El Protocolo IPv6

Versión – Fecha:	4.0 – 05/01/2004
Título:	El Protocolo IPv6
Tipo:	Documento Teórico
Autor(es):	6SOS
Editor:	Documento original facilitado por Jordi Palet Martínez, adaptación posterior por Alberto Cabellos-Aparicio

SUMARIO

Este documento describe desde un punto de vista técnico el nuevo protocolo IPv6, desarrollado por IETF. IPv6 (también conocido como IPng, “Internet Next Generation”) es una nueva versión de IP, diseñada como una evolución de IPv4 (el protocolo que se usa actualmente en Internet). IPv6 se puede instalar como una actualización de software en las máquinas y es capaz de trabajar con el actual protocolo IPv4. Se prevé que se empiece a desplegar de una manera gradual, puesto que hay que mantener todas las infraestructuras que actualmente funcionan con IPv4.

PALABRAS CLAVE

IPv6, protocolo, direcciones, anycast, multicast, unicast, autoconfiguración, seguridad, movilidad

TABLA DE CONTENIDO

1) Introducción 3
1.1. Sobre el documento 3
1.2. Motivos de IPv6 3
1.3. Características principales de IPv6 3
2) La cabecera IPv6 5
3) Direccionamiento en IPv6 8
3.1. Definición de dirección IPv6 8
3.2. Direcciones Unicast IPv6 8
3.2.1. Direcciones Unicast IPv6 Globales 8
3.2.2. Direcciones Unicast Locales de Enlace (Link-Local) 9
3.3. Direcciones Anycast IPv6 9
3.4. Direcciones Multicast IPv6 10
3.5. Representación de direcciones IPv6 11
4) Autoconfiguración en IPv6 13
4.1. Introducción 13
4.2. Stateless Autoconfiguration 13
4.3. Statefull Autoconfiguration 15

TABLA DE FIGURAS

Figura 2-1: La cabecera IPv4 5
Figura 2-2: Campos modificados y que desaparecen 5
Figura 2-3: Cabecera IPv6 6
Figura 2-4: Extensiones en IPv6 7
Figura 3-1: Estructura de dirección IPv6 8
Figura 3-2: Prefijos de subred 8
Figura 3-3: Tabla 3 - Estructura direcciones locales de enlace 9
Figura 3-4: Tabla 4 - Dirección anycast del router de la subred 9
Figura 3-5: Formato direcciones multicast 10
Figura 3-6: Significado bits de ámbito en Multicast 10
Figura 3-7: Representación de direcciones IPv6 11
Figura 3-8: Ejemplos de direcciones IPv6 11
Figura 3-9: Ejemplos de direcciones IPv6 11
Figura 3-10: Direcciones representadas en formato abreviado 11
Figura 3-11: Representación de prefijos IPv6 12
Figura 3-12: Representaciones con prefijos 12
Figura 3-13: Ejemplo dirección completa 12

1) Introducción

1.1. Sobre el documento

Este documento describe desde un punto de vista técnico el nuevo protocolo IPv6, desarrollado por IETF. IPv6[1] (también conocido como IPng, "Internet Next Generation") es una nueva versión de IP, diseñada como una evolución de IPv4 (el protocolo que se usa actualmente en Internet). IPv6 se puede instalar como una actualización de software en las máquinas y es capaz de trabajar con el actual protocolo IPv4. Se prevé que se empiece a desplegar de una manera gradual, puesto que hay que mantener todas las infraestructuras que actualmente funcionan con IPv4.

1.2. Motivos de IPv6

El motivo básico por el que surge, en el seno del IETF (Internet Engineering Task Force), la necesidad de crear un nuevo protocolo, que en un primer momento se denominó IPng (Internet Protocol Next Generation, o "Siguiente Generación del Protocolo Internet"), fue la evidencia de la falta de direcciones.

IPv4 tiene un espacio de direcciones de 32 bits, es decir, 2^{32} (4.294.967.296). En cambio, IPv6 nos ofrece un espacio de 2^{128} (340.282.366.920.938.463.463.374.607.431.768.211.456).

Sin embargo, IPv4 tiene otros problemas o "dificultades" que IPv6 soluciona o mejora.

Los creadores de IPv4, a principio de los años 70, no predijeron en ningún momento, el gran éxito que este protocolo iba a tener en muy poco tiempo, en una gran multitud de campos, no sólo científicos y de educación, sino también en innumerables facetas de la vida cotidiana.

Desde ese momento, y debido a la multitud de nuevas aplicaciones en las que IPv4 ha sido utilizado, ha sido necesario crear "añadidos" al protocolo básico. Entre los "parches" más conocidos, podemos citar medidas para permitir la Calidad de Servicio (QoS), Seguridad (IPsec)[2], y Movilidad[3], fundamentalmente.

El inconveniente más importante de estas ampliaciones de IPv4, es que fueron diseñadas posteriormente y es difícil usar más de un "añadido" simultáneamente.

1.3. Características principales de IPv6

Si resumimos las características fundamentales de IPv6 obtenemos la siguiente relación:

- Mayor espacio de direcciones.
- "Plug & Play": Autoconfiguración.
- Seguridad intrínseca en el núcleo del protocolo (IPsec).
- Calidad de Servicio (QoS) y Clase de Servicio (CoS).
- Multicast: Envío de UN mismo paquete a UN GRUPO de receptores.
- Anycast: Envío de UN paquete a UN receptor dentro de UN GRUPO.
- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los encaminadores (routers), alineados a 64 bits (preparados para su procesado óptimo con los nuevos

[1] *RFC2460 - Internet Protocol, Version 6 (IPv6)*
[2] *RFC2401 - Security Architecture for the Internet Protocol (IPsec)*
[3] *draft-ietf-mobileip-ipv6-24.txt Mobility Support in IPv6*

procesadores de 64 bits), y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del encaminador (router).

- Posibilidad de paquetes con carga útil (datos) de más de 65.535 bytes.
- Encaminado (enrutado) más eficiente en el troncal (backbone) de la red, debido a una jerarquía de direccionamiento basada en la agregación.
- Renumeración y “multi-homing”, que facilita el cambio de proveedor de servicios.
- Características de movilidad.

2) La cabecera IPv6

Hay que insistir, de nuevo, en que estas son las características básicas, y que la propia estructura del protocolo permite que este crezca, o dicho de otro modo, sea escalado, según las nuevas necesidades y aplicaciones o servicios lo vayan precisando.

Veamos, en primer lugar, la descripción de la cabecera de un paquete IPv4:

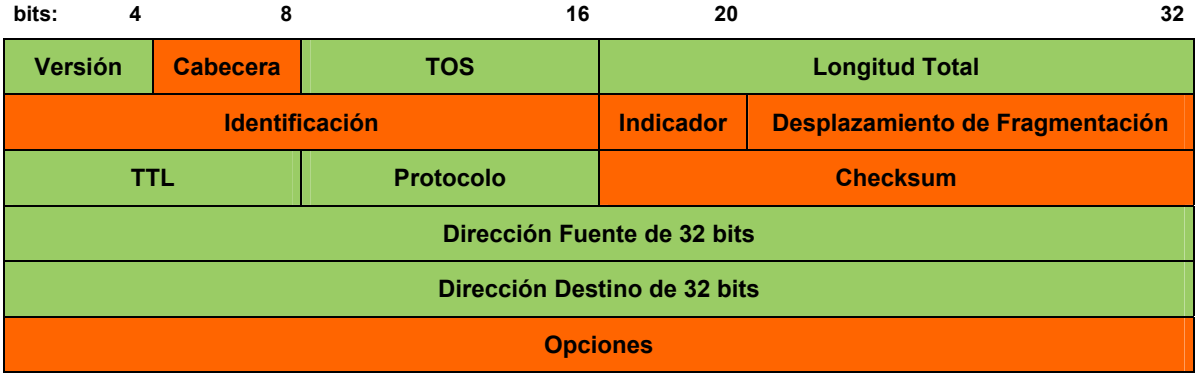

Figura 2-1: La cabecera IPv4

Como vemos, la longitud mínima de la cabecera IPv4 es de 20 bytes (cada fila de la tabla supone 4 bytes). A ello hay que añadir las opciones, que dependen de cada caso.

En la tabla anterior, hemos marcado, mediante el color de fondo, los campos que van a desaparecer en IPv6, y los que son modificados, según el siguiente esquema:

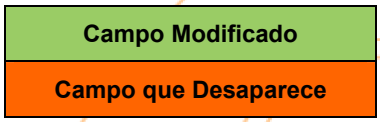

Figura 2-2: Campos modificados y que desaparecen

Hemos pasado de tener 12 campos, en IPv4, a tan solo 8 en IPv6.

El motivo fundamental por el que los campos son eliminados, es la innecesaria redundancia. En IPv4 estamos facilitando la misma información de varias formas. Un caso muy evidente es el checksum o verificación de la integridad de la cabecera: Otros mecanismos de encapsulado ya realizan esta función (IEEE 802 MAC, framing PPP, capa de adaptación ATM, etc.).

El caso del campo de "Desplazamiento de Fragmentación", es ligeramente diferente, dado que el mecanismo por el que se realiza la fragmentación de los paquetes es totalmente modificado en IPv6, lo que implica la total "inutilidad" de este campo. En IPv6 los encaminadores no fragmentan los paquetes, sino que de ser precisa, dicha fragmentación/desfragmentación se produce extremo a extremo.

Algunos de los campos son renombrados:

- **Longitud total** ➔ longitud de carga útil (payload length), que en definitiva, es la longitud de los propios datos, y puede ser de hasta 65.536 bytes. Tiene una longitud de 16 bits (2 bytes).
- **Protocolo** ➔ siguiente cabecera (next header), dado que en lugar de usar cabeceras de longitud variables se emplean sucesivas cabeceras encadenadas, de ahí que desaparezca el campo de opciones. En muchos casos ni siquiera es procesado por los encaminadores, sino tan sólo extremo a extremo. Tiene una longitud de 8 bits (1 byte).

- **Tiempo de vida** ➔ límite de saltos (Hop Limit). Tiene una longitud de 8 bits (1 byte).

Los nuevos campos son:

- **Clase de Tráfico (Traffic Class)**, también denominado Prioridad (Priority), o simplemente Clase (Class). Podría ser más o menos equivalente a TOS en IPv4. Tiene una longitud de 8 bits (1 byte).
- **Etiqueta de Flujo (Flow Label)**, para permitir tráficos con requisitos de tiempo real. Tiene una longitud de 20 bits.

Estos dos campos, como se puede suponer, son los que nos permiten una de las características fundamentales e intrínsecas de IPv6: Calidad de Servicio (QoS), Clase de Servicio (CoS), y en definitiva un poderoso mecanismo de control de flujo, de asignación de prioridades diferenciadas según los tipos de servicios.

Por tanto, en el caso de un paquete IPv6, la cabecera tendría el siguiente formato:

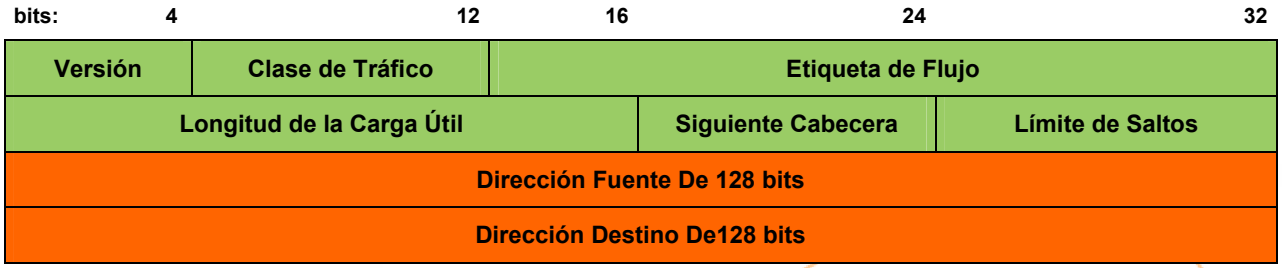

Figura 2-3: Cabecera IPv6

El campo de versión, que es igual a 6, lógicamente, tiene una longitud de 4 bits.

La longitud de esta cabecera es de 40 bytes, el doble que en el caso de IPv4, pero con muchas ventajas, al haberse eliminado campos redundantes.

Además, como ya hemos mencionado, la longitud fija de la cabecera, implica una mayor facilidad para su procesado en encaminadores y conmutadores, incluso mediante hardware, lo que implica unas mayores prestaciones.

A este fin ayuda, como hemos indicado anteriormente, el hecho de que los campos están alineados a 64 bits, lo que permite que las nuevas generaciones de procesadores y microcontroladores, de 64 bits, puedan procesar mucho más eficazmente la cabecera IPv6.

El valor del campo “siguiente cabecera”, indica cual es la siguiente cabecera y así sucesivamente. Las sucesivas cabeceras, no son examinadas en cada nodo de la ruta, sino sólo en el nodo o nodos destino finales. Hay una única excepción a esta regla: cuando el valor de este campo es cero, lo que indica opción de examinado y proceso “salto a salto” (hop-by-hop). Así tenemos, por citar algunos ejemplos, cabeceras con información de encaminado, fragmentación, opciones de destino, autenticación, encriptación, etc., que en cualquier caso, deben de ser procesadas en el orden riguroso en que aparecen en el paquete.

Sin entrar en más detalles, véanse a continuación los siguientes ejemplos gráficos del uso del concepto de las “cabeceras de extensión” (definidas por el campo “siguiente cabecera”), mecanismo por el que cada cabecera es “encadenada” a la siguiente y anterior (en caso de existir):

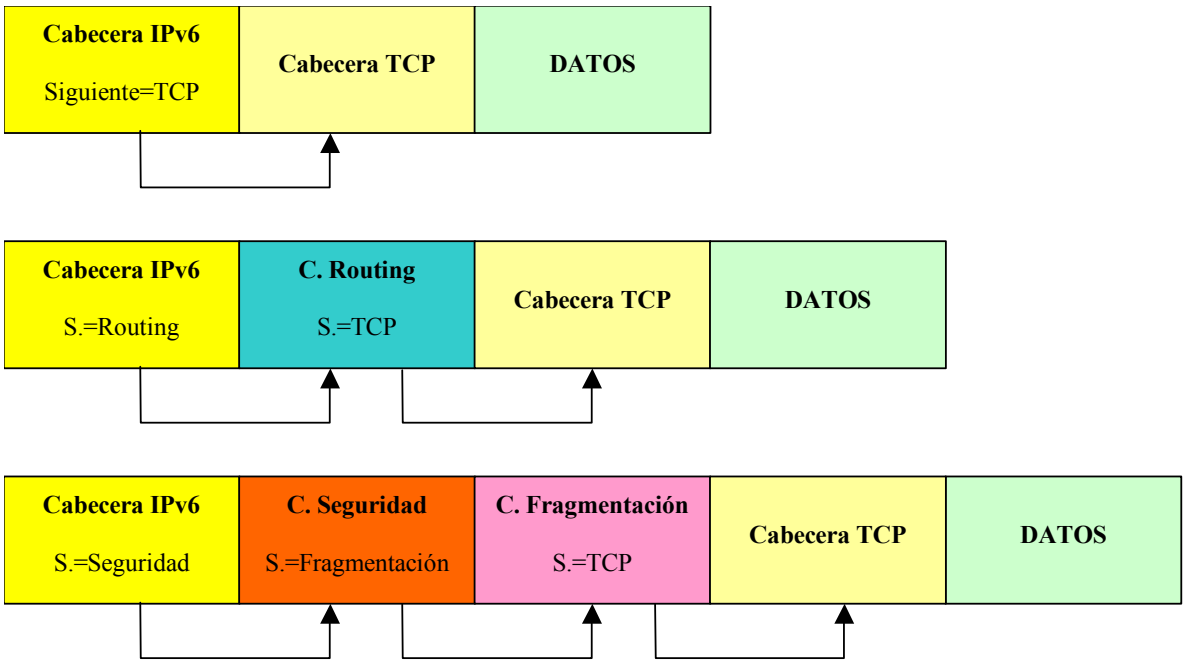

Figura 2-4: Extensiones en IPv6

El MTU (Unidad Máxima de Transmisión), debe de ser como mínimo, de 1.280 bytes, aunque se recomiendan tamaños superiores a 1.500 bytes. Los nodos descubren el valor MTU a través de la inspección de la ruta[4]. Se prevé así una optimización de los paquetes y del número de cabeceras, dado el continuo crecimiento de los anchos de banda disponibles, así como del incremento del propio tráfico.

Dado que IPv6 no realiza verificación de errores de la cabecera, en tráfico UDP, se requiere el empleo del su propio mecanismo de checksum.

[4] *RFC1981 - Path MTU Discovery for IP version 6*

3) Direccionamiento en IPv6

3.1. Definición de dirección IPv6

Como hemos comentado anteriormente, las direcciones IPv6[5] son identificadores de 128bits de longitud. Identifican interfaces de red (ya sea de forma individual o grupos de interfaces). A una misma interfaces de un nodo se le pueden asignar múltiples direcciones IPv6. Dichas direcciones se clasifican en tres tipos:

- *Unicast*: Identificador para una única interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección. Es el equivalente a las direcciones IPv4 actuales.
- *Anycast*: Identificador para un conjunto de interfaces (típicamente pertenecen a diferentes nodos). Un paquete enviado a una dirección anycast es entregado en una (cualquiera) de las interfaces identificadas con dicha dirección (la que este más "cerca"). Nos permite crear, por ejemplo, ámbitos de redundancia, de forma que varias máquinas puedan ocuparse del mismo tráfico según una secuencia determinada (por el routing), si la primera "cae".
- *Multicast*: Identificador para un conjunto de interfaces (por lo general pertenecientes a diferentes nodos). Un paquete enviado a una dirección multicast es entregado a todas las interfaces identificadas por dicha dirección. La misión de este tipo de paquetes es evidente: aplicaciones de retransmisión múltiple (broadcast).

3.2. Direcciones Unicast IPv6

3.2.1. Direcciones Unicast IPv6 Globales

Las direcciones unicast, son agregables con máscaras de bits contiguos, similares al caso de IPv4, con CIDR (Class-less Interdomain Routing). Como hemos visto, hay varias formas de asignación de direcciones unicast, y otras pueden ser definidas en el futuro.

Los nodos IPv6 pueden no tener ningún conocimiento o mínimo de la estructura interna de las direcciones IPv6, dependiendo de su misión en la red (por ejemplo, host frente a router). Pero como mínimo, un nodo debe considerar que las direcciones unicast (incluyendo la propia), no tienen estructura:

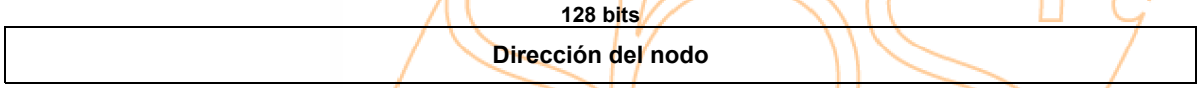

Figura 3-1: Estructura de dirección IPv6

Un host algo más sofisticado, conocería el prefijo de la subred del enlace al que esta conectado:

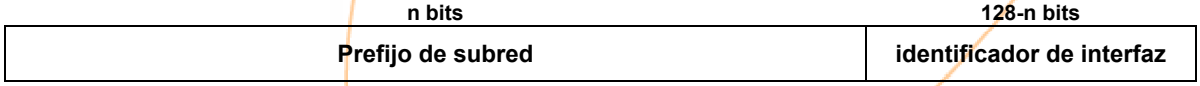

Figura 3-2: Prefijos de subred

Dispositivos más sofisticados pueden tener un conocimiento más amplio de la jerarquía de la red, sus límites, etc., en ocasiones dependiendo de la posición misma que el dispositivo o host/router, ocupa en la propia red.

[5] *RFC2373 - IP Version 6 Addressing Architecture*

El “identificador de interfaz” se emplea, por tanto, para identificar interfaces en un enlace, y deben de ser únicos en dicho enlace. En muchos casos también serán únicos en un ámbito más amplio. Por lo general, el identificador de interfaz coincidirá con la dirección de la capa de enlace de dicha interfaz. El mismo identificador de interfaz puede ser empleado en múltiples interfaces del mismo nodo, sin afectar a su exclusividad global en el ámbito IPv6.

3.2.2. Direcciones Unicast Locales de Enlace (Link-Local)

Las direcciones locales de enlace han sido diseñadas para direccionar un único enlace para propósitos de auto-configuración (mediante identificadores de interfaz), descubrimiento del vecindario, o situaciones en las que no hay routers. Por tanto, los encaminadores no pueden retransmitir ningún paquete con direcciones fuente o destino que sean locales de enlace (su ámbito esta limitado a la red local). Tienen el siguiente formato:

10 bits	54 bits	64 bits
1111111010	**0**	**Identificador de interfaz**

Figura 3-3: Tabla 3 - Estructura direcciones locales de enlace

Se trata de direcciones FE80::<ID de interfaz>/10.

3.3. Direcciones Anycast IPv6

Una dirección anycast identifica múltiples interfaces. Con una topología de encaminadotes adecuada, los paquetes destinados a una dirección anycast se entregarán a una sola interfaz (la que este más “cerca”, dentro del grupo de direcciones anycast). Si una dirección multicast define una comunicación “uno” a “muchos”, una dirección anycast se define como “uno” a “uno-entre-muchos”.

Para que los paquetes se entreguen a la dirección anycast más “cercana”, el “routing” de la red debe conocer qué interfaz tienen asignada una dirección anycast y sus distancias (en términos de “routing”).

Las direcciones anycast no tienen un espacio propio dentro del direccionamiento IPv6, utilizan el mismo espacio que las direcciones unicast (es decir, no podemos diferenciar entre direcciones unicast y anycast). El ámbito de las direcciones anycast se equipara con el unicast, así pues, pueden existir direcciones anycast de ámbito de sitio, de enlace o global. También remarcar, que este tipo de direcciones solo pueden usarse como dirección de destino, jamás como fuente.

Existe una dirección anycast, requerida para cada subred, que se denomina “dirección anycast del router de la subred”[6] (subnet-router anycast address). Su sintaxis es equivalente al prefijo que especifica el enlace correspondiente de la dirección unicast, siendo el indicador de interfaz igual a cero:

n bits	128-n bits
Prefijo de subred	**0**

Figura 3-4: Tabla 4 - Dirección anycast del router de la subred

Todos los routers han de soportar esta dirección para las subredes a las que están conectados. Los paquetes enviados a la “dirección anycast del router de la subred”, serán enviados a un router de la subred.

La utilidad de estas direcciones es para implementar los siguientes mecanismos:

[6] *RFC2526 - Reserved IPv6 Subnet Anycast Addresses*

- Comunicación con el servidor más “cercano”: Estas direcciones permiten que un cliente pueda comunicarse con un servidor de entre un grupo, y que la red le seleccione el que sea más cercano.
- Descubrimiento de Servicios: Al configurar un nodo con IPv6, no haría falta especificarle la dirección del servidor DNS, Proxy etc.. Podría existir una dirección anycast que identificara a esos servicios.
- Movilidad: Nodos que tienen que comunicarse con un router, del conjunto disponible en su red.

3.4. Direcciones Multicast IPv6

Una dirección multicast en IPv6, puede definirse como un identificador para un grupo de nodos. Un nodo puede pertenecer a uno o varios grupos multicast.

Las direcciones multicast[7] tienen el siguiente formato:

8	4	4	112 bits
11111111	**000T**	**ámbito**	**Identificador de Grupo**

Figura 3-5: Formato direcciones multicast

Los primeros 8 bits indican que se trata de una dirección multicast, el bit “T” indica:

- “T” = 0 ➔ Indica una dirección permanente, asignada por la autoridad de numeración global de Internet.
- “T” = 1 ➔ Indica una dirección temporal.

Los bits “ámbito” tienen los siguientes significados:

0	**Reservado**
1	**Ambito Local de Nodo**
2	**Ambito Local de Enlace**
3	**No asignado**
4	**No asignado**
5	**Ambito Local de Sitio**
6	**No asignado**
7	**No asignado**
8	**Ambito Local de Organización**
9	**No asignado**
A	**No asignado**
B	**No asignado**
C	**No asignado**
D	**No asignado**
E	**Ambito Global**
F	**Reservado**

Figura 3-6: Significado bits de ámbito en Multicast

[7] *RFC2375 - IPv6 Multicast Address Assignments*

El “Identificador de Grupo”, identifica, como cabe esperar, el grupo de multicast concreto al que nos referimos, bien sea permanente o temporal, dentro de un determinado ámbito.

Por ejemplo, si asignamos una dirección multicast permanente, con el identificador de grupo 101 (hexadecimal), al grupo de los servidores de tiempo (NTS), entonces:

- FF01::101 significa todos los NTS en el mismo nodo que el paquete origen
- FF02::101 significa todos los NTS en el mismo enlace que el paquete origen
- FF05::101 significa todos los NTS en el mismo sitio que el paquete origen
- FF0E::101 significa todos los NTS en Internet

3.5. Representación de direcciones IPv6

La representación de las direcciones IPv6 sigue el siguiente esquema:

```
x:x:x:x:x:x:x:x
```

Figura 3-7: Representación de direcciones IPv6

Donde “x” es un valor hexadecimal de 16 bits, de la porción correspondiente a la dirección IPv6. No es preciso escribir los ceros a la izquierda de cada campo.

Ejemplos:

```
FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
1080:0:0:0:8:800:200C:417A
```

Figura 3-8: Ejemplos de direcciones IPv6

Dado que, por el direccionamiento que se ha definido, podrán existir largas cadenas de bits “cero”, se permite la escritura de su abreviación, mediante el uso de “::”, que representa múltiples grupos consecutivos de 16 bits “cero”. Este símbolo sólo puede aparecer una vez en la dirección IPv6. Ejemplos, las direcciones:

```
1080:0:0:0:8:800:200C:417A (una dirección unicast)
FF01:0:0:0:0:0:0:101 (una dirección multicast)
0:0:0:0:0:0:0:1 (la dirección loopback)
0:0:0:0:0:0:0:0 (dirección no especificada)
```

Figura 3-9: Ejemplos de direcciones IPv6

Pueden representarse como:

```
1080::8:800:200C:417A (una dirección unicast)
FF01::101 (una dirección multicast)
::1 (la dirección loopback)
:: (dirección no especificada)
```

Figura 3-10: Direcciones representadas en formato abreviado

La representación de los prefijos IPv6 se realiza del siguiente modo:

```
dirección-IPv6/longitud-del-prefijo
```

Figura 3-11: Representación de prefijos IPv6

Donde:

- dirección-IPv6 = una dirección IPv6 en cualquiera de las notaciones válidas
- longitud-del-prefijo = valor decimal indicando cuantos bits contiguos de la parte izquierda de la dirección componen el prefijo

Por ejemplo, las representaciones válidas del prefijo de 60 bits 12AB00000000CD3, son:

```
12AB:0000:0000:CD30:0000:0000:0000:0000/60
12AB::CD30:0:0:0:0/60
12AB:0:0:CD30::/60
```

Figura 3-12: Representaciones con prefijos

Por tanto, para escribir una dirección completa, indicando la subred, podríamos hacerlo como:

```
12AB:0:0:CD30:123:4567:89AB:CDEF/60
```

Figura 3-13: Ejemplo dirección completa

4) Autoconfiguración en IPv6

4.1. Introducción

La autoconfiguración es el conjunto de pasos por los cuales un host decide como autoconfigurar sus interfaces en IPv6. Este mecanismo es el que nos permite afirmar que IPv6 es "Plug & Play".

El proceso incluye la creación de una dirección de enlace local, verificación de que no esta duplicada en dicho enlace y determinación de la información que ha de ser autoconfigurada (direcciones y otra información).

Las direcciones pueden obtenerse de forma totalmente manual, mediante DHCPv6 (stateful o configuración predeterminada), o de forma automática (stateless o descubrimiento automático, sin intervención).

Este protocolo define el proceso de generar una dirección de enlace local, direcciones globales y locales de sitio, mediante el procedimiento automático (stateless). También define el mecanismo para detectar direcciones duplicadas.

La autoconfiguración "stateless" (sin intervención), no requiere ninguna configuración manual del host, configuración mínima (o ninguna) de routers, y no precisa servidores adicionales. Permite a un host generar su propia dirección mediante una combinación de información disponible localmente e información anunciada por los routers. Los routers anuncian los prefijos que identifican la subred (o subredes) asociadas con el enlace, mientras el host genera un "identificador de interfaz", que identifica de forma única la interfaz en la subred. La dirección se compone por la combinación de ambos campos. En ausencia de router, el host sólo puede generar la dirección de enlace local, aunque esto es suficiente para permitir la comunicación entre nodos conectados al mismo enlace.

En la autoconfiguración "stateful" (predeterminada), el host obtiene la dirección de la interfaz y/o la información y parámetros de configuración desde un servidor. Los servidores mantienen una base de datos con las direcciones que han sido asignadas a cada host.

Ambos tipos de autoconfiguración (stateless y stateful), se complementan. Un host puede usar autoconfiguración sin intervención (stateless), para generar su propia dirección, y obtener el resto de parámetros mediante autoconfiguración predeterminada (stateful).

El mecanismo de autoconfiguración "sin intervención" se emplea cuando no importa la dirección exacta que se asigna a un host, sino tan sólo asegurarse que es única y correctamente enrutable.

El mecanismo de autoconfiguración predeterminada, por el contrario, nos asegura que cada host tiene una determinada dirección, asignada manualmente.

La autoconfiguración esta diseñada para hosts, no para routers, aunque ello no implica que parte de la configuración de los routers también pueda ser realizada automáticamente (generación de direcciones de enlace local). Además, los routers también tienen que "aprobar" el algoritmo de detección de direcciones duplicadas.

4.2. Stateless Autoconfiguration

El procedimiento de autoconfiguración stateless[8] (sin intervención o descubrimiento automático), ha sido diseñado con las siguientes premisas:

[8] *RFC2462 - IPv6 Stateless Address Autoconfiguration*

- Evitar la configuración manual de dispositivos antes de su conexión a la red. Se requiere, en consecuencia, un mecanismo que permita a los host obtener o crear direcciones únicas para cada una de sus interfaces, asumiendo que cada interfaz puede proporcionar un identificador único para si misma (identificador de interfaz). En el caso más simple, el identificador de interfaz consiste en la dirección de la capa de enlace, de dicha interfaz. El identificador de interfaz puede ser combinado con un prefijo, para formar la dirección.
- Las pequeñas redes o sitios, con máquinas conectadas a un único enlace, no deberían requerir la presencia de un servidor "stateful" o router, como requisito para comunicarse. Para obtener, en este caso, características "plug & play", empleamos las direcciones de enlace local, dado que tienen un prefijo perfectamente conocido que identifica el único enlace compartido, al que se conectan todos los nodos. Cada dispositivo forma su dirección de enlace local anteponiendo el prefijo de enlace local a su identificador de interfaz.
- En el caso de redes o sitios grandes, con múltiples subredes y routers, tampoco se requiere la presencia de un servidor de configuración de direcciones "stateful", ya que los host han de determinar, para generar sus direcciones globales o de enlace local, los prefijos que identifican las subredes a las que se conectan. Los routers generan mensajes periódicos de anunciación, que incluyen opciones como listas de prefijos activos en los enlaces.
- La configuración de direcciones debe de facilitar la renumeración de los dispositivos de un sitio, por ejemplo, cuando se desea cambiar de pro-veedor de servicios. La renumeración se logra al permitir que una misma interfaz pueda tener varias direcciones, que recibe "en préstamo". El tiempo del "préstamo" es el mecanismo por el que se renuevan las direcciones, al expirar los plazos para las viejas, sin que se conceda una prórroga. Al poder disponer de varias direcciones simultáneamente, permite que la transición no sea "disruptora", permitiendo que ambas, la vieja y la nueva dirección den continuidad a la comunicación durante el período de transición.
- Sólo es posible utilizar este mecanismo en enlaces capaces de funciones multicast, y comienza, por tanto, cuando es iniciada o activada una interfaz que permite multicast.
- Los administradores de sistemas necesitan la habilidad de especificar que mecanismo (stateless, stateful, o ambos), deben ser usados. Los mensajes de anunciación de los routers incluyen indicadores para esta función.

Los pasos básicos para la autoconfiguración, una vez la interfaz ha sido activada, serían:

Se genera la dirección "tentativa" de enlace local, como se ha descrito antes.

1. Verificar que dicha dirección "tentativa" puede ser asignada (no esta duplicada en el mismo enlace).
2. Si esta duplicada, la autoconfiguración se detiene, y se requiere un procedimiento manual (por ejemplo, usando otro identificador de interfaz).
3. Si no esta duplicada, la conectividad a nivel IP se ha logrado, al asignarse definitivamente dicha dirección "tentativa" a la interfaz en cuestión.
4. Si se trata de un host, se interroga a los posibles routers para indicar al host lo que debe de hacer a continuación.
5. Si no hay routers, se invoca el procedimiento de autoconfiguración "stateful".
6. Si hay routers, estos contestarán indicando fundamentalmente, como obtener las direcciones si se ha de utilizar el mecanismo "stateful", u otra información, como tiempos de vida, etc.

Hay algunos detractores de este mecanismo, ya que implica que cualquier nodo puede ser identificado en una determinada red si se conoce su identificador IEEE (dirección MAC). Por ello, para permitir que la dirección no sea estática y por tanto facilitar la privacidad, se implementan extensiones de privacidad[9].

[9] *RFC3041 - Privacy Extensions for Stateless Address Autoconfiguration in IPv6*

4.3. Statefull Autoconfiguration

DHCP para IPv6 es un protocolo UDP cliente/servidor, diseñado para reducir el coste de gestión de nodos IPv6 en entornos donde los administradores precisan un control sobre la asignación de los recursos de la red, superior al facilita-dos por el mecanismo de configuración "stateless".

Como ya hemos indicado, ambos mecanismos pueden usarse de forma concurrente para reducir el coste de propiedad y administración de la red.

Para lograr este objetivo, se centraliza la gestión de los recursos de la red, tales como direcciones IP, información de encaminado, información de instalación de Sistemas Operativos, información de servicios de directorios, sobre uno o varios servidores DHCP, en lugar de distribuir dicha información en ficheros de con-figuración locales en cada nodo.

Además, DHCP ha sido diseñado para ser fácilmente extensible con nuevos parámetros de configuración, a través de "extensiones" que incorporan esta nueva información. Al respecto es fundamental el documento dhc-v6exts-12.txt.

Los objetivos de DHCPv6 son:

- DHCP es un mecanismo, no una política. La política es establecida por el administrador de la red y DHCP le permite propagar los parámetros adecuados, según dicha política.
- DHCP es compatible, lógicamente, con el mecanismo de autoconfiguración "stateless".
- DHCP no requiere configuración manual de parámetros de red en clientes DHCP, excepto en casos donde dicha configuración se requiere debido a medidas de seguridad.
- DHCP no requiere un servidor en cada enlace, dado que debe funcionar a través de reles DHCP.
- DHCP coexiste con nodos configurados estáticamente, así como con implementaciones existentes en la red.
- Los clientes DHCP pueden operar en enlaces donde no hay routers IPv6.
- Los clientes DHCP proporcionan la habilidad de renumerar la red.
- Un cliente DHCP puede hacer múltiples y diferentes peticiones de parámetros de configuración, de uno o varios servidores DHCP simultáneamente. DHCP proporciona suficiente información para permitir a los servidores DHCP el seguimiento del estado de configuración de los clientes.
- DHCP incorpora los mecanismos apropiados de control de tiempo y retransmisiones para operar eficazmente en entornos con una alta latencia y/o reducido ancho de banda.

Los cambios fundamentales entre DHCPv4 y DHCPv6, están basados en el soporte inherente del formato de direccionamiento y autoconfiguación IPv6; son las siguientes:

- La dirección de enlace local permite a un nodo tener una dirección tan pronto como arranca, lo que significa que todos los clientes tienen una dirección IP fuente para localizar un servidor o rele en su mismo enlace.
- Los indicadores de compatibilidad BOOTP y broadcast han desaparecido.
- El multicast y los ámbitos de direccionamiento permiten el diseño de paquetes de descubrimiento, que definen por si mismos su rango por la dirección multicast, para la función requerida.
- La autoconfiguración stateful ha de coexistir e integrarse con la stateless, soportando la detección de direcciones duplicadas y los dos tiempos de vida de IPv6, para facilitar la renumeración automática de direcciones y su gestión.
- Se soportan múltiples direcciones por cada interfaz.

Algunas opciones DHCPv4 ya no son precisas, debido a que los parámetros de configuración se obtienen a través de ND o del protocolo de localización de servicios[10].

- De esta forma, se soportan las siguientes funciones nuevas:
- Configuración de actualizaciones dinámicas de DNS.
- Desaprobación de direcciones, para renumeración dinámica.
- Reles preconfigurados con direcciones de servidores, o mediante multicast.
- Autenticación.
- Los clientes pueden pedir múltiples direcciones IP.
- Las direcciones pueden ser reclamadas mediante el mensaje de "iniciar-reconfiguración".
- Integración entre autoconfiguración de direcciones "stateless" y "stateful"
- Permitir reles para localizar servidores fuera del enlace.

[10] *RFC2165 - Service Location Protocol*