utilizado.

El ancho de banda efectivo de las redes que utilizan el modo full-dúplex se duplica respecto al modo half-dúplex. Así, una red half-dúplex funcionando a 100 Mbps aumentará su velocidad a 200 Mbps si utiliza el modo full-dúplex, ya que cada equipo conectado podrá tener un flujo máximo de información de 100 Mbps en un sentido y otros 100 Mbps en el sentido contrario de forma simultánea.

RECUERDA

A partir de la versión IEEE 802.3x publicada en 1997 se incluye en el estándar el formato de trama Ethernet II, por tanto, en la actualidad, ambos formatos de trama están incluidos en el estándar. El más utilizado es el formato Ethernet II (también conocido como DIX), principalmente por reducir la sobrecarga, eliminando la cabecera LLC.

Una de las características incluidas en la especificación IEEE 802.3u fue la capacidad de **autonegociación** entre *switch* y los equipos para determinar principalmente dos características, la velocidad de transmisión 10/100 Mbps y el modo de transmisión half-dúplex o full-dúplex.

La mayor parte de los dispositivos de interconexión admiten esta característica, de forma que la comunicación entre los mismos y los equipos de la red es autoconfigurable de forma transparente al usuario.

El controlador de la tarjeta de red suele tener la posibilidad de configurar las características de la tarjeta en modo autoconfiguración o se puede forzar un modo determinado de funcionamiento.

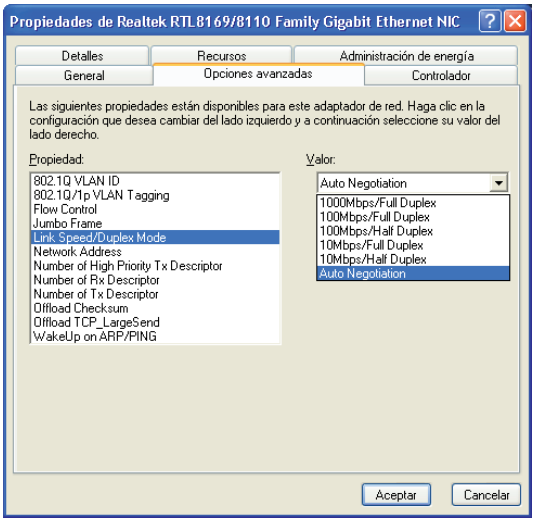


Figura 6.28. *Configuración del modo de funcionamiento de la tarjeta de red en Windows XP*

6.9 MÁS VELOCIDAD: GIGABIT ETHERNET Y 10-GIGABIT ETHERNET

Entre los años 1998 y 1999 el IEEE amplió el estándar IEEE 802.3 para incluir un nuevo tipo de redes, llamado de forma genérica **Gigabit Ethernet**. Este estándar se desarrolló bajo dos especificaciones: la primera, desarrollada en 1998, llamada **IEEE 802.3z** o también **1000BASE-X**, que utiliza fibra óptica. La segunda, desarrollada en 1999, llamada **IEEE 802.3ab**, también conocida como **1000BASE-T**, que utiliza cable de cobre de par trenzado. La principal característica de Gigabit Ethernet es que la velocidad de transmisión es de 1.024 Mbps o 1 Gbps.

1000BASE-X está basado en la utilización de fibra óptica como medio de transmisión. Además utiliza las especificaciones a nivel físico del estándar **Fiber Channel** (ANSI X3 T11), pero mantiene la compatibilidad con Ethernet en el nivel de enlace. La arquitectura Fiber Channel utiliza cuatro capas, aunque la especificación 1000BASE-X utiliza solo las dos primeras, llamadas FC-0 y FC-1.

6.9.1 1000BASE-T

El estándar 1000BASE-T permite la transmisión de datos a 1 Gbps o 1.024 Mbps utilizando cable UTP, pero manteniendo todas las funciones de Ethernet del nivel 2.

El estándar permite el uso de cable UTP de categoría 5 que cumpla la norma EIA/TIA 568, revisada en 1995. Para cableado de categoría 5 anterior a este año (y que siguiera la norma original EIA/TIA 568 publicada en 1991) no se recomienda su uso en 1000BASE-T. Para simplificar la adopción de criterios de cableado en muchas ocasiones se recomienda el uso de cable UTP de categoría 5e (5 mejorado) o superior.

El diseño de 1000BASE-T planteó algunos problemas, además del aumento de la complejidad de los circuitos digitales en las tarjetas de red. En primer lugar, cada uno de los pares de un cable de categoría 5 permite transmitir datos a una velocidad de 125 Mbps. Para aumentar la velocidad de transmisión, en 1000BASE-T se utilizan los cuatro pares del cable, tanto para la transmisión como para la recepción. La transmisión de los dos sentidos de la comunicación por los mismos pares es posible gracias a la utilización de técnicas de cancelación de eco. De esta forma, se lograría una velocidad de 500 Mbps. Para llega a 1 Gbps se utiliza una técnica de modulación por amplitud de pulso que utiliza cinco niveles para la cuantificación llamada **PAM-5**. Después de este tratamiento y para el envío de la señal en banda base se utiliza codificación **8B/10B**.

El segundo gran problema planteado en Gigabit Ethernet es debido al uso de CSMA/CD y está relacionado con el tamaño mínimo de la trama, que es de 64 bytes. Debido al aumento de velocidad en Gigabit Ethernet, las tramas más pequeñas se transmiten tan rápido que no es posible detectar colisiones. Para solucionarlo es necesario aumentar el tamaño mínimo de las tramas y esto se consigue añadiendo un campo de relleno llamado **extensión de portadora** (*carrier extension*), que se añade al final de la trama para garantizar que la longitud mínima nunca será inferior a 512 bytes (4.096 bits), que es el tamaño mínimo necesario para detectar las colisiones en Gigabit Ethernet.

Esta solución repercute negativamente en la eficiencia de la red cuando se transmiten muchas tramas pequeñas, ya que una gran parte del ancho de banda se emplea en transmitir bits de relleno y no información. Para paliar en parte este efecto, se permite agrupar varias tramas pequeñas en lo que se conoce como **modo ráfaga** (*frame bursting*), en el cual se pueden enviar varias tramas pequeñas consecutivas, sin necesidad de utilizar *carrier extension*, hasta un máximo de 65.536 bits.

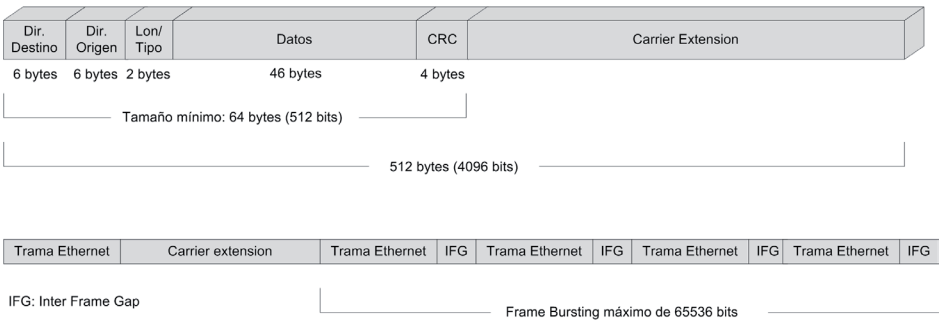


Figura 6.29. *Extensión de portadora y modo ráfaga en Gigabit Ethernet*

Gigabit Ethernet puede funcionar tanto en modo half-dúplex como en modo full-dúplex. En modo half-dúplex se sigue usando el método CSMA/CD de acceso al medio como en las implementaciones anteriores de 10 y 100 Mbps. En modo full-dúplex, al no utilizarse CSMA/CD, tampoco es necesario utilizar el relleno de portadora o *carrier extension* ni el modo ráfaga. De hecho, en la práctica casi todos los sistemas que utilizan Gigabit Ethernet lo hacen en modo full-dúplex.

En resumen, las principales características de 1000BASE-T son:

- ✓ Cable de cobre de par trenzado categorías 5e o 6.
- ✓ Velocidad de transmisión: 1.024 Mbps o 1 Gbps.
- ✓ Longitud máxima del cable: 100 metros.
- ✓ Técnica de transmisión PAM-5 con codificación 8B/10B.
- ✓ Transmisión half-dúplex o full-dúplex.

6.9.2 1000BASE-X

Las implementaciones 1000BASE-X utilizan como medio de transmisión la fibra óptica. A continuación se proporcionan las principales características de los dos tipos de implementaciones 1000BASE-X publicadas:

- 1000BASE-SX
  - Emplea las codificaciones 8B/10B y NRZ-I.
  - Se utiliza fibra óptica multimodo.
  - La distancia máxima es de 275 metros para fibra de 62,5/125 µm o de 550 metros para fibra de 50/125 µm.
- 1000BASE-LX
  - Emplea las codificaciones 8B/10B y NRZ-I.
  - Se utiliza tanto fibra óptica monomodo como multimodo.
  - La distancia máxima para fibra multimodo es de 550 metros o de 5 km para fibra monomodo.

Ambas implementaciones de Gigabit Ethernet son utilizadas en modo full-dúplex principalmente para dar soporte al troncal (*backbone*) de las redes Ethernet de mediana o gran envergadura.

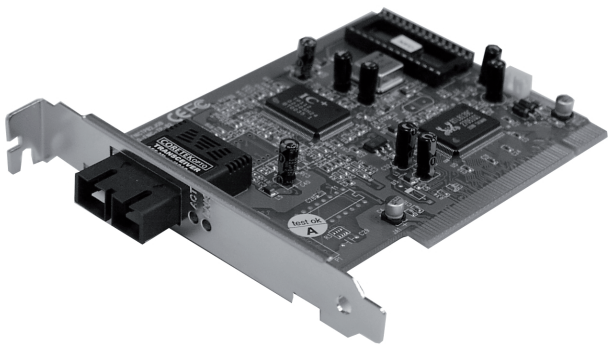


Figura 6.30. *Tarjeta Gigabit Ethernet con conectores SC*

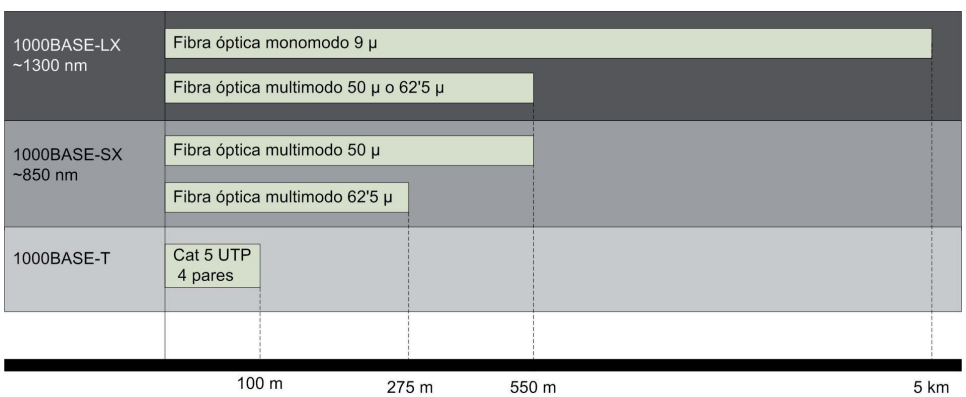


Figura 6.31. *Distancias máximas en Gigabit Ethernet*

Implementación	Estándar IEEE	Año	Velocidad (Mbps)	Codificación	Tipo de cable	Full-dúplex
10BASE-T	802.3i	1990	10	Manchester	UTP Cat.3	Sí*
100BASE-TX	802.3u	1995	100	4B/5B y MLT-3	UTP Cat.5	Sí*
100BASE-FX	802.3u	1995	100	4B/5B y NRZ-I	Fibra óptica	Sí*
100BASE-T4	802.3u	1995	100	8B/6T y NRZ-I	UTP Cat.3	No
1000BASE-T	802.3ab	1999	1000	PAM-5 y 8B/10B	UTP Cat.5, 5e o 6	Sí
1000BASE-X	802.3z	1998	1000	NRZ-I y 8B/10B	Fibra óptica	Sí

*El modo full-dúplex no está especificado en el estándar original. Este modo es admitido a partir del estándar IEEE 802.3x en el año 1997.

6.9.3 10-GIGABIT ETHERNET

En el año 2002 se publicó un nuevo estándar llamado **10-Gigabit Ethernet** (IEEE 802.3ae), abreviado como 10GbE, y que funciona a velocidades de 10 Gbps sobre fibra óptica. Las implementaciones físicas que incluye el estándar IEEE 802.3ae son:

- **10GBASE-SR**, utiliza fibra óptica multimodo para distancias de hasta 300 metros.
- **10GBASE-LR**, utiliza fibra óptica monomodo para distancias de hasta 10 km.
- **10GBASE-LX4**, utiliza multiplexación por división de onda (WDM) tanto para fibra óptica multimodo como monomodo.
- **10GBASE-ER**, utiliza fibra monomodo para cubrir distancias de hasta 30 km.
- **10GBASE-SW**, **10GBASE-LW**, **10GBASE-EW**, son similares a las implementaciones SR, LR y ER, pero con la posibilidad de interconectarse con equipos que utilicen estándares sobre fibra óptica de redes WAN.

Posteriormente han aparecido algunas ampliaciones del estándar 10-Gigabit Ethernet:

- **10GBASE-LRM** (IEEE 802.3aq). Publicada en 2006 para proporcionar compatibilidad con el cableado de las redes FDDI.
- **10GBASE-CX4** (IEEE 802.3ak). Publicada en 2004. Es la primera especificación de 10-Gigabit Ethernet que utiliza cable de cobre (un tipo especial llamado InfiniBand) con una longitud máxima de 15 metros.
- **10GBASE-T** (IEEE 802.3an). Publicada en 2006. Utiliza cable de cobre de categoría 6a para cubrir una distancia máxima de 100 metros.

IMPORTANTE

InfiniBand es una interfaz de comunicaciones punto a punto de altas prestaciones cuyas primeras especificaciones fueron desarrolladas por varias empresas entre las que se encuentran Intel, AMD, Sun, IBM, Dell, Cisco o Silicon Graphics y que se publicaron en el año 2000.

El desarrollo de la tecnología 10-Gigabit Ethernet se ha enfocado principalmente al uso de Ethernet para redes WAN, gracias sobre todo a las distancias cubiertas por las especificaciones que utilizan fibra óptica. Por lo tanto, se puede decir que la evolución de Ethernet está enfocada a introducirse como tecnología en redes WAN. Uno de los principales reclamos es la posibilidad de que los operadores de telecomunicaciones puedan ofrecer a sus clientes conectividad Ethernet de extremo a extremo con el ahorro en costes y la simplicidad de gestión que ello supone.

6.10 ASIGNACIÓN DE PINES EN UTP PARA ETHERNET: CABLE DIRECTO Y CRUZADO

Como se ha visto anteriormente, los estándares 10BASE-T y 100BASE-TX utilizan cable UTP de cuatro pares, de los cuales se utilizan dos, uno para transmisión y otro para recepción. En los estándares de cable UTP para Gigabit Ethernet y 10-Gigabit Ethernet, sin embargo, fue necesario utilizar los cuatro pares simultáneamente tanto en recepción como en transmisión.

La asignación de pines en el cable UTP y su correspondiente conector RJ-45 (su nombre formal es **8P8C**) sigue el estándar **EIA/TIA 568** de cableado estructurado. Realmente en este estándar hay dos asignaciones, conocidas como **T568A** y **T568B**. La asignación T568B es la más reciente y la más utilizada en la actualidad. Estas asignaciones siguen un código de colores utilizado en la cubierta plástica de cada hilo de un cable UTP. El uso habitual es la conexión de un equipo (a través de su tarjeta de red o NIC) a un *switch*. En este caso, el par utilizado por el equipo para transmitir es asignado como *par de recepción* en el *switch*, y el par de recepción en el equipo será el *par de transmisión* en el *switch*.

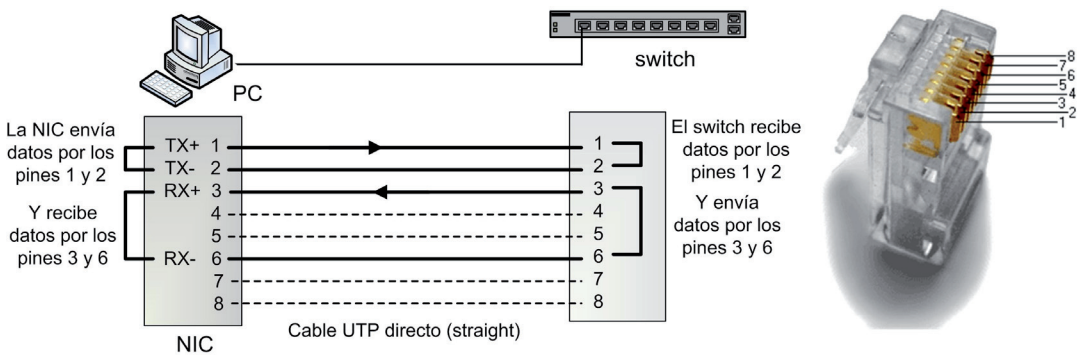


Figura 6.32. *Conexión entre una NIC y un switch mediante cable UTP*

Los cables UTP utilizados en redes Ethernet con la configuración anterior se conocen como **cable UTP directo**. La mayor parte de los cables utilizados en redes Ethernet siguen esta configuración y se utilizan para conectar un equipo de red (a través de su NIC) a un dispositivo de interconexión, típicamente un *switch*. Sin embargo, existe un caso en el que este tipo de cable no funcionará y es cuando sea necesario conectar dos *switches* entre sí.

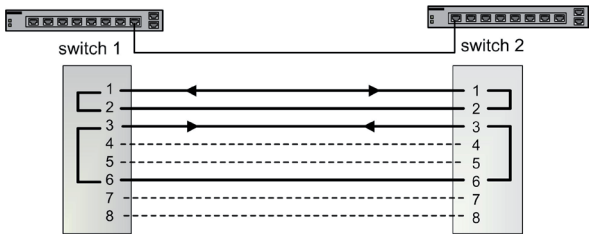


Figura 6.33 *Conexión entre dos switches utilizando un cable UTP directo*

Como se observa en la figura anterior, al conectar dos *switches* utilizando la configuración de un cable UTP directo, los dos *switches* intentan transmitir por el mismo par (por los pines 3 y 6), por lo que sus datos "colisionarán". Además intentarán recibir datos por el mismo par (por los pines 1 y 2). Para solucionar este problema se utiliza una configuración llamada **cable UTP cruzado**, que consiste en cruzar los pares de transmisión y recepción.

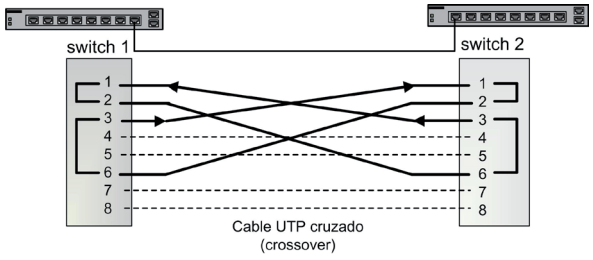


Figura 6.34 *Conexión entre dos switches utilizando un cable UTP directo*

La configuración de cable UTP cruzado también se puede utilizar para conectar dos tarjetas de red Ethernet directamente sin utilizar un *switch*. Esta característica puede ser útil cuando queramos conectar dos equipos y no tengamos un *switch*.

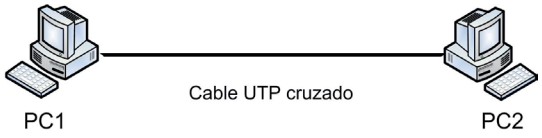


Figura 6.35 *Conexión entre dos PC utilizando un cable UTP cruzado*

La función de los pares en una tarjeta de red se conoce formalmente como **MDI** (*Medium Dependent Interface*), y la función de los pares en un dispositivo de interconexión como un *switch* (o como en los antiguos *hubs*) se conoce como **MDI-X** (*Medium Dependent Interface Crossover*).

Para evitar el uso de cable UTP cruzado algunos modelos de *hubs* incluían un puerto especial que podía ser configurado como MDI (si se iba a conectar a otro *hub*) o como MDIX (si se iba a conectar a un PC). Posteriormente se han desarrollado puertos que detectan automáticamente qué tipo de configuración necesitan para funcionar correctamente con el dispositivo al que esté conectado, esta característica se conoce como **puerto Auto MDI/MDI-X**.

EJERCICIOS PROPUESTOS

1. Representa gráficamente la señal eléctrica producida por una tarjeta de red 100BASE-TX para el envío del dato 010100000011.

2. Con un capturador de tramas se ha obtenido la siguiente información, expresada en formato hexadecimal. No se incluye el preámbulo y el byte de comienzo de trama.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00	FF	FF	FF	FF	FF	FF	00	00	48	B7	E7	B2	00	2B	E0	E0
16	03	FF	FF	00	28	00	01	00	00	00	00	FF	FF	FF	FF	FF
32	FF	04	53	00	00	00	00	00	00	48	B7	E7	B2	57	FD	00
48	01	FF	FF	FF	FF	00	00	00	00	00	00	00	B3	78	12	C9

- ¿De qué tipo de trama se trata? Obtén los valores de todos los campos de la cabecera y su función.

3. Repite el ejercicio anterior con las siguientes capturas:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00	00	A0	C5	38	70	70	00	13	8F	73	76	DA	08	00	45	00
16	00	28	AA	99	40	00	80	06	81	42	0A	0C	02	0D	D4	AA
32	EE	30	09	FE	00	50	BD	B2	FF	5E	7B	EB	A8	89	50	10
64	44	70	B0	9B	00	00	00	00	00	00	00	00	F6	A1	06	BA

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00	00	13	8F	73	76	DA	00	20	EA	2F	E5	EE	81	00	00	03
16	08	06	00	01	08	00	06	04	00	02	00	20	EA	2F	E5	EE
32	AC	00	00	01	00	13	8F	73	76	DA	AC	A8	64	0D	88	88
64	88	88	88	88	88	88	88	88	88	88	88	88	4A	26	09	C4

4. Obtén información sobre las tramas Jumbo.

5. Algunos fabricantes de equipos de red ofrecen unos dispositivos llamados **conversores de medios**. Obtén información sobre su función en las redes Ethernet, así como sus principales características. Incluye información de dos modelos concretos de conversores.

TEST DE CONOCIMIENTOS

1 La dirección MAC de las tarjetas de red Ethernet las configura:
- **a)** El usuario del equipo.
- **b)** El administrador de la red.
- **c)** Cualquier usuario con permisos de administración.
- **d)** No se puede cambiar.

2 La diferencia entre una trama Ethernet II y una trama IEEE 802.3 es:
- **a)** El tercer campo de la cabecera es el Tipo en Ethernet, y la Longitud en IEEE 802.3.
- **b)** No hay diferencia en la trama MAC, la diferencia es que la trama IEEE 802.3 encapsula una trama LLC.
- **c)** Las direcciones de la trama Ethernet son de 6 bytes y en IEEE 802.3 son de 2 bytes.
- **d)** La trama Ethernet necesita una longitud mínima de los datos de 46 bytes y la trama IEEE 802.3 no.

3 En las redes 100BASE-TX se utiliza la codificación:
- **a)** Manchester.
- **b)** Manchester diferencial.
- **c)** MLT-3 junto con la codificación binaria 4B/5B.
- **d)** NRZ-I junto con la codificación binaria 4B/5B.

4 El modo de operación full-dúplex:
- **a)** No funciona utilizando un *hub*.
- **b)** No necesita CSMA/CD.
- **c)** Se puede utilizar tanto en Fast Ethernet como en Gigabit Ethernet.
- **d)** Todas las anteriores son correctas.

5 Una de las características de funcionamiento de CSMA/CD es que:
- **a)** Se pueden configurar los dispositivos con una mayor prioridad de transmisión.
- **b)** Una señal de congestión indica que se ha borrado la colisión y que los medios no se encuentran ocupados.
- **c)** Antes de transmitir, un dispositivo escucha y espera hasta que los medios no se encuentren ocupados.
- **d)** Cuando ocurre una colisión, el dispositivo manda una trama de error a los niveles superiores.

6 ¿Cuál de las siguientes es un ejemplo de dirección MAC de nivel 2?
- **a)** 192.201.63.251
- **b)** 19-22-01-63-25
- **c)** 0000.1234.FEG
- **d)** 00-00-12-34-FE-AA

7 ¿Cuáles de los enlaces siguientes soportan una conexión Ethernet Full Duplex?

a) *Switch* a PC.
b) *Hub* a *hub*.
c) *Switch* a *hub*.
d) *Hub* a PC.

8 La conmutación en Ethernet:

a) Proporciona mayor velocidad a la conexión a Internet.
b) Permite la conexión de un número mayor de equipos.
c) Permite el uso del modo full-dúplex.
d) Permite el uso del estándar Gigabit Ethernet.

9 Cuando una tarjeta de red detecta una trama con errores utilizando la información del campo FCS:

a) Descarta la trama.
b) Pide la retransmisión de la trama.
c) Notifica del error al nivel superior.
d) Gracias a CSMA/CD no puede haber errores.

10 La característica de autonegociación incluida en el estándar IEEE 802.3u permite la negociación automática de:

a) El tipo de trama.
b) La velocidad.
c) El modo de transmisión half-dúplex o full-dúplex.
d) Tanto el modo de transmisión como la velocidad.

7 Equipos de interconexión de red

7.1 FUNCIONES Y MODELO DE REFERENCIA OSI

En las redes actuales los equipos de interconexión más extendidos son los *switches* y los *routers*. Cada uno de ellos lleva a cabo su función de interconexión en diferentes niveles del modelo OSI. Así, los *switches*, llevan a cabo la interconexión de equipos en el nivel 2 del modelo OSI. Los *routers* llevan a cabo la interconexión de equipos en el nivel 3 del modelo OSI.

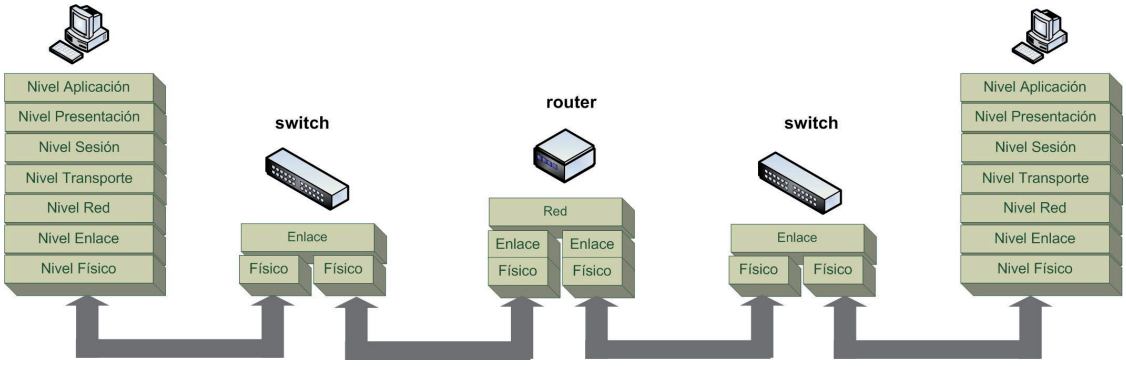


Figura 7.1 *Modelo OSI y los niveles de interconexión*

Como se vio en el capítulo anterior, los *switches* se utilizan como dispositivo de interconexión en las redes Ethernet conmutadas, de hecho, se puede decir que el *switch* es el elemento de interconexión estándar en las redes locales actuales. La gran mayoría de las redes locales actuales utilizan *switches*. Sin embargo, para la interconexión de dos o más redes son necesarios otros dispositivos que llevan a cabo las funciones del nivel 3, estos dispositivos son los *routers*.

Se podría decir que los *switches* sirven para unir equipos (dentro de una red LAN) y los *routers* sirven para unir redes.

7.2 *ROUTERS*

El direccionamiento IP permite disponer de rangos de direcciones asignados a diferentes redes interconectadas entre sí. Para poder interconectar dos o más redes es necesario el uso de un dispositivo de interconexión llamado *router* o encaminador.

Un **router** es un dispositivo de interconexión utilizado para unir redes y encaminar el tráfico entre ellas. La arquitectura de la interconexión de redes está basada fundamentalmente en el uso de estos dispositivos.

Los *routers* están conectados a dos o más redes lógicas diferentes, por tanto, un *router* debe tener una interfaz de red por cada red a la que está conectado, y cada una de las interfaces de red del *router* deberá tener asignada una dirección IP válida en cada una de las redes.

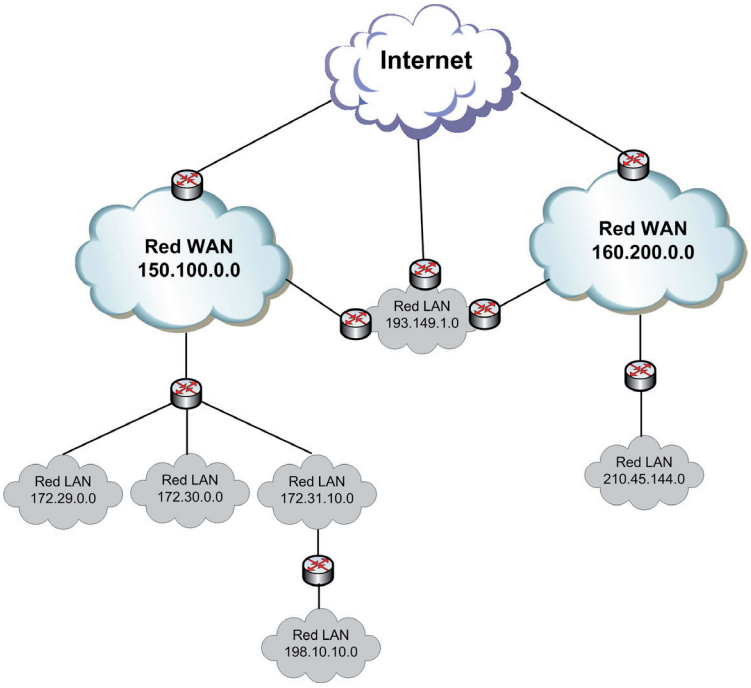


Figura 7.2. *Interconexión de redes IP mediante routers*

En la figura anterior se puede observar la interconexión de redes IP utilizando *routers* y formando con ello una estructura jerárquica de redes que en última instancia es lo que forma Internet. En la figura se observa como uno de los *routers* está conectado a cuatro redes distintas, por lo que deberá tener asignada una dirección IP por cada red. El caso más sencillo es la interconexión de dos redes. En este caso el *router* posibilita el intercambio de tráfico entre las redes a las que está conectado.

Uno de los principales usos de los *routers* es unir redes de diferentes tecnologías, por ejemplo, los *routers* que unen una red LAN con una red WAN. El ejemplo más común sería el *router* que proporcionan los ISP para proporcionar conexión a Internet a sus clientes. Dicho *router* se encarga de unir la red del cliente (red LAN, habitualmente con tecnología Ethernet) con la red del ISP (red WAN que utiliza como tecnología de acceso ADSL, cable o incluso 3G inalámbrico).

En topologías más complejas es necesario utilizar *routers* conectados a más de dos redes, en este caso los *routers* deben llevar a cabo un procesamiento más complejo de la información para decidir el interfaz de red por el que debe encaminar cada datagrama. Para ello se utilizan los algoritmos y protocolos de encaminamiento vistos en el capítulo 5. Por tanto, pueden existir dos tipos de *routers*: los *routers* de acceso y los *routers* de distribución, ambos se estudian en los dos próximos apartados.

7.2.1 *ROUTER* DE ACCESO

Un *router* de acceso es un dispositivo de red que permite encaminar tráfico entre dos redes normalmente unidas mediante un enlace WAN. Normalmente este tipo de *routers* une la red de un proveedor de acceso a Internet (ISP) con un cliente.

Para el caso de clientes residenciales o pequeñas empresas, la principal función de este *router* es unir la red del cliente con la red del ISP, para lo cual el *router* deberá adaptar los datos entre los protocolos utilizados en ambos tipos de redes. Es decir, su función principal es proporcionar acceso a Internet. También se conoce como **router SOHO** (*Small Office, Home Office*). Además de la función de encaminamiento del tráfico entre las dos redes, suelen tener otras funciones adicionales.

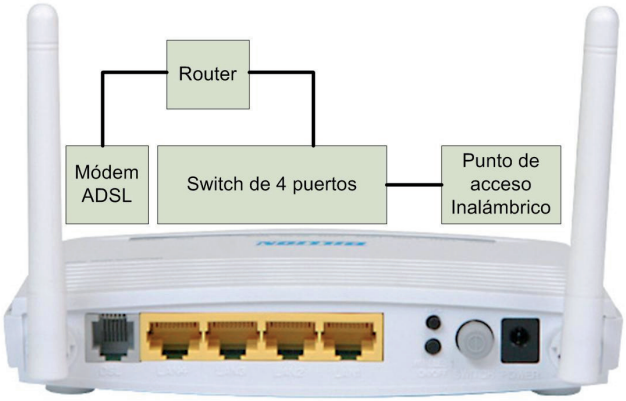


Figura 7.3. *Funciones típicas en un router de acceso residencial*

Como se observa en la figura anterior, un *router* de este tipo puede incluir hasta cuatro funciones diferentes:

- **Router**: se encarga de pasar los datos entre las dos redes que une, adaptando los protocolos.
- **Módem**: el módem se encarga de la transmisión de los datos en el enlace WAN mediante la técnica de la modulación.
- **Switch**: este tipo de *routers* también incluye cuatro puertos Ethernet.
- **Punto de acceso**: el *router* permite la conexión de dispositivos mediante enlaces inalámbricos Wi-Fi.

Las tecnologías de acceso a redes WAN más utilizadas actualmente son ADSL y cable, por lo tanto existen *routers* de los dos tipos:

- **Router ADSL**. En este tipo de *routers*, el enlace WAN se establece mediante la tecnología ADSL que permite la transmisión de datos en banda ancha mediante una conexión telefónica convencional. Estos *routers* presentan como interfaz WAN un conector RJ-11 telefónico.

Figura 7.4. *Conexiones en un router residencial ADSL*

- **Router de cable**. Este tipo de *router* utiliza la tecnología de cable coaxial proporcionada por algunas empresas de telecomunicaciones. Se utiliza un estándar conocido como **DOCSIS** (*Data Over Cable Service Interface Specification*). Externamente se diferencia del *router* ADSL por la interfaz de conexión WAN, que es un conector para cable coaxial.

Figura 7.5. *Conexiones en un router residencial de cable*

Cuando las necesidades de interconexión son más avanzadas es necesario utilizar *routers* de acceso que proporcionen dichas funciones avanzadas. Por ejemplo, cuando es necesario conectar varias sedes de una empresa entre sí utilizando la red privada de un operador, o cuando es necesario utilizar balanceo de carga o configuraciones de acceso redundantes.

Figura 7.6. *Routers de acceso de la serie 2800 de Cisco*

7.2.2 *ROUTER* DE DISTRIBUCIÓN (*CORE ROUTER*)

Este tipo de *routers* se caracterizan por tener una capacidad mayor de procesamiento que los *routers* anteriores y por proporcionar conectividad a más de dos redes. Se utilizan en las redes de grandes empresas o instituciones, así como en los propios ISP. Los *routers* de este tipo son los que forman el llamado *core* o troncal de Internet.

Estos *routers* deben implementar protocolos de enrutamiento para optimizar el enrutamiento de datagramas. Además, sus interfaces de red son altamente configurables permitiendo la inserción de módulos con la interfaz adecuada para cada tipo de red.

Figura 7.7. *Router de distribución de la marca Juniper*

7.3 CARACTERÍSTICAS ADICIONALES DE LOS *ROUTERS*

Además de las funciones de enrutamiento del tráfico, los *routers* también pueden llevar a cabo otras funciones, algunas de ellas fundamentales en las redes actuales.

7.3.1 CORTAFUEGOS (*FIREWALL*)

Prácticamente la totalidad de los *routers* actuales proporcionan funciones de cortafuegos como uno de los elementos de seguridad en las redes de datos. Un *router* con funciones de *firewall* permite establecer las reglas por las cuales se regula el tráfico intercambiado entre las redes.

El uso más frecuente del *firewall* es filtrar el tráfico de entrada de una red pública (normalmente Internet) hacia una red privada, con objeto de evitar accesos no autorizados a la red privada. Lógicamente, para que el nivel de seguridad que proporciona un *firewall* sea efectivo, todo el tráfico de entrada debe pasar por el *router* con funciones de *firewall*. También puede llevar a cabo el filtrado de información que viaja desde la red privada a la pública.

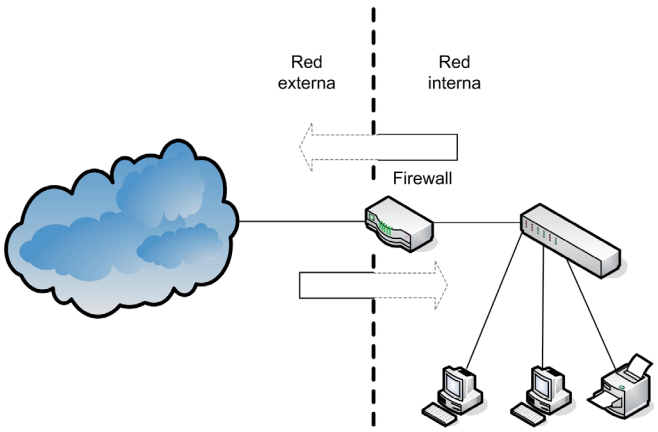


Figura 7.8. *Router con funciones de firewall*

Las reglas que se utilizan para decidir qué información proveniente de la red exterior puede entrar en la red privada son definidas por un administrador y suelen estar basadas en la información contenida en los niveles 3 ó 4. Ejemplos típicos son el filtrado por puertos, por direcciones IP o por tipo de protocolo.

En la siguiente figura, se indica una posible configuración de un *firewall* utilizando lo que se conoce como **DMZ** o zona desmilitarizada. En la DMZ se sitúan equipos que proporcionan servicios a través de la red externa y que, por tanto, no deben ser filtrados, como servidores web, servidores de correo, etc.

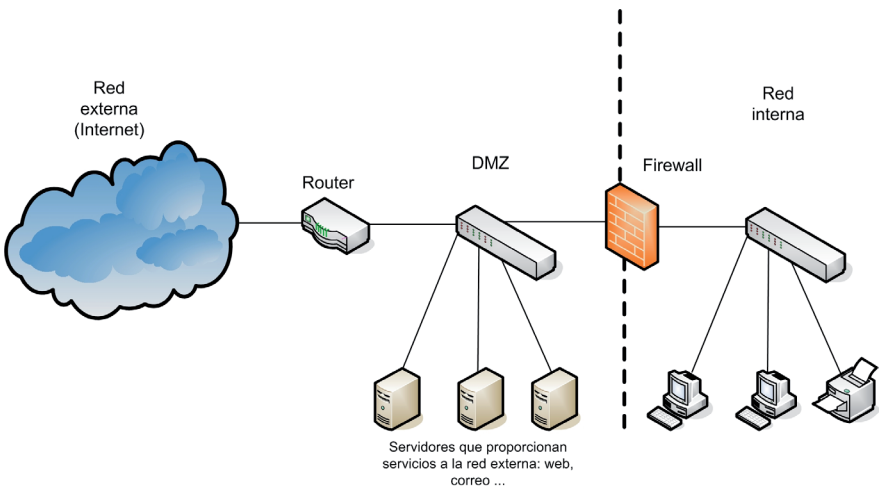


Figura 7.9. *Configuración de red con firewall y DMZ*

7.3.2 NAT (*NETWORK ADDRESS TRANSLATION*)

NAT (*Network Address Translation*, traducción de dirección de red) es un estándar creado por la IETF (Internet Engineering Task Force) que permite traducir las direcciones de una red, llamada *red interna*, cuando se conecte a otra red, llamada *red externa*.

El direccionamiento utilizado normalmente en las redes internas que utilizan NAT es un direccionamiento privado, es decir, se utilizan los rangos de direccionamiento privado o no enrutable. La red externa a la que se conecta una red que utiliza NAT normalmente es Internet. Para llevar a cabo este proceso, las direcciones IP se mapean desde el dominio interno de direcciones al dominio externo, proporcionando encaminamiento transparente a las máquinas finales.

Por lo tanto, NAT se puede utilizar para dar salida a redes públicas (normalmente Internet) a ordenadores que se encuentran dentro de una red con direccionamiento privado.

RECUERDA

Los rangos de direcciones que se pueden utilizar en redes privadas son los siguientes:
- 10.0.0.0 / 8
- 172.16.0.0 / 12
- 192.168.0.0 /16

Otra función que proporciona NAT es la de poder realizar cambios en la topología de la red interna y que dichos cambios no sean visibles en la red externa, es decir, se trata de ocultar información sobre la topología de la red interna. El proceso de traducción de direcciones se lleva a cabo en el dispositivo de red que une la red interna y la red externa, normalmente un *router*.

Hay varios tipos de NAT, pero el más utilizado actualmente es una variante llamada **NAPT** (*Network Address and Port Translation*). Este método se utiliza para que redes privadas puedan acceder a Internet a través de una única dirección IP. Para ello se utiliza un mapeo tanto de la dirección IP origen como del puerto origen de la red interna.

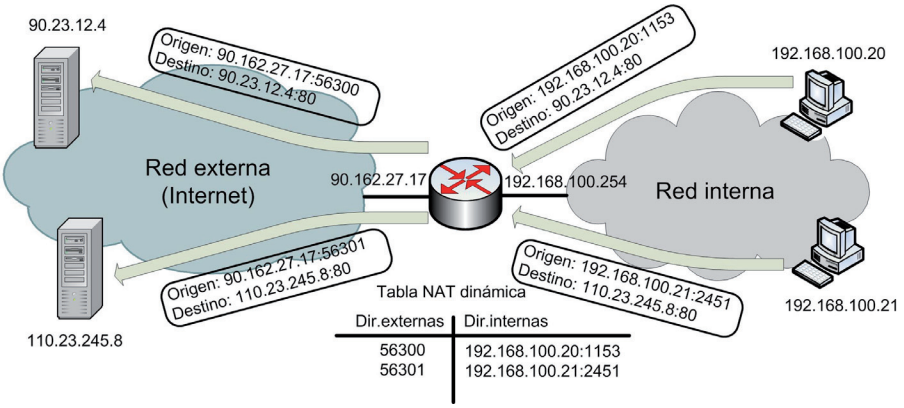


Figura 7.10. *Ejemplo de traducción de direcciones NAPT*

Como se observa en la figura, para utilizar esta técnica es necesario que el *router* modifique tanto la dirección IP origen como el puerto.

En la actualidad, prácticamente todos los *routers* implementan esta técnica, ya que NAPT ha sido adoptado como una de las principales soluciones a la escasez de direcciones públicas en Internet.

7.3.3 BALANCEO DE TRÁFICO

El balanceo de tráfico se utiliza cuando una empresa o institución tiene contratados dos o más accesos a Internet y se desea balancear el tráfico de salida de la red interna. De esta forma se consigue aumentar la capacidad de conexión de los equipos de la red a Internet y mejorar la gestión de la misma. Esta característica también se conoce como **multihoming**.

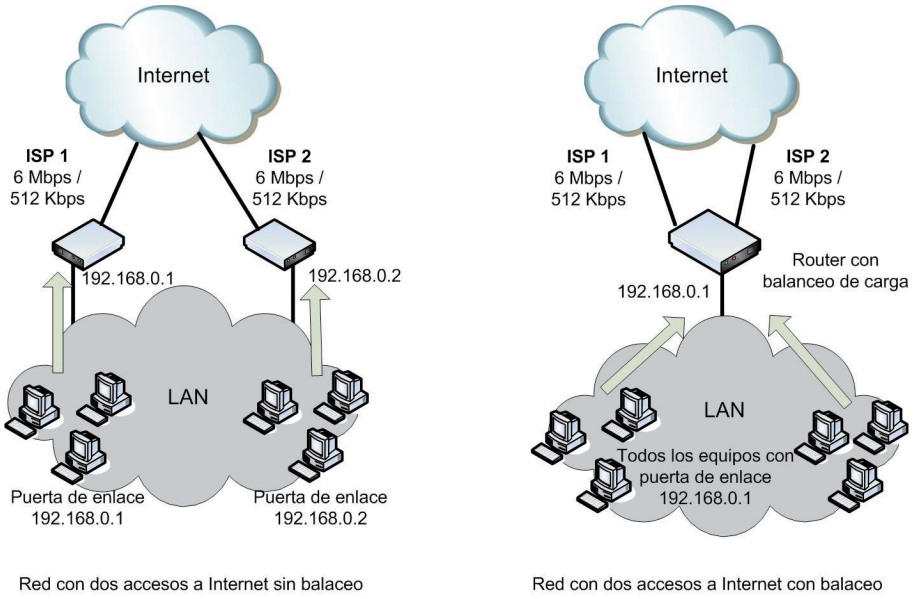


Figura 7.11. *Balanceo de carga*

7.3.4 PROXY

El término **proxy** se aplica generalmente a una aplicación que actúa como intermediario entre dos sistemas finales y que es conocida como **servidor proxy**. Los servidores proxy funcionan en el nivel de aplicación, por tanto es necesario ejecutar un servicio proxy por cada tipo de aplicación. Algunos modelos de *routers* implementan servidores proxy.

El tipo de servidor proxy más utilizado es el servidor proxy web, el cual se utiliza para centralizar todas las conexiones a páginas web de una red. Esta característica ofrece la posibilidad de llevar a cabo mecanismos de seguridad como filtrado de páginas web, validación de usuarios...

Los servidores proxy web también pueden proporcionar un mecanismo llamado **proxy-caché**, que consiste en almacenar las páginas web a las que se ha accedido en una caché. Esta característica acelera la conexión a las páginas web más visitadas. Los proxy-cachés implementan algoritmos para decidir cuándo una página debe ser descartada de la caché.

Para que un cliente acceda a páginas web a través de un proxy es necesario configurar adecuadamente el navegador web.

Proxy transparente, las conexiones a páginas web son enrutadas a servidores proxy de forma transparente sin llevar a cabo ninguna configuración en el ordenador del usuario. Normalmente estos servidores proxy interceptan el tráfico dirigido al puerto 80.

7.3.5 SERVIDOR VPN (VIRTUAL PRIVATE NETWORK, RED PRIVADA VIRTUAL)

Una VPN consiste en un conjunto de sistemas o dispositivos interconectados a través de canales seguros, sobre una red pública, permitiendo el acceso remoto de los recursos y servicios de la red de forma transparente y segura como si los usuarios estuvieran conectados de forma local. Por tanto, el uso de VPN es una alternativa sobre el acceso remoto tradicional y las líneas dedicadas. De esta forma se puede aprovechar la conectividad que ofrece una red pública (por ejemplo, Internet) o una red privada de un operador para proporcionar conectividad de forma segura.

La implementación de VPN se hace mediante *routers* que soporten esta característica, ya que un dispositivo de VPN opera a nivel de red, a través de conexiones seguras utilizando encapsulación, encriptado y autenticación. De esta forma se transportan de forma segura datagramas IP estableciendo túneles en ambos puntos de la conexión que negocian un esquema de encriptado y autenticación previo al transporte.

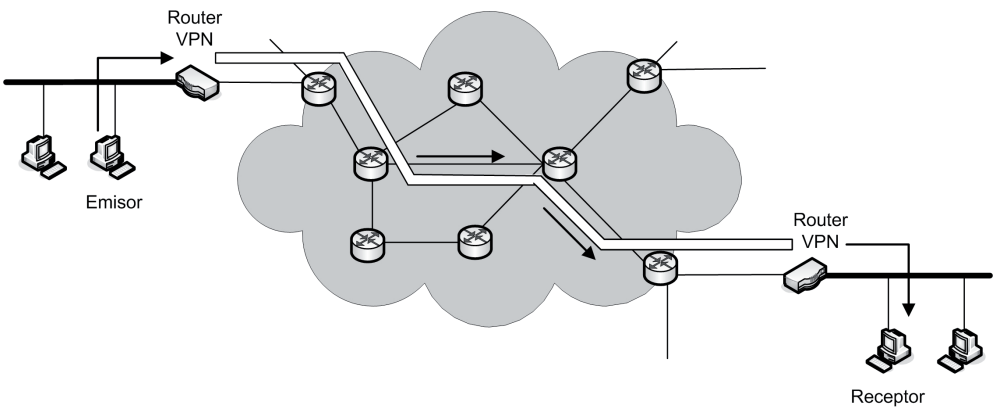


Figura 7.12. *VPN*

Para llevar a cabo la creación de túneles es necesario que los *routers* soporten protocolos de *tunneling*. Dos de los protocolos más importantes, que surgieron en 1996, son el ***Point-to-Point Tunneling Protocol*** **(PPTP)**, desarrollado por Microsoft, y el ***Layer Two Forwarding*** **(L2F)**, desarrollado por Cisco. La principal diferencia que existe entre ellos es que aplican túneles en diferentes niveles: los túneles PPTP encapsulan paquetes PPP en IP (nivel 3) y L2F utiliza protocolos de nivel 2, como Frame Relay y ATM, para crear los túneles.

A partir de estos protocolos ha surgido un tercero, que utiliza las características de los dos anteriores: **Layer Two Tunneling Protocol (L2TP)**. L2TP encapsula los paquetes originales dentro de una trama PPP, los comprime cuando es posible y, después, los encapsula dentro de un paquete de tipo UDP asignado al puerto 1701. Puesto que el paquete con formato UDP es un paquete IP, L2TP utiliza el modo de transporte IPsec para asegurar el túnel, basándose en la configuración de seguridad establecida en la configuración del usuario para el túnel L2TP. De forma predeterminada, IKE negocia la seguridad para el túnel L2TP mediante la autenticación basada en certificados (que utiliza certificados de equipo, no de usuario, para comprobar que los equipos de origen y de destino confían el uno en el otro) y mediante autenticación por claves compartidas previamente. Este tipo de autenticación no se recomienda porque es un método relativamente débil.

Debido a ello, se suele utilizar L2TP para crear el túnel y los protocolos de IPsec para proteger la información que viaja por el túnel. La creación de túneles VPN con esta técnica se conoce como **L2TP/IPsec**.

7.4 EL *SWITCH* O CONMUTADOR

7.4.1 ANTECEDENTES

En las redes actuales el *switch* es el dispositivo utilizado como elemento de interconexión de los equipos que forman parte de las mismas, existiendo una gran variedad de modelos para cubrir todas las necesidades de las redes actuales, tanto de pequeñas redes con unos pocos equipos como de grandes redes con cientos o incluso miles de equipos.

Sin embargo, su uso no se ha hecho extensivo a prácticamente todas las redes hasta hace unos años, cuando su precio permitió utilizarlo de forma masiva. Repasemos brevemente los dispositivos utilizados hasta ese momento.

- **Hub** o **concentrador**

  En las primeras redes 10BASE-T el dispositivo utilizado como elemento central de interconexión era el *hub* o concentrador. Un *hub* se puede considerar un dispositivo de interconexión de nivel 1, ya que opera exclusivamente en el nivel 1 del modelo OSI. Como ya se ha comentado anteriormente, cuando un *hub* recibe datos por uno de sus puertos, lo que hace es simplemente retransmitir esos datos por el resto de los puertos, es decir, lleva a cabo una simple transferencia de niveles eléctricos.

  Con la llegada de la Ethernet conmutada y el abaratamiento de los *switches*, los *hub* dejaron de utilizarse y actualmente prácticamente no se utilizan.

Figura 7.13. *El modelo de hub 3com Superstack II de 24 puertos fue muy utilizado en redes LAN*

- Puente (*bridge*)

Un puente, a diferencia de un *hub*, operaba en el nivel físico y de enlace, por lo que se les considera dispositivos de interconexión de nivel 2. Su función principal era la de dividir una red grande en segmentos más pequeños. Para llevar a cabo esta función, los puentes contienen la lógica necesaria para separar el tráfico de cada segmento.

El rendimiento de las primeras redes Ethernet que utilizaban CSMA/CD dependía en gran medida del número de equipos conectados, ya que cuantos más equipos, más colisiones y más reintentos sucesivos penalizando dicho rendimiento si el número de colisiones era muy elevado. En esta situación se utilizaban los puentes, dividiendo la red en dos segmentos, repartiendo el número de equipos y, por tanto, la carga de datos. Se dice que los puentes reducen **el dominio de colisión**. Un dominio de colisión está formado por todos los equipos que propagan sus tramas por un medio común y que por tanto son susceptibles de producir colisión.

No hay que confundir un dominio de colisión con un dominio de difusión. Un **dominio de difusión** está formado por todos los equipos que recibirían una trama de *broadcast* dentro de una red. Los puentes reducen los dominios de colisión pero mantienen los dominios de difusión.

Los puentes normalmente tienen dos puertos, en cada uno de los cuales se conecta un segmento de red. Cuando se recibe una trama por uno de los puertos, el puente lee la trama para obtener la dirección de destino. Si dicha dirección se corresponde con un equipo conectado al segmento de red desde el que se envió la trama, ésta no se propaga al otro segmento. Si la dirección de destino se corresponde con un equipo conectado al otro segmento, reenvía la trama por el puerto correspondiente.

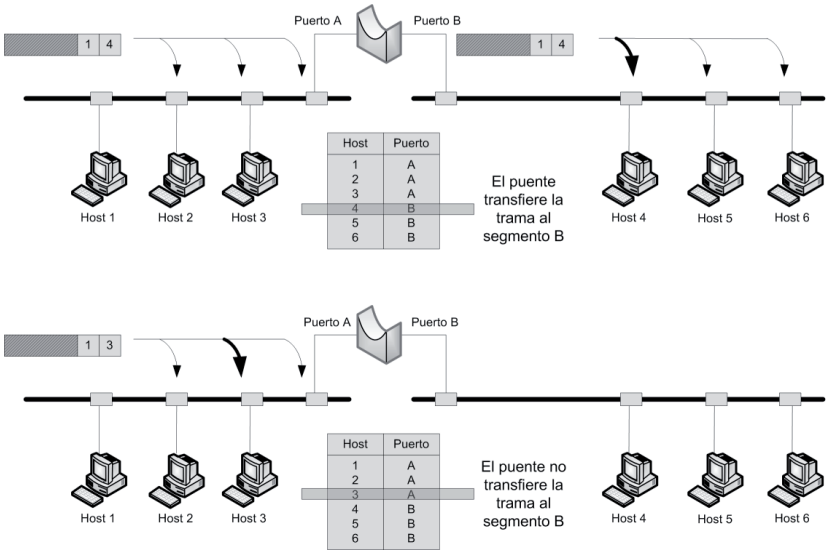


Figura 7.14. *Funcionamiento de un puente*

Como se observa en la figura, el puente debe almacenar en una tabla interna todas las direcciones físicas de la red y el segmento al que pertenecen. En función de la forma en la que se obtenga esta información existen dos tipos de puentes:

- **Puente simple**. La tabla se gestiona de forma manual, es decir, un técnico debe introducir los datos adecuados. Es una técnica fácil de implementar pero difícil de mantener.
- **Puente transparente**. Han sido los más utilizados. La tabla se genera de forma dinámica por medio de un proceso de aprendizaje. Este proceso es igual al que se utiliza en los *switches*, que se verá en el próximo apartado.

La otra gran función de los puentes era conectar dos redes LAN que utilicen protocolos diferentes en el nivel de enlace, como, por ejemplo, Ethernet y Token Ring, aunque en la actualidad esto tampoco sería necesario. Con la aparición de los conmutadores, los puentes han ido progresivamente desapareciendo y actualmente se pueden considerar extinguidos.

7.4.2 FUNCIONAMIENTO DE UN *SWITCH*

Un *switch* es el dispositivo de interconexión utilizado en Ethernet que posibilita el uso de la conmutación Ethernet. Externamente un *switch* es muy similar a un *hub*, y se utiliza en los mismos casos que los *hubs*, es decir, como elemento de interconexión de las redes Ethernet en estrella. Sin embargo, internamente un *switch* es un dispositivo con unas prestaciones muy superiores a los *hubs*.

Aunque el término *switch* tiene su traducción al español, que sería **conmutador**, lo cierto es que apenas se utiliza.

Figura 7.15. *Moderno switch de 52 puertos (48+4) de la marca D-Link*

Al *switch* se le considera un dispositivo de interconexión de nivel 2, ya que opera tanto en el nivel 1 como en el nivel 2 del modelo OSI. Su funcionamiento es muy similar a un puente multipuerto. Cuando un *switch* recibe una trama por uno de sus puertos, en lugar de redirigir la trama al resto de los puertos como hacen los *hubs*, la reenvía solo al puerto donde está conectado el dispositivo al que va dirigida la trama.

Los *switches* utilizan una sencilla técnica para conocer qué dispositivos están conectados a sus puertos. Esta técnica se basa en almacenar la dirección MAC de los dispositivos y asociar dicha dirección al puerto en el que están conectados. Esta asociación se almacena en una tabla interna en la memoria del *switch*.

Puerto	Dirección MAC
8	00:04:3B:8C:A5:73
3	00:0C:29:95:1F:B1
1	00:17:D8:65:20:03
2	00:09:7D:27:77:A8
4	00:24:98:C2:23:44

La técnica para generar la tabla de direcciones MAC sigue el siguiente procedimiento:

- Inicialmente la tabla estará vacía.

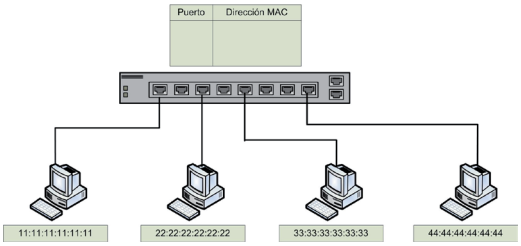


Figura 7.16. *Estado inicial de un switch con la tabla de direcciones MAC vacía*

- Cuando el *switch* recibe una trama por uno de sus puertos con una dirección de destino que no está en la tabla, reenvía la trama al resto de los puertos (igual que un *hub*).

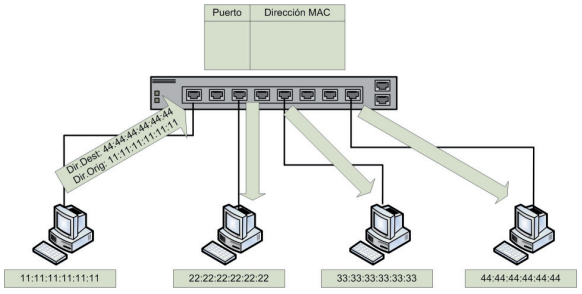


Figura 7.17. *Reenvío de una trama a todos los puertos*

- Si la dirección origen de una trama no está en la tabla, almacena dicha dirección y el puerto desde el que ha recibido la trama.

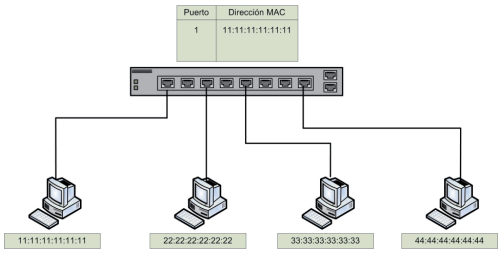


Figura 7.18. *Almacenamiento de la dirección origen en la tabla*

- Si la dirección destino está en la tabla, envía dicha trama directamente al puerto de destino.

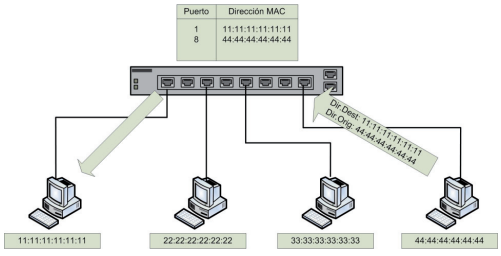


Figura 7.19. *Reenvío directo al puerto de destino*

- Cada cierto tiempo los datos de la tabla de direcciones se invalidan para actualizar posibles cambios en la topología de la red, por ejemplo, que un dispositivo cambie de puerto.

Esta técnica considera la posibilidad de que exista más de una dirección MAC en un puerto. Esta situación se puede dar cuando lo que hay conectado en el puerto es otro *switch* (o *hub*). Por ello, cuando recibe una trama con una dirección destino que no está en la tabla de direcciones, reenvía la trama al resto de los puertos, aunque algunos de ellos ya tuvieran entrada en la tabla.

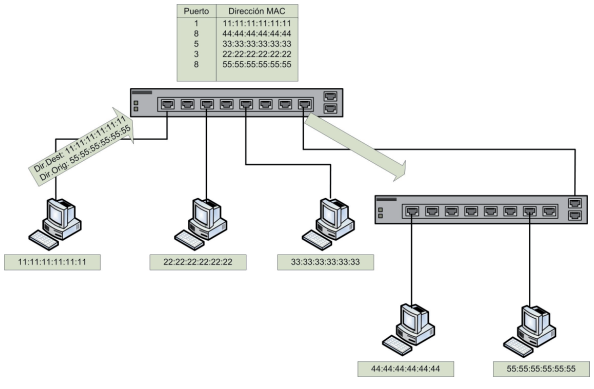


Figura 7.20. *Tabla de direcciones con varias entradas por puerto*

El reenvío que hace el *switch* de una trama cuando no encuentra la dirección MAC de destino en la tabla de direcciones no se hace realmente como en un *hub*. En los *switches* cada puerto tiene asociado un *buffer* de memoria. Lo que hace el *switch* es copiar la trama a los *buffers* del resto de los puertos. De esta forma nunca habrá más de una trama en ninguno de los enlaces que unen el *switch* y los dispositivos y, por tanto, no habrá colisiones.

Al igual que en los puentes, cada puerto en un *switch* es un dominio de colisión separado, con lo cual no propaga colisiones. Si se conectan equipos a cada uno de los puertos del *switch*, cada equipo forma su propio dominio de colisión. Al igual que los puentes, todos los equipos conectados a un *switch* pertenecen al mismo dominio de difusión.

Una de las características de los *switches*, al igual que los *hubs*, es el número de puertos que ofrecen para la conexión de los dispositivos a la red. Existen *switches* de 4 y 8 puertos para pequeñas redes domésticas, aunque en entornos más profesionales los valores típicos suelen oscilar entre 24 y 48 puertos.

En los próximos apartados se mostrarán algunas de las principales características de los *switches*.

7.4.3 PUERTOS

Uno de los aspectos básicos que define las prestaciones de los *switches* son los puertos, que son los elementos que permiten la conexión del *switch* a otros dispositivos. El primer dato sobre los puertos es su número. En el mercado podemos encontrar *switches* con diferente cantidad de puertos, que van desde 4 puertos los más básicos hasta varios cientos de puertos los más sofisticados. Además del número de puertos que proporciona un *switch*, conviene tener en cuenta otras características.

7.4.3.1 Velocidad y medio de transmisión

Dado que Ethernet permite varias velocidades y medios de transmisión, otras de las características destacables sobre los puertos de los *switches* son precisamente la velocidad a la que pueden trabajar y el medio de transmisión utilizado. Podemos encontrar puertos definidos como **10/100**, es decir, que pueden funcionar bajo los estándares 10BASE-T y 100BASE-TX. Otra posibilidad es encontrar puertos **10/100/1000**, es decir, añaden el estándar 1000BASE-T. También se pueden encontrar puertos que utilicen fibra óptica usando conectores hembra de algún formato para fibra óptica. Existen puertos 100BASE-FX y 1000BASE-X.

Por último, los *switches* de altas prestaciones pueden ofrecer puertos que cumplan con el estándar 10GbE, tanto en fibra como en cable UTP.

7.4.3.2 Funcionamiento Half/Full-dúplex

Como se ha visto en los apartados anteriores, el método de acceso al medio CSMA/CD obliga a que las comunicaciones en una LAN sean half-dúplex. Sin embargo, el uso de *switches* permite las comunicaciones full-dúplex, por lo que el ancho de banda efectivo respecto a redes con *hub* se duplica. Así, una red Fast Ethernet con una velocidad de 100 Mbps aumentará a 200 Mbps utilizando un *switch* que permita el modo full-dúplex. Lógicamente, este modo de funcionamiento también lo deben soportar las tarjetas de red de los dispositivos conectados al *switch*. Todos los *switches* fabricados en la actualidad admiten ambos modos. Habitualmente la selección del modo se hace de forma automática negociando con la NIC del equipo conectado al puerto mediante el método de autoconfiguración del estándar IEEE 802.3.

Algunos *switches* admiten la posibilidad de configurar manualmente el modo de transmisión y la velocidad de cada uno de sus puertos.

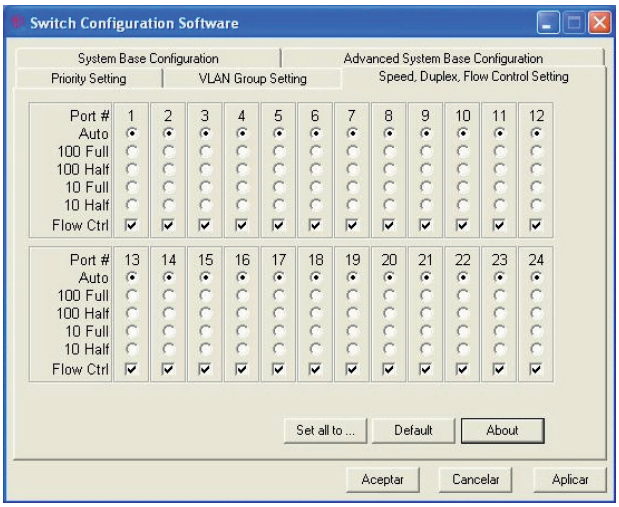


Figura 7.21. *Configuración por software de los puertos de un switch*

7.4.3.3 Modo Auto MDI/MDI-X

En el apartado 6.10 se explicaban los dos tipos de configuraciones de cable UTP utilizadas en redes Ethernet. La configuración de cable UTP directo se utiliza para conectar equipos a un *switch*. Pero también existe la configuración de cable UTP cruzado necesaria para conectar dos *switches* entre sí o dos PC entre sí.

Los primeros *hubs* o *switches* tenían puertos especiales que realizaban el ajuste necesario en la asignación de los pines para poder utilizar un cable UTP directo. Este tipo de puertos se conocían como **puertos MDI/MDI-X** o **puertos uplink**.

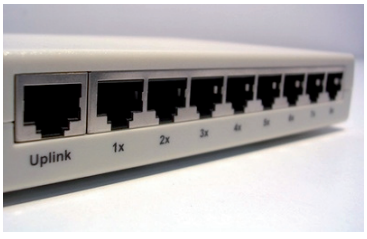


Figura 7.22. *Puerto MDI/MDI-X o uplink en un switch*

En la actualidad, la mayor parte de los *switches* y NIC funcionan con el llamado modo **Auto MDI/MDI-X**, que detecta de forma automática el tipo de cable conectado y realiza la asignación conveniente de los pines del conector. De esta forma, si utilizamos un *switch* que tenga esta característica, no es necesario tener en cuenta el tipo de cable utilizado en una conexión.

7.4.4 PUERTOS MODULARES: GBIC Y SFP

La mayor parte de los *switches* de gamas media y alta ofrecen los llamados puertos modulares. Estos puertos realmente no tienen ningún conector específico, sino que a ellos se conecta un módulo que contiene el puerto. De esta forma podemos adaptar el puerto al tipo de medio y velocidad que necesitemos. Es habitual que los fabricantes ofrezcan módulos de diferentes tipos con conectores RJ-45 o de fibra óptica. Los puertos modulares proporcionan flexibilidad en la configuración de los *switches*.

Existen dos tipos de módulos para conectar a los puertos modulares: el primer tipo de módulo que apareció es el módulo **GBIC** (*Gigabit Interface Converter*), diseñado para ofrecer flexibilidad en la elección del medio de transmisión para Gigabit Ethernet. Posteriormente apareció el módulo **SFP** (*Small Form-factor Puggable*), que es algo más pequeño que GBIC (de hecho, también se denomina **mini-GBIC**) y que ha sido utilizado por los fabricantes para ofrecer módulos tanto Gigabit como 10GbE en fibra o en cable UTP.

Figura 7.23. *Módulos SFP y GBIC*

Figura 7.24. *Puertos modulares para módulos SFP*

7.4.5 *BUFFERS*

El elemento clave en los *switches* para llevar a cabo el proceso de conmutación son los *buffers*, que son zonas de memoria donde las tramas son almacenadas antes de ser reenviadas al puerto correspondiente. Esta característica, además, permite al *switch* conectar puertos que trabajen a diferentes velocidades.

Los *buffers* pueden ser implementados en la salida de los puertos, en la entrada de los puertos o una combinación de ambos. Lo más habitual es implementarlos en la salida, ya que es el modo más eficiente, consiguiéndose unos índices de eficacia cercanos al 98%.

Los *buffers* se implementan en memorias RAM integradas en la circuitería del dispositivo, como se observa en la siguiente fotografía.

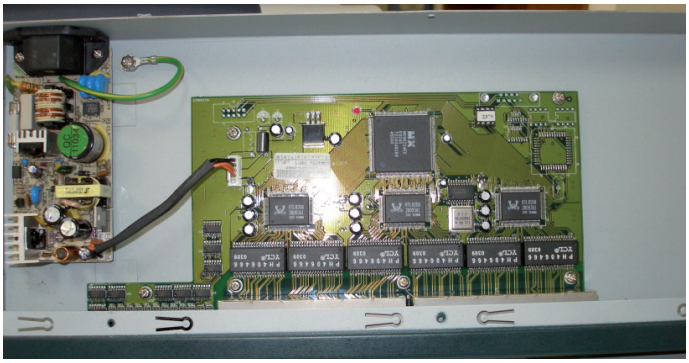


Figura 7.25. *Circuitería de un switch donde se observan los seis chips de memoria para los buffers en la zona inferior*

7.4.6 TÉCNICAS DE CONMUTACIÓN

Existen dos técnicas para llevar a cabo la transferencia de los datos entre puertos de un *switch*:

- **Reenvío directo (*cut-through*)**. En esta técnica, cuando un *switch* comienza a recibir datos por un puerto, no espera a leer la trama completa para reenviarla al puerto destino. En cuanto lee la dirección de destino de la trama MAC, comienza a transferir los datos al puerto destino.

  Esta técnica proporciona unos tiempos de retardo bastante bajos, sin embargo, tiene como inconveniente que solo puede usarse cuando las velocidades de todos los puertos son iguales.

  Otro problema que plantea la técnica *cut-through*, debido a su forma de funcionamiento, es que los *switches* propagan tramas erróneas o tramas afectadas por colisiones. Una posible mejora para evitar la propagación de tramas con colisiones es retrasar el reenvío hasta que se lean los primeros 64 bytes de trama, ya que las colisiones solo se pueden producir en los primeros 64 bytes de la trama. Esta mejora sin embargo aumenta el tiempo de retardo.

- **Almacenamiento y reenvío (*store and forward*)**. En este caso, cuando un *switch* recibe datos por un puerto, almacena la trama completa en el *buffer* para luego reenviarla al puerto destino. La utilización de esta técnica permite realizar algunas comprobaciones de error antes de ser enviada al puerto de destino.

  El tiempo de retardo introducido es variable, ya que depende del tamaño de la trama, aunque suele ser superior al proporcionado por la técnica *cut-through*, sin embargo, es imprescindible utilizar esta técnica cuando existen puertos funcionando a diferentes velocidades.

7.4.7 CONTROL DE BUCLES: SPANNING TREE

El algoritmo **Spanning Tree** (árbol de expansión) se utiliza en los *switches* para prevenir los bucles lógicos que pueden aparecer en una red. Los bucles se producen cuando existen varios caminos distintos entre dos puntos de la red y su efecto es que las tramas pueden circular de forma indefinida atrapadas en un bucle sin conseguir alcanzar su destino, lo que además afectará negativamente al rendimiento de la red. El algoritmo Spanning Tree ayuda a los *switches* a elegir el camino más idóneo y, por tanto, elimina los bucles.

El uso de este algoritmo está especificado en el estándar **IEEE 802.1D**. En 1998 se hizo una revisión del mismo añadiendo variaciones para optimizar su funcionamiento, el resultado se llamó **Spanning Tree rápido** y está especificado en la norma **IEEE 802.1w**.

7.4.8 POWER OVER ETHERNET (POE)

Power Over Ethernet (alimentación eléctrica por Ethernet), también conocido como **PoE**, es una tecnología que permite el envío de alimentación eléctrica junto con los datos en el cableado de una red Ethernet. La primera versión de esta tecnología se publicó en el estándar **IEEE 802.3af** en 2003 y en el año 2009 se publicó una revisión y ampliación en el estándar **IEEE 802.3at**.

La tecnología PoE permite suministrar alimentación eléctrica a dispositivos conectados a una red Ethernet, simplificando por tanto la infraestructura de cableado para su funcionamiento. Un dispositivo que soporte PoE obtendrá tanto los datos como la alimentación por el cable de red Ethernet.

Los dispositivos que utilizan esta característica son puntos de acceso inalámbricos Wi-Fi, cámaras de video IP, teléfonos de VoIP, *switches* remotos y en general cualquier dispositivo que esté conectado a una red Ethernet, que no tenga un consumo energético muy elevado y que su ubicación física dificulte la instalación de cableado.

En el estándar PoE se distinguen dos dispositivos:

- **PSE** (*Power Sourcing Equipment*). Son los dispositivos que generan la alimentación que viajará por los cables de datos Ethernet. Hay a su vez dos tipos:
  - **Endspans**, son *switches* Ethernet que incluyen la electrónica para la transmisión de la señal de alimentación eléctrica.
  - **Midspans**, son inyectores de potencia que se ubican entre un *switch* sin PoE y el dispositivo que requiere alimentación por PoE.
- **PD** (*Powered Devices*). Son los dispositivos que reciben alimentación eléctrica mediante la tecnología PoE.

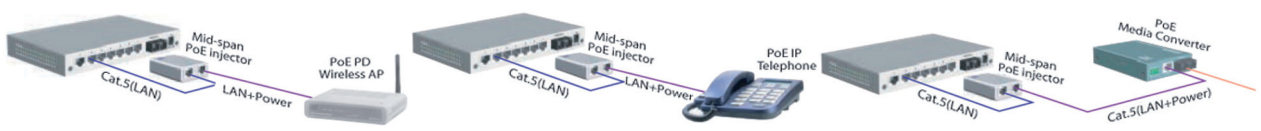


Figura 7.26. *Inyector de potencia PoE*

El estándar IEEE 802.3at especifica dos tipos de sistemas PoE: tipos I y II. El tipo I cumple las características de la primera versión del estándar IEEE 802.3af y el tipo II es el nuevo sistema PoE con características mejoradas. El siguiente cuadro muestra un resumen de las características de los dos tipos.

	Tipo I (IEEE 802.3af)	Tipo II (IEEE 802.3at)
Categoría mínima de cableado	Categoría 3	Categoría 5
Potencia suministrada por el PSE	15,4 W	30 W
Potencia máxima disponible para el PD	12,95 W	25,5 W
Rango de tensión de salida del PSE	44 – 57 V cc	50 – 57 V cc
Tensión nominal de salida del PSE	48 V cc	53 V cc
Corriente máxima	350 mA por par	600 mA por par

7.4.9 *SWITCHES* DE NIVEL 3 Y NIVEL 3/4

Los *switches* de gama alta utilizados en el troncal de redes Ethernet de mediana y gran envergadura suelen ofrecer capacidades de enrutamiento de paquetes IP. A este tipo de *switches* se los conoce como *switches* de nivel 3. Un *switch* de nivel 3 realiza todas las funciones de conmutación de un *switch* pero, además, proporciona funciones de enrutamiento IP.

También pueden existir *switches* que ofrecen características relacionadas con funciones del nivel 4, como control de puertos. A estos *switches* se les conoce como *switches* de nivel 3/4.

EJERCICIOS PROPUESTOS

1. Busca en Internet varios modelos de *routers* e indica sus principales características. Incluye modelos que tengan características avanzadas como VPN, función de proxy, balanceo de tráfico…

2. Busca información en Internet sobre varios modelos de *switches* e indica sus principales características, como número de puertos, propiedades de los mismos, tamaño de *buffers*, velocidad de conmutación, velocidad de transferencia, puertos modulares, VLAN, PoE…

TEST DE CONOCIMIENTOS

1 Una de las principales diferencias entre un *hub* y un *switch* es que:

a) Los *hubs* son dispositivos de nivel 1 y los *switches* de nivel 3.

b) Los *hubs* solo funcionan a 10 Mbps y los *switches* a 100/1000 Mbps.

c) Los *hubs* no pueden unirse entre sí y los *switches* sí.

d) Los *hubs* solo admiten el modo half-dúplex y los *switches* admiten tanto half como full-dúplex.

2 Los *switches* utilizan principalmente dos métodos para la conmutación de tramas. ¿Cuál de estos métodos se fija en la dirección de destino y reenvía inmediatamente la trama?

a) CSMA/CD.

b) Full-dúplex.

c) *Cut-through*.

d) *Store and forward*.

3 Los *switches* mantienen tablas de encaminamiento que incluyen:

a) La dirección IP y la dirección MAC de cada equipo conectado.

b) La dirección MAC y el puerto al que está conectado cada equipo.

c) La dirección MAC y la dirección de red a la que pertenece cada equipo.

d) Los *switches* no tienen tablas de encaminamiento.

4 Una de las principales características de NATP es que:

a) El dispositivo que implemente NATP debe alterar la cabecera de los paquetes TCP y UDP.

b) Las direcciones IP deben ser asignadas automáticamente.

c) Solo se puede utilizar para conectarse a Internet.

d) Solo se puede utilizar con direcciones IP públicas.

5 Las reglas de filtrado en los *firewalls* utilizan información:

a) Siempre del nivel de aplicación.

b) De los niveles 3 y 4.

c) De cualquier nivel del modelo OSI.

d) Solamente del nivel de red.

6 ¿De qué manera se evita la aparición de bucles lógicos en una red con *switches* con caminos redundantes?

a) Mediante *buffers* en los puertos.

b) Utilizando puertos Auto MDI/MDI-X.

c) Mediante el algoritmo Spanning Tree.

d) No pueden aparecer bucles lógicos con *switches* solo con *hubs*.

8 Proyecto e implantación de una red telemática

8.1 OBTENCIÓN DE INFORMACIÓN

El primer paso para abordar un proyecto de cualquier naturaleza es la obtención de información. Pero, ¿qué información es necesaria para la puesta en servicio de una red de área local? En primer lugar, como en todos los proyectos, es necesario conocer en detalle cuáles son las necesidades del cliente, es decir, qué uso va a dar el cliente a la red. Y, en segundo lugar, es necesario conocer las características y peculiaridades del cliente que puedan afectar al diseño de la red, como pueden ser el tipo de infraestructuras, número de personas que lo utilizarán, los elementos informáticos que harán uso de la red telemática, etc.

Por tanto, para ese primer paso de obtención de información se deberán realizar una serie de entrevistas con el personal adecuado de la empresa o institución para la que se va a realizar la puesta en servicio de la red. Es muy conveniente que estas entrevistas estén adecuadamente preparadas para que sean lo más eficientes posible, ya que, en la práctica, es muy posible que la persona que atiende nuestra entrevista no disponga de todo el tiempo que a nosotros nos gustaría.

Para intentar que las reuniones para la obtención de información sean lo más eficientes posible, puede ser de gran utilidad elaborar previamente a las entrevistas un cuestionario que nos ayude a recoger la información sobre las necesidades del cliente. También será conveniente tener preparados en el momento de la entrevista los datos que necesitamos conocer sobre el cliente, para, o bien solicitarlos en la entrevista, o bien obtenerlos por simple observación de sus instalaciones. En este aspecto, es importante que el cliente nos muestre las instalaciones donde se va a realizar el proyecto, todas las dependencias que estén involucradas. Es decir, es muy interesante tener un contacto visual con el entorno donde se va a desarrollar la implantación de la red. En esa primera inspección visual se deberá tomar nota de aspectos relevantes que afectarán el enfoque y las características del proyecto.

Algunos elementos en los que hay que pensar en el primer contacto visual de las instalaciones del cliente son:

- Dónde se encuentra el punto de demarcación, es decir, la acometida del exterior al interior del edificio de los operadores de telecomunicaciones que proporcionen los servicios de datos al cliente.
- Ubicación de la sala de telecomunicaciones. Si no existe, habrá que decidir dónde establecerla.
- La existencia de falsos suelos o falsos techos para el tendido del cableado.
- La existencia de "bajadas" o conductos verticales para la instalación del cableado vertical.
- Disposición de las áreas de trabajo, donde estarán ubicados los usuarios de la red telemática. Pueden ser despachos, o áreas diáfanas.
- La implementación de una red inalámbrica implica también estudiar la ubicación de los puntos de acceso inalámbricos.

Hay también otras informaciones sobre la empresa para la que vamos a realizar el proyecto que conviene conocer:

- Expectativas de crecimiento.
- Tipo de uso previsto de la red telemática.
- Existencia de personal técnico y su nivel de cualificación.

RECUERDA

Primer paso en la planificación de una red de área local: **OBTENCIÓN DE INFORMACIÓN**. Que se puede desglosar en:

- Conocer las necesidades del cliente.
- Conocer las características y peculiaridades del cliente que puedan afectar al diseño del propio proyecto.

8.2 DIMENSIONADO

Uno de los pasos que se deberá llevar a cabo en la planificación de la red es el adecuado dimensionado del sistema de cableado estructurado. A continuación se exponen algunos criterios generales para llevar a cabo el dimensionado de los diferentes elementos que formarán parte de dicho sistema de cableado estructurado:

- **Dimensionado de las tomas de usuario**. Se deben instalar dos tomas de datos en cada puesto de trabajo más un número de tomas extra para dispositivos de uso compartido como impresoras, fotocopiadoras, puntos de acceso inalámbricos, etc.
- **Dimensionado del cableado horizontal**. Se deberá calcular el cableado necesario para conectar todas las tomas de usuario con el repartidor de cableado horizontal añadiendo un porcentaje extra de cableado para posibles ampliaciones. Un valor típico puede ser del 5%. Además, habrá que añadir tanto los latiguillos del puesto de trabajo para conectar la roseta al equipo del usuario como los latiguillos de parcheo utilizados en el armario de comunicaciones.
- **Dimensionado del cableado vertical**. Se debe decidir el tipo de cableado y el número de pares utilizados. Habitualmente se utiliza cable de fibra óptica multimodo si la longitud del tendido no supera los 500 metros y cable de fibra óptica monomodo si el tendido supera dicha longitud. El número de fibras utilizadas dependerá de cada instalación. También serán necesarios latiguillos de fibra óptica.
- **Dimensionado del cableado troncal de campus**. Se suele utilizar cableado de fibra óptica monomodo que conecta cada uno de los distribuidores de edificio con el distribuidor de campus. Tanto en el cableado vertical como de campus de deberá sobredimensionar el número de fibras utilizadas para tener en cuenta futuras ampliaciones.
- **Dimensionado de las canalizaciones**. Las canalizaciones interiores deberán ser dimensionadas para prever futuras ampliaciones. De esta forma, las canalizaciones principales deberán dejar una capacidad libre de hasta el 50% de su capacidad total.

De igual forma, con la información del número de tomas de usuario por planta y la estimación de futuras ampliaciones se deberá hacer un cálculo del número de *switches* necesarios, así como sus principales características, para dar servicio a la red de datos.

8.3 PLANOS Y ESQUEMAS

Se deberá disponer de los planos de todas las plantas donde se va a realizar la instalación de la red. Estos planos deberán ser suministrados por el cliente preferentemente en algún formato electrónico estándar como puede ser el formato **AutoCad** (archivos de tipo DWG). En estos planos se detallará la ubicación de todos los elementos que forman parte de la red de área local debidamente etiquetados.

Existen alternativas de software gratuito para poder visualizar y editar archivos de AutoCad. Uno de los más interesantes es **DraftSight**, disponible en Windows, Linux y Mac:
www.3ds.com/es/products/draftsight/overview/

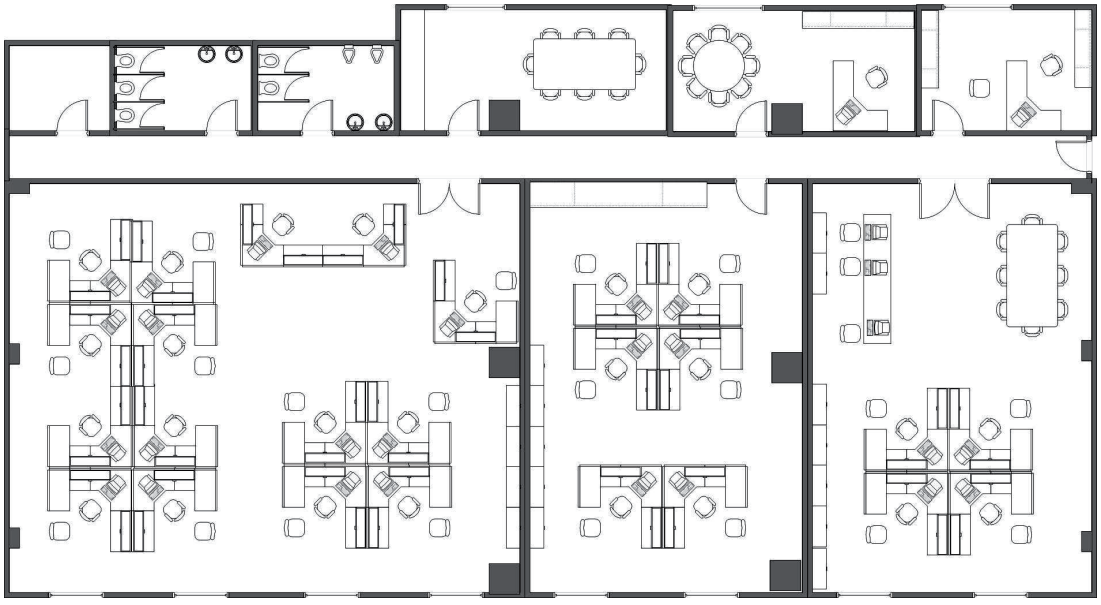


Figura 8.1. *Plano de planta*

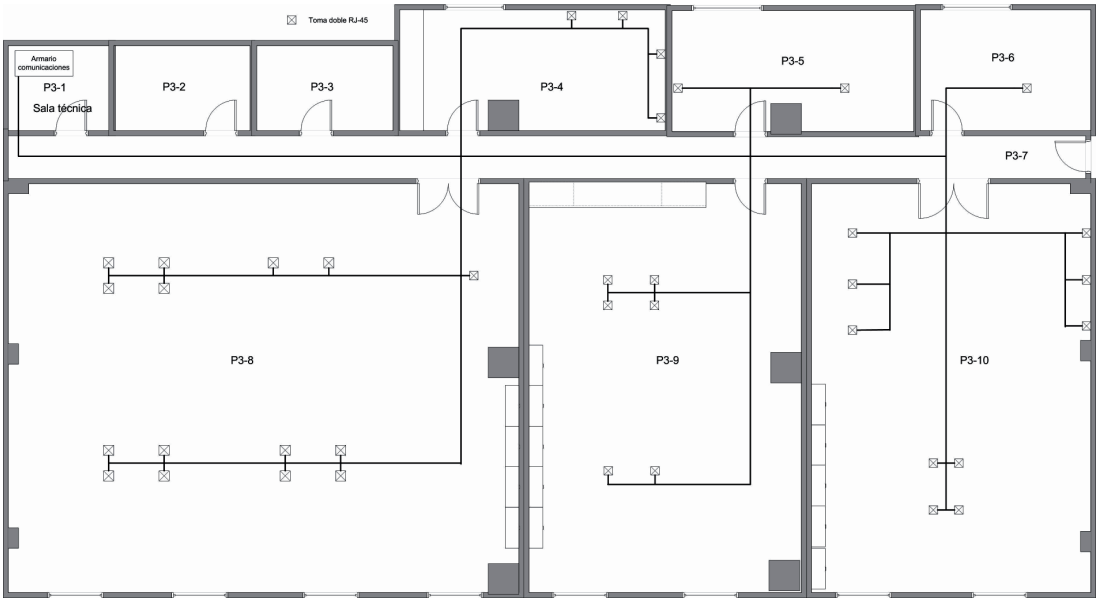


Figura 8.2. *Plano de la planta donde se han ubicado los puntos de red*

Además de los planos de todas las plantas en las que se realizará la instalación de la red se debe incluir:

- Esquema de interconexión global de todos los elementos que componen la infraestructura.
- Esquemas de todos los armarios instalados donde se indique todo el equipamiento que incluyen.

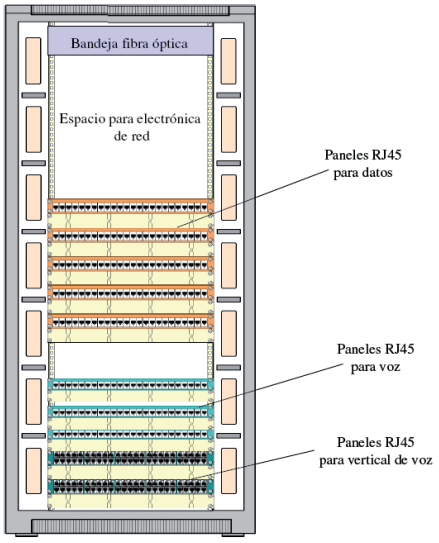


Figura 8.3. *Armario rack*

Esquema unifilar de todo el sistema eléctrico de uso exclusivo de las infraestructuras de la red.

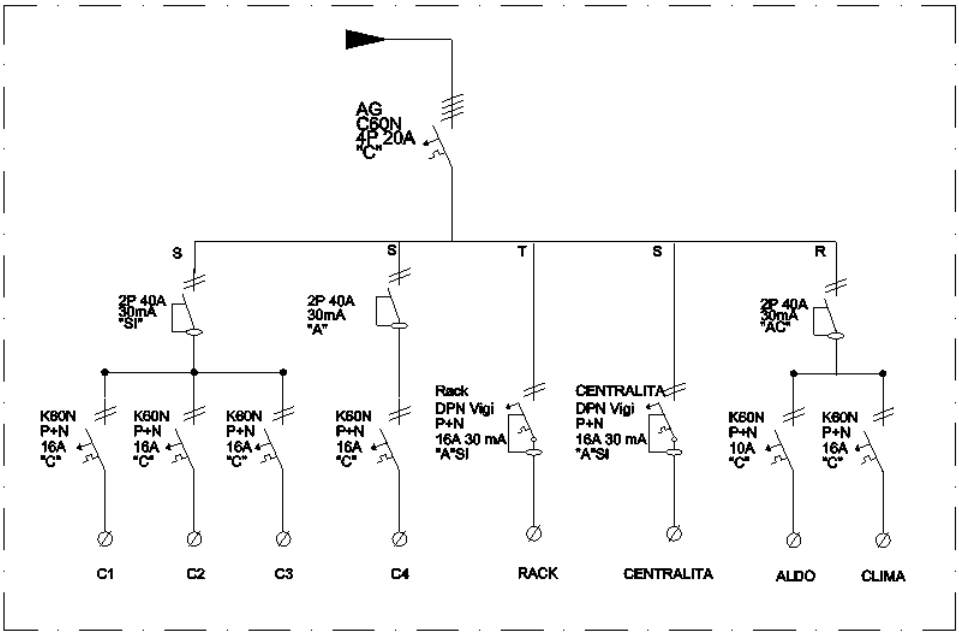


Figura 8.4. *Esquema unifilar de una red de voz y datos*

8.4 ESPECIFICACIONES TÉCNICAS DE DISEÑO

En lo referente a la infraestructura de cableado, normalmente se sigue la normativa establecida en la norma UNE-EN 50173, que es el estándar español sobre cableado estructurado. Este estándar está desarrollado directamente de la norma europea EN 50173, que a su vez se basa en la norma internacional ISO/IEC 11801. Además, la *memoria técnica del proyecto* podrá contener diferentes especificaciones de diseño de algunos de los elementos que forman parte de la red. A continuación se ofrecen algunos ejemplos aplicados a diferentes elementos de la infraestructura de la red.

8.4.1 ESPACIOS PARA DISTRIBUIDORES

A continuación se ofrecen algunas especificaciones de ejemplo relacionadas con los espacios donde se ubican los distribuidores del cableado:

- Una vez instalados todos los elementos en los **distribuidores**, incluidos los equipos de electrónica de red previstos, se deberá disponer de al menos un 25% de espacio libre para futuras ampliaciones. En caso contrario, se deberá realizar la instalación de un armario adicional para cumplir dicho criterio.

- Los *distribuidores* deberán instalarse en habitáculos que presenten las dimensiones adecuadas para posibilitar el trabajo de instalación y mantenimiento de los mismos. A modo de ejemplo, en la siguiente figura se muestra un esquema con las dimensiones de un habitáculo de 6 m^2 destinado para un distribuidor que presente una configuración con dos armarios de comunicaciones.

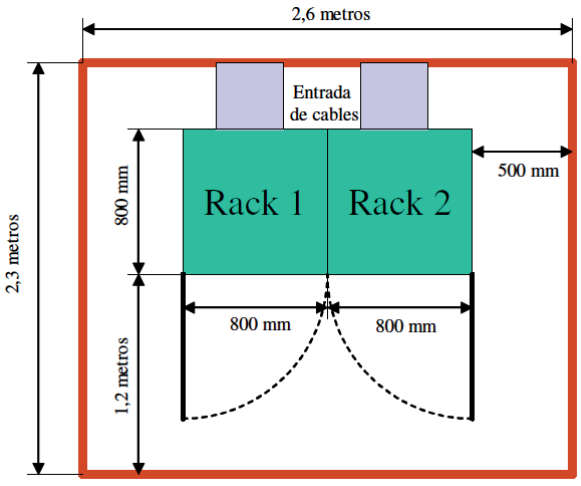


Figura 8.5. *Esquema del habitáculo para un distribuidor*

- El *cuarto de comunicaciones* necesario para ubicar los armarios distribuidores de cableado deberá disponer de una puerta con cerradura y apertura hacia fuera y existirá una bajante vertical, en la parte posterior de los armarios, para la entrada de cables y para el acceso a las canalizaciones troncales del cableado horizontal y del cableado vertical. El *cuarto de comunicaciones* deberá disponer de los siguientes elementos y servicios:
  - Un cuadro eléctrico provisto de dos interruptores diferenciales de 25 A y 30 mA de sensibilidad para alimentación de los armarios (una línea para cada armario) con corriente monofásica a 220 V.
  - 2 tomas de corriente libres protegidas mediante magneto-térmico de 16 A para enchufar herramientas y aparatos eléctricos.
  - Una toma de tierra independiente, de resistencia inferior a 5 ohmios, para su conexión a los armarios.
  - Luminarias para proporcionar una luminosidad de al menos 300 lux.
  - Ventilación natural directa o forzada, con el objeto de mantener unas condiciones ambientales de temperatura entre 18 ºC y 30 ºC y humedad relativa entre 30% y 55%.
  - Las ventanas del cuarto deberán estar protegidas con rejas para impedir el acceso de intrusos y deberán disponer de persianas o mecanismos similares para evitar la incidencia directa de la luz solar sobre los equipos.

8.4.2 CABLEADO VERTICAL Y HORIZONTAL

Al igual que en el apartado anterior, se exponen a continuación algunas especificaciones de ejemplo referidas en este caso tanto al cableado vertical como al cableado horizontal.

- Las canalizaciones del cableado troncal vertical discurrirán preferentemente por bandejas situadas en patinillos o en bajantes de plantas preparadas al efecto. Los posibles tramos horizontales que deba recorrer el cableado troncal hasta la *sala de comunicaciones* en la que se encuentre el *distribuidor de edificio* se realizarán mediante bandeja de las dimensiones adecuadas, soportada preferentemente sobre tabique o, en su defecto, sobre techo.
- El cableado horizontal desde los *distribuidores de planta* hasta las tomas de usuario se tenderá preferentemente a través de bandejas perimetrales que hay que ubicar en pasillos y zonas comunes. Estas bandejas se soportarán sobre tabique o sobre techo.
- Con el fin de que la distribución de las bandejas no afecte a la estética interior del edificio, se considera adecuado instalar falso techo para cubrir dichas bandejas. El falso techo deberá ser registrable, al menos, a lo largo de todo el tramo de canalización. Alternativamente, en caso de que la estética interior del edificio lo requiera y no exista falso techo, se podrá emplear canaleta vista soportada sobre tabique, en lugar de bandejas.
- El acceso desde las bandejas perimetrales a las tomas de usuario se efectuará mediante canaleta o tubo rígido de dimensiones adecuadas, a través de orificios practicados en los tabiques.

8.4.3 TOMAS DE USUARIO

En este apartado se exponen algunos ejemplos de especificaciones de diseño relacionadas con las **tomas de usuario** en las áreas de trabajo:

- Se recomienda la instalación de *suelo técnico* en salas destinadas a un uso que requiera movilidad de los puestos de trabajo y/o exista alta densidad de puestos de trabajo. El suelo técnico se montará preferiblemente sin estructura para facilitar el movimiento de losas y la posible reestructuración de la sala. Las cajas se situarán bajo losetas del falso suelo que presenten un orificio para el paso de los latiguillos, o bien estarán embutidas en cajas acopladas a las losetas y dotadas de una tapa protectora.
- Como alternativa al falso suelo, se podrá realizar un tendido de canalización perimetral e instalar las cajas en pared, siempre y cuando sea funcional y operativamente posible alinear las mesas de trabajo contra una o ambas paredes del local, dejando un pasillo lateral o central y espacio suficiente entre cada fila de mesas para el acceso a cada puesto sin causar molestias a los usuarios que se encuentren en ellas. El espacio mínimo entre hileras deberá ser de 1,20 metros.
- Se evitarán las ubicaciones de puestos en zonas separadas de las paredes a fin de evitar el uso de canaletas de media caña o columnas de cableado que encarecerían de manera importante la instalación y conservación del cableado.
- En los locales destinados a despachos o en los que exista un número relativamente bajo de puestos de trabajo, se recomienda realizar un tendido de canalización perimetral y situar las cajas de las tomas de datos en la pared.

- La ubicación de las cajas de tomas de cableado seguirá las siguientes recomendaciones:
  - Las cajas se posicionarán en un punto cercano a la mesa del usuario.
  - Se recomienda el uso de mesas de oficina que incorporan un mecanismo guía para el tendido de los latiguillos del teléfono y del ordenador y un orificio para conducir los latiguillos desde la parte inferior de la mesa a la parte superior, a fin de dejar la superficie de trabajo libre de cables.
  - La distancia desde las tomas a los equipos (ordenador y teléfono) deberá ser inferior a 3 metros, para evitar superar la longitud máxima de latiguillo de usuario, establecida en 5 metros.
  - Las tomas de datos deberán estar accesibles en todo momento, es decir, no se deben colocar armarios, estanterías u otro tipo de mobiliario o elementos delante de ellas.
  - La ubicación de las cajas y las mesas deberá ser tal que se evite el tendido de cables (latiguillos) por el suelo, ya que se corre el riesgo de tropezar con ellos y arrancarlos o deteriorarlos.
  - Se evitará la instalación de las cajas detrás de puertas o detrás de objetos que impidan su acceso, como p. ej. armarios, estanterías, paneles de calefacción, etc.

8.4.4 ETIQUETADO

No existe una referencia exacta sobre los criterios de etiquetado de los diferentes elementos del sistema de cableado estructurado, aunque sí es muy aconsejable que exista un procedimiento de etiquetado lo más claro posible. A continuación se ofrecen unas pautas generales para llevar a cabo dicho etiquetado:

- **Distribuidores de planta**. Se puede utilizar un código que corresponda a la planta y otro código que identifique el número de armario, si hubiera más de un armario de comunicaciones dentro del distribuidor de planta. En algunos casos se utiliza una letra para identificar el armario. Ejemplo:

1A	Distribuidor primera planta, armario A.
1B	Distribuidor primera planta, armario B.
S1.1	Distribuidor sótano 1, armario 1.

- **Cableado de subsistema vertical**. Se suele asignar un código a cada manguera de cableado vertical para identificar el tipo de cableado, el identificador de armario de distribución de planta al que se conecta y un número asociado al último par de la manguera. Ejemplos:

VD-1A-100	Identifica un enlace vertical de datos (VD) que conecta con el distribuidor de planta 1A (armario A de la primera planta) y que incluye hasta el par número 100.
VF-8.1-12	Identifica un enlace vertical de fibra óptica (VF) que conecta con el distribuidor de planta 8.1 (primer armario de la planta 8) hasta la fibra número 12.

- **Tomas de usuario**. La identificación de las tomas de usuario se suele hacer indicando el código del distribuidor de planta al que está conectado y se añade un código único identificativo. La asignación del número de identificación de la toma de usuario dentro de cada distribuidor de planta se suele hacer siguiendo unos determinados criterios.

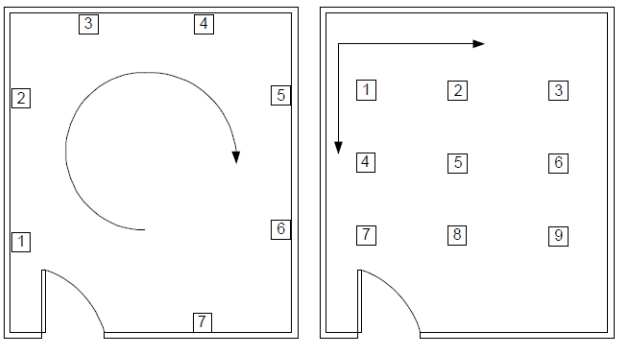


Figura 8.6. *Criterios de numeración de tomas de usuario*

Ejemplos de identificadores de tomas de usuario:

1A-15 y 1A-16	Identifica las tomas 15 y 16 situadas en la primera planta y conectadas al armario A.
3.2-23	Identifica la toma 23 de la tercera planta y que está conectada al armario 2.
S1.1-10	Identifica la toma 10, situada en el sótano 1 y conectada al armario 1.

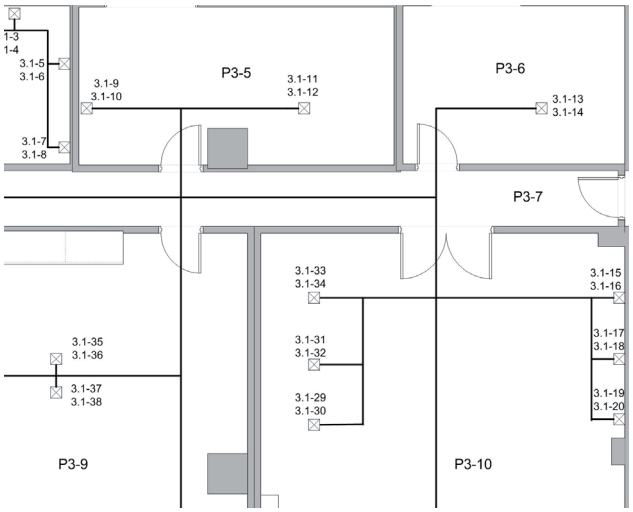


Figura 8.7. *Etiquetado en plano de las tomas de usuario*

- **Cableado horizontal**. El etiquetado del cableado horizontal puede seguir los mismos criterios que el de las tomas de usuario y, de hecho, se puede utilizar el mismo código asignado a la toma de usuario. Por ejemplo, un cable horizontal etiquetado como 3.2-23 identifica el par que conecta la toma 23 con el armario 2 de la primera planta.
- **Paneles de parcheo**. Para el etiquetado de los puertos de los paneles de parcheo se sigue igualmente una numeración correlativa. En muchas ocasiones el número de identificación de los puertos del panel de parcheo se corresponde con el identificador de la toma de usuario para facilitar las labores de mantenimiento.

8.4.5 MATERIALES Y EQUIPAMIENTO

Otro de los aspectos que hay que considerar en la planificación de la puesta en servicio de una red son las especificaciones técnicas de los materiales utilizados, así como las condiciones de instalación. En muchos casos, estas especificaciones técnicas vienen impuestas por las diferentes normativas que se deben cumplir. Por ejemplo, todos los materiales utilizados deben cumplir las normativas antiincendios. En cuanto al cableado y los elementos de conexión, estos deben cumplir habitualmente la normativa UNE-EN 50173.

8.4.5.1 Cableado horizontal

A continuación se indican algunos ejemplos de especificaciones técnicas referidas al cableado horizontal:

- El cableado horizontal se realizará de una sola tirada entre la roseta de usuario y el panel de conectores del armario repartidor de planta, estando terminantemente prohibidos los puntos de transición, empalmes o inserción de otros dispositivos.
- Como mínimo se instalarán dos cables balanceados de categoría 6 y constituirán enlaces permanentes y canales de clase E, según las especificaciones de la norma EN 50173.
- En caso de instalarse fibra óptica será multimodo de índice gradual 62,5/125 µm.
- La distancia máxima entre la roseta de usuario y conector ubicado en el armario distribuidor de planta será de 90 metros (longitud mecánica). Se entregará una gráfica con la distribución estadística de los enlaces del SH dependientes de cada DP.

8.4.5.2 Tomas de usuario

Se indican algunos ejemplos representativos de especificaciones técnicas referidas a los materiales utilizados en las tomas de usuario.

- Las tomas de telecomunicaciones se instalarán preferentemente en cajas modulares de superficie, que serán de diferentes medidas:
  - Caja para 4 tomas RJ45 hembra.
  - Caja para 8 tomas RJ45 hembra.
  - Caja para 12 tomas RJ45 hembra.
- Las tomas de usuario en las que terminará el extremo del cable horizontal UTP serán de tipo RJ45 hembra y categoría 6, según especificación EN 60603-7-4.

- En caso de utilizar cableado horizontal de tipo STP, éste terminará en tomas RJ49 hembra y categoría 6, según especificación EN 60603-7-5.
- En ambos casos, la parte trasera del conector en la que se inserta el cable será de tipo IDC 110 y estará rotulada al menos con el código de colores normalizado según N 60603-7 opción B (equivalente al código EIA/TIA 568-B).
- Los latiguillos de usuario estarán compuestos por cable de cobre de 4 pares trenzados balanceados de tipo UTP, terminados en conectores RJ45 machos y categoría 6, debiendo cumplir la especificación EN 50288-6-2. Las medidas estándar de los latiguillos que hay que emplear serán de 1 m, 2 m, 3 m y 5 m.

8.4.5.3 Cableado vertical

Se indican en este apartado algunos ejemplos de especificaciones técnicas de los materiales utilizados en el cableado vertical:

- El cableado vertical se realizará de una sola tirada entre los dos distribuidores que hay que unir, estando terminantemente prohibido el uso de empalmes o inserciones de otros dispositivos intermedios.
- Para la vertical de datos se utilizarán mangueras de 12 fibras ópticas multimodo de índice gradual 62,5/125 µm, según especificación EN 60793-2-10:2002-A1b, y deberá cumplir al menos la categoría OM1.
- Adicionalmente, deberá cumplir las condiciones mecánicas y ambientales, según especificaciones EN 60794-1, IEC 60794-2 y EN 60794-3.
- La manguera de 12 fibras ópticas multimodo se conectará a un panel de 12 fibras de 1 U de altura, dotado de casete organizador y distribuidor de fibras. El panel se terminará en conectores de tipo ST.

8.4.5.4 Cableado de campus

Se exponen a continuación algunos ejemplos de especificaciones técnicas relacionadas con elementos utilizados en el cableado de campus.

- El cableado de campus se realizará, salvo casos concretos y muy justificados, de una sola tirada entre los dos distribuidores que hay que unir, estando terminantemente prohibido el uso de empalmes o inserciones de otros dispositivos intermedios.
- Se utilizarán mangueras de 12 fibras ópticas monomodo de salto de índice de 9/125 µm, según especificación EN 60793-2-50:2002-B1, y deberá cumplir la categoría OS1.
- Adicionalmente, deberá cumplir las condiciones mecánicas y ambientales, según especificaciones EN 60794-1, IEC 60794-2 y EN 60794-3.
- La manguera de 12 fibras ópticas monomodo llevará una cubierta de protección de tipo PKP antihumedad y antiroedores y se conectará a un panel de 12 fibras de 1 U de altura, dotado de casete organizador y distribuidor de fibras. El panel se terminará en conectores de tipo SC simple.

8.4.5.5 Armarios de comunicaciones

Se exponen algunos ejemplos de especificaciones técnicas referentes a los armarios de comunicaciones:

- Armarios tipo Rack de 19", anchura de 800 mm y profundidad de 800 mm.
- Techo, parte trasera y laterales en chapa de acero, desmontables y con rejillas de ventilación.
- Ruedas dobles giratorias con banda de rodadura de goma.
- Tendrán una altura mínima de 42U, y máxima de 47U.
- Puerta frontal transparente, provista de juntas de goma y cerradura con llave.

En los armarios de comunicaciones se podrán configurar los siguientes módulos:

- VF. Paneles para las tomas verticales de datos (fibra óptica).
- VD. Paneles para las tomas verticales de datos (enlaces de cobre).
- HD. Paneles para las tomas horizontales de datos.
- EL. Hueco para la electrónica.

8.4.5.6 Alimentación

Se indican en este apartado algunos ejemplos de especificaciones técnicas de los materiales utilizados en la alimentación utilizada para los armarios de comunicaciones:

- Se instalarán regletas de tomas de corriente tipo Schuko de 16 A con toma de tierra. Todas las regletas contarán con protección magnetotérmica integrada, o bien serán cableadas hasta las bornas del magnetotérmico instalado en el armario.
- Las regletas serán de montaje en unidades de 19" y se instalarán en horizontal en el perfil posterior del Rack, mirando hacia la parte frontal. Se colocará un pasahilos para gestionar los cables de alimentación de los equipos conectados a la regleta.
- El número de tomas tipo Schuko será:
  - Un mínimo de 8 en los armarios DP que puedan contener algún tipo de electrónica de red.
  - Un mínimo de 12 en los armarios DE que puedan contener algún tipo de electrónica de red.
- La ubicación de los armarios garantizará una separación mínima de 3 metros respecto de las principales fuentes de señales parásitas (transformadores, onduladores, ascensores, etc.).
- Los armarios contarán con un kit de puesta a tierra que conectará al SPAT dedicado todas sus partes metálicas y las de los elementos que contenga.
- En caso de que el edificio posea un sistema de alimentación ininterrumpida (SAI) con la suficiente capacidad, se deberá conectar el armario distribuidor a dicho sistema, realizando todo lo necesario para ello.

8.4.5.7 Elementos de distribución

Se indican en este apartado algunos ejemplos de especificaciones técnicas de los materiales utilizados en la canalización del sistema:

- **Bandeja de rejilla de acero galvanizado**. Bandeja de rejilla con varillas de acero de 4,5 y 5 mm, de alta resistencia electrosoldadas, ajustada a las normas UNE 37-552-73 (ensayo sobre recubrimientos) y EN 50.085 (prenorma europea de ensayo de cargas para una deformación máxima f £ L/200, siendo L la distancia entre apoyos en mm). La distancia entre apoyos debe ser inferior o igual a 1 metro. Medidas: ancho de 60, 100, 200, 300, 450 y 600 mm; alto de 33, 62 y 100 mm; largo de 3.000 mm.
- **Tubo PVC**. Tubo flexible por espiral de PVC + PVC rígido, de grado de protección IP 67 y autoextinguible (según VL 94), resistente al impacto grado 4 según prenorma europea 50.086-1. Temperatura de operación entre -5 øC y 65 øC. Ajustado a la norma UNE 20.324/78 o DIN 40.050 (para los grados de protección).
- **Tubo flexible de poliamida**. Protección IP 67 ajustado a la norma UNE 20.324/78 o DIN 40.050, resistente al impacto grado 4 según prenorma europea 50.086-1. Temperatura de operación entre -30 ºC y 100 ºC. Resistente a fuel y aceites, no emisor de halógenos.
- **Tubo flexible de PVC**. PVC liso interior y exterior, autoextinguible de grado de protección IP 67 ajustado a norma UNE 20.324/78 o DIN 40.050. Temperatura de operación entre -5 ºC y 65 ºC.
- **Tubo metálico**. Fleje de acero laminado en frío (según DIN 1624) galvanizado por ambos lados + PVC exterior, flexible, autoextinguible con grado de protección IP 67 ajustado a norma UNE 20.324/78 y resistente al impacto grado 3 según prenorma europea 50.086-1. Temperatura de operación entre -20 ºC y 80 ºC.
- **Bandeja de PVC con tapa**. Temperatura de servicio entre -20 ºC a 60 ºC. Rigidez dieléctrica según UNE 21.316. Autoextinguible a 960 ºC (sin goteo del material inflamado o de partículas incandescentes) en el ensayo del hilo incandescente y no propagador de la llama en el ensayo de resistencia a la llama de plásticos autoportantes, según norma UNE 55.315. Difícilmente inflamable, clasificada como UL 94-VO. Coeficiente de dilatación lineal inferior a 0,07 mm/ºC m. Protección contra daños mecánicos y contra penetración de cuerpos sólidos según norma UNE 20.324.

8.4.6 DOCUMENTACIÓN

Los proyectos de puesta en servicio de redes locales, como cualquier otro tipo de proyectos, requieren la generación de una serie de documentos. Los documentos más comunes que será necesario redactar son los siguientes:

- **Memoria técnica del proyecto**. Es el documento de diseño base sobre el que se realizarán posteriormente los trabajos de ejecución de la puesta en servicio de la red local.
- **Informe del plan de ejecución**. Documento que incluye la temporización de los trabajos para llevar a cabo la puesta en servicio de la red local. También se suele incluir en este informe una relación del personal técnico que participará, así como su función y cualificación. Todo lo relativo al desarrollo de los aspectos técnicos del proyecto se puede englobar en el llamado *plan de implantación*.
- **Plan de mantenimiento y formación**. Documento que normalmente exige el cliente donde se deben indicar los procedimientos de mantenimiento requeridos por la red, así como los conocimientos sobre la misma que deben adquirir los técnicos que vayan a mantener dicha red.

- **Informe de certificación de calidad**. En muchas ocasiones el cliente exige diferentes certificaciones relacionadas con la implantación en los procesos de prestación del servicio de planes de calidad. El certificado más importante en este ámbito es el relacionado con las normas ISO 9000.
- **Informe de certificación EN-50173**. Como se ha visto anteriormente, existen métodos estandarizados para comprobar las características del cableado. Los dispositivos conocidos como certificadores emiten dichos informes que en muchos casos son también exigidos por los clientes como garantía de la correcta instalación del cableado.
- **Presupuestos**. Un elemento importante dentro de la documentación es la información relativa a los costes necesarios para llevar a cabo el proyecto. En los presupuestos habrá que desglosar todos los gastos indicando tanto el coste de los materiales como el coste por la mano de obra de los técnicos.
- **Planos de la instalación**. Es habitual entregar al cliente diferentes planos de las instalaciones indicando la ubicación de los diferentes elementos que forman parte de la red.

IMPORTANTE

Un ejemplo de los principales puntos a tratar en la **memoria técnica del proyecto** sería:

- **Objeto del documento**. Contiene una breve explicación del contenido de la memoria técnica del proyecto.
- **Alcance**. Contiene una breve explicación sobre la finalidad y el ámbito de aplicación del documento.
- **Normativa de referencia**. En este apartado se deberán enumerar todas las normativas que se cumplirán para la realización del proyecto.
- **Descripción del lugar** de la instalación.
- **Estudio de la solución aportada**.
  - Red de servicio.
  - Red de acceso.
  - Recinto TIC.
  - Subsistemas.
  - Electrónica de red.
  - Canalizaciones.
  - Red eléctrica.

La documentación técnica final que normalmente es necesario entregar al cliente deberá incluir la siguiente información:

- Esquema general de las infraestructuras de comunicación.
- Número y tipo de tomas de usuario.
- Grado de ampliación de las infraestructuras existentes (cuando corresponda).
- Descripción completa y diagrama de cada uno de los armarios de comunicaciones.
- Descripción detallada y cálculos de dimensionamiento del sistema eléctrico.

- Canalizaciones empleadas, indicando dimensiones, accesorios necesarios y material de fabricación. Se detallarán los procedimientos de instalación de cada tipo de canalización en cada zona concreta del edificio.
- Tipo de cables y n.º de conductores. Tipo de conectores y rosetas. Se detallarán los materiales de fabricación y las características exigibles.
- Dispositivos de red utilizados, normalmente *switches* y puntos de acceso, aunque también pueden incluirse otros como *routers*, *firewalls*, balanceadores de carga, inyectores de potencia PoE, convertidores de medios, etc. Se deberá indicar marca, modelo y sus principales características.
- Procedimientos detallados de instalación de todos los elementos que aseguren la calidad del sistema.
- Descripción completa de la obra civil asociada.
- Etiquetado y documentación de todo el sistema.
- Plan de implantación, incluyendo fases de ejecución y estimación del tiempo empleado en completar cada fase. En el caso en que se necesite un plan de migración del servicio de voz y datos, se incluirá en detalle.

8.4.7 NORMATIVA APLICABLE

Las normativas aplicables a la puesta en servicio de redes de área local pueden ser de varios tipos:

- **Normativas generales**. Estas normativas se refieren a aspectos genéricos que no están relacionados directamente con infraestructuras de comunicaciones, pero que pueden incluir condiciones de obligado cumplimiento en la puesta en servicio de las redes.
  - Reglamento de seguridad e higiene en el trabajo.
  - Ordenanzas municipales de prevención de incendios.
  - Reglamento electrotécnico de baja tensión, del Ministerio de Industria, Energía y Turismo.
  - Normas tecnológicas de la edificación – Instalaciones, del Ministerio de Obras Públicas, Transporte y Medio Ambiente.
  - Norma básica de la edificación – Condiciones de protección contra incendios en los edificios (NBE CPI-96).
- **Normativas específicas de infraestructuras de comunicación**. Las dos primeras referencias se refieren a la normativa de obligado cumplimiento en el caso de que la red telemática entre en el ámbito de las llamadas ICT (infraestructuras comunes de telecomunicaciones). El resto de referencias se refieren a los requisitos del cableado para cualquier red telemática.
  - Reglamento regulador de las infraestructuras comunes de telecomunicaciones, aprobado en el R. D. 346/2011, para el acceso a los servicios de telecomunicaciones en el interior de las edificaciones.
  - Desarrollo del reglamento regulador de las infraestructuras comunes de telecomunicaciones para el acceso a los servicios de telecomunicación en el interior de las edificaciones aprobado en la Orden ITC/1644/2011.

- UNE-EN 50173-1: 2009. Tecnología de la información. Sistemas de cableado genérico. Parte 1: Requisitos generales.
- UNE-EN 50174-1:2011. Tecnología de la información. Instalación del cableado. Parte 1: Especificación de la instalación y aseguramiento de la calidad.
- UNE-EN 50174-2:2011. Tecnología de la información. Instalación del cableado. Parte 2: Métodos y planificación de la instalación en el interior de los edificios.
- UNE-EN 50174-3:2005. Tecnología de la información. Instalación del cableado. Parte 3: Métodos y planificación de la instalación en el exterior de los edificios.
- UNE-EN 50346:2004. Tecnologías de la información. Instalación de cableado. Ensayo de cableados instalados.
- UNE-EN 50085-1/A1:1999. Sistemas de canales para cables y sistemas de conductos cerrados de sección no circular para instalaciones eléctricas. Parte 1: Requisitos generales.
- UNE-EN 61386-23:2005. Sistemas de tubos para la conducción de cables. Parte 23: Requisitos particulares. Sistemas de tubos flexibles.
- UNE-EN 61537:2007. Conducción de cables. Sistemas de bandejas y de bandejas de escalera.

■ **Normativas sobre compatibilidad electromagnética**. La compatibilidad electromagnética persigue tanto la reducción de las emisiones electromagnéticas de los equipos como su inmunidad frente a perturbaciones ajenas, presentes en el medio de transmisión. Ejemplos:

- UNE-EN 61000 – 6 – 3:2002. Compatibilidad electromagnética (CEM). Parte 6: Normas genéricas. Sección 3: Norma de emisión en entornos residenciales, comerciales y de industria ligera.
- UNE-EN 61000 – 6 – 1: 2007. Compatibilidad electromagnética (CEM). Parte 6-1: Normas genéricas. Inmunidad en entornos residenciales, comerciales y de industria ligera.
- UNE-EN 55024:2001. Equipos de tecnología de la información. Características de inmunidad. Límites y métodos de medida.

■ **Normativas sobre protección contra incendios**. Estas normativas se refieren a la utilización de cableado con cubierta retardante del fuego y escasa emisión de humos tóxicos, así como al uso de canalizaciones apropiadas:

- IEC 332. Norma relativa a la propagación de la llama y el retardo del fuego.
- IEC 754. Norma relativa a la emisión de gases tóxicos.
- IEC 1034. Norma relativa a la emisión de humo.
- UNE-EN 13501-1:2007. Clasificación en función del comportamiento frente al fuego de los productos de construcción y elementos para la edificación.

8.5 PUESTA EN SERVICIO

La fase de puesta en servicio se refiere a la ejecución de los trabajos necesarios para implantar la red siguiendo los criterios elaborados durante la fase de planificación. Una de las tareas realizadas durante esta fase es el seguimiento. Para llevar a cabo dicho proceso de seguimiento será necesario establecer una serie de condiciones:

- **Interlocutores**. Durante la fase de ejecución del proyecto y para llevar a cabo el seguimiento se deberán especificar las personas encargadas de supervisar, junto con los responsables del proyecto, los trabajos de puesta en servicio.
- **Reuniones de seguimiento**. El intercambio de información utilizada para realizar el seguimiento del proyecto se hace en las reuniones de seguimiento. Estas reuniones, además, se utilizarán para proponer cambios o establecer soluciones para circunstancias no previstas en la planificación.
- **Informes de seguimiento**. La información sobre la marcha del proyecto deberá quedar reflejada en estos informes.

8.5.1 PLAN DE IMPLANTACIÓN

Una de las herramientas de gestión utilizadas en la puesta en servicio de las redes locales es el llamado **plan de implantación**, que no es más que una guía de las fases técnicas que se deben ir completando de forma secuencial para la consecución del proyecto.

Se entregará un plan de implantación detallado, en el que se incluirá un diagrama de Gantt o cronograma y se especificarán claramente las diferentes fases y actividades del proyecto, indicándose su duración, las fechas de inicio y fin de las mismas, los horarios, las áreas de trabajo, la cantidad de personal y los perfiles de trabajo que hay que emplear en cada fase del proyecto y la descripción detallada de cada actividad y procedimientos detallados de instalación especificando en qué consiste, cómo se va a ejecutar y el resultado que hay que obtener una vez finalizada. Las fechas, horarios y zonas de trabajo deberán haber sido consensuadas previamente por parte de la empresa instaladora con el/la administrador/a del centro correspondiente.

Las fases que formarán parte del plan de implantación dependerán del proyecto concreto. A continuación se muestra un ejemplo genérico:

1. Suministro de materiales.
2. Instalación y acondicionado del *distribuidor de edificio* y los *distribuidores de planta*.
3. Instalación de canalización vertical y canalización horizontal de zonas comunes.
4. Instalación de cableado troncal vertical.
5. Instalación de cableado horizontal en las cajas de telecomunicaciones, terminados en los conectores RJ45 hembra.
6. Instalación de paneles de parcheo y conexionado del cableado horizontal en los mismos.
7. Certificación de los enlaces según normativa vigente.
8. Etiquetado de la instalación completa.
9. Terminación del cableado vertical en los paneles de fibra y de parcheo correspondientes.

10. Parcheo de tomas de datos a la electrónica de red.
11. Instalación de los latiguillos en los puestos de usuario.
12. Elaboración de la documentación de fin de proyecto.
13. Entrega de documentación.

8.5.2 CERTIFICACIÓN DE LA INSTALACIÓN

En muchas ocasiones y para asegurar la calidad de la instalación se debe llevar a cabo la certificación del cableado. Todos los enlaces instalados de cableado horizontal deben ser certificados de acuerdo con los procedimientos descritos en la norma EN 50346: 2002 con el aparato de medida homologado y calibrado al efecto, debiéndose presentar el modelo de equipo y su fecha de última calibración.

La certificación medirá para cada enlace los valores de todos los parámetros especificados por la norma EN 50173 para la clase correspondiente. La información de certificación normalmente se puede entregar en formato electrónico.

Cada enlace certificado estará etiquetado con el número de toma (n.º armario – caja – dígito o letra de la toma).

La aceptación de la infraestructura estará condicionada por tanto al cumplimiento de la clase correspondiente por parte de todos los enlaces. Adicionalmente, se deberán realizar todas las pruebas, comprobaciones y depuraciones necesarias de funcionamiento de la infraestructura de cableado en su totalidad, antes de la puesta en servicio a nivel de usuario.

PROYECTO
ID. Cable: S 1H-083
LUGAR:
Fecha / Hora: 11/03/2011 11:35:37am
OPERADOR:
Versión de Software: 2.3600
NVP: 68.2% Fecha de calibración: 25/08/2010

Sumario de Pruebas:PASA
Paso Libre: 5.1 dB (NEXT del Remoto 12-36)
Límite de Prueba: ISO11801 Channel Class E
Tipo de Cable: Cat 6A UTP
DTX-1800 N/S: 8662005 DTX-CHA001
DTX-1800R N/S: 8662006 DTX-CHA001
Version de Limites: 1.5000

Mapa de Cableado: PASA Result. TERM. RJ45: 1 2 3 4 5 6 7 8
(T568B) TERM. RJ45: 1 2 3 4 5 6 7 8

Par	Longitud (m)	Lím.	Tiempo de Prop. ns	Lím.	Diferenc. Retardo ns	Lím.	Resistencia ohm.	Lím.	Impedancia ohm.	Lím.	Pérdida inserción Result. (dB)	Frec. MHz	Lím. (dB)
12	112.0		548	555	27	50	15.1	25.0			5.1	248.5	35.8
36	107.1		524	555	3	50	14.6	25.0			5.3	249.0	35.9
45	106.5		521	555	0	50	14.6	25.0			6.0	250.0	35.9
78	112.9		552	555	31	50	15.4	25.0			5.2	246.5	35.7

	Resultados Principales						Resultados del Remoto					
	Peor Margen			Peor Valor			Peor Margen			Peor Valor		
Par	Margen (dB)	Frec. MHz	Lím. (dB)	Margen (dB)	Frec. MHz	Lím. (dB)	Margen (dB)	Frec. MHz	Lím. (dB)	Margen (dB)	Frec. MHz	Lím. (dB)
RL												
12	10.0	215.5	8.7	10.0	215.5	8.7	9.0	3.0	19.0	14.4	155.5	10.1
36	9.3	53.3	14.7	12.9	216.5	8.6	6.5	67.0	13.7	9.4	247.0	8.1
45	8.8	69.5	13.6	11.2	236.0	8.3	6.8	5.9	19.0	7.7	191.0	9.2
78	9.3	102.5	11.9	10.2	146.0	10.4	9.2	3.0	19.0	10.9	182.0	9.4
PS NEXT												
12	7.5	7.5	56.1	10.4	192.0	32.2	7.4	79.5	38.8	11.4	228.0	30.9
36	7.7	30.9	45.8	9.7	224.0	31.0	6.9	79.5	38.8	10.4	238.5	30.5
45	9.1	30.9	45.8	10.8	224.0	31.0	8.4	7.5	56.1	10.6	224.0	31.0
78	8.3	7.6	55.9	12.2	192.0	32.2	8.9	5.0	59.0	12.5	246.5	30.3
PS ACR-N												
12	8.2	7.5	50.4	17.1	236.0	-4.2	7.3	3.1	58.0	18.4	248.0	-5.6
36	8.9	9.6	47.8	14.8	224.0	-2.8	8.0	4.1	56.1	15.8	238.5	-4.5
45	10.7	7.5	50.4	16.3	224.0	-2.8	8.5	4.3	55.8	17.2	245.5	-5.3
78	8.0	3.3	58.0	19.4	234.0	-4.0	8.1	3.9	56.6	17.7	246.5	-5.4
NEXT												
12-36	7.5	4.9	61.7	11.1	222.5	34.0	5.1	79.3	41.6	9.9	228.5	33.8
12-45	12.4	237.0	33.5	12.4	237.0	33.5	11.7	5.8	60.5	13.3	247.5	33.2
12-78	5.8	7.6	58.5	10.1	192.0	35.1	8.2	66.8	42.9	11.4	157.0	36.6
36-45	6.6	30.9	48.5	9.0	224.0	33.9	6.2	22.8	50.7	9.9	224.0	33.9
36-78	9.0	122.0	38.5	9.0	122.0	38.5	8.6	5.0	61.5	13.8	246.5	33.2
45-78	13.4	9.4	57.0	14.6	188.5	35.2	11.7	83.5	41.3	12.8	247.5	33.2
ACR-N												
12-36	7.6	4.8	57.3	16.1	222.5	0.3	7.7	79.3	22.5	15.6	238.5	-1.5
12-45	14.7	4.3	58.3	18.3	237.0	-1.4	12.4	5.8	55.5	19.3	246.0	-2.4
12-78	6.0	3.3	60.5	16.9	234.0	-1.0	7.1	3.3	60.5	21.9	248.5	-2.7
36-45	8.2	30.9	36.8	14.5	224.0	0.1	7.1	7.5	52.9	15.4	224.0	0.1
36-78	11.1	9.8	50.3	21.0	246.0	-2.4	9.2	5.0	56.8	18.9	246.5	-2.4
45-78	14.1	9.4	50.7	24.4	244.5	-2.2	9.9	4.1	58.6	18.2	245.5	-2.3
ACR-F												
12-36	17.5	126.0	21.2	17.9	204.5	17.0	16.7	210.0	16.8	16.7	210.0	16.8
12-45	18.0	249.0	15.3	18.0	249.0	15.3	18.6	245.0	15.5	18.6	245.0	15.5
12-78	12.6	4.6	50.0	12.8	242.0	15.6	11.7	249.0	15.3	11.7	249.0	15.3
36-12	16.6	212.0	16.7	16.6	212.0	16.7	17.5	126.0	21.2	18.1	204.5	17.0
36-45	11.4	236.5	15.8	11.5	243.0	15.5	12.5	159.0	19.2	12.9	241.0	15.6
36-78	14.9	179.5	18.2	14.9	179.5	18.2	16.4	182.0	18.1	17.6	223.5	16.3
45-12	18.4	243.0	15.5	18.4	243.0	15.5	17.1	248.5	15.4	17.1	248.5	15.4

Figura 8.8. *Informe de la certificación de una instalación de red*

TEST DE CONOCIMIENTOS

1 En la documentación de la puesta en servicio de una red local se debe incluir:
- **a)** Memoria técnica del proyecto.
- **b)** Presupuestos.
- **c)** Planos.
- **d)** Todos los anteriores.

2 En el cableado horizontal, la distancia máxima que puede existir entre la roseta de usuario y el conector ubicado en el armario de distribución de planta es de:
- **a)** 200 metros.
- **b)** 100 metros.
- **c)** 90 metros.
- **d)** 50 metros.

3 Los armarios de comunicaciones habitualmente son del tipo:
- **a)** Rack de 19".
- **b)** Rack de 25".
- **c)** Rack de 29".
- **d)** Rack de 10".

4 La distancia máxima recomendada entre las tomas de usuario y los equipos es de:
- **a)** 10 metros.
- **b)** 5 metros.
- **c)** 4 metros.
- **d)** 3 metros.

5 El cuarto de comunicaciones deberá disponer de un cuadro eléctrico con dos interruptores diferenciales de:
- **a)** 15 A.
- **b)** 20 A.
- **c)** 25 A.
- **d)** 30 A.

6 Para el correcto dimensionado del sistema se instalarán en cada puesto de trabajo al menos:
- **a)** Una toma de datos.
- **b)** Dos tomas de datos.
- **c)** Tres tomas de datos.
- **d)** El número de tomas de datos se calculan por m^2, no por puestos de trabajo.

9 Normas de gestión de la calidad

Una de las funciones que se debe llevar a cabo dentro del diseño e implantación de las redes telemáticas es la elaboración de la documentación técnica. En muchos casos, dicha documentación técnica debe seguir una serie de normas y ajustarse a ciertas metodologías englobadas en lo que se conoce como sistema de gestión de la calidad.

En este capítulo se expondrán de forma general los conceptos más relevantes relacionados con la aplicación de **sistemas de gestión de calidad** en las empresas, exponiendo las principales características del sistema de gestión de calidad de referencia en el mundo, conocido como ISO 9000.

9.1 INTRODUCCIÓN A LA CALIDAD

Aplicado en el ámbito de los procesos productivos o de realización de servicios, el término **calidad** se refiere al grado de cumplimiento de los requisitos de un producto o servicio. Dicho grado de cumplimiento lo establece normalmente el cliente.

Lo cierto es que el concepto de calidad tal como lo conocemos hoy surge en el siglo XX, es decir, es algo bastante reciente. El primer concepto relacionado con la calidad apareció a principios del siglo XX, donde Frederick W. Taylor implantó sistemas de calidad basados en la **inspección**. Todo lo que se fabricaba debía inspeccionarse para detectar posibles errores. De esta forma se mejoraba la calidad de la producción pero el coste era muy elevado.

Figura 9.1. *La calidad basada en la inspección*

En torno a 1929, Walter A. Shewhart y Edwards Deming desarrollan el control estadístico de procesos, que permite aplicar los conceptos de calidad, pero optimizando los costes asociados. Este sistema se implantará de forma extensa durante la Segunda Guerra Mundial.

Figura 9.2. *Edward Deming, uno de los padres de los conceptos modernos sobre calidad*

En la década de los cincuenta, dentro de un programa de reconstrucción para Japón, varios expertos en calidad viajan a Japón para promover el uso de las técnicas de calidad en las empresas japonesas, factor que se considera clave en el resurgimiento de muchas de ellas. Actualmente los estándares de calidad japoneses están entre los más valorados. Dichos estándares están basados en lo que se conoce como **calidad total**, donde se promueve la implantación de técnicas de calidad no solo al entorno productivo, sino a cualquier ámbito de la empresa.

9.2 EL SISTEMA DE CALIDAD DE UNA EMPRESA

En la actualidad, el sistema de calidad en una empresa constituye un factor de competitividad cada vez más importante. Para ser más competitivos, es necesario identificar y satisfacer las necesidades de los clientes al menor coste posible y, en este aspecto, un sistema de calidad contribuye a lograr estos objetivos.

Los elementos en los que se basa la implantación de sistemas de calidad en una empresa son:

- **Orientación al cliente**. Todos los sistemas de calidad actuales tienen al cliente como eje central, ya que, en último término, es el cliente el que valora la calidad de los productos/servicios que consume. Dos de las estrategias utilizadas en los sistemas de calidad relacionadas con esta función son:
  - Buen servicio de atención al cliente.
  - Sistemas de medición de la satisfacción del cliente.
- **Compromiso de toda la organización**. En los sistemas de calidad se entiende que es necesario que todos los empleados de la empresa se involucren en la implantación de dichos sistemas. En este aspecto un factor clave es la motivación.
- **Prevención**. Una de las metas que persiguen los sistemas de calidad es que los procesos productivos de la empresa sean los más adecuados para que los productos cumplan con los criterios de calidad deseados. En definitiva, se trata de prevenir lo mejor posible la aparición de defectos en la fabricación del producto.
- **Control y seguimiento de resultados**. Otro aspecto fundamental es la realización de mediciones sobre los procesos productivos para poder evaluar si se están cumpliendo los objetivos. De esta forma se pueden detectar y corregir errores en un corto plazo de tiempo. Otra herramienta muy útil en el seguimiento de los productos es la **trazabilidad**, que es la operación mediante la cual es posible encontrar y seguir el rastro en todas las etapas de producción, transformación y distribución de un producto. Para ello se emplean herramientas tales como etiquetados de código de barras, etiquetas electrónicas, soportes informáticos, etc.
- **Uso de un sistema de referencia de calidad**. Otro factor que influye en la implantación de sistemas de calidad es la existencia de sistemas de referencia que proporcione a las empresas una referencia y un apoyo. En este sentido, el sistema de gestión de calidad más extendido a nivel mundial es el denominado ISO 9001, que veremos en los próximos apartados.
- **Mejora continua**. Los sistemas de calidad parten de la idea de que todo es mejorable, por ello, hay que establecer en la empresa mecanismos que favorezcan la evolución de los procesos para su constante mejora.

9.3 PLANES DE CALIDAD

El **Plan de Calidad** de una empresa es la planificación de todas las tareas necesarias para conseguir implantar un sistema de gestión de la calidad, para ello es importante que dicho Plan de Calidad sea conocido y aplicado en toda la empresa. Los principales aspectos que se deberán desarrollar en un Plan de Calidad son:

- ✓ Identificación de los clientes y sus posibles necesidades.
- ✓ Establecimiento de estrategias para conseguir los objetivos de la calidad.
- ✓ Rediseño de los procesos y procedimientos de trabajo.
- ✓ Documentar todas las actividades.
- ✓ Implicar a todo el equipo humano de la organización en la planificación con el apoyo total de la dirección.
- ✓ Estudio económico previo.
- ✓ Elaboración de cronogramas.
- ✓ Asignación de responsables.
- ✓ Asignación de los recursos necesarios para conseguirlo.
- ✓ Cubrir las necesidades de formación.
- ✓ Plan de incentivos a los empleados.
- ✓ Definición de programas de control.
- ✓ Disposiciones legales que hay que seguir, como normativas, permisos, licencias…
- ✓ Desarrollar un plan de seguimiento y de auditorías para comprobar si el Plan de Calidad se desarrolla según lo previsto, para en caso contrario realizar las correcciones.

Para poner en práctica el Plan de Calidad se verán involucrados la mayor parte de los departamentos o áreas de la organización. Las principales funciones dentro del seguimiento del Plan de Calidad de los diferentes departamentos son:

- **Calidad**. El departamento más implicado será, lógicamente, el de calidad, encargándose de toda la parte de planificación, seguimiento, motivación del Plan de Calidad.
- **Comercial**. En este departamento se encargarán de la identificación de los clientes y sus necesidades, así como de realizar el seguimiento de la satisfacción de los clientes.
- **Producción**. Este departamento se encargará principalmente del rediseño de los procesos y procedimientos de trabajo, así como de la documentación de todas las actividades de producción.
- **Financiero**. Este departamento será el encargado de realizar labores de gestión económicas tales como el estudio económico previo o el plan de incentivos a los empleados.
- **Recursos humanos**. En este departamento se llevarán a cabo todas las actividades relacionadas con la gestión de personal incluyendo la contratación del mismo y la gestión de los planes de formación.

9.4 NORMATIVA Y CERTIFICACIONES

Conscientes, desde las instituciones y organismos públicos, de la importancia de la calidad en el crecimiento de las empresas, estos han apoyado su implantación en función de diferentes elementos legislativos. En España se han elaborado una serie de leyes y se han creado instituciones con el fin de proporcionar al conjunto empresarial del país los medios necesarios para asegurar y mejorar la calidad. A todos los elementos creados por la Administración para apoyar, regular y asegurar la calidad en las empresas los llamaremos **la infraestructura de la calidad**.

La primera ley que da apoyo a la calidad en España es la Ley de Industria, Ley 21/1992, de 16 de julio (aparecida en el BOE 176 de 23 de julio). Posteriormente se completa con el *Reglamento de la infraestructura para la calidad y la seguridad industrial*, aparecido en el Real Decreto 2200/1995, de 28 de diciembre (publicado en el BOE 32 de 6 de febrero), y que posteriormente es modificado por el Real Decreto 411/1997, de 21 de marzo de 1997.

La infraestructura para la calidad está basada en los siguientes elementos (Ley de Industria, artículo 19):

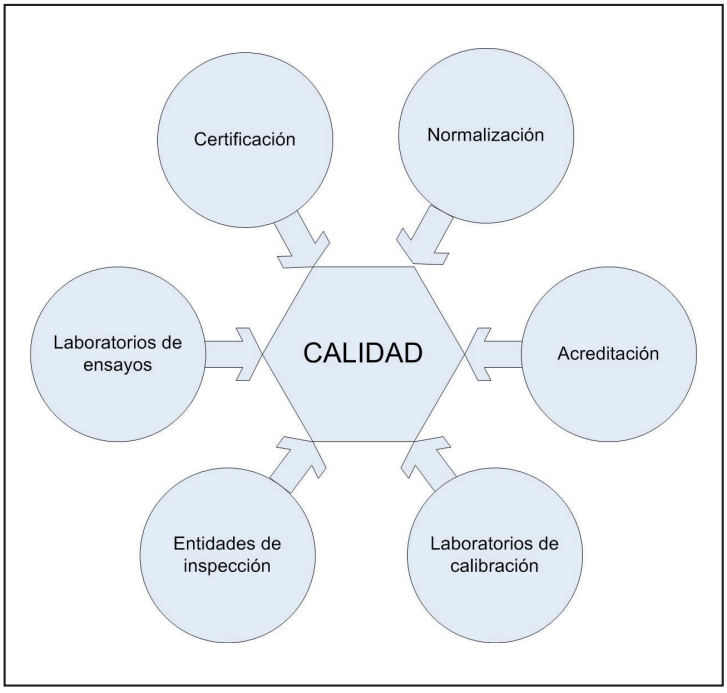


Figura 9.3. *Elementos de la infraestructura para la calidad*

9.4.1 NORMALIZACIÓN

La normalización es el proceso de elaboración de un conjunto de normas que establezca unos criterios comunes para llevar a cabo una acción, por ejemplo, la elaboración de un producto o la prestación de un servicio. En la actualidad, la normalización se considera fundamental en el desarrollo industrial y tecnológico.

A través de la normalización también se establecen normas para, por ejemplo, definir magnitudes, unidades y símbolos, normas de calidad para productos, gestión de la calidad para empresas, normas dimensionales, métodos de ensayo…

Las normas son redactadas por los llamados **organismos de estandarización**. Dichos organismos pueden tener ámbito internacional, continental o nacional.

- **Internacional**. El principal organismo de estandarización es el **ISO** (Organización Internacional de Estandarización). Todas las normas aprobadas por dicho organismo tiene asignado un código que comienza por las letras **ISO**, por ejemplo, ISO 9000.

Figura 9.4. *Logo de la ISO*

- **Europeo**. El principal organismo europeo de normalización es el **CEN** (Comité Europeo de Normalización). Las normas aprobadas en dicho comité reciben un código que comienza por las letras **EN**.
- **Nacional**. El organismo español encargado de la publicación de normas es **AENOR** (Asociación Española de Normalización y Certificación). Las normas publicadas en este organismo reciben un código que comienza por **UNE**.

Cuando una norma nacional deriva de otra de mayor alcance se suele indicar en el propio código de numeración de la norma, conservando el código del organismo de alcance superior. Además, es habitual que al final del código se añada el año de publicación de la norma. Por ejemplo, el código asignado a la norma de gestión de sistemas de calidad es **UNE-EN ISO 9001:2008**.

En el capítulo 1 se hizo un repaso de los principales organismos de estandarización específicos para aspectos tecnológicos relacionados con las telecomunicaciones y las redes de datos. Dos de los más importantes son ITU y IEEE:

Figura 9.5. *Logos de ITU e IEEE*

9.4.2 CERTIFICACIÓN

La **certificación** es el elemento de la infraestructura de calidad que se encarga de comprobar qué producto, proceso o servicio cumple una determinada norma. Esta comprobación la realiza una entidad independiente de las partes interesadas.

En España, las certificaciones las emiten una serie de organismos de certificación que previamente han demostrado su capacidad para hacerlo ante la Administración del Estado. El organismo más conocido que puede emitir certificaciones es AENOR, aunque existen muchos otros. Los certificados que se pueden emitir pueden ser de varios tipos:

Certificados para sistemas de gestión. En este caso la entidad certificadora comprueba si una empresa cumple con todos los requisitos de una norma relacionada con la gestión. La norma sobre sistemas de gestión de calidad más conocida es la ISO 9001. La certificación es voluntaria y, cuando se obtiene, la empresa está autorizada para utilizar un distintivo que acredita que dicha empresa cumple la norma.

Figura 9.6. *Logotipo de AENOR para una empresa registrada que cumple la norma ISO 9001*

Certificados de productos. En este caso se comprueba que un producto cumple las especificaciones técnicas y las características incluidas en una norma. Si se obtiene el certificado se debe marcar el producto con el correspondiente logotipo. Para este tipo de certificaciones es habitual que intervengan otras entidades como laboratorios de ensayo o entidades de inspección que se encargan de comprobar las propiedades y características del producto.

Figura 9.7. *Logotipo de producto certificado*

9.4.3 ACREDITACIÓN

La **acreditación** es el procedimiento por el cual un organismo autorizado reconoce formalmente que una organización es competente para la realización de una determinada actividad relacionada con la infraestructura de calidad.

Por tanto, los organismos de acreditación son los encargados de comprobar, mediante evaluaciones independientes e imparciales, la competencia de los siguientes evaluadores de la conformidad:

- ✓ Entidades de certificación.
- ✓ Laboratorios de ensayo.
- ✓ Laboratorios de calibración.
- ✓ Entidades de inspección.
- ✓ Verificadores medioambientales.

En España, el único organismo reconocido para llevar a cabo tareas de acreditación es **ENAC** (Entidad Nacional de Acreditación).

Figura 9.8. *Logotipo de ENAC*

9.4.4 LABORATORIOS DE ENSAYO

Los laboratorios de ensayo son entidades públicas o privadas reconocidas como imparciales e independientes que se encargan de comprobar si las propiedades de un producto, proceso o servicio cumple una norma específica.

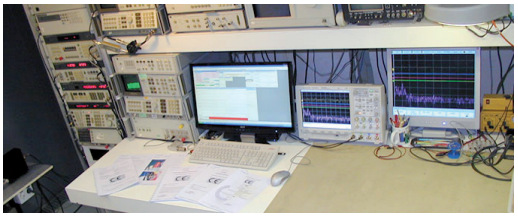


Figura 9.9. *Laboratorio de ensayo*

Un laboratorio de ensayo debe estar acreditado por ENAC y tendrá un alcance determinado dependiendo de la capacidad y competencia técnica del mismo. Todos los laboratorios de ensayo deben cumplir la norma UNE-EN ISO 17025 para poder ser acreditados por ENAC.

9.4.5 LABORATORIOS DE CALIBRACIÓN

Los laboratorios de calibración son las entidades de la infraestructura para la calidad que se encargan de calibrar los instrumentos de medida de los laboratorios de ensayo. Para llevar a cabo las tareas de calibración de los instrumentos de medida se realizan mediciones y se comparan estas medidas con patrones de referencia para certificar que el error está dentro de unos márgenes de tolerancia.

Los laboratorios de calibración tienen que estar acreditados por ENAC dentro de un alcance técnico determinado, dicha acreditación se realiza en función de la norma UNE-EN ISO 17025.

9.4.6 ENTIDADES DE INSPECCIÓN

Las entidades de inspección se encargan de realizar las auditorías iniciales y periódicas de los sistemas de control de calidad de las empresas. Además, se encargan de llevar a cabo estudios, realizar ensayos y revisiones de productos, equipos o instalaciones industriales en materia de seguridad.

Al igual que el resto de elementos de la infraestructura para la calidad, las entidades de inspección deben estar acreditadas por ENAC para llevar a cabo su función.

9.5 PROCESOS Y PROCEDIMIENTOS

Se entiende por **proceso** en el contexto de los sistemas de gestión de calidad una secuencia de tareas o actividades interrelacionadas que tiene como fin producir un determinado resultado a partir de unos elementos de entrada y que se vale para ello de unos ciertos recursos.

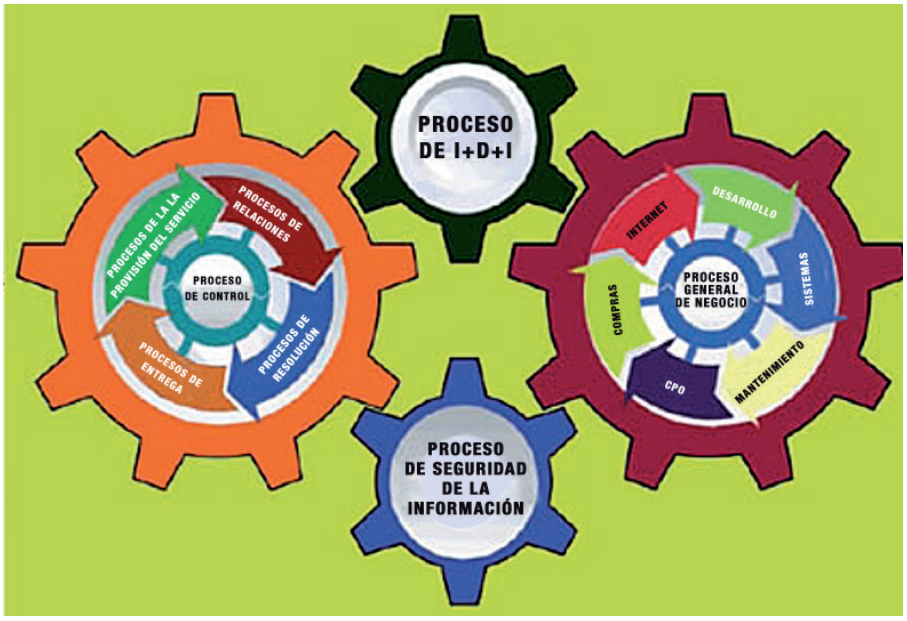


Figura 9.10. *Todas las actividades de una organización se pueden ver como procesos*

Los procesos incluyen los siguientes elementos:

- **Entradas**: materiales, componentes, información, energía, etc., que son necesarios para realizar el proceso.
- **Salidas**: resultado del proceso.
- **Proveedor**: la entidad que proporciona las entradas al proceso. Los proveedores pueden ser internos (dentro de la organización) o externos (empresas proveedoras externas a la organización).

- **Cliente**: destinatario del proceso. Éste puede ser interno o externo.
- **Recursos**: elementos que se se necesitan para llevar a cabo el proceso.
- **Actividades y procedimientos**: las actividades son el conjunto de tareas que es necesario completar para llevar a cabo el proceso. La descripción de cómo se lleva a cabo una determinada actividad se conoce como procedimiento.
- **Indicador**: es un valor numérico que mide alguna característica del proceso.
- **Propietario del proceso**: es el responsable del proceso.
- **Controles**: son las reglas que nos permiten conocer el estado del proceso. Normalmente se basan en la utilización de los indicadores.

Veamos ahora un ejemplo de proceso en una empresa cuya actividad es el diseño, construcción y mantenimiento de equipos informáticos. Un proceso típico podría ser el **montaje de equipos informáticos**. Dicho proceso refleja la secuencia de tareas que se llevan a cabo en la empresa para montar/construir un equipo informático.

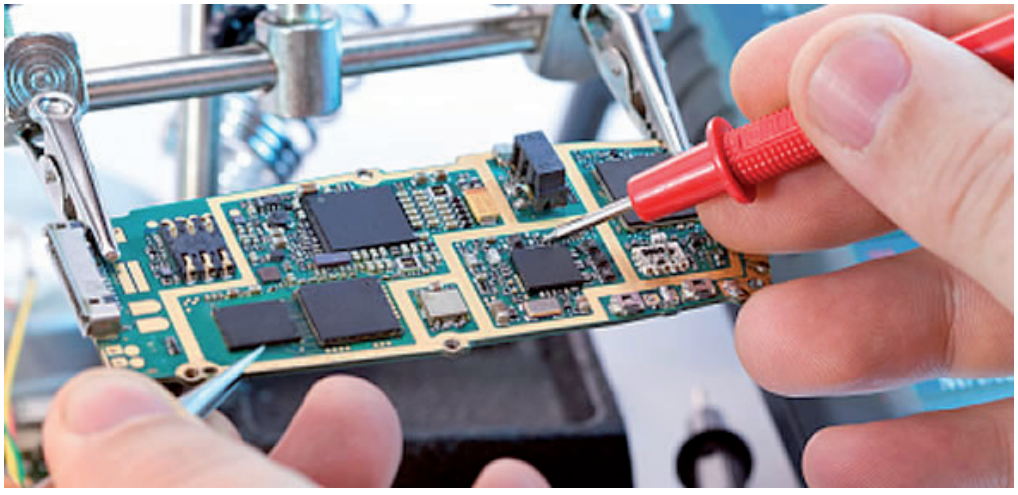


Figura 9.11. *El montaje de equipos informáticos puede ser visto como un proceso*

Sus elementos serían los siguientes:

- **Entradas**: todos los elementos utilizados para el montaje, placa base, discos duros, carcasas, microprocesadores, memorias, etc.
- **Salida**: los equipos informáticos ya montados y operativos.
- **Proveedor**: en este caso todos los proveedores son externos y serían las empresas que nos suministran las entradas. Podría ser un solo proveedor o varios.
- **Cliente**: en este caso los clientes son a su vez empresas que van a vender los equipos informáticos. Es decir, nuestra empresa no venderá equipos al usuario final.

- **Recursos**: en este caso los recursos necesarios serían todo el instrumental necesario para el montaje, el mobiliario y la mano de obra, es decir, los técnicos.
- **Actividades y procedimientos**: las actividades serían todas las tareas que es necesario realizar para obtener la salida del proceso. Aquí se incluyen tanto las actividades de montaje como de comprobación y testeo, actividades de seguimiento, de puesta a punto, etc. Cada una de las actividades se puede describir mediante su correspondiente procedimiento.
- **Indicador**: un indicador podría ser el número de equipos finalizados por día, o el número de equipos con errores de montaje detectados en una semana…
- **Propietario** del proceso: en este caso puede ser el departamento de producción.
- **Controles**: el control más inmediato en este caso es establecer el número de equipos que se deben montar en un período de tiempo, de forma que al hacer un seguimiento de este dato se puede controlar si el proceso está funcionando correctamente o existe algún problema.

En la descripción anterior de los procesos se ha definido también el término "procedimiento". Un **procedimiento** describe cómo se hace una determinada tarea o actividad dentro de un proceso. Por tanto, un procedimiento suele estar reflejado como un documento donde se explica cómo hacer una actividad, quién la debe hacer, dónde, cuándo, los materiales, equipos y documentos utilizados, así como los controles que se llevan a cabo sobre dicha actividad.

El enfoque basado en procesos de las actividades y tareas de una empresa es uno de los elementos imprescindibles para implantar un sistema de gestión de calidad. Los pasos para ello son:

1. Llevar a cabo la identificación y secuencia de los procesos.
2. Elaborar la descripción de cada uno de ellos, definiendo todos sus elementos.
3. Realizar el seguimiento y la medición de los procesos para conocer los resultados que se obtienen.
4. Proponer la mejora de los procesos en función del seguimiento realizado.

Los procesos no tienen que estar directamente relacionados con las actividades de producción o prestación de servicios. A continuación se exponen algunos ejemplos típicos de procesos:

- ✓ Proceso comercial.
- ✓ Proceso de compras.
- ✓ Proceso de subcontratación.
- ✓ Proceso de facturación.
- ✓ Proceso de diseño.
- ✓ Formación.
- ✓ Mantenimiento.
- ✓ Planificación estratégica de la dirección.
- ✓ Servicio posventa.
- ✓ Proceso de planificación de actividades.
- ✓ Proceso de selección de proveedores.

9.6 NORMAS PARA LA GESTIÓN DE LA CALIDAD: ISO 9000

9.6.1 FAMILIA DE NORMAS ISO 9000

La **Organización Internacional de Normalización** (ISO) se encarga de la publicación de una familia de normas relacionadas con los sistemas de gestión de calidad y que se agrupan bajo el código **ISO 9000**. Estas normas pueden ser usadas por cualquier tipo de empresa de cualquier tamaño y características. Son válidas tanto para empresas fabricantes como para empresas de servicios y organizaciones públicas. La familia de normas ISO 9000 está formada por tres normas:

ISO 9000:2005	**Fundamentos y vocabulario** Esta norma describe los fundamentos de los sistemas de gestión de calidad y define los principales conceptos relacionados con la calidad. La última versión de esta norma es del año 2005.
ISO 9001:2008	**Requisitos** Esta norma incluye todos los requisitos que debe cumplir un sistema de gestión de calidad, por tanto esta norma es CERTIFICABLE. Su última versión es del año 2008.
ISO 9004:2009	**Gestión para el éxito sostenido de una organización** Esta norma incluye el enfoque de gestión de la calidad para asegurar el cumplimiento de los requisitos de calidad a largo plazo. Esta norma no es certificable y su última versión es del año 2009.

9.6.2 LA NORMA UNE-EN ISO 9001:2008

Como se ha visto en el apartado anterior, esta norma incluye los requisitos que un sistema de gestión de calidad debe cumplir. Si una empresa cumple dichos requisitos recibe la denominación de "empresa certificada". Las empresas certificadoras se encargan de comprobar que un sistema de gestión de calidad cumple la norma ISO 9001. Las principales características de esta norma son:

- ✓ Esta norma sustituye a la norma ISO 9001:2000.
- ✓ Norma certificable.
- ✓ La norma incide en el ENFOQUE BASADO EN PROCESOS.
- ✓ Todos los requisitos de esta norma internacional son genéricos y se pretende que sean aplicables a todas las organizaciones sin importar su tipo, tamaño y producto suministrado.
- ✓ Los términos y definiciones aplicados en esta norma son los que aparecen en la norma ISO 9000:2005.

- ✓ Se ha intentado que exista una cierta compatibilidad con la norma ISO 14001 (sistemas de gestión medioambiental, actualmente ISO 14001:2004).
- ✓ Los requisitos que las organizaciones deben cumplir sobre esta norma se encuentran especificados en los capítulos 4, 5, 6, 7 y 8 de la misma.
- ✓ Exclusiones permitidas. Las únicas exclusiones que permite la norma son las que se refieren al capítulo 7, siempre y cuando estas exclusiones no afecten a la capacidad o responsabilidad de la organización para proporcionar productos que cumplan los requisitos del cliente y los reglamentos aplicables.

9.6.3 CONTENIDO CERTIFICABLE DE LA NORMA ISO 9001

A continuación se describen brevemente los contenidos de los capítulos de la norma ISO 9001:2008 que incluyen los requisitos a cumplir por los sistemas de gestión de calidad:

■ **Capítulo 4. SISTEMA DE GESTIÓN DE CALIDAD**

- Este capítulo contiene todo lo relacionado con el enfoque basado en procesos: identificación de procesos, análisis, recursos, control, seguimiento, mejora continua.
- Además contiene la descripción de la documentación que se debe incluir en el sistema de gestión de la calidad.

■ **Capítulo 5. RESPONSABILIDAD DE LA DIRECCIÓN**

En este capítulo se habla de los elementos clave en los que se basa la responsabilidad de la dirección, que son:

- Transmitir a todos los miembros de la organización su prioridad por conseguir la satisfacción del cliente y cumplimentar las prescripciones legales.
- Enunciar su política de calidad comunicándola a toda la organización.
- Establecer objetivos de calidad para todos los niveles.
- Asumir la responsabilidad de la revisión del sistema de la calidad. Las herramientas utilizadas para llevar a cabo la revisión podrán ser las siguientes:
  - Informes de las auditorías internas realizadas en el período.
  - Reclamaciones, sugerencias e informaciones de los clientes.
  - Resultados de la ejecución de los procesos y de la evaluación de los productos.
  - Informes sobre las acciones correctivas y preventivas realizadas.
  - Estudios realizados por la dirección en relación con el desarrollo del sistema.
  - Modificaciones internas o externas con influencia sobre el sistema de calidad.
  - Recomendaciones para la mejora.

  Los resultados de la revisión del sistema de calidad serán la mejora de los productos y la eficacia de los procesos.
- Asegurar los recursos necesarios para el desarrollo del sistema.

Capítulo 6. GESTIÓN DE LOS RECURSOS

Este capítulo está dedicado a establecer los requisitos sobre la gestión de los recursos de la empresa, que pueden ser de tres tipos:

- Recursos humanos: personas capaces para el desarrollo de los procesos.
- Infraestructura: La norma establece que la empresa proporcione y mantenga la infraestructura adecuada para el desarrollo de los procesos. La infraestructura puede ser:
  - Edificios, espacios de trabajo y servicios asociados.
  - Equipos para los procesos (tanto hardware como software).
  - Servicios de apoyo tales como transporte o comunicación.
- Ambiente de trabajo: se cuidará que el ambiente de trabajo sea el más adecuado para la eficacia de las operaciones.

Capítulo 7. REALIZACIÓN DEL PRODUCTO

Planificación

- Planificar la realización del producto (o la prestación del servicio). Aquí se incluyen:
  - Las especificaciones que definen el producto final.
  - La documentación adecuada, la metodología más conveniente y los recursos necesarios para llevar a cabo el proceso de ejecución del producto.
  - Los controles necesarios para garantizar el cumplimiento de los requisitos del producto tales como inspecciones, mediciones, actividades de evaluación y seguimiento y ensayos de todo tipo, así como los criterios de aceptación y rechazo.
  - Definición de los registros de calidad necesarios para dejar constancia del cumplimiento de los requisitos establecidos.
  - Determinar los requisitos relacionados con el producto (por ejemplo, requisitos legales o reglamentarios).
  - Establecer canales de comunicación eficaces con el cliente (información sobre el producto, consultas, contratos, atención de pedidos, información sobre la satisfacción, quejas…).

Diseño y desarrollo

- Planificación del diseño y desarrollo.
- Documentar los resultados esperados del diseño y desarrollo, los procedimientos de revisión, de verificación y de validación, así como el procedimiento de control de cambios del diseño y desarrollo.

Compras

Garantizar que los productos comprados se reciben de acuerdo con las especificaciones determinadas para los mismos. Para ello los productos deben adquirirse a proveedores previamente evaluados y seleccionados.

Producción y prestación del servicio

- Control de la producción y de la prestación del servicio.
- Identificación y trazabilidad.
- Preservación del producto (manipulación, embalaje, almacenamiento y protección).

Control de los dispositivos de seguimiento y de medición

■ **Capítulo 8. MEDICIÓN, ANÁLISIS Y MEJORA**

- Demostrar la conformidad del producto, mediante el seguimiento y la medición de los procesos y productos.
- Control del producto no conforme.
- Asegurarse de la conformidad del sistema de gestión de la calidad (auditorías internas).
- Mejorar continuamente la eficacia del sistema de gestión de la calidad.

9.6.4 PROCESO DE CERTIFICACIÓN DE LA NORMA ISO 9001:2008

Los pasos que las empresas u organismos que deseen obtener la certificación de la norma ISO 9001 tienen que dar son los siguientes:

1. **Solicitud**: el primer paso es solicitar la certificación a cualquier entidad de certificación acreditada por ENAC.
2. **Análisis de la documentación**: la entidad certificadora comprueba y analiza la documentación sobre el sistema de gestión de calidad de la empresa y emite un informe.
3. **Visita previa**: los auditores de la entidad de certificación conciertan una entrevista en las instalaciones de la empresa para comprobar el grado de implantación del sistema de calidad y aclaran las posibles dudas que puedan surgir.
4. **Auditoría inicial**: estudio oficial del cumplimiento de los requisitos de la norma ISO 9001. Se redacta un informe donde se reflejan las posibles no conformidades.
5. **Plan de acciones correctoras**: en caso de existir no conformidades, la empresa tiene un plazo para presentar un plan de acciones correctoras dirigido a subsanar dichas no conformidades.
6. **Concesión**: una vez superada la auditoría y aprobado el posible plan de acciones correctoras se concede el certificado.
7. **Vigencia y renovación**: el certificado es válido durante tres años, pasados los cuales es necesario realizar una auditoría de renovación de certificado. Además, se realizarán auditorías anuales de seguimiento.

9.6.5 DOCUMENTACIÓN EN UN SISTEMA DE GESTIÓN DE CALIDAD

Uno de los elementos clave en un sistema de gestión de calidad es la documentación, utilizada para describir cómo se organizan todas las actividades de una organización. Uno de los lemas de la calidad es "Escribir todo lo que se hace, hacer todo lo que está escrito".

En el capítulo 4 de la norma ISO 901:2008 se describen los tipos de documentos que debe contener un sistema de gestión de calidad, además dicha norma especifica que se deben establecer procedimientos para el control y la gestión de dicha documentación. A continuación se describen todos los tipos de documentos requeridos:

- **Registros**

  Son los documentos que se utilizan para reflejar todos los resultados que sean necesarios para demostrar la conformidad con los requisitos y la operación eficaz del sistema. Con los datos generados en los registros se pueden llevar a cabo estudios sobre la eficiencia de los procesos, así como para realizar auditorías. Algunos ejemplos de registros son:

  – Resultados de calibración y verificación de maquinaria.
  – Resultados de validación del diseño y desarrollo.
  – Evaluaciones de los proveedores.
  – Resultados de las acciones preventivas.
  – Resultados de las acciones correctivas.

- **Instrucciones de trabajo**

  Son documentos técnicos donde se especifican de forma clara y ordenada las instrucciones para llevar a cabo una actividad determinada. Este tipo de documentos son elaborados por el personal técnico, aprobados por la autoridad técnica correspondiente y suelen estar disponibles en el propio puesto de trabajo.

  Las instrucciones de trabajo deben contener información clara y precisa de quién hace la actividad, cómo se hace, quién la supervisa, cuándo se hace, los materiales utilizados y el procedimiento de control, verificación y registro de dicha actividad.

- **Procedimientos**

  En este tipo de documentos se describe la realización de las diferentes actividades de la empresa. Se debe especificar tanto la información general de cada actividad como quién la debe realizar, cuándo se realiza, el proceso donde está enmarcada, las actividades relacionadas y cualquier otra información de interés. Los procedimientos no deben incluir descripciones de los trabajos técnicos, ya que esta información estará contenida en las instrucciones de trabajo. Algunos ejemplos de procedimientos que pueden elaborarse en una empresa son los siguientes: control de los procesos de realización, compras, evaluación de proveedores, planificación y control de la producción.

  La norma ISO 9001 indica una serie de procedimientos que deben estar documentados y que son los siguientes:

  – **Control de los documentos**: en este procedimiento se debe indicar la forma de actualizar, almacenar e identificar la documentación de la empresa referida al sistema de calidad.

  – **Control de los registros**: igualmente, la empresa debe especificar en este procedimiento la gestión de los registros, es decir, identificación, almacenamiento, protección, recuperación, disposición, vigencia.

  – **Auditoría interna**: en este procedimiento se indica cómo se llevan a cabo las auditorías internas.

  – **Control del producto no conforme**: en este procedimiento se debe indicar la identificación de los tipos de no conformidades, es decir, los productos que no cumplen las especificaciones.

– **Acción correctiva**: en este caso se deben especificar las acciones que hay que realizar cuando existan productos no conformes.

– **Acción preventiva**: en este procedimiento se deben indicar las acciones que ha de tomar la empresa para prevenir la aparición de productos no conformes.

■ **Manual de calidad**

Este documento es el elemento principal de toda la documentación del sistema de gestión de calidad y en él se incluyen referencias al resto de documentos del sistema. El manual de calidad deberá incluir información sobre la política de calidad y los objetivos de la organización, una breve explicación de los requisitos aplicables de la norma (los capítulos del 4 al 7 mencionados anteriormente), una descripción de la relación entre los procesos (mapa de procesos), y los detalles y justificación de cualquier exclusión de la norma (aplicable solo a requisitos del capítulo 7).

Por último, hay que indicar que el manual de calidad debe ser aprobado por la dirección de la organización y revisado al menos una vez al año, con el objetivo de mantenerlo actualizado.

EJERCICIOS PROPUESTOS

1. Visita la página web de AENOR (*www.aenor.es*) y responde las siguientes cuestiones:

- ¿Cuál es el precio de la norma ISO 9001:2008 en AENOR?
- ¿En qué año comenzó AENOR a realizar tareas de normalización?
- En la certificación de sistemas de gestión, ¿cuántos meses pueden transcurrir como máximo desde la auditoría inicial a la primera auditoría de seguimiento?
- ¿Cuál sería el precio y duración de un curso de calibración de equipos de medida en AENOR, impartido en el mes de marzo?

2. Visita la página web de ENAC (*www.enac.es*) y responde a las siguientes cuestiones:

- ¿Cuáles son las tarifas que aplica ENAC para la acreditación de un sistema de gestión de calidad UNE-EN ISO 9001?
- ¿Cada cuánto tiempo se hace una reevaluación de una entidad acreditada por ENAC?
- Obtén al menos cinco entidades acreditadas por ENAC para certificar sistemas de calidad en tu comunidad autónoma de residencia.
- Obtén otras cinco entidades acreditadas por ENAC como laboratorios de ensayo de tipo eléctrico en tu comunidad autónoma de residencia.

3. Una de las formas de describir un proceso es utilizando una ficha de procesos. En este ejercicio se pide rellenar la siguiente ficha para dos procesos elegidos por el alumno referentes a la prestación del servicio de alojamiento en un hotel.

HOTEL EC				REF-0023
PROCESO:		PROPIETARIO:		
MISIÓN:		DOCUMENTACIÓN:		
ENTRADA:				
PROVEEDOR:				
SALIDA:				
CLIENTE:				
INSPECCIONES:		REGISTROS:		
INDICADORES:		VARIABLES DE CONTROL:		

HOTEL EC				REF-0024
PROCESO:		PROPIETARIO:		
MISIÓN:		DOCUMENTACIÓN:		
ENTRADA:				
PROVEEDOR:				
SALIDA:				
CLIENTE:				
INSPECCIONES:		REGISTROS:		
INDICADORES:		VARIABLES DE CONTROL:		

TEST DE CONOCIMIENTOS

1 ¿Qué factor es el que más influye en la mejora de la competitividad de una empresa?

a) Tener un director exigente.
b) Implantar un sistema de gestión de la calidad.
c) Ofrecer productos a bajo coste.
d) Tener el número mínimo de personal contratado.

2 El elemento clave en un sistema productivo es:

a) El equipo directivo.
b) El cliente.
c) Los proveedores.
d) La inspección del producto.

3 La implantación de un sistema de gestión de la calidad es un compromiso:
- **a)** De la dirección exclusivamente.
- **b)** De toda la organización.
- **c)** De toda la organización excepto los empleados sin categoría específica.
- **d)** Solo del departamento de calidad, con ayuda de la dirección.

4 Algunas de las actividades relacionadas con la calidad como la contratación del personal o los planes de formación se realizan en el departamento de:
- **a)** Calidad.
- **b)** Comercial.
- **c)** Producción.
- **d)** Recursos humanos.

5 ¿Qué elemento de la infraestructura de la calidad se encarga de comprobar si las propiedades de un producto se corresponden con las especificaciones?
- **a)** Entidades de acreditación.
- **b)** Entidades de inspección.
- **c)** Laboratorios de ensayos.
- **d)** Laboratorios de calibración.

6 La normalización en España la realiza:
- **a)** Solo ENAC.
- **b)** AENOR y ENAC.
- **c)** Solo AENOR.
- **d)** Cualquier empresa certificada para normalizar, aunque AENOR es la principal.

7 ¿Qué departamento se encarga de hacer el seguimiento de la satisfacción del cliente?
- **a)** Departamento de recursos humanos.
- **b)** Departamento de producción.
- **c)** Departamento de calidad.
- **d)** Departamento financiero.

8 El certificado de Registro de Empresas se obtiene si se cumplen los requisitos de la norma:
- **a)** UNE-EN ISO 9004:2000.
- **b)** UNE-EN ISO 9001:2008.
- **c)** UNE-EN ISO 14001:2004.
- **d)** UNE-EN ISO 9000:2005.

9 ¿Qué elemento de la infraestructura de calidad se encarga de comprobar si los instrumentos de medida de un laboratorio de ensayo miden correctamente?
- **a)** Entidades de acreditación.
- **b)** Laboratorios de calibración.
- **c)** Entidades de inspección.
- **d)** Centro Español de Metrología.

10 ¿Cómo se llama la acción de comprobar si una empresa u organización cumple con una determinada norma de gestión de la calidad?
- **a)** Normalizar.
- **b)** Certificar.
- **c)** Acreditar.
- **d)** Autorizar.

11 ¿Qué entidad realiza en España la tarea de comprobar que las entidades de certificación realizan su función con garantías?
- **a)** ENAC.
- **b)** ISO.
- **c)** AENOR.
- **d)** Las respuestas *b* y *c* son correctas.

12 La infraestructura de la calidad se refiere a:
- **a)** El departamento de calidad de cada empresa.
- **b)** Las normas publicadas por la ISO.
- **c)** El apoyo de las instituciones públicas mediante leyes y reales decretos.
- **d)** Todas las empresas que hacen auditorías.

Solucionario de los test de conocimientos

- CAPÍTULO 1:

  1A 2B 3B 4A 5C 6B 7B 8D 9D 10C 11C

- CAPÍTULO 2:

  1C 2C 3B 4B 5C 6A 7C 8B 9B 10A 11A 12D

- CAPÍTULO 3:

  1C 2D 3D 4B 5D 6D 7A 8D 9A 10D

- CAPÍTULO 4:

  1D 2A 3C 4B 5C 6C

- CAPÍTULO 5:

  1C 2B 3D 4C 5C 6B 7C 8A 9A 10C 11B 12C

- CAPÍTULO 6:

  1D 2A 3C 4D 5C 6D 7A 8C 9A 10D

- CAPÍTULO 7:

  1D 2C 3B 4A 5B 6C

- CAPÍTULO 8:

  1D 2C 3A 4D 5C 6B

- CAPÍTULO 9:

  1B 2A 3B 4D 5C 6C 7C 8B 9B 10B 11A 12C

Índice Alfabético

CERTIFICADO DE PROFESIONALIDAD

Diseño de Redes Telemáticas

Esta obra trata de ofrecer una visión general de las redes telemáticas, incluyendo los principios generales sobre la transmisión de datos, los diferentes medios de transmisión, así como las principales características de los sistemas de cableado estructurado.

En la segunda parte se da un amplio repaso a las tecnologías, protocolos y dispositivos utilizados en el diseño e implantación de redes telemáticas, incluyendo un capítulo con las principales pautas de cómo afrontar un proyecto de diseño de una red telemática. El último capítulo está dedicado a un elemento clave en el desarrollo de cualquier servicio o producto actual y que cualquier técnico debería conocer: el *sistema de gestión de la calidad* en una empresa.

El autor mantiene un blog sobre las redes telemáticas donde el lector puede ampliar información: *redestelematicas.com*

9 788499 642611

ra-ma.es

Ra-Ma®