CAPITULO II

EL PROTOCOLO IPv6

2.1 Introducción a IPv6

2.2 Características de IPv6

2.3 Notación IPv6

2.4 Tipos de direcciones IPv6

2.5 Datagrama IPv6

2.6 DNS para IPv6

2.7 Principales protocolos en IPv6

2.8 Seguridades

2.9 Organismos administradores, políticas de distribución y asignación de direcciones IPv6.

2.1 Introducción a IPv6

El Protocolo de *Internet* versión 6, mejor conocido como IPv6, es la versión más reciente de este protocolo y el sucesor de IPv4, la versión anterior, la cual no había sufrido cambios importantes desde 1981 cuando se dio a conocer por primera vez. Antes de adoptar este nombre, el protocolo IPv6 fue conocido como IPng (*Internet Protocol next generation*), y hasta la fecha existen personas que lo siguen llamando de esta manera. *[LIB014]*

Al observar el salto desde IPv4 hasta IPv6 (omitiendo la opción que parecería ser más lógica, IPv5) surge la duda en cuanto a por qué no se utilizó IPv5 como el nombre para el protocolo sucesor. Y la respuesta es muy simple: IPv5 nunca fue considerado para ser la nueva versión del protocolo. El nombre IPv5 fue asignado a un protocolo experimental, cuyo objetivo era el de la transmisión de datos en tiempo real. Este protocolo fue conocido originalmente como ST-2 (*Stream Protocol Version 2*), pero su función fue reemplazada eventualmente por ***RSVP*** (*Resource Reservation Setup Protocol*). Incluso, a raíz de este suceso, se han hecho peticiones para que en un futuro las versiones aumenten en números pares.

Hasta hace algunos años, el IPv4 había resultado ser un protocolo completo y de fácil implementación. El problema es que no se anticiparon algunas situaciones que eventualmente se convertirían en limitantes para la utilización del mismo.

Estas son algunas de estas situaciones:

El crecimiento desmedido del Internet y la reducción del espacio para asignar direcciones IP.
El crecimiento del Internet y la capacidad de los enrutadores pertenecientes al backbone de Internet para mantener grandes tablas de enrutamiento.
La necesidad de una configuración simple.
La necesidad de una mayor seguridad a nivel IP.
La necesidad de un mejor soporte en la transmisión de datos en "tiempo real", mejor conocido como "Calidad de Servicio".

Para resolver estas limitantes, la IETF (*Internet Engineering Task Force*) desarrolló un grupo de protocolos y estándares conocido como IPv6. Este protocolo fue diseñado con la intención de afectar en lo más mínimo a las capas inferiores y superiores, evitando agregar características totalmente nuevas a esta versión, manteniendo así la estructura básica original del protocolo. *[LIB008]*

2.2 Características de IPv6

IPv6 presenta ciertas características que contrastan con la versión 4 de este protocolo. Estas características se listan a continuación:

- Mayor espacio para direccionamiento.
- Simplificación de la cabecera.
- Cabeceras de extensión.
- Mejor soporte para calidad de servicio.
- Mayor seguridad en el protocolo.
- Direccionamiento jerárquico y enrutamiento eficientes.

2.2.1 Mayor espacio para direccionamiento

En el protocolo IPv6 se incrementó el tamaño de las direcciones IP de 32 bits a 128 bits. El propósito de utilizar 128 bits no es exclusivamente para aumentar la cantidad de direcciones IP, ya que aunque 128 bits pueden representar hasta $3.4x10^{38}$ posibles direcciones, el espacio para direccionamiento en IPv6 ha sido diseñado para soportar múltiples niveles de direccionamiento jerárquico (niveles tales como el diseño de subredes). Por el momento solo hay una pequeña cantidad de estas direcciones asignadas, lo que indica que existe un gran número de direcciones disponibles para ser utilizadas en un futuro. *[WWW019]*

2.2.2 Simplificación de la cabecera

La cabecera IPv6 fue modificada para disminuir el tiempo que tardaban los enrutadores en procesarla. Esto se logró eliminando algunos campos obsoletos y moviendo los campos opcionales y los que no se consideraban indispensables a las cabeceras de extensión, las cuales se colocan después de la cabecera IPv6.

2.2.3 Cabeceras de extensión

IPv6 puede ser expandido para soportar nuevas características, agregando cabeceras de extensión después de la cabecera IPv6. A diferencia del campo de "Opciones" de la cabecera IPv4, el cual solo puede contener 40 bytes, el tamaño de las cabeceras de extensión es limitado únicamente por el tamaño del paquete IPv6.

2.2.4 Mejor soporte para calidad de servicio

Se agregó la capacidad de etiquetar paquetes que pertenezcan a un mismo tipo de tráfico, para los cuales el emisor haya solicitado un manejo especial, como el envío de datos "en tiempo real".

2.2.5 Mayor seguridad en el protocolo

Se hizo obligatorio el soporte para ***IPSec*** (*IP Security*), el cual es un protocolo para la transmisión de datos a través de redes inseguras. Este requerimiento ofrece una solución para seguridad en redes y permite la interoperabilidad confiable entre diferentes implementaciones IPv6.

2.2.6 Direccionamiento jerárquico y enrutamiento eficientes

Las direcciones IPv6 globales utilizadas en la porción IPv6 del *Internet* fueron diseñadas para crear una infraestructura de enrutamiento eficiente y jerárquica, basada en la existencia de diferentes proveedores de servicio de *Internet*, cada uno con diferentes características. Debido a estas características, en la parte IPv6 del *Internet* los enrutadores pertenecientes al *backbone* manejan tablas de enrutamiento mucho más pequeñas.

2.3 Notación IPv6

2.3.1 Representación de direcciones IPv6 en texto

Las direcciones en IPv6 están representadas en la forma x:x:x:x:x:x:x:x, en donde cada "x" es un fragmento de 16 bits escrito en notación hexadecimal. Cada uno de estos fragmentos debe estar separado por un ":". El siguiente es un ejemplo de una dirección IPv6:

3FFE:8B34:23C4:B34A:023C:0002:F436:1234

16 bits

Otra notación común es utilizada cuando se requiere especificar direcciones IPv4. En este caso, únicamente los dos últimos fragmentos de la dirección, es decir, los últimos 32 bits, serán denotados en forma decimal, separados por un punto. A continuación se muestra una dirección de este tipo:

3FFE:8B34:23C4:B34A:023C:0002:148.210.30.5

Dirección IPv4

2.3.2 Compresión de ceros

Al crear direcciones IPv6, existe la posibilidad de que en ellas aparezcan grandes cadenas de ceros. Es en estos casos donde se puede utilizar la compresión de ceros.

Cuando existen ceros a la izquierda de un fragmento de la dirección, estos pueden ser comprimidos. La dirección

3FFE:8B340:23C:B34A:003F:08B3:23C4:0001

se puede escribir de la siguiente manera:

3FFE:8B34:23C:B34A:3F:8B3:23C4:1

También al tener únicamente ceros en un fragmento de la dirección, no es necesario escribirlos todos, basta con escribir uno. La dirección

3FFE:8B34:0000:0000:23C4:0000:0000:0001

se puede escribir de la siguiente manera:

3FFE:8B34:0:0:23C4:0:0:1

El último caso en la compresión de ceros es cuando se tiene un grupo de fragmentos conteniendo únicamente de ceros. En este caso, se puede utilizar "::", pero solamente una vez en la dirección. La dirección

3FFE:8B34:0000:0000:0000:0000:0000:0001

se puede escribir de la siguiente manera:

3FFE:8B34::1

En veces, el mal uso de la compresión de ceros, puede resultar en direcciones erróneas. Para ejemplificar lo anterior utilizaremos la siguiente dirección:

3FFE:8B34:0000:0000:3FC0:0000:0000:0001

INCORRECTO	CORRECTO	
3FFE:8B34::3FC0::1	3FFE:8B34:0000:0000:3FC0::1 ó 3FFE:8B34::3FC0:0000:0000:1	No se pueden utilizar dos "::" en una sola dirección. Esto nos llevará a una confusión de cuantos ceros se encuentran entre cada fragmento.
3FFE:8B34:0000:0000:3FC::1	3FFE:8B34:0000:0000:3FC0::1	Solamente se pueden omitir los ceros a la izquierda de un fragmento de la dirección. Los ceros a la derecha no pueden ser omitidos.

Tabla 2.1 Mal uso en la compresión de ceros

2.3.3 Prefijo

El prefijo, al igual que en IPv4, indica cuantos bits del lado izquierdo de la dirección identifican la red. Este número debe ser escrito en notación decimal, y debe escribirse al final de la dirección, separado por un "/", como se muestra en la siguiente dirección:

3FFE:8B4C:234A::34BC:23B4/48

El prefijo se puede usar en una dirección en particular como la dirección mostrada previamente, pero también puede ser utilizada para una dirección de red, como la siguiente:

3FFE:8B4C:234A::/48

La notación en puntos decimales o de máscara utilizada en IPv4, no es permitida para especificar un prefijo en IPv6.

El espacio de direcciones en IPv6 utiliza un esquema similar al utilizado por IPv4, en el cual los bits más a la izquierda de la dirección indican el tipo de dirección. A estos bits se les conoce como el formato del prefijo. *[LIB014]*

A continuación se muestra una tabla con los tipos de direcciones, así como su formato del prefijo:

Alocación	Formato del Prefijo	Fracción del espacio de direcciones
Reservado	0000 0000	1/256
Sin asignación	0000 0001	1/256
Reservado para NSAP	0000 001	1/128
Reservado para IPX	0000 010	1/128
Sin asignación	0000 011	1/128
Sin asignación	0000 1	1/32
Sin asignación	0001	1/16
Direcciones *Unicast* Globales Agregables	001	1/8
Sin asignación	010	1/8
Sin asignación	011	1/8
Sin asignación	100	1/8
Sin asignación	101	1/8
Sin asignación	110	1/8
Sin asignación	1110	1/16
Sin asignación	1111 0	1/32
Sin asignación	1111 10	1/64
Sin asignación	1111 110	1/128
Sin asignación	1111 1110 0	1/512
Direcciones *Unicast Link-local*	1111 1110 10	1/1024
Direcciones *Unicast Site-local*	1111 1110 11	1/1024
Direcciones *Multicast*	1111 1111	1/256

Tabla 2.2 ***Espacio de direcciones***

Las direcciones con formato del prefijo iniciando en 001 hasta 111, a excepción de las direcciones *Multicast*, deben tener un identificador de interfase de 64 bits, siguiendo el estándar EUI-64.

2.4 Tipos de direcciones IPv6

2.4.1 Unicast

Una dirección de tipo *Unicast* está asignada la mayoría de las veces a una sola interfase. Es permitido que varias interfases tengan la misma dirección *Unicast*, mientras aparezcan como una sola al entorno exterior. Entre las direcciones de este tipo se encuentran las direcciones Globales Agregables, de Uso Local, compatibles con IPv4, así como la dirección de *loopback* y la dirección no especificada. *[LIB005]*

2.4.1.1 La dirección no especificada

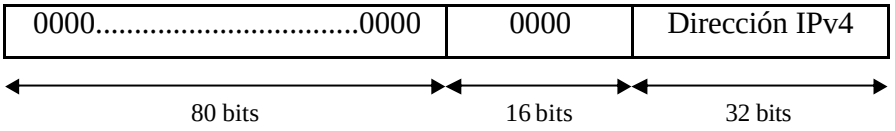
A la dirección 0:0:0:0:0:0:0:0, o simplemente ::, se le conoce como la dirección no especificada. Esta dirección significa ausencia de dirección, y no puede ser utilizada como dirección fuente o destino, ni puede ser incluida en la cabecera de enrutamiento.

2.4.1.2 La dirección *loopback*

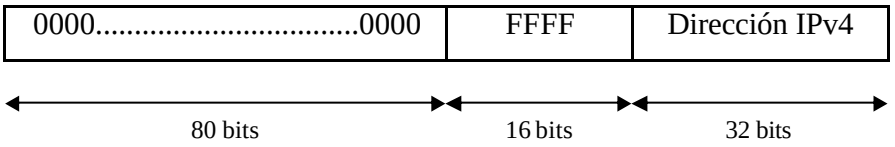
A la dirección 0:0:0:0:0:0:0:1, o simplemente ::1, se le conoce como la dirección de *loopback* o autoprueba. Esta dirección es útil cuando un *host* desea mandarse un paquete a sí mismo. Esta dirección no puede ser asignada a ninguna interfase, y tampoco puede ser utilizada como dirección fuente. Un paquete con una dirección destino de este tipo nunca debe de salir del nodo, y ningún enrutador debe procesarlo.

2.4.1.3 Direcciones IPv6 con direcciones IPv4

Algunas direcciones IPv6 contienen direcciones IPv4 dentro de ellas, y existen dos tipos. Las "Direcciones IPv6 compatibles con IPv4" son para nodos que soportan ambos protocolos (IPv6 e IPv4), y se conforman de la siguiente manera:

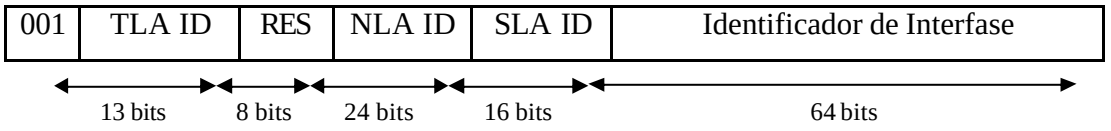


Las "Direcciones IPv6 mapeadas a IPv4" son para nodos que solamente soportan IPv4, y se conforman de la siguiente manera:



2.4.1.4 Direcciones Unicast Globales Agregables

Las Direcciones Unicast Globales Agregables son equivalentes a las direcciones IPv4 públicas. Como su nombre lo dice, este tipo de direcciones son globales, es decir, son únicas en todo el Internet. El formato de estas direcciones es el siguiente:



Como se puede ver, el formato del prefijo es 001, lo cual indica que la dirección debe empezar con un 2 o un 3 hexadecimal. Algunas de las direcciones que se están utilizando actualmente empiezan con 3FFE, que son las utilizadas por los ***TLA's***. Otras direcciones utilizadas son 2001 y 2002 para uso público.

Una ventaja de IPv6 es el enrutamiento jerárquico, el cual invo lucra distintos niveles de enrutamiento, como los siguientes:

TLA ID (*Top Level Aggregator ID)* – Es un identificador para los TLA. Un TLA es el nivel más alto de la jerarquía de enrutamiento. Estos TLA son controlados por ***IANA*** (*Internet Assigned Numbers Authority*).

RES – Este espacio es reservado en caso de que en un futuro se necesiten más bits para los TLA's o NLA's.

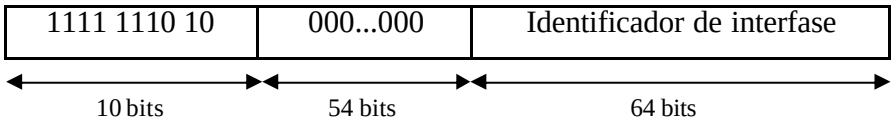
NLA (*Next Level Aggregator ID)* – Es un identificador para los NLA. Un NLA puede ser un proveedor de *Internet*.

SLA (*Site Level Aggregator ID*) – Es un identificador para los SLA. Un SLA es utilizado por organizaciones individuales para identificar subredes dentro de su sitio.

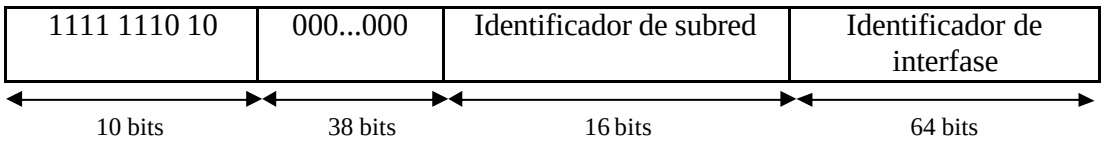
Identificador de Interfase – Indica la interfase en una red específica. Su funcionamiento se explicará más adelante.

2.4.1.5 Direcciones *Unicast* de uso local

Existen dos tipos de direcciones de uso local: *Link-local* (Enlace Local) y *Site-local* (Sitio Local). Las direcciones *Link-local* son utilizadas por nodos para comunicarse con sus ***nodos vecinos*** dentro de un mismo enlace. Un paquete con esta dirección nunca debe abandonar el enlace. Estas direcciones se pueden reconocer por su prefijo FE80::/64.



Las direcciones *Site-local* son equivalentes a las direcciones privadas en IPv4 (10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16). Estas direcciones se pueden utilizar para redes que no tienen acceso al *Internet*. Un paquete con esta dirección no puede ser reenviado por ningún enrutador en esa red. Estas direcciones se puedenreconocer por su prefijo FEC0::/64.



2.4.1.6 Identificador de Interfase

Como se había mencionado anteriormente, la mayoría de las direcciones *Unicast* requieren un identificador de interfase. Este sirve para identificar una interfase en un enlace, y debe ser único. El identificador de interfase se utiliza en el formato EUI-64 desarrollado por la ***IEEE*** (*Institute of Electrical and Electronic Engineers*). En la especificación EUI-64 se indica como se debe convertir una dirección ***MAC*** de 48 bits en un identificador de interfase de 64 bits. *[LIB007]*

A continuación se muestra el formato de una dirección MAC de 48 bits:

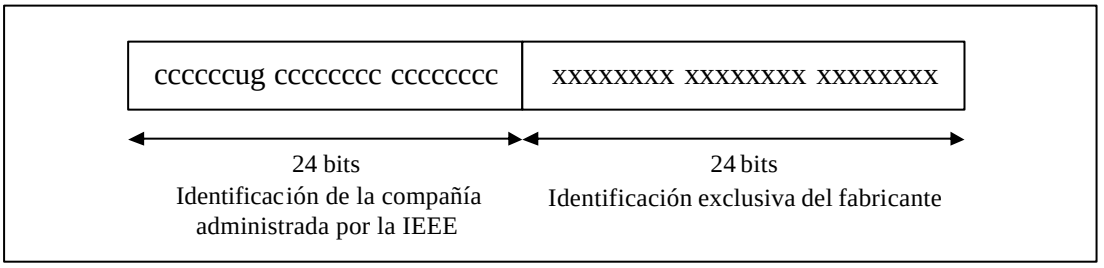


Figura 2.1 Dirección MAC de 48 bits

En donde las "c" significan la compañía, la "u" es el bit Universal/Local, la "g" es el bit Individual/Grupo, y las "x" son la identificación del fabricante.

Para convertir una dirección MAC de 48 bits en un identificador de interfase de 64 bits, se deben insertar dos octetos con los valores 0xFF y 0xFE entre la identificación de la compañía y la identificación exclusiva del fabricante. Para hacer este identificador de interfase válido para IPv6 se debe cambiar el valor del bit "u" a su complemento. A continuación se muestra el proceso completo de conversión:

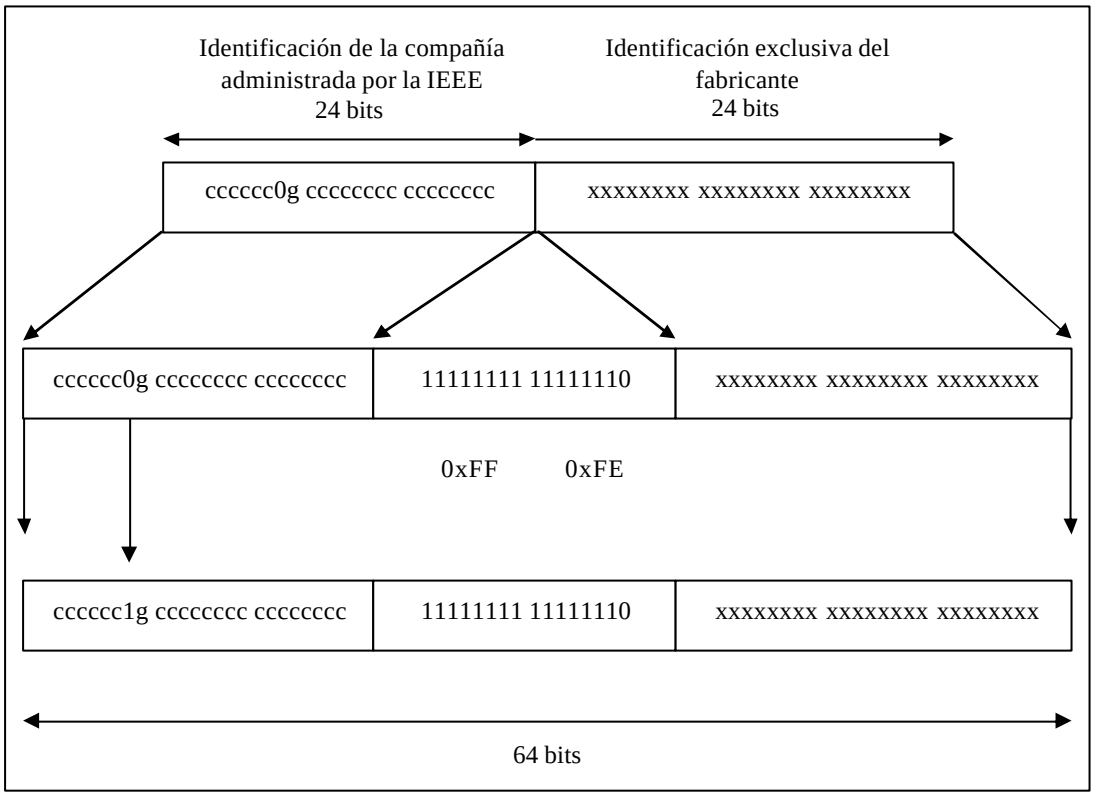
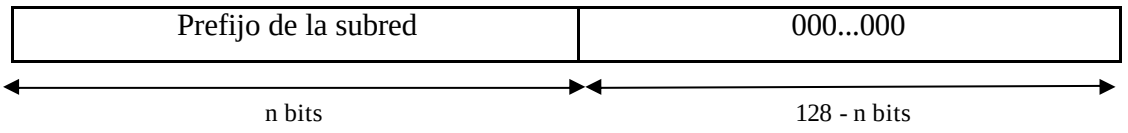


Figura 2.2 Conversión de una dirección MAC a un identificador de interfase

2.4.2 Anycast

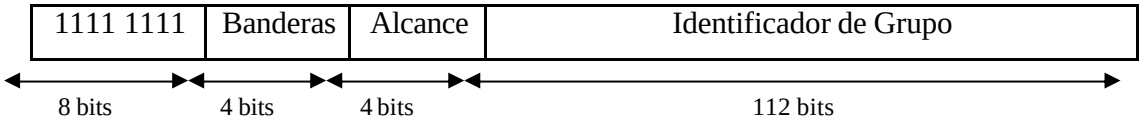
Una dirección ***Anycast*** identifica múltiples interfases. Un paquete con este tipo de dirección es entregado a una sola interfase, generalmente la "más cercana". La interfase "más cercana" es la que tiene menor distancia en términos de enrutamiento. Una dirección *Anycast* no puede ser diferenciada de una dirección *Unicast*. Estas direcciones solamente pueden ser utilizadas como direcciones destino. *[LIB003]*

El formato de una dirección *Anycast* es el siguiente:



2.4.3 Multicast

Una dirección *Multicast* identifica a múltiples interfases (pueden encontrarse en distintos nodos), como su nombre lo indica. Un paquete con una dirección *Multicast*, se entregará a todas las interfases identificadas con esa dirección. Una dirección de este tipo no debe ser utilizada como dirección fuente o como dirección dentro de un encabezado de enrutamiento. A continuación se muestra el formato de una dirección *Multicast*:



El formato del prefijo de una dirección *Multicast* es 1111 1111, lo cual facilita su identificación, ya que todas las direcciones de este tipo comienzan con 0xFF.

Las banderas son 4 bits, aunque en realidad 3 son reservados y deben estar siempre en 0. Solamente se usa el bit de más a la derecha que es conocido como el bit "T". Cuando este bit se encuentra en 0, indica una dirección *Multicast* que está permanentemente asignada ("Bien conocidas"), y es asignada por una autoridad de numeración en *Internet*. Cuando este bit se encuentra en 1, indica una dirección *Multicast* no permanentemente asignada.

El campo de alcance es de 4 bits, y sirve para restringir el tráfico de *Multicast*. A continuación se muestran los posibles valores:

0 – Reservado

1 – Alcance Nodo Local

2 – Alcance Enlace Local

3 – Sin asignación

4 – Sin asignación

5 – Alcance Sitio Local

6 – Sin asignación

7 – Sin asignación

8 – Alcance Organización Local

9 – Sin asignación

A – Sin asignación

B – Sin asignación

C – Sin asignación

D – Sin asignación

E – Alcance Global

F – Reservado

El identificador de grupo consta de 112 bits, e indica el grupo *Multicast* único en el alcance. Puede contener direcciones *Multicast* permanentemente asignadas o no permanentemente asignadas.

2.4.3.1 Direcciones *Multicast* Predefinidas

Las siguientes direcciones *Multicast* "Bien conocidas" han sido predefinidas:

FF00:0:0:0:0:0:0:0	ó	FF00::	Direcciones *Multicast* Reservadas
FF01:0:0:0:0:0:0:0	ó	FF01::	
FF02:0:0:0:0:0:0:0	ó	FF02::	Estas direcciones no deberán ser
FF03:0:0:0:0:0:0:0	ó	FF03::	asignadas a ningún grupo *Multicast*.
FF04:0:0:0:0:0:0:0	ó	FF04::	
FF05:0:0:0:0:0:0:0	ó	FF05::	
FF06:0:0:0:0:0:0:0	ó	FF06::	
FF07:0:0:0:0:0:0:0	ó	FF07::	
FF08:0:0:0:0:0:0:0	ó	FF08::	
FF09:0:0:0:0:0:0:0	ó	FF09::	
FF0A:0:0:0:0:0:0:0	ó	FF0A::	
FF0B:0:0:0:0:0:0:0	ó	FF0B::	
FF0C:0:0:0:0:0:0:0	ó	FF0C::	

FF0D:0:0:0:0:0:0:0	ó	FF0D::
FF0E:0:0:0:0:0:0:0	ó	FF0E::
FF0F:0:0:0:0:0:0:0	ó	FF0F::

Las siguientes direcciones son para los nodos, y tienen un alcance de tipo 1 (Nodo Local) y 2 (Enlace Local):

FF01:0:0:0:0:0:0:1	ó	FF01::1	Direcciones de todos los nodos
FF02:0:0:0:0:0:0:1	ó	FF02::1	

Las siguientes direcciones son para los enrutadores, y tienen un alcance de tipo 1 (Nodo Local), 2 (Enlace Local) y 5(Sitio Local):

FF01:0:0:0:0:0:0:2	ó	FF01::2	Direcciones de todos los enrutadores
FF02:0:0:0:0:0:0:2	ó	FF02::2	
FF05:0:0:0:0:0:0:2	ó	FF05::2	

Por último, existe una dirección llamada “dirección del nodo solicitado”, y se compone de los últimos 24 bits de una dirección *Unicast* o *Anycast*, anexados al prefijo FF02:0:0:0:0:1:FF00::/104, resultando en una dirección *Multicast* del rango de FF02:0:0:0:0:1:FF00:0000 hasta FF02:0:0:0:0:1:FFFF:FFFF. Esta dirección sirve para facilitar la búsqueda de direcciones en la operación de resolución de direcciones.

Por ejemplo, la dirección de nodo solicitado correspondiente a la dirección 4380::23BA:3EFF:F238:7D53, sería FF02:0:0:0:0:1:FF38:7D53. Puede haber otros nodos con la misma dirección de nodo solicitado, ya que pueden variar solamente en los bits de más a la derecha. Sin embargo, el número de nodos “molestados” en una resolución de direcciones será menor utilizando la dirección de nodo solicitado.

2.5 Datagrama IPv6

2.5.1 Forma General de un datagrama IPv6

El IPv6 cambia completamente el formato de datagrama. Como se muestra en la figura un datagrama IPv6 tiene un encabezado base de tamaño fijo, seguido por ceros o más encabezados de extensión, seguidos a su vez por datos. *[LIB011]*

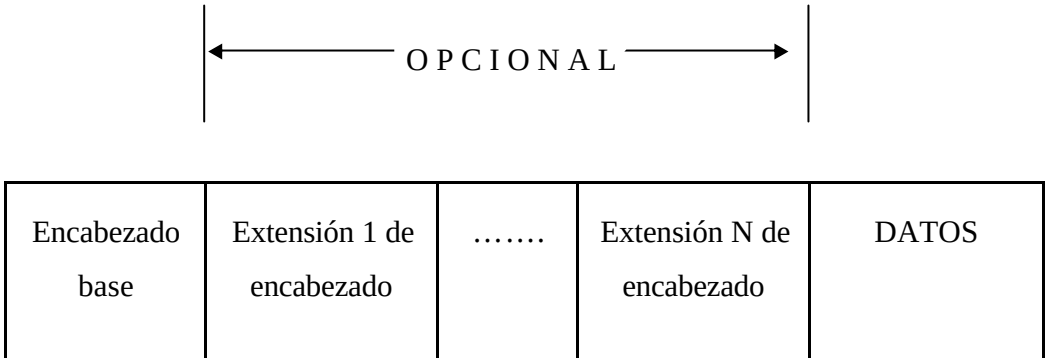


Figura 2.3 Forma General de un datagrama IPv6

2.5.2 Formato del encabezado base del IPv6

Es interesante que aun cuando debe adaptarse a direcciones extensas, un encabezado base IPv6 contiene menos información que un encabezado de datagrama IPv4. Las opciones y algunos de los campos fijos que aparecen en un encabezado de datagrama del IPv4 se han cambiado por encabezados de extensión en el IPv6. En general, el cambio en los encabezados en los datagramas refleja los cambios en el protocolo:

- La alineación se ha cambiado de múltiplos de 32 bits a múltiplos de 64 bits.
- Los campos de longitud de encabezado se han eliminado y el campo de longitud de datagrama ha sido reemplazado por el campo *PAYLOAD LENGTH (LONGITUD PAYLOAD).*
- El tamaño de los campos de dirección de fuente y destino se ha incrementado en 16 octetos cada uno.
- La información de fragmentación se ha movido de los campos fijos en el encabezado base, hacia un encabezado de extensión.

- El campo *TIME-TO-LIVE (LÍMITE DE SALTO)* ha sido reemplazado por el *HOP LIMIT.*
- El campo *SERV1CE TYPE* ha sido reemplazado por el campo *FLOW LABEL (ETIQUETA DE FLUJO).*
- El campo *PROTOCOL* ha sido reemplazado por un campo que especifica el tipo del próximo encabezado.

La figura muestra el contenido y el formato de un encabezado base IPv6. Varios campos en un encabezado base IPv6 corresponden directamente a los campos en un encabezado IPv4. Como en el IPv4, el campo inicial *VERS* de 4 bits especifíca la versión del protocolo; *VERS* siempre contiene el número 6 en un datagrama IPv6. Como en el IPv4, los campos *SOURCE ADDRESS (DIRECCIÓN FUENTE) y DESTINATION ADDRESS (DIRECCION DE DESTINO)* especifican la dirección del emisor y del recipiente. En el IPv6, sin embargo, cada dirección requiere 16 octetos. El campo *HOP LIMIT* corresponde al campo *TIME- TO-LIVE del* IPv4. A diferencia del IPv4, que interpreta un tiempo límite como una combinación de conteo de saltos y tiempo máximo, el IPv6 interpreta el valor como un límite estricto del máximo número de saltos que un datagrama puede realizar antes de ser desechado.

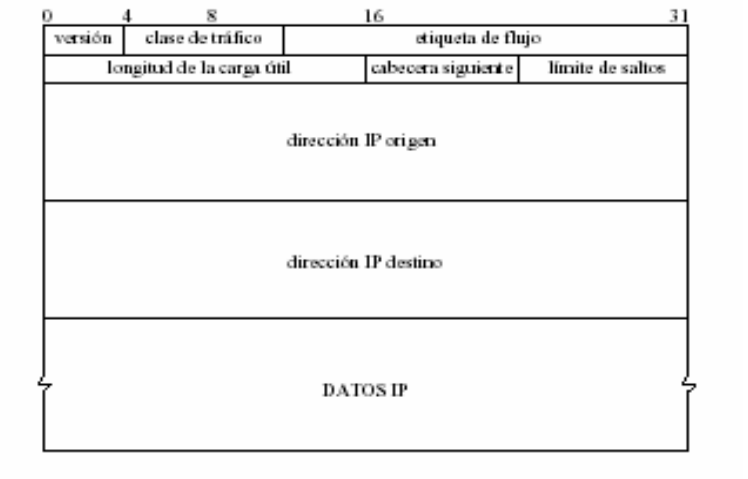


Figura 2.4 Formato del encabezado base de 40 octetos del IPv6

Explicación del Datagrama IP

Versión	Contiene la versión del protocolo IP
Clase de Tráfico	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	Permite tráficos con requisitos de tiempo real. Tiene una longitud de 20 bits.
Longitud de la carga util	Es la longitud de los propios datos, y puede ser de hasta 65.536 bytes. Tiene una longitud de 16 bits (2 bytes).
Cabecera siguiente	Indica cual es la siguiente cabecera y así sucesivamente. 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).
Limite de saltos	Especifica el numero de segundos que se permite al Datagrama circular por la red antes de ser descartado Tiene una longitud de 8 bits (1 byte).
Dirección IP de Origen	Dirección IP del Origen
Dirección IP del Destino	Dirección IP del Destino
Datos IP	Datos del datagrama

Tabla 2.3 Explicacion del Datagrama IPv6

2.6 DNS para IPv6

El DNS (*Domain Name System*) para las direcciones IPv6 tuvo dos cambios principalmente: un nuevo registro de recursos (AAAA) y un nuevo dominio para consultas en reversa. *[WWW017]*

2.6.1 Registro de recursos (AAAA)

Este nuevo registro de recursos es utilizado para resolver un nombre de dominio a una dirección IPv6. Es llamado AAAA, debido a que las direcciones IPv6 (128 bits) son cuatro veces más grandes que las direcciones IPv4 (32 bits). Previamente, las direcciones IPv4 utilizaban el registro de recursos llamado A.

2.6.2 Dominio IP6.INT

Este nuevo dominio fue creado para resolver consultas en reversa, es decir, resolver un nombre de *host* basado en una dirección IPv6. Para una consulta en reversa, la dirección IPv6 se divide en fragmentos de 4 bits, o *nibbles*, y se escribe empezando con el fragmento que tenga el bit menos significativo, hasta el fragmento que tenga el bit más significativo. Además, se le agregará ".IP6.INT" después de la dirección [3]. A continuación se muestra un ejemplo con la dirección 1234:B4:344C:5:6:7:8:AB32 (expresada en su totalidad como 1234:00B4:344C:0005:0006:0007:0008:AB32):

2.3.B.A.8.0.0.0.7.0.0.0.6.0.0.0.5.0.0.0.C.4.4.3.4.B.0.0.4.3.2.1.IP6.INT.

nibble

2.7 Principales protocolos en IPv6

IPv6 básicamente adopta los mismos protocolos que los existentes en las redes IPv4: ICMPv6, RIP, OSPF, BGP, etc. Pero además se está trabajando en nuevos protocolos como son IDRP (ISO Inter-Domain Routing Protocol) e IS-IS (Intermediate System to Intermediate System). A continuación vamos a realizar un breve análisis de los principales protocolos para IPv6 y sus nuevas características de funcionamiento.

2.7.1 Protocolo ICMPv6

El Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol), descrito originalmente en el documento ***RFC***792 para IPv4, ha sido actualizado para permitir su uso bajo IPv6.

El protocolo resultante de dicha modificación es ICMPv6, y se le ha asignado un valor, para el campo de "siguiente cabecera", igual a 58. ICMPv6 es parte integral de IPv6 y debe

ser totalmente incorporado a cualquier implementación de nodo IPv6. ICMPv6 es empleado por IPv6 para reportar errores que se encuentran durante el procesado de los paquetes, así como para la realización de otras funciones relativas a la capa "Internet", como diagnósticos ("ping"). *[LIB014]*

El formato genérico de los mensajes ICMPv6 es el siguiente:

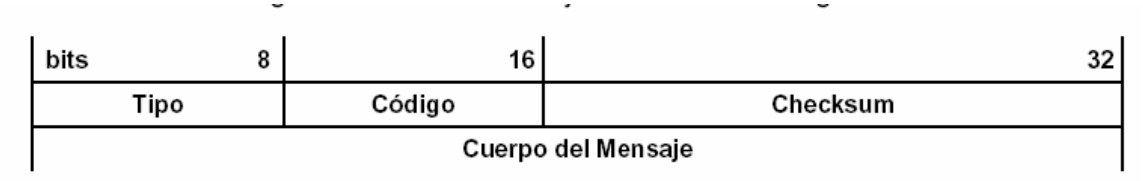


Figura 2.5 Formato ICMPv6

El campo "tipo" indica el tipo de mensaje, y su valor determina el formato del resto de la cabecera.

El campo "código" depende del tipo de mensaje, y se emplea para crear un nivel adicional de jerarquía para la clasificación del mensaje. El checksum o código de redundancia nos permite detectar errores en el mensaje ICMPv6.

Los mensajes ICMPv6 se agrupan en dos tipos o clases: mensaje de error y mensajes informativos. Los mensajes de error tienen cero en el bit de mayor peso del campo "tipo", por lo que sus valores se sitúan entre 0 y 127. Los valores de los mensajes informativos oscilan entre 128 y 255.

Los mensajes definidos por la especificación básica son los siguientes:

Mensajes de error ICMPv6		
Tipo	Descripción y Códigos	
1	Destino no alcanzable (Destination Unreachable)	
	Código	Descripción
	0	Sin ruta hacia el destino
	1	Comunicación prohibida administrativamente
	2	Sin asignar
	3	Dirección no alcanzable
	4	Puerto no alcanzable
2	Paquete demasiado grande (Packet Too Big)	
3	Tiempo excedido (Time Exceeded)	
	Código	Descripción
	0	Límite de saltos excedido
	1	Tiempo de desfragmentación excedido
4	Problema de parámetros (Parameter Problem)	
	Código	Descripción
	0	Campo erróneo en cabecera
	1	Tipo de "cabecera siguiente" desconocida
	2	Opción IPv6 desconocida
Mensajes informativos ICMPv6		
Tipo	Descripción	
128	Solicitud de eco (Echo Request)	
129	Respuesta de eco (Echo Reply)	

Figura 2.6 Mensajes ICMPv6

Se esta trabajando en nuevos tipos de mensajes, siendo el más interesante de ellos el definido en un borrador de IETF (draft-ietf-ipngwg-icmp-name-lookups- 05.txt), que permitirá solicitar a un nodo información completa como su "nombre de dominio comp letamente cualificado" (Fully-Qualified-Domain-Name). Por razones de seguridad, las cabeceras ICMPv6 pueden ser autenticadas y encriptadas, usando la cabecera correspondiente. El uso de este mecanismo permite, además, la prevención de ataques ICMP, como el conocido "Negación de Servicio" (DoS o Denial of Service Attack).

2.7.2 Neighbor Discovery - El "ARP" de IPv6

En IPv6, el protocolo equivalente, en cierto modo, a ARP en IPv4, es el que denominamos "descubrimiento del vecindario". Sin embargo, incorpora también la funcionalidad de otros protocolos IPv4, como "ICMP Router Discovery" y "ICMP Redirect".

Tal como indica esta "traducción", consiste en el mecanismo por el cual un nodo que se incorpora a una red, descubre la presencia de otros, en su mismo enlace, para determinar sus direcciones en la capa de enlace, para localizar los routers, y para mantener la información de conectividad ("reachability") acerca de las rutas a los "vecinos" activos. El protocolo ND (abreviatura común de "Neighbor Discovery"), también se emplea para mantener limpios los "caches" donde se almacena la información relativa al contexto de la red a la que esta conectado un nodo (host o router), y por tanto para detectar cualquier cambio en la misma. Cuando un router, o una ruta hacia él, falla, el host buscará alternativas funcionales. ND emplea los mensajes de ICMPv6, incluso a través de mecanismos de multicast en la capa de enlace, para algunos de sus servicios. El protocolo ND es bastante completo y sofisticado, ya que es la base para permitir el mecanismo de autoconfiguración en IPv6.

Define, entre otros, mecanismos para: descubrir routers, prefijos y parámetros, autoconfiguración de direcciones, resolución de direcciones, determinación del siguiente salto, detección de nodos no alcanzables, detección de direcciones duplicadas o cambios,

redirección, balanceo de carga entrante, direcciones anycast, y anunciación de proxies. ND define cinco tipos de paquetes ICMPv6:

- Solicitud de Router (Router Solicitation) – generado por una interfaz cuando es activada, para pedir a los routers que se "anuncien" inmediatamente. Tipo en paquete ICMPv6 = 133.

- Anunciación de Router (Router Advertisement) – generado por los routers periódicamente (entre cada 4 y 1800 segundos) o como consecuencia de una "solicitud de router", a través de multicast, para informar de su presencia así como de otros parámetros de enlace y de Internet, como prefijos (uno o varios), tiempos de vida, configuración de direcciones, límite de salto sugerido, etc. Es fundamental para permitir la renumeración. Tipo en paquete ICMPv6 = 134.
- Solicitud de Vecino (Neighbor Solicitation) – generado por los nodos para determinar la dirección en la capa de enlace de sus vecinos, o para verificar que el nodo vecino sigue activo (es alcanzable), así como para detectar las direcciones duplicadas. Tipo en paquete ICMPv6 = 135.
- Anunciación de Vecino (Neighbor Advertisement) – generado por los nodos como respuesta a la "solicitud de vecino", o bien para indicar cambios de direcciones en la capa de enlace. Tipo en paquete ICMPv6 = 136.
- Redirección (Redirect) – generado por los routers para informar a los host de un salto mejor para llegar a un determinado destino. Equivalente, en parte a "ICMP redirect". Tipo en paquete ICMPv6 = 137.

El protocolo ND, frente a los mecanismos existentes en IPv4, reporta numerosas ventajas:

- El descubrimiento de routers es parte de la base del protocolo, no es preciso recurrir a los protocolos de encaminado.
- La anunciación de router incluye las direcciones de la capa de enlace, no es necesario ningún intercambio adicional de paquetes para su resolución.
- La anunciación de router incluye los prefijos para el enlace, por lo que no hay necesidad de un mecanismo adicional para configurar la máscara de red.
- La anunciación de router permite la autoconfiguración de direcciones.
- Los routers pueden anunciar a los host del mismo enlace el ***MTU*** (tamaño máximo de la unidad de transmisión).
- Se extienden los ***multicast*** de resolución de direcciones entre 232 direcciones, reduciendo de forma importante las interrupciones relativas a la

resolución de direcciones en nodos distintos al objetivo, y evitando las interrupciones en nodos sin IPv6.

- Las redirecciones contienen la dirección de la capa de enlace del nuevo salto, lo que evita la necesidad de una resolución de dirección adicional.
- Se pueden asignar múltiples prefijos al mismo enlace y por defecto los host aprenden todos los prefijos por la anunciación de router. Sin embargo, los routers pueden ser configurados para omitir parte o todos los prefijos en la anunciación, de forma que los host consideren que los destinos están fuera del enlace; de esta forma, enviarán el tráfico a los routers, quién a su vez lo redireccionará según corresponda.
- A diferencia de IPv4, en IPv6 el receptor de una redirección asume que el siguiente salto esta en el mismo enlace. Se prevé una gran utilidad en el sentido de no ser deseable o posible que los nodos conozcan todos los prefijos de los destinos en el mismo enlace (enlaces sin multidifusión y media compartida).
- La detección de vecinos no alcanzables es parte de la base de mejoras para la robustez en la entrega de paquetes frente a fallos en routers, particiones de enlaces, nodos que cambian sus direcciones, nodos móviles, etc.
- A diferencia de ARP, en ND se puede detectar fallos de la mitad del enlace, es decir, con conectividad en un sólo sentido, evitando el tráfico hacia ellos.
- A diferencia de IPv4, no son precisos campos de preferencia (para definir la "estabilidad" de los routers). La detección de vecinos no alcanzables sustituirá los caminos desde routers con fallos a otros activos.
- El uso de direcciones de enlace local para identificar routers, permite a los hosts que mantengan su asociación con los mismos, en el caso de que se realice una renumeración para usar nuevos prefijos globales.
- El límite de saltos es siempre igual a 255, lo que evita que haya envíos accidentales o intencionados desde nodos fuera del enlace, dado que los routers decrementan automáticamente este campo en cada salto.

- Al realizar la resolución de direcciones en la capa ICMP, se independiza el protocolo del medio, permitiendo mecanismos de autenticación y seguridad normalizados.

En resumen, ND reemplaza, con grandes mejoras e importantes ventajas, a ARP.

2.7.3 Protocolo DHCPv6

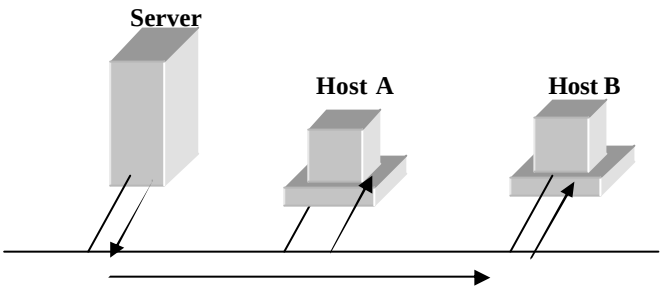
DHCP para IPv6 es un protocolo UDP cliente/servidor, diseñado para reducir el coste de gestión de nodos IPv6 en entornos donde los administradores precisan un control sobre la asignación de los recursos de la red, superior al facilitados por el mecanismo de configuración "stateless". *[LIB008]* Como 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 configuración locales en cada nodo.
DHCPv6 soporta los siguientes tipos de mensajes

Tipo de Mensaje	Descripción
SOLICITUD	Usado por los clientes para localizar los servidores de DHCP
ANUNCIO	Usado por los servidores como una contestación SOLICITAR.
DEMANDA	Usado por los clientes para recibir información de los servidores.
CONFIRMACION	Usó por los clientes para verificar que su dirección y parámetros de configuración todavía son válidos.
RENOVAR	Usó por los clientes para renovar sus parámetros de configuración con su servidor DHCP original cuando está a punto de expirar.
REBIND	Usado por los clientes para extender la vida de su dirección y renueva sus parámetros de configuración con cualquier servidor de DHCP cuando está a punto de expirar.
RESPONDER	Usado por servidores DHCP para responder a los mensajes DEMANDA, CONFIRMACION, RENOVAR, REBIND, RELEASE, y DECLINE MESSAGES.
LANZAR	Usado por los clientes para lanzar su dirección IP
DECLINE	Usado por los clientes para indicar que una o más direcciones asignadas a ellos ya está en uso.
RECONFIG-INIT	Usado por los servidores de DHCP para informar a los clientes que el servidor tiene información de configuración nueva o actualizada. Los clientes deben realizar una demanda para obtener la

	información actualizada.
INFORM	Enviado por los clientes para pedir los parámetros de la configuración sin la asignación de cualquier dirección IP al cliente.
RELAY-FORW	Usado por los relay de DHCP para adelantar los mensajes del cliente a los servidores. El relay encapsula el mensaje del cliente en una opción en el mensaje relay-forward.
RELAY-REPL	Usado por los servidores DHCP para enviar los mensajes a los clientes a través de un relay. El mensaje del cliente se encapsula como una opción en el mensaje relay-reply. El relay desencapsula el mensaje y lo envía al cliente.

Tabla 2.4 Tipos de mensajes DHCPv6

Figura Esquema DHCPv6



Los *hosts* obtienen información de la dirección de interfaz y/o configuración desde un servidor. Para ello, el servidor dispone de una base de datos que contiene información de las direcciones que han sido asignadas a determinados *hosts.* Este proceso es la implementación del protocolo *Dynamic Host Configuration Protocol* para IPv6-DHCPv6 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 relés 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 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:

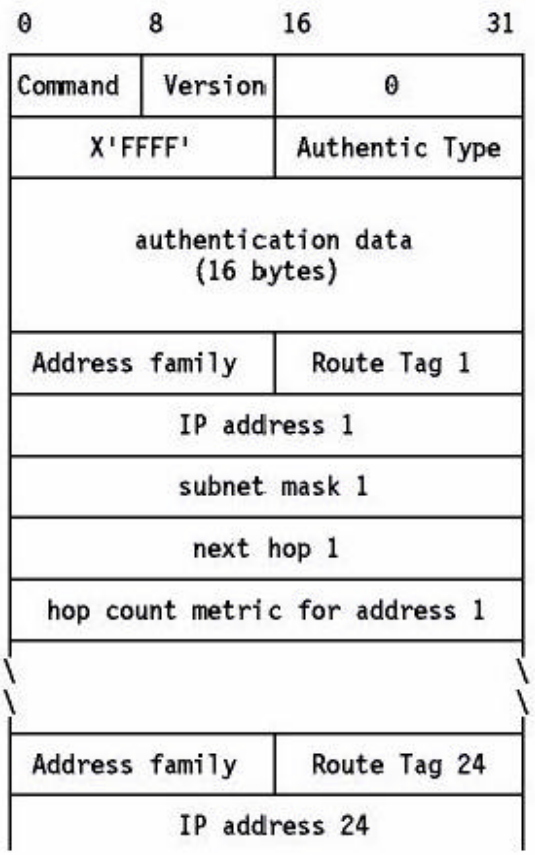
- Configuración de actualizaciones dinámicas de DNS.
- Desaprobación de direcciones, para renumeración dinámica.
- Relés preconfigurados con direcciones de servidores, o mediante multicast.
- Autenticación.
- Los clientes pueden pedir múltiples direcciones IP.
- Las direcciones pueden ser reclamadas mediante el mensaje de "iniciarreconfiguración".
- Integración entre autoconfiguración de direcciones "stateless" y "stateful"
- Permitir relés para localizar servidores fuera del enlace.

2.7.4 Protocolo RIPng

La especificación del Protocolo de Información de Rutas (RIP – "Routing Information Protocol") para IPv6, recoge los cambios mínimos e 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 lo general atravesando un nuevo router.

Los campos del mensaje RIPng son los siguientes:



Comando	Es 1 para una petición RIP o 2 para una respuesta
Versión	Es 2. Le dice al "router" RIP-1 que ignore los campos reservados, los que deben ser cero (si el valor es 1, los "routers" deben desechar los mensaje con valores distintos de cero en estos campos, ya que los originó un "router" que dice ser RIP, pero que envía mensajes que no cumplen el protocolo).
Dirección IP	Es la dirección IP de para esta entrada de encaminamiento: un host o una subred(caso en el que el número de host es cero).
Metrica de conteo de salto	Es el número de saltos hasta el destino. La cuenta de saltos para una interfaz conectada directamente es de 1, y cada "router" intermedio la incrementa en 1 hasta un máximo de 15, con 16 indicando que no existe ruta hasta el destino.

Familia de direcciones	Puede ser X'FFFF' sólo en la primera entrada, indicando que se trata de una entrada de autentificación.
Tipo de autentificación	Define como se han de usar los restantes 16 bytes. Los únicos tipos definidos son 0, indicando ninguna autentificación, y 2 indicando que el campo contiene datos de password.
Datos de autentificación	El password es de 16 bytes, texto ASCII plano, alineado a la izquierda y rellenado con caracteres nulos ASCII (X'00').
Etiqueta de ruta	Es un campo dirigido a la comunicación de información acerca del origen de la información de encaminamiento. Está diseñado para la interoperabilidad entre RIP y otros protocolos de encaminamiento. Las implementaciones de RIP-2 deben conservarlo, aunque RIP-2 no especifica como se debe usar.
Mascara de subred	La máscara de subred asociada con la subred a la que se refiere esta entrada.
Siguiente salto	Una recomendación acerca del siguiente salto que el "router" debería usar para enviar datagramas a la subred o al host dado en la entrada.

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 siguientes 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.). *[WWW007]*

2.7.5 Protocolo OSPFv6

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 lo 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 uso de máscaras diferentes para la misma red ("variable length subnetting"), lo 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. *[WWW014]*

Datagrama OSPF

Hay cinco tipos de paquetes diferentes usados por OSPF. Todos los paquetes de OSPF empiezan con una cabecera estandar de 16-byte. La siguiente figura muestra el datagrama OSPF:

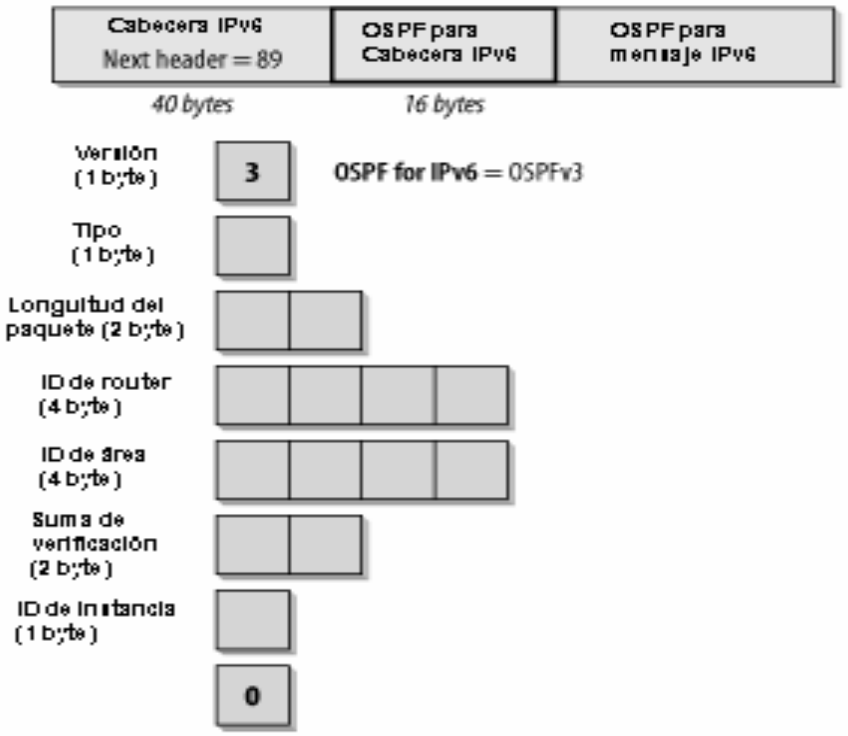


Figura 2.7 Datagrama OSPF

Los campos de la cabecera OSPF se explican a continuación en la siguiente tabla:

Version (1 byte)	OSPF para IPv6 usa la versión número 3
Tipo (1 byte)	Este campo representa el tipo de mensajes OSPF.
Longitud del paquete (2 bytes)	Representa la longitud del paquete del protocolo OSPF en bytes, incluso la cabecera OSPF.
ID de router (4 bytes)	Es la identificación del router que origina este paquete. Cada router debe tener una única ID. La ID de router debe ser unica.
ID de área(4 bytes)	Es la ID del área de la interfaz dónde se origino el OSPF. Identifica el área a que el paquete pertenece. Todos los paquetes de OSPF son asociados con una sola área.
Suma de verificación (2 bytes)	OSPF usa el cálculo de la suma de verificación normal para las aplicaciones de IPv6.
ID de instancia (1 byte)	Identifica la instancia OSPF a la que cada paquete pertenece. El ID de instancia es un número del 8-bits asignado a cada interfaz de ruteo. El valor predefinido es 0. El ID de instancia permite a multiples instancias del protocolo OSPF correr en una sola conexión.

2.8 Seguridades

De forma recurrente vemos cómo se achaca a Internet el hecho de ser un medio de comunicación inseguro. Este es un tema con muchas aristas y que debe ser examinado en cada una de sus partes.

Sin embargo, el problema de seguridad en el nivel de red sigue sin ser tenido en cuenta y comienza a producirse una serie de ataques cada vez más sofisticados y basados en la suplantación de la identidad de máquinas conectadas a la red, dando la posibilidad de violar un acceso prohibido o dando la posibilidad de escudriñar (o desviar) la información a intrusos.

Como respuesta surgen mecanismos de barrera como los cortafuegos, pero los protocolos siguen sin incorporar medidas específicas de seguridad. Pero esto es sólo una parte del

problema. La seguridad integral comprende servicios tanto de confidencialidad como de autentificación, integridad y no rechazo para los que se requieren técnicas criptográfícas que están sujetas a diferentes normativas de exportación y uso en determinados países, lo que hace complicado su uso generalizado en un medio que se tiene por libre (en cuanto a la naturaleza de la información intercambiada y su formato) y homogéneo (en cuanto al tipo de protocolos/aplicaciones empleados).

Se corre el peligro de fracturar la Internet en zonas donde se puedan intercambiar información de forma segura y otras en que no, bien por considerarse tecnología de uso militar, bien por el derecho que se guardan algunos gobiernos a poder intervenir –e interpretar- las comunicaciones de sus ciudadanos.

2.8.1 Seguridad en IPv6

La seguridad es una de las grandes ventajas que presenta IPv6. El nuevo protocolo de comunicación incluye, de forma obligatoria e intrínseca en su núcleo, la especificación de seguridad IPSec.

IPv6 recoge todo lo que hemos aprendido de IPv4, tanto lo bueno como lo malo, y lo mejora. En el caso de la seguridad, el nuevo protocolo utiliza también IPSec como lo hace IPv4. Con IPv6 todo el tráfico de la red va a ser autenticado, vamos a saber quién es el origen, quién el destino, realizando un mejor y más exhaustivo seguimiento de la información y su envío. *[WWW019]*

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 lo contemplan.

Las especificaciones IPSec han sido definidas para trabajar en la capa inferior de la pila (Stack) de protocolos TCP/IP, funcionando por lo tanto en el nivel de datagrama y siendo independientes del resto de protocolos de capas superiores (TCP, UDP...).
La seguridad en IPSec se proporciona mediante dos aspectos de seguridad (Security Payload):

1. Cabecera de autenticación (Authentication Header, **AH**). Esta cabecera es la encargada de proporcionar autenticidad a los datos (datagramas) que se reciben en dos aspectos:
Los datagramas provienen del origen especificado. Se garantiza la autenticidad del origen de los datos (no pueden ser repudiados).
Los datagramas (y por tanto los datos que contienen) no han sido modificados.

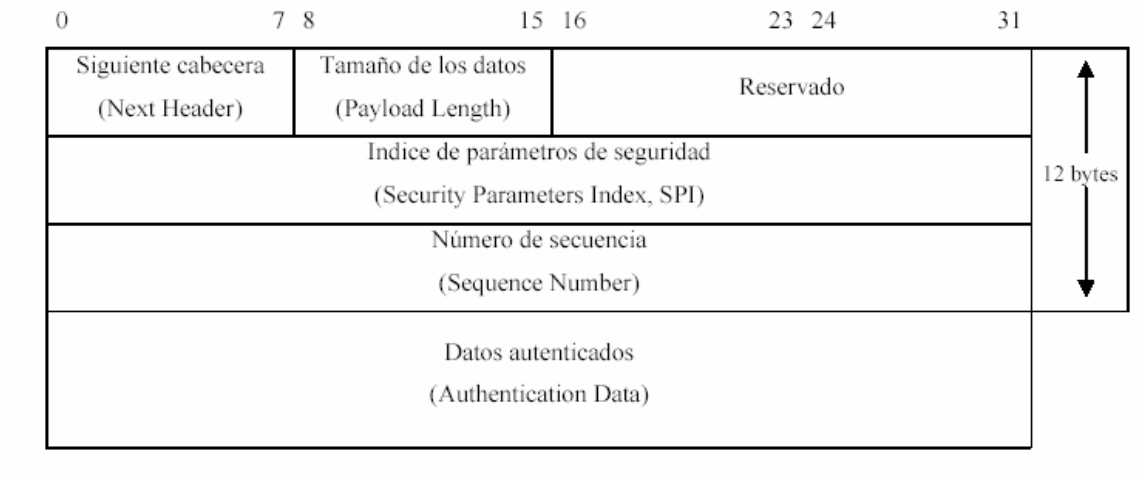


Figura 2.8 Esquema de la cabecera de autenticación (AH).

El **tamaño de los datos** (Payload Length) especifica la longitud de los datos en palabras de 32 bits (4 bytes).
El **índice de parámetros de seguridad** (SPI) es un número de 32 bits, lo que nos permite tener hasta 2^32 conexiones de IPSec activas en un mismo ordenador.

El **número de secuencia** (Sequence Number) identifica en número del datagrama en la comunicación, estableciendo un orden y evitando problemas de entrega de datagramas fuera de orden o ataques externos mediante la reutilización (Replay Attacks) de datagramas
Los **datos autenticados** (Authentication Data) se obtienen realizando operaciones (depende del algoritmo de cifrar escogido) entre algunos campos de la cabecera IP, la clave secreta que comparten emisor y receptor y los datos enviados.

2. Cabecera de cifrado de seguridad (Encrypted Security Payload, **ESP**). De esta forma se arantiza que tan sólo el destinatario legítimo del datagrama (datos) pueda descifrar el contenido del datagrama.
La autenticidad y el cifrado de datos (o datagramas) requiere que tanto el emisor como el receptor compartan una clave, un algoritmo de cifrado/descifrado y una serie de parámetros (como el tiempo de validez de la clave) que diferencian una comunicación segura de otra. Estos parámetros conforman la **asociación de seguridad** (Security Association, SA) que permite unir la autenticidad y la seguridad en IPSec.

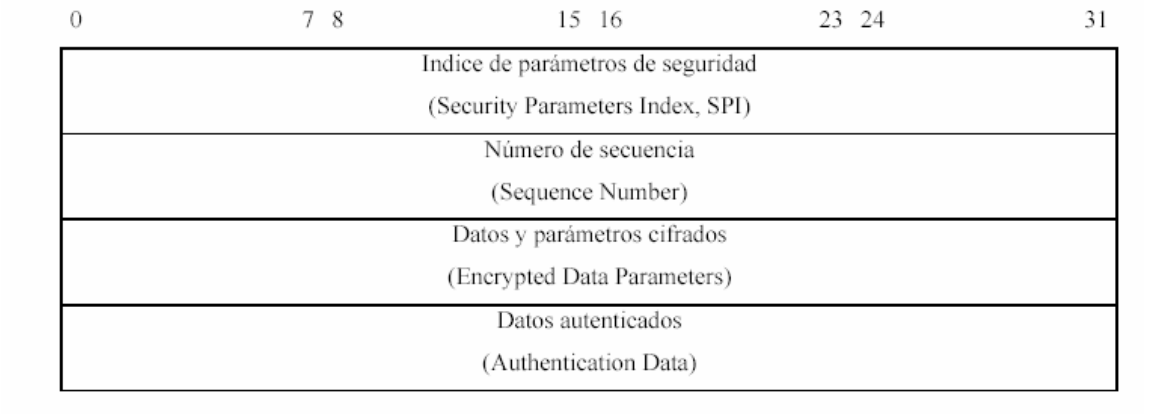


Figura 2.9 Esquema de la cabecera de cifrado de seguridad (ESP)

El **índice de parámetros de seguridad** (SPI) y el **número de secuencia** (Sequence Number) tienen el mismo significado que en la cabecera de autenticación (AH).
Los **datos autenticados** (Authentication Data) aseguran que el texto cifrado no ha sido modificado utilizando un algoritmo de Hash (depende del algoritmo de cifrar escogido).

Debido a que tanto la cabecera de autenticación (AH) como la cabecera de cifrado de seguridad (ESP) pueden ser utilizadas independientemente, se recomienda que en el caso de ser necesario tanto la autenticidad como la privacidad se incluya la cabecera de cifrado tras la de autenticación. De esta forma autenticamos los datos cifrados. *[WWW018]*

En un ordenador con múltiples conexiones (consultar el correo mientras se baja un fichero por FTP y se consulta el saldo bancario...) podemos tener varias asociaciones de seguridad (como mucho una por conexión). Para poder diferenciar entre ellas utilizaremos un **índice de parámetros de seguridad** (Security Parameter Index, SPI) que nos permitirá al recibir un datagrama saber a que asociación de seguridad hace referencia, y de esta forma poder autenticarlo y/o descifrarlo.
Al iniciar una comunicación que utilice los servicios IPSec con un único destino (direcciones unicast) este nos debe comunicar a que índice de parámetros de seguridad (SPI) debemos hacer referencia. Análogamente en una comunicación con varios destinos (direcciones multicast o anycast) todos los destinatarios deben compartir el mismo número de índice (SPI).

Las especificaciones IPSec tienen una gran versatilidad que les permite ser utilizadas en las distintas soluciones adoptadas actualmente en INTERNET (comunicación entre distintos ortafuegos (Firewalls), configuración de ordenadores móviles...). El procedimiento de autenticación permite que junto al protocolo de vecindad (Neighbor Discovery Protocol) se puedan asegurar intercambios seguros entre los distintos routers, evitando la intercepción de los datagramas. Una de las soluciones más adoptadas actualmente para la implementación de la seguridad en INTERNET es el uso de Firewalls. Este esquema de actuación consiste en no permitir un acceso directo de los ordenadores a INTENET, colocando una máquina intermedia (denominada cortafuegos o Firewall) que mediante un sencillo conjunto de reglas filtra todo el tráfico de INTERNET (entrante y saliente).

La nueva configuración que se propone con la ayuda de las especificaciones IPSec consiste en realizar un túnel virtual seguro (Secure Tunnel) de forma que dos firewalls estén virtualmente conectados a través de INTERNET de una forma transparente para los

usuarios. De esta forma, el intercambio de información vendrá regulado por una comunicación entre los dos firewalls mediante datagramas IP versión 6 encapsulados en datagramas IP versión 6 autenticados (y cifrados si se requiere privacidad).

Las comunicaciones entre dos organizaciones (supongamos para nuestro ejemplo el MIT y la UAB) son realizadas de forma transparente y segura a través de los firewalls.

Cuando un ordenador de la UAB desea conectarse a uno del MIT, envía el datagrama correspondiente al firewall. Este se encarga de encapsularlo en un datagrama auténtico (y cifrado si se desea privacidad) y enviarlo al otro extremo del ***túnel*** por INTERNET. Al recibir el firewall del MIT este datagrama, comprueba su autenticidad, lo descifra (si es necesario), lo desencapsula y lo envía al ordenador correspondiente. De esta forma tan sencilla podemos proporcionar un canal seguro y auténtico entre dos puntos cualesquiera conectados a INTERNET.

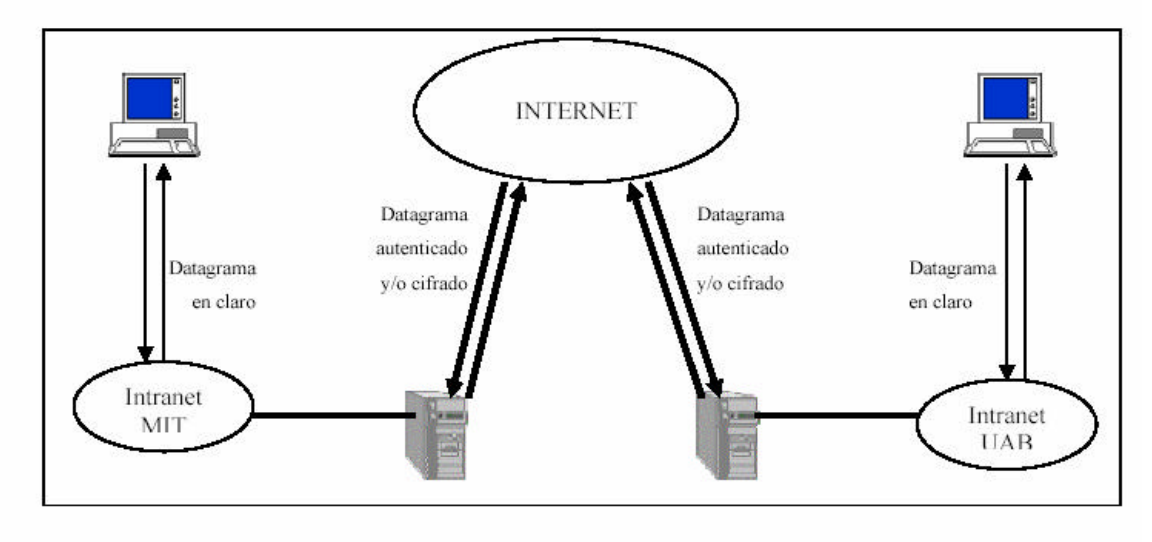


Figura 2.10 Esquema de seguridad proporcionado por IPSec

2.9 Organismos administradores, políticas de distribución y asignación de direcciones IPv6.

Las motivaciones para revisar la política provisional para IPv6 de 1999 comenzaron con la reunión de APNIC celebrada en Taiwán en agosto de 2001. Discusiones sucesivas se mantuvieron en octubre de 2001 en las reuniones de RIPE y ARIN.

Durante éstos encuentros los participantes reconocieron la urgente necesidad de políticas más completas y detalladas. Uno de los resultados de los encuentros fue el establecimiento de una lista de discusión para debatir una política revisada en forma conjunta con el deseo de desarrollar una política general que todos los RIRs puedan utilizar. En éste documento no se dan detalles de las discusiones individuales que condujeron a las políticas descriptas en el mismo; información detallada acerca de estas puede encontrarse en las minutas de cada uno de los meetings que se encuentran en los siguientes sitios web:www.apnic.net, www.arin.net, y www.ripe.net. *[LIB003]*

Las direcciones Ipv6 son un recurso público que debe ser manejado considerando los intereses a largo plazo de la comunidad de Internet. Aunque los registros regionales adopten políticas de asignación de acuerdo a sus propios procesos internos, las políticas de direcciones deben ser uniformes entre los registros. Tener políticas significativamente variadas en las diferentes regiones no es deseable pues puede conducir a situaciones donde puede ocurrir el ¨registry shopping" con organizaciones solicitando direcciones a los registros que tengan las políticas más favorables para sus intereses particulares. Esto puede conducir a que las políticas en una región socaven los esfuerzos de registros de otras regiones con respecto a la prudente administración del espacio de direcciones. En los casos en que las variaciones regionales de las políticas sean razonablemente necesarias el abordaje preferido es el de presentar el tema a los otros registros regionales para lograr un acercamiento de consenso que todos los registros apoyen.

Comparado con Ipv4, el Ipv6 tiene un aparente interminable espacio de direcciones. Si bien esto es superficialmente cierto, políticas de adjudicación de poca visión y desperdicio pueden resultar en la adopción de prácticas que conduzcan a un prematuro vaciamiento del espacio de direcciones.

Debe notarse que el espacio de direcciones de 128 bit es dividido en tres partes lógicas, con el uso de cada componente administrado en forma diferente. Los 64 bits de más a la derecha, el Interface Identifier, será frecuentemente un globalmente único IEEE identifier (por ej., mac address). Aunque ésta sea una forma "ineficiente" de usar el campo Interface Identifier, desde el punto de vista de maximizar el número de nodos direccionables, el esquema de numeración fue explícitamente elegido para simplificar la Stateless Address

Autoconfiguration. Los 16 bits del medio de una dirección indican el ID de la subred. Por este campo será frecuentemente utilizado en forma ineficiente, pero los beneficios operacionales de un ancho de campo de subred regular fueron considerados para compensar las desventajas. Las decisiones para utilizar en forma ineficiente los bits hacia la derecha de /48 fueron hechas bajo el conocimiento y la presunción de que los bits a la izquierda de /48 serían prudentemente administrados. Si así se hace, esto será conveniente para la esperada duración de IPv6.

2.9.1 Definiciones

Los siguientes términos y sus definiciones son de gran importancia para la comprensión de los objetivos, contextos y políticas descriptas en este documento. La responsabilidad de la administración del espacio de direcciones de IPv6 está distribuida globalmente de acuerdo con la estructura jerárquica que se muestra debajo.

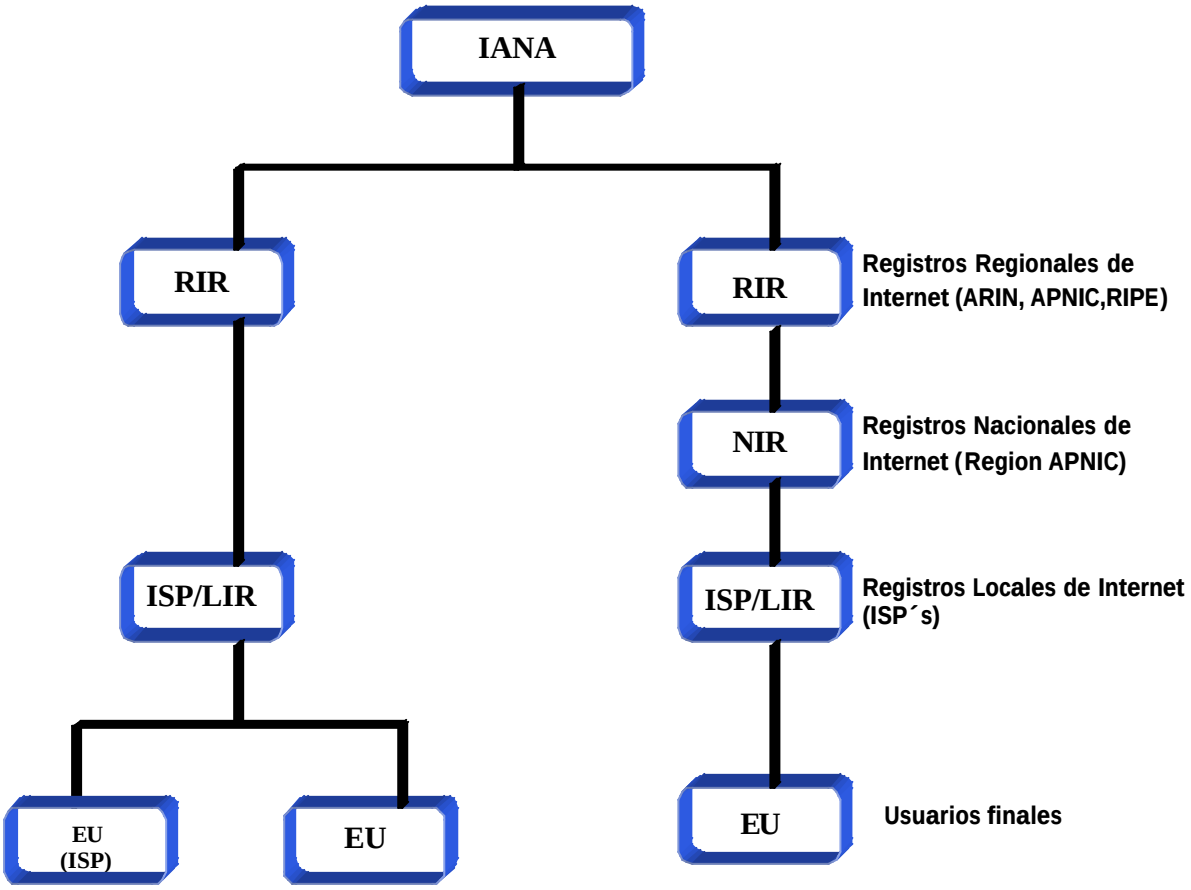


Figura 2.11 Estructura jerárquica de la administración del espacio de direcciones IPv6

2.9.2 Registro de Internet (IR)

Un Internet Registry (IR) es una organización responsable de la distribución de espacios de direcciones IP a sus miembros o clientes y de la registración de esa distribución. Los IRs están clasificados de acuerdo a su función principal y alcance territorial dentro de la estructura jerárquica delineada en la figura de arriba.

2.9.3 Registros Regionales de Internet (RIR)

Los Regional Internet Registries (RIRs) son establecidos yautorizados por las comunidades regionales respectivas, y reconocidos por el IANA para servir y representar grandes regiones geográficas. El rol principal de los RIRs es administrar y distribuir el espacio de direcciones público de Internet dentro de las respectivas regiones.

2.9.4 Registros Nacionales de (NIR)

Un National Internet Registry (NIR) adjudica, principalmente, espacios de direcciones a sus miembros o constituyentes, los cuales son generalmente LIRs a un nivel nacional. Los NIRs existen mayormente en la región de Asia Pacífico.

2.9.5 Resgistros Locales de Internet (LIR)

Un Local Intenet Registry (LIR) es un IR que asigna, principalmente, espacios de direcciones a los usuarios de los servicios de red que éste provee. Los LIRs son generalmente ISPs, cuyos clientes sonprincipalmente usuarios finales y posiblemente otros ISPs.

2.9.6 Adjudicar

Adjudicar significa distribuir el espacio de direcciones a los IRs con el propósito de que ellos realicen la subsiguiente distribución.

2.9.7 Asignar

Asignar significa delegar espacio de direcciones a un ISP o usuario final, para su uso específico dentro de la infraestructura de Internet que ellos operan. Las asignaciones deben ser realizadas solamente para los propósitos específicos documentados por organizaciones específicas y no para ser sub-asignadas a otras partes.

2.9.8 Utilización

A diferencia de Ipv4, IPv6 es generalmente asignado a end sites en cantidades fijas (/48). La utilización real de direcciones dentro de cada asignación será bastante baja comparada con las asignaciones de Ipv4. En IPv6, "utilización" es medida en términos de los bits a la izquierda del límite /48. En otras palabras, la utilización se refiere a la asignación de /48s a los end sites, y no al número de direcciones asignadas dentro de /48s individuales en esos end sites.

2.9.9 HD-Ratio

El HD-Ratio es un modo de medir la eficiencia de asignación de direcciones. Es una adaptación del H-Ratio, y es expresado de la siguiente manera:

$$HD = \frac{\text{Log (numero de objetos adjudicados)}}{\text{Log (número máximo de objetos adjudicables)}}$$

donde, los objetos son direcciones IPv6 de sites (/48s) asignadas desde un prefijo IPv6 de un tamaño dado.

2.9.10 Usuarios Finales

Un end site es definido como un usuario final (suscriptor) que tiene una relación de negocios con un proveedor de servicios que involucra:

- Al proveedor de servicios asignando un espacio de direcciones al usuario final

- Al proveedor de servicios otorgando un servicio de tránsito para el usuario final hacia otros sites
- Al proveedor de servicios transportando el tráfico del usuario final
- Al proveedor de servicios anunciando un prefijo de ruta agregado que contiene la asignación del usuario final

2.9.11 Objetivos de la administración del espacio de direcciones IPv6

El espacio de direcciones IPv6 es un recurso público que debe ser administrado de manera prudente teniendo en cuenta los intereses de Internet a largo plazo. Una administración responsable del espacio de direcciones involucra balancear un conjunto de objetivos que a veces compiten entre sí. *[LIB010]*

Los siguientes son los objetivos relevantes para la política de direcciones de IPv6.

Unicidad

Cada asignación y/o adjudicación del espacio de direcciones debe garantizar la unicidad en todo el mundo. Este es un requerimiento indispensable para asegurar que cada host público en Internet pueda ser identificado unívocamente.

Registro

El espacio de direcciones de Internet debe ser registrado en una base de datos accesible por miembros autorizados dentro lacomunidad de Internet. Esto es necesario para asegurar la unicidad de cada dirección de Internet y para proveer información de referencia sobre los problemas de Internet en todos los niveles, desde los RIRs e IRs hasta los usuarios finales.

El objetivo del registro debería ser aplicado dentro del contexto consideraciones de privacidad razonables y leyes aplicables.

Agrupación

Cuando sea posible, el espacio de direcciones debería ser distribuido de manera jerárquica, de acuerdo a la topología de la infraestructura de la red. Esto es necesario para permitir la agregación de información de ruteo por parte de los ISPs, y para limitar la expansión de las tablas de ruteo en Internet. Esta meta es particularmente importante en el direccionamiento

de IPv6, donde el tamaño del espacio de direcciones total tiene implicaciones significativas tanto para el ruteo interno como externo.

Las políticas de direcciones IPv6 deberían buscar evitar la fragmentación de los rangos de direcciones. Más aún, los RIRs deberían aplicar prácticas para maximizar el potencial de que las adjudicaciones subsecuentes sean contiguas con las adjudicaciones que poseídas actualmente. Sin embargo, no puede haber garantías de adjudicación contigua.

Conservación

Aunque IPv6 provee un espacio de direcciones extremadamente grande, las políticas de direcciones deberían evitar su desperdicio innecesario. Los pedidos de espacios de direcciones deberían estar avalados por documentación apropiada y debería evitarse la acumulación de direcciones no utilizadas.

Equidad

Todas las políticas y prácticas relacionadas al uso del espacio de direcciones públicas deberían aplicarse justa y equitativamente a todos los miembros potenciales y existentes de la comunidad de Internet, independientemente de su ubicación, nacionalidad, tamaño o cualquier otro factor.

Minimización de sobrecarga

Es deseable minimizar la sobrecarga asociada a la obtención de espacio de direcciones. La sobrecarga incluye la necesidad de solicitar espacio adicional a los RIRs muy frecuentemente, la sobrecarga asociada con la administración de espacios de direcciones que crecen vía expansiones sucesivas de pequeños de incrementos en lugar de a través de menos expansiones, más grandes.

Conflicto entre objetivos

Los objetivos descriptos arriba a menudo entrarán en conflicto unos con otros, o con las necesidades individuales de los IRs o usuarios finales. Todos los IRs, al evaluar los pedidos de adjudicación y asignación deben juzgar, buscando balancear las necesidades de los solicitantes con las necesidades de la comunidad de Internet como un todo.

En la política de direcciones de IPv6, el objetivo de agregación es considerado el más importante.

2.9.12 Principios de la política IPv6

Para cumplir con los objetivos descritos en la sección anterior, las políticas que a continuación mencionamos, discuten y siguen los principios básicos descritos en cada una de ellas.

2.9.12.1 Espacio de direcciones no debe ser considerado propietario

Es contrario a los objetivos mencionados y no se encuentra entre los intereses de la comunidad de Internet en su conjunto que los espacios de direcciones sean considerados propietarios.

Las políticas se basan en el entendimiento de que el espacio globalmente-único de direcciones ***unicast*** de IPv6 es licenciado para su uso en lugar de adueñado. Específicamente, las direcciones IP serán adjudicadas y asignadas en base a una licencia, con licencias sujetas a renovación periódica. La otorgación de una licencia esta sujeta a condiciones específicas a aplicarse al comienzo como así también en cada renovación de la misma. *[WWW009]*

Los RIRs generalmente renovarán las licencias automáticamente, siempre que las organizaciones solicitantes hagan un esfuerzo de buena-fé para cumplir con el criterio bajo el cuál calificaron o fueron otorgadas una adjudicación o asignación. Sin embargo, en aquellos casos en que una organización no está utilizando el espacio de direcciones como se espera, o está mostrando mala fé en regirse por las obligaciones asociadas, los RIRs se reservan el derecho de no renovar la licencia.

Hay que notar que cuando una licencia es renovada, la nueva licencia será evaluada y controlada bajo las políticas de direcciones de IPv6 aplicables en el lugar y momento de la renovación, las cuales podrían diferir de las políticas bajo las cuales fue originalmente adjudicada o asignada.

2.9.12.2 Rutabilidad no garantizada

No hay garantías de que la adjudicación o asignación de una dirección será ruteable globalmente. Sin embargo, los RIRs deben aplicar procedimientos que reduzcan la posibilidad de fragmentación del espacio de direcciones, lo que podría llevar a la pérdida de ruteabilidad.

2.9.12.3 Adjudicación Mínima

Los RIRs aplicarán un tamaño mínimo para adjudicaciones de IPv6 para facilitar el filtro basado en el prefijo. El tamaño mínimo de adjudicación para un espacio de direcciones IPv6 es /32.

2.9.12.4 Consideraciones de la infraestructura de IPv4

Cuando un proveedor de servicios de Ipv4 pide espacio IPv6 para una transición final de servicios existentes a IPv6, el número de clientes actuales de Ipv4 podría ser usado para justificar un pedido más grande del que estaría justificado si el mismo estuviera basado solamente en la infraestructura IPv6.

2.9.13 Políticas para adjudicaciones y asignaciones

2.9.13.1 Criterio de adjudicación inicial

Para calificar para la adjudicación inicial de un espacio dedirecciones IPv6, una organización debe:

a) ser un LIR;

b) no ser un end site;

c) planear proveer conectividad IPv6 a organizaciones a las cuales asignará /48s, anunciando esa conectividad a través de su única dirección agregada de adjudicación; y

d) tener un plan para realizar al menos 200 asignaciones de /48 a otras organizaciones dentro de un período de 2 años.

2.9.13.2 Tamaño de adjudicación inicial

Las organizaciones que cumplan con el criterio de adjudicación inicial pueden recibir un mínimo de adjudicaciones de /32. Las organizaciones podrían calificar para una

adjudicación inicial más grande que /32 entregando documentación que justifique razonablemente el pedido. Si así lo hicieran, el tamaño de adjudicación estará basado en el número de usuarios existentes y en la extensión de la infraestructura de la organización.

2.9.13.3 Adjudicación subsiguiente

Las organizaciones que ya tengan una adjudicación IPV6 pueden recibir adjudicaciones subsiguientes de acuerdo a las siguientes políticas.

Criterio de alocación subsiguiente

La adjudicación subsiguiente será provista cuando una organización (ISP/LIR) satisfaga el umbral de evaluación de utilización histórica de direcciones en términos del número de sites en unidades de asignaciones de /48. El HD-Ratio es usado para determinar los umbrales de utilización que justifican la adjudicación de direcciones adicionales.

HD-Ratio aplicado

El valor HD-Ratio de 0.8 es adoptado como una aceptable utilización de direcciones para justificar la adjudicación de espacio de dirección adicional.

Tamaño de la adjudicación subsiguiente

Cuando una organización ha logrado una aceptable utilización de su espacio de direcciones adjudicado, está inmediatamente calificada para obtener una adjudicación adicional que resulte en una duplicación de su espacio de direcciones adjudicado. Cuando sea posible, la adjudicación será realizada de bloques de direcciones adyacentes, es decir que su adjudicación existente es extendida un bit hacia la izquierda. Si una organización necesita más espacio de direcciones, debe proveer documentación justificando sus requerimientos para un período de 2 años. La adjudicación se basará en este requerimiento.

2.9.13.4 Adjudicación de LIR a ISP

No hay una política específica para la adjudicación de espacio de direcciones de una organización (LIR) a los ISPs subordinados. Cada LIR podría desarrollar su propia política para ISPs subordinados para alentar una utilización óptima del bloque de direcciones total

adjudicado al LIR. Sin embargo, todas las asignaciones de /48 a end sites deben ser registradas por el LIR o por sus ISPs subordinados de modo que el RIR/NIR puede evaluar apropiadamente el HD-Ratio cuando es necesaria una adjudicación subsiguiente.

2.9.14 Asignación

Los LIRs deben realizar asignaciones IPV6 de acuerdo con las siguientes provisiones.

Asignación del espacio de direcciones

Las asignaciones deben ser realizadas de acuerdo con las recomendaciones existentes, las cuales resumimos aquí como:

- /48 en el caso general, excepto para suscriptores muy grandes
- /64 cuando cuando se conoce por diseño que una y solo una subred es necesaria
- /128 cuando se conoce absolutamente que uno y solo un dispositivo se está conectando.

A los RIRs/NIRs no les concierne el tamaño de direcciones que los LIR/ISP realmente asignan. Por lo tanto, los RIRs/NIRs no pedirán información detallada sobre redes de usuarios IPV6 como lo hicieron en Ipv4.

Asignación de multiples /48s a un solo site

Cuando un solo end site requiere un bloque de direcciones de /48 adicional, debe pedir la asignación con documentación o materiales que justifiquen el pedido. Los pedidos de bloques múltiples o adicionales de /48s serán procesados y revisados (ej: evaluación de la justificación) al nivel de los RIR/NIR.

Asignación a la infraestructura del operador

Una organización (ISP/LIR) puede asignar un /48 por PoP como un servicio de infraestructura de un operador de servicio IPv6. Cada asignación a un PoP es considerada como una asignación sin tener en cuenta el número de usuarios que usen el PoP. Puede obtenerse una asignación separada para operaciones propias del operador.

2.9.15 Registración

Cuando una organización que posee una adjudicación de espacio IPv6, hace asignaciones de espacios IPv6, debe registrar la información de asignaciones en una base de datos accesible a los RIRs como corresponde (la información registrada por un RIR/NIR puede ser cambiada en el futuro por una base de datos para registrar manejo de direcciones). La información es registrada en unidades de redes /48 asignadas. Cuando a una organización se le asigna más de una /48 la organización que la asigna es responsable de asegurar que el espacio de direcciones esté registrado en una base de datos RIR/NIR. Los RIR/NIRs usarán los datos registrados para calcular el HD-Ratio en el momento de la solicitud, para subsecuentes adjudicaciones y para verificar eventuales cambios en las asignaciones.

Los IRs deben mantener sistemas y prácticas que protejan la seguridad de la información personal y comercial que es usada en la evaluación de solicitudes, pero que no es requerida para registración pública. *[WWW008]*

2.9.16 Reverse lookup

Cuando un RIR/NIR delega espacio de direcciones Ipv6 a una organización, también está delegando la responsabilidad de manejar la zona de reverse lookup que corresponde al espacio de direcciones IPv6 asignado. Cada organización debe manejar debidamente su zona de reverse lookup. Cuando una organización hace una asignación de direcciones, debe delegar a la organización asignada, bajo pedido, la responsabilidad de manejar la zona de reverse lookup que corresponde a la dirección asignada.

2.9.17 Poseedores de IPv6 ya existentes

Las organizaciones que hayan recibido adjudicaciones de IPv6 /35 bajo la política previa de IPv6 están inmediatamente autorizadas a expandir su asignación a un bloque de direcciones /32 sin necesidad de justificación, siempre y cuando satisfagan los criterios del el bloque o de direcciones , /32 contendrá el bloque más pequeño ya adjudicado (uno o múltiples /35 bloques en muchos casos) que ya ha sido reservado por el RIR para una subsecuente asignación a la organización. Las solicitudes de espacio adicional más allá del mínimo tamaño /32 serán evaluadas.