Una red de área local necesita una serie de elementos para funcionar, fundamentalmente equipos, adaptadores de red, cableado y dispositivos de interconexión. Sin embargo, esto no es suficiente para que la red funcione correctamente, ya que necesita de una serie de programas que se ejecutan en los equipos y que se encargan de controlar las comunicaciones.

3.1 INTRODUCCIÓN A LOS PROTOCOLOS

En una red de comunicación es necesario que todos los equipos sigan una serie de normas para que la comunicación se pueda llevar a cabo correctamente y con fluidez. A las normas se les denomina **protocolos** y deben respetarse o de lo contrario la comunicación no se realizará en buenas condiciones.

Los problemas más importantes que deben resolver los protocolos de comunicación en una red de área local son el encaminamiento, el direccionamiento, el control del acceso al medio, la saturación del receptor, el mantenimiento del orden, el control de errores y la multiplexación. Estos problemas se resuelven en los distintos niveles de la arquitectura de red donde se ubica cada protocolo específico.

3.2 MODELO DE INTERCONEXIÓN DE SISTEMAS ABIERTOS (OSI)

El modelo **OSI** (Open Systems Interconnection o Interconexión de Sistemas Abiertos) está basado en una propuesta establecida en el año 1983 por la organización internacional de normas **ISO** (ISO 7498) como un avance hacia la normalización a nivel mundial de protocolos. El modelo se llama **modelo de referencia OSI de la ISO**, puesto que se ocupa de la conexión de **sistemas abiertos**, esto es, sistemas que están preparados para la comunicación con sistemas diferentes. Usualmente lo llamaremos sólo modelo OSI para acortar.

OSI emplea una arquitectura en niveles a fin de dividir los problemas de interconexión en partes manejables. Posteriores estándares de ISO definieron las implementaciones en cada nivel para asegurar que se consigue una compatibilidad total entre ellos. La aproximación en niveles asegura modularidad y facilita que el **software** pueda mejorarse sin necesidad de introducir cambios revolucionarios, además de permitir la compatibilidad entre equipos diferentes. Consta de siete niveles, mostrados en la tabla 3.1.

Tabla 3.1. Los siete niveles de OSI

Nivel	Nombre
7	Aplicación
6	Presentación
5	Sesión
4	Transporte
3	Red
2	Enlace de datos
1	Físico

Pero, ¿cómo llegó la ISO, partiendo desde cero, a definir una arquitectura a siete niveles de esas características? Los principios teóricos en los que se basaron para la realización de OSI fueron fundamentalmente los siguientes:

- Cada capa de la arquitectura está pensada para realizar una función bien definida.
- El número de niveles debe ser suficiente para que no se agrupen funciones distintas, pero no tan grande que haga la arquitectura inmanejable.
- Debe crearse una nueva capa siempre que se necesite realizar una función bien diferenciada del resto.
- Las divisiones en las capas deben establecerse de forma que se minimice el flujo de información entre ellas, es decir, que la interfaz sea más sencilla.
- Permitir que las modificaciones de funciones o protocolos que se realicen en una capa no afecten a los niveles contiguos.
- Utilizar la experiencia de protocolos anteriores. Las fronteras entre niveles deben situarse donde la experiencia ha demostrado que son convenientes.
- Cada nivel debe interaccionar únicamente con los niveles contiguos a él (es decir, el superior y el inferior).
- La función de cada capa se debe elegir pensando en la definición de protocolos estandarizados internacionalmente.

OSI está definido más bien como modelo, y no como arquitectura. La razón principal es que la ISO definió solamente la función general que debe realizar cada capa, pero no mencionó en absoluto los servicios y protocolos que se deben usar en cada una de ellas. Esto quiere decir que, al contrario que el resto de arquitecturas de redes, el modelo OSI se definió antes de que se diseñaran los protocolos.

Las funciones encomendadas a cada una de las capas OSI son las siguientes:

- **Nivel físico**: tiene que ver con la transmisión de dígitos binarios por un canal de comunicación. Las consideraciones de diseño tienen que ver con el propósito de asegurarse de que, cuando un lado envíe un "1", se reciba en el otro lado como "1", no como "0". Las preguntas típicas aquí son: ¿qué voltaje deberá usarse para representar un 1 y para representar un 0?, ¿cuántos microsegundos dura cada dígito?, ¿en qué frecuencia de radio se va a transmitir?, ¿cuántas puntas tiene el conector de la red y para qué sirve cada una?, etc. Aquí las consideraciones de diseño tienen mucho que ver con las interfaces mecánica, eléctrica y de procedimientos y con el medio de transmisión físico que está bajo la capa física.
- **Nivel de enlace**: su tarea principal es detectar y corregir todos los errores que se produzcan en la línea de comunicación. También se encarga de controlar que un emisor rápido no sature a un receptor lento, ni se pierdan datos innecesariamente. Finalmente, en redes donde existe un único medio compartido por el que circula la información, este nivel se encarga de repartir su utilización entre las estaciones. La unidad mínima de datos que se transfiere entre entidades pares a este nivel se llama **trama** o **marco**.

- **Nivel de red**: se ocupa de determinar cuál es la mejor ruta por la que enviar la información. Esta decisión tiene que ver con el camino más corto, el más rápido, el que tenga menor tráfico, etc. Por todo esto, la capa de red debe controlar también la congestión de la red, intentando repartir la carga lo más equilibrada posible entre las distintas rutas. También a este nivel se realiza gran parte del trabajo de convertir y adaptar los mensajes que circulan entre redes heterogéneas. La unidad mínima de información que se transfiere a este nivel se llama **paquete**.
- **Nivel de transporte**: es el nivel más bajo que tiene independencia total del tipo de red utilizada y su función básica es tomar los datos procedentes del nivel de sesión y pasarlos a la capa de red, asegurando que lleguen correctamente al nivel de sesión del otro extremo. A este nivel, la conexión es realmente de extremo a extremo, ya que no se establece ninguna conversación con los niveles de transporte de todas las máquinas intermedias.
- **Nivel de sesión**: a este nivel se establecen sesiones (conexiones) de comunicación entre los dos extremos para el transporte ordinario de datos. A diferencia del nivel de transporte, a este nivel se proporcionan algunos servicios mejorados, como la reanudación de la conversación después de un fallo en la red o una interrupción, etc.
- **Nivel de presentación**: a este nivel se controla el significado de la información que se transmite, lo que permite la traducción de los datos entre las estaciones. Por ejemplo, si una estación trabaja con un código concreto y la estación del otro extremo maneja uno diferente, el nivel de presentación es el encargado de realizar esta conversación. Para conversaciones confidenciales, este nivel también codifica y encripta los datos para hacerlos incomprensibles a posibles escuchas ilegales.
- **Nivel de aplicación**: es el nivel que está en contacto directo con los programas o aplicaciones informáticas de las estaciones y contiene los servicios de comunicación más utilizados en las redes. Como ejemplos de servicios a este nivel se pueden mencionar la transferencia de archivos, el correo electrónico, la mensajería instantánea, las videoconferencias, etc.

Este modelo no es perfecto y, de hecho, algunas cuestiones adolecen de un mal diseño. La más importante, en lo que se refiere a las capas, es que algunas de ellas están prácticamente vacías (es decir, hay muy pocos protocolos definidos dentro de éstas y a la vez son bastante triviales), mientras que otras están llenas a rebosar. Por ejemplo, las capas de sesión y presentación no se usan en la mayoría de las aplicaciones, mientras que las capas más inferiores están saturadas que en revisiones posteriores se han dividido en múltiples subcapas.

Otro problema que tiene OSI es que existen algunas funciones que se repiten en muchas de las capas, lo que hace que muchos servicios y programas estén duplicados, a la vez que contribuye a un aumento del tamaño de las cabeceras de control de los bloques de información que se transmiten.

3.3 EL NIVEL FÍSICO

El nivel físico de una arquitectura es quizá la parte más importante de la red. La razón fundamental es que la mayoría de los protocolos de las capas superiores, dependen de sus características físicas (velocidad, tasa de error, medio compartido o no, etc.). Por ejemplo, si la transmisión ofrece una tasa de error muy baja, el protocolo de control de errores a niveles superiores puede ser muy simple. En caso de que el medio soporte una capacidad de transmisión elevada, entonces el sistema de comunicaciones podrá ofrecer servicios como transmisión de vídeo y datos a alta velocidad.

Todas las arquitecturas de redes por niveles (OSI, TCP/IP, ATM, etc.) distinguen un nivel físico que es el encargado de realizar el transporte de la información a través del medio físico de transmisión. Esta tarea fundamental se debe llevar a cabo teniendo en cuenta dos condiciones básicas:

- Si se envía un "1" utilizando la variación de alguna propiedad física del medio, al receptor le deberá llegar exactamente esa misma variación de la propiedad para que pueda interpretarlo como un "1" y no como un "0".
- Cuando el emisor envía una sucesión de dígitos binarios, se debe garantizar que se reciban en el mismo orden en el otro extremo.

Para poder realizar este transporte, los protocolos del nivel físico deben tener en cuenta muchas cuestiones de fondo. Podemos exponer las más importantes: ¿de qué manera se envían los dígitos binarios por el medio?, ¿qué ocurre si el medio sólo permite la transmisión en un sentido?, ¿cómo se corrigen las distorsiones y perturbaciones que sufre la señal en el camino?, ¿es posible que por el mismo medio circulen varias transmisiones a la vez?, ¿qué medio de transmisión resulta más adecuado para el envío de la información?

Sobre un cable de comunicación o el aire se pueden realizar diferentes tipos de comunicaciones que se clasifican en diferentes criterios:

- Teniendo en cuenta la sincronización: debe existir un mecanismo que permita saber al receptor cuándo está recibiendo información y cuándo llega cada dígito o bit del mensaje. Hay dos tipos de comunicaciones:
  - Síncrona: se usa una señal periódica que identifica la llegada de cada dígito del mensaje.
  - Asíncrona: se usa una señal especial que se envía al principio y al final de cada dígito del mensaje.
- Teniendo en cuenta las características de la señal:
  - Analógica: la señal enviada puede tomar un número infinito de valores. Este tipo de señal se utilizaba tradicionalmente en el sistema telefónico convencional y era muy propenso a propagar interferencias.

  - **Digital**: la señal enviada solamente puede tomar un número limitado de valores. Este tipo de señal mejora la calidad de las comunicaciones y permite controlar mejor el ruido y los errores.
- Teniendo en cuenta el sentido de la comunicación:
  - **Simplex**: la transmisión sólo se puede realizar en un sentido, por lo que se necesitan dos medios de transmisión para que la comunicación pueda ser en las dos direcciones.
  - **Semidúplex**: la transmisión se puede realizar en los dos sentidos, pero no a la vez.
  - **Dúplex integral**: la transmisión se puede realizar en los dos sentidos y al mismo tiempo.

Todo medio está limitado por una velocidad de transmisión máxima. La velocidad de transmisión se mide en **bits por segundo** o **bps**. Las velocidades actuales que se pueden conseguir con algunos medios de transmisión son una combinación de su capacidad y de las características de la señal utilizada.

3.4 PROTOCOLOS DE NIVEL DE ENLACE

La tarea que lleva a cabo el nivel físico es aceptar un flujo original de información en bruto (procedente del nivel del enlace) e intentar entregar dicha información a su destino a través del medio de transmisión. No se garantiza que este flujo de información esté libre de errores. El número de dígitos recibidos puede ser menor, igual o mayor y sus valores pueden ser diferentes a los dígitos transmitidos. Será el nivel de enlace de datos el que detecte esos errores y tomará las medidas necesarias para corregirlos. Para conseguir este objetivo, habitualmente se divide la información a transmitir en pequeños bloques de datos, cada uno de los cuales llevan asociado un código detector de error y un número de orden o secuencia.

Este número de secuencia se usa para que el receptor pueda mantener el orden. También se usa en caso de que uno de ellos sufra un error, de forma que se podrá identificar el que el emisor debe retransmitir. De esta forma, se consigue que un error no implique la retransmisión de todo el mensaje, sino sólo una pequeña parte de él.

La máxima responsabilidad que asume el nivel de enlace es el control de errores. Esta tarea no es fácil teniendo en cuenta que los circuitos electrónicos y los cables de comunicación no son perfectos y sufren distorsiones que procedes del exterior. Por otra parte, existe la posibilidad de incluir suficiente información de control en cada bloque de forma que el receptor pueda ser capaz de reconstruir la información original en caso de que llegue errónea. Puesto que esa **información redundante** crece exponencialmente con el tamaño de la información, generalmente no se utiliza y se gana en eficiencia cuando se retransmite un bloque dañado.

El nivel de enlace de datos tiene un número de **funciones** específicas por desarrollar. Entre estas funciones, los protocolos de enlace de datos deben realizar las siguientes:

- Agrupar los dígitos o caracteres recibidos por el nivel físico en bloques de información, llamados **tramas** (o frames), a los que va asociada información de control para proporcionar todos los servicios de esta capa y unas marcas que señalizan el comienzo y el fin.
- Detectar y solucionar los errores generados en el canal de transmisión (tramas erróneas, incompletas o perdidas totalmente).
- Controlar el flujo, para evitar saturar al receptor, es decir, permitirle el tiempo de proceso necesario para no perder ninguna trama.
- Controlar el diálogo, en canales semidúplex o donde se utiliza un medio compartido, será necesario establecer los turnos para la transmisión.
- Identificar a unos equipos de otros a través del direccionamiento, ya que muchas veces los mensajes llegan a todos y solamente el destinatario es el autorizado a recogerlo.

Habitualmente, los protocolos de nivel de enlace de datos se dividen en dos categorías: los protocolos de enlace de datos de alto nivel, diseñados para establecer una interfaz común y así facilitar la interacción con protocolos de niveles superiores y los protocolos de enlace de datos de bajo nivel, centrados fundamentalmente en el control de acceso al medio.

3.4.1 Protocolos de control de enlace lógico (LLC)

Los protocolos de enlace de datos de alto nivel o **LLC** (Logical Link Control o Control de Enlace Lógico) están diseñados para ofrecer todos los servicios necesarios a los protocolos de nivel de red que están por encima y gestionar las funciones más importantes. Los protocolos más importantes que se utilizan actualmente en este nivel de la arquitectura de red son HDLC e IEEE 802.2.

El protocolo **HDLC** (High-level Data Link Control o Control de Enlace de Datos de Alto Nivel) es un estándar a nivel de enlace de datos basado en el protocolo SDLC inventado por IBM para su red SNA. Se utiliza en RDSI y en X.25, aunque no se siguen sus especificaciones completas, ya que es un protocolo muy extenso (se utilizaban más bien otros protocolos basados en éste, como SDLC, LAP-B, LAP-D, PPP, LLC o Frame Relay).

El protocolo HDLC y sus derivados son orientados a conexión y utilizan unas marcas especiales para delimitar el principio y el fin de las tramas, que son números de 8 bits con esta forma: “01111110”. Para el control de errores utiliza una variante de la codificación CRC-CCITT, además de los acuses de recibo en las transmisiones y los números de secuencia en las tramas, lo que lo hace muy robusto. Por todo ello, las redes que utilizan HDLC en su nivel de enlace de datos no necesitan controlar la mayoría de los errores en los niveles superiores.

El estándar **IEEE 802.2** define los protocolos de la capa LLC en redes Ethernet. IEEE 802.2 permite tres clases distintas de servicio que se pueden utilizar según las necesidades: servicio no orientado a la conexión y no fiable (para poder enviar tramas a uno o varios equipos a la vez), servicio no orientado a la conexión y fiable y servicio orientado a la conexión y fiable. Si el servicio es fiable, entonces las tramas incluyen un número de secuencia que permite mantener el orden de los mensajes recibidos en el destino. Una cabecera de trama 802.2 está basada en el protocolo HDLC, aunque con algunas diferencias. Esta cabecera de control se inserta dentro del campo de datos de una trama IEEE 802.3.

3.4.2 Protocolos de control de acceso al medio (MAC)

En redes locales, lo normal es que exista un único medio de transmisión por el que todas las estaciones se comunican. Por ello, es necesario diseñar protocolos que permitan el uso por turnos de las estaciones que quieren transmitir. El problema del reparto del medio es a veces difícil de solucionar, sobre todo porque puede existir gran cantidad de estaciones que no se sabe cuándo van a transmitir, aunque normalmente lo hacen muy esporádicamente.

Los protocolos encargados de "moderar" en una conversación entre estaciones que comparten el medio se encuentran en la parte inferior del nivel de enlace de datos, y en algunas arquitecturas, como OSI, se han incluido en una subcapa llamada **subnivel de acceso al medio** o **MAC** (Medium Access Control). El control de acceso al medio es una de las características que diferencian las redes LAN de las WAN. En estas últimas, lo normal es que los enlaces entre nodos o estaciones de la red sean punto a punto, es decir, solamente comunican dos estaciones en los extremos, aunque cada una de ellas tenga más de un enlace.

Cuando dos o más estaciones transmiten a la vez en un medio de difusión (es decir, en el mismo segmento de red), se produce un fenómeno denominado **colisión**. En esas circunstancias, las señales enviadas se "mezclan" y ninguna de ellas puede ser interpretada correctamente (se pierden), por lo que normalmente no es deseable que ocurra. Algunas tarjetas de red tienen un indicador luminoso que advierte de las colisiones producidas; si se ilumina muchas veces, es probable que la red no esté funcionando correctamente. Las colisiones se producen siempre dentro del ámbito de un segmento de red, por lo que también se conoce como **dominio de colisión**.

Las estaciones pueden acceder al medio de transmisión para comprobar si éste está siendo utilizado por alguna estación para transmitir. Cuando la estación receptora recoge la información que le ha sido enviada, el medio queda otra vez libre para enviar más tramas; mientras tanto, el medio está ocupado. Dependiendo del protocolo utilizado, las estaciones pueden comprobar si el medio está libre o no.

Los algoritmos utilizados para resolver el problema del reparto del canal poseen dos características principales que los definen:

- **El control del tiempo para transmitir**. Existen dos opciones: utilizar un tiempo **continuo** (se puede transmitir en cualquier momento) o **ranurado** (el tiempo se divide en intervalos discretos y la transmisión de una trama se debe realizar siempre al inicio de uno de esos intervalos).
- **La detección de portadora**. La estación puede realizar esta operación (para comprobar si hay alguien transmitiendo) o puede funcionar **sin detección de portadora** (la estación envía y luego comprueba si se ha producido una colisión).

Se conocen muchos algoritmos para repartir un canal de acceso múltiple (actualmente se utilizan más de 20 en las redes de difusión que funcionan en todo el mundo). Muchos de ellos utilizan las mismas ideas de base, aunque con pequeñas modificaciones. Los más importantes se explican brevemente en los siguientes apartados.

3.4.3 Protocolos de contienda

Los protocolos de contienda están diseñados para evitar, en la medida de lo posible, aunque no completamente, que se produzcan colisiones. Se utilizan en redes donde circula una gran cantidad de tráfico y, cada vez que una colisión es detectada, los equipos que han enviado tramas afectadas por ella deben volver a retransmitirlas. Esto puede hacer que la capacidad de transmisión de la red se vea afectada.

La ventaja del uso de los protocolos de contienda para el control de acceso al medio consiste en que el fallo de un equipo nunca va a afectar al funcionamiento de la red y resulta muy sencillo añadir nuevos equipos porque sólo hay que conectarlos. Como inconveniente principal podemos destacar una bajada del rendimiento de la red cuando se producen colisiones, sobre todo en un medio compartido por muchas estaciones.

Uno de los protocolos de contienda más utilizados actualmente en redes locales, es el **CSMA** (Carrier Sense Multiple Access o Acceso Múltiple con Detección de Portadora). Este protocolo tiene varias versiones:

- **CSMA persistente**: consiste en que, cuando una estación desea transmitir, primero escucha el canal para ver si éste está ocupado. Si hay otra estación transmitiendo, se espera a que termine y cuando la estación detecta un canal en reposo, transmite una trama. Si ocurre una colisión (porque otra estación también ha detectado el canal libre y ha transmitido una trama a la vez), la estación espera un tiempo aleatorio y comienza de nuevo. Este protocolo es mejor que los de tipo ALOHA, ya que, cuando las estaciones detectan el canal ocupado, no interrumpen esa comunicación.
- **CSMA no persistente**: funciona de forma similar al anterior, pero, en este caso, cuando una estación desea transmitir y encuentra el canal ocupado, no hace un chequeo continuo de él hasta que quede libre. En su lugar, espera un tiempo aleatorio y vuelve a comprobar el estado del canal. Si está nuevamente ocupado, vuelve a repetir el proceso; en caso contrario, envía la trama por el canal.

- CSMA con detección de colisiones (CSMA/CD): las estaciones también esperan a transmitir si el canal se encuentra ocupado. Una vez que el canal queda libre, la estación comienza a transmitir. Inmediatamente, esa estación es capaz de comprobar si se está produciendo una colisión, por lo que puede abortar ese envío de forma casi instantánea. El no transmitir las tramas completas cuando se produce una colisión ahorra tiempo y ancho de banda.
- CSMA/CA (Carrier Sense Multiple Access and Colision Avoidance o Acceso Múltiple con Detección de Portadora y Prevención de Colisiones): se utiliza en las redes locales inalámbricas (estándar IEEE 802.11). Funciona de igual forma que el protocolo CSMA, pero, en caso de que el medio esté ocupado, todas las estaciones que desean transmitir establecen un turno ranurado siguiendo un protocolo de mapa de bits.

3.4.4 Protocolos de paso de testigo

Los protocolos de paso de testigo (token passing) están libres de colisiones porque cada una de las estaciones tiene un intervalo definido de tiempo para transmitir. Para ello, utilizan una trama especial llamado testigo que las estaciones se van pasando unas a otras en orden. Solamente la estación que tiene en su poder ese testigo podrá transmitir y, cuando lo haga, cederá el testigo a la siguiente. Este protocolo impide que se produzcan colisiones, pero se complica debido a que determinados errores físicos en la red o cuelgues en las estaciones pueden hacer que se pierda el testigo, por lo que son necesarios mecanismos que permitan restaurarlo.

3.4.5 Otros protocolos

El protocolo de mapa de bits es un ejemplo de acceso al medio en el que no se producen colisiones porque las estaciones mantienen un orden para utilización del canal. El tiempo de uso del canal se alterna en dos intervalos de tiempo: un primer intervalo de tiempo se dedica a que las estaciones se "hagan oír" e indiquen si desean transmitir una trama y una segunda parte en la que las estaciones que han mostrado su intención de transmitir lo hagan (solamente una trama). El primer intervalo de tiempo se divide en tantas ranuras como estaciones se encuentren conectadas al cable. Estas ranuras están numeradas de forma ascendente y, si una estación desea transmitir (por ejemplo, la 6), colocará un "1" en su ranura correspondiente (en este caso, será la ranura número 6). Las estaciones que no hayan puesto un "1" en su ranura en el intervalo de tiempo anterior no pueden transmitir, y deben esperar a que se realice otra vuelta.

3.5 ETHERNET

El estándar IEEE 802 posee un conjunto de especificaciones muy amplio para redes de área local y define sus protocolos a nivel físico, MAC y enlace de datos.

3.5.1 Introducción a Ethernet

Si bien ya se han visto las especificaciones de este estándar a nivel físico, ahora hay que introducir las correspondientes a nivel MAC y nivel de enlace:

- **IEEE 802.2**: define el subnivel de enlace de datos LLC.
- **IEE 802.3**: estándar que define las diferentes tecnologías Ethernet. Utiliza el protocolo CSMA/CD en la subcapa de acceso al medio.
- **IEEE 802.4**: este estándar define una LAN de topología en bus (Token Bus) que utiliza el protocolo de paso de testigo de la subcapa MAC.
- **IEEE 802.5**: define una LAN con topología en anillo (Token Ring) y el protocolo de paso de testigo.
- **IEEE 802.6**: estándar que define las características de una red de área metropolitana (MAN) que utiliza una topología en doble bus. Para el protocolo de la capa MAC, se ha definido un algoritmo parecido a ALOHA ranurado, aunque mucho más perfeccionado.
- **IEEE 802.7**: define las características de una LAN que transmite en banda ancha.
- **IEEE 802.11**: estándar que define las redes locales inalámbricas. Define una transmisión mediante ondas infrarrojas (se trata de la primera versión del estándar IEEE 802.11 que no se utiliza) y microondas, y un acceso al medio mediante el protocolo CSMA/CA. Actualmente, existen varias revisiones de este estándar que permiten mayores velocidades de transmisión (de hasta 2400 Mbps).
- **IEE 802.12**: estándar que define las redes locales 100VG-AnyLAN con el protocolo de **prioridad de demanda** para el control del acceso al medio. Este método consiste en que es el concentrador de cableado el que decide qué estación debe transmitir en un momento dado, por lo que nunca se producen colisiones.

Los estándares IEEE 802.8, 802.9, 802.10, 802.15, Y 802.16 no definen realmente ningún tipo de red local ni protocolos, sino que se trata más bien de comités consultivos que estudian temas relacionados con la transmisión por fibra óptica (802.8), transmisión de voz y datos en redes locales (802.9), seguridad en LAN (802.10), redes de cable para comunicaciones de banda ancha (802.14), redes personales inalámbricas (802.15) y acceso inalámbrico de banda ancha (802.16).

3.5.2 Ethernet y el modelo OSI

El estándar IEEE 802 se utiliza actualmente en muchas arquitecturas de redes comerciales, como TCP/IP, Novell o la utilizada por Microsoft para sus redes locales. El estándar Ethernet también se ha utilizado para definir los protocolos de nivel físico y nivel de enlace de datos del modelo OSI.

3.5.3 Direccionamiento MAC

Las direcciones a nivel de enlace de las redes Ethernet, que normalmente se consideran direcciones de la subcapa MAC, están formadas por números binarios que identifican a las estaciones del resto (por lo que deben ser únicas). Dependiendo del protocolo utilizado, estas direcciones pueden tener un mayor o

menor número de dígitos: por ejemplo, en el estándar de Ethernet (cableado o inalámbrico), Bluetooth y Token Ring, las direcciones MAC son números binarios de 48 dígitos que se suelen expresar como grupos de ocho bits representados en hexadecimal y separados por puntos. Por ejemplo, una dirección MAC podría ser la siguiente:

18.3E.A0.64.F2.01

Las direcciones MAC suelen ir grabadas de fábrica en el propio adaptador de red, de forma que no pueden ser modificadas. Para impedir que en una red puedan existir dos estaciones con las mismas direcciones MAC, los fabricantes suelen convenir en los números que asignan a sus dispositivos. En el caso de las direcciones ethernet y Token Ring, la primera mitad (los 24 primeros bits) identifica al fabricante, mientras que los dígitos restantes identifican de forma única cada adaptador, en una asignación realizada por el propio fabricante. Existen otros tipos de direcciones, como loas empleadas en redes ARCNet, que pueden ser establecidas por el usuario.

En las redes que están construidas con conmutadores también es necesario que exista un mecanismo que identifique de forma única a unas estaciones de otras. Esto es debido a que estos dispositivos funcionan sin necesidad de realizar sobre ellos ninguna configuración previa. Por esta razón, los conmutadores deben ser capaces de obtener las direcciones de los equipos que están conectados a cada uno de sus puertos, almacenarlas y utilizarlas posteriormente para saber por qué puertos deben enviar los mensajes.

La dirección MAC FF.FF.FF.FF.FF.FF es una dirección especial que no puede ser asignada a ningún adaptador de red ni a ningún puerto de comunicación de ningún dispositivo. Esta dirección se utiliza como destino cuando hay que enviar un mismo mensaje a todos los equipos que forman parte de la red. Cuando un puente o un conmutador reciben un mensaje con esta dirección de destino, están obligados a enviarlo a través de todos sus puertos, para que llegue a todos los equipos que tienen conectados.

3.5.4 Trama Ethernet

En una trama Ethernet se incluyen las direcciones MAC de los equipos de origen y destino, un relleno para que la trama tenga una longitud fija (en caso de que el campo de datos sea pequeño) y un código para detectar errores (CRC).

Tabla 3.2 Formato de una trama Ethernet 802.3

Preámbulo	Marca de inicio	MAC destino	MAC origen	802.1Q	Longitud	Datos	Relleno	CRC
56 bits	10101011	48 bits	48 bits	32 bits	16 bits	Hasta 1500 bytes		32 bits

3.5.5 Tecnologías Ethernet

IEEE 802.3 es un estándar que define una familia completa de configuraciones, abarcando diferentes velocidades (desde 10 Mbps hasta 10Gbps), topologías (bus o estrella) y cableado (par trenzado, coaxial y fibra óptica). La tabla 3.3. resume las posibles configuraciones establecidas por el estándar y la nomenclatura utilizada para nombrarlas.

Tabla 3.3. Distintas configuraciones de Ethernet

	Velocidad de transmisión			
Cableado	**10 Mbps (Ethernet)**	**100 Mbps (Fast Ethernet)**	**1 Gbps (Gigabit Ethernet)**	**10 Gpbs (Ethernet a 10Gb)**
Coaxial delgado	10Base-2. Topología en bus	-	-	-
Coaxial grueso	10Base-5. Topología en bus	-	-	-
Par trenzado	10Base-T- Topología en estrella	100Base-T. Topología en estrella	1000Base-T. Topología en estrella	-
Fibra óptica	10Base-F. Topología en estrella	100Base-F. Topología en estrella.	1000Base-F. Topología en estrella	10GBase-S. 10GBase-L. Topología en estrella.

3.6 OTROS PROTOCOLOS DE NIVEL DE ENLACE

En una red local es posible que coexistan diferentes protocolos de nivel de enlace de datos, por ejemplo, es posible que en la red existan equipos que utilizan los protocolos de la red Microsoft y equipos que utilizan los protocolos de Novell. Para solucionar estos problemas, han surgido los protocolos NDIS y ODI, utilizados a nivel de enlace de datos para que una estación de la red pueda utilizar diferentes protocolos de comunicación a niveles superiores, permitiendo también el uso de varios adaptadores simultáneos.

La especificación **ODI** (Open Data-Link Interface o Interfaz Abierta de Enlace de Datos) fue introducida inicialmente en el año 1989 por Novell y Apple, con el objetivo de permitir el uso de múltiples arquitecturas de comunicaciones y múltiples tarjetas de red en una misma estación. ODI define una interfaz en la que aparece el **LSL** (Link Support Layer o Capa de Soporte al Enlace), que se encarga de gestionar distintos protocolos a niveles inferiores, y el **MLID** (Multiple Link Interface Drivers o Enlace Múltiple a Controladores de Interfaz) que se encarga de gestionar el uso de varios adaptadores de red simultáneos.

Por su parte, el protocolo **NDIS** (Network Driver Interface Specification o Especificación de Interfaz de Adaptador de Red) fue diseñado por Microsoft y 3Com para estaciones con sistema operativo DOS, Microsoft Windows y OS/2 también con el propósito de permitir que una estación pudiera manejar diferentes adaptadores de red. A diferencia de ODI, NDIS no da soporte a diferentes arquitecturas y pilas de protocolos (solamente maneja los protocolos de la red Microsoft), pero permite el uso de conexiones de red como RDSI, Frame Relay, ATM, Ethernet o Token Ring. Así mismo, NDIS y ODI pueden coexistir sin problemas dentro de un mismo ordenador, lo que permite extender los tipos de conexiones simultáneas que se pueden realizar.

3.7 PROTOCOLOS DE NIVEL DE RED

La capa de red se encarga de llevar los bloques de información desde el origen hasta el destino. Que esos bloques alcancen al receptor puede suponer muchos saltos por estaciones intermedias, característica que diferencia a esta capa con el nivel de enlace de datos, que sólo se preocupa de la comunicación entre estaciones conectadas al mismo cable. En una red local que utiliza un medio compartido, solamente existe una ruta posible para comunicar dos estaciones, por lo que el nivel de red apenas tiene trabajo; en su lugar, el nivel de enlace deberá realizar la tarea de comprobar si el mensaje va destinado a la estación (y si procede, capturarlo) o no, comprobando la dirección MAC del destinatario.

Para poder realizar su trabajo convenientemente, la capa de red debe conocer la topología física y seleccionar las mejores rutas a través de ella; también deberá tener en cuenta rutas alternativas a modo de evitar congestionamientos o zonas más saturadas, de la misma forma que un viajero selecciona el camino a seguir. Normalmente, la capa de red utiliza algún método (dependiendo del protocolo) para guardar toda la información concerniente a la topología física de la red.

Las funciones principales que llevan a cabo los protocolos del nivel de red son las siguientes:

- **Encaminamiento**: el objetivo principal de una red es hacer llegar los mensajes desde el origen al destino. Generalmente, existen varias rutas alternativas posibles y, por ello, se requiere el uso de un procedimiento que seleccione la ruta más corta, rápida y con la mínima utilización de recursos.
- **Control de la congestión**: cuando en una zona determinada de una red se concentra una gran cantidad de tráfico que hace que su funcionamiento sea ralentizado o entorpecido (con pérdida de mensajes), entonces se dice que se ha producido congestión. Para solucionarlo, se pueden establecer mecanismos que intenten paliar esta situación: rechazando los nuevos paquetes que van llegando o impidiendo que los equipos vecinos saturen la red con más mensajes.

- Direccionamiento: para poder encaminar correctamente los paquetes hacia su destino, se necesita que exista un mecanismo que identifique unívocamente a emisores y receptores. Este mecanismo o direccionamiento a nivel de red suele coexistir en la arquitectura con el direccionamiento a nivel de enlace, que se utiliza para distinguir entre estaciones conectadas al mismo medio (que suele ser compartido). El direccionamiento a nivel de red se puede comparar con el sistema postal. Para que el cartero pueda entregar la correspondencia (paquetes) al destinatario correcto (nodo receptor), es necesario que éste distinga cada uno de los posibles receptores y conozca dónde viven (el enlace o enlaces a los que está conectado en la red). Habitualmente, se utiliza un direccionamiento que permite al cartero conocer la localización exacta del destinatario y la ruta a seguir para alcanzarlo (por ejemplo, el país, provincia, localidad, calle, número, piso, puerta y nombre).

3.7.1 Protocolo de Internet (IP)

Uno de los protocolos más utilizados actualmente a nivel de red, tanto en redes locales como en redes de área extensa, es IP. En los apartados siguientes se explica con detalle.

3.7.1.1 INTRODUCCIÓN A IP

Internet es una red que no posee una estructura bien definida, aunque en general se puede identificar una jerarquía de interconexión: existen varias redes troncales principales (de un gran ancho de banda) conectadas mediante nodos encaminadores rápidos y redes regionales (de menor capacidad) donde están conectadas las LAN y los proveedores de acceso. Por esta razón, muchas personas se refieren a Internet como “la red de redes”.

Para que esta estructura funcione correctamente, se diseñaron en los años ochenta varios protocolos a nivel de red que permitieran que los paquetes fueran enviados correctamente a través de gran cantidad de redes heterogéneas. El más importante es **IP** (Internet Protocol o Protocolo de Interred), definido en RFC 791, que establece el direccionamiento a este nivel y define el formato de los paquetes que se transmiten. El protocolo IP es no orientado a la conexión y no fiable, de forma que el establecimiento de conexiones y el control de errores lo debe llevar a cabo algún protocolo de transporte a niveles superiores, como **TCP** (Transmission Control Protocol o Protocolo de Control de la Transmisión). También existen otros protocolos a nivel de red que se encargan de seleccionar las mejores rutas para el envío de mensajes hacia su destino, generando la información necesaria y actualizando las tablas de los encaminadores.

3.7.1.2 DIRECCIÓN IP

Las direcciones IP que identifican encaminadores y estaciones de la red tienen un tamaño fijo de 32 bits (en la versión 4 del protocolo). Estas direcciones se pueden especificar directamente en binario, aunque resulta más cómodo utilizar la notación decimal con puntos. Para pasar una dirección de binario a decimal, sólo hay que convertir los números tomando de ocho en ocho dígitos; posteriormente se separa cada número en decimal con puntos (de 0 a 255) para construir la dirección completa.

Puesto que no pueden existir dos estaciones o nodos de la red que tengan la misma dirección IP, con este método se pueden nombrar 2^{32} = 4294967296 (aunque, como se verá después, no se pueden usar todas). Cuando se diseñó este método, se consideró que esta cantidad era suficiente para el ritmo de crecimiento esperado de Internet. Hoy en día se ha llegado al límite y las direcciones IP se han agotado.

Una dirección IP tiene dos partes principales: un **identificador de red** y un **identificador de estación** dentro de esa red. El identificador de red se utiliza para numerar cada una de las redes que componen Internet de forma única. Por su parte, el identificador de estación se usa para numerar cada uno de los equipos que forman parte de una red. De esta forma, las direcciones IP tienen una estructura jerárquica igual a las direcciones postales, aunque en este caso solamente a dos niveles. Gracias a este formato, cuando se lee una dirección IP de un equipo de Internet, se puede saber de una forma aproximada dónde se encuentra, simplemente examinando la red a la que pertenece. Así, los protocolos de encaminamiento pueden utilizar esta información para buscar los destinatarios y calcular las mejores rutas de una forma más sencilla.

El problema que plantea la división de las direcciones IP en un número de red y un número de estación consiste en que se trata de números finitos y, por lo tanto, estamos estableciendo límites. A la hora de dividir un número de 32 bits en dos partes, tenemos muchas opciones que podemos considerar. Las más importantes son:

- **Usar ocho bits para número de red y 24 bits para número de estación**, lo que nos permite tener un máximo de 256 redes distintas y 16 millones de equipos por red.
- **Usar 16 bits para número de red y 16 bits para número de estación**, lo que nos permite tener un máximo de 65.536 redes distintas y 65.536 equipos por red.
- **Usar 24 bits para número de red y ocho bits para número de estación**, lo que nos permite tener un máximo de 16 millones de redes distintas y 256 equipos por red.

Para decidir cuál es la mejor opción para Internet, debemos pensar cómo es esta red en realidad. En Internet existe un número muy reducido de redes de gran tamaño, algunas más de tamaño mediano y muchísimas redes de pequeño tamaño.

Si comparamos este hecho con las tres opciones anteriores, vemos que ninguna de ellas se adapta por sí sola a cómo es en realidad Internet.

Sin embargo, si se seleccionan las tres opciones conjuntamente, entonces sí se adapta a la realidad de Internet. Para poder utilizar estas tres opciones a la vez, necesitamos usar un nuevo campo dentro de la dirección IP que identifique su tipo (A, B o C). Este campo se sitúa al principio de la dirección y puede tomar tres valores, dependiendo del tipo de dirección que se esté utilizando. A este tipo de dirección se le denomina **clase** (tabla 3.4).

Tabla 3.4. Campo de clase de dirección en IP

Clase IP	Valor de Campo
A	0
B	10
C	110

Se puede observar que el campo de clase de dirección no es de longitud fija (ocupa un bit para la clase A, dos bits para la B y tres para la C). Gracias a esto, se consigue aprovechar mejor el campo de número de red de la case A, ya que solamente tiene ocho bits. En la tabla 3.5 se indican los rangos de direcciones en decimal asignados a cada clase.

Además de las clases A, B y C, en IP versión 4 se definieron las clases D (campo de clase "1110") y E (campo de clase "11110"). La clase D no se usa para asignar direcciones a equipos, sino para crear grupos de equipos de **multidifusión** o broadcast (esto permite enviar el mismo mensaje a un grupo de equipos a la vez). Por su parte, la clase E se reservó para investigación y desarrollo.

Tabla 3.5. Rangos de direcciones para las clases de IP

Clase IP	Rango	N.º de redes	N.º de estaciones
A	1.0.0.0 – 127.255.255.255	127	16777216
B	128.0.0.0 – 191.255.255.255	16384	65536
C	192.0.0.0 – 223.255.255.255	2097152	256
D	224.0.0.0 – 239.255.255.255	-	-
E	240.0.0.0 – 247.255.255.255	-	-

La complejidad en el uso de las direcciones IP radica en que existen diferentes divisiones de formato: la división en grupos de ocho bits para las conversiones entre decimal y binario, además de la división en redes y estaciones que es relativa a la clase. Por ejemplo, en la dirección "192.168.3.1", el número "192" contiene la clase y el número de red. Por esta razón, la división en redes y estaciones se hace intentando tomar grupos de ocho bits, para evitar que un número decimal pueda contener parte de número de red y parte de número estación.

Ante la escasez de direcciones IPv4 que existe en la actualidad, se ha diseñado una nueva versión de protocolo IP que permite extender el rango de direcciones disponibles y solucionar otros problemas: **IP versión 6**. Esta nueva versión del protocolo está definida en RFC 1752 (recomendaciones), RFC 2373 (direccionamiento y RFC 2460 (especificación completa) y posee las siguientes características:

- Utiliza el algoritmo de encaminamiento RIPing.
- Es capaz de manjar miles de millones de direcciones de estación diferentes, ya que traba con direcciones de 16 bytes.
- Se simplifica la configuración de las estaciones, ya que se reservan 48 bits como número de estación para la subred más pequeña y se puede utilizar la dirección MAC para numerar los equipos de forma automática.
- Reduce el tamaño de las tablas de encaminamiento en los nodos.
- Permite una mayor velocidad de proceso en los nodos, ya que el formato de paquete solo contiene siete campos en su cabecera (en lugar de 13 que tenía la versión 4)
- Es compatible con la versión 4 del protocolo (aunque no totalmente, pero esta cuestión se resuelve utilizando protocolos de traducción de direcciones), de forma que los dos pueden coexistir durante algunos años para permitir una implantación progresiva.

La forma de representar las direcciones IPv6 es distinta de la versión 4, ya que ahora existen 128 bits en lugar de 32. En realidad, las direcciones IPv6 se pueden representar de tres formas diferentes:

- Por ocho números en hexadecimal de 16 bits, separados por dos puntos.
- Igual que la anterior, pero suprimiendo todos los ceros consecutivos en la dirección y sustituyéndolos por "::". Estos "::" solamente pueden aparecer una vez en la dirección.
- Utilizando una notación mixta formada por una parte de dirección v6 (seis números hexadecimales de 16 bits separados por dos puntos) y otra de v4 (cuatro números decimales de ocho bits).

Una dirección IPv6 también tiene varios campos: los primeros bits forman un **prefijo**, que indica el tipo de dirección (véase la tabla 3.6); los bits centrales especifican un número de red (que puede no existir) y los bits finales especifican un número de red (que puede no existir) y los bits finales especifican un número de estación.

Tabla 3.6. Tipos de prefijos en IPv6

Prefijo	Descripción
00	Dirección IPv4.
2 ó 3	Dirección asignada por un proveedor de acceso a Internet.
De FE80 a FEBF	Direcciones privadas dentro del ámbito de la subred.
De FEC0 a FFFF	Direcciones privadas dentro del ámbito de la red (intranet).
FF	Dirección de multidifusión.

En IPv6 también existen las máscaras de red y su función es idéntica a la versión anterior del protocolo. Por su parte, también se utilizan los prefijos, pero en este caso su representación es justamente la contraria a IPv4: un prefijo /50, por ejemplo, indica que los 50 últimos bits de la dirección se reservan para numerar estaciones. La razón de este cambio estriba en que ahora se utiliza gran cantidad de dígitos binarios para numerar redes y subredes, mientras que el número de estaciones es menor con respecto a ellas.

La característica fundamental que define al protocolo IPv6 es la posibilidad de las estaciones para realizar una configuración automática de sus parámetros de red. Gracias a esta característica, no es necesario disponer de conocimientos avanzados para realizar la configuración de la dirección IP de un equipo de la red.

3.7.1.3 ASIGNACIÓN DE DIRECCIONES

Las direcciones IP se configuran manualmente en las estaciones y es el **NIC** (Network Information Center o Centro de Información de la Red) la institución encargada de asignar las direcciones de Internet, para impedir duplicados. Esta autoridad sólo asigna la clase de red y el número de red, y cada administrador de red deberá asignar los sufijos de identificador de estación. Se asignan direcciones de clase A a grandes redes (con muchas estaciones), mientras que se dejan las de clase C a pequeñas redes. Dentro del ámbito de una red local, es el administrador el encargado de asignar las direcciones a los equipos.

Hay algunas direcciones que no se pueden asignar a ninguna estación ya que su uso está reservado para el propio protocolo. Por ejemplo, las direcciones con número de red a 0 se refieren a la red actual (la IP 0.0.0.0 se usa por las estaciones cuando están siendo arrancadas, hasta que se completa la carga del sistema operativo, pero no se usa después). El rango desde 127.0.0.0 hasta 127.255.255.255 se reserva porque se utiliza la dirección 127.0.0.1 para especificar la estación actual, de forma que puede referirse a ella cuando se desea especificar el ordenador local (al igual que podría utilizar la dirección IP asignada). Las direcciones IP con número de estación todo a unos (en binario) se refieren a la red (una red también debe tener una dirección IP por cuestiones de encaminamiento). Las direcciones con número de estación todo a unos (en binario) se utilizan para **difusión** (broadcast), es decir, enviar mensajes a todas las estaciones dentro de la misma red (es decir, para todas estaciones que tienen el mismo identificador de número de red). No hay que confundir las direcciones de difusión de las redes (utilizadas para enviar un mensaje a todas las estaciones dentro de la misma red) con las direcciones de clase D, que, más bien, se utilizan para agrupar estaciones y enviarles mensajes de difusión (éstas pueden pertenecer a redes distintas).

Actualmente, a las clases de direcciones IP también se las conoce por "/8" (clase A), "/16" (clase B) y "/24" (clase C), refiriéndose a que la dirección IP tiene 8, 16 o 24 bits de **prefijo** (compuesto por los bits de clase más los de número de red), respectivamente. Derivada de esta nueva notación, ha aparecido otra nueva forma

de nombrar una dirección IP. Ésta consiste en especificar la dirección en notación decimal con puntos seguida de una barra inclinada y del número de bits que componen el prefijo. Ejemplos de este tipo de notación aparecen en la tabla 3.7.

Tabla 3.7. Ejemplos de direcciones IP

Dirección de estación	Observaciones
118.64.248.86/8	Clase A. Se usan ocho bits para el prefijo de red y 24 bits como número de estación.
129.0.186.63/16	Clase B. Se usan 16 bits para el prefijo de red y 16 bits como número de estación
221.118.7.19/24	Clase C. Se usan 24 bits para el prefijo de red y 8 bits como número de estación

Supongamos que tenemos dos LAN, 198.64.126.0 Y 216.89.3.0. Si utilizamos un encaminador para interconectarlas, éste tendrá dos direcciones IP diferentes (una para cada red que conecta). Cada una de esas direcciones será del tipo correspondiente a la LAN.

La complejidad actual que tienen muchas redes locales hace que la asignación de direcciones pueda llegar a ser muy tediosa y la tarea se complica aún más si se utilizan direcciones IPv6. Por esta razón, en muchas situaciones resulta mucho más efectivo utilizar protocolos que asignan las direcciones de forma automática, como DHCP. También se utilizan protocolos como DNS que permiten utilizar direcciones formadas por letras o nombres en lugar de números, lo que facilita su uso por parte de los usuarios de la red.

3.7.1.4 ENRUTAMIENTO

La razón principal del uso de las direcciones IP consiste en simplificar y optimizar los algoritmos de encaminamiento. Al igual que ocurre con el servicio postal, dividir la dirección en partes permite llegar al destinatario de una forma sencilla y rápida, puesto estas direcciones guardan información sobre su localización. Este método también permite reducir el tamaño de las tablas de encaminamiento.

Antes de hablar del encaminamiento en las estaciones finales de la red, vamos a tratar el funcionamiento de los encaminadores. Cada uno de estos dispositivos dispone de una tabla con los posibles destinos en forma de direcciones IP. En cada fila de esta tabla se especifica la dirección de las redes a las que se puede llegar (destinos), la dirección IP del puerto del encaminador por el que debe salir el mensaje y el número de encaminadores intermedios que es necesario atravesar (o algún otro parámetro que especifique el coste de ese camino, lo que se conoce como la **métrica**). Estas tablas las utilizan los protocolos de encaminamiento y se actualizan dinámicamente mediante el envío de información entre los encaminadores. En una tabla de encaminamiento puede aparecer más de una

entrada con la misma dirección IP de red de destino, y esta situación se da cuando existen varias rutas distintas que alcanzan ese destino.

Las tablas de encaminamiento que usan los encaminadores y otros equipos de una red pueden incluir información adicional además de las direcciones de destino y equipos intermedios. En general, las tablas de encaminamiento pueden incluir la siguiente información:

- **Protocolo de encaminamiento**: es el tipo de protocolo que creó la entrada en la tabla de encaminamiento. Hay que tener en cuenta que un encaminador puede soportar el uso de diferentes protocolos de encaminamiento al mismo tiempo (RIP, IGRP, EIGRP, OSPF, etc.).
- **Red de destino**: dirección IP de la red de destino a alcanzar.
- **Máscara de red**: máscara de red aplicada a la dirección de la red de destino. La mayoría de los protocolos modernos no incluyen este campo, ya se incluye el prefijo de red en la dirección IP de destino.
- **Siguiente**: dirección IP del siguiente equipo (encaminador) para alcanzar el destino.
- **Métrica**: información sobre el coste de esa ruta (dependiendo del algoritmo de encaminamiento utilizado).
- **Interfaz**: nombre del puerto del equipo local por donde enviar el mensaje hacia el destino. Ejemplos de nombres de puertos en encaminadores son “Serial0/0”, “Ethernet0/1”, etc.

3.7.2 Protocolo IPX

El protocolo IPX forma parte del nivel de red definido en la arquitectura de protocolos Novell; en este apartado se comentará por encima ya que la tendencia actual es hacia la desaparición del ya mencionado protocolo (las últimas versiones de Novell se orientan a trabajar sobre TCP/IP y así ofrecer una completa conectividad con redes de área extensa). En versiones anteriores se utilizaba un encapsulado de TCP/IP sobre IPX/SPX o al revés.

IPX define un servicio de envío de paquetes sin conexión y, al contrario que su homólogo IP, provee de entrega de información de procesos y no entre máquinas. En este caso, también se trata de un protocolo dependiente de la red subyacente y el formato de mensaje puede definirse de diferente manera para cada red.

Las direcciones IPX en una red Novell se asignan a los servidores NetWare, mientras que las estaciones clientes se identifican por su dirección MAC. Una dirección IPX consta de dos partes:

- Dirección externa de la red (o número de subred) que especifica el número de red y tiene un tamaño de 8 bytes (de 0 a FFFFFFFF).
- Dirección interna (o número de nodo) que especifica el servidor dentro de esa red y tiene una longitud de 12 bytes (de 0 a FFFFFFFFFFFF).

Estas direcciones pueden configurarse de forma manual, aunque también es posible dejar al sistema operativo que establezca direcciones aleatorias. Además, dentro de cada paquete IPX se incluye junto con las direcciones externa e interna otro **número de conector** que identifica las aplicaciones que se comunican (con longitud de 4 bytes, de 0 a FFFF), aunque éste se asigna internamente por la arquitectura.

3.8 DIRECCIONES FÍSICAS Y LÓGICAS

Como se explica en los apartados anteriores, los equipos de una red local están identificados por dos direcciones: una dirección MAC (también conocida como **dirección física**) y una dirección IP (también llamada **dirección lógica**). Las direcciones físicas son utilizadas por el nivel de enlace de datos para identificar los equipos y llevar a cabo un control de acceso al medio compartido, por su parte, las direcciones de red se utilizan para identificar los equipos y realizar el encaminamiento.

Otros protocolos importantes a nivel de red son **ARP** (Address Resolution Protocol o Protocolo de Resolución de Direcciones) y **RARP** (Reverse Address Resolution Protocol o Protocolo de Resolución de Direcciones Inverso). Estos protocolos se utilizan para que los equipos puedan conocer la dirección MAC de otro equipo a partir de su dirección IP o al revés. Estos protocolos son necesarios para mantener de una manera coherente los mecanismos de asignación de direcciones a nivel de enlace y nivel de red.