UNIVERSIDAD ADVENTISTA DE CENTROAMÉRICA

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS DE LA MATERIA DE TELEMÁTICA Y REDES

10 DE NOVIEMBRE , 2000

ABRAHAM SALGADO ZELEDON

INDICE

INTRODUCCIÓN

Debido a la preocupación reciente por el agotamiento inminente del conjunto actual de direcciones de Internet y el deseo de proporcionar funcionalidad adicional para dispositivos modernos, se encuentra en proceso de normalización una actualización de la versión actual del Protocolo Internet (IP, *Internet Protocol*) denominada IPv4. La nueva versión, denominada IP versión 6 (IPv6), resuelve problemas de diseño no previstos en IPv4 y está preparada para llevar Internet al siglo XXI. En este documento se describen los problemas de Internet IPv4 y cómo 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 y está diseñado para técnicos de redes y profesionales de soporte técnico que ya están familiarizados con conceptos básicos de redes y con TCP/IP.

La versión actual de IP (conocida como versión 4 o IPv4) no ha cambiado sustancialmente desde la publicación de 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.

CARACTERÍSTICAS DEL IPv6

A continuación se enumeran las características del nuevo protocolo IPv6:

- Nuevo formato de encabezado
- Gran espacio de direcciones
- Direccionamiento jerárquico e infraestructura de enrutamiento eficientes
- Configuración de direcciones sin estado y con estado
- Seguridad integrada
- Mayor compatibilidad con QoS
- Nuevo protocolo para la interacción de nodos vecinos
- Capacidad de ampliación

En las secciones siguientes se describe cada uno de estos tipos de túnel más detalladamente.

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 $3,4x10^{38}$ 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

La 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. Para obtener más información, consulte "Direcciones de unidifusión global agregables".

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 vínculo se configuran automáticamente con direcciones IPv6 para el vínculo (que se denominan direcciones locales de vínculo) y con direcciones derivadas de prefijos anunciados por enrutadores

locales. Incluso en ausencia de un enrutador, los hosts del mismo vínculo pueden configurarse automáticamente con direcciones locales de vínculo 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 vínculo). 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.

Diferencias entre IPv4 e IPv6

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

Tabla 1 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). Para obtener más información, consulte "Direccionamiento IPv6".
La compatibilidad con IPSec es opcional.	La compatibilidad con IPSec es obligatoria. Para obtener más información, consulte "Encabezado de IPV6".
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). Para obtener más información, consulte "Encabezado de IPV6".
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. Para obtener más información, consulte "Encabezado de IPV6".

El encabezado incluye una suma de comprobación.	El encabezado no incluye una suma de comprobación. Para obtener más información, consulte "Encabezado de IPv6".
El encabezado incluye opciones.	Todos los datos opcionales se mueven a extensiones de encabezado IPv6. Para obtener más información, consulte "Encabezado de 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 vínculo.	Las tramas de solicitud de ARP se reemplazan por mensajes Neighbor Solicitation (Solicitud de vecino) de multidifusión. Para obtener más información, consulte "Descubrimiento de vecino".
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 obtener más información, consulte "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. Para obtener más información, consulte "Descubrimiento de vecino".
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 vínculo. Para obtener más información, consulte "Direcciones IPv6 de multidifusión".
La configuración debe efectuarse manualmente o a través de DHCP.	No se necesita configuración manual ni DHCP. Para obtener más información, consulte "Configuración automática de direcciones".
Utiliza registros de recursos (A) de dirección de host en el Sistema de	Utiliza registros de recursos (AAAA) de dirección de host en el Sistema de

nombres de dominio (DNS, *Domain Name System*) para asignar nombres de host a direcciones IPv4.	nombres de dominio (DNS) para asignar nombres de host a direcciones IPv6. Para obtener más información, consulte "IPv6 y DNS".
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. Para obtener más información, consulte "IPv6 y DNS".

Paquetes IPv6 sobre medios LAN

Una trama de nivel de vínculo que contiene un paquete IPv6 tiene la siguiente estructura:

- Encabezado y finalizador de nivel de vínculo: encapsulación del paquete IPv6 en el nivel de vínculo.
- Encabezado IPv6: el nuevo encabezado de IPv6. Para obtener más información, consulte "Encabezado de IPv6".
- Carga: la carga del paquete IPv6. Para obtener más información, consulte "Encabezado de IPv6".

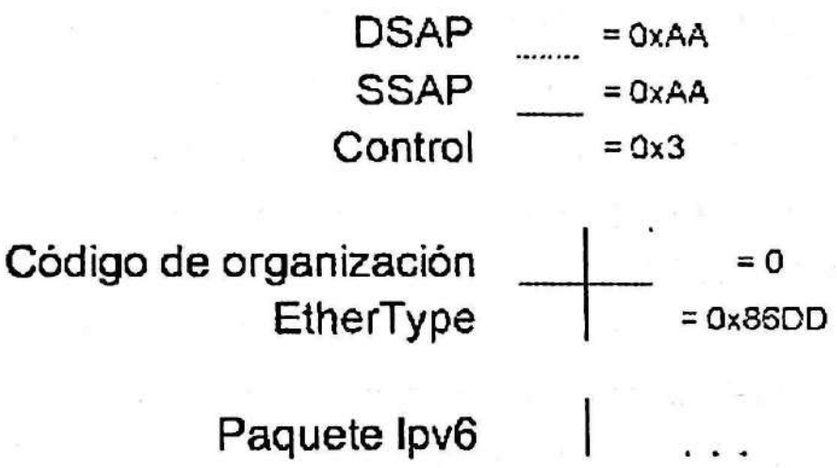
Para las tecnologías típicas de LAN, como Ethernet, Token Ring e Interfaz de datos distribuidos por fibra (FDDI, *Fiber Distributed Data Interface*), los paquetes IPv6 se encapsulan de dos maneras distintas: con el encabezado de Ethernet II o con un encabezado de Protocolo de acceso a subredes (SNAP, *Sub-Network Access Protocol*) que se utilizan en IEEE 802.3 (Ethernet), IEEE 802.5 (Token Ring) y FDDI.

Encapsulación de Ethernet II

Con la encapsulación de Ethernet II, los paquetes IPv6 se indican al establecer el valor 0x86DD en el campo EtherType del encabezado de Ethernet II (IPv4 se indica al establecer el valor 0x800 en el campo EtherType). Con la encapsulación de Ethernet II, los paquetes IPv6 pueden tener un tamaño mínimode 46 bytes y un tamaño máximo de 1.500 bytes.

Encapsulación de IEEE 802.3, IEEE 802.5 y FDDI

En redes IEEE 802.3 (Ethernet), IEEE 802.5 (Token Ring) y FDDI, se utiliza el encabezado de Protocolo de acceso a subredes (SNAP) y el campo EtherType se establece en el valor 0x86DD para indicar IPv6. La figura 3 muestra la encapsulación de SNAP.



Para la encapsulación de IEEE 802.3 con el encabezado de SNAP, los paquetes IPv6 pueden tener un tamaño mínimo de 38 bytes y un tamaño máximo de 1.492 bytes. Para la encapsulación FDDI con el encabezado de SNAP, los paquetes IPv6 pueden tener un tamaño máximo de 4.352 bytes. Para obtener información acerca de los tamaños máximos de los paquetes IPv6 para redes IEEE 802.5, consulte RFC 2470.

IMPLEMENTACION DEL IPv6

Implementación de IPv6 de Microsoft Research

La implementación de IPv6 de Microsoft Research es un protocolo de IPv6 que se ejecuta en Windows NT 4.0 y Windows 2000. Actualmente no existen planes para asegurar la compatibilidad con Windows 95, Windows 98 o Windows CE. La implementación de IPv6 de Microsoft Research se ejecuta como un protocolo independiente que contiene sus propias versiones del Protocolo de control de transporte (TCP, *Transmission Control Protocol*) y del Protocolo de datagramas de usuario (UDP, *User Datagram Protocol*). Puede experimentar con IPv6 sin que se vean afectadas las comunicaciones IPv4.
La implementación de IPv6 de Microsoft Research incluye archivos compilados para la instalación, código fuente y diversas herramientas y archivos suplementarios. Consulte el sitio Web de la implementación de IPv6 de Microsoft Research para ver la última versión y una lista de características y protocolos compatibles con IPv6.

Microsoft IPv6 Technology Preview para Windows 2000

Microsoft IPv6 Technology Preview para Windows 2000 es un derivado de la implementación de IPv6 de Microsoft Research diseñado para los programadores de aplicaciones. Se puede utilizar para iniciar el aprendizaje y la experimentación con IPv6, con el objetivo final de ejecutar aplicaciones sobre IPv6. Tal como sugiere su nombre, Microsoft IPv6 Technology Preview para Windows 2000 sólo se puede instalar en un equipo en el que se ejecute una versión de Windows 2000.

Direccionamiento IPv6

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 $3,4 \times 10^{38}$) 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 ($6,5 \times 10^{23}$) 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 $6,5 \times 10^{23}$ 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 RFC 2373.

Asignación 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 2 se muestra la asignación del espacio de direcciones de IPv6 por FP.

Tabla 2 Asignación actual del espacio de direcciones de IPv6

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 vínculo	1111 1110 10	1/1024
Direcciones de unidifusión local de sitio	1111 1110 11	1/1024
Direcciones de multidifusión	1111 1111	1/256

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 vínculo y direcciones de unidifusión local de sitio. Éstas sólo representan el 15 por ciento de todo el espacio de direcciones de IPv6.

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:

Tipos de direcciones IPv6

Hay tres tipos de direcciones IPv6:

1. Unidifusión

   Una dirección de unidifusión identifica a una sola interfaz en el ámbito del tipo de dirección de unidifusión. Con la tipología 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, 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.

2. Multidifusión

   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.

3. Cualquier difusión

   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.

Nota En RFC 2373 no se define una dirección de difusión. Todos los tipos de direccionamiento IPv4 se realizan en IPv6 mediante direcciones de multidifusión. Por ejemplo, la subred y las direcciones de difusión limitada de IPv4 se reemplazan por la dirección de multidifusión de todos los nodos de ámbito local de vínculo de FF02::1.

Vínculos y subredes

De forma similar a IPv4, el prefijo de subred de IPv6 (Id. de subred) se asigna a un único vínculo. Se pueden asignar varios Id. de subred al mismo vínculo. Esta técnica se denomina red múltiple.

Direcciones IPv6 de unidifusión

Los siguientes tipos de direcciones son direcciones IPv6 de unidifusión:

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

Direcciones de unidifusión global 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.

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.

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. Para obtener más información acerca de las direcciones de unidifusión global agregables, consulte RFC 2374.

Direcciones de unidifusión de uso local

Hay dos tipos de direcciones de unidifusión de uso local:

1. Direcciones locales de vínculo utilizadas entre vecinos de vínculo y para procesos Neighbor Discovery.
2. Direcciones locales de sitio utilizadas entre nodos que se comunican con otros nodos del mismo sitio.

Direcciones locales de vínculo

Los nodos utilizan las direcciones locales de vínculo identificadas mediante FP 1111 1110 10 cuando se comunican con nodos vecinos en el mismo vínculo. Por ejemplo, en una red IPv6 de vínculo único sin enrutador, las direcciones locales de vínculo se utilizan para la comunicación entre los hosts del vínculo. Las direcciones locales de vínculo equivalen a direcciones IPv4 configuradas automáticamente en sistemas que ejecutan Microsoft Windows con el prefijo 169.254.0.0/16. El ámbito de una dirección local de vínculo es el vínculo local.
Se necesita una dirección local de vínculo para los procesos Neighbor Discovery (Descubrimiento de vecino) y siempre se configura automáticamente, incluso en

ausencia de todas las demás direcciones de unidifusión. Para obtener más información acerca del proceso de configuración automática para direcciones de vínculo local, consulte "Configuración automática de direcciones".
Las direcciones locales de vínculo siempre empiezan por FE80. Con el identificador de interfaz de 64 bits, el prefijo para las direcciones locales de vínculo es siempre FE89::/64. Un enrutador IPv6 nunca reenvía el tráfico de vínculo local más allá del vínculo.

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 vínculo, 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. Para obtener más información, consulte "Configuración automática de direcciones".

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.

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 vínculo o reenviarse mediante un enrutador de IPv6.

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.

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. Para obtener más información

acerca de los cuatro tipos de asignaciones de direcciones NSAP, consulte RFC 1888.

- 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.

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.

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 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 3 se muestran los valores definidos para el campo Scope.

Tabla 3 Valores definidos para el campo Scope

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

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

Para identificar todos los enrutadores de los ámbitos locales de nodo, de vínculo 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 vínculo)
- 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, 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.

Dirección de nodo solicitado

La dirección de nodo solicitado facilita una consulta eficiente de los nodos de red durante la resolución de direcciones. En IPv4, la trama de solicitud de ARP se envía a la difusión de nivel MAC, lo que afecta a todos los nodos del segmento de red, incluidos los que no utilizan IPv4. IPv6 utiliza el mensaje Neighbor Discovery (Descubrimiento de vecino) para realizar la misma operación. Sin embargo, en vez de utilizar la dirección de multidifusión de todos los nodos de ámbito de vínculo local como destino del mensaje Neighbor Solicitation (Solicitud de vecino), lo que afectaría a todos los nodos IPv6 del vínculo local, se utiliza la dirección de multidifusión de nodo solicitado. La dirección de multidifusión de nodo solicitado consta del prefijo FF02::1:FF00:0/104 y los últimos 24 bits de la dirección IPv6 que se va a resolver.

Por ejemplo, para el nodo con la dirección IPv6 local de vínculo FE80::2AA:FF:FE28:9C5A, la dirección de nodo solicitado correspondiente es FF02::1:FF28:9C5A. Para resolver la dirección FE80::2AA:FF:FE28:9C5A en la dirección de su nivel de vínculo, un nodo puede enviar un mensaje Neighbor Solicitation a la dirección de nodo solicitado FF02::1:FF28:9C5A. El nodo que utiliza la dirección FE80::2AA:FF:FE28:9C5A escucha el tráfico de multidifusión en la dirección del nodo solicitado y, para las interfaces que corresponden a una tarjeta adaptadora de red física, habrá registrado la dirección de multidifusión correspondiente con la tarjeta adaptadora de red.

El resultado del uso de la dirección de multidifusión de nodo solicitado es que, para las resoluciones de direcciones, algo que ocurre comúnmente en los vínculos, no se necesita un mecanismo que afecte a todos los nodos de la red. Si se utiliza la dirección de nodo solicitado, muy pocos nodos se ven afectados durante la resolución de direcciones. En la práctica, debido a la relación existente entre la dirección MAC de Ethernet, el Id. de interfaz y la dirección de nodo solicitado, la dirección de nodo solicitado actúa como dirección de pseudo-unidifusión para una resolución de direcciones eficiente.

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.

Figura 10 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.

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 vínculo 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 vínculo para el tráfico del vínculo 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 vínculo (FF02::1).
- La dirección de nodo solicitado para cada dirección de unidifusión.

- Las direcciones de multidifusión de los grupos unidos.

Direcciones IPv6 para un enrutador

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

- Una dirección local de vínculo 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 vínculo (FF02::1).
- La dirección de multidifusión de todos los enrutadores del ámbito local de vínculo (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.

Identificadores de interfaz de IPv6

Todas las direcciones que utilizan los prefijos comprendidos entre 001 y 111 deben utilizar también un identificador de interfaz de 64 bits que está derivado de la dirección EUI-64. La dirección EUI-64 de 64 bits fue definida por el Instituto de ingeniería eléctrica y electrónica (IEEE, *Institute of Electrical and Electronic Engineers*). Las direcciones EUI-64 se asignan a una tarjeta adaptadora de red o se derivan de direcciones IEEE 802.

Nota En este documento se trata la derivación de los identificadores de interfaz de IPv6 según RFC 2373. Para tratar cuestiones relativas a la privacidad, se describe una derivación alternativa del identificador de interfaz de IPv6 que cambia con el tiempo en el borrador para Internet titulado "Privacy Extensions for

Stateless Address Autoconfiguration in IPv6" (Extensiones de privacidad para la configuración automática de direcciones sin estado en IPv6).

Direcciones IEEE 802

Los identificadores de interfaz tradicionales de los adaptadores de red utilizan una dirección de 48 bits denominada dirección IEEE 802. Consta de un Id. de compañía de 24 bits (también conocido como Id. del fabricante) y un Id. de extensión de 24 bits (también conocido como Id. de tarjeta). La combinación del Id. de compañía, que se asigna en exclusiva a cada fabricante de adaptadores de red, y el Id. de tarjeta, que se asigna en exclusiva a cada adaptador de red en el momento del montaje, genera una dirección exclusiva global de 48 bits. Esta dirección de 48 bits también se denomina dirección física, de hardware o de control de acceso a medios (MAC, *Media Access Control*).

Los bits definidos en la dirección IEEE 802 son:

Universal/Local (U/L): el bit situado junto al bit de orden inferior en el primer byte se utiliza para indicar si la dirección se administra universal o localmente. Si el bit U/L está establecido en el valor 0, IEEE ha administrado la dirección a través de la designación de un Id. de compañía. Si el bit U/L está establecido en el valor 1, la dirección se administra localmente. El administrador de la red ha suplantado la dirección del fabricante y ha especificado otra dirección. El bit U/L bit se designa mediante u en la figura 11.

Individual/Group (I/G) (Individual/Grupo): el bit de orden inferior del primer byte se utiliza para indicar si se trata de un dirección individual (de unidifusión) o de grupo (de multidifusión). Cuando está establecido en el valor 0, la dirección es de unidifusión. Cuando está establecido en el valor 1, la dirección es de multidifusión. El bit I/G se designa mediante g en la figura 11.

Para una dirección de adaptador de red 802.x típica, tanto el bit U/L como el bit I/G se establecen en el valor 0, que corresponde a una dirección MAC de unidifusión administrada de forma universal.

Identificadores de interfaz IEEE EUI-64

La dirección IEEE EUI-64 representa un nuevo estándar en el direccionamiento de interfaces de red. El Id. de la compañía también tiene 24 bits, pero el Id. de extensión es de 40 bits, lo que representa un espacio de direcciones mucho mayor para el fabricante de adaptadores de red. La dirección EUI-64 utiliza los bits U/L e I/G del mismo modo que la dirección IEEE 802.

Asignar direcciones IEEE 802 a direcciones EUI-64

Para crear una dirección EUI-64 a partir de una dirección IEEE 802, los 16 bits de 11111111 11111110 (0xFFFE) se insertan en la dirección IEEE 802 entre el Id. de la compañía y el Id. de extensión.

Obtener identificadores de interfaz para direcciones IPv6

Para obtener el identificador de interfaz de 64 bits para direcciones de unidifusión IPv6, el bit U/L de la dirección EUI-64 se complementa (si es 1, se establece en el valor 0 y si es 0, en el valor 1).

Para obtener un identificador de interfaz de IPv6 a partir de una dirección IEEE 802, en primer lugar deberá asignar la dirección IEEE 802 a una dirección EUI-64 y, después, complementar el bit U/L.

Ejemplo de conversión de dirección IEEE 802

El Host A tiene la dirección MAC Ethernet 00-AA-00-3F-2A-1C. En primer lugar, se convierte al formato EUI-64 por la inserción de FF-FE entre el tercer y el cuarto bytes, lo que genera 00-AA-00-FF-FE-3F-2A-1C. A continuación, el bit U/L, que es el séptimo del primer byte, se complementa. El primer byte en forma binaria es 00000000. Cuando se complementa el séptimo bit, se convierte en

00000010 (0x02). El resultado final es 02-AA-00-FF-FE-3F-2A-1C que, cuando se convierte a la notación hexadecimal con puntos, pasa a ser el identificador de interfaz 2AA:FF:FE3F:2A1C. Como resultado, la dirección local de vínculo que corresponde al adaptador de red con la dirección MAC 00-AA-00-2A-1C es FE80::2AA:FF:FE3F:2A1C.

Nota Cuando complemente el bit U/L, agregue 0x2 al primer byte si la dirección se administra universalmente y reste 0x2 del primer byte si la dirección se administra localmente.

Asignar direcciones de multidifusión IPv6 a direcciones Ethernet

Cuando envía paquetes de multidifusión IPv6 a través de un vínculo Ethernet, la dirección MAC de destino es 33-33-mm-mm-mm-mm, donde mm-mm-mm-mm es una asignación directa de los últimos 32 bits de la dirección de multidifusión IPv6.

Para recibir de un modo eficiente paquetes de multidifusión IPv6 a través de un vínculo Ethernet, los adaptadores de red Ethernet pueden almacenar otras direcciones MAC de interés en una tabla del adaptador de red. Si se recibe una trama Ethernet con una dirección MAC de interés, se pasa a las capas superiores para su procesamiento. Para todas las direcciones de multidifusión que escucha el host, existe una entrada correspondiente en la tabla de direcciones MAC de interés.

Por ejemplo, un host con la dirección MAC Ethernet 00-AA-00-3F-2A-1C (dirección local de vínculo FE80::2AA:FF:FE3F:2A1C) registra las siguientes direcciones MAC de multidifusión con el adaptador Ethernet:

- La dirección 33-33-00-00-00-01, que corresponde a la dirección de multidifusión de todos los nodos de ámbito local de vínculo FF02::1.
- La dirección 33-33-FF-3F-2A-1C, que corresponde a la dirección de nodo solicitado FF02::1:FF3F:2A1C. Recuerde que la dirección de nodo solicitado se compone del prefijo FF02::1:FF00:0/104 y los últimos 24 bits de la dirección IPv6 de unidifusión.

Según sea necesario, se agregan o se quitan direcciones de multidifusión adicionales de la tabla de direcciones de interés del adaptador de red Ethernet en el host que escucha.

IPv6 y DNS

En 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

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.microsoft.com 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.

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.2.0.0.0.0.0.0.0.0.0.0.0.0.0.C.E.F.IP6.INT.

La compatibilidad con DNS que se describe en RFC 1886 representa un método sencillo de asignar nombres de hosts a direcciones IPv6 y proporcionar una resolución de nombres inversa. Sin embargo, esta compatibilidad no proporciona un método sencillo para propagar los cambios a registros AAAA, debido a la nueva numeración del sitio o a la delegación de zonas de búsqueda inversa en límites de bits arbitrarios (IP6.INT se designa en límites de cuarteto). Estas cuestiones se resuelven mediante un nuevo registro de recursos "A6" que se describe en el borrador de Internet titulado "DNS Extensions to Support IPv6 Address Aggregation and Renumbering" (Extensiones DNS que admiten cambiar la numeración y agregar direcciones IPv6).

Direcciones IPv4 y sus equivalentes en IPv6

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

Tabla 4 Asignación actual del espacio de direcciones de 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 vínculo (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

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.

Encabezado de IPv4

En la figura 17 se muestra el encabezado de IPv4, que se describe en RFC 791.

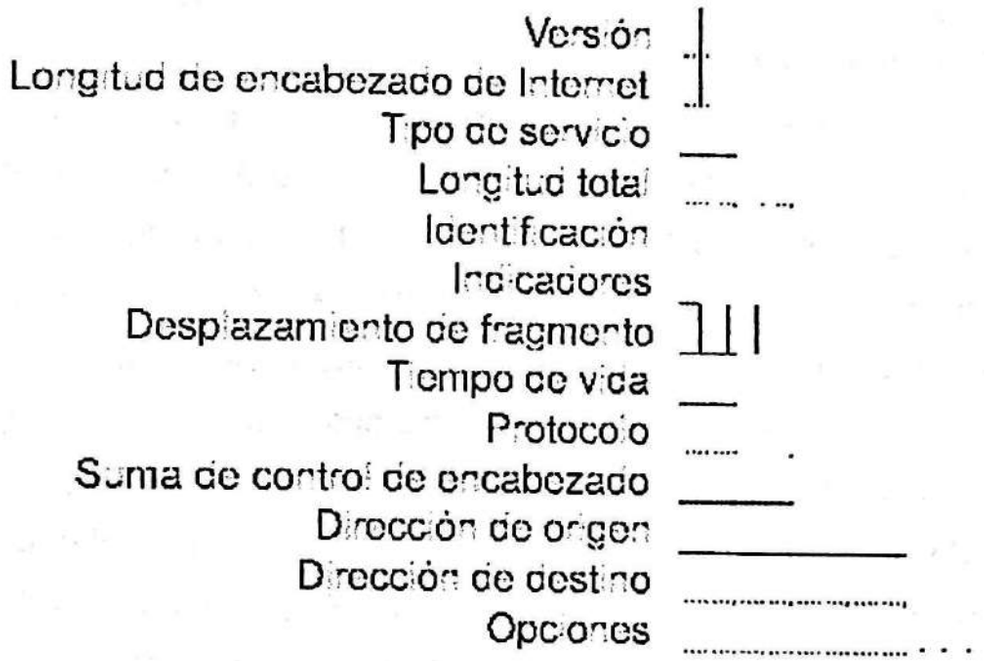


Figura 17 Encabezado de IPv4

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 vínculo. 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 vínculos 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 RFC 791, deben disminuir TTL en uno como mínimo. Por lo tanto, TTL se convierte en un recuento de vínculos 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).

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 documento.

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).

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 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 vínculos 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 5 se muestran valores típicos del campo Next Header para un encabezado de IPv6 o un encabezado de extensión IPv6.

Tabla 5 Valores del campo Next Header

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)

Diferencias entre los encabezados de IPv4 e IPv6

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

Tabla 6 Campos de encabezado de IPv4 y sus equivalentes en 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 vínculo.
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.

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 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.

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 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

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 21 se muestra el encabezado Hop-by-Hop Options.

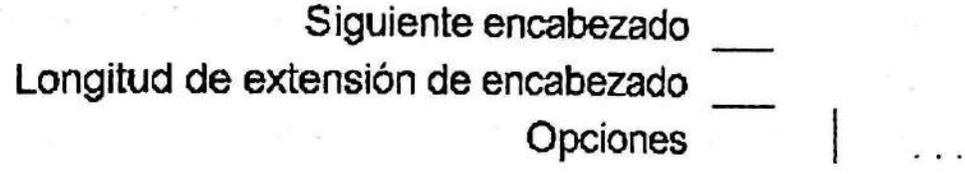


Figura 21 Encabezado Hop-by-Hop Options (Opciones de salto a salto).

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 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*).

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 22 se muestra el encabezado Destination Options.

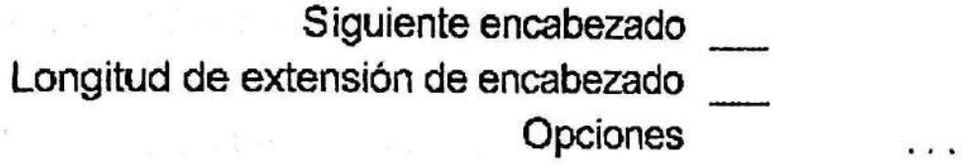


Figura 22 Encabezado Destination Options (Opciones de destino)

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.

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.

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 24 se muestra el encabezado Fragment.

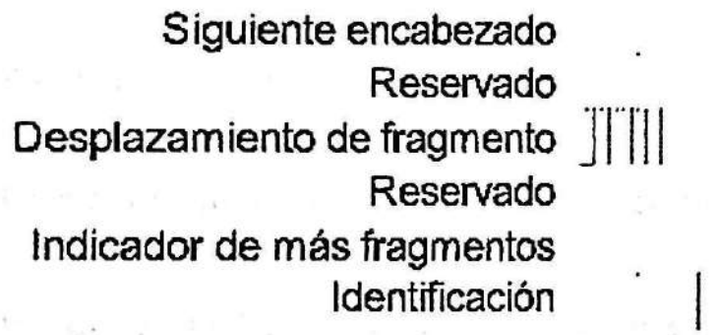


Figura 24 Encabezado Fragment (Fragmento)

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 vínculo 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.

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 RFC 2402, forma parte de la arquitectura de seguridad para el Protocolo Internet definida en RFC 2401.

El encabezado Authentication se identifica por el valor 51 en el campo Next Header (Encabezado siguiente) del encabezado anterior.

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).

En este documento no se trata en detalle cómo proporciona el encabezado Authentication posibilidades de autenticación e integridad de datos a través de técnicas criptográficas. Para obtener más información, consulte RFC 2402.

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.

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).

En este documento no se trata en detalle cómo proporcionan el encabezado de extensión y el finalizador ESP posibilidades de confidencialidad, autenticación e integridad de los datos a través de técnicas criptográficas. Para obtener más información, consulte RFC 2406.

MTU de IPv6

IPv6 requiere que el nivel de vínculo admita un tamaño mínimo de 1.280 bytes para los paquetes IPv6. Los niveles de vínculo que no admiten este tamaño deben proporcionar una combinación de fragmentación y reensamblado de nivel de vínculo transparente para IPv6. En los niveles de vínculo 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 vínculo 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 que se describe en "Descubrimiento de MTU de ruta de acceso". 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.

Sumas de comprobación de nivel superior

La implementación actual de TCP y UDP para IPv4 incorpora en el cálculo de suma de comprobación un pseudo-encabezado que incluye los campos Source Address (Dirección de origen) y Destination Address (Dirección de destino) de IPv4. Este cálculo de suma de comprobación debe modificarse para que el tráfico de TCP y UDP que se envía a través de IPv6 incluya direcciones IPv6.

El pseudo-encabezado de IPv6 incluye los campos Source Address, Destination Address, un campo Upper-Layer Packet Length (Longitud de paquete de nivel superior) que indica la longitud de PDU de nivel superior, y un campo Next Header (Encabezado siguiente) que indica el protocolo de nivel superior para el que se va a calcular la suma de comprobación.

Este pseudo-encabezado se utiliza también para el cálculo de suma de comprobación de ICMPv6.

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. MLD se describe más detalladamente en "Descubrimiento de escucha de multidifusión".

- Neighbor Discovery (ND o Descubrimiento de vecino)

  Neighbor Discovery es un conjunto de cinco mensajes ICMPv6 que administran la comunicación entre nodos en un vínculo. 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. Neighbor Discovery se describe más detalladamente en "Descubrimiento de vecino".

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

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 RFC 2463 e incluyen Echo Request (Solicitud de eco) y Echo Reply (Respuesta de eco).

Encabezado de ICMPv6

En la figura 29 se muestra la estructura de todos los mensajes ICMPv6.

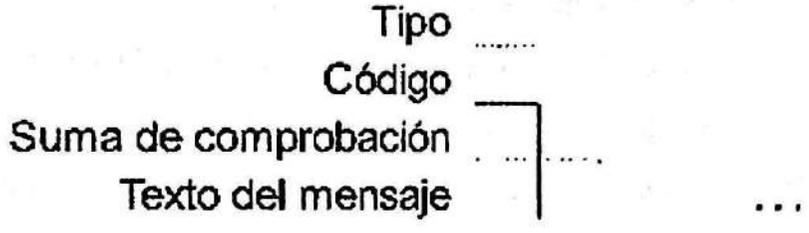


Figura 29 Estructura de los mensajes ICMPv6

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.

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 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 7 se muestra el valor del campo Code para los distintos mensajes Destination Unreachable.

Tabla 7 Mensajes ICMPv6 Destination Unreachable (Destino inaccesible)

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 vínculo 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.

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 vínculo de reenvío es menor que el tamaño del paquete IPv6.

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 vínculo 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 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 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 8 se muestran los valores del campo Code para los mensajes Parameter Problem.

Tabla 8 Mensajes ICMPv6 Parameter Problem (Problema de parámetro)

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.

Mensajes informativos ICMPv6

Los mensajes informativos ICMPv6, definidos en 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 34 se muestra el mensaje ICMPv6 Echo Request.

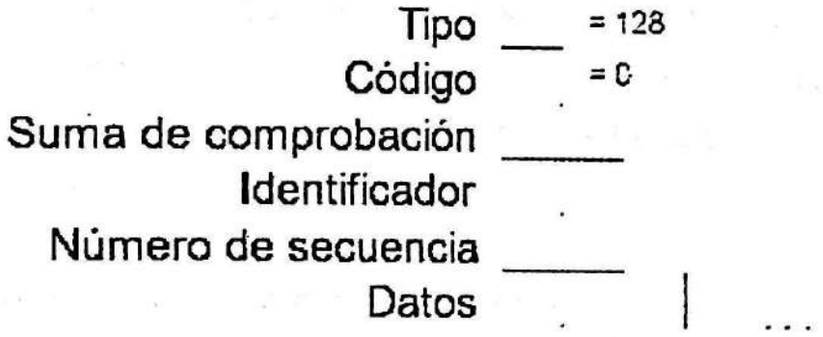


Figura 34 Mensaje ICMPv6 Echo Request (Solicitud de eco)

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 35 se muestra el mensaje ICMPv6 Echo Reply.

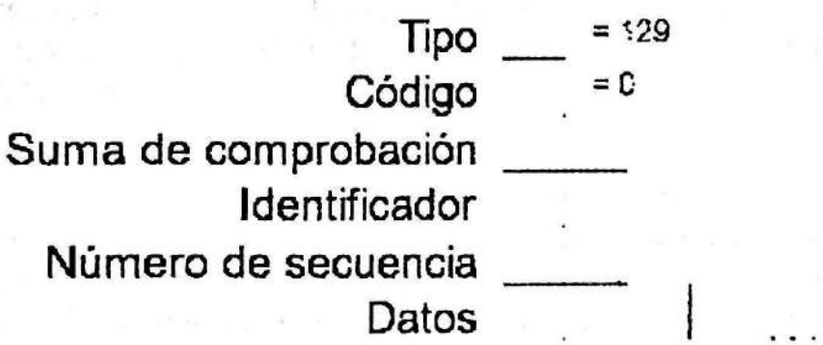


Figura 35 Mensaje ICMPv6 Echo Reply (Respuesta de eco)

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.

Diferencias entre los mensajes ICMPv4 e ICMPv6

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

Tabla 9 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	Destination Unreachable-Communication with destination administratively prohibited (Destino inaccesible: comunicación con el destino prohibida administrativamente)

administrativamente) (Type 3, Code 10)	(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) (Type 12, Code 0)	Parameter Problem (Problema de parámetro) (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). Para obtener más información, consulte "Descubrimiento de vecino".

Descubrimiento de MTU de ruta de acceso

La unidad MTU de ruta de acceso es la MTU de vínculo mínima de todos los vínculos 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 vínculo 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 vínculo con una MTU de vínculo 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 vínculo 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 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 vínculo mínima de 1.280 bytes como MTU de ruta de acceso.

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 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.

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 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:

1. Multicast Listener Query (Consulta de escucha de multidifusión)

   Los enrutadores utilizan los mensajes Multicast Listener Query para consultar en un vínculo 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.

2. 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.

3. 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 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.

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 vínculo conectado para hosts a la escucha.

En el encabezado IPv6, la dirección de origen es la dirección local de vínculo 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 vínculo (FF02::1). Para Multicast-Address-Specific Query, la dirección de destino es la dirección de multidifusión específica que se consulta.

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.

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 vínculo 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 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.

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 vínculo 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 vínculo (FF02::2).

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.

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 vínculo de un nodo vecino al que se va a reenviar un paquete IPv6 y determinar cuándo ha cambiado la dirección de nivel de vínculo 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 vínculo.
- 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 10 se muestran y describen los procesos ND documentados en RFC 2461.

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

Proceso	Descripción
Descubrimiento de enrutadores	Proceso por el que un host descubre los enrutadores locales de un vínculo conectado. Equivale al proceso Router Discovery (Descubrimiento de enrutador) de ICMPv4. Para obtener más información, consulte "Descubrimiento de enrutadores".
Descubrimiento de prefijos	Proceso por el que los hosts descubren los prefijos de red para destinos de vínculos locales. Es similar al proceso Address Mask Request/Reply (Solicitud y respuesta de máscara de dirección) de ICMPv4. Para obtener más información, consulte "Descubrimiento de enrutadores".
Descubrimiento de parámetros	Proceso por el que los hosts descubren parámetros de funcionamiento adicionales, incluida la unidad MTU de vínculo y el límite de saltos predeterminado para los paquetes salientes. Para obtener más información, consulte "Descubrimiento de enrutadores".
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). Para obtener más información, consulte "Configuración automática de direcciones".
Resolución de direcciones	Proceso por el que los nodos resuelven la dirección IPv6 de un vecino en su dirección de nivel de vínculo. Equivale a ARP en IPv4. Para obtener más información, consulte "Resolución de direcciones".
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 vínculo. Para obtener más información, consulte "Algoritmo de host de envío".
Detección de inaccesibilidad a un vecino	Proceso por el que un nodo determina que el nivel IPv6 de un vecino ya no recibe paquetes. Para obtener más información, consulte "Detección de inaccesibilidad a un vecino".
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. Para obtener más información, consulte "Detección de direcciones duplicadas".
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. Para obtener más información, consulte "Función de redirección".

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.

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 vínculo, información de MTU en el vínculo y datos de redirección.

Para asegurarse de que los mensajes ND recibidos se originaron en un nodo del vínculo 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 vínculo. Con un límite de saltos de 255, un enrutador no podría reenviar el mensaje ND desde un nodo situado fuera del vínculo.

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 41.

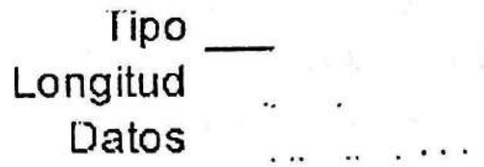


Figura 41 Formato de una opción de Neighbor Discovery (Descubrimiento de vecino)

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

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

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

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.

Opción Source/Target Link-Layer Address (Dirección de nivel de vínculo de origen y destino)

La opción Source Link-Layer Address indica la dirección de nivel de vínculo 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 vínculo de destino) indica la dirección de nivel de vínculo 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 42.

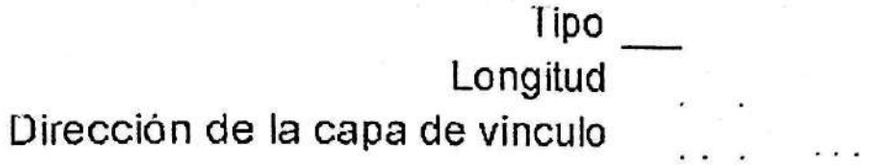


Figura 42 Formato de las opciones Source y Target Link-Layer Address (Dirección de nivel de vínculo de origen y destino)

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 vínculo) es un campo de longitud variable que contiene la dirección de nivel de vínculo del origen o del destino. Cada nivel de vínculo definido para IPv6 debe especificar el formato de la dirección de nivel de vínculo en las opciones Source y Target Link-Layer Address.

Por ejemplo, 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 vínculo tiene una longitud de 48 bits (6 bytes). En la figura 43 se muestran las opciones Source y Target Link-Layer Address para Ethernet.

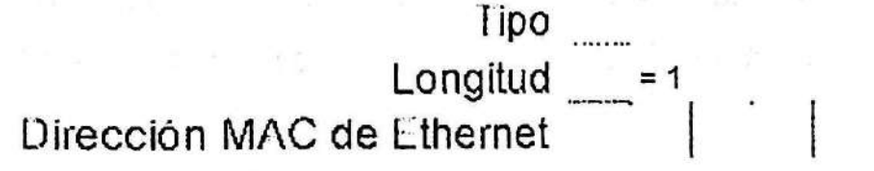


Figura 43 Formato de las opciones Source y Target Link-Layer Address (Dirección de nivel de vínculo de origen y destino) para Ethernet

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.

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 vínculo): cuando se establece en el valor 1, indica que las direcciones que implica el prefijo están disponibles en el vínculo 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 vínculo. 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 vínculo. 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 vínculo no se debe enviar y lo omite el host receptor.

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.

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.

Opción MTU

La opción MTU se envía en mensajes Router Advertisement (Anuncio de enrutador) para indicar la unidad MTU de IPv6 del vínculo. Normalmente, esta opción sólo se utiliza cuando la MTU de IPv6 para un vínculo 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 entornos con puentes o conmutados de nivel 2, pueden coexistir en el mismo segmento de red distintas tecnologías de nivel de vínculo con MTU de niveles de vínculo diferentes. En este caso, las diferencias en las unidades MTU de IPv6 entre nodos de la misma red no se detectan a través del proceso Path MTU

Discovery (Descubrimiento de MTU de ruta de acceso). La opción de MTU se utiliza para indicar la unidad MTU de IPv6 de nivel superior que admiten todas las tecnologías de nivel de vínculo en el segmento de red.
Considere la configuración conmutada que se muestra en la figura 46.

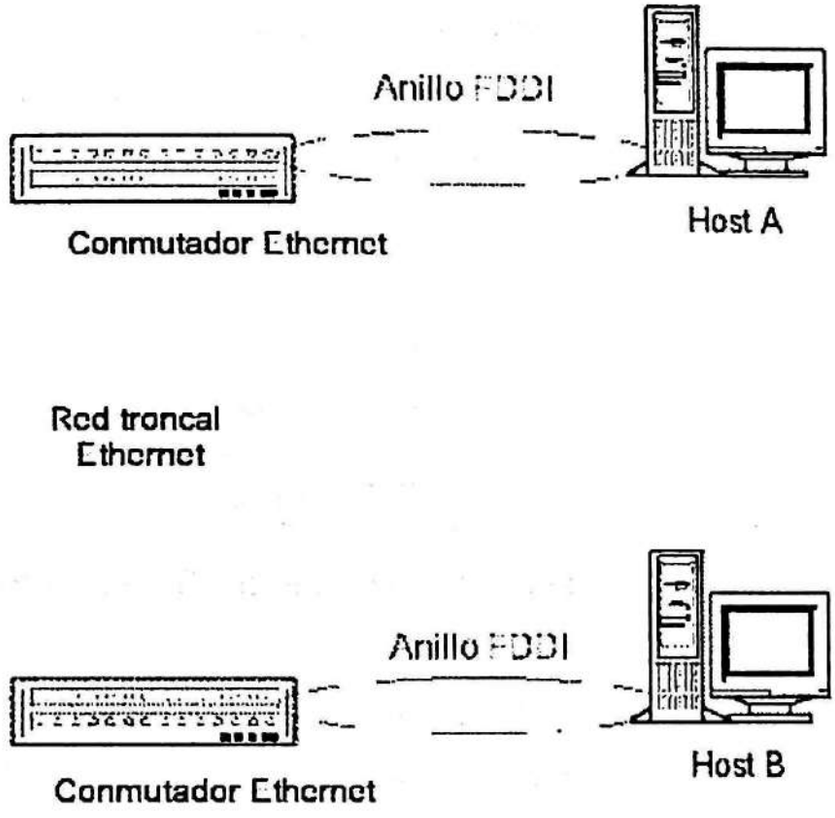


Figura 46 Entorno conmutado de nivel 2 que utiliza la opción MTU

Dos hosts IPv6, el Host A y el Host B, están conectados dos conmutadores Ethernet (de nivel 2) distintos mediante puertos de Interfaz de datos distribuidos por fibra (FDDI, *Fiber Distributed Data Interface*). Los dos conmutadores están conectados mediante una red troncal Ethernet. Cuando el Host A y el Host B negocian una conexión TCP, cada uno informa de un tamaño máximo de segmento TCP de 4.312 (la unidad MTU de nivel de vínculo FDDI de 4.352 menos 40 bytes del encabezado IPv6). Cuando se inicia el flujo de datos de TCP

en la conexión, los conmutadores descartan (sin notificarlo) los paquetes IPv6 mayores de 1.500 bytes que se envían del Host A al Host B y viceversa.
Con la opción MTU, el enrutador para el segmento de red (no mostrado) informa de una MTU de IPv6 de 1.500 en el mensaje Router Advertisement (Anuncio de enrutador) para todos los hosts del segmento de red. Cuando el Host A y el Host B ajustan sus respectivas MTU de IPv6 de 4.312 a 1.500, los datos de la conexión TCP de tamaño máximo que se transfieren no son descartados por los conmutadores intermedios.
En la figura 47 se muestra el formato de la opción MTU.

Figura 47 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 vínculo 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 vínculo.

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)

Router Solicitation (Solicitud de enrutador)

El mensaje Router Solicitation es enviado por los hosts IPv6 para descubrir los enrutadores IPv6 que hay en el vínculo. 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 vínculo 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 vínculo de todos los enrutadores (FF02::2).
- El campo Hop Limit (Límite de saltos) se establece en el valor 255.

En la figura 48 se muestra el formato del mensaje Router Solicitation.

Figura 48 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 vínculo de origen): esta opción de ND contiene la dirección de nivel de vínculo 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.

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 vínculo, la unidad MTU de vínculo, 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 vínculo 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 vínculo asignada a la interfaz de envío.

- El campo Destination Address se establece como dirección de multidifusión local de vínculo 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.

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 vínculo de origen): esta opción contiene la dirección de nivel de vínculo 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 vínculo.

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

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

Solicitud de vecino

Los hosts IPv6 envían el mensaje Neighbor Solicitation (Solicitud de vecino) para descubrir la dirección de nivel de vínculo de un nodo IPv6 en un vínculo. Incluye la dirección de nivel de vínculo 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 vínculo 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 50 se muestra el formato del mensaje Neighbor Solicitation.

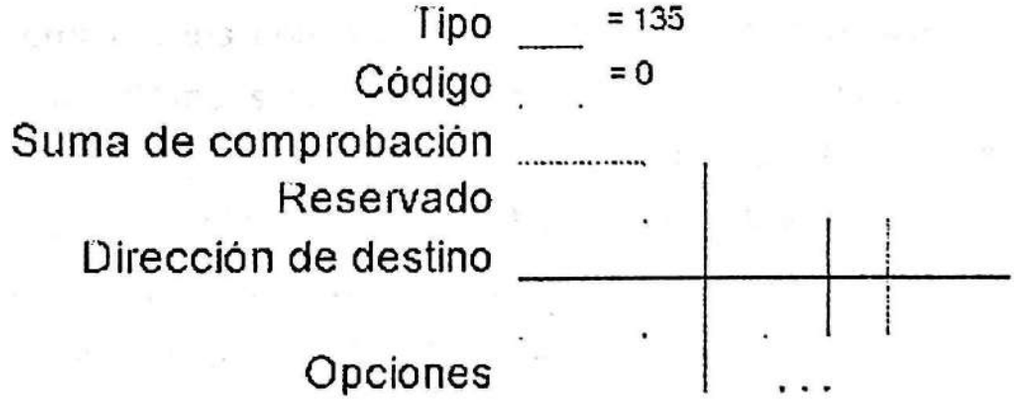


Figura 50 Formato del mensaje Neighbor Solicitation (Solicitud de vecino)

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 vínculo de origen): esta opción contiene la dirección de nivel de vínculo 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.

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 vínculo. El mensaje Neighbor Advertisement contiene información que necesitan los nodos para determinar el tipo de mensaje Neighbor Advertisement, la dirección de nivel de vínculo del remitente y la función del remitente en la red.

Por ejemplo, si el vínculo 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 vínculo de todos los nodos.

En el encabezado IPv6 del mensaje Neighbor Advertisement:

- El campo Source Address se establece en la dirección local de vínculo 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 vínculo de todos los nodos (FF02::1).
- El campo Hop Limit (Límite de saltos) se establece en el valor 255.

En la figura 51 se muestra el formato del mensaje Neighbor Advertisement.

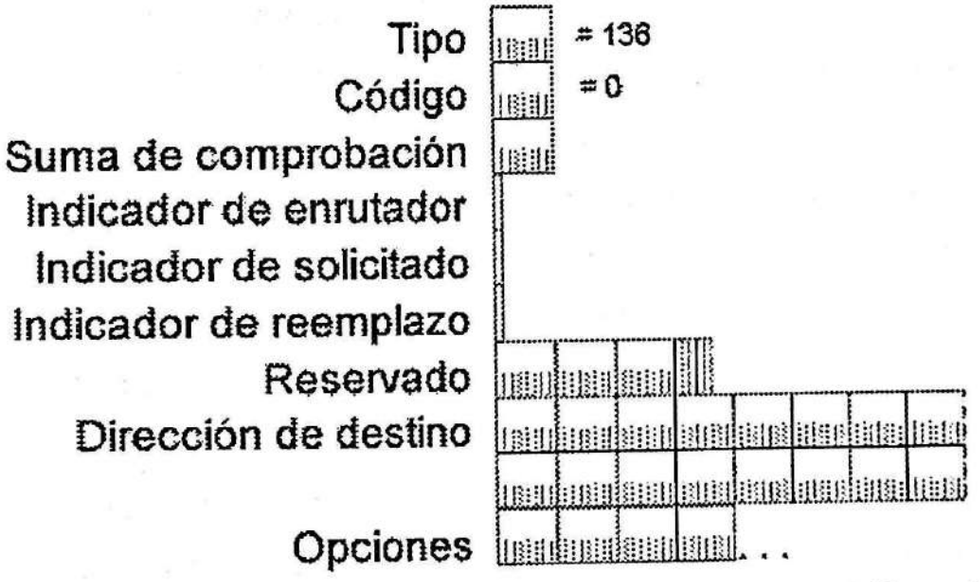


Figura 51 Formato del mensaje Neighbor Advertisement (Anuncio de vecino)

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 vínculo especificada en la opción de dirección de nivel de vínculo de destino incluida debe suplantar a la dirección de nivel de vínculo 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 vínculo que se incluye sólo actualiza una entrada de caché de vecino si no se conoce la dirección de nivel de vínculo. 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. Para obtener más información acerca de la caché de vecino, consulte "Procesos de descubrimiento de vecinos".

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 vínculo ha cambiado.

Opción Target Link-Layer Address (Dirección de nivel de vínculo de destino): esta opción contiene la dirección de nivel de vínculo 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.

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 vínculo 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 vínculo 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.

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 vínculo, el campo Target Address se establece en la dirección de vínculo local de un enrutador local. Para el tráfico del vínculo, 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 vínculo objetivo): esta opción contiene la dirección de nivel de vínculo 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.

Procesos de Neighbor Discovery (Descubrimiento de vecino)

El protocolo ND (Neighbor Discovery o Descubrimiento de vecino) proporciona intercambios de mensajes para los siguientes procesos:

- Resolución de direcciones (incluida la detección de direcciones duplicadas)
- Descubrimiento de enrutadores (incluye descubrimiento de parámetros y prefijos)
- Detección de inaccesibilidad a un vecino
- Función de redirección

Para obtener información acerca de la configuración automática de direcciones, consulte "Configuración automática de direcciones". Para obtener información acerca de la determinación del salto siguiente, consulte "Algoritmo de host de envío".

Para facilitar interacciones entre nodos vecinos, en RFC 2461 se definen las siguientes estructuras de datos de host como ejemplo de cómo se puede almacenar información para procesos ND:

- Caché de vecino

  Almacena la dirección IP de vínculo de un vecino, su dirección de nivel de vínculo correspondiente y una indicación de la posibilidad de acceso al vecino. La caché de vecino equivale a la caché de ARP en IPv4.

- Caché de destino

  Almacena información acerca de direcciones IP de salto siguiente o de reenvío para los destinos a los que se ha enviado tráfico recientemente. Las entradas de la caché de destino contienen la dirección IP de destino (local o remota), la dirección IP de salto siguiente resuelta anteriormente y la unidad MTU de ruta de acceso para el destino.

- Lista de prefijos

  Enumera los prefijos del vínculo. Cada entrada de la lista de prefijos define un intervalo de direcciones IP para destinos a los que se puede

tener acceso directo (vecinos). Esta lista se llena con prefijos anunciados por enrutadores en el mensaje Router Advertisement (Anuncio de enrutador).

- Lista de enrutadores predeterminados

  Enumera direcciones IP que corresponden a enrutadores del vínculo que envían mensajes Router Advertisement y pueden ser enrutadores predeterminados.

En RFC 2461 se definen estas estructuras de datos como ejemplo de un modelo conceptual de host IPv6. No es necesaria una implementación de IPv6 para crear estas estructuras de datos exactamente, siempre y cuando el comportamiento externo del host sea coherente con las especificaciones de RFC 2461. Por ejemplo, la implementación de IPv6 de Microsoft Research e IPv6 Technology Preview para Windows 2000 utilizan una tabla de enrutamiento en lugar de una lista de prefijos y una lista de enrutadores predeterminados.

Resolución de direcciones

El proceso de resolución de direcciones para los nodos IPv6 consiste en el intercambio de mensajes Neighbor Solicitation (Solicitud de vecino) y Neighbor Advertisement (Anuncio de vecino) para resolver la dirección de nivel de vínculo de la dirección de salto siguiente en el vínculo para un destino dado. El host remitente envía un mensaje Neighbor Solicitation de multidifusión para la interfaz apropiada. La dirección de multidifusión del mensaje Neighbor Solicitation es la dirección de multidifusión de nodo solicitado derivada de la dirección IP de destino. El mensaje Neighbor Solicitation incluye la dirección de nivel de vínculo del host de envío en la opción Source Link-Layer Address (Dirección de nivel de vínculo de origen). Para obtener información acerca de cómo determina un host la dirección de salto siguiente para un destino, consulte "Algoritmo de host de envío".

Cuando el host de destino recibe el mensaje Neighbor Solicitation, actualiza su propia caché de vecino basándose en la dirección de origen del mensaje Neighbor Solicitation y la dirección de nivel de vínculo especificada en la opción Source Link-Layer Address. A continuación, el nodo de destino envía un anuncio de vecino de unidifusión al remitente del mensaje Neighbor Solicitation. El mensaje Neighbor Advertisement incluye la opción Target Link-Layer Address (Dirección de nivel de vínculo de destino).

Después de recibir el mensaje Neighbor Advertisement del destino, el host de envío actualiza su caché de vecino con una entrada para el destino basada en la información que se especifique en la opción Target Link-Layer Address. En este momento, se puede enviar tráfico IPv6 de unidifusión entre el host de envío y el destino del mensaje Neighbor Solicitation.

Ejemplo de resolución de direcciones

El Host A tiene la dirección MAC Ethernet 00-AA-00-11-11-11 y una dirección local de vínculo correspondiente FE80::2AA:FF:FE11:1111. El Host B tiene la dirección MAC Ethernet 00-AA-00-22-22-22 y una dirección local de vínculo FE80::2AA:FF:FE22:2222. Para enviar un paquete al Host B, el Host A debe utilizar la resolución de direcciones para resolver la dirección de nivel de vínculo del Host B.

A partir de la dirección IP del Host B, el Host A envía un mensaje Neighbor Solicitation (Solicitud de vecino) multidifusión de nodo solicitado a la dirección FF02::1:FF22:2222.

El Host B, que ha registrado la dirección de multidifusión de nodo solicitado 33-33-22-22-22-22 con su adaptador Ethernet, recibe y procesa la solicitud de vecino. El Host B responde con un mensaje Neighbor Advertisement (Anuncio de vecino) de unidifusión.

Los nodos IPv4 utilizan mensajes ARP Request (Solicitud de ARP) y un método denominado ARP gratuito para detectar una dirección IP duplicada en el vínculo local. De forma similar, los nodos IPv6 utilizan el mensaje Neighbor Advertisement (Anuncio de vecino) para detectar el uso de direcciones duplicadas en el vínculo local.

Con la función ARP gratuito de IPv4, los campos Source Protocol Address (Dirección de protocolo de origen) y Target Protocol Address (Dirección de protocolo de destino) del encabezado del mensaje ARP Request se establecen en la dirección IPv4 cuya duplicación se está detectando. En la detección de direcciones duplicadas de IPv6, el campo Target Address (Dirección de destino) del mensaje Neighbor Solicitation (Solicitud de vecino) se establece en la dirección IPv6 cuya duplicación se está detectando.

La detección de direcciones duplicadas se diferencia de la resolución de direcciones en lo siguiente:

- En el mensaje Neighbor Solicitation para la detección de direcciones duplicadas, el campo Source Address (Dirección de origen) del encabezado IPv6 se establece en la dirección no especificada (::). La dirección que se consulta para determinar si hay duplicación no puede utilizarse hasta que se confirme que no hay duplicados.
- En la respuesta Neighbor Advertisement (Anuncio de vecino) a un mensaje Neighbor Solicitation (Solicitud de vecino) para la detección de direcciones duplicadas, el campo Destination Address (Dirección de destino) del encabezado IP se establece en la dirección de multidifusión de todos los nodos del ámbito local de vínculo (FF02::1). El indicador Solicited (Solicitado) del mensaje Neighbor Advertisement se establece en el valor 0. Como el remitente del mensaje Neighbor Solicitation para la detección de direcciones duplicadas no utiliza la dirección IP deseada, no puede recibir anuncios de vecino de unidifusión. Por lo tanto, el anuncio de vecino es de multidifusión.

Cuando se recibe el anuncio de vecino multidifusión con el campo Target Address (Dirección objetivo) establecido en la dirección IP para la que se detecta la duplicación, el nodo deshabilita el uso de la dirección IP duplicada en la interfaz. Si el nodo no recibe un anuncio de vecino que impida el uso de la dirección IPv6, inicializa la dirección en la interfaz.

Ejemplo de detección de dirección duplicada

El Host B tiene una dirección local de vínculo FE80::2AA:FF:FE22:2222. El Host A intenta utilizar la dirección local de vínculo FE80::2AA:FF:FE22:2222. Sin embargo, antes de que el Host A pueda utilizar esta dirección local de vínculo, debe comprobar su unicidad a través de la detección de direcciones duplicadas. El Host A envía un mensaje Neighbor Solicitation de multidifusión de nodo solicitado a la dirección FF02::1:FF22:2222.

El Host B, que ha registrado la dirección de multidifusión de nodo solicitado 33-33-22-22-22-22 con su adaptador Ethernet, recibe y procesa la solicitud de vecino. El Host B detecta que la dirección de origen es la dirección no especificada. Entonces, el Host B responde con un mensaje Neighbor Advertisement (Anuncio de vecino) de multidifusión.

Router Discovery (Descubrimiento de enrutadores)

El descubrimiento de enrutadores es el proceso mediante el cual los nodos intentan descubrir el conjunto de enrutadores del vínculo local. El descubrimiento de enrutadores en IPv6 es similar al proceso ICMP Router Discovery para IPv4, que se describe en RFC 1256.

Una diferencia importante entre el descubrimiento de enrutadores de ICMPv4 y de IPv6 es el mecanismo mediante el cual se selecciona un nuevo enrutador predeterminado cuando el actual deja de estar disponible. En el descubrimiento de enrutadores ICMPv4, el mensaje Router Advertisement incluye un campo Advertisement Lifetime (Tiempo de vida de anuncio). El tiempo de vida de anuncio es el tiempo tras el cual se puede considerar que el enrutador deja de estar disponible, cuando escucha su último mensaje Router Advertisement. En el peor de los casos, un enrutador puede dejar de estar disponible y los hosts no intentarán descubrir un nuevo enrutador predeterminado hasta que haya transcurrido el tiempo de Router Advertisement.

IPv6 tiene un campo Router Lifetime (Tiempo de vida de enrutador) en el mensaje Router Advertisement. Este campo indica el tiempo durante el cual el enrutador se puede considerar un enrutador predeterminado. Sin embargo, si el enrutador predeterminado actual deja de estar disponible, la condición se detecta a través del proceso de detección de inaccesibilidad a un vecino, en lugar de a través del campo Router Lifetime del mensaje Router Advertisement. Dado que la detección de inaccesibilidad a un vecino determina que ya no se puede tener acceso al enrutador, se elige inmediatamente un nuevo enrutador de la lista de enrutadores predeterminados. Para obtener más información, consulte "Detección de inaccesibilidad a un vecino".

Además de configurar un enrutador predeterminado, con el descubrimiento de enrutadores de IPv6 también se configura lo siguiente:

- La configuración predeterminada del campo Hop Limit (Límite de saltos) del encabezado de IPv6.
- Una determinación de si el nodo debe utilizar un protocolo de direcciones con estado, como el Protocolo de configuración dinámica de host para IPv6 (DHCPv6), para direcciones y otros parámetros de configuración.
- Los cronómetros que se utilizan en el proceso de detección de posibilidad de acceso y en la retransmisión de mensaje Neighbor Solicitation.
- La lista de prefijos de red definidos para el vínculo. Cada prefijo de red contiene el prefijo de red IPv6 y sus tiempos de vida válido y preferido. Si se indica, un prefijo de red combinado con el identificador de interfaz crea una configuración de dirección IP sin estado para la interfaz de recepción. Un prefijo de red también define el intervalo de direcciones para nodos del vínculo local.
- La unidad MTU del vínculo local.

Los procesos de descubrimiento de enrutadores IPv6 son los siguientes:

- Los enrutadores IPv6 envían periódicamente un mensaje Router Advertisement a través del vínculo local para anunciar su existencia como enrutadores. También proporcionan parámetros de configuración tales como el límite de saltos predeterminado, MTU y prefijos.
- Los hosts IPv6 activos del vínculo local reciben mensajes Router Advertisement (Anuncio de enrutador) y utilizan su contenido para el mantenimiento de la lista de enrutadores predeterminados, la lista de prefijos y otros parámetros de configuración.
- Un host que se inicia envía un mensaje Router Solicitation (Solicitud de enrutador) a la dirección de multidifusión de todos los enrutadores de ámbito local de vínculo (FF02::2). Al recibir un mensaje Router Solicitation, todos los

enrutadores del vínculo local envían un mensaje Router Advertisement unidifusión al nodo que envió la solicitud de enrutador. El nodo recibe los mensajes Router Advertisement y utiliza su contenido para crear las listas de prefijos y enrutadores predeterminados, así como para establecer otros parámetros de configuración. El número de solicitudes de enrutador enviadas antes de abandonar el proceso de descubrimiento de enrutadores se especifica mediante una variable que se puede configurar. En RFC 2461, se utiliza el nombre de variable MAX_RTR_SOLICITATIONS y se recomienda un valor de 3.

Ejemplo de descubrimiento de enrutador y prefijo

El Host A tiene la dirección MAC Ethernet 00-AA-00-11-11-11 y una dirección local de vínculo correspondiente FE80::2AA:FF:FE11:1111. El Enrutador 1 tiene la dirección MAC Ethernet 00-AA-00-22-22-22 y una dirección local de vínculo correspondiente FE80::2AA:FF:FE22:2222. Para reenviar paquetes a destinos situados fuera del vínculo, el Host A debe descubrir la presencia del Enrutador 1. El Host A envía un mensaje Router Solicitation de multidifusión a la dirección FF02::2.

El Enrutador 1, que ha registrado la dirección de multidifusión 33-33-00-00-00-02 con su adaptador Ethernet, recibe y procesa la solicitud de enrutador. El Enrutador 1 responde con un mensaje Router Advertisement (Anuncio de enrutador) de unidifusión que contiene parámetros de configuración y prefijos de vínculo local

Detección de inaccesibilidad a un vecino

La accesibilidad se define como la capacidad de enviar correctamente un paquete IPv6 al nodo vecino y que el paquete sea recibido y procesado correctamente por el nivel IPv6 del vecino. Para un nodo que envía un paquete a un enrutador, el paquete se entrega al nivel IPv6 del enrutador y, después, se reenvía al salto siguiente. Para un nodo que envía un paquete a un nodo vecino, el paquete se envía al nivel IPv6 del nodo. Es importante tener en cuenta que la definición de accesibilidad no implica la entrega en un nodo remoto a través de un enrutador, sólo al enrutador vecino.

Cuando un vecino está inaccesible, IPv6 detecta la situación e intenta corregirla. Para determinar si un vecino está accesible, IPv6 se basa en los protocolos de nivel superior que indican el progreso de la comunicación o en la recepción de un mensaje Neighbor Advertisement (Anuncio de vecino) enviado en respuesta a un mensaje Neighbor Solicitation (Solicitud de vecino) de unidifusión.

En el caso del tráfico de tipo TCP, el progreso de la comunicación se indica cuando se reciben nuevos datos o segmentos de confirmación de datos enviados. Para el tráfico de tipo UDP, puede que no haya indicación de progreso. En tal caso, el nodo envía mensajes Neighbor Solicitation (Solicitud de vecino) de unidifusión al vecino del salto siguiente para supervisar de forma continua la posibilidad de acceso al mismo.

Sólo se considera prueba de posibilidad de acceso la recepción de un mensaje Neighbor Advertisement que se ha solicitado. El mensaje Neighbor Advertisement solicitado, cuyo indicador Solicited (Solicitado) está establecido en el valor 1, sólo se envía en respuesta a un mensaje Neighbor Solicitation. Los mensajes Neighbor Advertisement o Router Advertisement (Anuncio de enrutador) no solicitados no se consideran pruebas de posibilidad de acceso.

El proceso de detección de imposibilidad de acceso a vecino permite detectar una posibilidad de acceso simétrica. En este caso, los paquetes deben ser capaces de viajar desde y hacia el nodo vecino. Cuando se envía un mensaje Neighbor Solicitation y se recibe un anuncio de vecino solicitado, se confirma la ruta de acceso entre ambos nodos. Para un mensaje Neighbor Advertisement o Router Advertisement no solicitados, sólo se confirma la ruta de acceso del nodo que envía el mensaje. Esto se denomina posibilidad de acceso asimétrica.

Para un nodo local específico, la posibilidad de acceso sólo es confirmada por el nodo que envía el mensaje Neighbor Solicitation y recibe el mensaje Neighbor Advertisement. El nodo que envía el mensaje Neighbor Advertisement no recibe ninguna confirmación de que dicho mensaje llegó al nodo previsto. Para que dos nodos vecinos determinen la posibilidad de acceso, cada uno de ellos debe

intercambiar con el otro mensajes Neighbor Solicitation y Neighbor Advertisement.

La posibilidad de acceso de un nodo vecino se determina mediante al supervisar el estado de la entrada del nodo vecino en la caché del vecino. En RFC 2461 se definen los siguientes estados para una entrada de caché de vecino:

- INCOMPLETE (Incompleto)

  Se lleva a cabo en este momento la resolución de direcciones IPv6, en la que se utiliza una solicitud de vecino multidifusión de nodo solicitado. El estado INCOMPLETE se especifica cuando se crea una nueva entrada de caché de vecino, pero aún no tiene la dirección de nivel de vínculo correspondiente del nodo. El número de mensajes Neighbor Solicitation de multidifusión que se envían antes de abandonar el proceso de resolución de direcciones y quitar la entrada de caché de vecino se especifica mediante una variable que se puede configurar. RFC 2461 utiliza el nombre de variable MAX_MULTICAST_SOLICIT y recomienda un valor de 3.

- REACHABLE (Con posibilidad de acceso)

  La posibilidad de acceso se ha confirmado al recibir un mensaje Neighbor Advertisement de unidifusión solicitado. La entrada de caché de vecino permanece en estado REACHABLE hasta que transcurre el número de milisegundos que se indica en el campo Reachable Time (Tiempo de accesible) del mensaje Router Advertisement (Anuncio de enrutador).

- STALE (Obsoleto)

  El tiempo de posibilidad de acceso (desde que se recibió la confirmación de posibilidad de acceso) ha finalizado. La entrada de caché de vecino pasa al estado STALE después de que se anule el valor (milisegundos) del campo Reachable Time y se mantiene en ese estado hasta que se

envía un paquete al vecino. El estado STALE también se especifica cuando se recibe un mensaje Neighbor Advertisement no solicitado que anuncia una dirección de nivel de vínculo.

- DELAY (Retardo)

  Para que los protocolos de nivel superior tengan tiempo de proporcionar una confirmación de posibilidad de acceso antes de enviar mensajes Neighbor Solicitation, el estado de la caché de vecino cambia a DELAY y espera durante un período de tiempo que se puede configurar. En RFC 2461 se utiliza el nombre de variable DELAY_FIRST_PROBE_TIME y se recomienda un valor de 5 segundos. Si no se recibe ninguna confirmación de posibilidad de acceso durante el tiempo de retardo, la entrada pasa al estado PROBE (Sondeo) y se envía un mensaje Neighbor Solicitation de unidifusión.

- PROBE (Sondeo)

  La confirmación de posibilidad de acceso está en progreso para una entrada de caché de vecino que se encontraba en los estados STALE y DELAY. Los mensajes Neighbor Solicitation de unidifusión se envían a intervalos que corresponden al valor especificado en el campo Retrans Timer (Cronómetro de retransmisión) en el mensaje Router Advertisement recibido por el host. El número mensajes Neighbor Solicitation que se envían antes de abandonar el proceso de detección de posibilidad de acceso y quitar la entrada de caché de vecino se especifica mediante una variable que se puede configurar. En RFC 2461, se utiliza el nombre de variable MAX_UNICAST_SOLICITS y se recomienda un valor de 3.

Si el vecino al que no se puede tener acceso es un enrutador, el host elige a otro enrutador de la lista de enrutadores predeterminados y lleva a cabo la resolución de direcciones y la detección inaccesibilidad.

Si un enrutador se convierte en host, debe enviar un mensaje Neighbor Advertisement de multidifusión con el indicador Router (Enrutador) configurado con el valor 0. Si un host recibe un mensaje Neighbor Advertisement de un enrutador en el que el indicador Router está establecido en el valor 0, el host quita el enrutador de la lista de enrutadores predeterminados y, si es necesario, elige otro enrutador.

Función de redirección

Los enrutadores utilizan la función de redirección para informar a los hosts de origen de un vecino más adecuado para el primer salto al que se debe reenviar el tráfico para un destino determinado. Existen dos casos en los que se utiliza la redirección:

1. Un enrutador informa a un host de origen de la dirección IP de un enrutador disponible en el vínculo local que se encuentra "más próximo" al destino. La "proximidad" se utiliza en el enrutamiento para alcanzar el segmento de red de destino. Esta condición puede darse cuando hay varios enrutadores en un segmento de red y el host de origen elige un enrutador predeterminado que no resulta el más apropiado para llegar al destino.
2. Un enrutador informa a un host de origen de que el destino es un vecino (se encuentra en el mismo vínculo que el host de origen). Esta condición puede darse cuando la lista de prefijos de un host no incluye el prefijo del destino. Como el destino no coincide con un prefijo de la lista, el host de origen reenvía el paquete a su enrutador predeterminado.

En el proceso de redirección IPv6 se siguen los pasos que se describen a continuación:

1. El host de origen reenvía un paquete de unidifusión a su enrutador predeterminado.
2. El enrutador procesa el paquete y detecta que la dirección del host de origen corresponde a un vecino. Además, detecta que la dirección del host de origen y del salto siguiente se encuentran en el mismo vínculo.
3. El enrutador reenvía el paquete a la dirección de salto siguiente adecuada.
4. El enrutador envía un mensaje Redirect al host de origen. En el campo Target Address (Dirección de destino) del mensaje Redirect se especifica la dirección de salto siguiente del nodo a la que el host de origen debería enviar los paquetes dirigidos al destino.

Para los paquetes que se redirigen a un enrutador, el campo Target Address se establece en la dirección local de vínculo del enrutador. Para los paquetes que se redirigen a un host, el campo Target Address se establece en la dirección de destino del paquete enviado inicialmente.

El mensaje Redirect incluye la opción Redirected Header (Encabezado de redirección). También puede incluir la opción Target Link-Layer Address (Dirección de nivel de vínculo de destino).

5. Al recibir el mensaje Redirect, el host de origen actualiza la entrada de la dirección de destino en la caché de destino con la dirección especificada en el campo Target Address. Si se incluye la opción Target Link-Layer Address en el mensaje Redirect, su contenido se emplea para crear o actualizar la entrada de caché de vecino correspondiente.

Los mensajes Redirect sólo son enviados por el primer enrutador de la ruta de acceso entre el host de origen y el destino. Los hosts nunca envían mensajes Redirect y los enrutadores nunca actualizan las tablas de enrutamiento al recibir un mensaje Redirect.

Ejemplo de redirección

El Host A tiene la dirección MAC Ethernet 00-AA-00-11-11-11 y la dirección local de vínculo correspondiente FE80::2AA:FF:FE11:1111. También tiene la dirección local de sitio FEC0::1:2AA:FF:FE11:1111/64. El Enrutador 1 tiene la dirección MAC Ethernet 00-AA-00-22-22-22 y la dirección local de vínculo correspondiente FE80::2AA:FF:FE22:2222. También tiene la dirección local de sitio FEC0::1:2AA:FF:FE22:2222/64. El Enrutador 2 tiene la dirección MAC Ethernet 00-AA-00-33-33-33 y la dirección local de vínculo correspondiente FE80::2AA:FF:FE33:3333. También tiene la dirección local de sitio FEC0::1:2AA:FF:FE33:3333/64. El Host A envía un paquete a un host situado fuera del vínculo a la dirección FEC0::2:2AA:FF:FE99:9999 (que no se muestra) y utiliza el Enrutador 1 como enrutador predeterminado. Sin embargo, el Enrutador 2 es el mejor enrutador para llegar al destino.

El Host A envía el paquete destinado a FEC0::2:2AA:FF:FE99:9999 al Enrutador 1

El Enrutador 1 recibe el paquete del Host A y detecta que el Host A es un vecino. También detecta que el Host A y la dirección de salto siguiente para el destino se encuentran en el mismo vínculo. A partir del contenido de su tabla de enrutamiento local, el Enrutador 2 reenvía el paquete de unidifusión recibido del Host 2 al Enrutador 2

Para informar al Host A de que los siguientes paquetes destinados a FEC0::2:2AA:EE:FE99:9999 se deben enviar al Enrutador 2, el Enrutador 1 envía un mensaje Redirect al Host A.

Algoritmo de envío de host

El proceso por el que un host IPv6 envía un paquete IPv6 es una combinación de las estructuras de hosts locales y del protocolo Neighbor Discovery (ND). Un host IPv6 utiliza el siguiente algoritmo cuando envía un paquete a un destino arbitrario:

1. Comprobar si en la caché de destino hay una entrada que coincide con la dirección de destino.
2. Si en la caché de destino se encuentra una entrada que coincide con la dirección de destino, obtener la dirección del salto siguiente en la entrada de caché de destino. Vaya al paso 3.

   Si en la caché de destino no se encuentra una entrada que coincida con la dirección de destino, determinar si la dirección de destino coincide con un prefijo de la lista de prefijos.

   Si la dirección de destino coincide con un prefijo de la lista, la dirección del salto siguiente se establece en la dirección de destino. Vaya al paso 3.

Si la dirección de destino no coincide con ningún prefijo de la lista, la dirección del salto siguiente se establece en la dirección del enrutador predeterminado actual. Vaya al paso 3.

Si no hay ningún enrutador predeterminado (y no hay enrutadores en la lista de enrutadores predeterminados), la dirección del salto siguiente se establece en la dirección de destino.

3. Comprobar si en la caché de vecino hay una entrada que coincide con la dirección del salto siguiente.
4. Si en la caché de vecino se encuentra una entrada que coincide con la dirección de salto siguiente, obtener la dirección de nivel de vínculo.

Si en la caché de vecino se encuentra una entrada que coincide con la dirección de salto siguiente, utilizar la resolución de direcciones para obtener la dirección de nivel de vínculo para la dirección de salto siguiente.

5. Enviar el paquete con la dirección de nivel de vínculo de la entrada de caché de vecino.

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 vínculo 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 vínculo. 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 RFC 2462.

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.

automáticamente

Nota Con excepción de una configuración automática para direcciones locales de vínculo, 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.

Tipos de configuración automática

Hay tres tipos de perfiles de configuración automática:

1. 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).

2. 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 vínculo local.

3. 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 vínculo.

Proceso de configuración automática

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

1. Se deriva una dirección local de vínculo provisional a partir del prefijo local de vínculo 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 vínculo 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 vínculo provisional.
3. Si se envía un mensaje Neighbor Advertisement en respuesta al mensaje Neighbor Solicitation que se recibió, esto indica que otro nodo del vínculo local utiliza la dirección local de vínculo 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 vínculo provisional es única y válida. Se inicializa la dirección local de vínculo

para la interfaz. La dirección de nivel de vínculo 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 vínculo) 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 vínculo 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.

Resumen

En este documento se ha tratado 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. Asimismo, se ha descrito cómo IPv6 resuelve problemas de diseño de protocolo de IPv4, los nuevos encabezados de IPv6 y de extensión, ICMPv6 (el sustituto de ICMP en IPv4), MLD (el sustituto de IGMP en IPv4), los procesos de descubrimiento de vecinos de IPv6 que administran la interacción entre nodos IPv6 vecinos y la configuración automática de direcciones IPv6. 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.

Para obtener más información

Para obtener la última información acerca de Windows 2000, visite el sitio World Wide Web en http://www.microsoft.com/latam/ntserver/nts/default.asp , el foro de Windows NT Server en MSN™ y el servicio electrónico The Microsoft Network (GO WORD: MSNTS).

Para obtener la información más reciente acerca de IPv6, consulte el sitio World Wide Web del grupo de trabajo de IPv6 en http://www.ietf.org/html.charters/ipngwg-charter.html . Este sitio contiene vínculos al conjunto actual de RFC y borradores de Internet que describen el conjunto de protocolos de IPv6.

Para obtener la información más reciente acerca del diseño de la distribución de IPv6 basada en estándares, consulte el sitio World Wide Web del grupo de trabajo Next Generation Transition (ngtrans o Transición a la siguiente generación) en http://www.ietf.org/html.charters/ngtrans-charter.html . Este sitio contiene vínculos al conjunto actual de RFC y borradores de Internet que describen varias herramientas de distribución y estrategias de transición a Internet.