IP versión 6 (Parte 03) - Encabezado.

Madrid, setiembre de 2013.

Por: Alejandro Corletti Estrada (acorletti@darFe.es - acorletti@hotmail.com)

1. Presentación.

Este tercer artículo de la serie presenta cómo está definido y se debe trabajar con el encabezado de IP versión 6. Como iremos viendo, en virtud de su nuevo esquema de direccionamiento, en que varios de sus campos son nuevos, otros que modifican su funcionalidad y algunos que son eliminados, se genera bastante documentación al respecto. Hemos intentado resumir todo lo posible, centrándonos en los aspectos de mayor importancia, y como siempre manteniendo un formato eminentemente técnico, basado en las RFC que lo regulan.

2. Introducción.

El desarrollo se basará en una serie de RFCs, que son las siguientes:

- **RFC 2460** Internet Protocol, Version 6 (IPv6) Specification
- **RFC 2474** Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
- **RFC 2780** IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers
- **RFC 4727** Experimental Values In IPv4, IPv6, ICMPv4, ICMPv6, UDP, and TCP Headers
- **RFC 5871** IANA Allocation Guidelines for the IPv6 Routing Header
- **RFC 6564** A Uniform Format for IPv6 Extension Headers

3. Desarrollo.

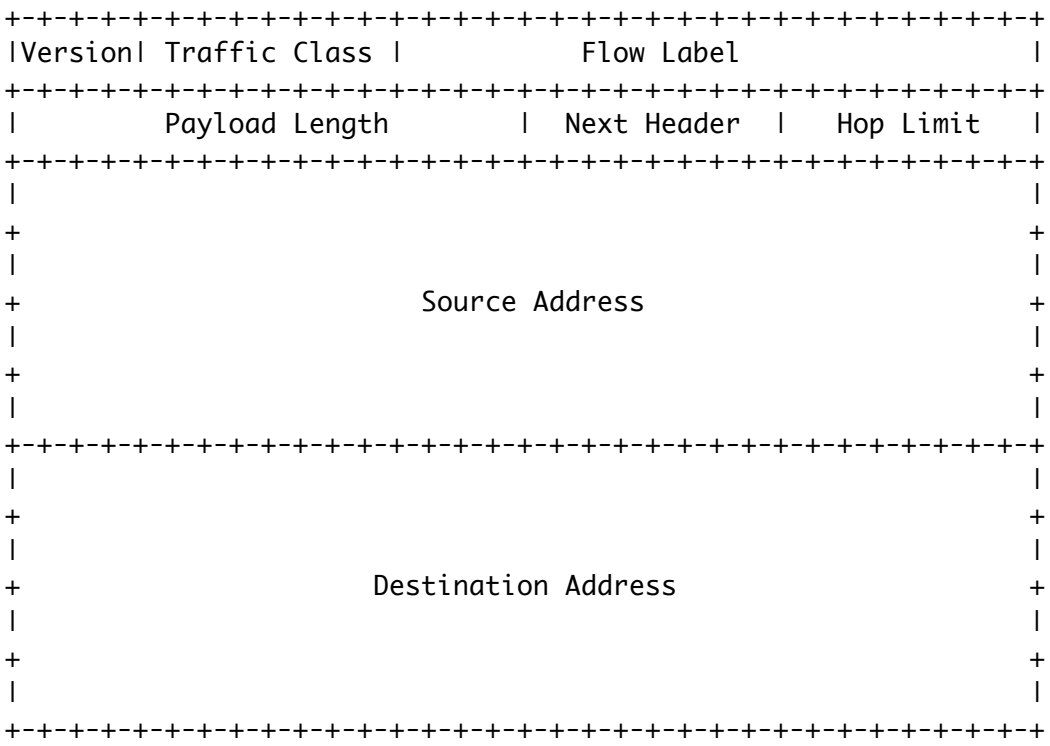
3.1. La **RFC 2780** "*IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers*".

Vamos a iniciar este artículo con la sola mención de esta RFC de marzo del año 2000 pues es la que deberíamos tomar como referencia inicial y guía para comprender todos los campos de este encabezado del protocolo IP (tanto en su versión 4 como en la 6), la misma es una especie de guía con definiciones y referencias de todos los valores y significados de los campos que componen este encabezado, a partir del **punto 5**. "*IANA Considerations for fields in the IPv6 header*" es donde encontrarás todos estos aspectos.

No merece la pena que le dediquemos tiempo en este artículo pues sería una traducción textual de la misma. Nuestro consejo es que cada vez que necesites ampliar un tema o comprender con mayor detalle algún significado del encabezado de IPv6, te dirijas a esta RFC y comiences por aquí tu búsqueda.

3.2. La **RFC 2460** "*Internet Protocol, Version 6 (IPv6) Specification*".

Al principio de esta RFC nos comenta un poco la evolución desde la versión 4, luego habla de su Terminología (merece la pena darle una mirada a este aspecto), pero nosotros nos centraremos a partir del punto 3. "*IPv6 Header Format*" de la misma donde nos presenta su encabezado de la siguiente forma:



Se puede apreciar que está agrupado en bloques de 32 bits por línea, separando varios campos, describe cada uno de ellos de la siguiente manera:

- Version: 4 bit donde debe figurar el valor "6".
- Traffic Class: 8 bit que se describen en la sección 7 de esta RFC.
- Flow Label: 20 bit que se describen en la sección 6 de esta RFC.
- Payload Length: 16 bit (entero sin signo). Se trata de la longitud del campo de datos (Payload de IPv6) en octetos. Se debe tener en cuenta aquí que cualquier "cabecera en extensión" que esté presente, será considerada también "payload" por lo tanto incluida también en este campo.
- Next Header: 8 bit selector. Identifica el protocolo que tiene en su nivel inmediatamente superior. Emplea los mismos valores que IPv4.
- Hop Limit: 8 bit (entero sin signo). Al igual que IPv4 este valor es decrementado en 1 por cada "salto" que pase, al llegar a cero, el paquete es descartado.
- Source Address: 128 bit que identifican la dirección origen.
- Destination Address: 128 bit que identifican a la dirección destino.

A continuación presentamos un ejemplo de este encabezado:

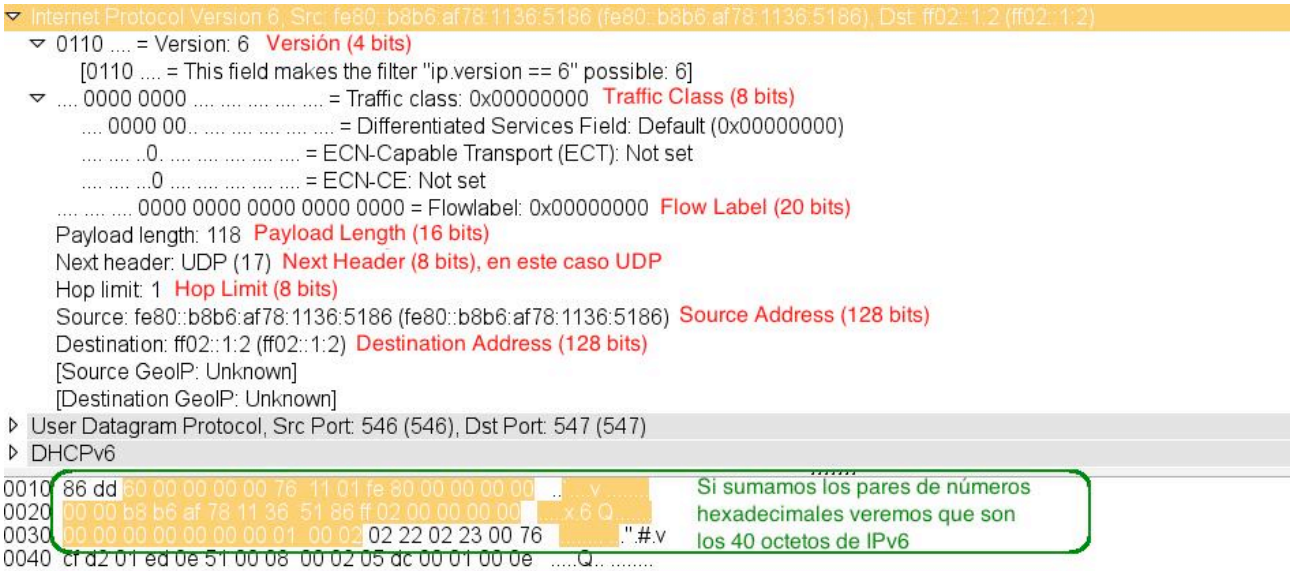
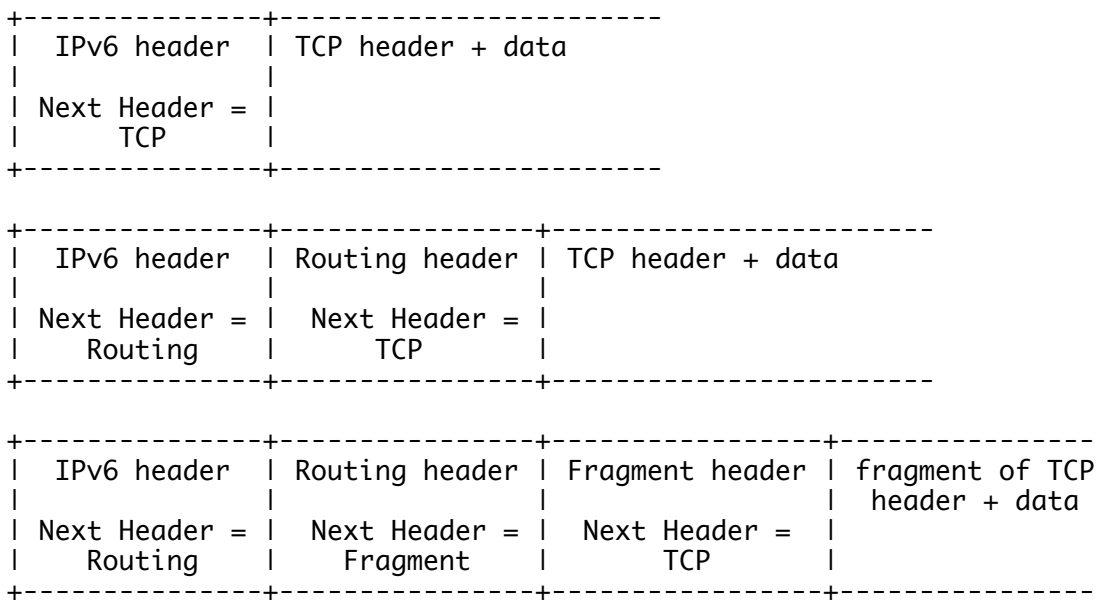


Imagen 1: En esta imagen, se puede apreciar la captura de un encabezado básico de **IPv6**, hemos aclarado en **rojo** cada uno de sus campos, y en **verde** si se desea corroborar el tamaño de 40 Bytes de este encabezado básico.

Esta RFC-2460 continúa en el **punto 4**. "*IPv6 Extension Headers*" desarrollando el funcionamiento de estos "Encabezados de extensión". En IPv4, lo realizaba a través del campo "*Opciones*", como parte del encabezado IPv4 (de hecho, luego de los primeros cuatro bits de IPv4 que se corresponden al campo "Versión", en IPv4 vienen cuatro bits más que identifican la "*Longitud de Cabecera*" en palabras de 4 Bytes, cosa que ya no es así en IPv6). IPv6 define que estos "Encabezados de Extensión" son información

adicional, encapsulada en encabezados separados que pueden ubicarse entre el encabezado de IPv6 y el del nivel superior. Para ser estricto con el funcionamiento de un modelo de capas, esto suena medio "chocante", pero así se ha definido y no hay más que hablar. Entonces, lo que estamos diciendo con los "Encabezados de Extensión" para entenderlo con sencillez, es que se trata de una especie de "nuevo encabezado" que se sitúa entre el nivel de red y el de transporte.

Continuando con el punto 4 de esta RFC, este menciona que hay un pequeño número de estos encabezados identificados por un valor que ya está definido y se insertará en el campo de 8 bits "*Next Header*" que acabamos de mencionar, y aclara que IPv6 puede soportar: cero, uno, o más de estos encabezados; cada uno de ellos deberá ser identificado por el campo "Next Header" del precedente encabezado (sea el básico o cada uno de los encabezados de extensión que se agreguen), poniendo los siguientes ejemplos:



Estos encabezado de extensión no son examinados en ningún nodo intermedio, es decir sólo los analizan los nodos destino (sea uno sólo cuando es Unicast, o sean varios en el caso de Multicast). La única excepción a este análisis intermedio es el encabezado de extensión: "**Salto a Salto**" , que DEBE encontrarse inmediatamente a continuación del encabezado básico y su existencia queda identificada por el valor "**cero**" en el campo "*Next Header". (*Más adelante en este texto, veremos que en la actualidad este aspecto tiene sus excepciones).

Cada "Encabezado de extensión" debe tener una longitud múltiplo de 8 octetos (o Bytes) para mantener la "alineación" en 8 Bytes del siguiente encabezado (en IPv4 es similar, pero en múltiplos de 4 Bytes).

IPv6 a fecha de hoy tiene definido los siguientes encabezados de extensión:

- Hop-by-Hop Options
- Routing (Type 0: este es el único "tipo" de Routing, que como veremos más

adelante está definido por esta RFC)

- Fragment
- Destination Options
- Authentication
- Encapsulating Security Payload

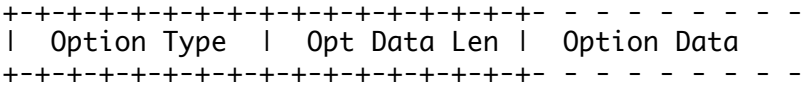
Los primeros cuatro están definidos en esta RFC y los dos últimos en la **RFC-2402** y la **RFC-2406** respectivamente, que desarrollaremos brevemente más adelante y con detalle cuando publiquemos el artículo de "**Seguridad en IPv6**" pues se tratan de IPSec.

Si bien no lo impone, la RFC-2460, recomienda que cuando exista más de un encabezado por extensión dentro de un mismo paquete, los mismos se coloquen en el siguiente orden:

a. IPv6 header
b. Hop-by-Hop Options header
c. Destination Options header
d. Routing header
e. Fragment header
f. Authentication header
g. Encapsulating Security Payload header
h. Destination Options header
i. upper-layer header

Cada Encabezado de extensión debe aparecer como máximo una vez. Con la única excepción de "**Destination Options**" que puede aparecer un máximo de dos veces. También aclara que si el nivel superior es otro encabezado de IPv6 (por ejemplo en túneles IPSec) este nuevamente puede tener sus propios encabezados de extensión

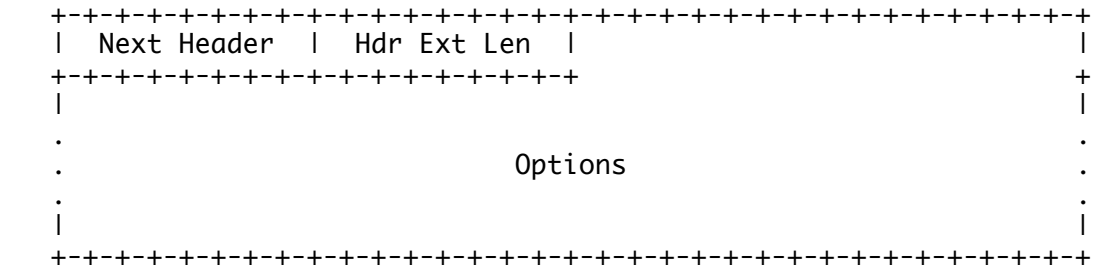
Continuando con la misma RFC, el punto 4.2. "*Options*", explica que hay dos encabezados de extensión (Hop by Hop y Destination Options) cuya longitud es variable, y para identificarla transporta o incorpora un formato especial llamado "*Type-Length-Value* (**TLV**)", que estará inserto dentro del campo "opciones" del encabezado convencional de todo "encabezado de extensión", está definido como se presenta a continuación:



- Option Type: 8-bit que identifican el tipo de Opción.
- Opt Data Len: 8-bit (entero sin signo). Longitud del campo de opción de datos (solo para esta opción). Esta es justamente la longitud mencionada.
- Option Data: datos específicos de esta Opción.

La secuencia de opciones en un encabezado DEBE ser procesada estrictamente en el orden en el que aparecen dentro del mismo, un receptor NO DEBE indagar dentro de un encabezado buscando un valor en particular o una determinada clase de opciones o procesarla.

El punto siguiente 4.3. "***Hop by Hop Options Header***" como su nombre lo indica define como debe ser tratada esta opción de "Salto por Salto", esta opción queda identificada con el valor "**0**" en el campo "Next Header" del encabezado básico de IPv6, y su formato es el siguiente:



- Next Header: 8-bit. Identifica el tipo de encabezado que continúa a este mismo, emplea los mismos valores que IPv4.
- Hdr Ext Len: 8-bit (entero sin signo). Define la longitud de esta cabecera de extensión en unidades de 8 Bytes, sin incluir los primero 8 Bytes.
- Options: Campo de longitud variable. Debe ser un entero múltiplo de 8 bytes donde figure la información de cada salto. Dentro del mismo contendrá uno o más TLV (que acabamos de describir en el párrafo anterior).

A continuación presentamos una imagen donde se puede apreciar cada uno de estos campos:

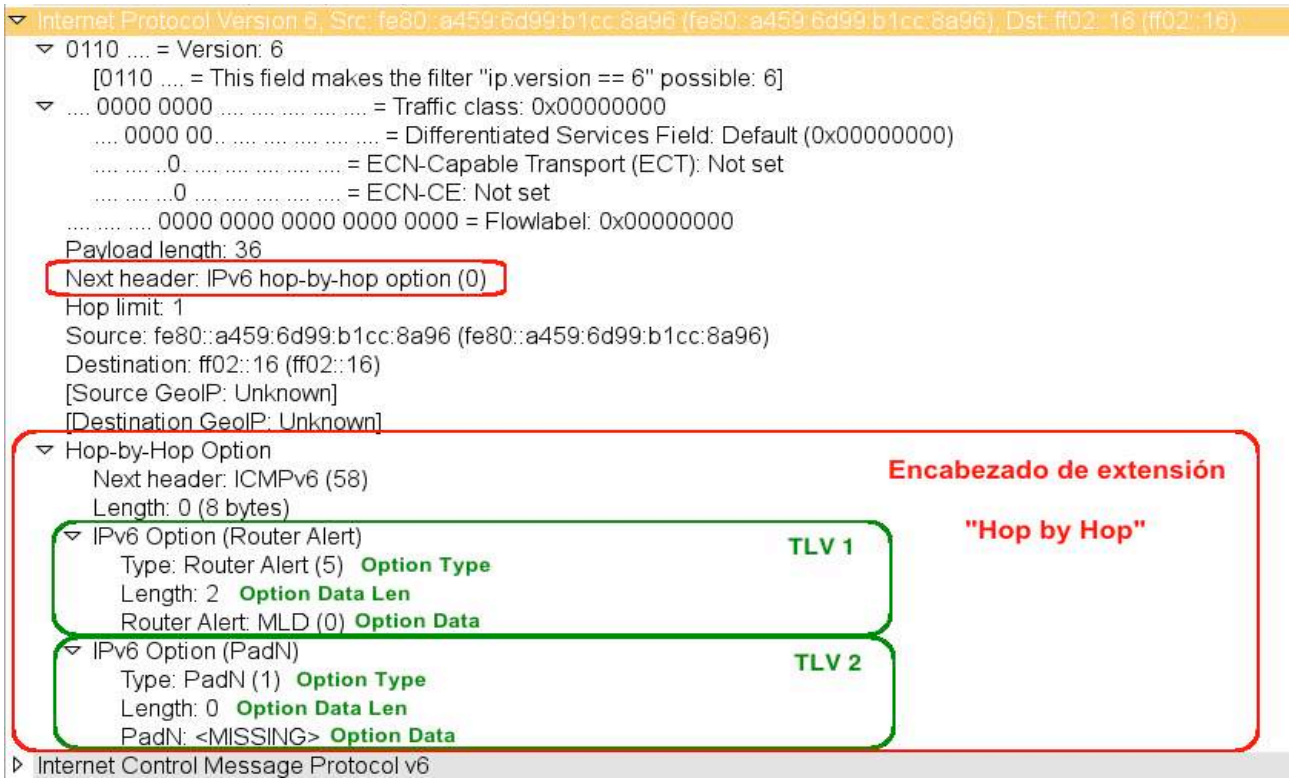
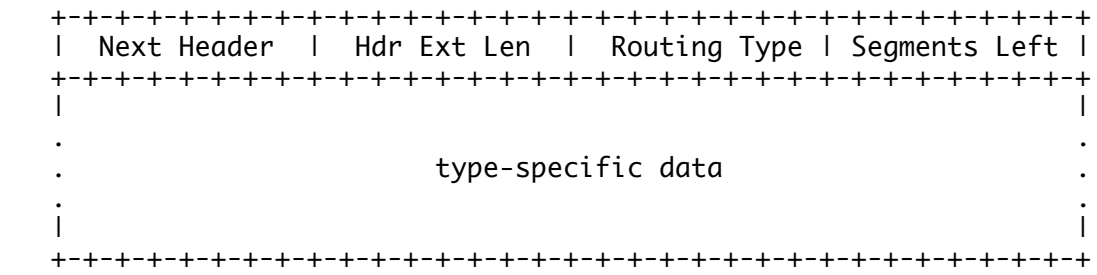


Imagen 2: En esta imagen, se puede apreciar la captura de un encabezado de extensión "**Hop by Hop**", en el cual hemos destacado en **rojo** todos sus campos, y en **verde** los dos TLV que en este caso cuenta el mismo.

Vamos a alterar el orden de esta RFC para cerrar este tema de los encabezados de extensión de longitud variable, es decir el anterior (*Hop by Hop*) y ahora "***Destination Options***" que se describe en el punto 4.6 de la misma. Esta opción se emplea para transportar información opcional que solo debe ser examinada en los nodos destino. Este encabezado en extensión se identifica por al valor "**60**" del encabezado inmediatamente precedente.

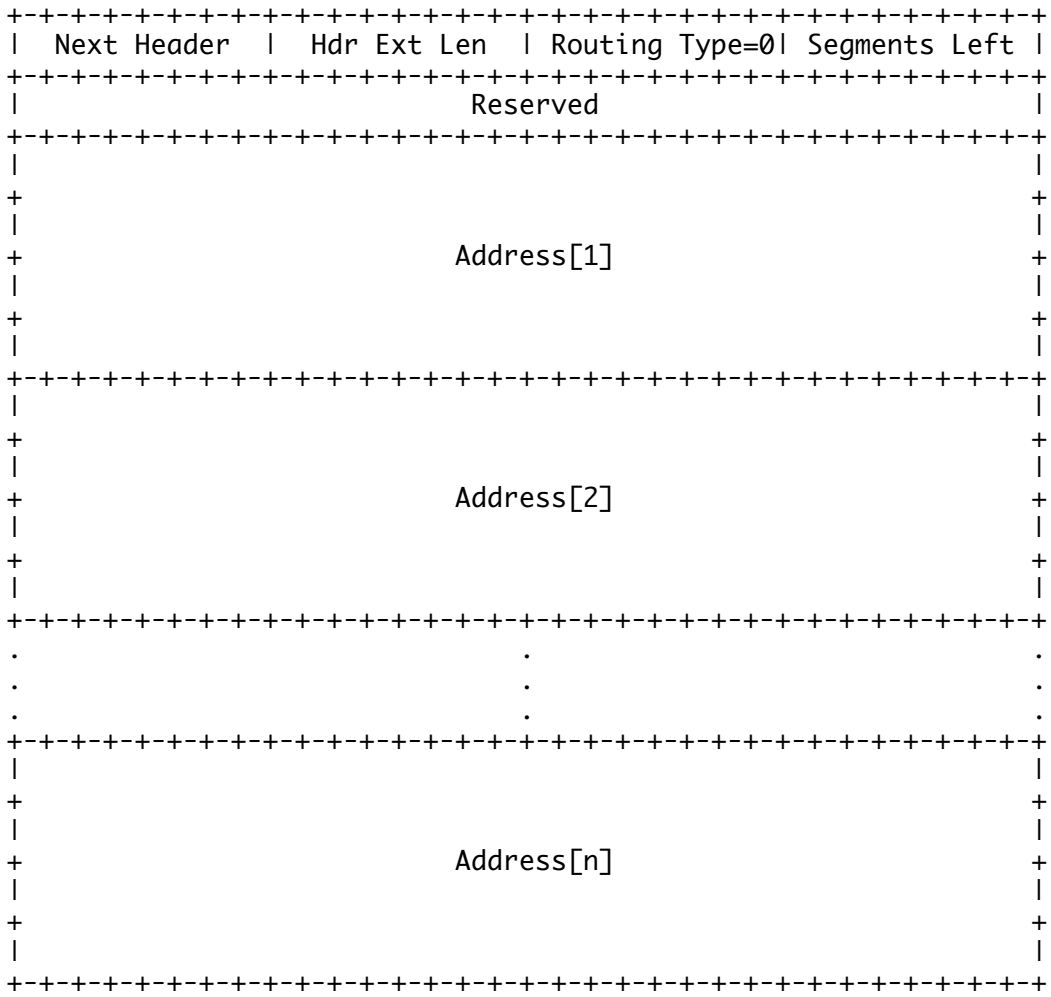
En cuanto al formato de este encabezado es exactamente igual al anterior, así que no nos detendremos en ello.

Volviendo al orden de esta RFC, vamos a desarrollar brevemente los dos encabezados de extensión que siguen la puntuación. El primero de ellos es el que se trata en el punto 4.4 "***Routing Header***" . Se emplea por quien envía el paquete IPv6 para listar uno o más nodos intermedios deben ser visitados en su camino hacia el nodo destino,. Esto en realidad no es ninguna novedad en cuanto a su lógica pues en IPv4 se empleaba de forma similar con las opciones "*Loose Source*" y "*Record Route*". Este encabezado de extensión se lo reconoce por el valor "**43**" en el encabezado inmediatamente precedente, y su formato es el siguiente:



- Next Header: 8-bit. Identifica el tipo de encabezado que continúa a este mismo, emplea los mismos valores que IPv4.
- Hdr Ext Len: 8-bit (entero sin signo). Define la longitud de esta cabecera de extensión en unidades de 8 Bytes, sin incluir los primero 8 Bytes.
- Routing Type: 8-bit. Identifica alguna variante de un encabezado particular de enrutado.
- Segments Left: 8-bit (entero sin signo). Número de segmentos de ruta que completan este encabezado.
- Type-specific data: Campo de longitud variable de formato determinado por el "Routing Type" (que veremos a continuación).

En estos 8-bit de "*Routing Type*", esta RFC sólo define el valor "0" para este campo (tal cual mencionamos al principio de este texto). Para este valor, el formato de este encabezado de extensión es el siguiente:



Como podemos apreciar, los únicos campos nuevos que vemos ahora son:

- Reserved: 32-bit. Que deben ser inicializado a "0" por el nodo origen e ignorados por el receptor.
- Address[1..n]: Vector de 128-bit de direcciones IPv6, numeradas de 1 a n.

En este tipo de enrutado NO DEBEN aparecer direcciones Multicast, ni tampoco en el encabezado básico de estos paquete.

Este encabezado no es examinado o procesado hasta que el mismo alcanza el nodo identificado en el campo "Dirección Destino" del encabezado básico de IPv6. Recién al alcanzar ese nodo, se evalúa la opción "Next Header" del encabezado IPv6 y allí se ejecuta un algoritmo que describe en detalle esta RFC, pero que nosotros lo explicaremos a través del ejemplo que esta recomendación propone y que es el siguiente.

Supongamos que un nodo fuente "**S**" envía un paquete al nodo destino "**D**" empleando el encabezado de extensión "Routing" para que el paquete pase por los nodos intermedios "**I1**, **I2** e **I3**" paquete viaja desde "**S**" hasta "**I1**". Los campos de sus encabezados serían los siguientes:

Primer paquete IPv6:

Source Address = **S** Hdr Ext Len = 6
Destination Address = **I1** Segments Left = **3**
Address[1] = **I2**
Address[2] = **I3**
Address[3] = **D**

Segundo paquete IPv6:

Source Address = **S** Hdr Ext Len = **6**
Destination Address = **I2** Segments Left = **2**
Address[1] = **I1**
Address[2] = **I3**
Address[3] = **D**

Tercer paquete IPv6:

Source Address = **S** Hdr Ext Len = **6**
Destination Address = **I3** Segments Left = **1**
Address[1] = **I1**
Address[2] = **I2**
Address[3] = **D**

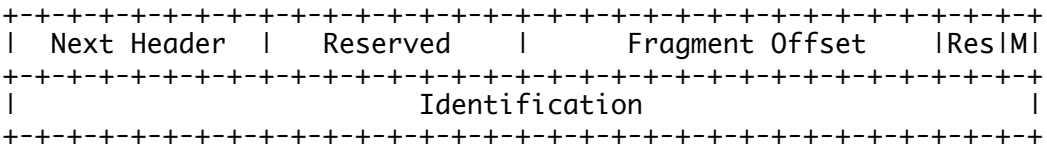
Cuarto paquete IPv6:

Source Address = **S** Hdr Ext Len = **6**
Destination Address = **D** Segments Left = **0**
Address[1] = **I1**
Address[2] = **I2**
Address[3] = **I3**

Es decir, cada nodo intermedio, analiza la dirección destino, cuando se corresponde a la propia, luego procesa "Next Header", al ver que existe la opción "Routing", mira el "Type" si es igual a "0", esta valor es correcto por lo tanto pasa a analizar el campo "Segments Left" (para nosotros es: "**Segmentos restantes**"), sobre la base de ese campo, genera un nuevo encabezado IPv6 básico con este nuevo nodo intermedio como dirección IP destino (reiteramos: dentro del encabezado básico, no en el de extensión) y envía este nuevo paquete hacia el próximo nodo intermedio, decrementando el valor del campo "Segments Left" y "rotando" el orden de los nodos intermedios, este proceso se repite hasta que el valor "Segments Left" es igual a "**0**" que indica que se trata del último paquete y es el nodo destino.

El punto que continúa en esta RFC es el 4.5 "***Fragment Header***", estos encabezados de fragmentación, los emplea nuevamente un nodo fuente para enviar paquetes que recibe de un nivel superior y cuyo tamaño es superior a lo que IPv6 calcula como MTU (Maximun Transfer Unit), que como hemos desarrollado en artículos anteriores, es la metodología que emplea IPv6 para determinar cuál es la cantidad máxima de Bytes que pueden enviar de extremo a extremo de esta ruta entre origen y destino. Nuevamente recalca que a diferencia de IPv4, la fragmentación en IPv6 no puede ser realizada por los routers intermedios, sino únicamente por los nodos origen y destino.

Este encabezado de extensión se reconoce por el valor "44" en el encabezado que inmediatamente lo precede y tiene el siguiente formato:



- Next Header: 8-bit. Identifica el tipo de encabezado que continúa a este mismo, emplea los mismos valores que IPv4.
- Reserved: 8-bit que se corresponde a un campo reservado (es decir que no se deben emplear). Deben ser inicializados a "0" por el transmisor e ignorados en el receptor.
- Fragment Offset: 13-bit (entero sin signo). Se mide en unidades de 8 octetos (64 bits) e indica en que parte del paquete original deben ser "re ensamblados" los datos que aquí están contenidos, por esa razón el primer paquete que transporte los datos fragmentados, llevará el valor "0" en este campo.
- Res: 2-bit otro campo reservado ídem al anterior.
- M flag: Indica si existen más fragmentos o se trata del último fragmento. Cuando su valor es "**1**" = more fragment; Si es "**0**" = last fragment.
- Identification: 32-bits. Este valor será el que identifique a todos los "fragmentos" que formen parte del mismo envío. La RFC sugiere que este valor sea diferente a cualquier otro que se haya generado "recientemente" entre la misma fuente y destino y se define el concepto de "recientemente" (no merece la pena detenernos en ello).

La RFC continúa detallando el funcionamiento de este encabezado de fragmentación, pero nosotros en este artículo no lo haremos pues su lógica funciona exactamente igual que como se hacía en IPv4 (y puede verse con todo detalle en el libro "**Seguridad por Niveles**"), con la única salvedad que:

- Los 3 campos que se emplean para Fragmentación (M Flag, Fragment Offset e Identification) en IPv4 se llamaban igual, pero estaban dentro de los veinte Bytes del encabezado básico.
- De estos mismos 3 campos, los dos primeros tienen la misma longitud, el tercero (Identification) ahora es el doble, en IPv4 era de 16 bits.
- Estos campos sólo "viajan" cuando se emplea encabezado de extensión para Fragmentación. En IPv4 estaban presentes en todos los datagramas pues formaban parte de los 20 bytes de su encabezado mínimo (si no se empleaba fragmentación sus valores eran "0").

NOTA: Un detalle que viene al caso mencionar es que en IPv4 existe otro bit que guarda estrecha relación con esta actividad, se trata del bit "**DF**" (Don`t Fragment). Este bit se empleaba para "ordenar" que ese paquete en concreto no podía ser fragmentado por ningún nodo intermedio (el caso típico, por ejemplo, era el de un "triple Handshake" de su protocolo superior TCP, este caso "sí o sí" deben ser tres paquetes, por lo tanto si en algún nodo intermedio se empleara fragmentación, entonces no se podría lleva a cabo esta secuencia en el nivel superior con el protocolo TCP, por lo tanto los tres datagramas lo ponían a "1"). Como hemos

repetido ya varias veces, en IPv6 sólo pueden fragmentar los nodos origen y destino, por lo que deja de tener sentido el empleo de este bit y por esa razón en IPv6 no existe.

El punto 4.6 de esta RFC, es "Destination Option" que ya lo habíamos desarrollado alterando el orden (para analizar conjuntamente los dos encabezados de extensión de longitud variable: Hop by Hop y Destination Options) así que pasaremos al punto 4.7 " "***No Next Header***" este encabezado se identifica con el valor "**59**" en el campo "Next Header" del encabezado que lo precede inmediatamente, e indica sencillamente que no existe ningún otro encabezado que continúe a este mismo.

A continuación presentamos una imagen de esta caso:

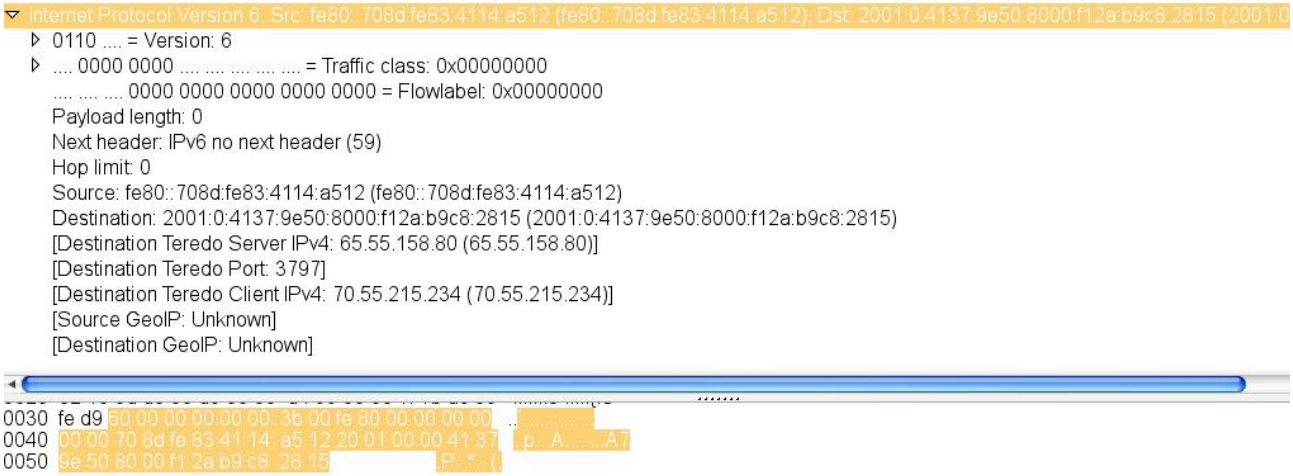


Imagen 3: En esta imagen, se puede apreciar el valor "**59**" (No Next Header) y en la parte inferior, nuevamente resaltado en **naranja** los 40 bytes de este encabezado, donde se ve claramente que allí acaba este paquete, es decir no continúa ningún otro protocolo.

El punto 5. "***Packet Size Issues***" aconseja que se empleen tamaños de paquetes no inferiores a 1280 bytes, y entra en mayores detalles sobre cuándo se aconseja o no fragmentar, no nos detendremos en ello.

El punto 6. "***Flow Labels***", presenta cómo estos 20 bit de "etiquetas de flujo" pueden se empleados por un nodo fuente para especiales solicitudes en el control de las rutas de ese paquete por los routers configurados con IPv6. A la fecha de la publicación de esta RFC (diciembre de 1998) aún se encontraban en uso experimental, y solo aclara que los routers que no controlen aún estos parámetros deben pasarlos en forma transparente y sin ejecutar modificaciones sobre estos bits.

> Para las definiciones vigentes al día de hoy, **La RFC-6437 "*IPv6 Flow Label Specification*"** actualiza algunos conceptos. La mencionada RFC, inclusive aclara que esta reemplaza a la **RFC-3697** y justamente al punto 6, y Apéndice A de la **RFC-2460**.

Volvamos a la RFC-2460 y sigamos con el punto 7. "***Traffic Classes***"

Este campo, de 8 bits está disponible para poder distinguir entre diferentes clases o prioridades de los paquetes IPv6. Menciona que a la fecha de esta RFC, ya existen varias pruebas sobre IPv4 de priorización de tráfico empleando los campos

"Precedencia" y "Tipo de Servicio" de esta versión anterior, estos trabajos se denominan "*Servicios diferenciados*", y la idea para IPv6 es similar. (Se debe tener en cuenta que a día de hoy para IPv4, también existe otro concepto que es el de "*Servicios Integrados*", que opera también de forma parecida).

En realidad para desarrollar este campo, debemos considerar la RFC 2474 "*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*", de la que sólo comentaremos que se trata de una propuesta, no es mandatoria, y que en pocos párrafos podríamos describir que:

La estructura que propone de estos 8 bit es la siguiente:

```
  0   1   2   3   4   5   6   7
+---+---+---+---+---+---+---+---+
|          DSCP           |  CU   |
+---+---+---+---+---+---+---+---+
  DSCP: differentiated services codepoint
  CU:   currently unused
```

Es decir propone no usar los últimos dos bits y se centra en los seis primeros, y tal vez lo más importante lo trata el **punto 6** de esta RFC: "*IANA Considerations*", que establece lo siguiente:

> Este espacio de direcciones ofrece 64 opciones (los seis primeros bits del octeto) llamados "codepoints", (de allí viene la abreviatura DSCP: *Differentiated Services Code Points*), este espacio está dividio en tres "pooles" para propósito de asignación y administración de "codepoints" de acuerdo a la siguiente tabla:

Pool	Codepoint space	Assignment Policy
1	xxxxx0	Standards Action
2	xxxx11	EXP/LU
3	xxxx01	EXP/LU (*)

> Pool 1: Para ser asignado a acciones estándar.
>
> Pool 2: Reservado para uso local o experimental.
>
> Pool 3: Inicialmente ídem al anterior, pero debería ser preferentemente empleado para acciones estándar si se agota el pool 1.

A continuación presentamos una imagen de este campo:

Imagen 4: En esta imagen, se puede apreciar la captura de un encabezado que emplea justamente el campo "Traffic Class", este caso como podemos ver, respeta los dos últimos bits de este octeto (puestos a cero), luego de los seis primeros emplea el valor "111000" por lo que nos encontraríamos concretamente dentro del "Pool 1", es decir una acción estándar.

Por último volviendo al **punto 8** de la RFC 2460, este describe las características de los niveles superiores para IPv6, iniciando este tema con la aclaración que cualquier protocolo de nivel superior que emplee el direccionamiento IP para verificación (Checksum) deberá considerar ahora los 128 bits en vez de los 32 de IPv4. En particular especifica cómo trabajar con los "Pseudo header" de TCP y UDP, pero no nos detendremos en ello.

Este mismo punto hace referencia al cambio de nomenclatura de TTL de IPv4 por "Hop Limit" de IPv6, pero su lógica sigue siendo la misma, y luego aclara que los protocolos de nivel superior cuando calculan el máximo tamaño de datos que pueden entregar ahora al nivel 3, deben tener en cuenta que antes por ejemplo debían dejar 20 byte para TCP y 20 para IP, ahora deberán dejar, en este mismo caso 20 para TCP y 40 para IPv6), es decir contemplar que serán (en el caso de TCP) 60 bytes en vez de los 40 que reservaban para IPv4.

No entraremos a desarrollar los anexos de esta RFC, pero si alguien desea profundizar, sobre todo en como se "empaquetan" los distintos encabezados de extensión variable, en el anexo B ofrece varios ejemplos muy claros.

3.3. Las **RFC 2402 y 2406** *"IP Authentication Header (AH)"* e *"IP Encapsulating Security Payload (ESP)"*.

En el punto anterior, cuando comentamos el tema de los encabezados en extensión, los dos últimos que se presentan son justamente estos dos, ambos conforman el núcleo de lo que se conoce como **IPSec**, en grandes rasgos el primero (AH) ofrece las opciones de autenticación e integridad de datos y el segundo (ESP) se emplea para confidencialidad. En este artículo no nos detendremos en IPSec, solamente queremos mencionar que de forma nativa todo IPSec fue concebido para operar sobre IPv6, por esa razón es que su más eficiente funcionamiento es justamente como "encabezados en extensión" de IPv6.

El funcionamiento de ambos está descrito en las RFC que mencionamos en el título de este punto, en estos párrafos, solamente ponemos de manifiesto cómo estas recomendaciones describen el empleo de estos encabezados en extensión:

La RFC 2402 (AH) en su **punto 3.1 "***Authentication Header Location*" nos describe que en el contexto de IPv6, AH es visto como un "payload" (carga, datos) de extremo a extremo y debería aparecer como un "encabezado en extensión" luego de las opciones "hop-by-hop, routing, and fragmentation":

```
          Encabezado antes de aplicar AH
        ----------------------------------------
IPv6    |             | ext hdrs |     |      |
        | orig IP hdr |if present| TCP | Data |
        ----------------------------------------

          Encabezado después de aplicar AH
        ------------------------------------------------------------
IPv6    |             |hop-by-hop, dest*, |    | dest |     |      |
        |orig IP hdr  |routing, fragment. | AH | opt* | TCP | Data |
        ------------------------------------------------------------
    * = si está presente podría estar antes de AH, después de AH, o ambos
```

Para el caso de la RFC 2406 (ESP) el punto es el mismo **3.1** "*ESP Header Location*" y nos presenta también un esquema muy similar:

```
          Encabezado antes de aplicar ESP

          ----------------------------------------
 IPv6     |             | ext hdrs |     |      |
          | orig IP hdr |if present| TCP | Data |
          ----------------------------------------
Encabezado después de aplicar ESP
          ------------------------------------------------------------
 IPv6     | orig |hop-by-hop,dest*,|   |dest|   |    | ESP   | ESP|
          |IP hdr|routing,fragment.|ESP|opt*|TCP|Data|Trailer|Auth|
          ------------------------------------------------------------
                                 |<---- encrypted ---->|
                                   |<---- authenticated ---->|
    * = si está presente podría estar antes de ESP, después de ESP, o ambos
```

A continuación presentamos una imagen de IPv6 empleando ESP:

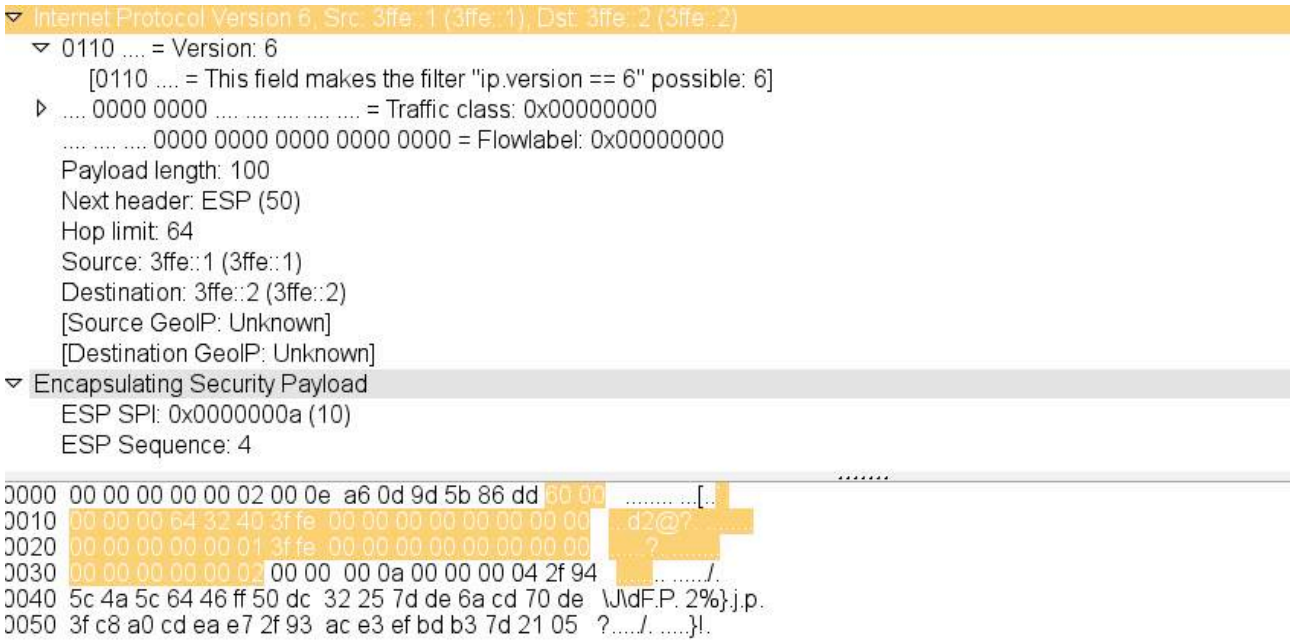


Imagen 5: En esta imagen podemos apreciar justamente este protocolo, en esta captura no hay ninguna opción intermedia, por lo tanto IPv6 lo indica como "Next Header = 50", e

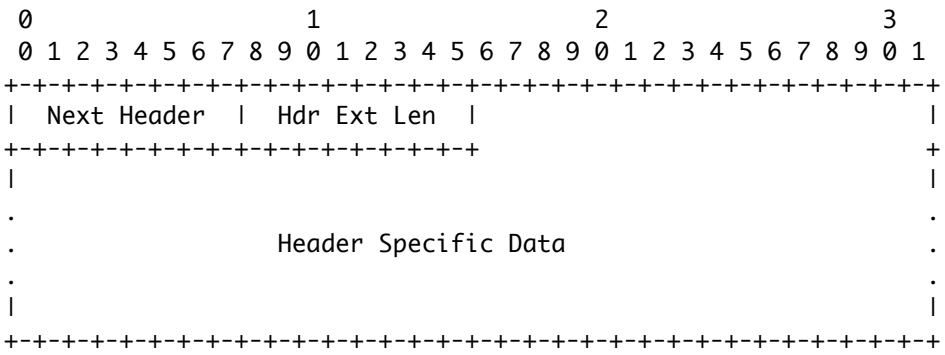
inmediatamente finalizado el encabezado básico de IPv6 comienza ESP. Si se presta atención en la parte inferior de la imagen, luego de los 40 octetos (en hexadecimal) del encabezado de IPv6 (que hemos resaltado en **naranja**), continúa ESP con los campos de su encabezado "00 00 00 0a (ESP SPI) 00 00 00 04 (Secuencia)" y a continuación todo lo que sigue va criptografiado, pues esa es la función de ESP.

3.4. La **RFC 6564** "*A Uniform Format for IPv6 Extension Headers*"

Hemos incluido esta RFC de abril de 2012 pues se trata de una actualización de la anterior (RFC 2460).

Lo más importante a destacar, es que tal cual describe en su introducción, la RFC 2460 establecía que los encabezados en extensión, con excepción del "Hop by Hop" no deben ser procesados en nodos intermedios, pero en la actualidad muchos desarrollos de IPv6 sobre routers y firewalls son capaces de procesar y/o ignorar cualquiera de ellos empleando lo que se denomina ASICs: *Application Specific Integrated Circuits*, en particular se evaluó esta RFC por razones de seguridad.

Para evitar problemas en nodos intermedios, cualquier encabezado en extensión definido a futuro deberá respetar el siguiente formato:



Este esquema no debe ser tenido en cuenta para los encabezados ya definidos con anterioridad (RFC-2460) sólo aplica a nuevos encabezados en extensión.