multicast, etc. Al tratarse el mecanismo multicast de una extensión que no se recogía en la versión original de IPv4, su soporte es opcional. El tráfico multicast es adecuado para servicios multimedia de internet (streaming) en directo, pero no se suele emplear. Para que una máquina se agregue/desagregue de un grupo multicast debe enviar mensajes basados en el protocolo IGMP (Internet Group Management Protocol). El uso más generalizado de multicast es en los protocolos de encaminamiento OSPF o RIP.

- Clase E: direcciones reservadas.
  - Los cinco primeros bits de la dirección llevan el valor «1111», por lo que el primer byte va de 240 a 255. Usos experimentales.

El número máximo de redes y de hosts (direcciones asignables) en una red clase A, B, C están resumidos en la siguiente tabla:

Tabla 3. Redes clases A, B y C (número de redes y de hosts)

	Número de redes	**Número de hosts**
Clase A	126	$2^{24} - 2$
Clase B	2^{14}	$2^{16} - 2$
Clase C	2^{21}	$2^{8} - 2 = 254$

En la columna «número de hosts» se restan dos direcciones que se destinan a la dirección de red y dirección de difusión. Estas direcciones no son asignables a ningún nodo de la red. En el direccionamiento IP se pueden encontrar direcciones especiales de varios tipos:

- Dirección de red: es la dirección de la red completa. Mantiene la parte de red con el valor identificativo de la misma y pone todos los bits de la parte host a «0». Sirve para identificar la red. Por ejemplo:
  - Clase A: 98.0.0.0
  - Clase B: 130.14.0.0
  - Clase C: 200.16.102.0

- Dirección de difusión (broadcast): se utiliza para enviar información a todos los elementos de la red. Se dice que es una difusión dirigida, ya que se especifica la red concreta a la que se quiere hacer broadcast. La dirección de difusión mantiene la parte de red con el valor identificativo de la misma y pone todos los bits de la parte host a «1». Por ejemplo:
  - Clase A: 98.255.255.255
  - Clase B: 130.14.255.255
  - Clase C: 200.16.102.255

- Dirección asignable: se utiliza para direccionar hosts (ordenadores, servidores, routers, impresoras, etc.). Presenta el siguiente formato: parte de red (= valor identificador de la red donde está el host). Parte de host no puede estar con todos los bits a 1 (dirección de broadcast) o a 0 (dirección de red).

- Clase A → 98.0.0.1
- Clase B → 130.14.255.254
- Clase C → 200.16.102.98

• Direcciones IP con usos especiales. Existen múltiples direcciones que tienen usos especiales y están registradas en la RFC 3330, como, por ejemplo:

- «Este host»: 0.0.0.0. Hace referencia a la propia máquina. Se emplea cuando el equipo no tiene asignada una dirección IP; el DHCP de la red detecta este tipo de direcciones en los datagramas y automáticamente asignará una IP válida para un host y se la enviará al host.
- Loopback: 127.x.x.x (x: «cualquier valor»). Hace referencia a «mi máquina», pero, a diferencia de la anterior, no sale por la tarjeta de red (se asocia la dirección 127.0.0.1 al local host o máquina local).
- Difusión limitada (todos los hosts de mi red): 255.255.255.255.
- Difusión dirigida: (parte de red = valor red específico) + (parte de hosts = «1...1» ⇒ Todo 1's).
- Reserva para pruebas de rendimiento: direcciones 192.18.0.x y 192.19.255.x.
- Direcciones IP privadas – RFC 1918. Se reservan para el direccionamiento en redes privadas, no utilizándose en redes públicas (internet). Estas direcciones son:
  - Clase A: 10.0.0.0 – 10.255.255.255
  - Clase B: 172.16.0.0 – 172.31.255.255
  - Clase C: 192.168.0.0 – 192.168.255.255

• Máscara de red. La máscara de red es una plantilla de 32 bits que indica qué parte de la dirección IP es de red (se representa con 1's en la plantilla) y qué parte es de hosts (0's en la plantilla). Las máscaras naturales (o por defecto; lo que se denomina direccionamiento classful o clásico) para las clases A, B y C son, respectivamente:

- Clase A: 255.0.0.0 (o «/8»; denominado prefijo IP, se sitúa a continuación de una dirección de red/asignable e indica el número de bits a «1» de la máscara).
- Clase B: 255.255.0.0 (o «/16»).
- Clase C: 255.255.255.0 (o «/24»).

Si expresamos en binario la dirección IP de un equipo y su máscara, podemos obtener la dirección de red asociada efectuando una operación «AND» lógica con aquellas. Ejemplo:

Dir.IP:	01101111.11000000.01011110.00000011
Mask:	11111111.00000000.00000000.00000000
Dir. Red:	01101111.00000000.00000000.00000000

• Wildcard. Mientras que un bit 0 en una máscara wildcard significa «coincide con los bits», un 0 en una máscara de subred significa «no coincidir». Así, una máscara wildcard de 0.0.0.255 es el equivalente a una máscara de subred de 255.255.255.0.

- Direcciones APIPA: APIPA (Automatic Private Internet Protocol Addressing o direccionamiento privado automático del protocolo de internet) es un protocolo que se introdujo con el sistema operativo Windows 98 para obtener la configuración de red cuando el sistema está configurado para obtener una dirección dinámicamente y, al iniciar, este no encuentra un servidor DHCP.

2.1.2.1. Subnetting o división de redes en subredes

El subnetting consiste en tomar bits de la parte de host dividiendo una red más grande en subredes. El número de bits tomados se indica en la máscara. El subnetting surge porque el direccionamiento clásico era demasiado rígido. Así, por ejemplo, las redes de clase A son solo 126 y contienen cada una 2^{24} nodos, un número inmanejable para los equipos de comunicaciones y por tanto sin uso práctico. Sin embargo, si se subdivide esta red se crean redes más pequeñas y manejables y se puede seguir aprovechando este rango de direcciones de la forma más eficiente posible.

Ejemplo: una dirección de red 10.0.0.0/10, o lo que es lo mismo: 10.0.0.0 con máscara 255.192.0.0, indica que se dedica un byte a la parte de red (por ser una clase A: el valor del primer byte –10– está comprendido entre 1 y 126), y dos bits adicionales (los dos más a la izquierda en el segundo byte) a la parte de subred, por lo que existen 4 subredes (es decir, todas las posibles combinaciones de 2 bits: «00», «01», «10» y «11»). Para la parte host quedan 32 – 10 = 22 bits, por lo que número de hosts posibles en cada una de las subredes será de $2^{22} - 2$ $\Rightarrow$ se restan dos direcciones porque cada subred contiene su propia dirección de red y de difusión/broadcast. En la tabla siguiente se muestran cuáles son estas direcciones para cada una de las subredes:

Tabla 4. Ejemplo de subnetting

Subred	Dirección de red	Dirección de difusión	Número de hosts en la subred
«00»	10.0.0.0	10.63.255.255	$2^{22} - 2$
«01»	10.64.0.0	10.127.255.255	$2^{22} - 2$
«10»	10.128.0.0	10.191.255.255	$2^{22} - 2$
«11»	10.192.0.0	10.255.255.255	$2^{22} - 2$

Si en nuestro ejemplo únicamente necesitásemos direccionar 2 subredes, tomaríamos las subredes «01» y «10», dejando libres «00» y «11», ya que las direcciones 10.0.0.0 y 10.255.255.255 serían las direcciones de red y difusión respectivamente de la red completa. En caso de necesitar hacer uso de las 4 subredes, ello no supondría ningún problema: se comenzaría por tomar la subred «00» y se terminaría por subred «11» (lo que se conoce como aplicación del criterio «subnet zero» y «subnet broadcast»). Este concepto, subnet zero, en la actualidad se aplica por defecto, ya no se consideran las redes clásicas y por tanto siempre es necesario indicar la dirección IP y su máscara de red, sea en notación decimal acompañando a la IP o en notación IPv4.

A la hora de hacer subnetting, podemos aplicar el mecanismo de VLSM (Variable Length Subnet Mask o máscara de subred de longitud variable) para un mejor reaprovechamiento de las direcciones IP. En una red con varias subredes, no todas tienen por qué tener el mismo tamaño. VLSM permite ajustar en cada subred la máscara (aumentando su número de bits a «1») para conseguir economía de IP (esto es, dejar en la parte de host –bits a «0» en la máscara– el menor número de bits que permita encajar las máquinas existentes). Por ejemplo:

10.20.0.0 /24 → 1.ª subred (254 máquinas; direcciones asignables: 10.20.0.1 a 10.20.0.254).

10.20.1.0 /24 → 2.ª subred (254 máquinas; direcciones asignables: 10.20.1.1 a 10.20.1.254).

10.20.2.0 /25 → 3.ª subred (126 máquinas; direcciones asignables: 10.20.2.1 a 10.20.2.126).

10.20.2.128 /25 → 4.ª subred (126 máquinas; direcciones asignables: 10.20.2.129 a 10.20.2.254).

2.1.2.2. Supernetting o agregación de redes

La técnica de supernetting también es llamada de agregación o reducción de direcciones. La agregación de redes permite reducir el tamaño de las tablas de encaminamiento y el tráfico de intercambio de información de ruteo porque posibilita que un router anuncie y tenga una única entrada en la tabla para un conjunto de rutas. Para ello, los routers deben soportar CIDR (Classless Interdomain Routing - RFC 1918), basado en el reparto de las redes clase C no asignadas aún en bloques de tamaño variable. De esta forma, si una instalación necesita 2.000 direcciones, se asignan 8 direcciones clase C contiguas en vez de una dirección clase B completa, aunque se podría hacer tanto supernetting como subnetting. En CIDR el encaminamiento no se realiza de acuerdo a la clase de red (de ahí el término «classless»: sin clase), sino solo según los bits de orden superior de la dirección IP, que se denominan prefijo IP, y viene dado por el número de bits a «1» de la máscara.

2.2. PROTOCOLO IP VERSIÓN 6

De los RFC que desarrollan el protocolo IPv6, cabe destacar la RFC 8200 (que deja obsoleta la RFC 2460, original de IPv6) y desarrolla las especificaciones del protocolo (formato de la cabecera fija y cabeceras de extensión, etc.). RFC 3513: direccionamiento (notación, tipos de direcciones).

A IPv6 también se le denomina IPng (Internet Protocol Next Generation). Este protocolo ha sido desarrollado para mejorar IPv4. Algunas de sus ventajas frente a este último son:

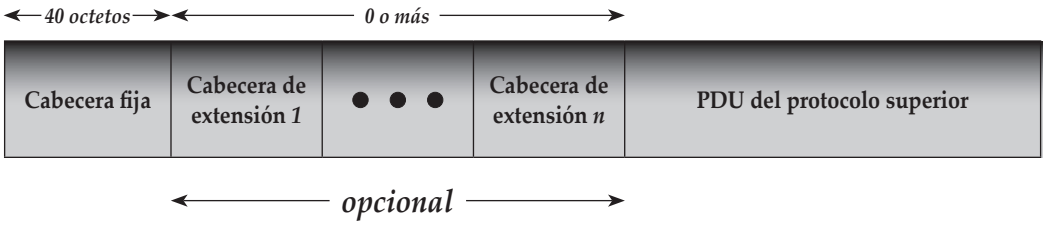
- Soluciona las limitaciones de direccionamiento mediante direcciones de 128 bits en vez de 32 bits.
- Reduce la complejidad para los usuarios y facilita el cambio de red, ya que permite autoconfiguración de direcciones y descubrimiento automático de vecindad (nodos conectados al mismo enlace/medio físico). La autoconfiguración puede ser stateful (predeterminada: la asignación de IP se lleva a cabo mediante un servidor DHCPv6) o stateless (sin intervención) y la lleva a cabo el protocolo NDP, Neighbour Discovery Protocol, que es la unión de DHCPv6 e ICMPv6.
- Mejora el enrutamiento (cálculo del next-hop o próximo salto más eficiente) y el procesamiento, gracias a:
  - Reducción del tiempo de proceso de la cabecera de los datagramas (cabecera con menos campos y de tamaño fijo: 40 bytes; desaparece la verificación de datos de cabecera, ya que otros mecanismos de nivel 2 realizan esta función)
  - No permite fragmentación intermedia (la realizan los extremos finales: hosts).
  - En backbone (redes públicas) permite una arquitectura jerárquica de direcciones basada en la agregación.
  - Datagramas alineados a 64 bits (preparados para los nuevos procesadores de 64 bits).
- Mejora la seguridad, incorporando extensiones para aportar autenticación, integridad y confidencialidad de los datos (IPSec nativo).

- Introduce QoS (Quality of Service, calidad de servicio) y CoS (Class of Service, clases de servicio), mediante el etiquetado de flujos.
- Posibilidad de paquetes con tamaño mayor que 64 KB (jumbogramas).
- Mejora los mecanismos multicast.
- Introduce las direcciones anycast.
- Desaparecen las direcciones broadcast, aunque se podrá hacer broadcast mediante direcciones multicast.

2.2.1. Datagrama IPv6 (formato)

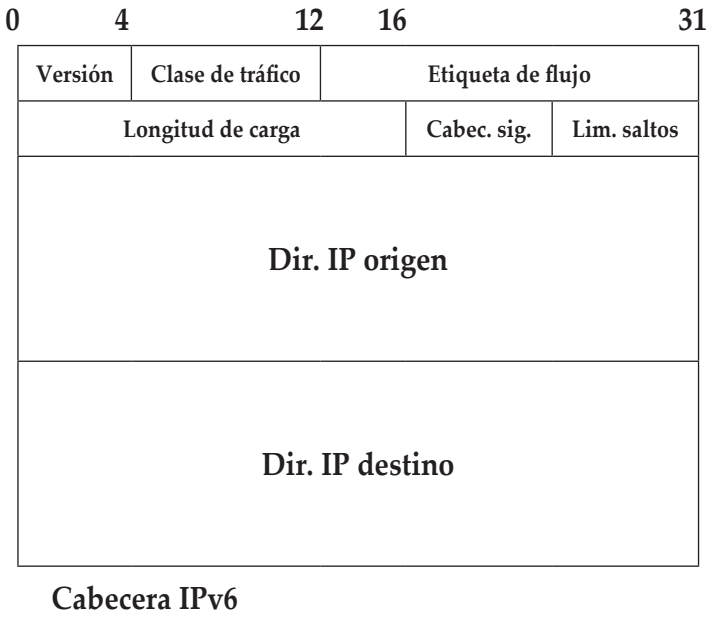
El datagrama IPv6 consta de: Cabecera fija (de 40 bytes) + Cabeceras de extensión (opcionales, en número «ilimitado») + PDU (Protocol Data Unit) del protocolo superior (lo que se encapsula en IPv6).

Figura 4. Formato del datagrama IPv4



La cabecera fija y las cabeceras de extensión opcionales incluyen el campo «cabecera siguiente», que llevará el tipo de cabecera de extensión que viene a continuación o el identificador del protocolo de nivel superior, según corresponda. La estructura de la cabecera fija de 40 bytes viene definida en el RFC 8200, tal y como se muestra a continuación:

Figura 5. Formato de la cabecera fija de 40 bytes



Las funciones de los ocho campos que componen la cabecera fija son:

- Versión (4 bits): versión del protocolo (6). Para IPv6 vale siempre 6 («0110»).
- Clase de tráfico / Prioridad (1 byte): clases o prioridades de paquetes.
- Etiqueta de flujo (20 bits): permite diferenciar aquellos paquetes que requieren un tratamiento especial. Este es el campo que indica la calidad de servicio. Muy útil para tráfico en tiempo real.
- Longitud carga útil (2 bytes): longitud del paquete después de la cabecera de 40 bytes. Es el tamaño de las cabeceras de extensión y los datos.
  - En IPv4, el campo Longitud incluía la longitud de la cabecera junto con los datos. En IPv6, no se considera la cabecera IPv6 (tamaño fijo), y las cabeceras de extensión se consideran parte de la carga. Así, el router no tiene que realizar cálculos de longitudes de datagramas.
  - Máximo tamaño de carga: 216 (bytes) = 64 KB.
  - IPv6 permite la definición de jumbogramas: paquetes de más de 64 KB, que solo tienen sentido si el MTU del nivel de enlace es superior a 64 KB. Ethernet puede llegar a utilizar tramas más grandes de 1522 B.
- Cabecera siguiente (1 byte): identifica el tipo de cabecera que sigue a la cabecera IPv6, indicamos algunos valores:
  - 0 (cabecera de opciones salto-a-salto).
  - 6 (TCP)
  - 17 (UDP).
  - 43 (cabecera de encaminamiento) - 44 (cabecera de fragmentación).
  - 51 (cabecera de autentificación) - 50 (cabecera ESP-Encapsulated Security Payload).
  - 60 (cabecera de opciones para el destino).
- Límite de saltos (1 byte): número restante de saltos permitidos. Cuando este campo tiene el valor cero el paquete es destruido y se envía de regreso al nodo fuente (dirección IP origen) un mensaje ICMPv6 tipo 3 (Time Exceeded).
- Dirección origen (16 bytes).
- Dirección destino (16 bytes): normalmente, dirección IP del destino del paquete. Puede no ser el último destinatario del paquete, si está presente la cabecera de encaminamiento.
- En cuanto a las cabeceras de extensión cabe destacar lo siguiente. De estas cabeceras algunas tienen formato fijo o variable (tipo, longitud y valor-datos de la opción), el orden de estas cabeceras se puede alterar, salvo la cabecera de opciones salto-a-salto, que siempre va la primera. Existen otras cabeceras adicionales, pero estas se enumeran en la RFC original de IPv6:
  - Cabecera de opciones salto-a-salto.
  - Cabecera de encaminamiento.
  - Cabecera de fragmentación.