

---

# El nivell de red

---

PID\_00218444

Ramon Musach Pi

*Ninguna parte de esta publicación, incluido el diseño general y la cubierta, puede ser copiada, reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sea éste eléctrico, químico, mecánico, óptico, grabación, fotocopia, o cualquier otro, sin la previa autorización escrita de los titulares del copyright.*

## Índice

<b>Introducción.....</b>	<b>5</b>
<b>1. Internet protocol (IP).....</b>	<b>9</b>
1.1. IPv4 .....	9
1.1.1. Direccionamiento IP .....	12
1.1.2. NAT ( <i>network address translation</i> ) .....	17
1.1.3. Subredes: CIDR ( <i>classless inter-domain routing</i> ) .....	20
1.2. Del direccionamiento IPv4 a IPv6 .....	21
1.3. Direccionamiento IPv6 .....	21
1.3.1. Características de IPv6 .....	21
1.4. Configuración TCP/IP estática para un equipo .....	25
<b>2. ICMP (<i>internet control message protocol</i>).....</b>	<b>28</b>
2.1. Ping .....	28
2.2. Traceroute (tracert) .....	29
<b>3. ARP (<i>address resolution protocol</i>).....</b>	<b>31</b>
<b>4. Router (o enrutador).....</b>	<b>33</b>
4.1. Las tablas de enrutamiento .....	35
4.2. Routers Wi-Fi .....	36
<b>5. Configuración de un router.....</b>	<b>37</b>



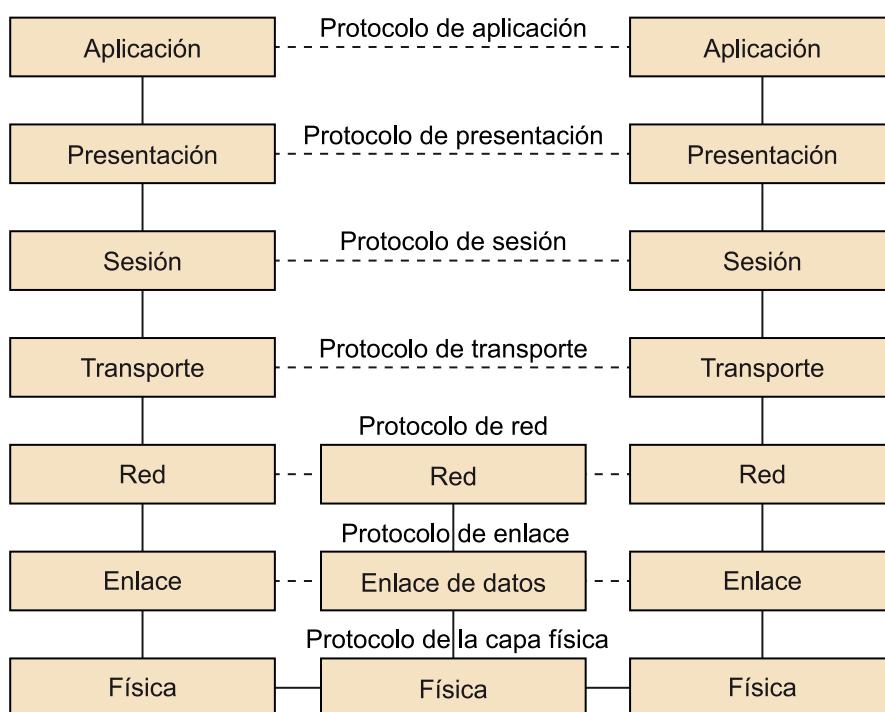
## Introducción

El nivel de red se encarga de transferir información entre sistemas finales mediante alguna red de comunicación. Proporciona conectividad y ofrece mecanismos para la selección del mejor camino entre dos nodos de la red, independientemente de que los nodos estén en redes diferentes, incluso muy separadas geográficamente.

Libera a las capas superiores, que trataremos en los dos próximos módulos, del modo de realizar la transmisión de datos y de las tecnologías de conmutación empleadas en las capas inferiores (física y de enlace).

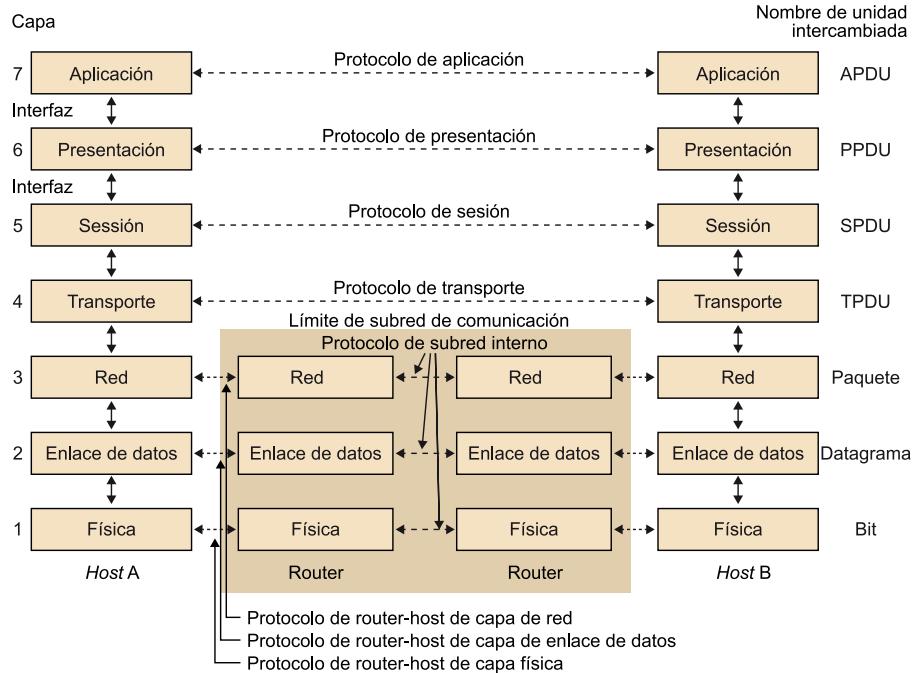
En el siguiente esquema vemos cómo las tres capas inferiores están relacionadas con la conexión y la comunicación con la red. Los paquetes transmitidos, creados por el emisor, pasan a través de uno o más nodos de la red, que actúan como retransmisores, hasta llegar al nodo destino.

Figura 1



Esquema que relaciona los diferentes protocolos del emisor, del receptor y de un nodo intermedio. Podemos apreciar que en el nodo intermedio solo se implementa hasta el nivel de red.

Figura 2



En este esquema se entra en más detalle en el proceso de comunicación que se puede establecer entre un nodo emisor y un receptor, con un nodo intermedio. Podemos apreciar que en el nodo intermedio, las capas física, de enlace y de red dan soporte a las dos tipologías de red que une y, por lo tanto, implementa los protocolos necesarios para una red y para la otra.

La capa de red no es una capa de extremo a extremo, en cambio sí que lo será la capa de transporte que trataremos en el próximo módulo. La **capa de transporte** es la primera capa de extremo a extremo entre sistemas finales (emisor y receptor). Por lo tanto, son los nodos finales los que llegan a implementar todos los niveles, a diferencia de los nodos intermedios (routers), que se quedan en el tercer nivel (i. e., capa de red).

#### Nota

En cuanto al modelo de internet, este es un modelo **TCP/IP**, donde por encima del nivel de red física está el nivel IP o nivel internet (nivel de *internet-working*).

Cuando dos equipos no están conectados a la misma red, hay que emplear nodos intermedios denominados **routers** (o enrutadores). Estos nodos son los encargados de conectar dos redes o más, con la función de que los datos de una red lleguen al destino de la otra. Para poder conocer hacia dónde se pueden dirigir los paquetes que van llegando, los routers disponen de unas tablas, llamadas **tablas de enrutamiento**. Para poder llevar a cabo estas funciones es necesario que tanto los routers como los equipos finales dispongan de un identificador único que permita localizarlos únicamente para que se les pueda enviar la información. En particular, en la red internet, estos identificadores se conocen como **direcciones IP**.

#### Nota

En internet, los routers solo implementan hasta el nivel IP (nivel de red), mientras que el TCP (nivel de transporte) solo se implementa en los extremos, es decir, en los ordenadores o equipos finales.

Las funciones de la capa de red están relacionadas con el direccionamiento, enrutamiento y la definición de las rutas. En concreto, se dispone de:

- Protocolos que describen la manera de enviar la información.
- Protocolos de enrutamiento que deciden por dónde deben pasar los paquetes hasta llegar al destino.

- Mecanismos para informar de errores que se produzcan en el envío de estos paquetes.

Dentro de este nivel IP (o nivel de red) tenemos diferentes protocolos, como el **IP** (*internet protocol*), el **ICMP** (*internet control message protocol*) y el **ARP** (*address resolution protocol*). Estos tres protocolos los trataremos en este módulo.



## 1. Internet protocol (IP)

IP (*internet protocol*) es un protocolo de la capa de red utilizado para identificar los nodos de la red. Las identificaciones de cada uno de los nodos se llevan a cabo con lo que se denomina **direcccionamiento IP**. El IP es un protocolo de red que actualmente tiene dos versiones, que analizaremos con más detalle: el **protocolo IPv4** (leído como “IP versión 4”) y su extensión **IPv6** (leído como “IP versión 6”).

El IP es un protocolo **no orientado a conexión** y, por lo tanto, no implementa mecanismos para garantizar la integridad de los datos que se envían por la red. Esto significa que no tiene mecanismos que permitan detectar pérdidas de paquetes de datos (llamados datagramas) o garantizar que se reciben en el mismo orden que han sido emitidos, dado que de esto se encarga la capa de transporte, que trataremos en el próximo módulo. Solo verifica que no haya errores en el contenido de la cabecera de cada paquete (o datagrama).

### 1.1. IPv4

Define el formato que se debe utilizar para enviar información entre dos puntos de la red. Fue propuesto en 1981 en el documento RFC-791.

#### Documento RFC

Un **documento RFC** o documento de demanda de comentarios, en inglés *request for comments*, es una compilación de propuestas sobre nuevas investigaciones y metodologías relacionadas con las tecnologías de internet. Los documentos llegan a tener vigencia cuando son aprobados por la **Internet Engineering Task Force (IETF)**.

Figura 3

Network Working Group Request for Comments: 1	Steve Crocker UCLA 7 April 1969
<b>Title: Host Software</b> <b>Author: Steve Crocker</b> <b>Installation: UCLA</b> <b>Date: 7 April 1969</b> <b>Network Working Group Request for Comment: 1</b>	

Cabecera del primer documento RFC (RFC-1) publicado el 7 de abril de 1969.

Para que la información que se quiere transmitir llegue al destino, esta no se puede enviar de cualquier manera, sino que hay que empaquetarla mediante el protocolo IP. Cada paquete que se crea se denomina datagrama, que será la unidad mínima que se transmitirá por la red. **Cada datagrama está formado por una cabecera (o encabezamiento IP) y los datos en sí que se quieren enviar.** La cabecera IP contiene una serie de campos de control, como por ejemplo toda la información de las máquinas de origen y de destino.

Figura 4



Cabecera de IPv4.

A continuación, detallamos el significado de cada uno de los campos que conforman la cabecera IPv4:

**a) Versión:** es un campo de cuatro bits que indica la versión del protocolo. En el caso de IPv4 toma el valor binario 0100 (4 en decimal), mientras que para IPv6 el valor es 0110 (6 en decimal).

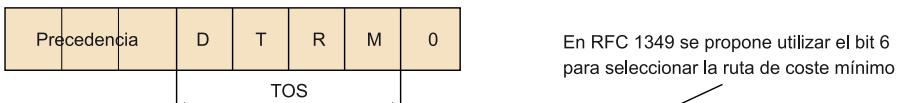
**b) IHL:** longitud de la cabecera. Considerando que la cabecera puede ser variable, dado que puede haber o no opciones, hay que explicitar su medida. Se expresa en palabras de 32 bits. Por lo tanto, el número de bytes de la cabecera tiene que ser múltiplo de 4 y dado que esta cabeza tiene solo 4 bits, la cabecera máxima que podemos llegar a construir es de 60 bytes. Y si no hay opciones, la cabecera IP ocupa como mínimo 20 bytes, y el valor de este campo es 5.

Cabecera mínima: 5 palabras x 32 bits/palabra = 160 bits x 1 byte/8 bits = 20 bytes.

Cabecera máxima: 15 palabras x 32 bits/palabra = 480 bits x 1 byte/8 bits = 60 bytes.

**c) Tipo de servicio (*type of service*):** especifica con 8 bits la calidad de servicio deseada para este paquete (o datagrama).

Figura 5



Precedencia: importancia o prioridad del paquete (8 niveles)

DTRM: tipo de transporte que se quiere (2 niveles):

D = 1 (poco retardo) T = 1 (caudal alto) R = 1 (fiabilidad alta) M = 1 (coste económico bajo)

Bits del tipo de servicio.

Ejemplos concretos de los bits del tipo de servicio los podemos encontrar en esta tabla:

	<b>D</b>	<b>T</b>	<b>R</b>	<b>M</b>
<b>TELNET</b>	1	0	0	0
<b>FTP control</b>	1	0	0	0
<b>FTP datos</b>	0	1	0	0
<b>SNMP</b>	0	0	1	0
<b>NNTP</b>	0	0	0	1

Ejemplo del uso de los bits del tipo de servicio

d) **Longitud total (length)**: es la longitud total del paquete, incluyendo los datos y el encabezamiento.

e) **Identificador del datagrama**: es el número de secuencia del datagrama. Por lo tanto, es el número único con el que se identifica cada datagrama que se genera.

En el supuesto de que la información no quema en un único datagrama, la información se divide en varios datagramas, convirtiéndose en fragmentos del hipotético datagrama original. En este caso, el identificador identifica el número de fragmento para que se pueda reconstruir la información original (i. e., el datagrama hipotético) al llegar al destino.

f) **Señalador (flags)**: en este campo de 3 bits, los dos bits de menos peso controlan la fragmentación de los paquetes. Un bit identifica si el paquete se puede fragmentar, y el otro si es el último fragmento del paquete o no.

g) **Desplazamiento de fragmento (fragmento offset)**: indica la posición que ocupa el fragmento actual en el paquete original mediante 13 bits.

h) **Tiempo de vida (también conocido como TTL, time to live)**: este campo es necesario para que no queden datagramas pululando indefinidamente por la red sin encontrar el destino. Determina el tiempo de vida del datagrama, es decir, los saltos (pasos por routers) que puede hacer un datagrama. Cada vez que atraviesa un router, el valor que hay en este campo disminuye en una unidad, y cuando llega a 0, el datagrama se descarta y se envía un paquete especial de notificación al ordenador que lo ha generado para que conozca que se ha descartado este datagrama y no ha llegado a su destino.

i) **Protocolo**: indica el tipo de paquete (denominado segmento) que transporta, por lo tanto, qué protocolo de capa superior (capa de transporte) ha generado el paquete.

j) **Suma de verificación de encabezamiento** (*header checksum*): este campo sirve para detectar errores en la cabecera (no errores en la información que se envía fuera de la cabecera, es decir, los datos en sí, dado que esta tarea corresponde a niveles superiores). Son 16 bits de control para saber si existe algún error de transmisión en el encabezamiento del paquete IP.

k) **Dirección de origen** (*source address*): especifica la dirección IP de la máquina que ha generado el paquete.

l) **Dirección de destino** (*destination address*): especifica la dirección IP de la máquina donde debe llegar el paquete.

m) **Opciones y relleno** (*options and padding*): las opciones, si hay, permiten que admita seguridad, o longitud variable. En el relleno se añaden ceros para que el encabezamiento sea múltiplo de 32 bits.

### 1.1.1. Direcccionamiento IP

Los nodos de una red se identifican de manera única mediante una dirección. En el direccionamiento IP, en concreto **IPv4**, esta dirección es un número de 32 bits que identifica cada uno de los nodos y también la red a la que están conectados.

Para simplificar la escritura de estas direcciones, los 32 bits se dividen en 4 bloques de 8 bits cada uno de ellos (octetos), empleándose a menudo notación decimal en lugar de notación binaria. Así, cada bloque será un número 0 y 255 ( $2^8 - 1$ ).

#### Nota

InterNIC fue el primer organismo encargado de las direcciones IP y números de dominio. Actualmente, es la ICANN (acrónimo de *Internet Corporation for Assigned Names and Numbers*, Corporación de Internet para la Asignación de Nombres y Números) el que tiene asignadas estas tareas.

#### Ejemplo

La notación de la dirección IP son cuatro cifras entre 0 y 255 separadas por puntos. Para poder calcular la dirección de red en binario habrá que pasar las cuatro cifras de manera independiente a notación binaria. Por ejemplo, la dirección 192.168.0.185 en binario sería:

$$192.168.0.185 = 11000000.10101000.00000000.10111001.$$

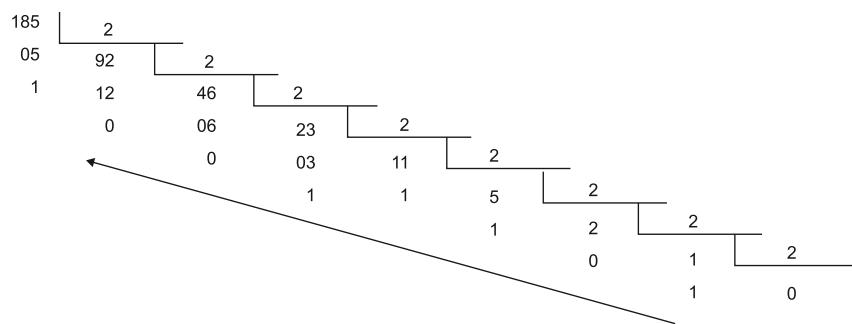
A menudo es necesario transformar números de decimal a binario y al revés. Explicamos cómo se puede llevar a cabo este proceso, facilitando alguna calculadora que realiza esta conversión.

#### a) Conversión de decimal a binario

Para realizar la conversión de decimal a binario hay que empezar a dividir el número entre 2 tantas veces como sea necesario. El valor binario del número decimal es la combinación del cociente de la última división más todos los restos de todas las divisiones en orden inverso (desde el último resto hasta el primero).

**Ejemplo:** el número 185 se puede transformar en su valor binario 010111001, mediante el proceso que se detalla en este gráfico:

Figura 6

**b) Conversión de binario a decimal**

Solo hay que ir multiplicando cada valor binario por la potencia de 2 que corresponda dada su posición.

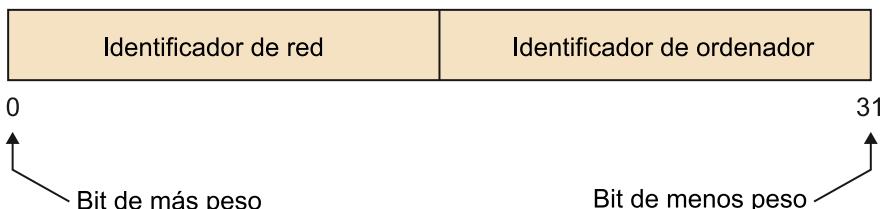
**Ejemplo:** Comprobamos a qué valor decimal corresponde el número binario 010111001

$$1 \cdot 2^0 + 0 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 + 1 \cdot 2^5 + 0 \cdot 2^6 + 1 \cdot 2^7 + 0 \cdot 2^8 = 185.$$

Como se puede ver, este formato permite generar un gran volumen de direcciones. La gestión de este gran volumen de direcciones puede ser complicada; por lo tanto, se propuso que la asignación de direcciones fuera jerárquica. ¿Podemos pensar por un momento cómo se llegaría a gestionar el direccionamiento si se adjudicaran las direcciones de manera secuencial una vez conectados a la red? Pensemos simplemente en cuántos ordenadores hay en el mundo conectados simultáneamente. Solo con este hecho ya tenemos la respuesta. ¡Sería imposible!

Podemos afirmar que una de las claves de la expansión de internet es por el sistema de direccionamiento jerárquico que incorpora el protocolo IP que utiliza. Así, en internet las **direcciones IP están compuestas por dos partes**. Una parte de la dirección IP sirve para identificar la red y la parte restante de esta dirección IP es la que identifica el equipo u ordenador. Así pues, las direcciones se pueden clasificar y organizar según la red a la que pertenezcan.

Figura 7



Los 32 bits (del 0 al 31) se reparten entre el identificador de red y el identificador del ordenador.

Los bits superiores de la dirección IP son la parte de red que nos indica la red a la que pertenece un conjunto de equipos; en definitiva, el router al que están conectados estos equipos. En cambio, los bits inferiores de la dirección IP identifican individualmente cada equipo dentro de la red.

Inicialmente las redes se dividieron en 5 clases: A, B, C, D y E.

**1) Redes de clase A.** En sus direcciones, el primer bloque de 8 bit (octeto) es el que identifica la red, donde el bit superior siempre es un 0, y los otros 3 bloques de 8 bits (24 bits) son los que identifican los equipos de cada una de estas redes. Dado que el primer bit siempre es un 0, los 7 bits restantes del primer bloque identifican la red, y el resto de los bits –es decir, 24– identifican sus equipos.

Figura 8

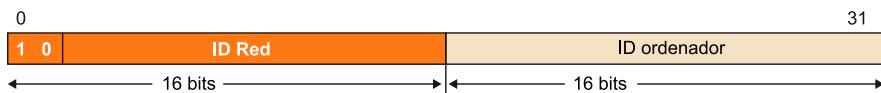


Estas direcciones están destinadas a empresas muy grandes, y el hecho de reservar tantas direcciones para este tipo de redes ha dado lugar a la falta actual de direcciones.

**2) Redes de clase B.** En una dirección de clase B los dos primeros octetos codifican las redes, y del número total de octetos los dos bits que pesan más siempre valen 10. Los 14 bits siguientes de estos dos primeros octetos se utilizan para identificar las redes.

Los dos últimos octetos (por lo tanto, 16 bits) son los que identifican los equipos conectados.

Figura 9



Observemos que habrá más redes de clase B que de clase A, pero cada red de clase B acepta menos equipos que una de clase A.

**3) Redes de clase C.** En sus direcciones se utilizan los tres primeros octetos para identificar las redes y se dedica el último a la identificación de cada equipo. Los tres bits que pesan más del identificador de red siempre tendrán por valor 110. Y en este caso se dispone de  $2^8$  (256) direcciones para identificar equipos en cada una de estas redes.

Figura 10

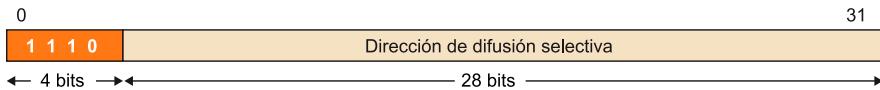


**4) Redes de clase D.** Se considera un tipo de red especial, denominadas redes de clases de multidestino (en inglés, *multicast*). Se crearon para permitir difusión selectiva o *multicast* en una dirección IP. Una dirección de difusión selectiva es una dirección exclusiva de red que permite identificar el grupo de

computadoras al que el mensaje del *multicast* está dirigido. Por lo tanto, una única estación puede transmitir simultáneamente una sola corriente de datos a múltiples receptores. Así, este tráfico es denominado punto multipunto.

En sus direcciones, los cuatro bits de más peso siempre valen 1110, y utiliza los otros 28 bits como dirección de difusión selectiva.

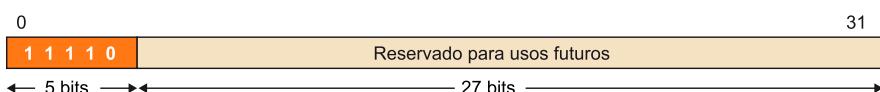
Figura 11



**5) Redes de clase E.** Sus direcciones se han reservado para usos futuros. Normalmente, la IETF (*Internet Engineering Task Force* o Comité de Expertos en Ingeniería de Internet) las usa para investigar y, por lo tanto, no se ha dado ninguna dirección de clase E para poderla utilizar en internet.

Se identifican del mismo modo que las otras, mediante los bits de más peso. En este caso, los cinco primeros bits tienen un valor fijo: 11110.

Figura 12



### Direcciones de propósito específico

A parte de la anterior clasificación de las direcciones también se han reservado toda una serie de direcciones para propósitos específicos:

**a) Direcciones de anfitrón.** Indican un equipo concreto de la red en la que nos encontramos. De este modo, la parte de la dirección de red será todo 0, y se mantendrá la parte de la dirección de equipo que corresponda.

**b) Direcciones de red.** Hacen referencia a la red pero no a los equipos de dentro de esta. Al contrario que la anterior, la parte de la dirección de red se mantiene y la parte de la dirección que corresponde al equipo será todo 0.

La dirección 0.0.0.0 es un caso especial, que a menudo no se implementa en los sistemas operativos actuales, y correspondería a “este anfitrón” de “esta red”.

**c) Direcciones de difusión (*broadcast*).** Se trata de una dirección especial que sirve para comunicarse a la vez con todos los equipos de una determinada red. Los primeros octetos de la dirección se mantienen e identifican la red (en función del tipo que sea habrá más o menos octetos), y cada uno de los octetos restantes que corresponden a los equipos toma el valor 255. Es decir, se mantiene la parte de la dirección de red y el resto de los octetos será 255.

Siempre que se mande un mensaje a la dirección de difusión, todos los equipos deben responder.

Observemos que si se enviara un datagrama a la dirección 255.255.255.255, se estaría enviando a todos los equipos de la red internet. Para evitarlo, los routers solo pueden reenviar tráfico de difusión (también denominado “mensajes de *broadcast*”) dentro de la red que lo ha emitido.

Red	Dirección IP	Clase	Dirección de red	Número máximo de ordenadores que puede tener esta red	Dirección del host	Dirección de broadcast
1	74.13.24.67	A	74.0.0.0	$2^{24}$	0.12.24.67	74.255.255.255
2	88.126.102.103	A	88.0.0.0	$2^{24}$	0.126.102.103	88.255.255.255
3	195.180.160.140	C	195.180.160.0	256	0.0.0.140	195.180.160.255
3	195.180.160.142	C	195.180.160.0	256	0.0.0.142	195.180.160.255
4	222.125.222.21	C	222.125.222.0	256	0.0.0.21	222.125.222.255
5	156.11.75.15	B	156.11.0.0	$2^{16}$	0.0.75.15	156.11.255.255

En esta tabla observamos algunas direcciones IP, habiendo numerado las redes a las que pertenecen (de modo que si dos direcciones IP son de ordenadores de la misma red, tienen el mismo número asignado), la clase de cada una de estas redes (A, B, C, etc.), la correspondiente dirección de red y el detalle de cuántos ordenadores puede tener como máximo cada red (dependerá del tipo de red). Y para cada dirección IP de la tabla, la dirección del host y la dirección de broadcast de la red.

d) **Direcciones de *loopback*.** Son direcciones utilizadas internamente por los equipos. Van desde la 127.0.0.0 hasta la 127.0.0.255. A menudo al iniciar el equipo, el sistema operativo crea una interfaz virtual, denominada *loopback*, con la dirección 127.0.0.1, que permite enviar datagramas desde el equipo en el que estamos a sí mismo. Esto sirve, por ejemplo, por si queremos tener un servidor instalado en nuestro ordenador y conectarnos, desde el mismo ordenador, al servidor. El servidor estará en la dirección 127.0.0.1, también conocida como *localhost*.

e) **Direcciones privadas.** Son utilizadas por las redes locales internas que no salen a internet. A cada estación de trabajo se le puede asignar una dirección dentro del rango de las direcciones privadas. Se utilizan habitualmente en redes de área local (LAN), donde no existe la necesidad de disponer de una dirección IP global para cada estación de trabajo, o en otros dispositivos, como impresoras conectadas a la red.

Su uso generalizado también vino provocado por la escasez de direcciones IP en este protocolo IPv4.

Los routers se configuran de manera que descartan cualquier tipo de tráfico dirigido a direcciones privadas. Este aislamiento facilita generalmente que desde fuera de la red privada no sea posible conectar con una máquina mediante estas direcciones. Por lo tanto, dado que no es posible realizar conexiones externas entre diferentes redes privadas a través de internet, dos redes privadas

de diferentes entornos (por ejemplo, empresas) pueden emplear los mismos rangos de direcciones sin que se genere ningún conflicto. Dado que dos redes privadas de diferentes entornos no se pueden comunicar entre sí utilizando direcciones privadas, no se producirán colisiones entre las diferentes redes privadas.

En el caso de querer establecer comunicaciones con el exterior, fuera de la red privada, el router de la red dispone de lo que se denomina una puerta de enlace con una dirección IP pública. Desde fuera de la red se puede llegar también a esta dirección IP pública del router, y será este dispositivo el que se encargará de enviar los paquetes recibidos al equipo que corresponda de la red privada.

Si queremos utilizar una dirección privada, habrá que usar un rango concreto. En esta tabla presentamos los rangos que definen direcciones privadas:

Clase	Rango red	Descripción	Definido en
A	10.0.0.0 - 10.255.255.255	1 red simple de clase A	RFC 1918 RFC 1597 (esta es la especificación original pero actualmente está obsoleta)
B	172.16.0.0 - 172.31.255.255	16 redes de clase B	
C	192.168.0.0 - 192.168.255.255	256 redes de clase C	
B	169.254.0.0 - 169.254.255.255	1 red simple de clase B	RFC 3300 y RFC 3927

Tal como hemos comentado, el problema de las direcciones privadas es que no pueden acceder directamente a internet. Los routers nunca enviará a internet el tráfico originado en equipos con direcciones privadas, o con destino a estas, ya que no sabrían cómo enrutarlo. Para evitar esta limitación, los routers incluyen una técnica llamada **NAT**, *network address translation*.

### 1.1.2. NAT (**network address translation**)

Tengamos en cuenta que cada equipo de una red IPv4 debe disponer de una dirección pública para poder acceder a la red internet. Pero a menudo las redes tienen más equipos que IP asignadas por las operadoras. Por ejemplo, un usuario que tiene contratada una conexión ADSL con una operadora solo recibe una IP pública, mientras que este mismo usuario dispone de múltiples dispositivos (ordenadores, *smartphones*, tabletas, etc.) que han de poderse conectar a internet empleando la misma conexión. Por lo tanto, este usuario solo tiene dos opciones, pedir más direcciones IP a su operadora o utilizar direcciones IP privadas, de manera que sea el router el que realice la conversión desde la dirección IP privada a la IP pública. Esta segunda opción es un proceso que se

conoce como NAT. La mayoría de los sistemas que utilizan NAT lo hacen para permitir que múltiples ordenadores de una red privada accedan a internet con una única dirección IP pública.

Desde mediados de los años noventa, la NAT ha sido una herramienta muy popular para reducir los problemas provocados por la reducción del espacio de direcciones IPv4. Además, se ha convertido en una función estándar e indispensable en todos los routers para conexiones domésticas y en pequeñas oficinas.

NAT es el proceso por el que se modifica la información sobre las direcciones en la cabecera del paquete IPv4, mientras este paquete está en tránsito por un router.

NAT está definida con detalle en los documentos llamados RFC-2663 y RFC-3022.

Dependiendo del tratamiento que se realiza de las direcciones, existen diferentes formas de NAT: 1) NAT estática, 2) NAT dinámica, 3) NAT con sobrecarga del TCP (también conocida como PAT, *port address translation*) y 4) LSNAT (*load sharing NAT*, o NAT con balanceo de carga). A continuación explicamos brevemente cada una de ellas:

**1) NAT estática.** Es el caso más sencillo, también conocida con el nombre de NAT básica o NAT de uno a uno. En este caso, cada dirección privada tiene su dirección pública equivalente. Será el administrador de la red quien deberá construir esta tabla de equivalencias dentro del router (en la parte de configuración de NAT), con las dificultades de gestión que puede implicar si se da un número elevado de traducciones que realizar. Fijémonos también en que este tipo de NAT tampoco supone ningún ahorro de direcciones públicas, pero sí que puede interesar asignar una dirección pública concreta a algunos servidores que continuamente puedan estar publicando en internet.

**2) NAT dinámica.** Con este modo, el router asigna de manera dinámica una dirección privada a una dirección pública. Al contrario que la NAT estática, el objetivo de la NAT dinámica es tener menos direcciones públicas que privadas. Para que esto sea viable, hay que asumir que todas las máquinas de la red privada no estarán conectadas al mismo tiempo a internet. **En este caso el administrador de la red deberá fijar los rangos de direcciones privadas y públicas utilizadas.**

**3) PAT (*port address translation*).** Es un tipo de NAT dinámica que permite reducir al máximo (hasta una) el número de direcciones IP públicas utilizadas dinámicamente. Para ello emplea el puerto TCP/UDP con el objetivo de identificar el equipo origen de la comunicación dentro de la red interna/privada.

Por lo tanto, es muy similar a la NAT dinámica pero añadiendo el rango de los puertos que se deben emplear. Este rango estará dentro del rango de puertos asignados por IANA para las aplicaciones clientes (del 1024 al 5000).

#### Ejemplo

Tipo de NAT	Dirección privada	Dirección pública
Estática	172.26.0.35	201.5.4.3
Estática	172.26.0.43	201.5.4.15
Dinámica	Rango: 172.26.0.50 a 172.26.0.80	Rango: 201.5.4.100 a 201.5.4.110
PAT	Rangos 172.26.1.101 a 172.26.1.254 172.26.2.101 a 172.26.2.254	201.5.4.18 Puertos del 1024 al 5000

En esta tabla podemos comprobar las equivalencias entre direcciones privadas y públicas, apreciándose las diferencias mencionadas entre los diferentes tipos de NAT.

4) LSNAT (*load sharing NAT*). Es un tipo de NAT concebido para solucionar el problema de servidores de aplicaciones sobresaturados, como portales o buscadores. Por ejemplo, es el que se aplica en portales como el de la UOC.

Si hay más solicitudes de las que el servidor puede atender, podemos o bien cambiar el servidor por uno más potente (con el riesgo asociado de que si falla, dejamos de dar estos servicios), o bien replicar el servidor existente con otras máquinas con las mismas prestaciones que el inicial. En este segundo caso, que es el que hace referencia a LSNAT, lo que se hará es aplicar un sistema que publique todos los servidores en internet, como si fuera un único servidor; y balancearemos la carga, la repartiremos, entre todos, de modo que si uno falla, se puedan redirigir las peticiones al resto de los servidores, sin que el usuario se percate de ello. Será un router o conmutador de altas prestaciones el que se encargue del redireccionamiento, y por lo tanto de balancear la carga de peticiones de los servidores.

En este caso tendremos  $n$  servidores con diferentes direcciones privadas, que están identificados por una misma dirección pública (la que se denomina *virtual IP address*). A menudo, el redireccionamiento hacia uno de los servidores (i. e., pasar de la *virtual IP address* a la IP privada de uno de los servidores), en lugar de llevarse a cabo en el router se realiza en un conmutador de altas prestaciones, dado que es necesaria una gran capacidad de carga y procesamiento.

#### Ejemplo

Un usuario que quiera acceder a un servicio web utilizará la dirección virtual, pero internamente esta dirección pública estará asociada a un número determinado de servidores, cada uno de ellos con la correspondiente dirección privada.

### 1.1.3. Subredes: CIDR (*classless inter-domain routing*)

Una vez definidas todas las clases de redes, se vio que el modelo tenía algunas carencias. Por ejemplo, en las redes de clase A y B, el número de direcciones es excesivamente elevado como para ser gestionadas por un único equipo. Para solucionarlo se propuso un mecanismo llamado **CIDR**, *classless inter-domain routing* (enrutamiento entre dominios sin clase), que detallaremos a continuación. EL CIDR es conocido normalmente con el sobrenombre de “subredes”.

CIDR permite dividir las direcciones asignadas a una red en subredes más pequeñas y manejables. Con CIDR la separación entre el equipo y la red se realiza con una máscara.

Por ejemplo, 147.44.2.11/24 nos indica que tiene 24 bits con valor ‘1’ que indican la dirección de red y 8 para la de los equipos. Por lo tanto, nos dice que la máquina 147.44.2.11 pertenece a la red 147.44.2.0. La máscara que permite obtener la dirección de red es 255.255.255.0 o, lo que es lo mismo, 24 bits con valor ‘1’. También nos está diciendo que solo habrá 255 máquinas (desde 0 hasta 254, siendo la 255 la dirección de *broadcast*).

Otro ejemplo podría ser la dirección de clase B de un equipo: 172.24.100.45 y una máscara igual a 27, es decir: 172.24.100.45/27. Dado que es una clase B y la máscara tiene 27 bits a ‘1’, nos encontramos con once bits de subred. Por lo tanto, la dirección de subred a la que pertenece el dispositivo es 172.24.100.32/27. En este habría 32 direcciones diferentes, donde la dirección 31 sería la de *broadcast* (todos los bits de dirección con valor ‘1’).

Detallémoslo gráficamente con esta tabla, en la que podemos apreciar como resultado final de la operación binaria AND realizada la subred a la que pertenece el dispositivo:

	<b>Dirección (en decimal)</b>	<b>En binario</b>
<b>Dirección del dispositivo</b>	172.24.100.45	10101100. 00011000. 01100100. 00101101
<b>Máscara (con 27 bits a “1”).</b>	255.255.255.0	11111111. 11111111. 11111111. 11100000
<b>Dirección de subred resultante.</b> Resulta de multiplicar (AND) la dirección y la máscara bit a bit.	172.24.100.32	10101100. 00011000. 01100100. 00100000

A menudo, al trabajar con redes esta división en subredes se realiza teniendo en cuenta determinados criterios, por ejemplo, para separar una red educativa de una red de gestión.

Con la creación de subredes se consigue:

- Aislar el tráfico de cada red y, por lo tanto, mejorar la seguridad y el rendimiento global de cada una de ellas.
- Simplificar la resolución de problemas, dado que al tenerlas segmentadas es más sencillo identificar su origen.

Así, con esta clasificación en subredes se simplifica el trabajo de los routers, dado que para decidir la ruta que debe tomar el datagrama no necesitan comprobar toda la dirección IP, sino solo la red de destino.

## 1.2. Del direccionamiento IPv4 a IPv6

Cuando se diseñó el protocolo de direccionamiento IPv4 se consideraba que habría bastantes direcciones para dar respuesta a un volumen elevado de equipos que quisieran conectarse a una red como internet. Pero con el tiempo y el incremento exponencial de necesidad de conexión de equipos a la red internet (sobre todo el elevado incremento de asignaciones en zonas de Asia), propiciado también por el incremento de dispositivos móviles con necesidades de conexión, ha provocado que las direcciones IPv4 se vayan agotando.

Para minimizar este problema se diseñó NAT, que tal y como hemos comentado permite utilizar direcciones privadas para acceder a la red con una única IP pública. Pero dado que esta solución no es escalable, lo que supone muchas dificultades de aplicación a los proveedores, se decidió incrementar los 32 bits de las direcciones IPv4 a 128, lo que dio lugar al direccionamiento IPv6.

## 1.3. Direccionamiento IPv6

La falta de direcciones IPv4 incentiva el diseño de este nuevo protocolo llamado IPv6. Inicialmente se planteó hacer solo una adaptación del protocolo IPv4, pero desde un primer momento ya se vio que el volumen de cambios aconsejaba la creación de un nuevo protocolo. Además, la solución NAT por sí misma también podía llegar a representar un grave problema de rendimiento en los routers, por el hecho de tener que mantener tablas de traducción de direcciones de millones de conexiones a la vez.

El direccionamiento IPv6, debido a que la longitud de la dirección IP pasa de 32 a 128 bits, provoca que el rango de direcciones de la red pase de  $2^{32}$  a  $2^{128}$  direcciones posibles.

### 1.3.1. Características de IPv6

A continuación, pasamos a describir las características del protocolo IPv6.

En cuanto a la cabecera de las direcciones IPv6, esta tiene una longitud fija de 40 bytes y consta de los campos que a continuación describiremos.

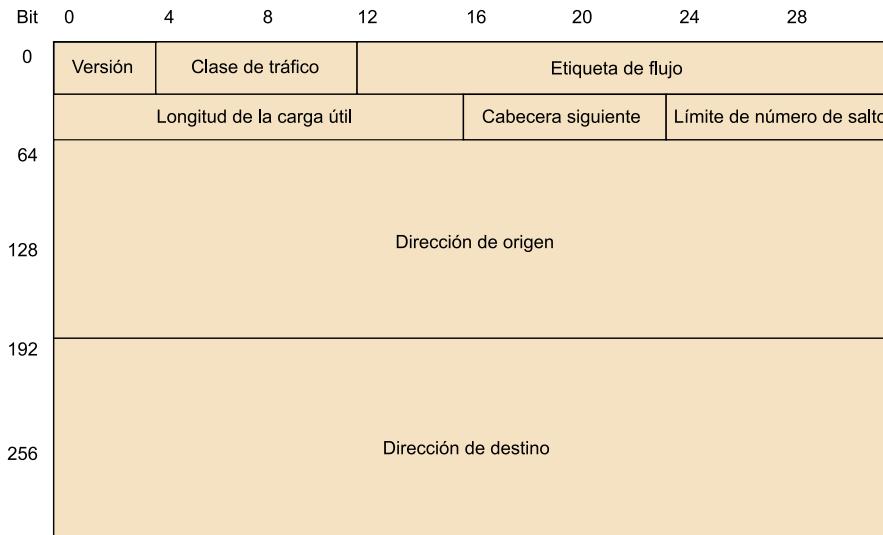
### Creación de subredes

Cabe señalar que existen algunas aplicaciones en línea que permiten automatizar los cálculos para la creación de subredes. Solo hay que hacer una búsqueda en internet con los términos: *network calculator* o *subnet calculator*. En concreto, encontraremos: <http://www.subnet-calculator.com/>

### Nota

La diferencia más relevante entre IPv4 e IPv6 es la longitud de las direcciones IP, pasando de 32 a 128 bits.

Figura 13



Cabecera IPv6. En cada línea del esquema tenemos 32 bits, que por las 10 líneas obtenemos los 320 bits (40 bytes) que tiene la cabecera.

- **Versión (version)**. De 4 bits. Contiene la versión del protocolo que contiene el paquete. En el caso de IPv6 el valor es 0110 (6 en decimal).
- **Clase de tráfico (traffic class)**. De 8 bits. Es equivalente al campo tipo de servicio de IPv4. Clasifica el paquete dentro de un tráfico determinado.
- **Etiqueta de flujo (flow label)**. De 20 bits. Para etiquetar un conjunto de paquetes con las mismas características.
- **Longitud de la carga útil (payload length)**. De 16 bits. Longitud del paquete en bytes sin contar la cabecera IP.
- **Cabecera próxima (next header)**. De 8 bits. Indica la posición en la que se puede encontrar la cabecera siguiente. Es una novedad en IPv6 y facilita a los routers el tiempo de proceso, al no haber opciones.
- **Número de saltos (hop limit)**. De 8 bits. Equivalente al campo TTL de IPv4, pero en este caso en lugar de contar tiempo cuenta número de saltos.
- **Dirección de origen (source address)**. De 128 bits, especifica la dirección IP de la máquina que ha generado el paquete.
- **Dirección de destino (destination address)**. De 128 bits, especifica la dirección IP de la máquina a la que debe llegar el paquete.

En este esquema podemos ver la comparativa entre las dos cabeceras, la de IPv4 y la de IPv6, con el detalle de las diferencias:

Figura 14

La figura muestra una comparación entre las cabeceras IPv4 y IPv6. La cabecera IPv4 (izquierda) tiene los siguientes campos: Versión (4), IHL, Tipo de servicio, Longitud total, Identificación, Banderas, Desplazamiento del fragmento, Tiempo de vida, Protocolo, Suma de verificación de la cabecera, Dirección origen, Dirección destino, y Opciones. La cabecera IPv6 (derecha) tiene los siguientes campos: Versión (6), Clase de tráfico, Etiqueta de flujo, Longitud de carga útil, Cabecera siguiente, Límite de saltos, Dirección origen, Dirección destino, y Opciones. Una leyenda indica que los cuadros naranjas representan campos que mantienen el número en IPv6, los beige representan campos eliminados en IPv6, los marrones representan campos que cambian de nombre y posición en IPv6, y el verde oscuro representa campos nuevos en IPv6.

Cabecera IPv4				Cabecera IPv6			
Versión 4	IHL	Tipo de servicio	Longitud total	Versión 6	Clase de tráfico	Etiqueta de flujo	
Identificación		Banderas	Desplazamiento del fragmento	Longitud de carga útil		Cabecera siguiente	Límite de saltos
Tiempo de vida	Protocolo	Suma de verificación de la cabecera					
Dirección origen				Dirección origen			
Dirección destino				Dirección destino			
Opciones				Opciones			

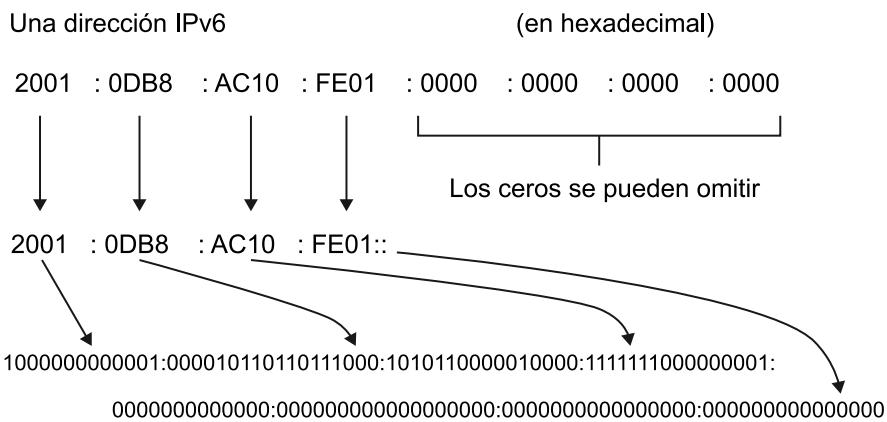
Legend:

- Campos que mantienen el número en IPv6
- Campos eliminados en IPv6
- Campos que cambian de nombre y posición en IPv6
- Campos nuevos en IPv6

Comparativa cabecera IPv4 e IPv6.

Al tener las direcciones muchos más bits, también cambia el modo de especificarlas. En IPv6, las direcciones se indican en hexadecimal y se utiliza como notación los dos puntos, en vez del punto. Con esta notación, cuando ponemos “::” estamos indicando que en este punto de la dirección se debe completar con ceros.

Figura 15



Ejemplo de dirección IPv6 en hexadecimal y en binario. Observemos que en la parte final de la dirección se está empleando el modo abreviado (“::”) para indicar los ceros consecutivos.

### Conversión de hexadecimal a binario, y a la inversa

Como podemos comprobar, en muchos casos las direcciones en IPv6 se expresan en notación hexadecimal.

El **sistema hexadecimal** (abreviado hex) es un sistema numérico con base 16. Se representa normalmente empleando los símbolos 0-9 y A-F o a-f. Este sistema numérico fue introducido por primera vez en informática en 1963 por IBM.

Para convertir un número hexadecimal a binario, cada uno de los dígitos hexadecimales debe convertirse por separado a binario, como si se tratara de un número decimal (véase la conversión decimal a binario). Cada cifra siempre deberá tener 4 dígitos binarios; por lo tanto, si el resultado tiene menos de 4 dígitos, se completará con ceros a la izquierda hasta llegar a 4.

Observemos que cada cifra hexadecimal representada por una letra (A, B, C, D, E o F) en los cálculos se sustituirá por su valor decimal (10, 11, 12, 13, 14 o 15, respectivamente).

Así, por ejemplo, B en hexadecimal corresponde a 11 en decimal, que convertido a binario con el procedimiento indicado es 1011.

Para convertir de binario a hexadecimal, se divide el número binario en grupos de 4 cifras, empezando por la derecha. Si el último bloque de 4 no está completo, se completa

con ceros a la izquierda. Cada bloque se pasa a decimal (ver proceso de conversión de binario a decimal), lo que da números entre 0 y 15. Los valores que se encuentren entre 10 y 15 son sustituidos por las letras correspondientes, el resto se toman directamente. La secuencia obtenida corresponde al número hexadecimal correspondiente.

Para hacer la **conversión de un número decimal a hexadecimal**, de manera manual, se opera igual que en la conversión decimal a binario, con la diferencia de que ahora se divide entre 16 en lugar de entre 2. Se van realizando divisiones sucesivas con los cocientes obtenidos hasta que el cociente sea inferior a 16. Los restos de las diferentes divisiones estarán entre 0 y 15, en lugar de entre 0 y 1. El número hexadecimal se obtendrá tomando el último cociente y todos los restos en orden inverso a como se han obtenido (primero el último resto, después el penúltimo y así hasta obtener el resto de la primera división). Para cada uno de ellos, si el valor está entre 0 y 9 se toma este valor directamente, y si está entre 10 y 15, se pone el número en el hexadecimal correspondiente siguiendo esta correspondencia: 10=A; 11=B; 12=C; 13=D; 14=E; 15=F.

### Direcciones de aplicaciones en línea

Existen aplicaciones en línea que permiten realizar rápidamente estas conversiones, como la que podemos encontrar en:

<http://www.mathsisfun.com/binary-decimal-hexadecimal-converter.html>

<http://calc.50x.eu/>

<http://es.ncalculators.com/digital-computation/binary-hex-converter.htm>

### Ejemplo 1

En este ejemplo se convierte el número hexadecimal 61B9430E a binario, empleando el procedimiento indicado, haciendo las conversiones dígito a dígito.

65B9432E = 0110 0101 1011 1001 0100 0011 0010 1110.

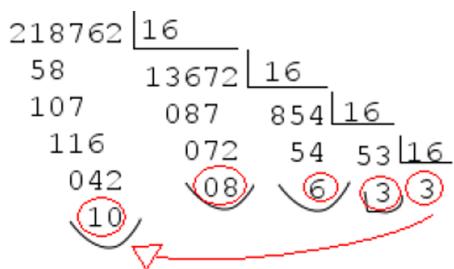
### Ejemplo 2

Dado el número binario 101 1010 0100 1101 1011 0101 1110 1010, con el procedimiento indicado obtendremos el número hexadecimal 5A4DB5EA.

### Ejemplo 3

Dado el número decimal 218762, encontramos el correspondiente valor hexadecimal:

Figura 16



Aplicando el procedimiento indicado, encontramos que será 3368A.

En el caso de querer hacer la **conversión de hexadecimal a decimal**, solo habrá que ir multiplicando cada dígito de derecha a izquierda por una potencia de 16, empezando por 16<sup>0</sup> y siguiendo por 16<sup>1</sup>, 16<sup>2</sup>, etc. Recordemos que las letras se consideran valores numéricos siguiendo la correspondencia indicada (A=10, B=11, etc.).

### Ejemplo 4

Convertimos el número 4A89D1 a número decimal:

$$4A89D1 = 1 \cdot 160 + 13 \cdot 161 + 9 \cdot 162 + 8 \cdot 163 + 10 \cdot 164 + 4 \cdot 165 = 4884945$$

### Ejemplo 5

El número decimal 93, cuya representación en sistema binario es 01011101, se puede escribir como 5D en hexadecimal (5 = 0101, D = 1101).

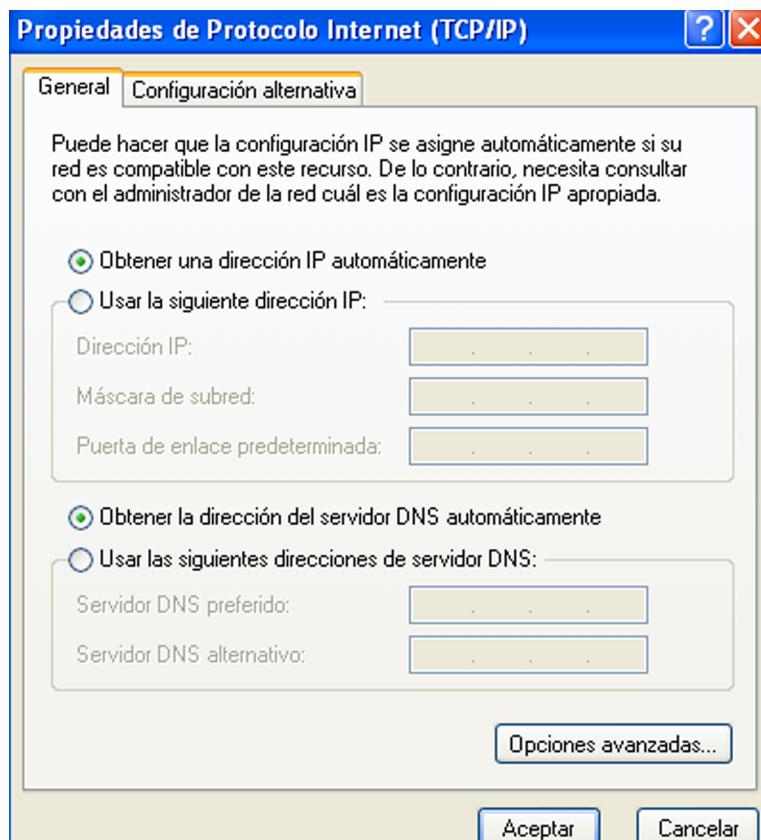
IPv6 representa, tal y como hemos comentado, una gran evolución de IPv4. A pesar de que mantiene las principales funciones, presenta nuevas características, las más relevantes de las cuales son estas:

- El aumento ya señalado del tamaño de la dirección IP, que pasa de 32 a 128 bits.
- Un formato de cabecera más simplificado, para mejorar su tratamiento en los routers.
- La posibilidad de extensión de las cabeceras y de las opciones. Estas opciones se ponen en cabeceras supplementarias IPv6 contenidas entre la cabecera IPv6 y la cabecera del paquete de transporte. Así, las opciones de estas cabeceras IPv6, que aquí pueden ser de longitud variable, no son tratadas por los routers intermedios.
- La definición de extensiones que permiten la autenticación de usuarios y la integridad de los datos mediante herramientas criptográficas.
- El hecho de contener modos de autoconfiguración, como la configuración *plug and play* de direcciones de nodos sobre una red aislada, empleando DHCP.
- La posibilidad de una transición sencilla de IPv4 a IPv6.

## 1.4. Configuración TCP/IP estática para un equipo

En el caso de que se deba asignar una dirección IP fija a un ordenador o a cualquier otro dispositivo, hay que ir a las opciones de **conexiones de red** del sistema operativo correspondiente. Yendo a sus propiedades, encontraremos **protocol internet** (TCP/IP) o **protocol internet version 4** (TCP/IPv4), de manera que accediendo a sus propiedades llegaremos a una pantalla como la que mostramos:

Figura 17

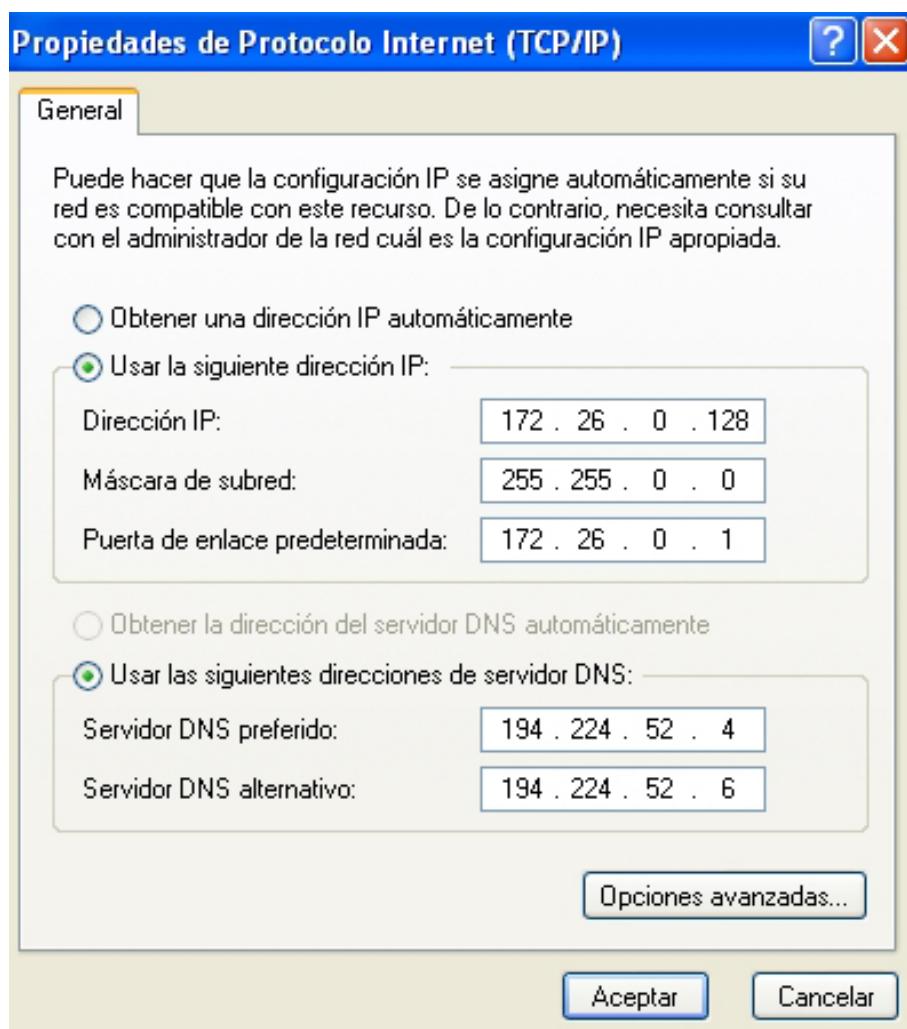


Pantalla de configuración del protocolo TCP/IP configurado con las opciones de asignación automática de IP y DNS (direcciónamiento dinámico).

En la imagen anterior aparece el concepto DNS. A pesar de que lo detallaremos cuando tratemos el nivel de aplicación, lo presentamos ya. Este **sistema de nombres de dominio**, en inglés *domain name system* (DNS), permite traducir direcciones IP con nombres que se pueden recordar de manera más sencilla. Un servicio DNS recibe las peticiones que le llegan y realiza rápidamente esta traducción. Por ejemplo, cuando escribimos una dirección web en el navegador, este realiza la consulta al servidor DNS para conocer la dirección IP que le corresponde.

A menudo los usuarios utilizan como servidor DNS el que proporciona su proveedor de servicios de internet. La dirección de estos servidores puede llegar a ser configurada de modo manual o automático mediante **DHCP** (*dynamic host configuration protocol*); en otros casos, los administradores de red pueden tener configurados sus propios servidores DNS.

Figura 18



Pantalla de configuración del protocolo TCP/IP con IP y DNS fijas (direcciónamiento estático).

Las opciones son las que aparecen: opción de que la dirección IP se asigne automáticamente o que quede determinada de manera fija (en este caso la tendremos que introducir, con la correspondiente máscara y dirección del router o puerta de enlace predeterminada); y lo mismo con los llamados campos DNS, dependiendo de si el servidor DHCP le indicará estos valores o se utilizarán una o dos direcciones IP fijas de servidores DNS. Aceptando estas opciones ya se tendrá configurado el protocolo.

Hay que destacar que la IP asignada debe estar dentro del rango de las direcciones de la red en la que se encuentra el router. Así, si el router tiene una IP 192.168.0.1, uno de los equipos podría tener, por ejemplo, una IP fija 192.168.0.45.

El hecho de que la IP se pueda asignar directamente, o que debamos fijarla, dependerá de cómo tengamos configurado el router (con DHCP activado o no).

En el caso de querer configurar TCP/IPv6, el proceso será parecido.

## 2. ICMP (*internet control message protocol*)

El ICMP corresponde a un mecanismo básico que se utiliza para gestionar las incidencias que se pueden llegar a producir en una red IP, independientemente de la tecnología utilizada en niveles inferiores. Por lo tanto, complementa el protocolo IP para tareas de control y notificación de errores.

Los mensajes ICMP son los que se incorporan dentro de los paquetes IP, poniendo el valor del campo protocolo de la cabecera IP a 1. Este valor 1 en este campo nos indica que el campo de datos contiene el mensaje ICMP.

Existen trece tipos de mensajes ICMP y una treintena de subtipos. Podemos encontrar la descripción detallada de este protocolo con **todos los tipos de mensaje ICMP** en el documento **RFC-792**: <http://www.rfc-es.org/rfc/rfc0792-es.txt>.

A pesar de que este protocolo está concebido para esta capa de red, existen algunas aplicaciones que lo usan directamente, como herramientas de diagnóstico de red. Entre ellas se encuentran **ping** y **traceroute**.

### 2.1. Ping

Permite ver si un equipo se encuentra conectado a la red utilizando el protocolo ICMP. Con la orden *ping* se comprueba la conectividad entre un *host* y un *host* remoto.

La mayoría de los sistemas operativos incorporan esta orden *ping*. Cuando se ejecuta la solicitud ***ping[dirección IP o nombre de un host remoto]***, se envían mensajes ICMP de tipo 8. Si el mensaje llega al destino, el *host* remoto responde con un mensaje ICMP de tipo 0, informando que está activo y el tiempo que se ha tardado en recibir la respuesta. Si el *host* remoto no está activo, o no existe, transcurrido un tiempo sin recibir nada se recibe por pantalla un mensaje de error, indicando que no se ha encontrado.

Este comando también permite comprobar si la tarjeta de red de nuestro propio ordenador está operativa y tiene configurado TCP/IP. Solo hay que hacer *ping 127.0.0.1* o, equivalentemente, *ping localhost*.

Figura 19

```
C:\Documents and Settings\Tutor>ping 192.168.0.1
Haciendo ping a 192.168.0.1 con 32 bytes de datos:

Respueta desde 192.168.0.1: bytes=32 tiempo=1ms TTL=64
Respueta desde 192.168.0.1: bytes=32 tiempo<1ms TTL=64
Respueta desde 192.168.0.1: bytes=32 tiempo<1ms TTL=64
Respueta desde 192.168.0.1: bytes=32 tiempo<1ms TTL=64

Estadísticas de ping para 192.168.0.1:
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
  Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

Se ha ejecutado la orden **ping 192.168.0.1**, que corresponde a la dirección del router de la red. Este ha respondido con los parámetros que se presentan en la captura de pantalla.

Figura 20

```
C:\Documents and Settings\Tutor>ping /?

Uso: ping [-t] [-a] [-n cuenta] [-l tamaño] [-f] [-i TTL] [-v TOS]
      [-r cuenta] [-s cuenta] [[-j lista-host] | [-k lista-host]]
      [-w tiempo de espera] nombre-destino

Opciones:
  -t            Ping el host especificado hasta que se pare.
                Para ver estadísticas y continuar - presionar Control-Inter;
                Parar - presionar Control-C.
  -a            Resolver direcciones en nombres de host.
  -n cuenta     Número de peticiones eco para enviar.
  -l tamaño     Enviar tamaño del búfer.
  -f            Establecer No fragmentar el indicador en paquetes.
  -i TTL        Tiempo de vida.
  -v TOS        Tipo de servicio.
  -r cuenta     Ruta del registro para la cuenta de saltos.
  -s count      Sello de hora para la cuenta de saltos.
  -j lista-host Afloja la ruta de origen a lo largo de la lista- host.
  -k lista-host Restringir la ruta de origen a lo largo de la lista- host.
  -w tiempo de espera Tiempo de espera en milisegundos para esperar cada
                      respuesta.
```

Se ha ejecutado **ping /?** y se nos muestran las diferentes opciones con las que se puede ejecutar este pedido.

## 2.2. Traceroute (tracert)

Permite descubrir los enrutadores intermedios entre el origen y el destino de los datagramas. Por lo tanto, permite averiguar qué rutas siguen los paquetes entre dos *hosts*, y en consecuencia todos los enrutadores por los que han pasado.

Muestra la dirección de cada una de las interfaces de los enrutadores por las que pasa el paquete.

La orden es: **traceroute [dirección IP o nombre DNS del host destino]** (o **tracert** en el sistema operativo Windows).

Con traceroute (tracert) se puede detectar la existencia de cuellos de botella en una red, identificando el origen del problema.

Al ejecutar por pantalla el comando, una de las columnas indica el número de saltos, el nombre o la dirección IP del enrutador correspondiente; las otras tres columnas señalan los tiempos asociados a tres intentos de llegar hasta el siguiente enrutador.

Figura 21

```
C:\Documents and Settings\Tutor>tracert www.adobe.com
Traza a la dirección www.wip4.adobe.com [192.150.16.64]
sobre un máximo de 30 saltos:

 1  <1 ms    <1 ms    <1 ms  192.168.0.1
 2      8 ms     6 ms     5 ms
 3     33 ms     6 ms     4 ms
 4     33 ms     5 ms     3 ms
 5     19 ms     5 ms     5 ms
 6  1632 ms     7 ms    13 ms
 7      52 ms    21 ms    31 ms
 8     38 ms    35 ms    29 ms
 9     40 ms    22 ms    19 ms
10     62 ms    28 ms    28 ms
11     61 ms    28 ms    27 ms
12     20 ms    32 ms    28 ms
13     53 ms    30 ms    47 ms
14     *        *        *
15     66 ms    59 ms    62 ms
16     63 ms    55 ms    56 ms
17     *        55 ms    *
53] 18     56 ms    49 ms    54 ms
19     65 ms    86 ms    61 ms  ae-14-14.bari.Madrid2.Level3.net [4.69.158.169]
20     *        86 ms    *
21     *        126 ms   *
51] 22     *        *        * Tiempo de espera agotado para esta solicitud.
23     105 ms   103 ms   *
31] 24     68 ms    243 ms   97 ms  X0-level3-1x10G.London.Level3.net [4.68.70.134]
25     163 ms   150 ms   249 ms  cr1-te-0-1-1-0.ft3.savvis.net [206.28.100.81]
26     214 ms   200 ms   192 ms  te-3-0-0.rar3.washington-dc.us.xo.net [207.88.12
.74]
27     209 ms   255 ms   257 ms  hr2-tengig-13-1-0.dallasdai.savvis.net [204.70.1
93.26]
28     210 ms   201 ms   195 ms  205.216.46.130
29     *        220 ms   203 ms  207.88.12.96.ptr.us.xo.net [207.88.12.96]
30     217 ms   *        192 ms  ae0d0.mcrl.dallas-tx.us.xo.net [216.156.0.82]

Traza completa.
```

Se ha ejecutado en Windows tracert (www.adobe.com) y se nos muestra buena parte de los datos de la ruta, con el número de salto, los tiempos de los tres intentos y las direcciones de los routers intermedios por los que han circulado los paquetes.

Figura 22

```
C:\Documents and Settings\Tutor>tracert /?
Uso: tracert [-d] [-h saltos_máximos] [-j lista_de_hosts] [-w tiempo_de_espera]
nombre_destino

Opciones:
  -d          No convierte direcciones en nombres de hosts.
  -h saltos_máximos  Máxima cantidad de saltos en la búsqueda del
                    objetivo.
  -j lista-de-host  Enrutamiento relajado de origen a lo largo de la
                    lista de hosts.
  -w tiempo_espera  Cantidad de milisegundos entre intentos.
```

Se ha ejecutado en Windows tracert /? y se nos muestran las diferentes opciones con las que se puede ejecutar este comando.

Su funcionamiento es el siguiente: se envía un paquete al *host* destino con el campo TTL=1. Así, el primer enrutador que lo recibe responde con un mensaje ICMP del tipo 11, que evidentemente contiene la dirección origen de este enrutador. Después se vuelve a enviar el mismo paquete pero ahora con TTL=2. En consecuencia, lo que lo descartará será el segundo enrutador por el que pase. Y así vamos enviando paquetes incrementando el TTL, y por lo tanto recibiendo las respuestas de los enrutadores. Cuando el paquete llega a la máquina destino, este paquete tiene un destinatario que es un servicio de aquella máquina que no espera ninguna petición. Por lo tanto, responde con un mensaje ICMP del tipo 3, que significa “*host* inabarcable”. De este modo ya sabemos que se ha llegado al destino y que no hay que seguir enviando paquetes con TTL mayores.

### 3. ARP (*adress resolution protocol*)

El protocolo ARP, *adress resolution protocol*, se encarga de encontrar la dirección física de un ordenador, empleada en las capas inferiores, a partir de su dirección de la capa de red. Está definido en los RFC 826 hasta 1982.

Los routers (enrutadores) necesitan conocer la dirección física, la dirección MAC, de una dirección IP. El que se encarga de este mapeo de direcciones es el protocolo ARP.

Cuando una estación debe enviar un paquete a una estación de la misma red local, la estación origen deduce que la estación destino está en la misma red a partir de la dirección IP de la estación de destino. Así, ya sabe que no debe enviar el paquete a ningún otro router.

Pero para poder enviarle las tramas Ethernet en las que irán los paquetes, es necesario que conozca la dirección física, la dirección MAC, del destinatario. Para obtenerla, emite un paquete dentro de una trama Ethernet con la dirección de *broadcast* como destino y con la dirección IP como contenido.

Si el destino es de la misma subred, entonces no pasa por el router, sino que es el equipo origen quien envía el datagrama al equipo destino directamente.

En cambio, si el destino pertenece a otra red, entonces el router contesta con la dirección MAC del router, y el equipo origen envía el datagrama al router, que se encargará de realizar el proceso hacia las otras redes a las que está conectado.

En definitiva, el funcionamiento es el siguiente: un *host* que quiere conocer la dirección MAC que tiene una cierta IP envía un paquete de tipo petición (ARP *request*) a la dirección de *broadcast* de la capa de enlace y espera a que la máquina que tenga aquella IP responda (ARP *response*).

Cuando se obtiene la respuesta, que contiene la dirección física, esta se almacena en local, en lo que se denomina **caché ARP** con las **correspondencias IP-MAC (dirección física- dirección IP)**. Por lo tanto, antes de realizar el proceso anterior, se comprueba si ya tiene la respuesta en su tabla ARP. Esta tabla se borra periódicamente para evitar que si una IP se asigna a otro equipo, al equipo antiguo le sigan llegando paquetes que ahora ya no son suyos.

Los sistemas operativos incorporan una orden llamada **arp** con la que podemos conocer, entre otras opciones, el contenido de esta tabla. En concreto, con la instrucción de sistema **arp -a** podemos conocer estos contenidos.

Figura 23

```
C:\Documents and Settings\Tutor>arp -a
Interfaz: 192.168.0.110 --- 0x10003
Dirección IP      Dirección física      Tipo
 192.168.0.1        f8-1a-■-7f-7b-ec    dinámico
```

Se ha ejecutado en Windows, arp -a y se nos muestran los contenidos de esta tabla.

Figura 24

```
C:\Documents and Settings\Tutor>arp /?
Muestra y modifica las tablas de conversión de direcciones IP en direcciones físicas que utiliza el protocolo de resolución de direcciones (ARP).

ARP -s [inet_addr] [eth_addr] [if_addr]
ARP -d [inet_addr] [if_addr]
ARP -a [inet_addr] [-N if_addr]

-a      Pide los datos de protocolo actuales y muestra las entradas ARP actuales. Si se especifica inet_addr, sólo se muestran las direcciones IP y física del equipo especificado. Si existe más de una interfaz de red que utilice ARP, se muestran las entradas de cada tabla ARP.
-g      Igual que -a.
inet_addr  Especifica una dirección de Internet.
-N if_addr  Muestra las entradas ARP para la interfaz de red especificada por if_addr.
-d      Elimina el host especificado por inet_addr. inet_addr puede incluir el carácter comodín * (asterisco) para eliminar todos los hosts.
-s      Agrega el host y asocia la dirección de Internet inet_addr con la dirección física eth_addr. La dirección física se indica como 6 bytes en formato hexadecimal, separados por guiones. La entrada es permanente.
eth_addr  Especifica una dirección física.
if_addr   Si está presente, especifica la dirección de Internet de la interfaz para la que se debe modificar la tabla de conversión de direcciones. Si no está presente, se utilizará la primera interfaz aplicable.

Ejemplo:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Agrega una entrada estática
> arp -a      .... Muestra la tabla arp.
```

Se ha ejecutado en Windows arp /? y se nos muestran las diferentes opciones con las que se puede ejecutar esta instrucción.

## 4. Router (o enrutador)

Es un dispositivo de red que permite interconectar redes (físicas y lógicas). Su estructura interna es parecida a la de un ordenador, dado que dispone de memoria, interfaces de entrada y salida, CPU (unidad central de procesamiento) y un sistema operativo.

Figura 25



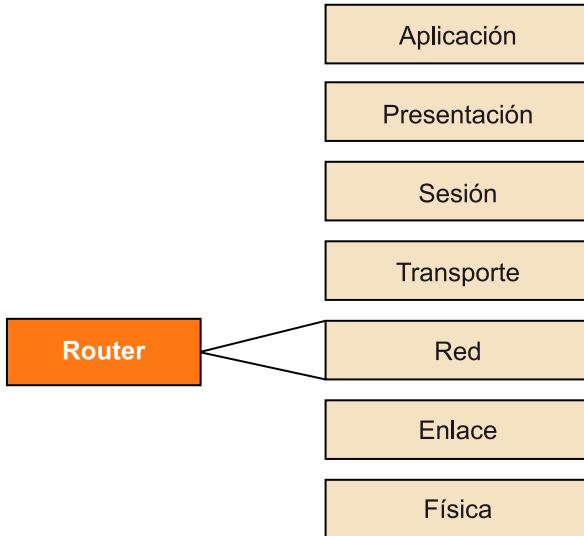
Dos modelos de routers, que también actúan como puntos de acceso Wi-Fi.

Se utiliza tanto en redes locales como en redes de gran alcance. Obtiene la información en el **nivel de red** para tomar las decisiones de enrutamiento o ruta más adecuada para enviar los datos recibidos, de manera que estos puedan llegar a su destino.

Permite la comunicación entre un único ordenador o dispositivo e internet, entre una red e internet o entre dos o más redes.

Su funcionalidad es la de proporcionar a los paquetes de datos (datagramas) que se transmiten una ruta segura y fiable desde el origen hasta el destino. Los routers trabajan en la capa 3 del modelo OSI, es decir, en la capa de red, y utilizan direcciones IP (*internet protocol*, protocolo de internet) para enrutar y conmutar los paquetes de datos en las diferentes interfaces.

Figura 26



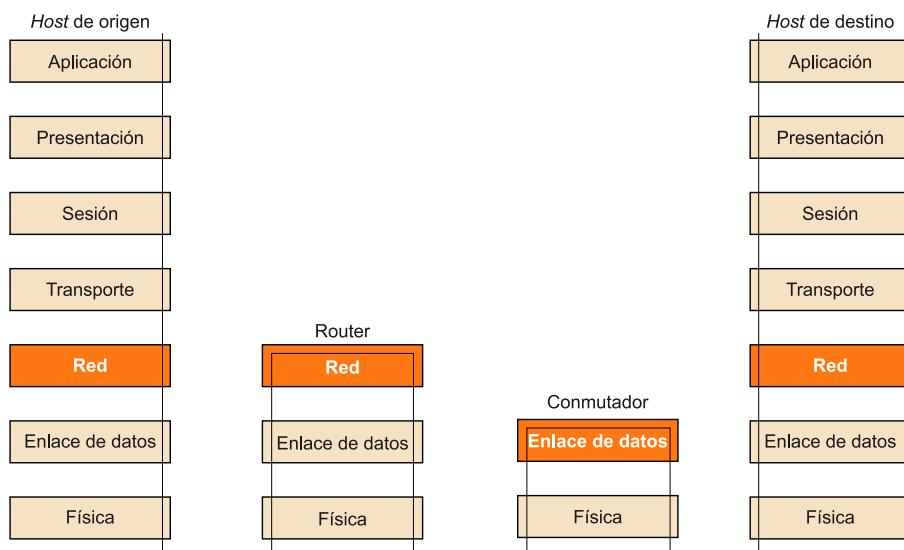
El router interviene en el nivel de la capa de red.

Por lo tanto, son dispositivos que tienen unas funciones clave para el buen funcionamiento de las redes. Para llevarlas a cabo se deben configurar diferentes parámetros de estos dispositivos.

Para llevar a cabo estas funcionalidades incorpora algunos algoritmos, como **RIP** (protocolo de información del enrutamiento), que calcula la distancia entre el enrutador y la estación receptora del paquete, teniendo en cuenta parámetros como el número de saltos necesarios.

La diferencia fundamental entre un **switch** (o comutador) y un **router** es que el primero opera en la capa de enlace, enviando paquetes mediante las direcciones MAC comentadas en el módulo anterior, y el segundo opera en la capa de red, empleando direcciones IP.

Figura 27



En este esquema podemos ver los niveles en los que actúan un **switch** y un router. Por lo tanto, queda justificado que los routers los presentamos en este módulo en el que estamos profundizando en la capa de red.

En cuanto a las funciones principales de los **routers**, estas están directamente asociadas con funcionalidades propias de la capa de red:

- **Segmentación.** Pueden segmentar el tráfico de una red mayor en varias redes más pequeñas. De este modo, los paquetes de difusión o *broadcast* se pueden canalizar directamente hacia la parte de la red que les corresponde.
- **Commutación.** Con esta funcionalidad, los paquetes de datos se van enviado por la interfaz correcta. La decisión se toma según las tablas de enrutamiento.
- **Determinación de la ruta.** Los routers determinan la ruta según diferentes parámetros, como el ancho de banda de la línea, el número de saltos que debe realizar un paquete de datos y los parámetros de rendimiento. Tengamos muy en cuenta, por lo tanto, que dos paquetes de datos con un mismo origen y destino pueden seguir rutas diferentes.

Existen dos categorías de routers: los más profesionales y los de un ámbito doméstico o de pequeñas oficinas. Los primeros están diseñados para crear redes corporativas de tamaño medio o grande, con amplias posibilidades de configuración y gestión. Los líderes en estos tipos de equipamientos son Cisco, 3Com, Nokia... En cuanto a los segundos, tenemos fabricantes como Intel, 3Com, D-Link, NetGear, Linksys, etc.

Cada router tiene sus propias características externas, por ejemplo en cuanto a número y tipo de puertos exteriores que ofrece.

#### 4.1. Las tablas de enrutamiento

El enrutamiento en el router se lleva a cabo mediante unas tablas, denominadas tablas de enrutamiento, que disponen de la información necesaria para interconectar todas las subredes que configuran Internet.

El router es el que decide la ruta que deben seguir los paquetes consultando su tabla de enrutamiento. Todo dispositivo que tenga una dirección IP asignada deberá disponer de una tabla de enrutamiento, ya sea una estación, router o cualquier otro dispositivo.

Presentamos una tabla de enrutamiento de una estación, con IP 172.26.0.27, con un adaptador Wi-Fi instalado. Esta tabla se ha obtenido mediante el comando de Windows **route print**.

Figura 28

C:\Documents and Settings\Tutor>route print					
<b>ILista de interfaces</b>					
0x1 .....	MS TCP Loopback interface				
0x10003 .. 00 0c 43 ae f8 f2 .....	802.11n USB Wireless LAN Card - Minipuerto				
el administrador de paquetes					
<b>Rutas activas:</b>					
Destino de red	Máscara de red	Puerta de acceso	Interfaz	Métrica	
0.0.0.0	0.0.0.0	172.26.0.1	172.26.0.27	25	
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1	
169.254.0.0	255.255.0.0	172.26.0.27	172.26.0.27	20	
172.26.0.0	255.255.255.0	172.26.0.27	172.26.0.27	25	
172.26.0.27	255.255.255.255	127.0.0.1	127.0.0.1	25	
172.26.255.255	255.255.255.255	172.26.0.27	172.26.0.27	25	
224.0.0.0	240.0.0.0	172.26.0.27	172.26.0.27	25	
255.255.255.255	255.255.255.255	172.26.0.27	172.26.0.27	1	
Puerta de enlace predeterminada:		172.26.0.1			
<b>Rutas persistentes:</b>					
ninguno					

Tabla de enruteamiento obtenida con el comando *route print* del sistema operativo Windows.

Las filas de la tabla se consultan no en el orden en el que aparecen sino en el orden de máscara decreciente (en primer lugar, las de 32 bits, etc).

Detallamos algunos de los elementos de la tabla:

- La primera entrada (0.0.0.0) permite a la estación comunicarse con estaciones remotas. Notemos que la máscara no tiene ningún bit en 1. Esta es la ruta por defecto. El enruteador establecido para acceder a estaciones remotas queda identificado en la tabla con la IP: 172.26.0.1. Corresponde a la puerta de enlace.
- La tercera entrada (169.254.0.0) corresponde a lo que se denomina *zeroconf route*, una dirección privada que se activa para autoconfigurarse la red, antes de activarse el DHCP.
- La dirección 172.26.0.27 corresponde a la dirección IP de la estación, y se denomina interfaz de *Loopback* (dirección con la que se conoce el ordenador local desde el mismo ordenador local).
- La octava entrada (255.255.255.255) solo nos indica que los *broadcasts* IP se restringirán a la red local.

## 4.2. Routers Wi-Fi

Actualmente la mayoría de routers incorporan la posibilidad adicional de conexión inalámbrica. Teniendo en cuenta que son dispositivos fundamentales a la hora de configurar una red inalámbrica, en el siguiente apartado de este tema trataremos el tema de la instalación de una red Wi-Fi, detallando el equipamiento Wi-Fi necesario, el proceso y los elementos que nos pueden llevar a configurarla, así como algunos programas que nos pueden ser útiles para trabajar con redes inalámbricas.



Figura 29

## 5. Configuración de un router

Antes de adentrarnos en el proceso de configuración de un enrutador, detallaremos los elementos que lo componen:

- Un software interno para gestión de las comunicaciones.
- Puertos para conectar el punto de acceso a internet o a la red cableada. Los puntos de acceso pueden disponer de uno o más puertos 10/100Base-T (RJ-45). Por lo tanto, llevan integrado un *hub* o *switch*; y en el caso de necesitar más puertos siempre se puede comprar un *hub* o *switch* independiente y conectarlo a uno de los puertos del router.

Y en el caso de que sea un router Wi-Fi:

- Un equipo de radio (de 2,4 Ghz en el caso de 802.11b y 802.11g, o de 5 Ghz en el caso de 802.11a).
- Una o dos antenas, que pueden o no apreciarse exteriormente.

Figura 30



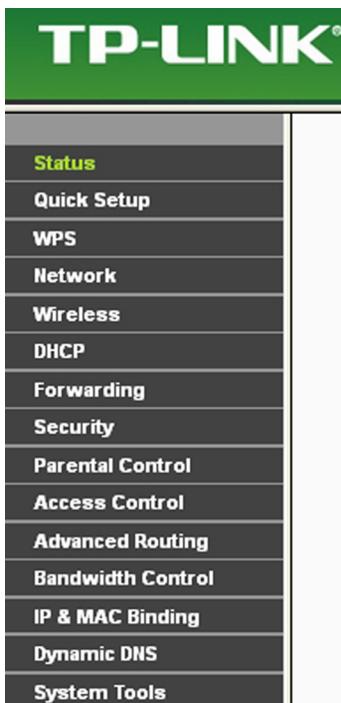
Router ADSL de Movistar, Home Station ADB P.dg A4001N1, diseñado por Telefónica I+D. Podemos observar las antenas, enlace a la línea ADSL, 4 puertos de enlace Ethernet para conectarlos a un ordenador, a un switch, a un hub..., botón de reset (para restablecerlo a la configuración de fábrica), botón para conectar/desconectar el Wi-Fi del router y el conector a la corriente eléctrica.

En cuanto al tema de los puertos, también podemos encontrar routers que disponen de otros, como:

- **Uplink port**, unos puertos especiales para conectar un *hub* o *switch* de una red local Ethernet.
- Puertos paralelos o USB para conectar por ejemplo una impresora.
- Puertos para conectar una antena externa para mejorar su alcance.

En cuanto a la **configuración y gestión del router**, a menudo solo hay que conectarse con un navegador a la dirección IP del router. Así, entraremos en una interfaz basada en páginas web desde la que podremos configurar sus parámetros.

Figura 31



Grupos de parámetros del router TP-LINK Wireless N Router WR841N que son accesibles y, buena parte de ellos, configurables desde esta interfaz.

Figura 32

The screenshot shows the Site Map of a Zyxel router's configuration interface. The main navigation bar at the top includes links for SITE MAP and HELP. Below the navigation bar, the Site Map title is displayed. The left sidebar contains links for Wizard Setup, Advanced Setup, Maintenance, and Logout. The main content area is divided into three columns:

- Wizard Setup:** Includes links for Wizard Setup, Password, LAN, Wireless LAN, WAN, NAT, Security, Dynamic DNS, Time and Date, Remote Management, UPnP, Logs, and Media Bandwidth Mgmt.
- Advanced Setup:** Includes links for Password, LAN, Wireless LAN, WAN, NAT, Security, Dynamic DNS, Time and Date, Remote Management, UPnP, Logs, and Media Bandwidth Mgmt.
- Maintenance:** Includes links for System Status, DHCP Table, Wireless LAN, Diagnostic, and Firmware.

Grupos de parámetros de configuración de un router Zyxel.

#### Nota

Aun así, también hay algunos routers que no utilizan una interfaz web, sino que requieren la introducción directa de una línea de comandos, lo que se conoce con el nombre de interfaz de línea de comandos (CLI, command line interface); o incluso que se requiera un sistema operativo particular, como es el caso de Airport Base Station de Apple.

Una vez hemos entrado en la parte de **configuración del router**, procederemos a revisar y, si hace falta, modificar su configuración.

Antes de nada, mencionaremos que cada router tiene una configuración propia, y **a menudo la configuración que viene predeterminada de fábrica ya puede satisfacer nuestros intereses**. No obstante, se recomienda variar los parámetros de seguridad que venden por defecto, como por ejemplo claves WEP/WPA y nombre de usuario y clave de acceso (*password*) para acceder a la configuración, dado que estos valores por defecto se pueden obtener fácilmente por internet.

Destacamos que podemos distinguir dos conjuntos de parámetros en la configuración de los routers: los que permiten gestionar la conexión de la red cableada o internet (**internet setting**, **IP setting**, **network setting** o similar) y los que gestionan la red inalámbricas (**wireless setting**, **AP setting** o parecido).

En el caso de **gestión de la red cableada**, los parámetros que hay que configurar en el router son los mismos que los que se configuran en un ordenador o dispositivo más de la red cableada. Por lo tanto, el router tendrá dos direcciones IP (y máscaras de subred), una que lo identifica dentro de la red inalámbrica y otra para identificarlo dentro de la red cableada.

Antes de realizar cambios en la configuración del router es recomendable disponer del manual de usuario que pone a nuestra disposición su fabricante y, al realizar cualquier cambio, documentarlo para poderlo revertir si es el caso. También existe la posibilidad de restablecer sus valores de configuración directamente a los valores de fábrica. Los routers profesionales disponen de más opciones que los domésticos.

Las opciones de configuración inciden en aspectos de gestión de la red como los siguientes:

- **Habilitar o deshabilitar la red inalámbrica** (**enable wireless networking**). Puede ser útil cuando solo queremos el punto de acceso con las funciones de router y para la red cableada.
- **Servidor DHCP**. A menudo los puntos de acceso tienen habilitado el servidor DHCP para asignar de manera automática las direcciones IP a los equipos que se conectan. Pero con esta opción podemos deshabilitarlo.
- **Potencia de transmisión** (**transmit power**). Esta opción está implementada en algunos puntos de acceso y permite variar la potencia de transmisión para dar más cobertura.
- **Registro de actividad** (**log file**). Algunos puntos de acceso ofrecen la posibilidad de dejar un registro de la actividad realizada. Puede permitir comprobar la actividad de la red y detectar posibles intrusiones.

En cuanto a las **redes inalámbricas**, el proceso de instalación es relativamente sencillo, considerando que los certificados Wi-Fi nos garantizan la buena compatibilidad entre los diferentes equipos y dispositivos.

Se pueden establecer dos tipos de redes inalámbricas: **modo ad hoc** o **modo infraestructura**.

Para instalar una red *ad hoc*, en primer lugar habrá que situar a poca distancia los diferentes equipos que se quiere interconectar, y en uno de los equipos se configurarán de manera manual los parámetros Wi-Fi. Para configurarlo habrá

que ejecutar el programa de utilidades Wi-Fi de la tarjeta Wi-Fi, o emplear la herramienta o aplicación Wi-Fi que incorpora el propio sistema operativo. En líneas generales habrá que configurar:

- El tipo de red, en modo *ad hoc*, BSS, equipo a equipo o términos similares.
- Poner un nombre a la red, lo que se conoce con el nombre de SSID (*service set identifier*) o nombre de red (*network name*).
- Canal, eligiendo algún número concreto de canal tipo de seguridad, puede ser WEP o WPA por ejemplo, con una clave de acceso.

Así, cualquier otro ordenador o dispositivo con adaptador Wi-Fi que tenga configurados los mismos parámetros, y en el mismo radio de cobertura, podrá formar parte de la red y compartir recursos con el resto de los ordenadores de la red.

Para configurar una red Wi-Fi en **modo infraestructura** será necesario configurar el router Wi-Fi. En cuanto a los **parámetros de los routers Wi-Fi** que podemos cambiar, destacaremos:

- **SSID (*service set identifier*)**, que es el nombre de la red (*network name*), lo que permite identificar el servicio y lo que aparece al realizar una busca de redes inalámbricas.
- **Canal (*channel*)**, con el que se emite la señal de onda portadora de radio. A menudo el sistema permite que la asignación de canal sea automática o manual. Antes de elegir un número de canal, es conveniente explorar las redes inalámbricas de la zona para poder emplear un canal que no se esté utilizando.
- **Seguridad (*security*)**, los parámetros de configuración de seguridad en el router permiten poder dar acceso a nuestra red inalámbrica a los equipos o usuarios que queramos, y/o cifrar el intercambio de información que se produzca. El tema de configuración de la seguridad, por su relevancia, lo trataremos en un próximo apartado.

Figura 33

En esta captura de pantalla se presentan los *wireless settings* de un router del fabricante TP-LINK. Se visualizan, entre otros, los parámetros SSID y Channel.

Figura 34

En esta captura de pantalla se presenta *wireless security* de un router del fabricante TP-LINK. Nos permite comprobar el protocolo de seguridad empleado WPA2-PSK, con cifrado AES, y la contraseña configurada (en la figura está borrada).

El área de cobertura, o zona en la que un ordenador o dispositivo puede conectarse con el router, depende de factores como la localización de este, las interferencias radioeléctricas, los tipos de antenas, los obstáculos que puedan existir entre el punto de acceso y el ordenador o dispositivo. En el caso de querer ampliar la zona de cobertura existe la posibilidad de ir situando diferentes **puntos de acceso** que complementen las coberturas del router.

Los puntos de acceso se configuran de un modo muy parecido a los routers y permiten extender el radio de cobertura de la red inalámbrica.

### Puntos de acceso (AP, *acces point*)

Un **punto de acceso** es un dispositivo encargado de conectar dispositivos Wi-Fi, con sus correspondientes tarjetas de red, para crear una red inalámbrica. Los puntos de acceso también son a menudo el puente de interconexión entre la red cableada e internet, por lo tanto, muchos de ellos también actúan como routers.

En cuanto a la configuración de los ordenadores o dispositivos que queramos conectar de manera inalámbrica a una red con un router o un punto de acceso, es necesario que estos dispongan del adaptador o tarjeta de red correspondiente, y que este quede configurado para que pueda acceder al router o a su punto de acceso de la red deseada. A menudo simplemente haciendo una exploración de las redes inalámbricas y aceptando la opción de conectar, el equipo ya se adaptará automáticamente a la configuración que le envíe el router. Solo habrá que introducir la clave WEP/WPA para establecer la conexión.

Si el router está configurado para no admitir conexiones automáticas, habrá que configurar cada equipo manualmente con los parámetros de la red, como tipo de red, nombre de la red, canal y seguridad.

También, en el caso de que el router no tenga activada la opción de asignación automática de las direcciones IP (DHCP activado), habrá que configurar el ordenador de manera manual. Este proceso dependerá del sistema operativo que tengamos instalado, a pesar de que los parámetros que deberemos introducir serán:

- **Número IP del ordenador.** Es importante señalar que es necesario que esté en el rango de direcciones aceptadas por el router. Por ejemplo, si el router tiene dirección 172.26.0.1, entonces los equipos se podrían asignar a los números 172.26.0.x, donde x tendrá valores entre 2 y 255.
- **Máscara de subred.** Generalmente será el número 255.255.255.0 para redes que dispongan de menos de 255 terminales.
- **Puerta de enlace.** Corresponde a la dirección IP del router. En el ejemplo anterior sería 172.26.0.1.
- **DNS.** En este caso, podemos configurarlo o bien de manera que automáticamente adquiera estos valores del router, o bien de modo que el usuario haya de introducir manualmente los DNS con los valores que le habrá facilitado su proveedor de servicios.

Una vez se haya instalado la red, solo habrá que comprobar que esta funciona correctamente. En concreto, se puede comprobar si hay conexión a internet en los diferentes equipos, si se localizan los recursos compartidos con otros equipos, etc.

