Con la evolución de la versión actual de IP, la versión 4 (IPv4), se ha hecho cada vez más evidente el agotamiento del espacio de direcciones. Aunque mecanismos como el Enrutamiento entre dominios sin clase, CIDR (Classless Inter-Domain Routing), y el uso de proxy ha servido para aumentar la longevidad de IPv4, se acometió el desarrollo de una versión mayor, más flexible: IP versión 6 (IPv6).

En su concepción original, Internet (entonces ARPANET) se diseñó principalmente para facilitar la comunicación entre entidades de investigación y organizaciones militares. Sin embargo, la extraordinaria longevidad y funcionalidad de la familia de protocolos de TCP/IP ha permitido que Internet se convierta en un mecanismo de comunicación de una amplitud que no se podría haber previsto en sus inicios.

En este momento existen nuevos campos que requieren capacidades de enrutamiento y direccionamiento como el que proporciona IP. Los teléfonos celulares, mensáfonos y los asistentes personales (PDA) se han convertido en accesorios ubicuos cuya naturaleza dicta los mecanismos para disponer de comunicaciones portables y seguras. Los medios de entretenimiento como la televisión digital y el audio en tiempo real requiere conectividad similar con el imperativo de velocidades de envío garantizadas. Además, un área sin cubrir durante mucho tiempo como la administración de alimentación y dispositivos demandan capacidades similares. La otrora fantástica «casa del futuro», con la temperatura, la luz y otros accesorios controlados electrónicamente, está acercándose a la realidad.

En todas estas áreas se utilizará IP en lugar de forzar el desarrollo de soluciones propietarias y requerirán mecanismos que no proporciona fácilmente IPv4. En lugar de investigar métodos para extender el espacio de direcciones ya limitado con un potencial futuro limitado, la investigación se ha dedicado a buscar una nueva versión de IP, IPv6. Para conseguir cubrir las demandas actuales y futuras, las capacidades clave que debe tener en cuenta el desarrollo de esta nueva versión de IP son:

- En primer lugar, cualquier nueva versión de IP debe ser capaz de coexistir e interoperar con las especificaciones actuales de IP. Los intentos de una conversión desde una versión hasta la siguiente serían irreales y caóticos. Por tanto, IPv6 debe disponer de mecanismos para la comunicación tanto con hosts con IPv6 como con hosts con IPv4.
- IPv6 debe admitir un espacio de direccionamiento exponencialmente mayor que IPv4.
- Los paquetes de IPv6 deben ser lo más ligeros posibles para facilitar la transmisión de IPv6 por distintos medios.
- Se debe incorporar a IPv6 la Calidad de servicio, QoS (Quality of Service), es decir, la capacidad de asignar prioridad y ancho de banda al tráfico y acomodar la funcionalidad que requieren las aplicaciones con baja latencia.
- Las capacidades de enrutamiento de IPv6 se deben diseñar para que se puedan especificar nodos intermedios de una ruta en los propios paquetes, de forma similar a las opciones Registro de ruta y Enrutamiento fuente débil de IPv4.
- Los mecanismos de transmisión segura de datos deben ser inherentes a la estructura de IPv6.

Con la perspectiva de las necesidades futuras y conscientes de temas pasados, el grupo de trabajo de IPv6 del IETF continúa trabajando en el desarrollo de una solución.

Introducción a IPv6

Como se describe en la RFC 2460, IPv6 es el sustituto de IPv4. Aumenta el tamaño de las direcciones de IP de 32 a 128 bits, lo que permite 2^{96} (2^{128-32}) veces el número de direcciones de IPv4. Es un total de 340.282.366.920.938.463.463.374.607.431.768.211.456 direcciones. Este aumento en el espacio de direcciones no sólo proporciona mayor número de hosts, sino una

jerarquía de direcciones mayor.

Se han mejorado las cabeceras de los paquetes, eliminando algunos campos de la cabecera de IPv4, haciendo que otros sean opcionales y utilizando cabeceras de extensión. Las cabeceras de extensión con cabeceras separadas que, con una excepción, no las examina ningún host en la ruta desde el origen hasta el destino, mejorando la eficiencia del enrutamiento. Además, permite una mayor flexibilidad en la codificación de opciones y capacidades de expansión para opciones futuras.

En IPv6 se introduce el etiquetado de flujos, lo que permite indicar que los paquetes pertenecen a determinado «flujo» de tráfico, de esta forma se permite manejar QoS y la administración de ancho de banda sin tener que analizar cabeceras de TCP ni de UDP. También se han introducido extensiones que permiten autenticación, asegurar la integridad de los datos y cifrado de paquetes opcional.

IPv6 incluye una terminología básica nueva:

- **Nodos:** Un nodo es cualquier dispositivo con IPv6.
- **Enrutador:** Es un dispositivo que reenvía paquetes que no están directamente dirigidos a él.
- **Host:** Es un nodo que no reenvía paquetes.
- **Interfaz:** Una interfaz es la conexión con un medio de transmisión por la que se envían los paquetes de IPv6. Aunque se realice una distinción entre enrutadores y hosts, es posible, aunque poco probable, que un único nodo tenga varias interfaces y, potencialmente, reenvíe paquetes a direcciones de otros nodos o solamente a un subconjunto de sus interfaces. Es decir, este dispositivo actuaría como un host (en las interfaces que no reenvía) y como un enrutador (en las interfaces que reenvía).
- **Enlace:** Un enlace es el medio por el que se transporta IPv6.
- **Vecinos:** Los vecinos son nodos que están conectados al mismo enlace.
- **MTU del enlace:** Una unidad máxima de transmisión, MTU (Maximum Transmission Unit) de un enlace es el tamaño máximo de paquete que se puede transportar por el medio del enlace, y se expresa en bytes.
- **Dirección del Nivel de enlace:** La dirección del Nivel de enlace es la dirección «física» de una interfaz, como la dirección de control de acceso al medio (MAC) en los enlaces Ethernet. En IPv6 todo el direccionamiento es a interfaces, no a los nodos.
- **Dirección unicast:** Una dirección unicast especifica que un paquete se debe enviar a una interfaz concreta.
- **Dirección multidifusión:** Una dirección de multidifusión se envía a un conjunto de interfaces, normalmente en varios nodos.
- **Dirección anycast:** Una dirección anycast, aunque identifica a varias interfaces, y normalmente a múltiples nodos, se envía sólo a la interfaz que es la más «cercana» al origen.

Direccionamiento

Representación textual de las direcciones de IPv6

Quizá la diferencia más obvia entre IPv4 a IPv6 sea el aumento del número de bits para el direccionamiento. En lugar de usar la notación decimal con puntos de 32 bits, IPv6 usa direccionamiento de 128 bits expresados en formato hexadecimal. La representación textual de estas direcciones puede variar, con las siguientes tres representaciones aceptadas:

- En la representación textual preferida, las direcciones son ocho secciones hexadecimales de 16 bits, separadas por dos puntos. Por ejemplo, una dirección de IPv6 para una interfaz

podría ser como:
ABCD:EF12:3456:7890:ABCD:EF12:3456:7890
Cualquier campo que contenga ceros delante no necesita presentarlos, aunque no se pueden dejar campos en blanco. Por ejemplo:
1234:0:0:0:ABCD:123:45:6

- Debido al mecanismo de asignación de direcciones de IPv6, serán comunes las cadenas de ceros. En consecuencia, una representación alternativa permite usar «::» para representar una parte de la dirección con bits a cero. El sustituto «::» se puede usar para representar más de una sección de bits a cero, pero no se puede utilizar más de una vez en una dirección. Por ejemplo:
1234:0:0:0:ABCD:0:0:123
se representaría como:
1234::ABCD:0:0:123
ó
1234:0:0:0:ABCD::123
pero no como
1234::ABCD::123

- El tercer método de representación textual de las direcciones se usa en un entorno con mezcla de nodos con IPv4 y con IPv6. En esta notación, las seis secciones de 16 bits de mayor orden (las de la izquierda) se muestran en hexadecimal, pero el resto se muestra en la familiar notación decimal con puntos. Por ejemplo, una dirección podría aparecer en cualquiera de estos formatos:
0:0:0:0:0:0:131.107.6.100 ó
::131.107.6.100 (formato comprimido)
0:0:0:0:0:FFFF:131.107.4.99 ó
::FFFF:131.107.4.99 (formato comprimido)
ABCD:EF:12:34:0:0:131.107.2.98 ó
ABCD:EF:12:34::131.107.2.98 (formato comprimido)

Direcciones unicast

Un campo de longitud variable de bits, denominado Prefijo de formato, FP (Format Prefix), permite identificar el tipo de dirección de IPv6. Un valor de 11111111 (FF) para el FP identifica una dirección como dirección de multidifusión. Cualquier otro valor en los bits de mayor orden identifica la dirección como dirección unicast. Las direcciones unicast se refieren a un único nodo de un enlace; sin embargo una única dirección unicast puede estar asignada a múltiples interfaces de dicho nodo, siempre que las interfaces aparezcan a los protocolos de nivel superior como una única entidad. Las direcciones unicast pueden ser de varios tipos, entre ellos direcciones unicast globales agregables, del enlace local, del sitio local y direcciones de IPv6 con direcciones IPv4 insertadas.

Direcciones unicast reservadas

En la actualidad, en la RFC 2373 se definen dos direcciones unicast reservadas especializadas. La primera es la dirección no específica. Esta dirección es la 0:0:0:0:0:0:0:0, ó :: en formato comprimido, no se puede asignar a ningún nodo ni se puede usar como dirección de origen en los paquetes de IPv6 ni en la cabeceras de los enrutadores. Normalmente se usa mientras los nodos inicializan IPv6 e indica que aún no han conseguido conocer su propia dirección. La segunda dirección unicast reservada es 0:0:0:0:0:0:0:1, ó ::1 en formato comprimido, es la dirección de retorno (loopback address), la que usa un nodo para enviarse paquetes a sí mismo, como la dirección de retorno 127.0.0.1 en IPv4.

Direcciones unicast globales agregables

En IPv4, bajo el Enrutamiento entre dominios sin clase, CIDR (Classless Inter-Domain Routing), los ISP, Proveedores de servicios de Internet, asignan direcciones en «pools» (bloques). Las direcciones unicast globales agregables de IPv6 funcionan de forma similar, y se usarán para la comunicación global en la parte activa con IPv6 de Internet. El formato de una dirección unicast global agregable, es:

FP	TLA ID	RES	NLA ID	SLA ID	ID de la interfaz
001	13 bits	8 bits	24 bits	16 bits	64 bits
Topología pública				Topología del sitio	Identificador de interfaz

Antes de describir la estructura interna de una dirección unicast global agregable es importante entender la estructura global de estas direcciones. Una dirección agregable se organiza en una estructura jerárquica en tres capas. El nivel superior de la jerarquía será la Topología pública, o la parte del espacio de direcciones que administra las entidades que proporcionan los servicios públicos de Internet. La Topología pública proporciona un mecanismo para lo que se refiere como proveedores de tránsito de gran ámbito y de conmutación pública para proporcionar agregados, o colecciones, de direcciones. Estos proveedores son responsables de proporcionar el enrutamiento que exista fuera de la estructura corporativa interna de la organización.

Como las organizaciones mantienen topologías de enrutamiento internas, una porción de una dirección agregable se utiliza para el enrutamiento interno. Es la parte Topología del sitio de la dirección, y representa los bits que identifican las rutas de enrutamiento interno. Una de las ventajas de esta idea en tres niveles para la asignación de direcciones es que si una compañía cambia el tránsito de los proveedores de tránsito de gran ámbito o usa varios proveedores, dicha compañía no necesita obtener una reasignación de las direcciones de Topología del sitio.

El identificador de interfaz de una dirección agregable es la parte que identifica las interfaces individuales de los enlaces físicos de la organización. De forma similar a como las direcciones de IPv4 usan los ID de red y los ID de host, en las direcciones de IPv6 se usan los identificadores de Interfaz y de sitio.

Estructura de una dirección unicast global agregable			
Abreviatura	**Campo**	**Tamaño**	**Descripción**
FP	Prefijo de formato (Format Prefix)	3 bits	«001» indica que es una dirección unicast global agregable.
TLA ID	ID de agregación de nivel superior (Top-Level Aggregation)	13 bits	Los TLA serán los responsables del mantenimiento de los niveles superiores de la jerarquía pública de enrutamiento. Con 13 bits para estos ID se puede disponer de hasta 8.192 TLA.
RES	Reservado	8 bits	La reserva de estos bits permite la expansión de los campos TLA y NLA, según las necesidades futuras.
NLA ID	ID de agregación de	24 bits	Los NLA los usarán las organizaciones que tienen asignado

	siguiente nivel (Next-Level Aggregation)		un TLA para crear una jerarquía interna de direccionamiento y permitir a los proveedores de tránsito identificar los sitios a los que sirven. El uso de 24 bits para este identificador permite que cada TLA de servicio a unos 16 millones de sitios si se utiliza plano, o aproximadamente el equivalente de toda una dirección de IPv4 si se usa jerárquicamente.
SLA ID	ID de agregación del nivel del sitio (Site-Level Aggregation)	16 bits	Los SLA permiten que las organizaciones crean una estructura interna de enrutamiento independiente de las estructuras externas. Aproximadamente pueden dar cabida a unas 65.535 subredes internas con el uso de 16 bits para los SLA.
ID de interfaz	ID de interfaz	64 bits	Los ID de interfaz deben ser únicos en el enlace y, a menudo, suelen coincidir con la dirección del Nivel de enlace, y podría estar asignada a múltiples interfaces de un único nodo permitiendo de esta forma el balance de carga por muchas interfaces.

Direcciones unicast de uso local

Las direcciones unicast de uso local se usan para la comunicación dentro del mismo enlace. Se utilizan en enlaces en los que no existen enrutadores, o para tareas como la autoconfiguración de dirección (proceso por el que los nodos consiguen una dirección de IPv6) y el descubrimiento de vecindad (un método que se usa para encontrar otros nodos en un enlace.)

Formato de una dirección unicast de enlace local		
10 bits	54 bits	64 bits
11111110101	0	ID de interfaz

Las direcciones unicast locales al sitio, equivalentes a las direcciones privadas de IPv4 que se utilizan para el direccionamiento y comunicación dentro de una única organización privada no deben reenviarse fuera del sitio donde se usan.

Formato de una dirección unicast local al sitio			
10 bits	38 bits	16 bits	64 bits
11111110101	0	ID de subred	ID de interfaz

Direcciones de IPv6 con direcciones de IPv4 integradas

Para facilitar la transición desde IPv4 hasta IPv6, se han desarrollado mecanismos para crear túneles de paquetes de IPv6 sobre una infraestructura de IPv4. Uno de los mecanismos para la codificación de paquetes permite que los nodos lleven direcciones de IPv4 en los bits de menor orden de los paquetes de IPv6 que usan una dirección unicast especializada. A este tipo de paquete se le

denomina dirección de IPv6 compatible con IPv4 y lleva ceros en todos los campos del identificador de interfaz excepto en los 32 bits de IPv4 de menor orden. Un segundo tipo de paquete de transición consiste en permitir que los nodos especifiquen direcciones para los nodos que no usan IPv6 de ninguna forma y preceder los 32 bits de la dirección de IPv4 con «FFFF» para indicar qué es lo que se denomina una «dirección de IPv6 con correspondencia en IPv4».

Formato de direcciones IPv6 con direcciones IPv4 integradas		
80 bits	16 bits	32 bits
0000.....0000	0000 ó FFFF	Dirección de IPv4

Direcciones anycast

Las direcciones anycast son estructuralmente idénticas a otras direcciones de unicast y se asignan de un bloque (pool) de direcciones unicast disponibles en una organización. Sin embargo, en lugar de asignarlas a un único nodo, como las direcciones unicast, se asignan a un grupo de nodos, normalmente los enrutadores del sitio. Todos los enrutadores tienen la misma dirección y se configuran para que usen su dirección como una dirección anycast.

Cuando un nodo de origen desea enviar un paquete a esta dirección, usa un mecanismo de descubrimiento del nodo más cercano propietario de la dirección. Es decir, el nodo origen no necesita conocer que la dirección es una dirección anycast, y la comunicación ocurre sólo entre el nodo origen y el enrutador más cercano configurado con la dirección anycast.

Como se indica en las RFC 2373 y 2526, las direcciones anycast aún tienen algunas limitaciones según progresa la investigación. Por el momento, las direcciones anycast no se pueden utilizar como dirección de origen en ningún paquete de IPv6, y sólo la pueden utilizar los enrutadores, no los hosts. Además, se requiere que los enrutadores dispongan de direcciones anycast para todas las subredes a los que están conectados, para asegurar que un enrutador local recibirá el paquete enviado a una dirección anycast de dicha subred.

Direcciones de multidifusión (multicast)

Como se define en las RFC 2373 y 2375, las direcciones de multidifusión se usan para el tráfico de IPv6 de multidifusión y sustituyen a las direcciones de difusión en IPv6. Una dirección de multidifusión se asigna a un grupo de nodos, pero al contrario que las direcciones anycast, todos los nodos configurados con la dirección de multidifusión recibirán los paquetes enviados a dicha dirección. Un nodo puede pertenecer a más de un grupo de multidifusión; sin embargo, ningún nodo puede utilizar una dirección de multidifusión como dirección de origen en ningún paquete ni se puede utilizar en las cabeceras de enrutamiento.

Formato de una dirección IPv6 de multidifusión			
8 bits	4 bits	4 bits	112 bits
11111111	Ind.	Ámb.	ID de grupo

Por ejemplo, la siguiente dirección de multidifusión se usa para enviar paquetes a grupos de enrutadores:

- `FF01:0:0:0:0:0:0:2 Nodo local; todos los enrutadores.`

Esta dirección identifica todas las interfaces de enrutamiento de un único nodo.

- `FF02:0:0:0:0:0:0:2 Enlace local; todos los enrutadores.`

Esta dirección identifica todos los enrutadores de un enlace.

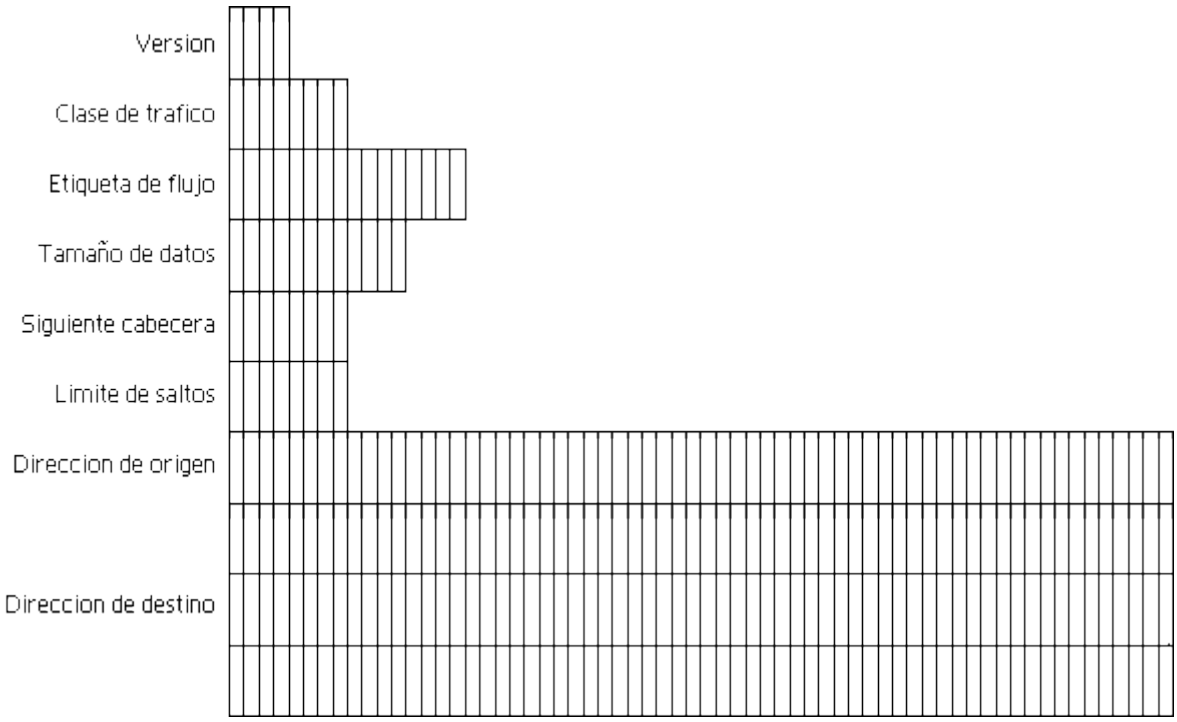
- `FF05:0:0:0:0:0:0:2 Sitio local; todos los enrutadores.`

Esta dirección identifica a todos los enrutadores de un sitio.

Campos de una dirección de multidifusión			
Abreviatura	**Campo**	**Tamaño**	**Descripción**
FP	Prefijo de formato	8 bits	«11111111» indica que es una dirección demultidifusión.
Ind.	Indicadores	4 bits	Los tres primeros bits del campo están reservados y deben estar a cero. Si el cuarto indicador es «0», significa una dirección de multidifusión asignada permanentemente; si es «1», esta dirección es «temporal», o no asignada por el Internet Assigned Numbers Authority (IANA).
Ámb.	Ámbito	4 bits	Los valores de ámbito limitan el ámbito de los grupos de multidifusión. Los valores «0» o «F» están reservados; «1» indica que es un ámbito de nodo local; «2» indica que es un ámbito de enlace local; «S» indica que el ámbito es de sitio local; «8» indica un ámbito de la organización; «E» indica un ámbito global; el resto de valores está sin asignar.
ID de grupo	ID de grupo	112 bits	Es un identificador único para el ID del grupo de multidifusión que aceptará paquetes enviados a esta dirección.

Formato de la cabecera de IPv6 y mecanismos de enrutamiento

La información de dirección en IPv6 comprende sólo una parte de la cabecera de un paquete. El resto de la cabecera contiene información necesaria pare que los nodos evalúen y procesen efectivamente cada paquete. El formato general de una cabecera de IPv6, es:



Campos de la cabecera de IPv6		
Campo	**Tamaño**	**Descripción**
Versión	4 bits	«0110» indica versión 6.
Clase de tráfico	8 bits	Se usa para identificar la «clase» de tráfico, o la prioridad, de forma que los paquetes se puedan reenviar con distintas prioridades para asegurar la QoS.
Etiqueta de flujo	20 bits	Los paquetes que pertenecen a un flujo de clase de tráfico concreto se etiquetan para identificar a qué «flujo» pertenecen.
Tamaño de los datos	16 bits	Tamaño, en bytes, del resto del paquete, incluyendo las cabeceras de extensión.
Siguiente cabecera	8 bits	Identifica el tipo de cabecera que sigue inmediatamente a la cabecera de IPv6. Usa los mismos valores que en el campo Protocolo de IPv4 (RFC 1700).
Límite de saltos	8 bits	Número de enlaces que puede atravesar un paquete antes de descartarlo. cada vez que se reenvía este campo se decrementa en 1.
Dirección de origen	128 bits	Dirección del nodo emisor.
Dirección de destino	128 bits	Dirección del nodo de destino, que puede ser un nodo final o un nodo intermedio.

A continuación de la cabecera de IPv6 puede haber una o más cabeceras de extensión, que se utilizan para incluir información adicional sobre el paquete, como información de enrutamiento, si el paquete se ha fragmentado y el siguiente salto de la ruta indicada por el emisor. A excepción de la cabecera denominada cabecera Opciones de salto a salto, ningún nodo en toda la ruta procesa estas cabeceras. Sólo el nodo de destino especificado en el paquete, ya sea un nodo de destino final o un

nodo de destino intermedio, debe evaluar y procesar todas las cabeceras de extensión. Las cabeceras de extensión tienen un tamaño múltiplo de 8 bytes para mantener el alineamiento del paquete y permitir que los nodos que no procesan las cabeceras de extensión las trasladen.

Los paquetes pueden incluir todas, algunas o ninguna de las cabeceras de extensión de IPv6, pero deberían al menos implementarlas en el orden en el que se relacionan. Cada cabecera de extensión no debería existir más de una vez en cada paquete, a excepción de la cabecera Opciones de destino, que se puede usar una vez para especificar opciones de IP y una segunda vez para especificar opciones de los niveles superiores. Todas las cabeceras de extensión, de todos los tipos, usan un campo siguiente cabecera, de 8 bits, que especifica el tipo de la siguiente cabecera a la actual. Si este campo contiene el valor «59», indica que no existen más cabeceras.

- **Cabecera Opciones salto a salto.** Todos los nodos de la ruta de envío deben examinar la cabecera Opciones salto a salto. Esta cabecera puede contener varias opciones, que se deben procesar en orden, donde se definen acciones que ocurren en los saltos intermedios en la ruta. El campo Siguiente cabecera identifica la cabecera que sigue a ésta, como se ha mencionado anteriormente. El campo tamaño de la cabecera de extensión especifica el tamaño de esta cabecera en bytes. El campo tipo de opción, de 8 bits, especifica la acción que debe tomar un nodo si no se reconocen las opciones del paquete. Como indica este identificador, el nodo puede descartar el paquete, saltar la opción y continuar con el resto de la cabecera o enviar un mensaje Tipo de opción no reconocida de ICMP a la dirección de origen.
- **Cabecera Opciones de destino.** La cabecera Opciones de destino es casi idéntica a la cabecera Opciones salto a salto, excepto que sólo se examina en el nodo de destino del paquete y no en los nodos intermedios de la ruta. El valor «60» en el campo siguiente cabecera de la cabecera anterior indica la presencia de la cabecera Opciones de destino. El resto de campos son idénticos a los de Opciones salto a salto.
- **Cabecera Enrutamiento.** En IPv6, un nodo de origen puede listar uno o más adiós (stop) en la ruta del paquete. La cabecera Enrutamiento no se examina hasta que el paquete alcanza el destino de la cabecera de IPv6. A continuación en el destino se examina la cabecera Enrutamiento, se procesa de acuerdo al algoritmo indicado en el campo Tipo de enrutamiento, y se usa el resultado para enviar el paquete a la dirección de siguiente destino especificada en el paquete. El campo de 8 bits Segmentos restantes indica el número de direcciones que quedan por visitar, y el campo de 32 bits Reservado se pone a cero y se ignora en la transmisión. Según se va enviando el paquete a cada nodo especificado en la cabecera de Enrutamiento, las direcciones visitadas se eliminan del paquete y se decrementa la cuenta de saltos, hasta que eventualmente el paquete llega a su destino final.
- **Cabecera Fragmentación.** IPv6 requiere una MTU de enlace mínima de 1.280 bytes; cualquier enlace que no admita esta especificación debe proporcionar mecanismos específicos del enlace para la fragmentación y reensamblado debajo del nivel IPv6. Si la MTU del enlace es de al menos 1.280 bytes, pero el paquete a enviar es muy grande para esta MTU, IPv6 proporciona sus propios mecanismos de fragmentación. En IPv6, el nodo de origen realiza la fragmentación, no los enrutadores. Sin embargo, la presencia de una cabecera Enrutamiento puede requerir que los nodos intermedios fragmenten el paquete como resultado de una MTU distinta en la ruta. Como cada uno de los saltos se convierte en nodo de origen según se envía el paquete a la siguiente dirección, al nodo sólo le interesa la MTU del enlace entre él mismo y el destino, en lugar de conocer la MTU de todos los enlaces de la red. El campo Desplazamiento de fragmentación determina el orden de reensamblado en el nodo de destino y a cada fragmento se le asigna un valor único en el campo Identificación para facilitar la retransmisión de paquetes perdidos. Un indicador M de valor «0» indica que éste es el último de los fragmentos y un valor de «1 » indica que existen más fragmentos a continuación.

- **Cabecera Autenticación.** La cabecera Autenticación se usa por sí misma o junto a las cabeceras Encapsulado de seguridad de los datos, ESP (Encapsulating Security Payload), para proporcionar verificación del origen de datos a integridad. Sin embargo, la cabecera Autenticación no proporciona cifrado de datos; en IPv6 es responsabilidad de ESP. Los formatos de las cabeceras de Autenticación y de ESP se describen en las RFC 2402 y 2406, y la seguridad en IP se describe en el Capítulo 20, «Seguridad en las comunicaciones de IP con Seguridad de IP (IPSec)». El campo tamaño de los datos, de 8 bits, de la cabecera Autenticación especifica el tamaño de la cabecera en palabras de 32 bits. El campo Reservado, de 16 bits, no se usa actualmente y se debe establecer a «0». El campo Índice de parámetros de seguridad, SPI (Security Paremeters Index), es un valor arbitrario de 32 bits. Junto con la dirección del nodo de destino y el protocolo de seguridad negociado entre ambos nodos, este valor identifica unívocamente la asociación de seguridad del paquete. El campo Número de secuencia se incrementa en 1 con cada paquete y no se permite que este contador dé la vuelta sin que los nodos emisor y receptor establezcan una nueva asociación de seguridad. El tamaño de los datos de autenticación es variable, pero debe ser un múltiplo de 32 bits y se rellena con lo necesario para cumplir con este requisito.
- **Mecanismos de transición.** Los mecanismos para la transición de IPv4 a IPv6 se definen en la RFC 1933. El objetivo principal del proceso de transición es la coexistencia de las dos versiones de los protocolos hasta que IPv4 desaparezca completamente en algún momento. Los planes de transición constan de dos categorías principales, la implementación de pilas duales y el túnel de IPv6 sobre IPv4.

Autoconfiguración en IPv6 (RFC2462)

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 a 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.

Cada dirección es cedida a una interfaz durante un tiempo predefinido (posiblemente infinito). Las direcciones tienen asociado un tiempo de vida, que indican durante cuanto tiempo esta vinculada dicha dirección a una determinada interfaz. Cuando el tiempo de vida expira, la vinculación se invalida y la dirección puede ser reasignada a otra interfaz en cualquier punto de Internet.

Para gestionar la expiración de los vínculos, una dirección pasa a través de dos fases diferentes mientras está asignada a una interfaz. Inicialmente, una dirección es "preferred" (preferida), lo que significa que su uso es arbitrario y no está restringido. Posteriormente, la dirección es "deprecated" (desaprobada), en anticipación a que el vínculo con su interfaz actual va a ser anulado.

Mientras esta en estado "desaprobado", su uso es desaconsejado, aunque no prohibido. Cualquier nueva comunicación (por ejemplo, una nueva conexión TCP), debe usar una dirección "preferida", siempre que sea posible.

Una dirección "desaprobada" debería ser usada tan solo por aquellas aplicaciones que ya la venían utilizando y alas que les es muy difícil cambiar a otra dirección sin interrupción del servicio.

Para asegurarse de que todas las direcciones configuradas son únicas, en un determinado enlace, los nodos ejecutan un algoritmo de detección de direcciones duplicadas, antes de asignarlas a una interfaz. Este algoritmo es ejecutado para todas las direcciones, independientemente de que hayan sido obtenidas mediante autoconfiguración stateless o stateful.

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.

Autoconfiguración Stateless

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

- 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 proveedor 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:

1. Se genera la dirección "tentativa" de enlace local.
2. Verificar que dicha dirección "tentativa" puede ser asignada (no esta duplicada en el mismo enlace).
3. Si esta duplicada, la autoconfiguración se detiene, y se requiere un procedimiento manual (por ejemplo, usando otro identificador de interfaz).
4. Si no esta duplicada, la conectividad a nivel IP se ha logrado, al asignarse definitivamente dicha dirección "tentativa" a la interfaz en cuestión.
5. Si se trata de un host, se interroga a los posibles routers para indicar al host lo que debe de hacer a continuación.
6. Si no hay routers, se invoca el procedimiento de autoconfiguración "stateful".
7. 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) y por ello ya se está trabajando para permitir que la dirección no sea estática.

Autoconfiguración Stateful - DHCPv6

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 facilitados por el mecanismo de configuración "stateless".

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 configuración 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.

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 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 relés DHCP.
- DHCP coexiste con nodos configurados estáticamente, así como con impiementaciones 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 relé 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 (RFC2165).

De esta forma, se soportan las siguientes funciones nuevas:

- Configuración de actualizaciones dinámicas de DNS.
- Desaprobación de direcciones, para renumeración dinámica.
- Relés 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 "iniciarreconfiguración".
- Integración entre autoconfiguración de direcciones "stateless" y "stateful"
- Permitir relés para localizar servidores fuera del enlace.

Renumeración

En los párrafos anteriores ya hemos descrito el mecanismo básico de renumeración, basado en el "préstamo" o alquiler de direcciones, en las fases de "preferida" y "desaprobada", y en el tiempo de vida de las mismas.

En cualquier caso, podemos describir el mecanismo de forma sencilla, como consistente en disminuir el tiempo de vida del prefijo en los paquetes de anunciación del router, de forma que las direcciones pasen a ser desaprobadas, frente a las nuevas, que pasan a ser preferidas.

Sin embargo, este mecanismo está básicamente diseñado para los host. En el caso de los routers, se trabaja en un nuevo documento "draft-ietf-ipngwgrouter-renum-10.txt", que permitirá mecanismos similares y más adecuados.

IPv6 sobre Ethernet (RFC2464)

Aunque ya han sido definidos protocolos para permitir el use de IPv6 sobre cualquier tipo de red o topología (Token Ring, FDDI, ATM, PPP, ...), como ejemplo mucho más habitual y básico, centraremos este apartado en Ethernet (CSMA/CD y tecnologías full-duplex basadas en ISO/IEC8802-3). Mas adelante, en este mismo documento, citaremos los protocolos adecuados para cada una de las otras tecnologías.

Los paquetes lPv6 se transmiten sobre tramas normalizadas Ethernet. La cabecera Ethernet contiene las direcciones fuente y destino Ethernet, y el código de tipo Ethernet con el valor hexadecimal 86DD.

El campo de datos contiene la cabecera IPv6 seguida por los propios datos, y probablemente algunos bytes para alineación/relleno, de forma que se alcance el tamaño mínimo de trama para el enlace Ethernet.

Formato de una dirección IPv6 sobre Ethernet		
48 bits	48 bits	16 bits
Dirección Ethernet Destino	Dirección Ethernet Fuente	1000011011011101 (86DD)

El tamaño máximo de la unidad de transmisión (MTU), para IPv6 sobre Ethernet, es de 1.500 bytes. Evidentemente, este puede ser reducido, manual o automáticamente (por los mensajes de anunciación de routers).

Para obtener el identificador de interfaz, de una interfaz Ethernet, para la autoconfiguración stateless, nos basamos en la dirección MAC de 48 bits (IEEE802). Tomamos los 3 primeros bytes (los de mayor orden), y les agregamos "FFFE" (hexadecimal), y a continuación, el resto de los bytes de la dirección MAC (3 bytes). El identificador así formado se denomina identificador EUI-64 (Identificador Global de 64 bits), según to define IEEE.

El identificador de interfaz se obtiene, a continuación, partiendo del EUI-64, complementando el bit U/L (Universal/Local). El bit U/L es el siguiente al de menor valor del primer byte del EUI-64 (el 2° bit por la derecha, el 2° bit de menor peso). AI complementar este bit, por to general cambiará su valor de 0 a 1; dado que se espera que la dirección MAC sea universalmente única, U/L tendrá un valor 0, y por tanto se convertirá en 1 en el identificador de interfaz IPv6.

Una dirección MAC configurada manualmente o por software, no debería ser usada para derivar de ella el identificador de interfaz, pero si no hubiera otra fórmula, su propiedad debe reflejarse en el valor del bit U/L.

Véase el esquema siguiente:

Para mapear direcciones unicast IPv6 sobre Ethernet, se utilizan los mecanismos ND para solicitud de vecinos.

Para mapear direcciones multicast IPv6 sobre Ethemet, se emplean los 4 últimos bytes de la dirección IPv6, a los que se antepone "3333".

Multi-homing

El mecanismo de asignación de direcciones IPv6 es totalmente jerárquico.

El multi-homing ("múltiples hogares") es el mecanismo por el cual un determinado sitio o red puede estar conectado a otros por múltiples caminos, por razones de seguridad, redundancia, ancho de banda, balanceo de carga, etc.

Dado que un determinado sitio utiliza el prefijo de su ISP, o proveedor de nivel superior, un sitio puede ser "multi-homed" simplemente teniendo varios prefijos. Frecuentemente, cada prefijo estará asociado a diferentes conexiones físicas, aunque no necesariamente, dado que se puede tratar de una sola conexión física y diversos túneles o conexiones virtuales.

La problemática se plantea por la dificultad de que un host decida, en una red "multi-homed", que dirección fuente utilizar.

IPsec

Una de las grandes ventajas de IPv6 es, sin duda, la total integración de los mecanismos de seguridad, autenticación y confidencialidad (encriptación), dentro del núcleo del protocolo.

Se trata por tanto de algo obligatorio, y no adicional ni "añadido" como en IPv4. Para ello, la siguiente cabecera puede tener valores AH (autenticación -"Authentication Header") y ESP (encriptación - "Encapsulation Security Payload"), que permiten, básicamente, emplear las mismas extensiones de protocolo empleadas en IPv4, y que de hecho, al haber sido desarrolladas con posterioridad al inicio de los trabajos de IPv6, ya to contemplan.

Dado que los mecanismos asociados ya han sido descritos, simplemente citamos las normas básicas que son aplicables: RFC2401 al RFC2412 y RFC2451.

Movilidad

La posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad, es otra de las motivaciones básicas de IPv6. Como no, ya se han iniciado trabajos al respecto en lPv4, pero las complicaciones para usar la movilidad en este caso son enormes.

La idea básica permite identificar a un nodo móvil por su dirección de partida ("home address"), independientemente de su punto de conexión a Internet en cada momento dado. Por supuesto, cuando no esta en su punto de origen o de partida, también esta asociado con la información que permite identificar su posición o dirección actual ("care-of-address"). Los paquetes enviados a un nodo móvil (a su dirección de origen), son transparentemente encaminados a su "dirección actual".

El protocolo también permite que los nodos IPv6 almacenen la información de vinculación entre la dirección de partida y la posición actual, a modo de caché, y por tanto sean capaces de enviar los paquetes destinados al nodo móvil, directamente a su "dirección actual".

Para ello, el protocolo define nuevas opciones de destino, una de las cuales ha de ser soportada incluso en paquetes recibidos por todos los nodos (aunque no sean móviles).

Además, hay que prever, dada la estructura habitual de las redes inalámbricas (ejemplo muy habitual, la telefonía celular), que un nodo móvil puede estar conectado simultáneamente a varias redes (varías células que se solapan), y debe de ser alcanzable por cualquiera de ellas.

Los trabajos iniciales están documentados en el RFC2002 (soporte de movilidad en IP) y sucesivos. Además, se han publicado ya las especificaciones para túneles inversos en redes IP móviles (RFC2344), en cuya actualización se esta trabajando.

Se trabaja también en apartados como los requisitos de autenticación, autorización y facturación, comúnmente denominadas AAA (Authentication, Authorization and Accounting), las extensiones de autenticación, las claves de registro AAA, la optimización de rutas (draft-ietf-mobiieipoptim-09.txt), claves de registro para la optimización de rutas, registros regionales, entre otros.

DNS (RFC1886)

El mecanismo fundamental por el cual nos referimos a direcciones IP para la localización de un host, es el uso de literales (URL).

Sin embargo, para que este mecanismo funcione, a más bajo nivel existe un protocolo denominado "Sistema de Nombres de Dominio" (Domain Name System o DNS).

Este mecanismo, definido para IPv4 (RFC1034 y RFC1035), fue actualizado por el RFC1886, básicamente incluyendo un nuevo tipo de registro para almacenar las direcciones IPv6, un nuevo dominio para soportar las "localizaciones" (lookups) basadas en IPv6, y definiciones actualizadas de tipos de consultas existentes que devuelven direcciones Internet como parte de procesos de secciones adicionales.

Las extensiones han sido diseñadas para ser compatibles con las aplicaciones existentes y, en particular, con las implementaciones del propio DNS.

El problema del sistema de DNS existente es fácilmente comprensible: Al hacer una consulta, las aplicaciones asumen que se les devolverá una dirección de 32 bits (IPv4). Para resolverlo, hay que definir las siguientes extensiones, antes indicadas:

- Un nuevo tipo de registro de recurso para mapear un nombre de dominio con una dirección IPv6: Es el registro AAAA (con un valor de tipo 28, decimal).
- Un nuevo dominio para soportar búsquedas basadas en direcciones. Este dominio es IP6.INT. Su representación se realiza en orden inverso de la dirección, separando los nibbles (hexadecimal) por puntos ("."), seguidos de ".IP6.INT". Así, la búsqueda inversa de la dirección 4321:0:1:2:3:4:567:89aó, seria "b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.INT"
- Redefinición de las consultas existentes, que localizan direcciones IPv4, para que puedan también procesar direcciones IPv6. Ello incluye TODAS las consultas, lógicamente (NS, MX, MB, ...).

Además, para soportar la agregación de direcciones IPv6, la renumeración y el multi-homing, se trabaja en un nuevo documento que incluye un nuevo tipo de registro de recurso (A6) para almacenar las direcciones IPv6 de forma que se agilice la renumeración de la red. Se prevé que este documento sustituya al RFC1886.

Otros documentos relevantes son: RFC2181 (clarificaciones a las especificaciones DNS), RFC2535 (extensiones de seguridad para DNS), RFC2672 (redirección de árboles DNS), RFC2673 (etiqueta binarias en DNS).

Protocolos de Routing

Básicamente se adoptan los mismo protocolos de encaminado que los existentes en las redes IPv4: RIP, OSPF y BGP. Pero además se está trabajando en IDRP (ISO Inter-Domain Routing Protocol) a IS-IS (Intermediate System to Intermediate System).

RIPng (RFC2080 y RFC2081)

La especificación del Protocolo de Información de Rutas (RIP - "Routing Information Protocol")

para IPv6, recoge los cambios mínimos a indispensables al RFC1058 y RFC1723 para su adecuado funcionamiento.

RIPng es un protocolo pensado para pequeñas redes, y por tanto se incluye en el grupo de protocolos de pasarela interior (IGP - "Interior Gateway Protocol"), y emplea un algoritmo denominado "Vector-Distancia". Se basa en el intercambio de información entre routers, de forma que puedan calcular las rutas más adecuadas, de forma automática.

RIPng sólo puede ser implementado en routers, donde requerirá como información fundamental, la métrica o número de saltos (entre 1 y 15), que un paquete ha de emplear, para llegar a determinado destino. Cada salto supone un cambio de red, por to general atravesando un nuevo router.

Además de la métrica, cada red tendrá un prefijo de dirección destino y la longitud del propio prefijo.

Estos parámetros han de ser configurados por el administrador de la red.

El router incorporará, en la tabla de encaminado, una entrada para cada destino accesible (alcanzable) por el sistema. Cada entrada tendrá como mínimo, los siguiente parámetros:

- El prefijo IPv6 del destino.
- La métrica (número de saltos entre este router y el destino).
- La dirección IPv6 del siguiente router, así como la ruta para llegar a él.
- Un indicador relativo al cambio de ruta.
- Varios contadores asociados con la ruta.

Además se podrán crear rutas internas (saltos entre interfaces del propio router), o rutas estáticas (definidas manualmente).

RIPng es un protocolo basado en UDP. Cada router tiene un proceso que envía y recibe datagramas en el puerto 521 (puerto RIPng).

El inconveniente de RIPng, al igual que en IPv4, siguen siendo, además de su orientación a pequeñas redes (diámetro de 15 saltos como máximo), en que su métrica es fija, es decir, no puede variar en función de circunstancias de tiempo real (retardos, fiabilidad, carga, etc.).

OSPFv6 (RFC2740)

El protocolo de encaminado "Abrir Primero el Camino más Corto" (OSPF -"Open Shortest Path First"), es también un protocolo IGP (para redes autónomas), basado en una tecnología de "estado de enlaces" ("link-state").

Se trata de un protocolo de encaminado dinámico, que detecta rápidamente cambios de la topología (como un fallo en un router o interfaz) y calcula la siguiente ruta disponible (sin bucles), después de un corto período de convergencia con muy poco tráfico de routing.

Cada router mantiene una base de datos que describe la topología del sistema autónomo (de la red), y es to que denominamos base de datos de "estado de enlaces". Todos los routers del sistema tienen una base de datos idéntica, indicando el estado de cada interfaz, y de cada "vecino alcanzable".

Los routers distribuyen sus "estados locales" a través del sistema autónomo (la red) por medio de desbordamientos ("flooding").

Todos los routers utilizan el mismo algoritmo, en paralelo, y construyen un árbol de las rutas más cortas, como si fueran la raíz del sistema. Este árbol de "rutas más cortas" proporciona la ruta a cada destino del sistema autónomo.

Si hubiera varias rutas de igual coste a un determinado destino, el tráfico es distribuido equilibradamente entre todas. El coste de una ruta se describe por una métrica simple, sin

dimensión.

Se pueden crear áreas o agrupaciones de redes, cuya topología no es retransmitida al resto del sistema, evitando tráfico de routing innecesario.

OSPF permite el use de máscaras diferentes para la misma red ("variable length subnetting"), to que permite el encaminado a las mejores rutas (las más largas o más específicas).

Todos los intercambios de protocolo OSPF son autenticados, y por tanto sólo pueden participar los routers verificados ("trusted").

OSPFv6 mantiene los mecanismos fundamentales de la versión para IPv4, pero se han tenido que modificar ciertos parámetros de la semántica del protocolo, así como el incremento del tamaño de la dirección. OSPFv6 se ejecuta basado en cada enlace, en lugar de en cada subred.

Además, ha sido necesario eliminar la autenticación del protocolo OSPFv6, dado que IPv6 incorpora estas características (AH y ESP).

A pesar de la mayor longitud de las direcciones, se ha logrado que los paquetes OSPFv6 sean tan compactos como los correspondientes para IPv4, eliminando incluso algunas limitaciones y flexibilizando la manipulación de opciones.

BGP4+ (RFC2283, RFC2545)

El Protocolo de Pasarelas de Frontera (BGP - "Border Gateway Protocol") es un protocolo de encaminado para la interconexión de sistemas autónomos, es decir, para el enrutado entre diferentes dominios.

Frecuentemente se emplea para grandes corporaciones y para la conexión entres proveedores de servicios (como ISP's).

Su principal función es, por tanto, el intercambio de información de disponibilidad o alcance entre varios sistemas BGP, incluyendo información de los sistemas autónomos que contienen, permitiendo así construir las rutas más adecuadas y evitar bucles de tráfico.

BGP4 incorpora mecanismos para soportar enrutado entre dominios sin clases ("classless interdomain routing"), es decir, el use de prefijos, agregación de rutas, y todos los mecanismos en los que se basa IPv6.

BGP se basa en que un dispositivo sólo informa a los otros dispositivos que se conectan a él, acerca de las rutas que el mismo emplea. Es decir, es una estrategia de "salto a salto". La implicación es la simplicidad de Internet, pero la desventaja es que este mecanismo impide políticas complejas, que precisan de técnicas como el enrutado de fuente ("source routing").

BGP usa TCP como protocolo de transporte, a través del puerto 179.

BGP4+ añade a BGP (RFC1771), extensiones multiprotocolo, tanto para IPv6 como para otros protocolos, como por ejemplo IPX.

Estrategias o Mecanismos de Transición (RFC1933)

La clave para la transición es la compatibilidad con la base instalada de dispositivos IPv4. Esta afirmación define un conjunto de mecanismos que los hosts y routers IPv6 pueden implementar para ser compatibles con host y routers IPv4.

Estos mecanismos permitirán usar infraestructuras IPv4 para IPv6 y viceversa, dado que se prevé que su uso será prolongado, e incluso indefinido en muchas ocasiones.

Doble pila (IPv4 a IPv6)

El camino más lógico y evidente de transición es el uso simultáneo de ambos protocolos, en pilas

separadas. Los dispositivos con ambos protocolos también se denominan "nodos IPv6/IPv4".

De esta forma, un dispositivo con ambas pilas pueden recibir y enviar tráfico a nodos que sólo soportan uno de los dos protocolos (nodos sólo IPv4 ó sólo IPv6).

El dispositivo tendrá una dirección en cada pila. Se pueden utilizar direcciones IPv4 a IPv6 relacionadas o no, y se pueden utilizar mecanismos manuales o automáticos para la asignación de las direcciones (cada una correspondiente al protocolo en cuestión).

El DNS podrá devolver la dirección IPv4, la dirección IPv6, o ambas.

Se puede emplear la dirección lPv4 (32 bits), anteponiéndole 80 bits con valor cero y 16 bits con valor 1, para crear una dirección IPv6 "mapeada desde IPv4".

Túneles IPv6 sobre IPv4

Los túneles proporcionan un mecanismo para utilizar las infraestructuras IPv4 mientras la red IPv6 esta siendo implantada. Este mecanismo consiste en enviar datagramas IPv6 encapsulados en paquetes IPv4.

Los extremos finales del túnel siempre son los responsables de realizar la operación de encapsulado del paquete IPv6 en IPv4.

Estos túneles pueden ser utilizados de formas diferentes:

- **Router a router.** Routers con doble pila (IPv6/IPv4) se conectan mediante una infraestructura IPv4 y transmiten tráfico IPv6. El túnel comprende un segmento que incluye la ruta completa, extremo a extremo, que siguen los paquetes IPv6.
- **Host a router.** Hosts con doble pila se conectan a un router intermedio (también con doble pila), alcanzable mediante una infraestructura IPv4. El túnel comprende el primer segmento de la ruta seguida por los paquetes.
- **Host a host.** Hosts con doble pila interconectados por una infraestructura IPv4. El túnel comprende la ruta completa que siguen los paquetes.
- **Router a host.** Routers con doble pila que se conectan a hosts también con doble pila. El túnel comprende el último segmento de la ruta.

Los túneles se clasifican según el mecanismo por el que el nodo que realiza el encapsulado determina la dirección del nodo extremo del túnel. En los dos primeros casos (router a router y host a router), el paquete IPv6 es tunelizado a un router. El extremo final de este tipo de túnel, es un router intermedio que debe desencapsular el paquete IPv6 y reenviarlo a su destino final. En este caso, el extremo final del túnel es distinto del destino del destino final del paquete, por lo que la dirección en el paquete IPv6 no proporciona la dirección IPv4 del extremo final del túnel. La dirección del extremo final del túnel ha de ser determinada a través de información de configuración en el nodo que realiza el túnel. Es lo que se denomina "túnel configurado", describiendo aquel tipo de túnel donde el extremo final del túnel es explícitamente configurado.

En los otros dos casos (host a host y router a host), el paquete IPv6 es tunelizado, durante todo el recorrido, a su nodo destino. El extremo final del túnel es el nodo destino del paquete, y por tanto, la dirección IPv4 está contenida en la dirección IPv6. Este caso se denomina "túnel automático".

Transmisión de IPv6 sobre dominios IPv4 (RFC2529)

Este mecanismo permite a hosts IPv6 aislados, sin conexión directa a routers IPv6, ser totalmente funcionales como dispositivos IPv6.

Para ello se emplean dominios IPv4 que soportan multicast como su enlace local virtual. Es decir, usamos multicast IPv4 como su "ethernet virtual".

De esta forma, estos hosts IPv6 no requieren direcciones IPv4 compatibles, ni túneles configurados.

Los extremos finales del túnel se determinan mediante ND. Es imprescindible que la subred IPv4 soporte multicast.

Este mecanismo se denomina comúnmente "6 over 4".

Conexión de dominios IPv6 sobre redes IPv4

El documento draft-ietf-ngtrans-6to4-04.txt nos indica un mecanismo comúnmente denominado "6 to 4", para asignar un prefijo de dirección IPv6 a cualquier sitio que tenga al menos una dirección IPv4 pública.

De esta forma, dominios o hosts IPv6 aislados, conectados a infraestructuras IPv4 (sin soporte de IPv6), pueden comunicar con otros dominios o hosts IPv6 con una configuración manual mínima.

Este mecanismo funciona aún cuando la dirección IPv4 global (pública) es única y se accede a la red mediante mecanismos NAT (Network Address Transtation), que es el caso más común en las redes actuales para el acceso a Internet a través de ISP's.

"Tunnel Server" y "Tunnel Broker"

El documento draft-ietf-ngtrans-broker-02.txt sienta las bases para aplicaciones que permiten utilizar, de forma libre y gratuita, nuestras direcciones IPv4 actuales, sobre las infraestructuras IPv4, para acceder a redes y sitios IPv6.

Estos mecanismos se hacen indispensables para labores de investigación, dado que se requieren direcciones IPv6 y nombres DNS permanentes.

La diferencia con el mecanismo "6to4" es que el "Tunnel Broker" no requiere la configuración de un router.

Se trata de ISP's IPv6 "virtuales", proporcionando conectividad IPv6 a usuarios que ya tienen conectividad IPv4.

El "tunnel broker" es el lugar donde el usuario se conecta para registrar y activar "su túnel". El "broker" gestiona (crea, modifica, activa y desactiva) el túnel en nombre del usuario.

El "tunnel server" es un router con pila doble (IPv4 a IPv6), conectado a Intemet, que siguiendo órdenes del "broker" crea, modifica o borra los servicios asociados a un determinado túnel/usuario.

El mecanismo para su configuración es tan sencillo como indicar, en un formulario Web, datos relativos al S.O., la dirección IPv4, un "apodo" para la máquina, y el país donde esta conectada. El servidor de túneles crea los registros DNS, el extremo final del túnel, y genera un script para la configuración del cliente.

Los mecanismos para la transición de IPv4 a IPv6 se definen en la RFC 1933. El objetivo principal del proceso de transición es la coexistencia de las dos versiones de los protocolos hasta que IPv4 desaparezca completamente. Los planes de transición constan de dos categorías principales, la implementación de pilas duales y el túnel de IPv6 sobre IPv4.