A. PROTOCOLO IP VERSION 6.

En este anexo se describe el nuevo conjunto de protocolos de IPv6 a través de la comparación, en la medida de lo posible, del conjunto de protocolos IPv6 con características o conceptos similares de IPv4. Así mismo se describe los problemas de IPv4 y como los resuelve IPv6, el direccionamiento de IPv6, el nuevo encabezado de IPv6 y sus extensiones, los reemplazos de IPv6 para el Protocolo de mensajes de control de Internet (ICMP, *Internet Control Message Protocol*) y el Protocolo de administración de grupos de Internet (IGMP, *Internet Group Management Protocol*), la interacción entre nodos vecinos y la configuración automática de direcciones IPv6. Este documento presenta los fundamentos de los conceptos de IPv6 basados en estándares de Internet.

Aunque actualmente no se utiliza de un modo prioritario, Internet se basará en IPv6 en el futuro. Es importante comprender este protocolo estratégico para empezar a planear una posible migración a IPv6.

1. INTRODUCCION.

La versión actual de IP (conocida como versión 4 o IPv4) no ha cambiado sustancialmente desde la publicación del RFC 791 en 1981. IPv4 ha demostrado su robustez, facilidad de implementación e interoperabilidad, y ha superado la prueba que representa ampliar una red interna para convertirla en un servicio global de las dimensiones actuales de Internet. Esto es un tributo a su diseño inicial.

Sin embargo, en el diseño inicial no se previó lo siguiente:

- **El reciente crecimiento exponencial de Internet y el inminente agotamiento del espacio de direcciones IPv4**

Las direcciones IPv4 son relativamente escasas, lo que ha obligado a algunas organizaciones a utilizar el Traductor de direcciones de red (NAT, *Network Address Translator*) para asignar múltiples direcciones privadas a una sola dirección IP pública. Aunque NAT permite reutilizar el espacio de direcciones privadas, no admite la seguridad basada en estándares en la capa de red o la asignación correcta de todos los protocolos de nivel superior y puede crear problemas cuando se conectan dos organizaciones que utilizan el espacio de direcciones privadas. Además, la creciente proliferación de dispositivos y aparatos conectados a Internet apunta a que el espacio de direcciones públicas de IPv4 se agotará dentro de un tiempo.

- **El crecimiento de Internet y la capacidad de los enrutadores troncales de Internet para mantener grandes tablas de enrutamiento**

Debido a la forma en la que se asignan los Id. de red IPv4, existen normalmente más de 70.000 rutas en la tabla de enrutamiento de los enrutadores troncales de Internet. La

infraestructura actual del enrutamiento de IPv4 en Internet es una combinación de enrutamiento plano y jerárquico.

- **La necesidad de una configuración más sencilla**

La mayor parte de las implementaciones actuales de IPv4 deben configurarse manualmente o mediante un protocolo de configuración de direcciones con estado, como el Protocolo de configuración dinámica de host (DHCP, *Dynamic Host Configuration Protocol*). Ante un número mayor de equipos y dispositivos que utilizan IP, existe la necesidad de emplear una configuración de direcciones más sencilla y automática, así como otros parámetros de configuración no basados en la administración de una infraestructura DHCP.

- **El requisito de seguridad en el nivel de IP**

La comunicación privada a través de un medio público como Internet requiere servicios de cifrado que protejan los datos que se envían ante posibles observaciones o modificaciones durante el tránsito. Aunque ahora existe un estándar para ofrecer seguridad a los paquetes de IPv4 (conocida como seguridad de Protocolo Internet o IPSec), es opcional y prevalecen las soluciones propietarias.

- **La necesidad de facilitar la entrega de datos en tiempo real, también denominada calidad de servicio (QoS, *Quality of Service*)**

Aunque existen estándares de QoS para IPv4, el tráfico en tiempo real se basa en el campo Type of Service (TOS o Tipo de servicio) de IPv4 y en la identificación de la carga, normalmente mediante un puerto UDP o TCP. Por desgracia, el campo Type of Service de IPv4 presenta una funcionalidad limitada y con el tiempo han surgido distintas interpretaciones locales. Además, la identificación de la carga mediante un puerto TCP y UDP no es posible cuando la carga de paquetes IPv4 está cifrada.

Para resolver estas preocupaciones, el Grupo de trabajo de ingeniería de Internet (IETF, *Internet Engineering Task Force*) ha desarrollado un conjunto de protocolos y estándares conocidos como IP versión 6 (IPv6). Esta nueva versión, antes denominada IP: la siguiente generación (*IP-The Next Generation* o IPng), incorpora los conceptos de muchos métodos propuestos para actualizar el protocolo IPv4. El diseño de IPv6 se ha diseñado intencionalmente para que afecte lo menos posible a los protocolos de nivel superior e inferior al evitar que se agreguen aleatoriamente nuevas características.

2. CARACTERISTICAS DE IPv6

A continuación se presentan las características del nuevo protocolo IPv6:

- **Nuevo formato de encabezado**

El encabezado de IPv6 presenta un nuevo formato diseñado para que la carga de trabajo del encabezado sea mínima. Para ello, se mueven los campos de opciones y los que no son esenciales a encabezados de extensión que se colocan tras el encabezado de IPv6. El

encabezado optimizado de IPv6 proporciona un procesamiento más eficiente en los enrutadores intermedios.

Los encabezados de IPv4 no pueden funcionar conjuntamente con los encabezados de IPv6. Un host o un enrutador deben utilizar una implementación de IPv4 e IPv6 para reconocer y procesar ambos formatos de encabezado. El nuevo encabezado de IPv6 es sólo el doble de grande que el de IPv4, aunque las direcciones de IPv6 son cuatro veces mayores que las de IPv4.

- **Gran espacio de direcciones**

IPv6 tiene direcciones IP de origen y destino de 128 bits (16 bytes). Aunque con 128 bits se pueden expresar más de $3{,}4 \times 10^{38}$ combinaciones posibles, el gran espacio de direcciones de IPv6 se ha diseñado para permitir varios niveles de subredes y asignaciones de redes de la red troncal de Internet a las subredes individuales de una organización.

Aunque actualmente sólo se asigna un pequeño número de las direcciones posibles para los hosts, hay muchas direcciones disponibles para su uso en el futuro. Con un número de direcciones disponibles mucho mayor, dejan de ser necesarias las técnicas de conservación de direcciones, como la distribución de NAT.

- **Direccionamiento jerárquico e infraestructura de enrutamiento eficientes**

Las direcciones globales de IPv6 utilizadas en la parte IPv6 de Internet están diseñadas para crear una infraestructura de enrutamiento jerárquica eficiente que se puede resumir, basada en la aparición de múltiples niveles de proveedores de servicios Internet. En Internet IPv6, los enrutadores troncales tienen tablas de enrutamiento mucho más pequeñas, que corresponden a la infraestructura de enrutamiento de Agregadores de nivel superior.

- **Configuración de direcciones sin estado y con estado**

Para simplificar la configuración de hosts, IPv6 permite la configuración de direcciones con estado, como la configuración de direcciones en presencia de un servidor DHCP, y la configuración de direcciones sin estado (configuración de direcciones en ausencia de un servidor DHCP). Con una configuración de direcciones sin estado, los hosts de un enlace se configuran automáticamente con direcciones IPv6 para el enlace (que se denominan direcciones locales de enlace) y con direcciones derivadas de prefijos anunciados por enrutadores locales. Incluso en ausencia de un enrutador, los hosts del mismo enlace pueden configurarse automáticamente con direcciones locales de enlace y se comunican sin configuración manual.

- **Seguridad integrada**

La compatibilidad con IPSec es un requisito del conjunto de protocolos IPv6. Este requisito proporciona una solución basada en estándares en respuesta a las necesidades de seguridad de red y aumenta la interoperabilidad entre distintas implementaciones de IPv6.

- **Mayor compatibilidad con QoS**

Los nuevos campos del encabezado de IPv6 definen cómo se identifica y se controla el tráfico. La identificación del tráfico mediante un campo Flow Label (Etiqueta de flujo) en el encabezado de IPv6 permite a los enrutadores identificar y proporcionar un tratamiento especial a los paquetes que pertenecen a un flujo, un conjunto de paquetes que viaja entre un origen y un destino. Como el tráfico se identifica en el encabezado de IPv6, se puede proporcionar compatibilidad con QoS incluso si la carga de paquetes está cifrada mediante IPSec.

- **Nuevo protocolo para la interacción de nodos vecinos**

El protocolo Neighbor Discovery (Descubrimiento de vecino) para IPv6 consiste en un conjunto de mensajes del Protocolo de mensajes de control de Internet para IPv6 (ICMPv6, *Internet Control Message Protocol for IPv6*) que administran la interacción de nodos vecinos (nodos que se encuentran en el mismo enlace). Neighbor Discovery reemplaza al Protocolo de resolución de direcciones (ARP, *Address Resolution Protocol*) basado en difusión, al protocolo de descubrimiento de enrutadores de ICMPv4 y a los mensajes Redirect (Redirección) de ICMPv4 con mensajes Neighbor Discovery de unidifusión y multidifusión.

- **Capacidad de ampliación**

IPv6 se puede ampliar fácilmente con nuevas características si se agregan encabezados de extensión tras el encabezado de IPv6. A diferencia de las opciones del encabezado de IPv4, que sólo permite 40 bytes de opciones, el tamaño de los encabezados de extensión de IPv6 sólo está limitado por el tamaño del paquete de IPv6.

3. DIFERENCIAS ENTRE IPv4 E IPv6

En la tabla A.1 se resaltan algunas de las principales diferencias entre IPv4 e IPv6.

IPv4	IPv6
Las direcciones de origen y de destino tienen una longitud de 32 bits (4 bytes).	Las direcciones de origen y de destino tienen una longitud de 128 bits (16 bytes).
La compatibilidad con IPSec es opcional.	La compatibilidad con IPSec es obligatoria.
No hay identificación de carga para el control de QoS por parte de los enrutadores en el encabezado de IPv4.	La identificación de carga para el control de QoS por parte de los enrutadores se incluye en el encabezado de IPv6 mediante el campo Flow Label (Etiqueta de flujo).
La fragmentación es posible en ambos enrutadores y en el host de envío.	La fragmentación no es posible en los enrutadores. Sólo es posible en el host de envío.
El encabezado incluye una suma de comprobación.	El encabezado no incluye una suma de comprobación.
El encabezado incluye opciones.	Todos los datos opcionales se mueven a

	extensiones de encabezado IPv6.
El Protocolo de resolución de direcciones (ARP) utiliza tramas de solicitud de ARP de difusión para resolver una dirección de IPv4 en una dirección de nivel de enlace.	Las tramas de solicitud de ARP se reemplazan por mensajes Neighbor Solicitation (Solicitud de vecino) de multidifusión.
Se utiliza el Protocolo de administración de grupos de Internet (IGMP) para administrar la pertenencia a grupos de subredes locales.	El protocolo IGMP se reemplaza por mensajes Multicast Listener Discovery (MLD o Descubrimiento de escucha de multidifusión).
Para determinar la dirección IPv4 de la mejor puerta de enlace predeterminada se utiliza el descubrimiento de enrutadores de ICMP, que es opcional.	El descubrimiento de enrutadores de ICMPv4 se reemplaza por los mensajes Router Solicitation (Solicitud de enrutador) y Router Advertisement (Anuncio de enrutador) de ICMPv6, que son necesarios.
Las direcciones de difusión se utilizan para enviar tráfico a todos los nodos de una subred.	No hay direcciones de difusión de IPv6. En su lugar, se utiliza una dirección de multidifusión para todos los nodos de ámbito local de enlace.
La configuración debe efectuarse manualmente o a través de DHCP.	No se necesita configuración manual ni DHCP.
Utiliza registros de recursos (A) de dirección de host en el Sistema de nombres de dominio (DNS, *Domain Name System*) para asignar nombres de host a direcciones IPv4.	Utiliza registros de recursos (AAAA) de dirección de host en el Sistema de nombres de dominio (DNS) para asignar nombres de host a direcciones IPv6.
Utiliza registros del recurso Puntero (PTR) en el dominio DNS IN-ADDR.ARPA para asignar direcciones de IPv4 a nombres de host.	Utiliza registros del recurso Puntero (PTR) en el dominio DNS IP6.INT para asignar direcciones de IPv6 a nombres de host.

Tabla A. 1. Diferencias entre IPv4 e IPv6

4. DIRECCIONAMIENTO IPV6

4.1 ESPACIO DE DIRECCIONES DE IPV6

La característica distintiva más evidente de IPv6 es el uso de direcciones mucho mayores. El tamaño de una dirección en IPv6 es de 128 bits, cuatro veces mayor que el de una dirección de IPv4. El espacio de direcciones de 32 bits permite hasta 4.294.967.296 direcciones. Un espacio de direcciones de 128 bits permite hasta 340.282.266.920.938.463.463.374.607.431.768.211.465 (o 3,4 x 10^{38}) direcciones.

A finales de la década de 1970, cuando se diseñó el espacio de direcciones de IPv4, era inimaginable que pudiera agotarse. Sin embargo, debido a los cambios tecnológicos y a una

práctica de asignaciones en la que no se previó el reciente aumento del número de hosts en Internet, el espacio de direcciones de IPv4 se fue agotando hasta tal punto que en 1992 se hizo evidente la necesidad de un reemplazo.

Con IPv6, resulta aún más difícil concebir que el espacio de direcciones de IPv6 se vaya a consumir. Para tener una idea algo más aproximada de lo que supone este número, un espacio de direcciones de 128 bits proporciona 655.570.793.348.866.943.898.599 (6,5 x 10^{23}) direcciones por metro cuadrado de la superficie terrestre.

Ciertamente, la decisión de que la dirección de IPv6 tenga una longitud de 128 bits no obedece a que pueda haber hasta 6,5 x 10^{23} direcciones por cada metro cuadrado de la Tierra. El tamaño relativamente grande de una dirección IPv6 se ha diseñado así para que se pueda subdividir en dominios de enrutamiento jerárquico que reflejen la topología de Internet actual. El uso de 128 bits permite varios niveles de jerarquía y ofrece flexibilidad para diseñar un enrutamiento y un direccionamiento jerárquico, algo que actualmente no ofrece la tecnología Internet basada en IPv4.
La arquitectura de direccionamiento de IPv6 se describe en el RFC 2373.

4.2 ASIGNACION ACTUAL

De modo similar al que se utiliza para dividir el espacio de direcciones de IPv4, el espacio de direcciones de IPv6 se divide según el valor de los bits de orden superior. Los bits de orden superior y su valor fijo se conocen como prefijo de formato (FP, *Format Prefix*).

En la tabla A.2 se muestra la asignación del espacio de direcciones de IPv6 por FP.

Asignación	Prefijo de formato (FP)	Fracción del espacio de direcciones
Reservado	0000 0000	1/256
Sin asignar	0000 0001	1/256
Reservado para la asignación de NSAP	0000 001	1/128
Reservado para la asignación de IPX	0000 010	1/128
Sin asignar	0000 011	1/128
Sin asignar	0000 1	1/32
Sin asignar	0001	1/16
Direcciones de unidifusión global agregables	001	1/8
Sin asignar	010	1/8
Sin asignar	011	1/8
Sin asignar	100	1/8
Sin asignar	101	1/8
Sin asignar	110	1/8

Sin asignar	1110	1/16
Sin asignar	1111 0	1/32
Sin asignar	1111 10	1/64
Sin asignar	1111 110	1/128
Sin asignar	1111 1110 0	1/512
Direcciones de unidifusión local de enlace	1111 1110 10	1/1024
Direcciones de unidifusión local de sitio	1111 1110 11	1/1024
Direcciones de multidifusión	1111 1111	1/256

Tabla A. 2. Asignación actual del espacio de direcciones de IPv6

El conjunto actual de direcciones de unidifusión que se pueden utilizar con nodos de IPv6 consta de direcciones de unidifusión global agregables, direcciones de unidifusión local de enlace y direcciones de unidifusión local de sitio. Éstas sólo representan el 15 por ciento de todo el espacio de direcciones de IPv6.

4.3 SINTAXIS DE LAS DIRECCIONES DE IPV6

Las direcciones de IPv4 se representan en formato de notación decimal con puntos. Esta dirección de 32 bits se divide en límites de 8 bits. Cada conjunto de 8 bits se convierte en su equivalente decimal y está separado por puntos. Para IPv6, la dirección de 128 bits se divide en límites de 16 bits y cada bloque de 16 bits se convierte en un número hexadecimal de 4 dígitos y se separa con signos de dos puntos (:). La representación resultante se denomina hexadecimal con dos puntos.

A continuación se muestra una dirección IPv6 en formato binario:

0010000111011010100100001101001100000000010100000010111100111011
0000001010101010000000001111111111111110001010001001110001011010

Esta dirección de 128 bits se divide en límites de 16 bits:

0010000111011010 1001000011010011 0000000001010000 0010111100111011
0000001010101010 0000000011111111 1111111000101000 1001110001011010

Cada bloque de 16 bits se convierte a hexadecimal y está delimitado por signos de dos puntos (:). El resultado es:

21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

La representación de IPv6 se puede simplificar aún más si se quitan los ceros a la izquierda de cada bloque de 16 bits. Sin embargo, cada bloque debe tener un dígito como mínimo. Al suprimir los ceros a la izquierda, la representación de la dirección se convierte en:

21DA:D3:0:2F3B:2AA:FF:FE28:9C5A

4.4 COMPRESIÓN DE CEROS

Algunos tipos de direcciones contienen largas secuencias de ceros. Para simplificar aún más la representación de direcciones de IPv6, una secuencia contigua de bloques de 16 bits establecida como 0 en formato hexadecimal con dos puntos se puede comprimir como "::".

Por ejemplo, la dirección local de enlace de FE80:0:0:0:2AA:FF:FE9A:4CA2 se puede comprimir en FE80::2AA:FF:FE9A:4CA2. La dirección de multidifusión FF02:0:0:0:0:0:0:2 se puede comprimir en FF02::2.

La compresión de cero sólo se puede utilizar para comprimir una serie contigua de bloques de 16 bits expresada en notación hexadecimal con dos puntos. No se puede utilizar la compresión de ceros para incluir una parte de un bloque de 16 bits. Por ejemplo, no se puede expresar FF02:30:0:0:0:0:0:5 como FF02:3::5.

Para determinar cuántos bits 0 se representan mediante "::", puede contar el número de bloques de la dirección comprimida, restar ese número a 8 y multiplicar el resultado por 16. Por ejemplo, en la dirección FF02::2, hay dos bloques (el bloque "FF02" y el bloque "2"). El número de bits expresado por "::" es 96 (96 = (8 – 2)∗16).

La compresión de ceros sólo se puede utilizar una vez en una dirección dada. De lo contrario, no se podría determinar el número de bits 0 representados por cada instancia de "::".

4.5 PREFIJOS IPv6

El prefijo es la parte de la dirección que indica los bits con valores fijos o los bits del identificador de red. Los prefijos para IPv6 se expresan del mismo modo que la notación de Enrutamiento entre dominios sin clase (CIDR, *Classless Inter-Domain Routing*) para IPv4. Un prefijo IPv6 se escribe con la notación *dirección*/*longitud de prefijo*. Por ejemplo, FE80::2AA:FF:FE9A:4CA2/64 indica que los primeros 64 bits de la dirección corresponden al prefijo de red. La notación de prefijo también se utiliza para expresar los identificadores de red o de subred. Por ejemplo, 21DA:D3::/48 es una subred.

Una dirección de nodo, con su prefijo, se puede utilizar para obtener el identificador de subred. Por ejemplo, el identificador de subred derivado de la dirección y el prefijo 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A/64 es 21DA:D3:0:2F3B::/64.

Nota Las implementaciones de IPv4 suelen utilizar una representación decimal con puntos del prefijo de red, que se conoce como máscara de subred. Para IPv6 no se utiliza la máscara de subred. Sólo se admite la notación de longitud de prefijo. Aunque se pueden definir prefijos a lo largo de los límites de bit, la notación hexadecimal con dos puntos para las direcciones IPv6 se expresa a lo largo de límites de cuarteto (4 bits). Para expresar

correctamente una subred con un prefijo cuya longitud no es múltiplo de 4, deberá realizar conversiones de notación hexadecimal a binaria para determinar el identificador de subred adecuado. Por ejemplo, para expresar la subred de la dirección y el prefijo de 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A/59, deberá convertir el "3" de "2F3B" a binario (0011), dividir el cuarteto entre el tercer y el cuarto dígito binario, y volver a realizar la conversión a hexadecimal. El resultado es el identificador de subred 21DA:D3:0:2F20::/59.

4.6 TIPOS DE DIRECCIONES IPv6

Hay tres tipos de direcciones IPv6:

- **Unidifusión (Unicast)**

Una dirección de unidifusión identifica a una sola interfaz en el ámbito del tipo de dirección de unidifusión. Con la topología de enrutamiento de unidifusión apropiada, los paquetes dirigidos a una dirección de unidifusión se entregan a una sola interfaz. Para ajustarse a los sistemas de equilibrio de carga, el RFC 2373 permite que varias interfaces utilicen la misma dirección, siempre y cuando las distintas interfaces aparezcan como una sola interfaz para la implementación de IPv6 en el host.

- **Multidifusión (Multicast)**

Una dirección de multidifusión identifica a varias interfaces. Con la topología de enrutamiento de multidifusión apropiada, los paquetes dirigidos a una dirección de multidifusión se entregan a todas las interfaces identificadas por la dirección.

- **Cualquier difusión (Anycast)**

Una dirección para cualquier difusión identifica a varias interfaces. Con la topología de enrutamiento apropiada, los paquetes dirigidos a una dirección para cualquier difusión se entregan a una sola interfaz, la más próxima que identifica la dirección. La interfaz "más próxima" se define como la más cercana en términos de distancia de enrutamiento. Una dirección de multidifusión se utiliza para la comunicación "de uno a muchos", con entrega a varias interfaces. Una dirección para cualquier difusión se utiliza para la comunicación "de uno a uno de muchos", con entrega a una sola interfaz.

En todos los casos, las direcciones IPv6 identifican interfaces, no nodos. Un nodo se identifica mediante cualquier dirección de unidifusión asignada a una de sus interfaces.

4.7 DIRECCIONES IPv6 DE UNIDIFUSIÓN

Los siguientes tipos de direcciones son direcciones IPv6 de unidifusión:

- Direcciones de unidifusión global agregables
- Direcciones locales de enlace
- Direcciones locales de sitio
- Direcciones especiales
- Direcciones NSAP e IPX

4.7.1 DIRECCIONES DE UNIDIFUSION GLOBALES AGREGABLES

Las direcciones de unidifusión global agregables, identificadas mediante FP 001, equivalen a las direcciones IPv4 públicas. Se pueden enrutar globalmente y es posible el acceso a las mismas en la parte de IPv6 de Internet, conocida como 6bone (red troncal de IPv6).

Como su nombre indica, las direcciones de unidifusión global agregables están diseñadas para ser agregadas o resumidas de modo que se obtenga una infraestructura de enrutamiento eficiente. A diferencia de la tecnología Internet basada en IPv4, que es una mezcla de enrutamiento plano y jerárquico, la tecnología Internet basada en IPv6 se diseñó desde el principio para permitir un direccionamiento y un enrutamiento jerárquicos eficientes. El ámbito (la región de la red interna IPv6 en la que la dirección es única) de una dirección de unidifusión global agregable es toda la red Internet de IPv6. En la figura A.1 se muestra la estructura de una dirección de unidifusión global agregable.

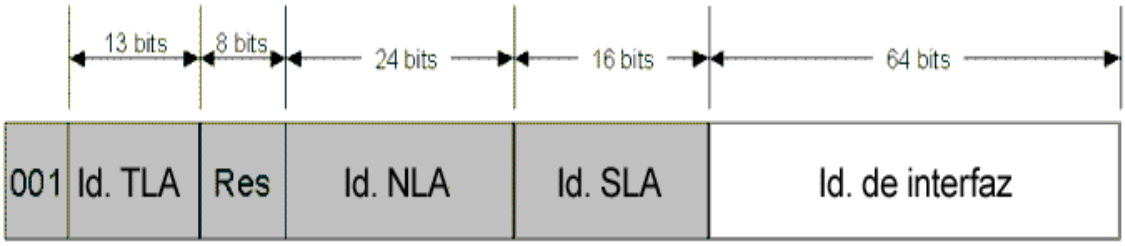

Figura A. 1. Dirección de unidifusión global agregable

Los campos de la dirección de unidifusión global agregable son:

TLA ID (Id. de TLA): indica el Agregador de nivel superior (TLA, *Top Level Aggregator*) para la dirección. El tamaño de este campo es de 13 bits. TLA identifica el nivel superior de la jerarquía de enrutamiento. La asociación IANA administra los TLA, que se asignan a registros locales de Internet que, a su vez, asignan TLA individuales a grandes proveedores de servicios Internet (ISP) de largo alcance. Un campo de 13 bits permite hasta 8.192 TLA distintos. Los enrutadores del nivel superior de la jerarquía de enrutamiento en Internet de IPv6 (denominados enrutadores libres predeterminados) no tienen una ruta predeterminada, sólo rutas con prefijos de 16 bits que corresponden a los TLA asignados.

Res: bits reservados para uso futuro al expandir el tamaño del Id. de TLA o del Id. de NLA. El tamaño de este campo es de 8 bits.

NLA ID (Id. de NLA): indica el Agregador de nivel siguiente (NLA, *Next-Level Aggregator*) para la dirección. El Id. de NLA se utiliza para identificar un sitio de cliente específico. El tamaño de este campo es de 24 bits. El Id. de NLA permite a un ISP crear varios niveles de jerarquía de direccionamiento dentro de una red para organizar el enrutamiento y el direccionamiento de los ISP en un nivel inferior e identificar sitios. La estructura de la red de los ISP es transparente para los enrutadores libres predeterminados.

SLA ID (Id. de SLA): indica el Agregador de nivel de sitio (SLA, *Site-Level Aggregator*) para la dirección. El Id. de SLA puede servir a una organización para identificar subredes dentro de su sitio. El tamaño de este campo es de 16 bits. La organización puede utilizar estos 16 bits en su sitio para crear 65.536 subredes o niveles múltiples de jerarquía de direccionamiento y una infraestructura de enrutamiento eficiente. Con una flexibilidad de 16 bits para las subredes, un prefijo de unidifusión global agregable asignado a una organización equivale a asignar a esa organización un Id. de red de Clase A de IPv4 (siempre y cuando el último octeto se utilice para identificar nodos en subredes). La estructura de la red del cliente es transparente para los ISP.

Interface ID (Id. de interfaz): indica la interfaz de una subred específica. El tamaño de este campo es de 64 bits.

Los campos de una dirección de unidifusión global agregable crean la estructura en tres niveles que se muestra en la figura A.2.

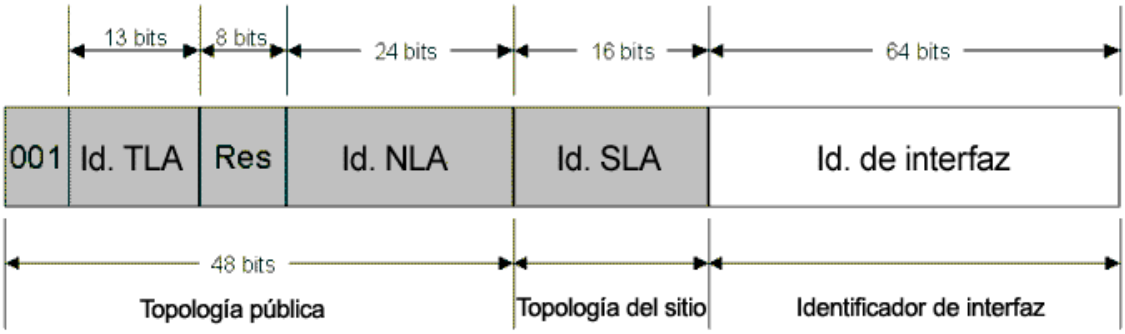

Figura A. 2. Estructura en tres niveles de la dirección de unidifusión global agregable

La topología pública es la colección de ISP grandes y pequeños que proporcionan acceso a la parte IPv6 de Internet. La topología del sitio es la colección de subredes del sitio de una organización. El identificador de interfaz identifica a una interfaz específica de una subred en el sitio de una organización.

4.7.2 DIRECCIONES LOCALES DE ENLACE

Los nodos utilizan las direcciones locales de enlace identificadas mediante FP 1111 1110 10 cuando se comunican con nodos vecinos en el mismo enlace. Por ejemplo, en una red IPv6 de enlace único sin enrutador, las direcciones locales de enlace se utilizan para la comunicación entre los hosts del enlace. El ámbito de una dirección local de enlace es el enlace local.

Se necesita una dirección local de enlace para los procesos Neighbor Discovery (Descubrimiento de vecino) y siempre se configura automáticamente, incluso en ausencia de todas las demás direcciones de unidifusión. En la figura A.3 se muestra la estructura de la dirección local de enlace.

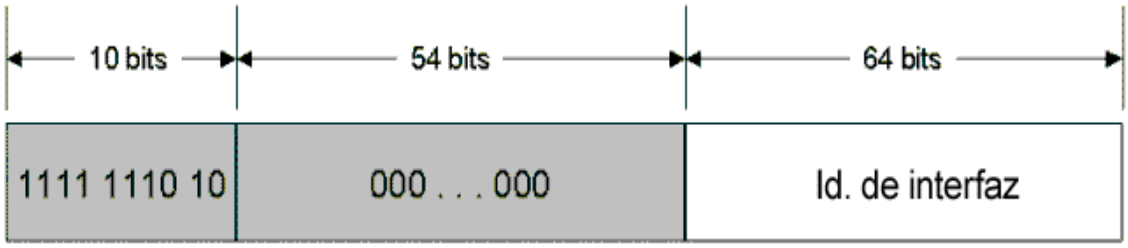

Figura A. 3. Dirección local de enlace

Las direcciones locales de enlace siempre empiezan por FE80. Con el identificador de interfaz de 64 bits, el prefijo para las direcciones locales de enlace es siempre FE89::/64. Un enrutador IPv6 nunca reenvía el tráfico de enlace local más allá del enlace.

4.7.3 DIRECCIONES LOCALES DE SITIO

Las direcciones locales de sitio, identificadas mediante FP 1111 1110 11, equivalen al espacio de direcciones privadas de IPv4 (10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16).

Por ejemplo, las intranets privadas que no tienen una conexión directa enrutada a Internet de IPv6 pueden utilizar direcciones locales de sitio sin entrar en conflicto con direcciones de unidifusión global agregables. No se puede tener acceso a las direcciones locales de sitio desde otros sitios y los enrutadores no deben reenviar el tráfico local fuera del sitio. Las direcciones locales de sitio se pueden utilizar junto con las direcciones de unidifusión global agregables. El ámbito de una dirección local de sitio es el sitio (la red interna de la organización).
A diferencia de las direcciones locales de enlace, las direcciones locales de sitio no se configuran automáticamente y deben asignarse a través de procesos de configuración de direcciones sin estado y con estado. En la figura A.4 se muestra la estructura de la dirección local de sitio.

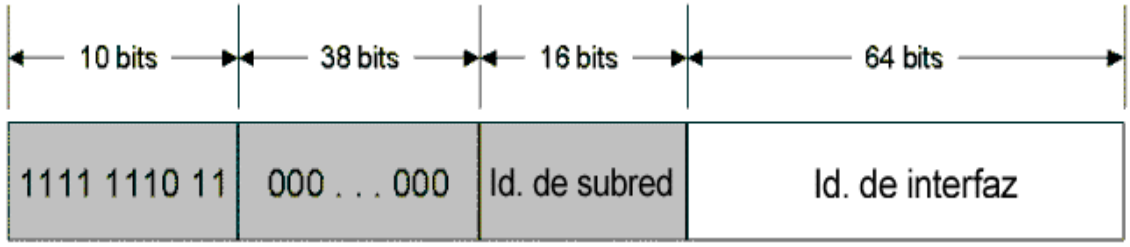

Figura A. 4. Dirección local de sitio

Los primeros 48 bits son siempre fijos para las direcciones locales de sitio, que empiezan por FEC0::/48. Después de los 48 bits fijos hay un identificador de subred de 16 bits (campo Subnet ID o Id. de subred) que proporciona 16 bits, con el que se pueden crear subredes en una organización. Con 16 bits, se pueden tener hasta 65.536 subredes en una estructura de subredes plana o se pueden subdividir los bits de orden superior del campo Id. de subred para crear una infraestructura de enrutamiento agregable y jerárquica. Después

del campo Subnet ID hay un campo Interface ID (Id. de interfaz) que identifica una interfaz específica en una subred.

La dirección de unidifusión global agregable y la dirección local de sitio comparten la misma estructura aparte de los 48 bits de la dirección. En las direcciones de unidifusión global agregables, el Id. de SLA identifica la subred en una organización. Para las direcciones locales de sitio, el Id. de subred realiza la misma función. Debido a esto, puede crear una infraestructura de enrutamiento de subredes que se utiliza para direcciones de unidifusión global agregables y locales de sitio.

4.7.4 DIRECCIONES IPv6 ESPECIALES

A continuación se muestran direcciones IPv6 especiales:

- **Dirección no especificada**

La dirección no especificada (0:0:0:0:0:0:0:0 ó ::) sólo se utiliza para indicar la ausencia de una dirección. Equivale a la dirección IPv4 no especificada 0.0.0.0. La dirección no especificada se suele utilizar como dirección de origen para paquetes que intentan comprobar la unicidad de una dirección provisional. La dirección no especificada no se asigna nunca a una interfaz ni se utiliza como dirección de destino.

- **Dirección de bucle de retroceso**

La dirección de bucle de retroceso (0:0:0:0:0:0:0:1 ó ::1) se utiliza para identificar una interfaz de bucle de retroceso, lo que permite que un nodo se envíe paquetes a sí mismo. Equivale a la dirección IPv4 de bucle de retroceso 127.0.0.1. Los paquetes dirigidos a la dirección de bucle de retroceso nunca deben enviarse a través de un enlace o reenviarse mediante un enrutador de IPv6.

4.7.5 DIRECCIONES DE COMPATIBILIDAD

Para ayudar a la migración de IPv4 a IPv6 y a la coexistencia de ambos tipos de hosts, se definen las siguientes direcciones:

- **Dirección compatible con IPv4**

La dirección compatible con IPv4, 0:0:0:0:0:0:w.x.y.z o ::w.x.y.z (donde *w.x.y.z* es la representación decimal con puntos de una dirección IPv4), es utilizada por nodos de doble pila que se comunican con IPv6 sobre una infraestructura de IPv4. Los nodos de doble pila son nodos con protocolos IPv4 e IPv6. Cuando se utiliza la dirección compatible con IPv4 como destino de IPv6, el tráfico de IPv6 se encapsula automáticamente con un encabezado de IPv4 y se envía al destino mediante la infraestructura de IPv4.

- **Dirección asignada de IPv4**

La dirección asignada de IPv4, 0:0:0:0:0:FFFF:w.x.y.z o ::FFFF:w.x.y.z, se utiliza para representar un nodo que es sólo de IPv4 ante un nodo IPv6. Se utiliza únicamente para la

representación interna. La dirección asignada de IPv4 nunca se utiliza como dirección de origen o de destino de un paquete IPv6.

4.7.6 DIRECCIONES NSAP E IPX

Para proporcionar un medio de asignar direcciones de Punto de acceso a servicios de red (NSAP, *Network Service Access Point*) y de Intercambio de paquetes entre redes (IPX, *Internetwork Packet Exchange*) a direcciones IPv6, se definen direcciones NSAP e IPX.

- **Dirección IP**

Las direcciones NSAP utilizan FP 0000001 y asignan los últimos 121 bits de la dirección IPv6 a una dirección NSAP.

- **Direcciones IPX**

Las direcciones IPX utilizan FP 0000010 y asignan los últimos 121 bits de la dirección IPv6 a una dirección IPX. Aún no se ha definido la asignación de una dirección IPX a una dirección IPv6.

4.8 DIRECCIONES IPv6 DE MULTIDIFUSIÓN

En IPv6, el tráfico de multidifusión funciona del mismo modo que en IPv4. Los nodos IPv6 ubicados arbitrariamente pueden atender al tráfico de multidifusión en una dirección de multidifusión IPv6 arbitraria. Los nodos IPv6 pueden escuchar a varias direcciones de multidifusión simultáneamente. Los nodos pueden unirse a un grupo de multidifusión o abandonarlo en cualquier momento.

Las direcciones de multidifusión utilizan FP 11111111. Es fácil clasificar una dirección IPv6 como de multidifusión, ya que siempre empieza por "FF". Las direcciones de multidifusión no se pueden utilizar como direcciones de origen o como destinos intermedios en un encabezado Routing (Enrutamiento).

Además de FP, las direcciones de multidifusión incluyen una estructura adicional para identificar sus indicadores, ámbito y grupo de multidifusión. En la figura A.5 se muestra la dirección de multidifusión IPv6.

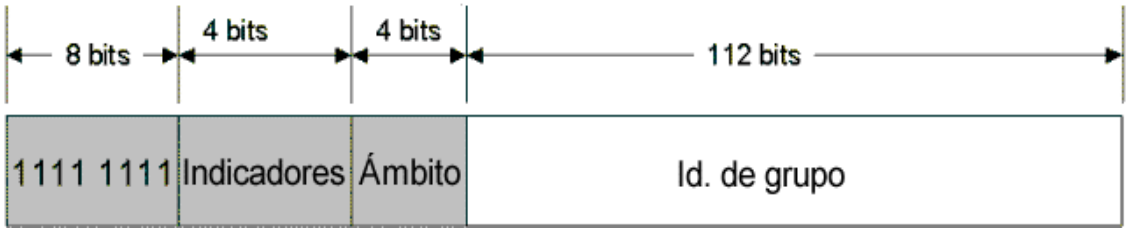

Figura A. 5. Dirección de multidifusión IPv6

Los campos del encabezado son los siguientes:

Flags (Indicadores): muestra los indicadores establecidos en la dirección de multidifusión. El tamaño de este campo es de 4 bits. Según el RFC 2373, el único indicador definido es el indicador de provisionalidad, Transient (T). El indicador T utiliza el bit de orden inferior del campo Flags. Cuando se establece en el valor 0, el indicador T indica que la dirección de multidifusión es una dirección asignada de forma definitiva (bien conocida) por la Autoridad de números asignados de Internet (IANA, *Internet Assigned Numbers Authority*). Cuando se establece en el valor 1, el indicador T especifica que la dirección de multidifusión es transitoria (no está definitivamente asignada).

Scope (Ámbito): indica el ámbito de la red interna de IPv6 para la que está previsto el tráfico de multidifusión. El tamaño de este campo es de 4 bits. Además de la información proporcionada por los protocolos de enrutamiento de multidifusión, los enrutadores utilizan el ámbito de multidifusión para determinar si se puede reenviar el tráfico de multidifusión. En la tabla A.3 se muestran los valores definidos para el campo Scope.

Valor	Ámbito
0	Reservado
1	Ámbito local de nodo
2	Ámbito local de enlace
5	Ámbito local de sitio
8	Ámbito local de organización
E	Ámbito global
F	Reservado

Tabla A. 3. Valores definidos para el campo Scope

Por ejemplo, el tráfico con la dirección de multidifusión FF02:: tiene un ámbito local de enlace. Un enrutador IPv6 nunca reenvía este tráfico más allá del enlace local.

Id. de grupo: identifica el grupo de multidifusión y es único en el ámbito. El tamaño de este campo es de 112 bits. Los Id. de grupo asignados definitivamente son independientes del ámbito. Los Id. de grupo transitorios sólo son relevantes para un ámbito determinado. Las direcciones de multidifusión comprendidas entre FF01:: y FF0F:: son direcciones bien conocidas y reservadas.

Para identificar todos los nodos de los ámbitos locales de nodo y de enlace, se definen las siguientes direcciones:

- FF01::1 (dirección de multidifusión para todos los nodos del ámbito local de nodo)
- FF02::1 (dirección de multidifusión para todos los nodos del ámbito local de enlace)

Para identificar todos los enrutadores de los ámbitos locales de nodo, de enlace y de sitio, se definen las siguientes direcciones:

- FF01::2 (dirección de multidifusión para todos los enrutadores del ámbito local de nodo)
- FF02::2 (dirección de multidifusión para todos los enrutadores del ámbito local de enlace)
- FF05::2 (dirección de multidifusión para todos los enrutadores del ámbito local de sitio)

Con 112 bits en el Id. de grupo, es posible tener 2^{112} Id. de grupo. Sin embargo, debido a la forma en la que las direcciones de multidifusión IPv6 se asignan a las direcciones MAC de multidifusión Ethernet, el RFC 2373 recomienda asignar el Id. de grupo a partir de los 32 bits de orden inferior de la dirección de multidifusión IPv6 y establecer en cero los demás bits del Id. de grupo original. Al utilizarse únicamente los 32 bits de orden inferior, cada Id. de grupo se asigna a una dirección MAC de multidifusión Ethernet única. En la figura A.6 se muestra la dirección de multidifusión IPv6 modificada.

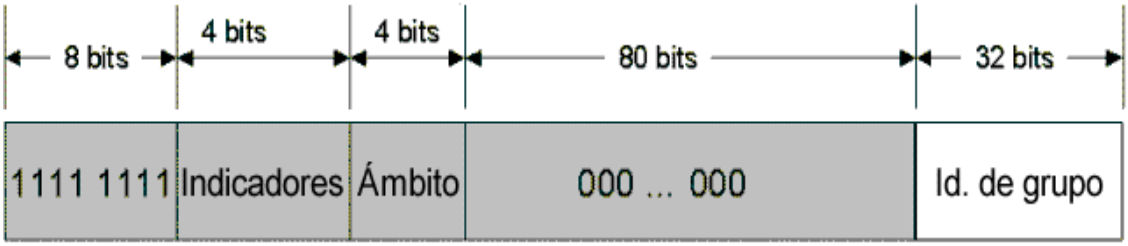

Figura A. 6. Dirección de multidifusión IPv6 modificada con un Id. de grupo de 32 bits

4.9 DIRECCIONES IPv6 PARA CUALQUIER DIFUSIÓN

Una dirección para cualquier difusión se asigna a varias interfaces. La infraestructura de enrutamiento reenvía los paquetes dirigidos a una dirección de unidifusión a la interfaz más próxima a la que esté asignada la dirección para cualquier difusión. Para facilitar la entrega, la infraestructura de enrutamiento debe conocer las interfaces a las que se asignan direcciones para cualquier difusión y su "distancia" en términos de medida de enrutamiento. Actualmente, las direcciones para cualquier difusión sólo se utilizan como direcciones de destino y se asignan únicamente a los enrutadores. Las direcciones para cualquier difusión se asignan fuera del espacio de direcciones de unidifusión y el ámbito de una dirección para cualquier difusión es el ámbito del tipo de dirección de unidifusión desde el que se asigna la dirección para cualquier difusión.

La dirección para cualquier difusión de Subred-Enrutador está predefinida y es necesaria. Se crea a partir del prefijo de subred para una interfaz dada. Para crear la dirección para cualquier difusión de Subred-Enrutador, los bits del prefijo de subred quedan fijos en sus valores correspondientes y los bits restantes se establecen en 0. La figura A.7 ilustra la dirección para cualquier difusión de Subred-Enrutador.

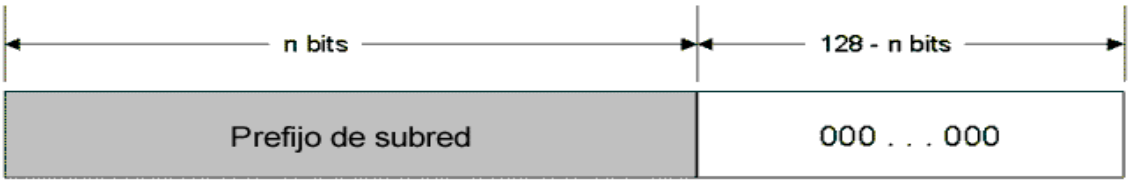

Figura A. 7. Dirección para cualquier difusión de Subred-Enrutador

Todas las interfaces de enrutador conectadas a una subred se asignan a la dirección para cualquier difusión de Subred-Enrutador de la subred. La dirección para cualquier difusión de Subred-Enrutador se utiliza para la comunicación con uno o varios enrutadores conectados a una subred remota.

4.10 DIRECCIONES IPv6 PARA UN HOST

Por lo general, un host IPv4 con un solo adaptador de red tiene una única dirección IPv4 asignada al adaptador. Sin embargo, un host IPv6 suele tener varias direcciones IPv6, incluso con una sola interfaz. A un host IPv6 se le asignan las siguientes direcciones de unidifusión:

- Una dirección local de enlace para cada interfaz.
- Direcciones de unidifusión para cada interfaz (que podrían ser una dirección local de sitio y una o varias direcciones de unidifusión global agregables).
- Una dirección de bucle de retroceso (::1).

Un host IPv6 típico es multitarjeta (tiene varias interfaces o direcciones) porque tiene al menos dos direcciones con las que puede recibir paquetes (una dirección local de enlace para el tráfico del enlace local y una dirección agregable o local de sitio que se puede enrutar).

Además, cada host escucha el tráfico en las siguientes direcciones de multidifusión:

- La dirección de multidifusión de todos los nodos del ámbito local de nodo (FF01::1).
- La dirección de multidifusión de todos los nodos del ámbito local de enlace (FF02::1).
- La dirección de nodo solicitado para cada dirección de unidifusión.
- Las direcciones de multidifusión de los grupos unidos.

4.11 DIRECCIONES IPv6 PARA UN ENRUTADOR

A un enrutador IPv6 se le asignan las siguientes direcciones de unidifusión:

- Una dirección local de enlace para cada interfaz.
- Direcciones de unidifusión para cada interfaz (que podrían ser una dirección local de sitio y una o varias direcciones de unidifusión global agregables).
- Una dirección para cualquier difusión de Subred-Enrutador.

- Direcciones adicionales para cualquier difusión (opcional).
- Una dirección de bucle de retroceso (::1).

Además, cada enrutador escucha el tráfico en las siguientes direcciones de multidifusión:

- La dirección de multidifusión de todos los nodos del ámbito local de nodo (FF01::1).
- La dirección de multidifusión de todos los enrutadores del ámbito local de nodo (FF01::2).
- La dirección de multidifusión de todos los nodos del ámbito local de enlace (FF02::1).
- La dirección de multidifusión de todos los enrutadores del ámbito local de enlace (FF02::1).
- La dirección de multidifusión de todos los enrutadores del ámbito local de sitio (FF05::2).
- La dirección de nodo solicitado para cada dirección de unidifusión.
- Las direcciones de multidifusión de los grupos unidos.

4.12 IPV6 Y DNS

En el RFC 1886 se describen varias mejoras realizadas en el Sistema de nombres de dominio (DNS) para IPv6, las cuales incluyen las novedades siguientes:

- Registro de recursos de direcciones de host (AAAA).
- Dominio IP6.INT para consultas inversas

4.12.1 REGISTRO DE RECURSOS DE DIRECCIONES DE HOST (AAAA)

Se utiliza un nuevo tipo de registro de recursos DNS, AAAA (denominado "cuatro as"), para resolver un nombre de dominio completo en una dirección IPv6. Es comparable al registro de recursos de direcciones de host (A) que se utiliza con IPv4. El tipo de registro de recursos se denomina AAAA (valor de tipo 28) porque las direcciones IPv6 de 128 bits son cuatro veces mayores que las direcciones IPv4 de 32 bits. A continuación, se muestra un ejemplo de un registro de recursos AAAA:

host1.unicauca.edu.co IN AAAA FEC0::2AA:FF:FE3F:2A1C

Un host debe especificar una consulta AAAA o una consulta general para un nombre de host específico para recibir datos de resolución de direcciones IPv6 en las secciones de respuesta de las consultas DNS.

4.12.2 EL DOMINIO IP6.INT

El dominio IP6.INT se ha creado para las consultas IPv6 inversas. Las consultas inversas, también denominadas consultas de puntero, determinan un nombre de host basado en la dirección IP. Para crear el espacio de nombres para las consultas inversas, cada dígito hexadecimal de la dirección IPv6 de 32 dígitos completamente expresada se convierte en un nivel independiente en el orden opuesto en la jerarquía de dominios inversa.

Por ejemplo, el nombre de dominio de búsqueda inversa para la dirección FEC0::2AA:FF:FE3F:2A1C (que de forma completa se expresa como FEC0:0000:0000:0000:02AA: 00FF:FE3F:2A1C) es:

C.1.A.2.F.3.E.F.F.F.0.0.A.A.2.0.0.0.0.0.0.0.0.0.0.0.0.C.E.F.IP6.INT.

4.13 DIRECCIONES IPv4 Y SUS EQUIVALENTES EN IPv6

En la tabla A.4 se muestran direcciones y conceptos de direccionamiento de IPv4 y sus equivalentes en IPv6.

Dirección IPv4	Dirección IPv6
Clases de direcciones de Internet	No se ha implementado en IPv6
Direcciones de multidifusión (224.0.0.0/4)	Direcciones de multidifusión IPv6 (FF00::/8)
Direcciones de difusión	No se ha implementado en IPv6
La dirección no especificada es 0.0.0.0	La dirección no especificada es ::
La dirección de bucle de retroceso es 127.0.0.1	La dirección de bucle de retroceso es ::1
Direcciones IP públicas	Direcciones de unidifusión global agregables
Direcciones IP privadas (10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16)	Direcciones locales de sitio (FEC0::/48)
Direcciones configuradas automáticamente (169.254.0.0/16)	Direcciones locales de enlace (FE80::/64)
Representación de texto: notación decimal con puntos	Representación de texto: formato hexadecimal con signos de dos puntos, supresión de ceros a la izquierda y compresión de ceros. Las direcciones compatibles con IPv4 se expresan en notación decimal con puntos.
Representación de bits de red: máscara de subred en notación decimal o longitud de prefijo	Representación de bits de red: sólo longitud de prefijo
Resolución de nombres DNS: registro de recursos de direcciones de host IPv4 (A)	Resolución de nombres DNS: registro de recursos de direcciones de host IPv6 (AAAA)
Resolución de DNS inversa: dominio IN-ADDR.ARPA	Resolución de DNS inversa: dominio IP6.INT

Tabla A. 4. Asignación actual del espacio de direcciones de IPv6

5. ENCABEZADO DE IPV6

El encabezado de IPv6 es una versión optimizada del encabezado de IPv4. Elimina campos innecesarios o que se utilizan raramente y agrega campos más apropiados para el tráfico en tiempo real. Revisar el encabezado de IPv4 puede ayudar a comprender el encabezado de IPv6.

5.1 ENCABEZADO DE IPV4

En la figura A.8 se muestra el encabezado de IPv4, que se describe en el RFC 791.

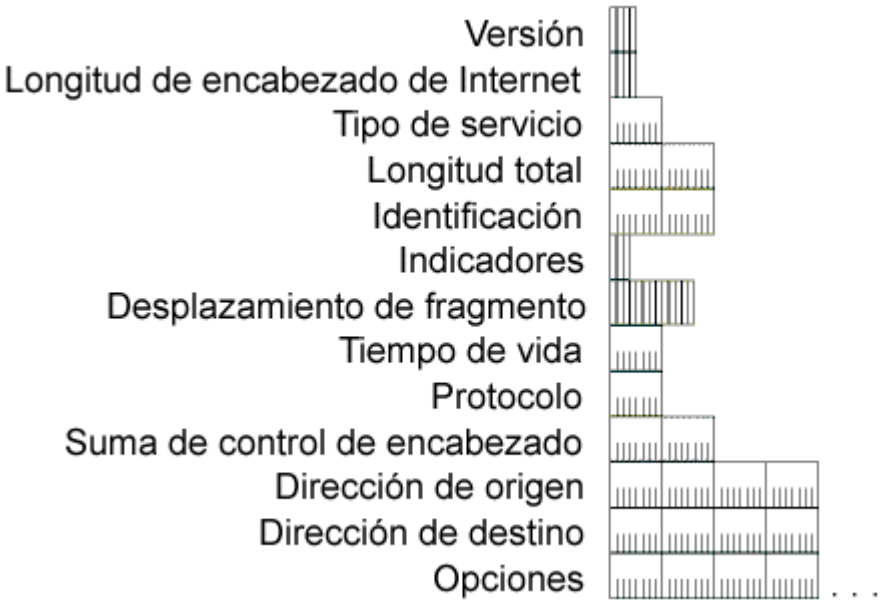

Figura A. 8. Encabezado de IPv4

Los campos del encabezado son los siguientes:

Version (Versión): indica la versión de IP y se establece en el valor 4. El tamaño de este campo es de 4 bits.

Internet Header Length (Longitud de encabezado de Internet): indica el número de bloques de 4 bytes que hay en el encabezado de IP. El tamaño de este campo es de 4 bits. Como el tamaño mínimo de un encabezado de IP es de 20 bytes, el valor menor del campo de longitud del encabezado de Internet (IHL, *Internet Header Length*) es 5. Las opciones de IP pueden ampliar el tamaño mínimo del encabezado de IP en incrementos de 4 bytes. Si una opción de IP no utiliza los 4 bytes del campo de opción de IP, los bytes restantes se rellenan con ceros, con lo que el encabezado de IP se convierte en un número de 32 bits (4 bytes). Con un valor máximo de 0xF, el tamaño máximo del encabezado de IP, incluidas las opciones, es de 60 bytes (15*4).

Type of Service (Tipo de servicio): indica el servicio deseado que espera este paquete para la entrega a través de enrutadores en la red IP interna. El tamaño de este campo es de 8 bits, entre los que se encuentran los que indican las características de preferencia, retardo, rendimiento y confiabilidad.

Total Length (Longitud total): indica la longitud total del paquete IP (encabezado de IP + carga IP) y no incluye tramas de nivel de enlace. El tamaño de este campo es de 16 bits, lo que puede indicar un paquete IP de hasta 65.535 bytes.

Identification (Identificación): identifica este paquete IP específico. El tamaño de este campo es de 16 bits. El origen del paquete IP selecciona el campo de identificación. Si el paquete IP está fragmentado, todos los fragmentos conservan el valor del campo de identificación de modo que el nodo de destino puede agrupar los fragmentos para reensamblarlos.

Flags (Indicadores): identifica los indicadores del proceso de fragmentación. El tamaño de este campo es de 3 bits; sin embargo, sólo hay 2 bits definidos para el uso actual. Hay dos indicadores: uno para señalar si el paquete IP se puede fragmentar y otro para indicar si hay otros fragmentos que siguen al fragmento actual.

Fragment Offset (Desplazamiento de fragmentos): indica la posición del fragmento en relación a la carga IP original. El tamaño de este campo es de 13 bits.

Time to Live (Tiempo de vida): indica el número máximo de enlaces por los que puede viajar un paquete IP antes de ser descartado. El tamaño de este campo es de 8 bits. El campo Time-to-Live (TTL) se utilizaba inicialmente como recuento del tiempo con el que un enrutador de IP determinaba el tiempo necesario (en segundos) para reenviar el paquete IP, con la disminución correspondiente de TTL. Los enrutadores modernos reenvían casi siempre un paquete IP en menos de un segundo y, según el RFC 791, deben disminuir TTL en uno como mínimo. Por lo tanto, TTL se convierte en un recuento de enlaces máximos con el valor especificado por el nodo de envío. Cuando el valor TTL es igual a 0, el paquete se descarta y se envía un mensaje Time Expired (Fin de tiempo de espera) de ICMP a la dirección IP de origen.

Protocol (Protocolo): identifica el protocolo de nivel superior. El tamaño de este campo es de 8 bits. Por ejemplo, TCP utiliza un protocolo de 6, UDP utiliza un protocolo de 17 e ICMP utiliza un protocolo de 1. El campo Protocol se utiliza para cancelar la multiplexación de un paquete IP en el protocolo de nivel superior.

Header Checksum (Suma de comprobación del encabezado): proporciona una suma de comprobación sólo para el encabezado de IP. El tamaño de este campo es de 16 bits. La carga IP no se incluye en el cálculo de suma de comprobación como carga IP y suele contener su propia suma de comprobación. Cada nodo IP que recibe paquetes IP consulta el campo Header Checksum del encabezado IP y descarta, sin notificarlo, el paquete IP si la comprobación de la suma no es correcta. Cuando un enrutador reenvía un paquete IP, debe

disminuir TTL. Por lo tanto, la suma de comprobación del encabezado se vuelve a calcular en cada salto entre el origen y el destino.

Source Address (Dirección de origen): almacena la dirección IP del host de origen. El tamaño de este campo es de 32 bits.

Destination Address (Dirección de destino): almacena la dirección IP del host de destino. El tamaño de este campo es de 32 bits.

Options (Opciones): almacena una o más opciones de IP. El tamaño de este campo es un múltiplo de 32 bits. Si la opción u opciones de IP no utilizan los 32 bits, se pueden agregar opciones de relleno para que el encabezado de IP sea un número de cuatro bloques de 4 bytes que puede indicar el campo Internet Header Length (Longitud de encabezado de Internet).

5.2 ESTRUCTURA DE UN PAQUETE IPV6

En la figura A.9 se muestra la estructura de un paquete IPv6.

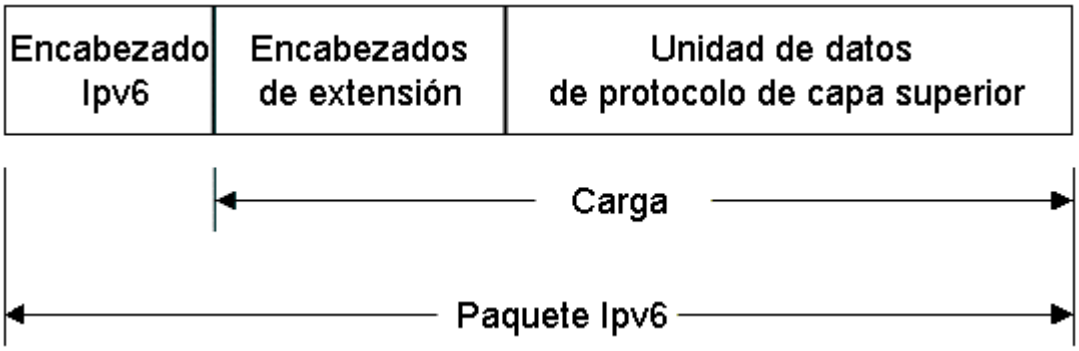

Figura A. 9. Estructura de un paquete IPv6

- **Encabezado de IPv6**

El encabezado de IPv6 siempre está presente y tiene un tamaño fijo de 40 bytes. Los campos del encabezado de IPv6 se describen detalladamente más adelante en este mismo anexo.

- **Encabezados de extensión**

Puede no haber ninguno o que haya varios encabezados de extensión con distintas longitudes. Un campo Next Header (Encabezado siguiente) en el encabezado de IPv6 indica el siguiente encabezado de extensión. En cada encabezado de extensión hay otro campo Next Header que indica el siguiente encabezado de extensión. El último encabezado de extensión indica el protocolo de nivel superior (como TCP, UDP o ICMPv6) contenido en la unidad de datos del protocolo de nivel superior.

El encabezado de IPv6 y los encabezados de extensión reemplazan al encabezado de IPv4 con opciones. El formato del nuevo encabezado de extensión permite ampliar IPv6 para que pueda responder a futuras necesidades y ofrezca más capacidades. A diferencia de las opciones del encabezado de IPv4, los encabezados de extensión de IPv6 no tienen un tamaño máximo y pueden ampliarse para aceptar todos los datos de extensión necesarios para la comunicación con IPv6.

- **Unidad de datos del protocolo de nivel superior**

La unidad de datos de protocolo (PDU, *Protocol Data Unit*) de nivel superior suele constar de un encabezado de protocolo de nivel superior y su carga (por ejemplo, un mensaje ICMPv6, un mensaje UDP o un segmento TCP).

La carga del paquete IPv6 es la combinación de los encabezados de extensión de IPv6 y la unidad PDU de nivel superior. Normalmente, puede tener hasta 65.535 bytes. Las cargas con una longitud superior a los 65.535 bytes se pueden enviar mediante la opción de carga Jumbo en el encabezado de extensión Hop-by-Hop Options (Opciones de salto a salto).

5.3 ENCABEZADO DE IPV6

En la figura A.10 se muestra el encabezado IPv6 tal como se define en el RFC 2460.

Figura A. 10. Encabezado de IPv6

Los campos del encabezado son los siguientes:

Version (Versión): se utilizan 4 bits para indicar la versión de IP, que se establece en el valor 6.

Traffic Class (Clase de tráfico): indica la clase o la prioridad del paquete IPv6. El tamaño de este campo es de 8 bits. El campo Traffic Class proporciona una funcionalidad similar a la del campo Type of Service (Tipo de servicio) de IPv4. En el RFC 2460, no están definidos los valores del campo Traffic Class. Sin embargo, se necesita una

implementación de IPv6 para proporcionar un medio que permita a un protocolo de nivel de aplicación especificar el valor del campo Traffic Class para experimentación.

Flow Label (Etiqueta de flujo): indica que este paquete pertenece a una secuencia específica de paquetes entre un origen y un destino, lo que requiere un control especial por parte de los enrutadores IPv6 intermedios. El tamaño de este campo es de 20 bits. El campo Flow Label se utiliza para conexiones de calidad de servicio que no son predeterminadas, como las que se necesitan para los datos en tiempo real (voz y vídeo). Para el control del enrutador predeterminado, el campo Flow Label se establece en el valor 0. Puede haber varios flujos entre un origen y un destino, lo que se distingue mediante etiquetas de flujo independientes con un valor distinto de cero.

Payload Length (Longitud de carga): indica la longitud de la carga IP. El tamaño de este campo es de 16 bits. El campo Payload Length incluye los encabezados de extensión y la unidad PDU de nivel superior. Con 16 bits, se puede indicar una carga IPv6 de hasta 65.535 bytes. Para longitudes de carga superiores a 65.535 bytes, el campo Payload Length se establece en el valor 0 y se utiliza la opción de carga Jumbo en el encabezado de extensión Hop-by-Hop Options (Opciones de salto a salto).

Next Header (Encabezado siguiente): indica el primer encabezado de extensión (si existe) o el protocolo de la unidad PDU de nivel superior (como TCP, UDP o ICMPv6). El tamaño de este campo es de 8 bits. Cuando se indica un protocolo de nivel superior por encima de la capa de Internet, se utilizan aquí los mismos valores que en el campo Protocol (Protocolo) de IPv4.

Hop Limit (Límite de saltos): indica el número máximo de enlaces por los que puede viajar el paquete IPv6 antes de que se descarte. El tamaño de este campo es de 8 bits. El campo Hop Limit es similar al campo TTL de IPv4, excepto en que no existe ninguna relación histórica en cuanto al tiempo (en segundos) que el paquete está en cola en el enrutador. Cuando el límite de saltos es igual a 0, el paquete se descarta y se envía un mensaje Time Expired (Fin de tiempo de espera) de ICMP a la dirección IP de origen.
Source Address (Dirección de origen): almacena la dirección IPv6 del host de origen. El tamaño de este campo es de 128 bits.

Destination Address (Dirección de destino): almacena la dirección IPv6 del host de destino actual. El tamaño de este campo es de 128 bits. En la mayoría de los casos, la dirección de destino se establece en la dirección de destino final. Sin embargo, si hay un encabezado de extensión de enrutamiento, la dirección de destino se puede establecer en la interfaz del siguiente enrutador de la lista de rutas de origen.

VALORES DEL CAMPO NEXT HEADER (ENCABEZADO SIGUIENTE)
En la tabla A.5 se muestran valores típicos del campo Next Header para un encabezado de IPv6 o un encabezado de extensión IPv6.

Valor (en notación decimal)	Encabezado
0	Encabezado Hop-by-Hop Options (Opciones de salto a salto)
6	TCP
17	UDP
41	Encabezado de IPv6 encapsulado
43	Encabezado Routing (Enrutamiento)
44	Encabezado Fragmentation (Fragmentación)
46	Protocolo de reserva de recursos (RSVP)
50	Carga de seguridad de encapsulación
51	Encabezado Authentication (Autenticación)
58	ICMPv6
59	No hay encabezado siguiente
60	Encabezado Destination Options (Opciones de destino)

Tabla A. 5. Valores del campo Next Header

5.4 DIFERENCIAS ENTRE LOS ENCABEZADOS DE IPV4 E IPV6

En la tabla A.6 se muestran las diferencias entre los campos de encabezado de IPv4 e IPv6.

Campo de encabezado de IPv4	Campo de encabezado de IPv6
Version (Versión)	El mismo campo, con números de versión distintos.
Header Length (Longitud del encabezado)	Se ha quitado en IPv6. IPv6 no incluye el campo Header Length porque el encabezado de IPv6 tiene siempre el tamaño fijo de 40 bytes. Cada encabezado de extensión tiene un tamaño fijo o indica su propio tamaño.
Type of Service (Tipo de servicio)	En IPv6, se ha reemplazado por el campo Traffic Class (Clase de tráfico).
Total Length (Longitud total)	En IPv6, se ha reemplazado por el campo Payload Length (Longitud de carga), que sólo indica el tamaño de la carga.
Identification (Identificación)	Se ha quitado en IPv6. En el encabezado de IPv6 no se incluye información de fragmentación. Se encuentra en un encabezado de extensión Fragment (Fragmento).
Fragmentation Flags (Indicadores de fragmentación)	Se ha quitado en IPv6. En el encabezado de IPv6 no se incluye información de fragmentación. Se encuentra en un encabezado de extensión Fragment.

Fragment Offset (Desplazamiento de fragmentos)	Se ha quitado en IPv6. En el encabezado de IPv6 no se incluye información de fragmentación. Se encuentra en un encabezado de extensión Fragment.
Time To Live (TTL o Tiempo de vida)	En IPv6, se ha reemplazado por el campo Hop Limit (Límite de saltos).
Protocol (Protocolo)	En IPv6, se ha reemplazado por el campo Next Header (Encabezado siguiente).
Header Checksum (Suma de comprobación de encabezado)	Se ha quitado en IPv6. En IPv6, la detección de errores en el nivel de bit para todo el paquete IPv6 se realiza en el nivel de enlace.
Source Address (Dirección de origen)	El campo es el mismo, excepto en que las direcciones de IPv6 tienen una longitud de 128 bits.
Destination Address (Dirección de destino)	El campo es el mismo, excepto en que las direcciones de IPv6 tienen una longitud de 128 bits.
Options (Opciones)	Se ha quitado en IPv6. Las opciones de IPv4 se reemplazan por encabezados de extensión de IPv6.

Tabla A. 6. Campos de encabezado de IPv4 y sus equivalentes en IPv6

5.5 ENCABEZADOS DE EXTENSIÓN DE IPV6

El encabezado de IPv4 incluye todas las opciones. Por lo tanto, cada enrutador intermedio debe comprobar su existencia y procesarlas cuando están presentes. Esto puede causar un deterioro del rendimiento en el reenvío de paquetes IPv4. Con IPv6, las opciones de entrega y reenvío pasan a los encabezados de extensión. El único encabezado de extensión que debe procesarse en cada enrutador intermedio es el encabezado de extensión Hop-by-Hop Options (Opciones de salto a salto). Así aumenta la velocidad de procesamiento del encabezado de IPv6 y mejora el rendimiento del proceso de reenvío.

En el RFC 2460 se definen los siguientes encabezados de extensión de IPv6 que deben admitir todos los nodos de IPv6:

- Encabezado Hop-by-Hop Options (Opciones de salto a salto)
- Encabezado Destination Options (Opciones de destino)
- Encabezado Routing (Enrutamiento)
- Encabezado Fragment (Fragmento)
- Encabezado Authentication (Autenticación)
- Encabezado Encapsulating Security Payload (ESP o Carga de seguridad de encapsulación)

En un paquete IPv6 típico, no hay encabezados de extensión. Si se precisa un tratamiento especial por parte de los enrutadores intermedios o del destino, el host de envío agrega uno o varios encabezados de extensión.

Cada encabezado de extensión debe adaptarse a los límites de 64 bits (8 bytes). Los encabezados de extensión de tamaño variable contienen un campo Header Extension Length (Longitud de extensión de encabezado) y deben utilizar el relleno cuando sea necesario para asegurarse de que el tamaño sea múltiplo de 8 bytes.

En la figura A.11 se muestra el campo Next Header (Encabezado siguiente) y ninguno o varios encabezados de extensión que componen una cadena de punteros. Cada puntero indica el tipo de encabezado que viene después del encabezado inmediato hasta que el protocolo de nivel superior se identifica definitivamente.

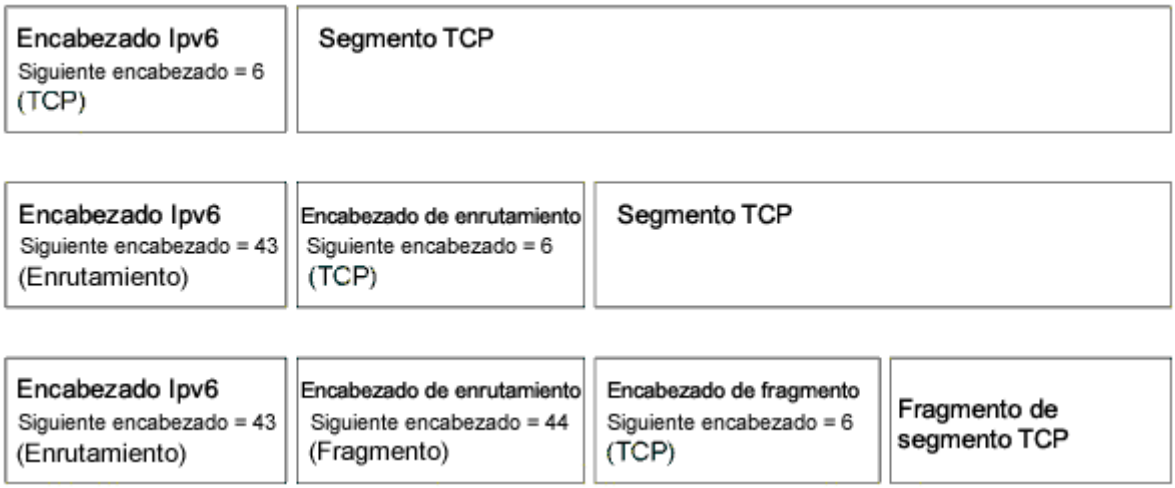

Figura A. 11. Encabezados de extensión de IPv6

ORDEN DE LOS ENCABEZADOS DE EXTENSIÓN

Los encabezados de extensión se procesan en el orden en el que se encuentran. Dado que el único encabezado de extensión procesado por todos los nodos de la ruta de acceso es el encabezado Hop-by-Hop Options (Opciones de salto a salto), debe ser el primero. Hay normas similares para otros encabezados de extensión. En el RFC 2460, se recomienda que los encabezados de extensión se coloquen en el encabezado de IPv6 en el orden siguiente:

1. Encabezado Hop-by-Hop Options (Opciones de salto a salto)
2. Encabezado Destination Options (Opciones de destino), para destinos intermedios cuando hay encabezado Routing (Enrutamiento).
3. Encabezado Routing (Enrutamiento)
4. Encabezado Fragment (Fragmento)
5. Encabezado Authentication (Autenticación)
6. Encabezado Encapsulating Security Payload (ESP o Carga de seguridad de encapsulación)
7. Encabezado Destination Options (Opciones de destino), para el destino final

5.5.1 ENCABEZADO HOP-BY-HOP OPTIONS (OPCIONES DE SALTO A SALTO)

El encabezado Hop-by-Hop Options se utiliza para especificar parámetros de entrega en cada salto de la ruta de acceso al destino. Se identifica por el valor 0 en el campo Next Header (Encabezado siguiente) del encabezado de IPv6. En la figura A.12 se muestra el encabezado Hop-by-Hop Options.

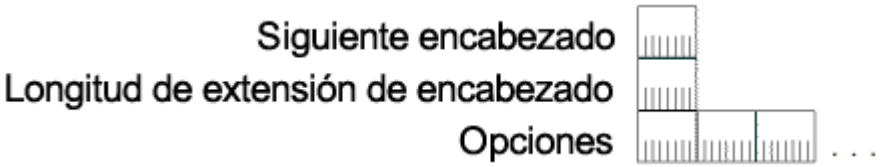

Figura A. 12. Encabezado Hop-by-Hop Options (Opciones de salto a salto)

El encabezado Hop-by-Hop Options consta de un campo Next Header (Encabezado siguiente), un campo Header Extension Length (Longitud de extensión del encabezado) y un campo Options (Opciones) que contiene una o varias opciones. El valor del campo Header Extension Length es el número de bloques de 8 bytes del encabezado de extensión Hop-by-Hop Options, sin incluir los 8 primeros bytes. Por lo tanto, para un encabezado Hop-by-Hop Options de 8 bytes, el valor del campo Header Extension Length es 0. Se utilizan opciones de relleno para garantizar límites de 8 bytes.

Una opción es un encabezado dentro del encabezado de opciones de salto a salto que describe una característica específica de la entrega del paquete o proporciona relleno. Cada opción se codifica en el formato tipo-longitud-valor (TLV), que se utiliza comúnmente en los protocolos TCP/IP. El tipo de opción identifica a la opción y determina el tipo de tratamiento por parte del nodo de procesamiento. La longitud de la opción identifica su longitud. El valor de la opción son los datos asociados a ésta.

En el RFC 2460, 2675 y 2711 se definen las siguientes opciones:

- La opción Pad1 (tipo de opción 0) se utiliza para insertar un solo byte de relleno.
- La opción PadN (tipo de opción 1) se utiliza para insertar 2 o más bytes de relleno.
- La opción Jumbo Payload (tipo de opción 194) se utiliza para indicar un tamaño de carga superior a 65.535 bytes. Con la opción Jumbo Payload (Carga Jumbo), se pueden indicar tamaños de carga de hasta 4.294.967.295 bytes mediante un campo Jumbo Payload Length (Longitud de carga Jumbo) de 32 bits. Un paquete IPv6 con un tamaño de carga mayor de 65.535 bytes se denomina *jumbograma*.
- La opción Router Alert (tipo de opción 5) se utiliza para indicar al enrutador que el contenido del paquete requiere procesamiento adicional. La opción Router Alert (Alerta de enrutador) se utiliza para el Descubrimiento de escucha de multidifusión (Multicast Listener Discovery) y el Protocolo de reserva de recursos (RSVP, *Resource ReServation Protocol*).

5.5.2 ENCABEZADO DESTINATION OPTIONS (OPCIONES DE DESTINO)

El encabezado Destination Options se utiliza para especificar parámetros de entrega de paquetes para destinos intermedios o para el destino final. Este encabezado se identifica mediante el valor 60 en el campo Next Header (Encabezado siguiente) del encabezado anterior. En la figura A.13 se muestra el encabezado Destination Options.

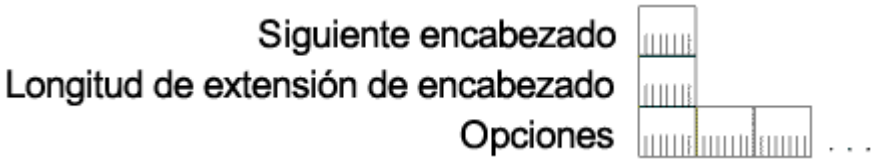

Figura A. 13. Encabezado Destination Options (Opciones de destino)

Los campos del encabezado Destination Options se definen del mismo modo que el encabezado Hop-by-Hop Options (Opciones de salto a salto).

El encabezado Destination Options se utiliza de dos maneras:

1. Si hay un encabezado Routing (Enrutamiento), especifica opciones de entrega o de proceso en cada destino intermedio.
2. También especifica opciones de entrega o de proceso en el destino final.

5.5.3 ENCABEZADO ROUTING (ENRUTAMIENTO)

De forma similar al enrutamiento de origen que admite IPv4, los nodos de origen de IPv6 pueden utilizar el encabezado de extensión Routing para especificar una ruta de origen, una lista de destinos intermedios para que el paquete viaje por su ruta de acceso al destino final. El encabezado Routing se identifica mediante el valor 43 en el campo Next Header (Encabezado siguiente) del encabezado anterior.

El encabezado Routing consta de un campo Next Header, un campo Header Extension Length (que se define del mismo modo que en el encabezado de extensión Hop-by-Hop Options), un campo Routing Type (Tipo de enrutamiento), un campo Segments Left (Segmentos restantes) y datos específicos del tipo de enrutamiento.

Para el tipo de enrutamiento 0, que se define en RFC 2460, los datos específicos del tipo de enrutamiento son una lista de direcciones de destinos intermedios. Cuando el paquete IPv6 llega a un destino intermedio, se procesa el encabezado Routing y la dirección del siguiente destino intermedio (según el valor del campo Segments Left) se convierte en la dirección de destino del encabezado de IPv6. En la figura A.14 se muestra el encabezado Routing para el tipo de enrutamiento 0.

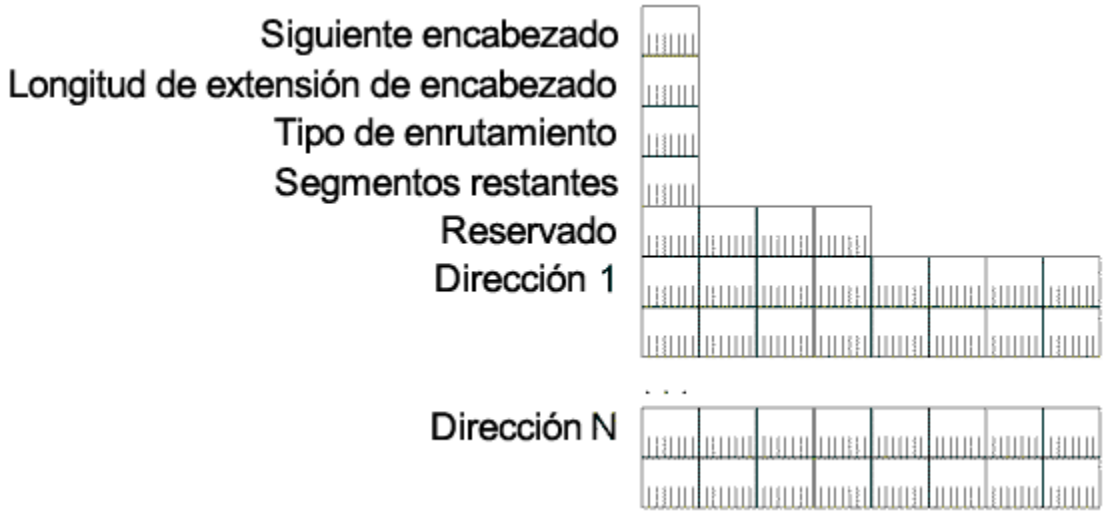

Figura A. 14. Encabezado Routing (Enrutamiento) para el tipo de enrutamiento 0

5.5.4 ENCABEZADO FRAGMENT (FRAGMENTO)

El encabezado Fragment se utiliza para los servicios de reensamblado y fragmentación de IPv6. Este encabezado se identifica por el valor 44 en el campo Next Header (Encabezado siguiente) del encabezado anterior. En la figura A.15 se muestra el encabezado Fragment.

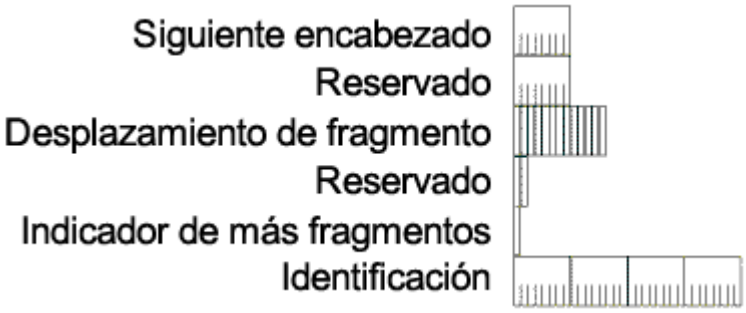

Figura A. 15. Encabezado Fragment (Fragmento)

El encabezado Fragment incluye un campo Next Header, un campo Fragment Offset (Desplazamiento de fragmentos) de 13 bits, un indicador More Fragments (Más fragmentos) y un campo Identification (Identificación) de 32 bits. Los campos Fragment Offset e Identification, y el indicador More Fragments se utilizan del mismo modo que los campos correspondientes del encabezado de IPv4. Como el uso del campo Fragment Offset se define mediante bloques de fragmentos de 8 bytes, el encabezado Fragment no se puede utilizar para los jumbogramas de IPv6.

En IPv6, sólo los nodos de origen pueden fragmentar las cargas. Si la carga enviada por el protocolo de nivel superior es mayor que la unidad MTU de enlace o de ruta de acceso,

IPv6 fragmenta la carga en el origen y utiliza el encabezado de extensión Fragment para proporcionar información de reensamblado.

Cuando se fragmenta un paquete IPv6, se divide inicialmente en una parte que se puede fragmentar y otra parte que no se puede fragmentar.

- La parte que no se puede fragmentar del paquete IPv6 original debe ser procesada por cada nodo intermedio entre el nodo de fragmentación y el destino. Esta parte consta del encabezado de IPv6, el encabezado Hop-by-Hop Options (Opciones de salto a salto), el encabezado Destination Options (Opciones de destino) para destinos intermedios y el encabezado Routing.
- La parte del paquete IPv6 original que se puede fragmentar sólo debe procesarse en el nodo de destino final. Esta parte consta del encabezado Authentication, el encabezado Encapsulating Security Payload (Carga de seguridad de encapsulación), el encabezado Destination Options para el destino final y la unidad PDU de nivel superior.

A continuación, se forman los paquetes del fragmento de IPv6. Cada paquete de fragmento consta de la parte que no se puede fragmentar, un encabezado Fragment y una porción de la parte que se puede fragmentar. En la figura A.16 se muestra el proceso de fragmentación para un paquete IPv6.

Figura A. 16. Proceso de fragmentación de IPv6

5.5.5 ENCABEZADO AUTHENTICATION (AUTENTICACIÓN)

El encabezado Authentication proporciona autenticación de datos (comprobación del nodo que envió el paquete), integridad de datos (comprobación de que los datos no fueron

modificados en el tránsito) y protección contra reproducción (garantía de que los paquetes capturados no se pueden volver a transmitir ni ser aceptados nuevamente como datos válidos) para el paquete IPv6. El encabezado Authentication, que se describe en el RFC 2402, forma parte de la arquitectura de seguridad para el Protocolo Internet definida en el RFC 2401.

El encabezado Authentication se identifica por el valor 51 en el campo Next Header (Encabezado siguiente) del encabezado anterior. En la figura A.17 se muestra el encabezado Authentication.

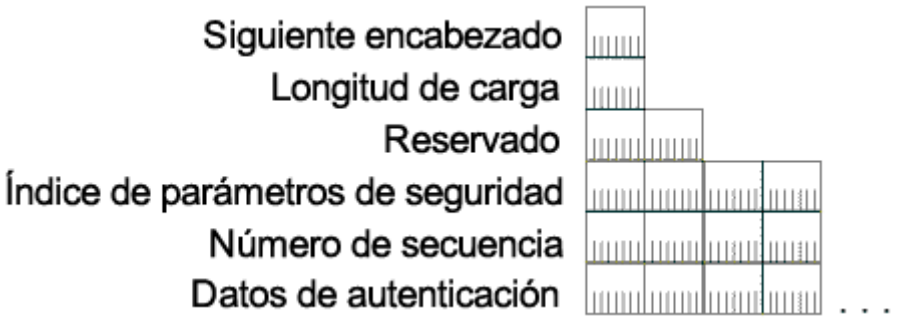

Figura A. 17. Encabezado Authentication (Autenticación)

El encabezado Authentication contiene un campo Next Header, un campo Header Length (Longitud del encabezado), un campo Security Parameters Index (SPI o Índice de parámetros de seguridad) que identifica una asociación de seguridad de seguridad IP (IPSec, *IP Security*) específica, un campo Sequence Number (Número de secuencia) que proporciona protección contra la reproducción y un campo Authentication Data (Datos de autenticación) que contiene un valor de comprobación de integridad (ICV, *Integrity Check Value*). ICV proporciona autenticación de datos e integridad.

El encabezado de extensión Authentication no proporciona servicios de confidencialidad mediante la encriptación de datos. Para proporcionar esta posibilidad, se puede utilizar el encabezado Authentication con el encabezado Encapsulating Security Payload (ESP o Carga de seguridad de encapsulación).

5.5.6 ENCABEZADO Y FINALIZADOR ENCAPSULATING SECURITY PAYLOAD (ESP O CARGA DE SEGURIDAD DE ENCAPSULACIÓN)

El encabezado y el finalizador Encapsulating Security Payload (ESP) proporcionan servicios de confidencialidad de datos, autenticación de datos e integridad de datos para la carga encapsulada. En cambio, el encabezado Authentication proporciona servicios de integridad y autenticación de datos para todo el paquete IPv6. El encabezado y el finalizador ESP se identifican por el valor 50 en el campo Next Header (Encabezado siguiente) del encabezado anterior. En la figura A.18 se muestran el encabezado y el finalizador ESP.

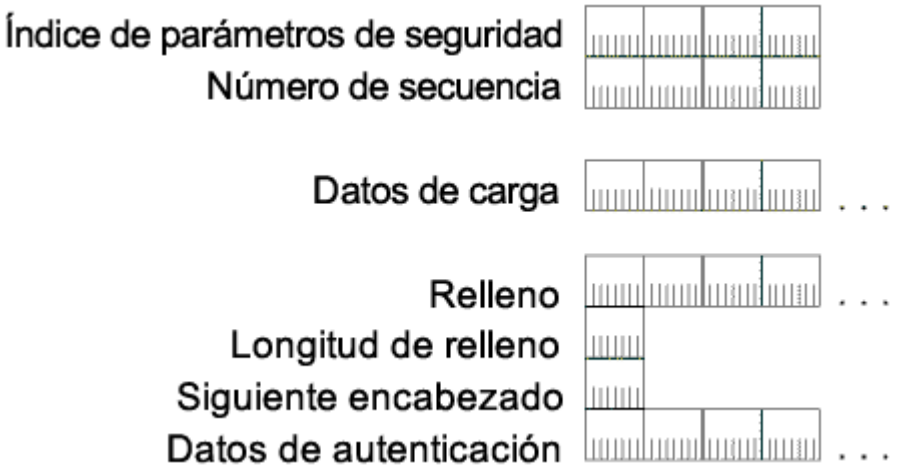

Figura A. 18. Encabezado y finalizador ESP

El encabezado ESP contiene un campo Security Parameters Index (SPI o Índice de parámetros de seguridad) que identifica la asociación de seguridad de IPSec y un campo Sequence Number (Número de secuencia) que proporciona protección contra la reproducción. El finalizador ESP contiene los campos Padding (Relleno), Padding Length (Longitud de relleno), Next Header y Authentication Data (Datos de autenticación). El campo Authentication Data contiene el valor de comprobación de integridad (ICV).

6. MTU DE IPV6

IPv6 requiere que el nivel de enlace admita un tamaño mínimo de 1.280 bytes para los paquetes IPv6. Los niveles de enlace que no admiten este tamaño deben proporcionar una combinación de fragmentación y reensamblado de nivel de enlace transparente para IPv6. En los niveles de enlace que admiten un tamaño de MTU que se puede configurar, se recomienda que se configuren con un tamaño de MTU de, al menos, 1.500 bytes (la unidad MTU IPv6 de encapsulación Ethernet II). La Unidad de recepción máxima (MRU, *Maximum Receive Unit*) de un enlace de protocolo punto a punto (PPP, *Point-to-Point Protocol*) es un ejemplo de MTU que se puede configurar.

Al igual que IPv4, IPv6 proporciona un proceso de descubrimiento de MTU de ruta de acceso mediante el mensaje Packet Too Big (Paquete demasiado grande) de ICMPv6. El descubrimiento de MTU de ruta de acceso permite la transmisión de paquetes IPv6 de tamaños superiores a 1.280 bytes.

Los hosts de origen de IPv6 pueden fragmentar cargas de protocolos de nivel superior que sean mayores que la unidad MTU de ruta de acceso mediante el proceso y el encabezado Fragment descrito anteriormente. Sin embargo, no se recomienda en absoluto utilizar la fragmentación de IPv6. Un nodo IPv6 debe ser capaz de reensamblar un paquete fragmentado con un tamaño de, al menos, 1.500 bytes.

7. ICMPV6

Al igual que IPv4, IPv6 no proporciona servicios para informar acerca de la existencia de errores. En su lugar, IPv6 utiliza una versión actualizada del Protocolo de mensajes de control de Internet (ICMP, *Internet Control Message Protocol*), denominado ICMP versión 6 (ICMPv6). ICMPv6 presenta las funciones comunes de ICMP IPv4 relativas a la elaboración de informes acerca de errores de entrega o reenvío y proporciona un servicio de eco simple para la solución de problemas.

El protocolo ICMPv6 también proporciona un marco para lo siguiente:

- **Multicast Listener Discovery (MLD o Descubrimiento de escucha de multidifusión)**

MLD es un conjunto de tres mensajes ICMP que reemplazan a la versión 2 del Protocolo de administración de grupos de Internet (IGMP) para que IPv4 administre la pertenencia a grupos de multidifusión de subred.

- **Neighbor Discovery (ND o Descubrimiento de vecino)**

Neighbor Discovery es un conjunto de cinco mensajes ICMPv6 que administran la comunicación entre nodos en un enlace. Neighbor Discovery reemplaza al Protocolo de resolución de direcciones (ARP), al proceso Router Discovery (Descubrimiento de enrutadores) de ICMPv4 y al mensaje Redirect (Redirección) de ICMPv4.

Una implementación de IPv6 requiere ICMPv6, que está documentado en el RFC 2463.

7.1 TIPOS DE MENSAJES ICMPV6

Hay dos tipos de mensajes ICMPv6:

1. **Mensajes de error**

Los mensajes de error se utilizan para informar de la existencia de errores en el reenvío o en la entrega de paquetes IPv6 por parte del nodo de destino o de un enrutador intermedio. El valor del campo Type (Tipo) de 8 bits en los mensajes de error ICMPv6 se encuentra en el intervalo comprendido entre 0 y 127 (el bit de orden superior se establece en el valor 0). Los mensajes de error ICMPv6 son Destination Unreachable (No se puede tener acceso al destino), Packet Too Big (Paquete demasiado grande), Time Exceeded (Fin de tiempo de espera) y Parameter Problem (Problema de parámetro).

2. **Mensajes informativos**

Los mensajes informativos se utilizan para proporcionar funciones de diagnóstico y otras funciones adicionales de host, como MLD y Neighbor Discovery. El valor del campo Type (Tipo) en los mensajes informativos ICMPv6 se encuentra en el intervalo comprendido entre 128 y 255 (el bit de orden superior se establece en el valor 1). Los mensajes informativos ICMPv6 se describen en el RFC 2463 e incluyen Echo Request (Solicitud de eco) y Echo Reply (Respuesta de eco).

7.1.1 ENCABEZADO DE ICMPV6

En la figura A.19 se muestra la estructura de todos los mensajes ICMPv6.

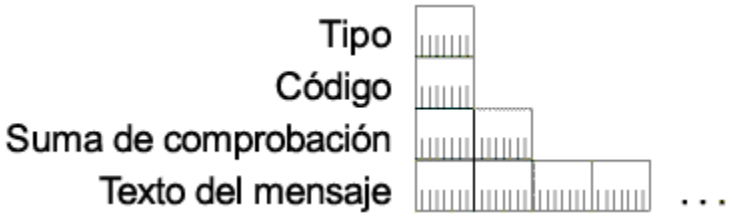

Figura A. 19. Estructura de los mensajes ICMPv6

Los campos del encabezado ICMPv6 son los siguientes:

Type (Tipo): indica el tipo de mensaje ICMPv6. El tamaño de este campo es de 8 bits. En los mensajes de error ICMPv6, el bit de orden superior se establece en el valor 0. En los mensajes informativos ICMPv6, el bit de orden superior se establece en el valor 1.

Code (Código): distingue entre varios mensajes dentro de un tipo de mensaje dado. El tamaño de este campo es de 8 bits. Si sólo hay un mensaje de un tipo dado, el campo Code se establece en 0.

Checksum (Suma de comprobación): almacena una suma de comprobación del mensaje ICMP. El tamaño de este campo es de 16 bits. El pseudo-encabezado de IPv6 se agrega al mensaje ICMPv6 cuando se calcula la suma de comprobación.

Message body (Cuerpo del mensaje): contiene datos específicos del mensaje ICMPv6.

7.1.2 MENSAJES DE ERROR ICMPV6

Los mensajes de error ICMPv6 se utilizan para informar de errores de reenvío o entrega por parte de un enrutador o del host de destino.

- ***DESTINATION UNREACHABLE (DESTINO INACCESIBLE)***

El enrutador o el host de destino envía un mensaje ICMPv6 Destination Unreachable cuando el paquete no se puede reenviar a su destino. En la figura A.20 se muestra el mensaje ICMPv6 Destination Unreachable.

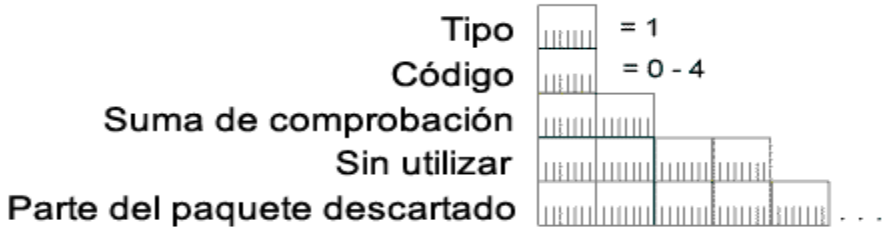

Figura A. 20. Mensaje ICMPv6 Destination Unreachable (Destino inaccesible)

En el mensaje Destination Unreachable, el campo Type (Tipo) se establece en el valor 1 y el campo Code (Código) se establece en un valor comprendido entre 0 y 4. Después del campo Checksum (Suma de comprobación) se encuentra el campo Unused (No utilizado), de 32 bits, y la porción del paquete descartado que hace que todo el paquete IPv6 que contiene el mensaje ICMPv6 no sea mayor de 1.280 bytes (la unidad MTU mínima de IPv6). El número de bytes del paquete descartado incluido en el mensaje varía si hay encabezados de extensión IPv6. Para un mensaje ICMPv6 sin encabezados de extensión, se incluyen 1.232 bytes del paquete descartado (1.280 menos un encabezado IPv6 de 40 bytes y un encabezado ICMPv6 Destination Unreachable de 8 bytes). En la tabla A.7 se muestra el valor del campo Code para los distintos mensajes Destination Unreachable.

Valor del código	Descripción
0	No se ha encontrado ninguna ruta que coincida con el destino en la tabla de enrutamiento.
1	La comunicación con el destino está prohibida por la directiva administrativa. Normalmente, se envía cuando un servidor de seguridad descarta el paquete.
2	La dirección se encuentra fuera del ámbito de la dirección de origen.
3	No se puede tener acceso a la dirección de destino. Normalmente, se envía debido a la incapacidad de resolver la dirección del nivel de enlace del destino.
4	No se puede tener acceso al puerto de destino. Normalmente, se envía cuando un paquete IPv6 que contiene un mensaje UDP ha llegado al destino, pero no había ninguna aplicación a la escucha en el puerto UDP de destino.

Tabla A. 7. Mensajes ICMPv6 Destination Unreachable (Destino inaccesible)

- ***PACKET TOO BIG (PAQUETE DEMASIADO GRANDE)***

Se envía un mensaje ICMPv6 Packet Too Big cuando el paquete no se puede reenviar debido a que la unidad MTU del enlace de reenvío es menor que el tamaño del paquete IPv6. En la figura A.21 se muestra el mensaje ICMPv6 Packet Too Big.

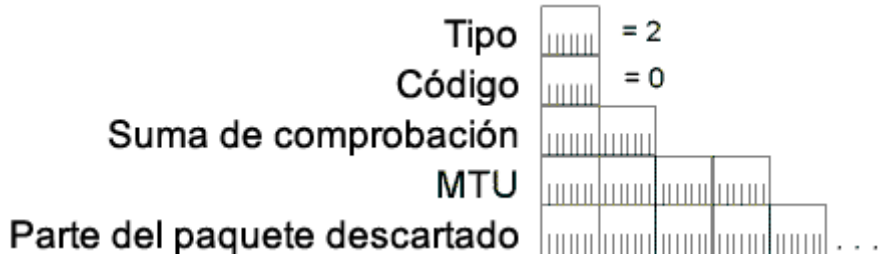

Figura A. 21. Mensaje ICMPv6 Packet Too Big (Paquete demasiado grande)

En el mensaje Packet Too Big, el campo Type (Tipo) se establece en el valor 2 y el campo Code (Código) se establece en el valor 0. Después del campo Checksum (Suma de comprobación) se encuentra el campo MTU, de 32 bits, en el que se almacena la unidad MTU del enlace sobre el que se iba a reenviar el paquete. Después sigue la parte del paquete descartado que hace que todo el paquete IPv6 que contiene el mensaje ICMPv6 tenga la longitud máxima de 1.280 bytes. El mensaje Packet Too Big se utiliza para el proceso Path MTU Discovery (Descubrimiento MTU de ruta de acceso) de IPv6 que se describe en "Path MTU Discovery (Descubrimiento de MTU de ruta de acceso)".

- ***TIME EXCEEDED (FIN DE TIEMPO DE ESPERA)***

Normalmente, un enrutador envía un mensaje ICMPv6 Time Exceeded cuando el campo Hop Limit (Límite de saltos) del encabezado de IPv6 es cero al recibir el paquete o después de reducir su valor durante el proceso de reenvío. En la figura A.22 se muestra el mensaje ICMPv6 Time Exceeded.

Figura A. 22. Mensaje ICMPv6 Time Exceeded (Fin de tiempo de espera)

En el mensaje Time Exceeded, el campo Type (Tipo) se establece en el valor 3 y el campo Code (Código) se establece en el valor 0 (cuando el campo Hop Limit del encabezado IPv6 pasa a 0) o en 1 (cuando se sobrepasa el tiempo de reensamblado de la fragmentación del host de destino). Después del campo Checksum (Suma de comprobación), se encuentra el

campo Unused (No utilizado), de 32 bits, y la parte del paquete descartado, de modo que todo el paquete IPv6 que contiene el mensaje ICMPv6 no tiene más de 1.280 bytes. La recepción de mensajes Time Exceeded para Code=0 indica que el límite de saltos de los paquetes salientes no es suficientemente grande para llegar al destino o que existe un bucle de enrutamiento.

- ***PARAMETER PROBLEM (PROBLEMA DE PARÁMETRO)***

El mensaje ICMPv6 Parameter Problem es enviado por un enrutador o por el destino. Ocurre cuando se detecta un error en el encabezado de IPv6 o en un encabezado de extensión, e impide que continúe el procesamiento de IPv6. En la figura A.23 se muestra el mensaje ICMPv6 Parameter Problem.

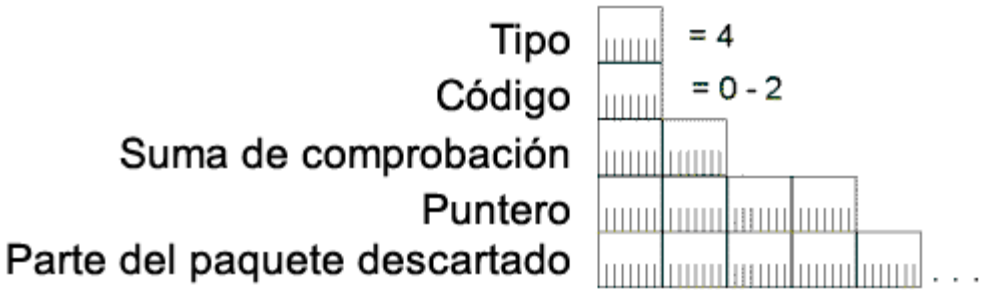

Figura A. 23. Mensaje ICMPv6 Parameter Problem (Problema de parámetro)

En el mensaje Parameter Problem, el campo Type (Tipo) se establece en el valor 4 y el campo Code (Código) es un valor comprendido entre 0 y 2. Después del campo Checksum (Suma de comprobación) se encuentra el campo Pointer (Puntero), de 32 bits, que indica el desplazamiento en bytes del paquete IPv6 en el que se detectó el error. Después del campo Pointer sigue la parte del paquete descartado, con un tamaño tal que todo el mensaje ICMPv6 no supera los 1.280 bytes. El valor del campo Pointer se establece en el desplazamiento correcto incluso cuando la ubicación del error no esté en la parte del paquete descartado. En la tabla A.8 se muestran los valores del campo Code para los mensajes Parameter Problem.

Valor del código	**Descripción**
0	Error en un campo del encabezado IPv6 o en un encabezado de extensión.
1	Valor no reconocido en el campo Next Header (Encabezado siguiente). Equivale al mensaje Destination Unreachable-Protocol Unreachable (Destino inaccesible o protocolo inaccesible) de IPv4.
2	Opción de IPv6 no reconocida.

Tabla A. 8. Mensajes ICMPv6 Parameter Problem (Problema de parámetro)

7.1.3 MENSAJES INFORMATIVOS ICMPV6

Los mensajes informativos ICMPv6, definidos en el RFC 2463, proporcionan capacidades de diagnóstico para la solución de problemas.

- ***ECHO REQUEST (SOLICITUD DE ECO)***

El mensaje ICMPv6 Echo Request se envía a un destino para solicitar un mensaje Echo Reply (Respuesta de eco) de inmediato. El servicio de mensajes Echo Request/Echo Reply proporciona un diagnóstico simple para la solución de diversos problemas de posibilidad de acceso y enrutamiento. En la figura A.24 se muestra el mensaje ICMPv6 Echo Request.

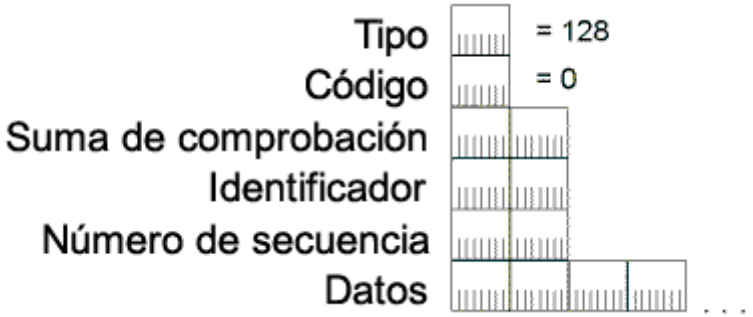

Figura A. 24. Mensaje ICMPv6 Echo Request (Solicitud de eco)

En el mensaje Echo Request, el campo Type (Tipo) se establece en el valor 128 y el campo Code (Código) se establece en el valor 0. Después del campo Checksum (Suma de comprobación), se encuentran los campos Identifier (Identificador) de 16 bits y Sequence Number (Número de secuencia). Los campos Identifier y Sequence Number se establecen mediante el host de envío y se utilizan para hacer coincidir un mensaje Echo Reply entrante con su mensaje Echo Request correspondiente. El campo Data (Datos) contiene cero o más bytes de datos opcionales y también lo establece el host de envío.

- ***ECHO REPLY (RESPUESTA DE ECO)***

Se envía un mensaje ICMPv6 Echo Reply en respuesta a la recepción de un mensaje ICMPv6 Echo Request. En la figura A.25 se muestra el mensaje ICMPv6 Echo Reply.

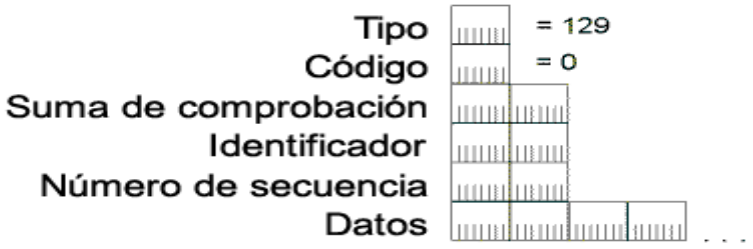

Figura A. 25. Mensaje ICMPv6 Echo Reply (Respuesta de eco)

En el mensaje Echo Reply, el campo Type (Tipo) se establece en el valor 129 y el campo Code (Código) se establece en el valor 0. Después del campo Checksum (Suma de comprobación) se encuentran los campos Identifier (Identificador) de 16 bits y Sequence Number (Número de secuencia). Los campos Identifier, Sequence Number y Data se establecen con los mismos valores que los del mensaje Echo Request que solicitó inicialmente el mensaje Echo Reply.

7.2 DIFERENCIAS ENTRE LOS MENSAJES ICMPV4 E ICMPV6

En la tabla A.9 se muestran los mensajes ICMPv4 y sus equivalentes en ICMPv6.

Mensaje ICMPv4	Equivalente en ICMPv6
Destination Unreachable-Network unreachable (Destino inaccesible: red inaccesible) (Type 3, Code 1)	Destination Unreachable-No route to destination (Destino inaccesible: no hay ruta al destino) (Type 1, Code 0)
Destination Unreachable-Host unreachable (Destino inaccesible: host inaccesible) (Type 3, Code 1)	Destination Unreachable-Address unreachable (Destino inaccesible: dirección inaccesible) (Type 1, Code 3)
Destination Unreachable-Protocol unreachable (Destino inaccesible: protocolo inaccesible) (Type 3, Code 2)	Parameter Problem-Unrecognized Next Header field (Problema de parámetro: no se reconoce el campo Next Header) (Type 4, Code 1)
Destination Unreachable-Port unreachable (Destino inaccesible: puerto inaccesible) (Type 3, Code 3)	Destination Unreachable-Port unreachable (Destino inaccesible: puerto inaccesible) (Tipo 1, Código 4)
Destination Unreachable-Fragmentation needed and DF set (Destino inaccesible: se necesita fragmentación y DF (Type 3, Code 4)	Packet Too Big (Paquete demasiado grande) (Type 2, Code 0)
Destination Unreachable-Communication with destination host administratively prohibited (Destino inaccesible: comunicación con el host de destino prohibida administrativamente) (Type 3, Code 10)	Destination Unreachable-Communication with destination administratively prohibited (Destino inaccesible: comunicación con el destino prohibida administrativamente) (Type 1, Code 1)
Time Exceeded-TTL expired (Fin de tiempo de espera: caducó TTL) (Type 11, Code 0)	Time Exceeded-Hop Limit exceeded (Fin de tiempo de espera: se excedió el límite de saltos) (Type 3, Code 0)
Time Exceeded-Fragmentation timer expired (Fin de tiempo de espera: caducó el cronómetro de fragmentación) (Type 11, Code 1)	Time Exceeded-Fragmentation timer exceeded (Fin de tiempo de espera: se excedió del cronómetro de fragmentación) (Type 3, Code 1)
Parameter Problem (Problema de parámetro)	Parameter Problem (Problema de parámetro)

(Type 12, Code 0)	(Type 4, Code 0 o Code 2)
Source Quench (Paquetes de control de flujo) (Type 4, Code 0)	Este mensaje no está implementado en IPv6.
Redirect (Redirección) (Type 5, Code 0)	Mensaje Neighbor Discovery Redirect (Redirección para descubrimiento de vecino) (Type 137, Code 0).

Tabla A. 9. Mensajes ICMPv4 y sus equivalentes en ICMPv6

7.3 DESCUBRIMIENTO DE MTU DE RUTA DE ACCESO

La unidad MTU de ruta de acceso es la MTU de enlace mínima de todos los enlaces que hay en una ruta de acceso entre un origen y un destino. Los paquetes IPv6 con un tamaño máximo de MTU de ruta de acceso no necesitan que el host los fragmente y todos los enrutadores de la ruta de acceso los reenviarán correctamente. Para descubrir la unidad MTU de ruta de acceso, el nodo de envío utiliza la recepción de mensajes ICMP Packet Too Big (Paquete demasiado grande).

La unidad MTU de ruta de acceso se descubre mediante el siguiente proceso:

1. El nodo de envío asume que la unidad MTU de la ruta de acceso es la MTU de enlace de la interfaz en la que se está reenviando el tráfico.
2. El nodo de envío envía datagramas IP con el tamaño de MTU de ruta de acceso.
3. Si un enrutador de la ruta de acceso no puede reenviar el paquete a través de un enlace con una MTU de enlace menor que el tamaño del paquete, descarta el paquete IPv6 y devuelve un mensaje Packet Too Big al nodo de envío. El mensaje ICMP Packet Too Big contiene la unidad MTU del enlace en el que se produjo el error de reenvío.
4. El nodo de envío configura la unidad MTU de ruta de acceso para los paquetes que se envían al destino con el valor del campo MTU en el mensaje ICMPv6 Packet Too Big.

El nodo de envío vuelve a empezar en el paso 2 y repite los pasos 2 a 4 tantas veces como sea necesario para descubrir la unidad MTU de ruta de acceso. La unidad MTU de ruta de acceso se determina cuando no se reciben mensajes ICMPv6 Packet Too Big adicionales o cuando se recibe un mensaje de confirmación del destino.

En el RFC 1981, se recomienda que los nodos IPv6 admitan el descubrimiento de MTU de ruta de acceso. Aquéllos que no lo hagan, deben utilizar la unidad MTU de enlace mínima de 1.280 bytes como MTU de ruta de acceso.

7.4 CAMBIOS EN MTU DE RUTA DE ACCESO

Debido a los cambios de la topología de enrutamiento, la ruta de acceso entre el origen y el destino puede cambiar con el tiempo. Cuando una nueva ruta de acceso necesita una MTU

de ruta de acceso menor, el proceso anterior empieza en el paso 3 y repite los pasos 2 a 4 hasta que se descubre la nueva MTU de ruta de acceso.

Las disminuciones de MTU de ruta de acceso se descubren inmediatamente a través de la recepción de mensajes ICMP Packet Too Big. El nodo de envío debe detectar los incrementos en la MTU de ruta de acceso. Tal como se describe en el RFC 1981, el nodo de envío puede intentar enviar un paquete IPv6 mayor después de un mínimo de 5 minutos (se recomienda 10 minutos) al recibir un mensaje ICMPv6 Packet Too Big.

8. MULTICAST LISTENER DISCOVERY (MLD O DESCUBRIMIENTO DE ESCUCHA DE MULTIDIFUSIÓN)

Multicast Listener Discovery (MLD) es el equivalente en IPv6 de la versión 2 del Protocolo de administración de grupos de Internet (IGMPv2) para IPv4. MLD es un conjunto de mensajes que se intercambian enrutadores y nodos, que permite a los enrutadores descubrir el conjunto de direcciones de multidifusión para las que hay nodos a la escucha en cada interfaz conectada. Al igual que IGMPv2, MLD sólo descubre la lista de direcciones de multidifusión para las que hay al menos una escucha, no la lista de escuchas de multidifusión para cada dirección de multidifusión. El descubrimiento de escucha de multidifusión (MLD) está documentado en el RFC 2710.

A diferencia de IGMPv2, MLD utiliza mensajes ICMPv6 en vez de definir su propia estructura de mensajes. Todos los mensajes MLD son mensajes ICMPv6 de los tipos 130, 131 y 132. Los tres tipos de mensajes MLD son:

- **Multicast Listener Query (Consulta de escucha de multidifusión)**

Los enrutadores utilizan los mensajes Multicast Listener Query para consultar en un enlace las escuchas de multidifusión. Existen dos tipos de mensajes Multicast Listener Query: General Query (Consulta general) y Multicast-Address-Specific Query (Consulta específica de dirección de multidifusión). El mensaje General Query se utiliza para consultar a escuchas de multidifusión de todas las direcciones de multidifusión. El mensaje Multicast-Address-Specific Query se utiliza para consultar escuchas de multidifusión de una dirección de multidifusión específica. Estos dos tipos de mensajes se distinguen mediante la dirección de destino de multidifusión en el encabezado IPv6 y una dirección de multidifusión en el mensaje Multicast Listener Query.

- **Multicast Listener Report (Informe de escucha de multidifusión)**

Una escucha de multidifusión utiliza Multicast Listener Report para informar del interés por recibir tráfico de multidifusión para una dirección de multidifusión determinada o para responder a un mensaje Multicast Listener Query.

- **Multicast Listener Done (Escucha de multidifusión terminada)**

Una escucha de multidifusión utiliza Multicast Listener Done para informar de que ya no tiene interés en recibir tráfico de multidifusión para una dirección de multidifusión determinada.

El paquete de un mensaje MLD consta de un encabezado IPv6, un encabezado de extensión Hop-by-Hop Options (Opciones de salto a salto) y el mensaje MLD. El encabezado de extensión Hop-by-Hop Options contiene la opción Router Alert (Alerta de enrutador) de IPv6 documentada en el RFC 2711. Se utiliza para asegurar que los enrutadores procesan los mensajes MLD enviados a direcciones de multidifusión en las que el enrutador no está a la escucha. En la figura A.26 se muestra el formato de un paquete de mensaje MLD.

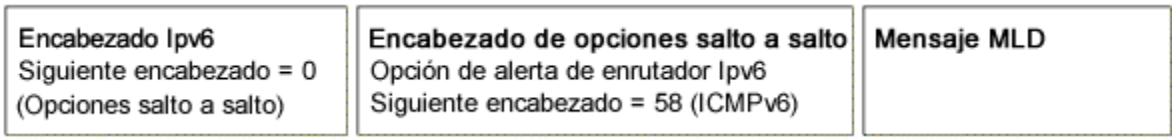

Figura A. 26. Formato de un paquete de mensaje MLD

8.1 MULTICAST LISTENER QUERY (CONSULTA DE ESCUCHA DE MULTIDIFUSIÓN)

Un mensaje MLD Multicast Listener Query equivale al mensaje IGMPv2 Host Membership Query (Consulta de pertenencia a grupo de hosts). Lo utiliza un enrutador para consultar un enlace conectado para hosts a la escucha.

En el encabezado IPv6, la dirección de origen es la dirección local de enlace de la interfaz en la que se envía la consulta. El campo Hop Limit (Límite de saltos) se establece en el valor 1. Para General Query, la dirección de destino es la dirección de multidifusión de todos los nodos de ámbito local de enlace (FF02::1). Para Multicast-Address-Specific Query, la dirección de destino es la dirección de multidifusión específica que se consulta.

En la figura A.27 se muestra el mensaje MLD Multicast Listener Query.

Figura A. 27. Mensaje MLD Multicast Listener Query (Consulta de escucha de multidifusión)

En el mensaje MLD Multicast Listener Query, el campo Type (Tipo) se establece en el valor 130 y el campo Code (Código) se establece en 0. Después del campo Checksum (Suma de comprobación), se encuentran los campos de 16 bits Maximum Response Delay (Retardo máximo de respuesta) y Reserved (Reservado). Maximum Response Delay especifica la cantidad de tiempo máxima en milisegundos en la que un miembro del grupo de multidifusión debe informar de su pertenencia al grupo mediante un mensaje MLD Multicast Listener Report. En General Query, el campo Multicast Address (Dirección de multidifusión) se establece en la dirección no especificada (::). En Multicast-Address-Specific Query, el campo Multicast Address se establece en la dirección de multidifusión específica que se consulta.

8.2 MULTICAST LISTENER REPORT (INFORME DE ESCUCHA DE MULTIDIFUSIÓN)

Un mensaje MLD Multicast Listener Report equivale al mensaje IGMPv2 Host Membership Report (Pertenencia a grupo de hosts). Lo utiliza un nodo de escucha para informar de su interés en recibir tráfico de multidifusión en una dirección de multidifusión específica o responder a un mensaje MLD General Query o Multicast-Address-Specific Query.

En el encabezado IPv6, la dirección de origen es la dirección local de enlace de la interfaz en la que se envía el informe. El campo Hop Limit (Límite de saltos) se establece en el valor 1 y la dirección de destino es la dirección de multidifusión sobre la que trata el informe.

En la figura A.28 se muestra el mensaje MLD Multicast Listener Report.

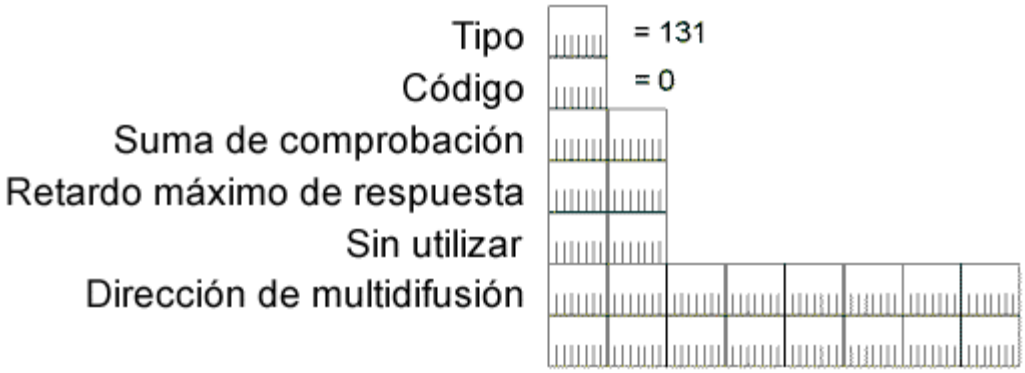

Figura A. 28. Mensaje MLD Multicast Listener Report (Informe de escucha de multidifusión)

En el mensaje MLD Multicast Listener Report, el campo Type (Tipo) se establece en 131 y el campo Code (Código) se establece en el valor 0. El campo Maximum Response Delay (Retardo de respuesta máximo) no se utiliza en un mensaje Multicast Listener Report y se establece en 0. El campo Multicast Address (Dirección de multidifusión) se configura con la dirección de multidifusión específica sobre la que trata el informe.

8.3 MULTICAST LISTENER DONE (ESCUCHA DE MULTIDIFUSIÓN TERMINADA)

Un mensaje MLD Multicast Listener Done equivale al mensaje IGMPv2 Leave Group (Abandonar grupo). Lo utiliza un nodo de escucha para informar a los enrutadores locales de que el host ya no escucha a una dirección de multidifusión específica.

En el encabezado IPv6, la dirección de origen es la dirección local de enlace de la interfaz en la que se envía el informe. El campo Hop Limit (Límite de saltos) se establece en el valor 1 y la dirección de destino es la dirección de multidifusión de todos los enrutadores de ámbito local de enlace (FF02::2). En la figura A.29 se muestra el mensaje MLD Multicast Listener Done.

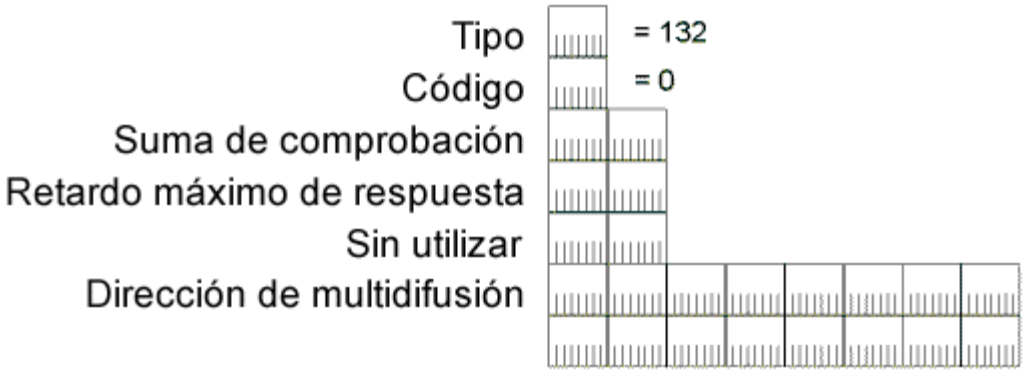

Figura A. 29. Mensaje MLD Multicast Listener Done (Escucha de multidifusión terminada)

En el mensaje MLD Multicast Listener Done, el campo Type (Tipo) se establece en el valor 132 y el campo Code (Código) se establece en el valor 0. El campo Maximum Response Delay (Retardo de respuesta máximo) no se utiliza en un mensaje Multicast Listener Done y se establece en 0. El campo Multicast Address (Dirección de multidifusión) se configura con la dirección de multidifusión específica para la que el nodo de envío informa a los enrutadores locales de que ya no está a la escucha.

9. DESCUBRIMIENTO DE VECINO

Neighbor Discovery (ND o Descubrimiento de vecino) de IPv6 es un conjunto de mensajes y procesos que determinan las relaciones entre nodos vecinos. ND reemplaza a los procesos ARP, ICMP Router Discovery (Descubrimiento de enrutadores) e ICMP Redirect (Redirección) que se utilizaban en IPv4 y proporciona funciones adicionales.

ND es utilizado por:

- Los hosts, para descubrir enrutadores vecinos.
- Los hosts, para descubrir direcciones, prefijos de direcciones y otros parámetros de configuración.

- Los nodos, para resolver la dirección de nivel de enlace de un nodo vecino al que se va a reenviar un paquete IPv6 y determinar cuándo ha cambiado la dirección de nivel de enlace de un nodo vecino.
- Los nodos, para determinar si aún se puede tener acceso a un vecino.
- Los enrutadores, para anunciar su presencia, los parámetros de configuración de host y los prefijos en el enlace.
- Los enrutadores, para informar a los hosts de una dirección de salto siguiente mejor para el reenvío de paquetes a un destino específico.

En la tabla A.10 se muestran y describen los procesos ND documentados en el RFC 2461.

Proceso	**Descripción**
Descubrimiento de enrutadores	Proceso por el que un host descubre los enrutadores locales de un enlace conectado. Equivale al proceso Router Discovery (Descubrimiento de enrutador) de ICMPv4.
Descubrimiento de prefijos	Proceso por el que los hosts descubren los prefijos de red para destinos de enlaces locales. Es similar al proceso Address Mask Request/Reply (Solicitud y respuesta de máscara de dirección) de ICMPv4.
Descubrimiento de parámetros	Proceso por el que los hosts descubren parámetros de funcionamiento adicionales, incluida la unidad MTU de enlace y el límite de saltos predeterminado para los paquetes salientes.
Configuración automática de direcciones	Proceso que consiste en configurar direcciones IP para interfaces en presencia o en ausencia de un servidor de configuración de direcciones con estado, como la versión 6 del Protocolo de configuración dinámica de host (DHCPv6).
Resolución de direcciones	Proceso por el que los nodos resuelven la dirección IPv6 de un vecino en su dirección de nivel de enlace. Equivale a ARP en IPv4.
Determinación del salto siguiente	Proceso por el que un nodo determina la dirección IPv6 del vecino al que se envía un paquete basándose en la dirección de destino. La dirección de reenvío o de salto siguiente es la dirección de destino o la dirección de un enrutador predeterminado en el enlace.
Detección de inaccesibilidad a un vecino	Proceso por el que un nodo determina que el nivel IPv6 de un vecino ya no recibe paquetes.

Detección de dirección duplicada	Proceso por el que un nodo determina que un nodo vecino aún no utiliza una dirección considerada para el uso. Equivale a utilizar tramas ARP gratuitas en IPv4.
Función de redirección	Proceso que consiste en informar al host de una dirección IPv6 mejor para el primer salto para llegar a un destino. Equivale al mensaje ICMP Redirect (Redirección) de IPv4.

Tabla A. 10. Procesos de Neighbor Discovery (Descubrimiento de vecinos) en IPv6

9.1 FORMATO DE LOS MENSAJES NEIGHBOR DISCOVERY (DESCUBRIMIENTO DE VECINO)

Al igual que los mensajes Multicast Listener Discovery (MLD o Descubrimiento de escucha de multidifusión), los mensajes Neighbor Discovery (ND) utilizan la estructura de mensajes de ICMPv6 y los tipos ICMPv6 133 a 137. Los mensajes ND constan de un encabezado de mensaje ND, compuesto por un encabezado ICMPv6 y datos específicos del mensaje ND, además de cero o más opciones de ND, tal como se muestra en la figura A.30.

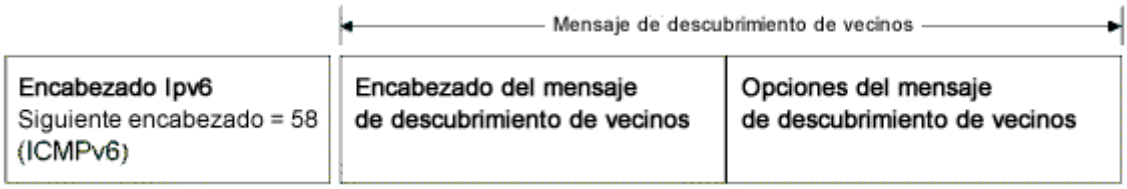

Figura A. 30. Formato de un mensaje Neighbor Discovery (Descubrimiento de vecino)

Hay cinco mensajes ND distintos:

- Router Solicitation (Solicitud de enrutador)
- Router Advertisement (Anuncio de enrutador)
- Neighbor Solicitation (Solicitud de vecino)
- Neighbor Advertisement (Anuncio de vecino)
- Redirect (Redirección)

Las opciones de los mensajes ND proporcionan información adicional, que normalmente indica direcciones MAC, prefijos de red en el enlace, información de MTU en el enlace y datos de redirección.

Para asegurarse de que los mensajes ND recibidos se originaron en un nodo del enlace local, todos los mensajes ND se envían con un límite de saltos de 255. Cuando se recibe un mensaje ND, se comprueba el campo Hop Limit (Límite de saltos) del encabezado IPv6. Si no se establece en el valor 255, el mensaje se descarta sin notificarlo. La comprobación de que un mensaje ND tiene un límite de saltos de 255 proporciona protección ante ataques en

la red basados en ND desde nodos situados fuera del enlace. Con un límite de saltos de 255, un enrutador no podría reenviar el mensaje ND desde un nodo situado fuera del enlace.

9.2 OPCIONES DE NEIGHBOR DISCOVERY (DESCUBRIMIENTO DE VECINO)

Las opciones de Neighbor Discovery tienen el formato Tipo-Longitud-Valor, tal como se muestra en la figura A.31.

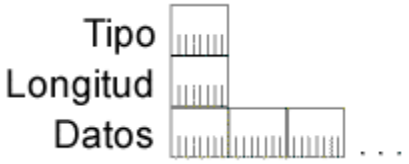

Figura A. 31. Formato de una opción de Neighbor Discovery (Descubrimiento de vecino)

El campo Type (Tipo) de 8 bits indica el tipo de opción de ND. En la tabla A.11 se enumeran los tipos de opciones de ND definidas en el RFC 2461.

Tipo	Nombre de la opción
1	Source Link-Layer Address (Dirección de nivel de enlace de origen)
2	Destination Link-Layer Address (Dirección de nivel de enlace de destino)
3	Prefix Information (Información de prefijo)
4	Redirected Header (Encabezado de redirección)
5	MTU

Tabla A. 11. Tipos de opciones de Neighbor Discovery (Descubrimiento de vecino) en IPv6

El campo Length (Longitud) de 8 bits indica la longitud de la opción completa en bloques de 8 bytes. Todas las opciones de ND deben adaptarse a los límites de 8 bytes. El campo Value (Valor), de longitud variable, contiene los datos de la opción.

9.2.1 OPCIÓN SOURCE/TARGET LINK-LAYER ADDRESS (DIRECCIÓN DE NIVEL DE ENLACE DE ORIGEN Y DESTINO)

La opción Source Link-Layer Address indica la dirección de nivel de enlace del remitente del mensaje ND. La opción Source Link-Layer Address se incluye en los mensajes Neighbor Solicitation (Solicitud de vecino), Router Solicitation (Solicitud de enrutador) y Router Advertisement (Anuncio de enrutador). La opción Source Link-Layer Address no se incluye cuando la dirección de origen del mensaje ND es la dirección no especificada (::).

La opción Target Link-Layer Address (Dirección de nivel de enlace de destino) indica la dirección de nivel de enlace del nodo vecino al que se deben dirigir los paquetes IPv6. La

opción Target Link-Layer Address se incluye en los mensajes Neighbor Advertisement y Redirect (Redirección).

Las opciones Source Link-Layer Address y Target Link-Layer Address tienen el formato que se muestra en la figura A.32.

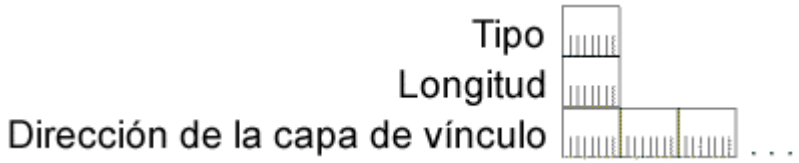

Figura A. 32. Formato de las opciones Source y Target Link-Layer Address (Dirección de nivel de enlace de origen y destino)

El campo Type (Tipo) se establece en el valor 1 para una opción Source Link-Layer Address y en el valor 2 para una opción Target Link-Layer Address. El campo Length (Longitud) se establece en el número de bloques de 8 bytes que contiene toda la opción. El campo Link-Layer Address (Dirección de nivel de enlace) es un campo de longitud variable que contiene la dirección de nivel de enlace del origen o del destino. Cada nivel de enlace definido para IPv6 debe especificar el formato de la dirección de nivel de enlace en las opciones Source y Target Link-Layer Address.

Por ejemplo, el RFC 2464 define cómo se envían paquetes IPv6 a través de redes Ethernet. También incluye el formato de las opciones ND Source y Target Link-Layer Address. En Ethernet, la dirección de nivel de enlace tiene una longitud de 48 bits (6 bytes). En la figura A.33 se muestran las opciones Source y Target Link-Layer Address para Ethernet.

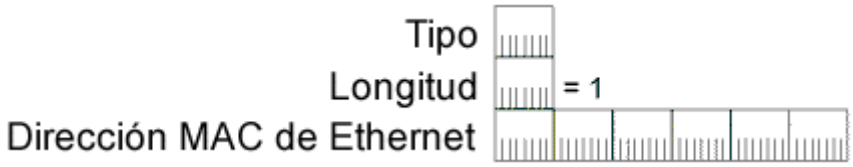

Figura A. 33. Formato de las opciones Source y Target Link-Layer Address (Dirección de nivel de enlace de origen y destino) para Ethernet

9.2.2 OPCIÓN PREFIX INFORMATION (INFORMACIÓN DE PREFIJO)

La opción Prefix Information se envía en mensajes Router Advertisement (Anuncio de enrutador) para indicar los prefijos de las direcciones e información acerca de la configuración automática de direcciones. En un mensaje Router Advertisement, puede haber varias opciones Prefix Information, que indican varios prefijos de direcciones. En la figura A.34 se muestra el formato de la opción Prefix Information.

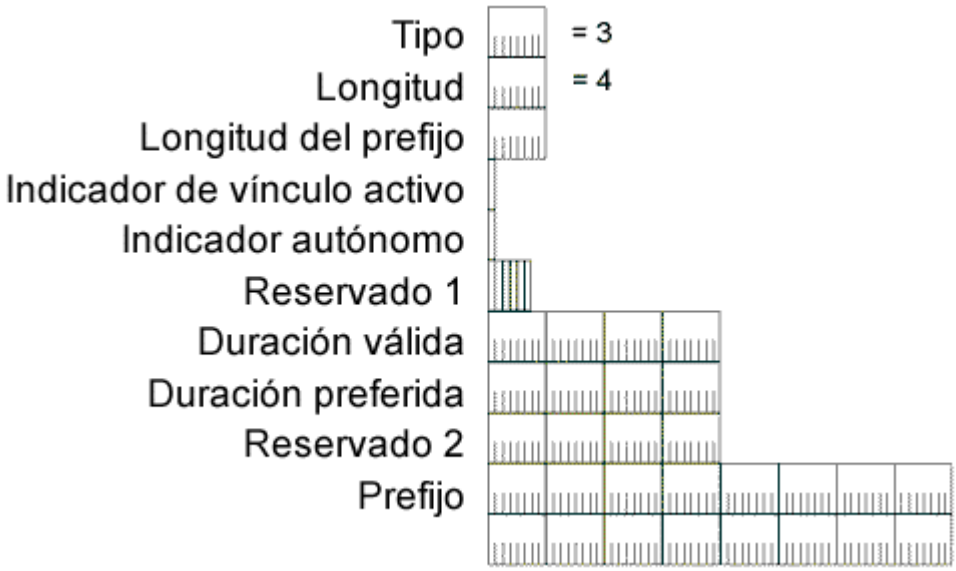

Figura A. 34. Formato de la opción Prefix Information (Información de prefijo)

Los campos de la opción Prefix Information son:

Type (Tipo): el valor de este campo es 3.

Length (Longitud): el valor de este campo es 4 (la opción completa tiene una longitud de 32 bytes).

Prefix Length (Longitud del prefijo): indica el número de bits a la izquierda del campo Prefix (Prefijo) que comprenden el prefijo de la dirección. El tamaño de este campo es de 8 bits. El campo Prefix Length tiene un valor comprendido entre 0 y 128.

On-link flag (Indicador en el enlace): cuando se establece en el valor 1, indica que las direcciones que implica el prefijo están disponibles en el enlace en el que se recibió el mensaje Router Advertisement (Anuncio de enrutador). Cuando se establece en el valor 0, no se supone que las direcciones que coinciden con el prefijo están disponibles en el enlace. El tamaño de este campo es de 1 bit.

Autonomous flag (Indicador autónomo): cuando se establece en el valor 1, indica que el prefijo se utiliza para crear una configuración de dirección autónoma (o sin estado). Cuando se establece en el valor 0, el prefijo incluido no se utiliza para crear una configuración de dirección sin estado. El tamaño de este campo es de 1 bit.

Reserved 1 (Reservado 1): campo de 6 bits reservado para un uso futuro y que se establece en el valor 0.

Valid Lifetime (Tiempo de vida válido): indica el número de segundos que una dirección mantiene su validez, en función del prefijo incluido y con la configuración de dirección sin

estado. El tamaño de este campo es de 32 bits. El campo Valid Lifetime también indica el número de segundos durante los que el prefijo incluido es válido para la determinación en el enlace. Para especificar un tiempo de vida válido infinito, el campo Valid Lifetime se establece en el valor 0xFFFFFFFF.

Preferred Lifetime (Tiempo de vida preferido):indica el número de segundos que una dirección se mantiene en estado de preferencia, en función del prefijo incluido y con la configuración de dirección sin estado. El tamaño de este campo es de 32 bits. Las direcciones de configuración automática sin estado que aún son válidas pueden encontrarse en estado de preferencia o de desaprobación. En el estado de preferencia, la dirección se puede utilizar para una comunicación sin restricciones. En el estado de desaprobación, no se recomienda el uso de la dirección para las nuevas comunicaciones. Sin embargo, pueden continuar las comunicaciones existentes que utilicen una dirección en estado de desaprobación. Una dirección pasa del estado preferido al de desaprobación cuando finaliza su tiempo de vida preferido. Para especificar un tiempo de vida preferido infinito, el campo Preferred Lifetime se establece en el valor 0xFFFFFFFF.

Reserved 2 (Reservado 2): campo de 32 bits reservado para su uso futuro que se establece en el valor 0.

Prefix (Prefijo): indica el prefijo para la dirección IPv6 derivada a través de la configuración automática sin estado. El tamaño de este campo es de 128 bits. La combinación del campo Prefix Length (Longitud del prefijo) y el campo Prefix (Prefijo) describen sin ambigüedad el prefijo que, al combinarse con el identificador de interfaz para el nodo, crea una dirección IPv6. Los bits del campo Prefix que sobrepasan el valor del campo Prefix Length se establecen en el valor 0. El prefijo local de enlace no se debe enviar y lo omite el host receptor.

9.2.3 OPCIÓN REDIRECTED HEADER (ENCABEZADO DE REDIRECCIÓN)

La opción Redirected Header se envía a los mensajes Redirect para especificar el paquete IPv6 que hizo que el enrutador enviara un mensaje Redirect. Puede contener todo el paquete IPv6 redirigido o una parte, según el tamaño del paquete IPv6 que se envió inicialmente. En la figura A.35 se muestra el formato de la opción Redirected Header.

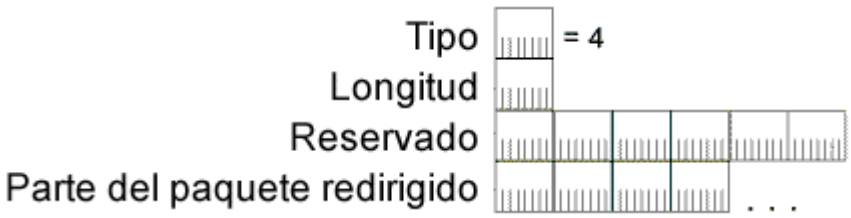

Figura A. 35. Formato de la opción Redirected Header (Encabezado de redirección)

Los campos de la opción Redirected Header son los siguientes:

Type (Tipo): el valor de este campo es 4.

Length (Longitud): el valor de este campo es el número de bloques de 8 bytes en toda la opción.

Reserved (Reservado): campo de 48 bits reservado para su uso futuro que se establece en el valor 0.

Portion of redirected packet (Porción del paquete de redirección): contiene el paquete IPv6 o una parte del paquete IPv6 que causó que se enviara el mensaje Redirect. La cantidad del paquete original incluida es la parte del paquete que cabe sin que el mensaje Redirect tenga una longitud superior a 1.280 bytes.

9.2.4 OPCIÓN MTU

La opción MTU se envía en mensajes Router Advertisement (Anuncio de enrutador) para indicar la unidad MTU de IPv6 del enlace. Normalmente, esta opción sólo se utiliza cuando la MTU de IPv6 para un enlace no es bien conocida o tiene que establecerse debido a una configuración de puente de transacciones. La opción MTU suplanta a la unidad MTU de IPv6 de la que informa el hardware de interfaz. En la figura A.36 se muestra el formato de la opción MTU.

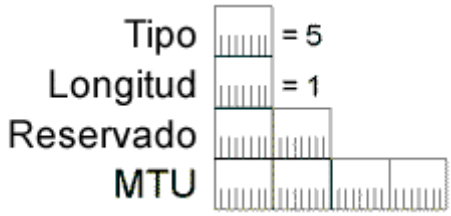

Figura A. 36. Formato de la opción MTU

Los campos de la opción MTU son:

Type (Tipo): el valor de este campo es 5.

Length (Longitud): el valor de este campo es 1 (hay 8 bytes en toda la opción).

Reserved (Reservado): campo de 16 bits reservado para su uso futuro que se establece en el valor 0.

MTU: indica la unidad MTU de IPv6 que debe utilizar el host para el enlace en el que se recibió el anuncio de enrutador. El tamaño de este campo es de 32 bits. El valor del campo MTU se omite si es mayor que la unidad MTU del enlace.

9.3 MENSAJES DE NEIGHBOR DISCOVERY (DESCUBRIMIENTO DE VECINO)

Todas las funciones de Neighbor Discovery (ND) de IPv6 se realizan con los siguientes mensajes:

- Router Solicitation (Solicitud de enrutador)
- Router Advertisement (Anuncio de enrutador)
- Neighbor Solicitation (Solicitud de vecino)
- Neighbor Advertisement (Anuncio de vecino)
- Redirect (Redirección)

9.3.1 ROUTER SOLICITATION (SOLICITUD DE ENRUTADOR)

El mensaje Router Solicitation es enviado por los hosts IPv6 para descubrir los enrutadores IPv6 que hay en el enlace. Un host envía una solicitud de enrutador de multidifusión para que los enrutadores IPv6 respondan inmediatamente, en vez de esperar un mensaje periódico Router Advertisement (Anuncio de enrutador).

Por ejemplo, si el enlace local es Ethernet, en el encabezado Ethernet del mensaje Router Solicitation:

- El campo Source Address (Dirección de origen) se establece en la dirección MAC del adaptador de red de envío.
- El campo Destination Address (Dirección de destino) se establece en el valor 33-33-00-00-00-02.

En el encabezado IPv6 del mensaje Router Solicitation hay los campos siguientes:

- El campo Source Address se establece en la dirección IPv6 asignada a la interfaz de envío o con la dirección IPv6 no especificada (::).
- El campo Destination Address se establece en la dirección de multidifusión local de enlace de todos los enrutadores (FF02::2).
- El campo Hop Limit (Límite de saltos) se establece en el valor 255.

En la figura A.37 se muestra el formato del mensaje Router Solicitation.

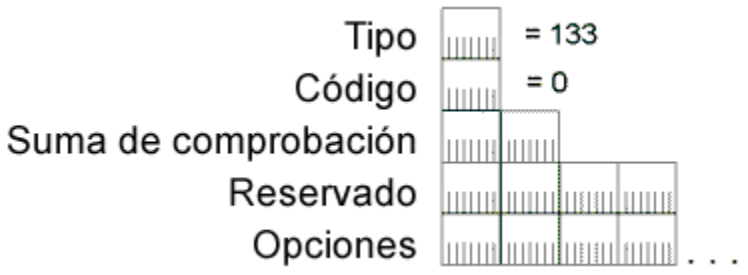

Figura A. 37. Formato del mensaje Router Solicitation (Solicitud de enrutador)

Los campos del mensaje Router Solicitation son los siguientes:

Type (Tipo): el valor de este campo es 133.

Code (Código): el valor de este campo es 0.

Checksum (Suma de comprobación): el valor de este campo es la suma de comprobación de ICMPv6.

Reserved (Reservado): campo de 32 bits reservado para su uso futuro que se establece en el valor 0.

Opción **Source Link-Layer Address** (Dirección de nivel de enlace de origen): esta opción de ND contiene la dirección de nivel de enlace del remitente. En un nodo Ethernet, la opción Source Link-Layer Address contiene la dirección MAC Ethernet del host de envío. El enrutador receptor utiliza la dirección de la opción Source Link-Layer Address para determinar la dirección MAC de unidifusión del host a la que se envía el anuncio de enrutador de unidifusión correspondiente.

9.3.2 ROUTER ADVERTISEMENT (ANUNCIO DE ENRUTADOR)

Los enrutadores IPv6 envían el mensaje Router Advertisement periódicamente o en respuesta a la recepción de un mensaje Router Solicitation (Solicitud de enrutador). Contiene la información que necesitan los hosts para determinar los prefijos de enlace, la unidad MTU de enlace, si se utiliza o no la configuración automática de direcciones y el tiempo durante el que las direcciones creadas mediante la configuración automática de direcciones son válidas y preferidas.

Por ejemplo, si el enlace local es Ethernet, en el encabezado Ethernet del mensaje Router Advertisement:

- El campo Source Address (Dirección de origen) se establece en la dirección MAC del adaptador de red de envío.
- El campo Destination Address se establece en 33-33-00-00-00-01 para un anuncio de enrutamiento periódico o la dirección MAC de unidifusión del host que envió una solicitud de enrutador.

En el encabezado IPv6 del mensaje Router Advertisement:

- El campo Source Address se establece en la dirección local de enlace asignada a la interfaz de envío.
- El campo Destination Address se establece como dirección de multidifusión local de enlace de todos los nodos (FF02::1) o la dirección IPv6 de unidifusión del host que envió el mensaje Router Solicitation (Solicitud de enrutador).
- El campo Hop Limit (Límite de saltos) se establece en el valor 255.

En la figura A.38 se muestra el formato del mensaje Router Advertisement.

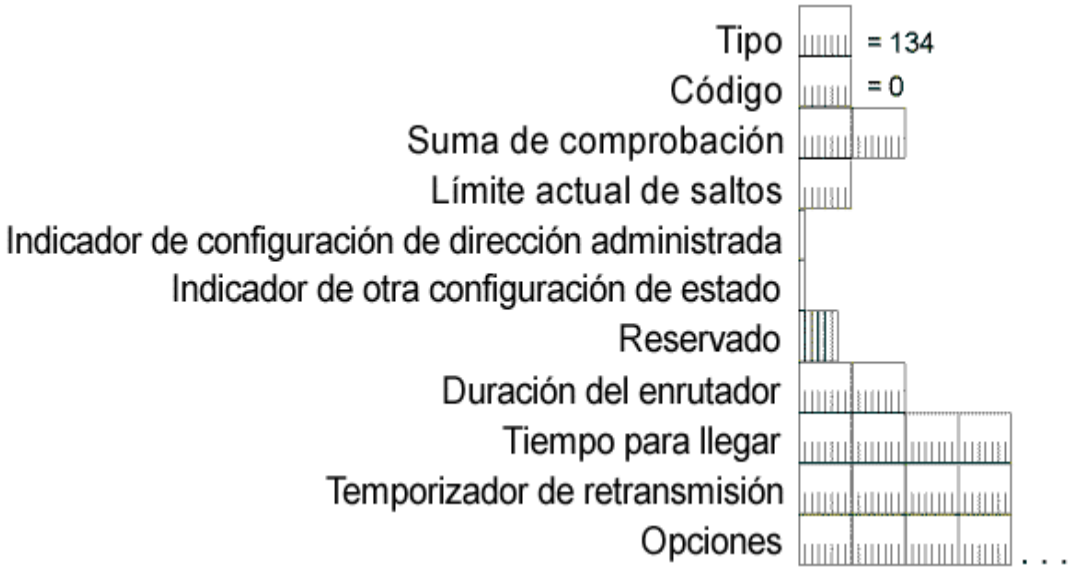

Figura A. 38. Formato del mensaje Router Advertisement (Anuncio de enrutador)

Los campos del mensaje Router Advertisement son:

Type (Tipo): el valor de este campo es 134.

Code (Código): el valor de este campo es 0.

Checksum (Suma de comprobación): el valor de este campo es la suma de comprobación de ICMPv6.

Cur Hop Limit (Límite de saltos actual): indica el valor predeterminado del campo Hop Count en el encabezado IPv6 para los paquetes enviados por hosts que reciben este mensaje Router Advertisement. El tamaño de este campo es de 8 bits. Un límite de salto actual de 0 indica que el enrutador no especifica el valor predeterminado del campo Hop Count.

Indicador **Managed Address Configuration** (Configuración de direcciones administradas): cuando se establece en el valor 1, indica que los hosts que reciben este mensaje Router Advertisement deben utilizar un protocolo de configuración de direcciones con estado (por ejemplo, DHCPv6) para obtener direcciones además de las derivadas de la configuración automática de direcciones sin estado. El tamaño de este campo es de 1 bit.

Indicador **Other Stateful Configuration** (Otra configuración con estado): cuando se establece en el valor 1, indica que los hosts que reciben este mensaje Router Advertisement deben utilizar un protocolo de configuración de direcciones con estado (por ejemplo, DHCPv6) para obtener información de configuración que no sea de dirección. El tamaño de este campo es de 1 bit.

Reserved (Reservado): campo de 6 bits reservado para su uso futuro que se establece en el valor 0.

Router Lifetime (Tiempo de vida del enrutador): indica el tiempo de vida (en segundos) del enrutador de forma predeterminada. El tamaño de este campo es de 16 bits. El valor máximo para el tiempo de vida del enrutador es de 65.535 segundos (18,2 horas, aproximadamente). Un tiempo de vida 0 indica que el enrutador no puede considerarse como un enrutador predeterminado. Sin embargo, el resto de información que contiene el anuncio de enrutador es válida.

Reachable Time (Tiempo accesible): indica la cantidad de tiempo (en milisegundos) que un nodo puede considerar accesible a un nodo vecino después de recibir una confirmación la posibilidad de acceso. El tamaño de este campo es de 32 bits. Un valor 0 en el campo Reachable Time indica que el enrutador no especifica el tiempo accesible. Para obtener más información, consulte "Detección accesibilidad a un vecino".

Retrans Timer (Cronómetro de retransmisiones): indica la cantidad de tiempo (en milisegundos) entre retransmisiones de mensajes Neighbor Solicitation. El tamaño de este campo es de 32 bits. El campo Retrans Timer se utiliza durante la detección de inaccesibilidad a un vecino. Un valor 0 en el campo Retrans Timer indica que el enrutador no especifica el cronómetro de retransmisiones.

Opción **Source Link-Layer Address** (Dirección de nivel de enlace de origen): esta opción contiene la dirección de nivel de enlace de la interfaz en la que se envió el mensaje Neighbor Solicitation. Esta opción se puede omitir cuando el enrutador equilibra las cargas entre varias direcciones de nivel de enlace.

Opción **MTU**: la opción MTU contiene la unidad MTU del enlace. Sólo debe enviarse a enlaces con MTU variable o en entornos conmutados con varias tecnologías de nivel de enlace en el mismo segmento de red.

Opciones de **Prefix Information** (Información de prefijo): las opciones de información de prefijo contienen los prefijos en enlace que se utilizan para la configuración automática de direcciones. El prefijo de enlace local nunca se envía como opción de información de prefijo.

9.3.3 SOLICITUD DE VECINO

Los hosts IPv6 envían el mensaje Neighbor Solicitation (Solicitud de vecino) para descubrir la dirección de nivel de enlace de un nodo IPv6 en un enlace. Incluye la dirección de nivel de enlace del remitente. Las solicitudes de vecino típicas son de multidifusión para la resolución de direcciones y de unidifusión cuando se está comprobando la posibilidad de acceso a un nodo vecino.

Por ejemplo, si el enlace local es Ethernet, en el encabezado Ethernet del mensaje Neighbor Solicitation:

- El campo Source Address (Dirección de origen) se establece en la dirección MAC del adaptador de red de envío.
- Para una solicitud de vecino multidifusión, el campo Destination Address se establece en la dirección MAC Ethernet que corresponde a la dirección IP de multidifusión del nodo solicitado del destino. Para una solicitud de vecino unidifusión, el campo Destination Address se establece en la dirección MAC de unidifusión del vecino.

En el encabezado IPv6 del mensaje Neighbor Solicitation:

- El campo Source Address se establece en la dirección IPv6 asignada a la interfaz de envío o, durante la detección de detecciones duplicadas, con la dirección IPv6 no especificada (::).
- Para una solicitud de vecino multidifusión, el campo Destination Address se establece en la dirección de multidifusión de nodo solicitado del destino. Para una solicitud de vecino unidifusión, el campo Destination Address se establece en la dirección IP de unidifusión del destino.
- El campo Hop Limit (Límite de saltos) se establece en el valor 255.

En la figura A.39 se muestra el formato del mensaje Neighbor Solicitation.

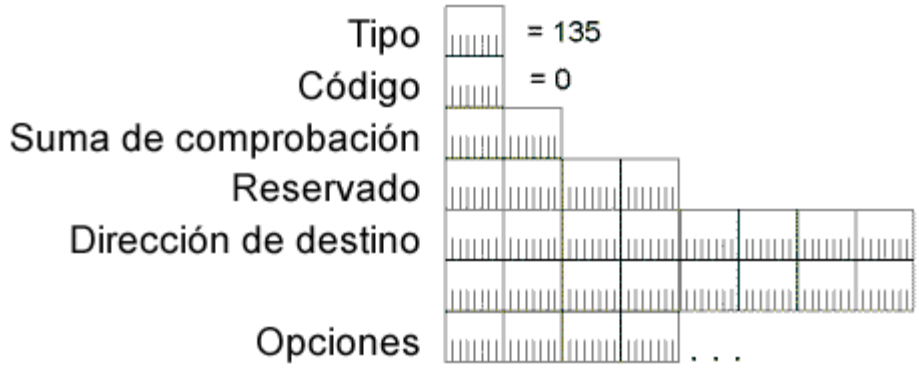

Figura A. 39. Formato del mensaje Neighbor Solicitation (Solicitud de vecino)

Los campos del mensaje Neighbor Solicitation son:

Type (Tipo): el valor de este campo es 135.

Code (Código): el valor de este campo es 0.

Checksum (Suma de comprobación): el valor de este campo es la suma de comprobación de ICMPv6.

Reserved (Reservado): campo de 32 bits reservado para su uso futuro que se establece en el valor 0.

Target Address (Dirección de destino): indica la dirección IP del destino. El tamaño de este campo es de 128 bits.

Opción **Source Link-Layer Address** (Dirección de nivel de enlace de origen): esta opción contiene la dirección de nivel de enlace del remitente. En un nodo Ethernet, la opción Source Link-Layer Address contiene la dirección MAC Ethernet del nodo de envío. El nodo receptor utiliza la dirección especificada en la opción Source Link-Layer Address para determinar la dirección MAC de unidifusión del nodo al que se envía el anuncio de vecino correspondiente. Durante la detección de direcciones duplicadas, cuando la dirección IPv6 de origen es la dirección no especificada (::), no se incluye la opción Source Link-Layer Address.

9.3.4 ANUNCIO DE VECINO

Un nodo IPv6 envía el mensaje Neighbor Advertisement (Anuncio de vecino) en respuesta a la recepción de un mensaje Neighbor Solicitation (Solicitud de vecino). Un nodo IPv6 también envía anuncios de vecino no solicitados para informar a los nodos vecinos de los cambios en las direcciones de nivel de enlace. El mensaje Neighbor Advertisement contiene información que necesitan los nodos para determinar el tipo de mensaje Neighbor Advertisement, la dirección de nivel de enlace del remitente y la función del remitente en la red.

Por ejemplo, si el enlace local es Ethernet, en el encabezado Ethernet del mensaje Neighbor Advertisement:

- El campo Source Address (Dirección de origen) se establece en la dirección MAC del adaptador de red de envío.
- Para el anuncio de vecino solicitado, el campo Destination Address se establece en la dirección MAC de unidifusión del remitente de la solicitud de vecino inicial. Para un anuncio de vecino no solicitado, el campo Destination Address se establece en 33-33-00-00-00-01, que es la dirección MAC Ethernet correspondiente a la dirección de multidifusión local de enlace de todos los nodos.

En el encabezado IPv6 del mensaje Neighbor Advertisement:

- El campo Source Address se establece en la dirección local de enlace asignada a la interfaz de envío.
- Para un anuncio de vecino solicitado, el campo Destination Address se establece en la dirección IP de unidifusión del remitente de la solicitud de vecino inicial. Para un anuncio de vecino no solicitado, el campo Destination Address se establece en la dirección de multidifusión local de enlace de todos los nodos (FF02::1).
- El campo Hop Limit (Límite de saltos) se establece en el valor 255.

En la figura A.40 se muestra el formato del mensaje Neighbor Advertisement.

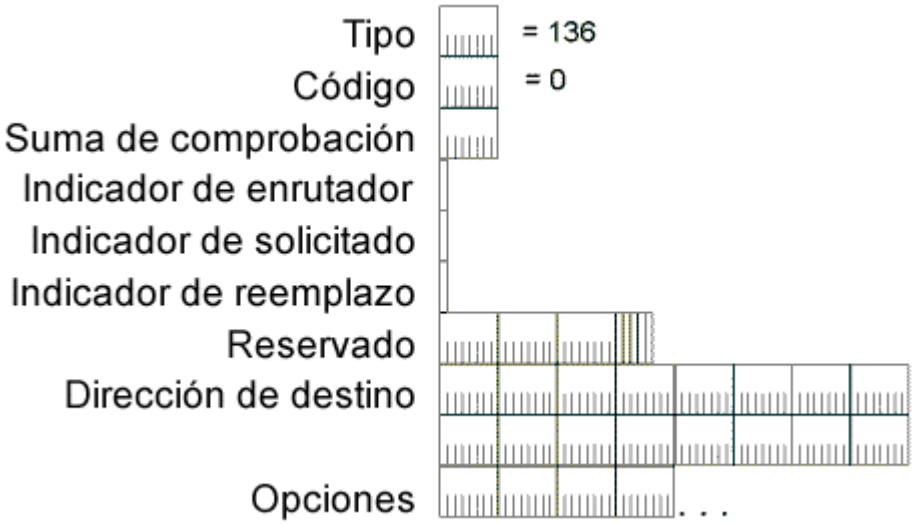

Figura A. 40. Formato del mensaje Neighbor Advertisement (Anuncio de vecino)

Los campos del mensaje Neighbor Advertisement son:

Type (Tipo): el valor de este campo es 136.

Code (Código): el valor de este campo es 0.

Checksum (Suma de comprobación): el valor de este campo es la suma de comprobación de ICMPv6.

Router flag (Indicador de enrutador): muestra la función del remitente del mensaje Router Advertisement (Anuncio de enrutador). El tamaño de este campo es de 1 bit. El indicador Router se establece en el valor 1 cuando el remitente es un enrutador y en 0 cuando no lo es. El indicador Router se utiliza en la detección de inaccesibilidad a vecino para determinar cuándo un enrutador cambia a host.

Solicited flag (Indicador solicitado): cuando se establece en el valor 1, indica que el mensaje Neighbor Advertisement se envió en respuesta a un mensaje Neighbor Solicitation (Solicitud de vecino). El tamaño de este campo es de 1 bit. El indicador Solicited se utiliza como confirmación de accesibilidad durante la operación de detección de inaccesibilidad a un vecino. El indicador Solicited se establece en el valor 0 para los anuncios de vecino multidifusión y para los anuncios de vecino unidifusión no solicitados.

Override flag (Indicador de suplantación): cuando se establece en el valor 1, indica que la dirección de nivel de enlace especificada en la opción de dirección de nivel de enlace de destino incluida debe suplantar a la dirección de nivel de enlace especificada en la entrada de caché del vecino. El tamaño de este campo es de 1 bit. Si el indicador Override está establecido en el valor 0, la dirección de nivel de enlace que se incluye sólo actualiza una entrada de caché de vecino si no se conoce la dirección de nivel de enlace. El indicador

Override se establece en el valor 0 para los anuncios con proxy y las direcciones para cualquier difusión solicitadas. El indicador Override se establece en el valor 1 en otros anuncios solicitados y no solicitados.

Reserved (Reservado): campo de 29 bits reservado para su uso futuro que se establece en el valor 0.

Target Address (Dirección de destino): indica la dirección que se anuncia. El tamaño de este campo es de 128 bits. En los mensajes Neighbor Advertisement solicitados, la dirección de destino se encuentra en el campo Target Address (Dirección de destino) de la solicitud de vecino correspondiente. Para los mensajes Neighbor Advertisement no solicitados, la dirección de destino es aquélla cuya dirección de nivel de enlace ha cambiado.

Opción **Target Link-Layer Address** (Dirección de nivel de enlace de destino): esta opción contiene la dirección de nivel de enlace del destino, que es el remitente del mensaje Neighbor Advertisement. Para un nodo Ethernet, la opción Target Link-Layer Address contiene la dirección MAC Ethernet del nodo de envío. Los nodos receptores utilizan la dirección especificada en la opción Target Link-Layer Address para determinar la dirección MAC de unidifusión del nodo que realiza el anuncio.

9.3.5 REDIRECT (REDIRECCIÓN)

Un enrutador de IPv6 envía el mensaje Redirect para informar a un host de origen de la existencia de una dirección mejor para el primer salto a un destino determinado. Los mensajes Redirect sólo son enviados por los enrutadores de tráfico de unidifusión, son sólo de unidifusión para los hosts de origen y únicamente son procesados por hosts.

Por ejemplo, si el enlace local es Ethernet, en el encabezado Ethernet del mensaje Redirect:

- El campo Source Address (Dirección de origen) se establece en la dirección MAC del adaptador de red de envío.
- El campo Destination Address (Dirección de destino) se establece en la dirección MAC de unidifusión del remitente de origen.

En el encabezado IPv6 del mensaje Neighbor Advertisement (Anuncio de vecino):

- El campo Source Address se establece en la dirección local de enlace asignada a la interfaz de envío.
- El campo Destination Address se establece en la dirección IP de unidifusión del host de origen.
- El campo Hop Limit (Límite de saltos) se establece en el valor 255.

En la figura A.41 se muestra el formato del mensaje Redirect.

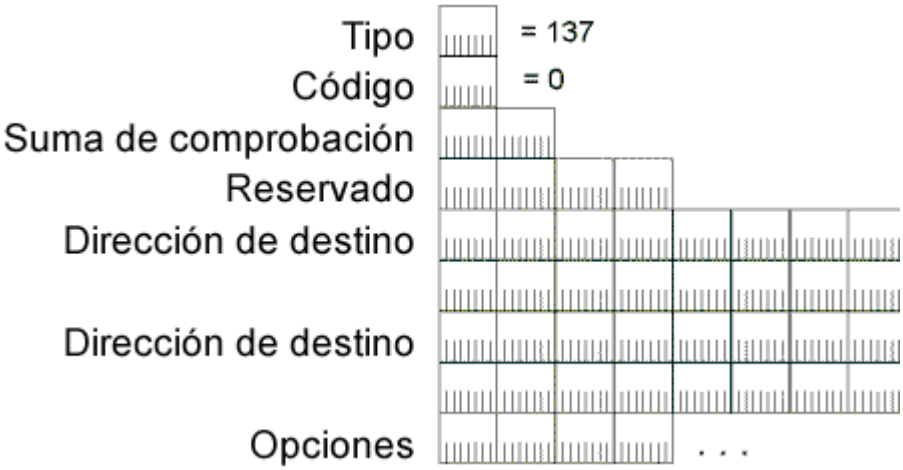

Figura A. 41. Formato del mensaje Redirect (Redirección)

Los campos del mensaje Redirect son:

Type (Tipo): el valor de este campo es 137.

Code (Código): el valor de este campo es 0.

Checksum (Suma de comprobación): el valor de este campo es la suma de comprobación de ICMPv6.

Reserved (Reservado): campo de 32 bits reservado para su uso futuro que se establece en el valor 0.

Target Address (Dirección de destino): indica la mejor dirección para el próximo salto de los paquetes dirigidos al nodo especificado en el campo Destination Address (Dirección de destino). El tamaño de este campo es de 128 bits. Para el tráfico externo al enlace, el campo Target Address se establece en la dirección de enlace local de un enrutador local. Para el tráfico del enlace, el campo Target Address se establece como el campo Destination Address del mensaje Redirect.

Destination Address (Dirección de destino): contiene la dirección de destino del paquete que causó que el enrutador enviara el mensaje Redirect. El tamaño de este campo es de 128 bits. Al recibirlo en el host de origen, los campos Target Address y Destination Address se utilizan para actualizar la información de reenvío del destino. Los paquetes enviados posteriormente al destino desde el host se reenvían a la dirección del campo Target Address.

Opción **Target Link-Layer Address** (Dirección de nivel de enlace objetivo): esta opción contiene la dirección de nivel de enlace del destino (el nodo al que se deben enviar los

paquetes siguientes). La opción Target Link-Layer Address sólo se puede incluir cuando la conoce el enrutador.

Opción **Redirected Header** (Encabezado de Redirección): esta opción incluye una parte del paquete original que hizo que se enviara el menaje Redirect. La cantidad del paquete original incluida es la parte del paquete redirigido que cabe sin que el mensaje Redirect completo tenga más de 1.280 bytes.

10. CONFIGURACIÓN AUTOMÁTICA DE DIRECCIONES

Uno de los aspectos más útiles de IPv6 es su capacidad para configurarse automáticamente, incluso sin ayuda de un protocolo de configuración con estado como el Protocolo de configuración dinámica de host para IPv6 (DHCPv6). De forma predeterminada, un host IPv6 puede configurar una dirección local de enlace para cada interfaz. Mediante el proceso de descubrimiento de enrutadores, un host también puede determinar las direcciones de los enrutadores, otros parámetros de configuración, direcciones adicionales y prefijos en el enlace. En el mensaje Router Advertisement (Anuncio de enrutador) incluye una indicación de si debe utilizarse un protocolo de configuración de direcciones con estado.

La configuración automática de direcciones sólo se puede llevar a cabo con interfaces compatibles con la multidifusión. La configuración automática de direcciones se describe en el RFC 2462.

10.1 ESTADOS DE DIRECCIONES CONFIGURADAS AUTOMÁTICAMENTE

Las direcciones que se configuran automáticamente se encuentran en uno o varios de los estados siguientes:

- **Tentative (Provisional)**

Se está comprobando si la dirección es única. La comprobación se realiza mediante el proceso de detección de direcciones duplicadas. Un nodo no puede recibir tráfico de unidifusión para una dirección provisional. Sin embargo, puede recibir y procesar mensajes Neighbor Advertisement (Anuncio de vecino) de multidifusión enviados como respuesta al mensaje Neighbor Solicitation (Solicitud de vecino) que se envió durante el proceso de detección de direcciones duplicadas.

- **Preferred (Preferida)**

Dirección cuya unicidad se ha comprobado. Un nodo puede enviar y recibir tráfico de unidifusión a y de direcciones preferidas. El período de tiempo que una dirección puede mantenerse en estado de preferencia está determinado por el campo de Preferred Lifetime (Tiempo de vida preferido) en la opción Prefix Information (Información de prefijo) de un mensaje Router Advertisement (Anuncio de enrutador).

- **Deprecated (Desaprobada)**

Dirección que, aunque es válida, no es recomendable utilizar para una nueva comunicación. En las sesiones de comunicación ya existentes aún pueden utilizarse direcciones desaprobadas. Un nodo puede enviar y recibir tráfico de unidifusión a y de direcciones desaprobadas.

- **Valid (Válida)**

Dirección desde la que se puede enviar y recibir tráfico de unidifusión. El estado de dirección válida incluye los estados de dirección preferida y desaprobada. El tiempo que una dirección se mantiene en estado de validez está determinado por el campo Valid Lifetime (Tiempo de vida válido) en la opción Prefix Information de un mensaje Router Advertisement. El tiempo de vida válido debe ser igual o mayor que el tiempo de vida preferido.

- **Invalid (No válida)**

Dirección para la que un nodo ya no puede enviar o recibir tráfico de unidifusión. Una dirección pasa al estado de no válida cuando caduca el tiempo de vida válido.

En la figura A.42 se muestra la relación entre los estados de una dirección configurada automáticamente y los tiempos de vida preferido y válido.

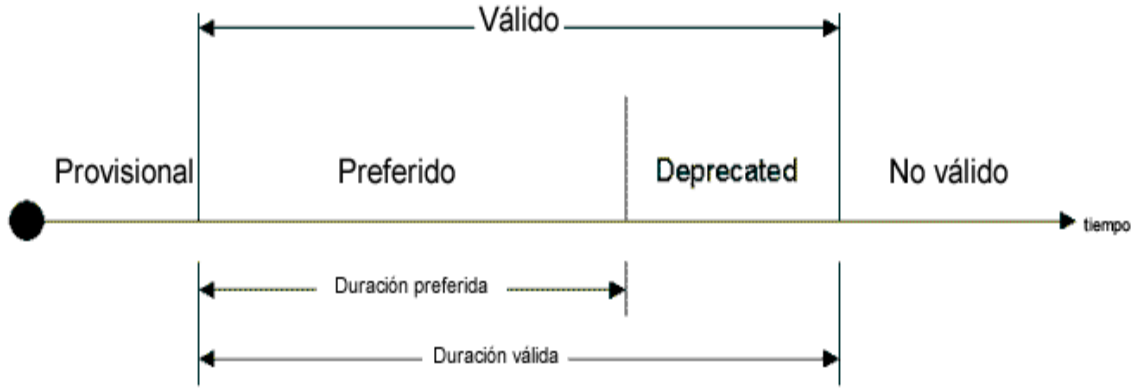

Figura A. 42. Estado y tiempos de vida de una dirección configurada automáticamente

Nota Con excepción de una configuración automática para direcciones locales de enlace, la configuración automática de direcciones sólo se especifica para los hosts. Los enrutadores deben obtener los parámetros de configuración y de dirección por otros medios, tales como la configuración manual.

10.2 TIPOS DE CONFIGURACIÓN AUTOMÁTICA

Hay tres tipos de perfiles de configuración automática:

- **Sin estado**

La configuración de direcciones se basa en la recepción de mensajes Router Advertisement (Anuncio de enrutador) con los indicadores Managed Address Configuration (Configuración de direcciones administradas) y Other Stateful Configuration (Otras configuraciones con estado) establecidos en el valor 0, y una o varias opciones Prefix Information (Información de prefijo).

- **Con estado**

La configuración se basa en el uso de un protocolo de configuración de direcciones con estado, como DHCPv6, para obtener direcciones y otras opciones de configuración. Un host utiliza la configuración de direcciones con estado cuando recibe mensajes Router Advertisement sin opciones de prefijo en los que el indicador Managed Address Configuration o el indicador Other Stateful Configuration están establecidos en el valor 1. Un host utilizará también el protocolo de configuración de direcciones con estado cuando no haya enrutadores en el enlace local.

- **Ambos**

La configuración se basa en la recepción de mensajes Router Advertisement con opciones Prefix Information y el indicador Managed Address Configuration o el indicador Other Stateful Configuration establecidos en el valor 1.

Para todos los tipos, se configura siempre una dirección local de enlace.

10.3 PROCESO DE CONFIGURACIÓN AUTOMÁTICA

El proceso de configuración automática para un nodo IPv6 es el siguiente:

1. Se deriva una dirección local de enlace provisional a partir del prefijo local de enlace FE80::/64 y el identificador de interfaz de 64 bits.
2. Mediante el proceso de detección de direcciones duplicadas, para comprobar la unicidad de una dirección local de enlace provisional, se envía un mensaje Neighbor Solicitation (Solicitud de vecino) con el campo de Target Address (Dirección de destino) establecido en la dirección local de enlace provisional.
3. Si se envía un mensaje Neighbor Advertisement en respuesta al mensaje Neighbor Solicitation que se recibió, esto indica que otro nodo del enlace local utiliza la dirección local de enlace provisional y se detiene la configuración automática de direcciones. En este momento, se debe realizar una configuración manual en el nodo.
4. Si no se recibe ningún mensaje Neighbor Advertisement (que se envía en respuesta al mensaje Neighbor Solicitation), se asume que la dirección local de enlace provisional es única y válida. Se inicializa la dirección local de enlace para la interfaz. La dirección de nivel de enlace de multidifusión de nodo solicitado correspondiente se registra con el adaptador de red.

Para un host IPv6, la configuración automática de direcciones continúa como se describe a continuación:

1. El host envía un mensaje Router Solicitation (Solicitud de enrutador).
2. Si no se recibe ningún mensaje Router Advertisement, el host utiliza un protocolo de configuración de direcciones con estado para obtener direcciones y otros parámetros de configuración.
3. Si se recibe un mensaje Router Advertisement, se configuran los campos Hop Limit (Límite de saltos), Reachable Time (Tiempo accesible), Retrans Timer (Cronómetro de retransmisión) y MTU (si existe la opción MTU).
4. Para cada opción Prefix Information (Información de prefijo) que se utilice:
   Si el indicador On-Link (En el enlace) se establece en el valor 1, se agrega el prefijo a la lista.
   Si el indicador Autonomous (Autónomo) se establece en el valor 1, el prefijo y el identificador de interfaz de 64 bits se utilizan para obtener una dirección provisional derivada.
   El proceso de detección de direcciones duplicadas se utiliza para comprobar la unicidad de la dirección provisional.
   Si se utiliza la dirección provisional, no se inicializa el uso de la dirección para la interfaz.
   Si no se utiliza la dirección provisional, se inicializa la dirección. Este proceso incluye la configuración de los tiempos de vida de validez y preferido, basados en los campos Valid Lifetime (Tiempo de vida válido) y Preferred Lifetime (Tiempo de vida preferido) de la opción Prefix Information. También incluye el registro de la dirección de nivel de enlace de multidifusión de nodo solicitado correspondiente con el adaptador de red.
5. Si el indicador Managed Address Configuration (Configuración de dirección administrada) del mensaje Router Advertisement está establecido en el valor 1, se utiliza un protocolo de configuración de direcciones con estado para obtener direcciones adicionales.
6. Si el indicador Other Stateful Configuration (Otras configuraciones con estado) del mensaje Router Advertisement está establecido en el valor 1, se utiliza un protocolo de configuración de direcciones con estado para obtener parámetros de configuración adicionales.