UD4. Capa de Red

Índice

Protocolos de la capa de red

La capa de red, o la capa 3 de OSI, proporciona servicios que permiten que los dispositivos finales intercambien datos a través de la red. Para lograr este transporte de extremo a extremo, la capa de red utiliza cuatro procesos básicos:

1. Direccionamiento de dispositivos finales: de la misma manera en que un teléfono tiene un número telefónico único, los dispositivos finales deben configurarse con una dirección IP única para su identificación en la red. Un dispositivo final con una dirección IP configurada se denomina “host”.

2. Encapsulación: la capa de red recibe una unidad de datos del protocolo (PDU) de la capa de transporte. En un proceso denominado “encapsulación”, la capa de red agrega la información del encabezado IP, como la dirección IP de los hosts de origen (emisor) y de destino (receptor). Una vez que se agrega la información de encabezado a la PDU, esta se denomina “paquete”.

3. Enrutamiento: la capa de red proporciona servicios para dirigir los paquetes a un host de destino en otra red. Para que el paquete se transfiera a otras redes, lo debe procesar un router. La función del router es seleccionar las rutas para los paquetes y dirigirlos hacia el host de destino en un proceso conocido como “enrutamiento”. Un paquete puede cruzar muchos dispositivos intermediarios antes de llegar al host de destino. Cada ruta que toma el paquete para llegar al host de destino se denomina “salto”.

4. Desencapsulación: cuando un paquete llega a la capa de red del host de destino, el host revisa el encabezado IP del paquete. Si la dirección IP de destino en el encabezado coincide con su propia dirección IP, se elimina el encabezado IP del paquete. Este proceso de eliminación de encabezados de las capas inferiores se conoce como “desencapsulación”. Una vez que la capa de red desencapsula el paquete, la PDU de capa 4 que se obtiene como resultado se transfiere al servicio correspondiente en la capa de transporte.

A diferencia de la capa de transporte (capa 4 de OSI), que administra el transporte de datos entre los procesos que se ejecutan en cada host, los protocolos de la capa de red especifican la estructura y el procesamiento de paquete que se utilizan para transportar los datos desde un host hasta otro. Operar sin tener en cuenta los datos transportados en cada paquete permite que la capa de red transporte paquetes para diversos tipos de comunicaciones entre varios hosts.

El protocolo IP

El protocolo IP es el servicio de capa de red implementado por la suite de protocolos TCP/IP.

IP se diseñó como protocolo con baja sobrecarga. Provee sólo las funciones necesarias para enviar un paquete desde un origen a un destino a través de un sistema interconectado de redes. El protocolo no fue diseñado para rastrear ni administrar el flujo de paquetes. De ser necesarias, otros protocolos en otras capas llevan a cabo estas funciones.

Las características básicas del protocolo IP son las siguientes:

Sin conexión: no se establece ninguna conexión con el destino antes de enviar los paquetes de datos.

No confiable: la entrega de paquetes no está garantizada.

Independiente de los medios: la operación es independiente del medio que transporta los datos.

El protocolo IP encapsula o empaqueta el segmento de la capa de transporte agregando un encabezado IP. Este encabezado se utiliza para entregar el paquete al host de destino. El encabezado IP permanece en su lugar desde el momento en que el paquete abandona la capa de red del host de origen hasta que llega a la capa de red del host de destino.

El proceso de encapsulación de datos capa por capa permite el desarrollo y el escalamiento de los servicios de las diferentes capas sin afectar otras capas. Esto significa que el protocolo IPv4 o IPv6, o cualquier protocolo nuevo que se desarrolle en el futuro, pueden empaquetar fácilmente los segmentos de la capa de transporte.

Los routers pueden implementar estos diferentes protocolos de capa de red para operar al mismo tiempo en una red desde y hacia el mismo host o hosts diferentes. El enrutamiento que realizan estos dispositivos intermediarios solo tiene en cuenta el contenido del encabezado del paquete que encapsula el segmento. En todos los casos, la porción de datos del paquete, es decir, la PDU de la capa de transporte encapsulada, no se modifica durante los procesos de la capa de red.

Paquete IPv4

Los paquetes IPV4 tienen dos partes:

Encabezado IP: identifica las características del paquete.

Contenido: contiene la información del segmento de capa 4 y los datos propiamente dichos.

Los encabezados de paquetes IPV4 constan de campos que contienen información importante sobre el paquete. Estos campos contienen números binarios que se examinan en el proceso de capa 3. Los valores binarios de cada campo identifican las distintas configuraciones del paquete IP.

Los campos importantes del encabezado de IPv4 incluyen los siguientes:

Versión: contiene un valor binario de 4 bits que identifica la versión del paquete IP. Para los paquetes IPv4, este campo siempre se establece en 0100.

Servicios diferenciados (DS): anteriormente denominado “Tipo de servicio” (ToS), se trata de un campo de 8 bits que se utiliza para determinar la prioridad de cada paquete. Los primeros 6 bits

identifican el valor del Punto de código de servicios diferenciados (DSCP), utilizado por un mecanismo de calidad de servicio (QoS). Los últimos 2 bits identifican el valor de Notificación explícita de congestión (ECN), que se puede utilizar para evitar que los paquetes se descarten durante momentos de congestión de la red.

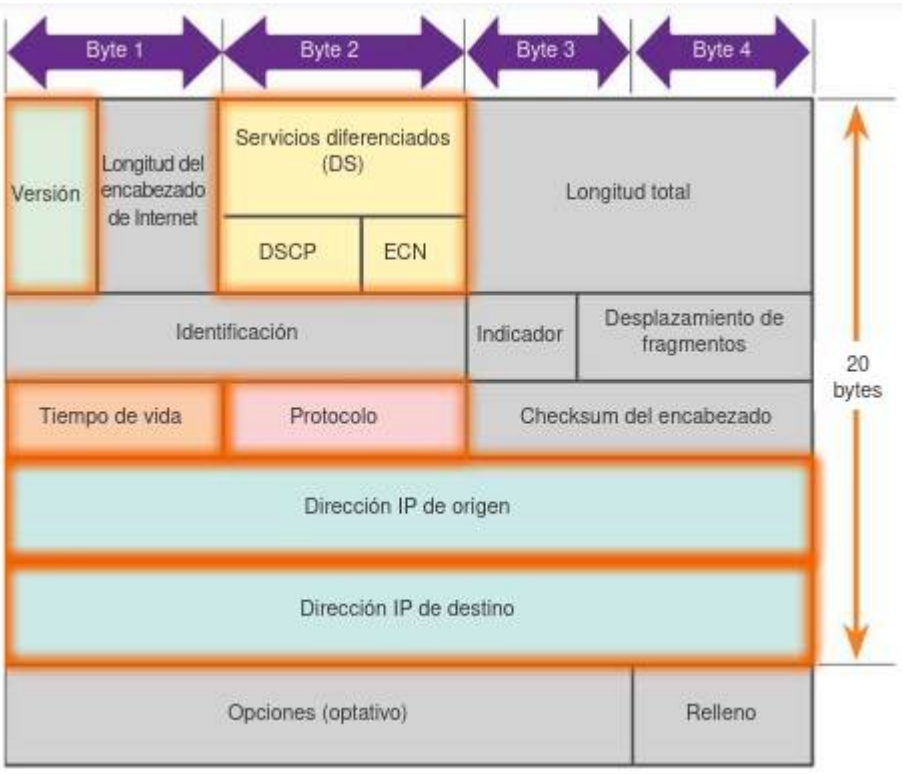
Tiempo de vida (TTL): contiene un valor binario de 8 bits que se utiliza para limitar la vida útil de un paquete. Se especifica en segundos, pero comúnmente se denomina “conteo de saltos”. El emisor del paquete establece el valor inicial de tiempo de vida (TTL), el que disminuye un punto por cada salto, es decir, cada vez que el paquete es procesado por un router. Si el campo TTL disminuye a cero, el router descarta el paquete y envía un mensaje del protocolo de mensajes de control de Internet (ICMP) de Tiempo superado a la dirección IP de origen. El comando traceroute utiliza este campo para identificar los routers utilizados entre el origen y el destino.

Protocolo: este valor binario de 8 bits indica el tipo de contenido de datos que transporta el paquete, lo que permite que la capa de red pase los datos al protocolo de capa superior correspondiente. Los valores comunes incluyen ICMP (1), TCP (6) y UDP (17).

Dirección IP de origen: contiene un valor binario de 32 bits que representa la dirección IP de origen del paquete.

Dirección IP de destino: contiene un valor binario de 32 bits que representa la dirección IP de destino del paquete.

Los dos campos que más comúnmente se toman como referencia son las direcciones IP de origen y de destino. Estos campos identifican de dónde proviene el paquete y adónde va. Por lo general, estas direcciones no se modifican durante la transferencia desde el origen hasta el destino.



Los campos restantes se utilizan para identificar y validar el paquete, o para volver a ordenar un paquete fragmentado.

Longitud del encabezado de Internet (IHL): contiene un valor binario de 4 bits que identifica la cantidad de palabras de 32 bits en el encabezado. El valor de IHL varía según los campos Opciones y Relleno. El valor mínimo para este campo es 5 (es decir, 5×32 = 160 bits = 20 bytes), y el valor máximo es 15 (es decir, 15×32 = 480 bits = 60 bytes).

Longitud total: en ocasiones denominado “Longitud del paquete”, este campo de 16 bits define el tamaño total del paquete (fragmento), incluidos el encabezado y los datos, en bytes. La longitud mínima de paquete es de 20 bytes (encabezado de 20 bytes + datos de 0 bytes), y la máxima es de 65 535 bytes.

Checksum del encabezado: este campo de 16 bits se utiliza para la verificación de errores del encabezado IP. El checksum del encabezado se vuelve a calcular y se compara con el valor en el campo checksum. Si los valores no coinciden, se descarta el paquete.

Es posible que un router deba fragmentar un paquete cuando lo reenvía de un medio a otro que tiene una MTU más pequeña. Cuando esto sucede, se produce una fragmentación, y el paquete IPV4 utiliza los siguientes campos para llevar a cabo un seguimiento de los fragmentos:

Identificación: este campo de 16 bits identifica de forma exclusiva el fragmento de un paquete IP original.

Indicadores: este campo de 3 bits identifica cómo se fragmenta el paquete. Se utiliza con los campos Desplazamiento de fragmentos e Identificación para ayudar a reconstruir el paquete original con el fragmento.

Desplazamiento de fragmentos: este campo de 13 bits identifica el orden en que se debe colocar el fragmento del paquete en la reconstrucción del paquete original sin fragmentar.

Paquete de IPv6

A través de los años, IPv4 se actualizó para enfrentar nuevos desafíos. Sin embargo, incluso con los cambios, IPv4 continúa teniendo tres problemas importantes:

Agotamiento de direcciones IP: IPv4 dispone de una cantidad limitada de direcciones IP públicas exclusivas. Si bien existen aproximadamente 4000 millones de direcciones IPv4, la cantidad creciente de dispositivos nuevos con IP habilitado, las conexiones permanentes y el crecimiento potencial de las regiones menos desarrolladas aumentan la necesidad de más direcciones.

Expansión de la tabla de enrutamiento de Internet: los routers utilizan tablas de enrutamiento para determinar cuál es el mejor camino. A medida que aumenta la cantidad de servidores (nodos) conectados a Internet, también lo hace la cantidad de rutas de la red. Estas rutas IPv4 consumen muchos recursos de memoria y del procesador en los routers de Internet.

Falta de conectividad de extremo a extremo: la traducción de direcciones de red (NAT) es una tecnología de implementación frecuente en las redes IPv4. La tecnología NAT proporciona una forma de que varios dispositivos compartan una misma dirección IP pública. Sin embargo, dado que comparten la dirección IP pública, la dirección IP de un host de red interno se oculta. Esto puede resultar problemático para las tecnologías que requieren conectividad de extremo a extremo.

A principios de los años noventa, el Internet Engineering Task Force (IETF) comenzó a preocuparse por los problemas de IPv4 y empezó a buscar un reemplazo. Esta actividad condujo al desarrollo de IP versión 6 (IPv6). IPv6 supera las limitaciones de IPv4 y constituye una mejora eficaz con características que se adaptan mejor a las demandas actuales y previsibles de las redes.

Las mejoras que proporciona IPv6 incluyen lo siguiente:

Mayor espacio de direcciones: las direcciones IPv6 se basan en un direccionamiento jerárquico de 128 bits, mientras que en IPv4 es de 32 bits. El número de direcciones IP disponibles aumenta drásticamente.

Mejora del manejo de los paquetes: el encabezado de IPv6 se simplificó con menos campos. Esto mejora el manejo de paquetes por parte de los routers intermediarios y también proporciona compatibilidad para extensiones y opciones para aumentar la escalabilidad y la duración.

Eliminación de la necesidad de NAT: con tal cantidad de direcciones IPv6 públicas, no se necesita traducción de direcciones de red (NAT). Los sitios de los clientes, ya sean las empresas más grandes o unidades domésticas, pueden obtener una dirección de red IPv6 pública. Esto evita algunos de los problemas de aplicaciones debidos a NAT que afectan a las aplicaciones que requieren conectividad de extremo a extremo.

Seguridad integrada: IPv6 admite capacidades de autenticación y privacidad de forma nativa. Con IPv4, se debían implementar características adicionales para este fin.

El espacio de direcciones IPv4 de 32 bits proporciona aproximadamente 4 294 967 296 direcciones únicas. De estas, solo 3700 millones de direcciones se pueden asignar, porque el sistema de direccionamiento IPv4 separa las direcciones en clases y reserva direcciones para multicast, pruebas y otros usos específicos.

Como se muestra en la ilustración, el espacio de direcciones IP versión 6 proporciona 340 282 366 920 938 463 463 374 607 431 768 211 456, o 340 sextillones de direcciones, lo que equivale a aproximadamente todos los granos de arena de la Tierra.

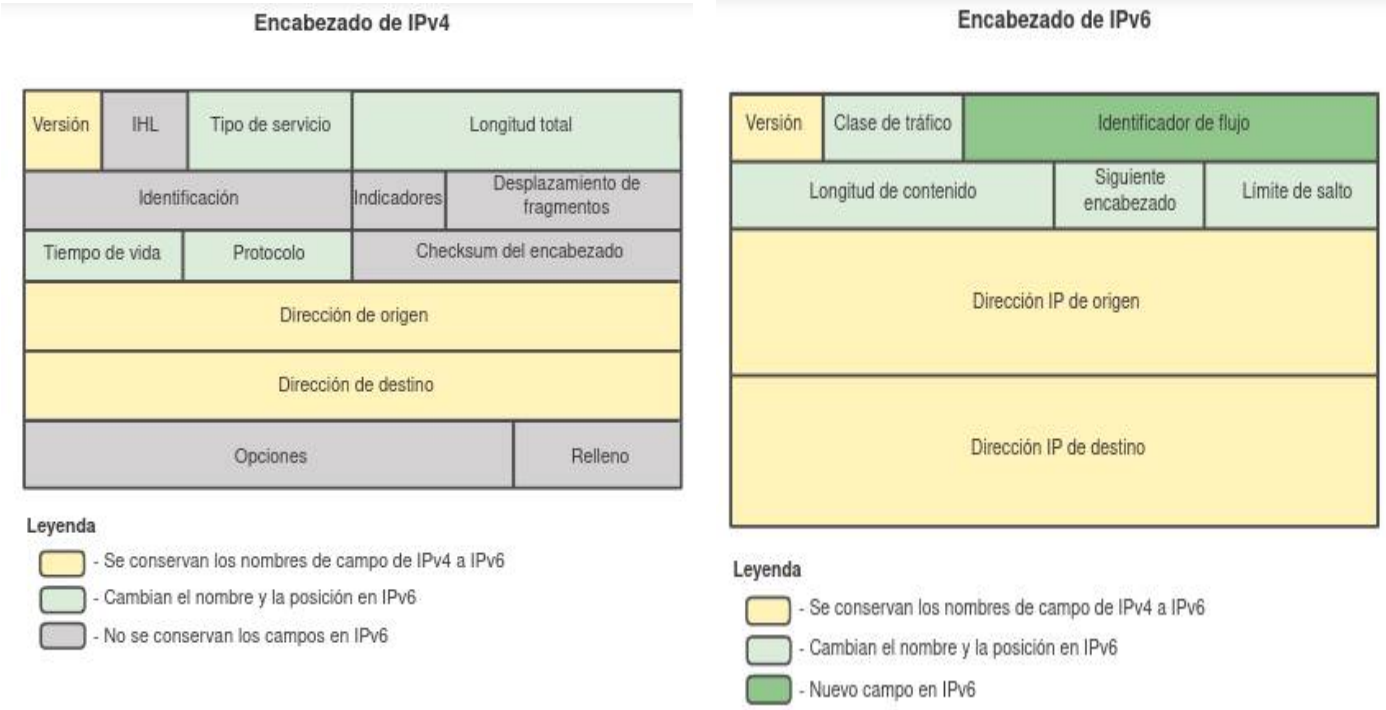
Una de las principales mejoras de diseño de IPv6 con respecto a IPv4 es el encabezado de IPv6 simplificado.

El encabezado de IPv4 consta de 20 octetos (hasta 60 bytes si se utiliza el campo Opciones) y 12 campos de encabezado básicos, sin incluir los campos Opciones y Relleno.

El encabezado de IPv6 consta de 40 octetos (en gran medida, debido a la longitud de las direcciones IPv6 de origen y de destino) y 8 campos de encabezado (3 campos de encabezado IPv4 básicos y 5 campos de encabezado adicionales).

Como se muestra en la ilustración, en IPv6 algunos campos permanecen iguales, algunos campos del encabezado de IPv4 no se utilizan, y algunos campos tienen nombres y posiciones diferentes.

Además, se agregó un nuevo campo a IPv6 que no se utiliza en Ipv4.



El encabezado de IPv6 simplificado ofrece varias ventajas respecto de IPv4:

Mayor eficacia de enrutamiento para un buen rendimiento y una buena escalabilidad de velocidad de reenvío.

Sin requisito de procesamiento de checksums.

Mecanismos de encabezado de extensión simplificados y más eficaces (en comparación con el campo Opciones de Ipv4).

Campos de IPv6

Versión: este campo contiene un valor binario de 4 bits que identifica la versión del paquete IP. Para los paquetes IPv6, este campo siempre se establece en 0110.

Clase de tráfico: este campo de 8 bits equivale al campo Servicios diferenciados (DS) de IPv4. También contiene un valor de Punto de código de servicios diferenciados (DSCP) de 6 bits utilizado para clasificar paquetes y un valor de Notificación explícita de congestión (ECN) de 2 bits utilizado para controlar la congestión del tráfico.

Identificador de flujo: este campo de 20 bits proporciona un servicio especial para aplicaciones en tiempo real. Se puede utilizar para indicar a los routers y switches que deben mantener la misma ruta para el flujo de paquetes, a fin de evitar que estos se reordenen.

Longitud de contenido: este campo de 16 bits equivale al campo Longitud total del encabezado de IPv4. Define el tamaño total del paquete (fragmento), incluidos el encabezado y las extensiones optativas.

Siguiente encabezado: este campo de 8 bits equivale al campo Protocolo de IPv4. Indica el tipo de contenido de datos que transporta el paquete, lo que permite que la capa de red pase los datos al protocolo de capa superior correspondiente. Este campo también se usa si se agregan encabezados de extensión optativos al paquete IPv6.

Límite de saltos: este campo de 8 bits reemplaza al campo TTL de IPv4. Cuando cada router reenvía un paquete, este valor disminuye en un punto. Cuando el contador llega a 0, el paquete se descarta y se reenvía un mensaje de ICMPv6 al host emisor en el que se indica que el paquete no llegó a destino.

Dirección de origen: este campo de 128 bits identifica la dirección IPv6 del host emisor.

Dirección de destino: este campo de 128 bits identifica la dirección IPv6 del host receptor.

Los paquetes IPv6 también pueden contener encabezados de extensión (EH), que proporcionan información optativa de la capa de red. Los encabezados de extensión son optativos y se colocan entre el encabezado de IPv6 y el contenido. Los EH se utilizan para realizar la fragmentación, aportar seguridad, admitir la movilidad, y más.

Direccionamiento IP

Estructura de la dirección IPv4

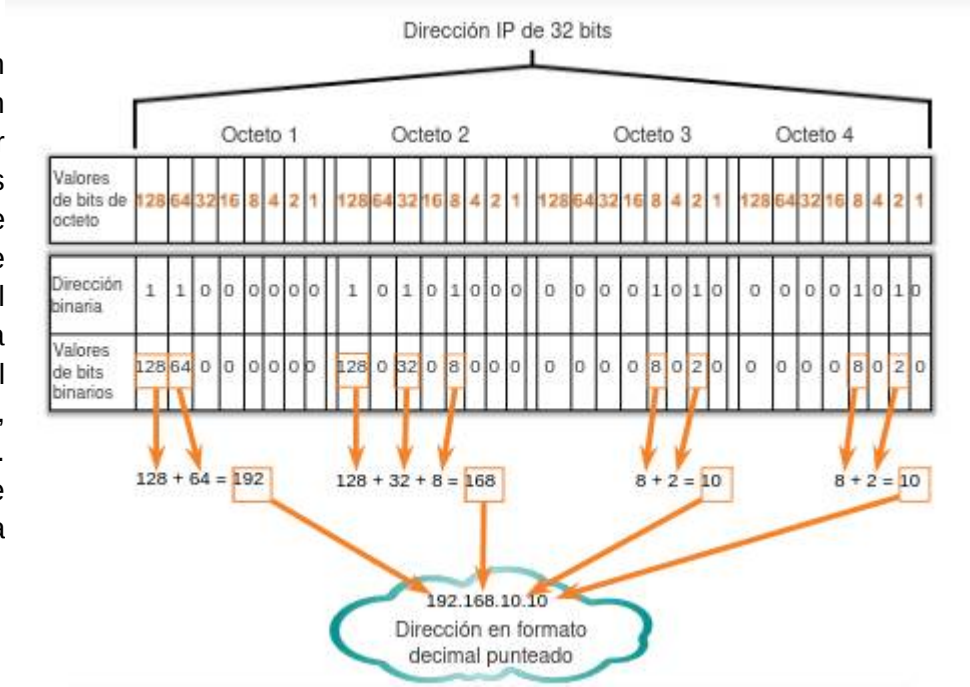
Para comprender el funcionamiento de los dispositivos en una red, debemos observar las direcciones y otros datos de la misma manera en que lo hacen los dispositivos: en notación binaria. La notación binaria es una representación de la información mediante unos y ceros solamente. Las PC se comunican mediante datos binarios. Los datos binarios se pueden utilizar para representar muchas formas distintas de datos. Por ejemplo, al pulsar letras en un teclado, esas letras aparecen en la pantalla de una manera que el usuario puede leer y comprender. Sin embargo, la PC traduce cada letra a una serie de dígitos binarios para su almacenamiento y transporte. Para traducir esas letras, la PC utiliza el Código Estadounidense Estándar para el Intercambio de Información (ASCII).

Mediante ASCII, la letra “A” se representa en forma de bit como “01000001”, mientras que la “a” minúscula se representa en forma de bit como “01100001”.

Si bien, por lo general, las personas no deben preocuparse por la conversión binaria de letras, es necesario comprender el uso del sistema binario para el direccionamiento IP. Cada dispositivo en una red se debe identificar de forma exclusiva mediante una dirección binaria. En redes IPv4, esta dirección se representa mediante una cadena de 32 bits (unos y ceros). A continuación, en la capa de red, los paquetes incluyen esta información de identificación única para los sistemas de origen y de destino. Por lo tanto, en una red IPv4, cada paquete incluye una dirección de origen de 32 bits y una dirección de destino de 32 bits en el encabezado de capa 3.

Para la mayoría de las personas, una cadena de 32 bits es difícil de interpretar e incluso más difícil de recordar. Por este motivo, representamos las direcciones IPv4 mediante el formato decimal punteado en lugar del binario. Esto significa que vemos a cada byte (octeto) como número decimal en el rango de 0 a 255. Para entender cómo funciona esto, es necesario tener aptitudes para la conversión de sistema binario a decimal.

En IPv4, las direcciones son números binarios de 32 bits. Sin embargo, para facilitar el uso por parte de las personas, los patrones binarios que representan direcciones IPv4 se expresan en formato decimal punteado. Esto primero se logra separando cada byte (8 bits) del patrón binario de 32 bits, llamado “octeto”, con un punto. Se le llama octeto debido a que cada número decimal representa un byte u 8 bits.



Máscara de subred IPv4

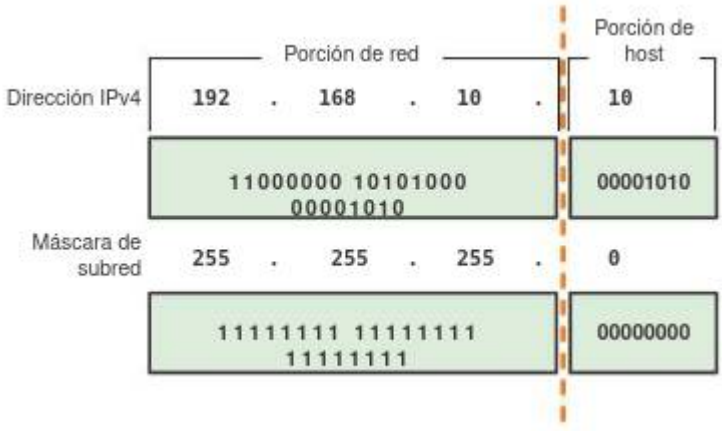
Es importante entender la notación binaria para determinar si dos hosts están en la misma red. Recuerde que una dirección IP es una dirección jerárquica que consta de dos partes: una porción de red y una porción de host. Pero al determinar la porción de red en comparación con la porción de host, es necesario analizar el stream de 32 bits, y no el valor decimal. Dentro del stream de 32 bits, una parte de los bits constituye la red y una porción de los bits constituye el host.

Los bits dentro de la porción de red de la dirección deben ser idénticos para todos los dispositivos que residen en la misma red. Los bits dentro de la porción de host de la dirección deben ser únicos para identificar un host específico dentro de una red. Independientemente de si los números decimales entre dos direcciones IPv4 coinciden, si dos hosts tienen el mismo patrón de bits en la porción de red especificada del stream de 32 bits, esos dos hosts residen en la misma red.

¿Pero cómo saben los hosts qué porción de los 32 bits es red y qué porción es host? Esa tarea le corresponde a la máscara de subred.

Cuando se configura un host IP, se asigna una máscara de subred junto con una dirección IP. Como sucede con la dirección IP, la máscara de subred tiene una longitud de 32 bits. La máscara de subred identifica qué parte de la dirección IP corresponde a la red y cuál al host.

La máscara de subred se compara con la dirección IP, de izquierda a derecha, bit por bit. Los 1 en la máscara de subred representan la porción de red, los 0 representan la porción de host. Como se muestra en la figura 1, la máscara de subred se crea al colocar un 1 binario en cada posición de bit que representa la porción de red y un 0 binario en cada posición de bit que representa la porción de host. Se debe tener en cuenta que la máscara de subred no contiene en efecto la porción de red o de host de una dirección IPv4, sino que simplemente le dice a la PC dónde buscar estas porciones en una dirección IPv4 dada.



Como sucede con las direcciones IPv4, la máscara de subred se representa en formato decimal punteado por cuestiones de facilidad de uso. La máscara de subred se configura en un dispositivo host, junto con la dirección IPv4, y es necesaria para que el host pueda determinar a qué red pertenece.

Valor de subred	Valor de bit							
	128	64	32	16	8	4	2	1
255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

Prefijos de red

El prefijo es otra forma de expresar la máscara de subred. Es la cantidad de bits establecidos en 1 en la máscara de subred. Se escribe con una barra “/” seguida de la cantidad de bits a 1. Por ejemplo, si la máscara de subred es 255.255.255.0, hay 24 bits establecidos en 1 en la versión binaria de la máscara de subred, de modo que el prefijo es 24 bits o /24.

	Decimal punteada	Bits importantes mostrados en sistema binario
Dirección de red	10.1.1.0/24	10.1.1.00000000
Primera dirección de host	10.1.1.1	10.1.1.00000001
Última dirección de host	10.1.1.254	10.1.1.11111110
Dirección de broadcast	10.1.1.255	10.1.1.11111111

Dirección de red	10.1.1.0/25	10.1.1.00000000
Primera dirección de host	10.1.1.1	10.1.1.00000001
Última dirección de host	10.1.1.126	10.1.1.01111110
Dirección de broadcast	10.1.1.127	10.1.1.01111111
Cantidad de hosts: 2^7 – 2 = 126 hosts		

Dirección de red	10.1.1.0/26	10.1.1.00000000
Primera dirección de host	10.1.1.1	10.1.1.00000001
Última dirección de host	10.1.1.62	10.1.1.00111110
Dirección de broadcast	10.1.1.63	10.1.1.00111111
Cantidad de hosts: 2^6 – 2 = 62 hosts		

	Decimal punteada	Bits importantes mostrados en sistema binario
Dirección de red	10.1.1.0/27	10.1.1.00000000
Primera dirección de host	10.1.1.1	10.1.1.00000001
Última dirección de host	10.1.1.30	10.1.1.00011110
Dirección de broadcast	10.1.1.31	10.1.1.00011111
Cantidad de hosts: 2^5 – 2 = 30 hosts		

Dirección de red	10.1.1.0/28	10.1.1.00000000
Primera dirección de host	10.1.1.1	10.1.1.00000001
Última dirección de host	10.1.1.14	10.1.1.00001110
Dirección de broadcast	10.1.1.15	10.1.1.00001111
Cantidad de hosts: 2^4 – 2 = 14 hosts		

La dirección de red es una manera estándar de hacer referencia a una red. Al referirse a la dirección de red, también es posible utilizar la máscara de subred o la duración de prefijo. Por ejemplo, la red que se muestra en la figura 1 podría indicarse como la red 10.1.1.0, la red 10.1.1.0 255.255.255.0 o la red 10.1.1.0/24. Todos los hosts en la red 10.1.1.0/24 tendrán los mismos bits de porción de red.

Dentro del rango de direcciones IPv4 de una red, la primera dirección se reserva para la dirección de red. Esta dirección tiene un 0 para cada bit de host en la porción de host de la dirección. Todos los hosts dentro de la red comparten la misma dirección de red.

La dirección de broadcast IPv4 es una dirección especial para cada red que permite la comunicación a todos los host en esa red. Para enviar datos a todos los hosts en una red a la vez, un host puede enviar un único paquete dirigido a la dirección de broadcast de la red, y cada host en la red que recibe este paquete procesa su contenido.

La dirección de broadcast utiliza la dirección más alta en el rango de la red. Ésta es la dirección en la cual los bits de la porción de host son todos 1. Todos 1 en un octeto en forma binaria es igual al número 255 en forma decimal. Por lo tanto, como se muestra en la figura 4, para la red 10.1.1.0/24, en la cual se utiliza el último octeto para la porción de host, la dirección de broadcast sería 10.1.1.255. Observe que la porción de host no siempre es un octeto entero. A esta dirección se la conoce como broadcast dirigido.

Para asegurarse de que a todos los hosts en una red se les asigne una dirección IP única dentro de ese rango de red, es importante identificar la primera y la última dirección de host. Se pueden asignar direcciones IP dentro de este rango a los hosts dentro de una red.

La porción de host de la **primera dirección de host** contiene todos bits 0 con un bit 1 que representa el bit de orden más bajo o el bit que está más a la derecha. Esta dirección es siempre un número mayor que la dirección de red. En este ejemplo, la primera dirección de host en la red 10.1.1.0/24 es 10.1.1.1. En muchos esquemas de direccionamiento, es común utilizar la primera dirección de host del router o la dirección de gateway predeterminado.

La porción de host de la **última dirección de host** contiene todos bits 1, con un bit 0 que representa el bit de orden más bajo o el bit que está más a la derecha. Esta dirección es siempre una menos que la dirección de broadcast. Por ejemplo la última dirección de host en la red 10.1.1.0/24 es 10.1.1.254.

La transmisión de **multicast** reduce el tráfico al permitir que un host envíe un único paquete a un conjunto seleccionado de hosts que forman parte de un grupo multicast suscrito. Para alcanzar hosts de destino múltiples mediante la comunicación unicast, sería necesario que el host de origen envíe un

paquete individual dirigido a cada host. Con multicast, el host de origen puede enviar un único paquete que llegue a miles de hosts de destino. La responsabilidad de la internetwork es reproducir los flujos multicast en un modo eficaz para que alcancen solamente a los destinatarios.

IPv4 tiene un bloque de direcciones reservadas para direccionar grupos multicast. Este rango de direcciones va de 224.0.0.0 a 239.255.255.255. El rango de direcciones multicast está subdividido en distintos tipos de direcciones: direcciones de enlace local reservadas y direcciones agrupadas globalmente. Un tipo adicional de dirección multicast son las direcciones agrupadas administrativamente, también llamadas direcciones de agrupamiento limitado.

Las direcciones IPv4 multicast de 224.0.0.0 a 224.0.0.255 son direcciones de enlace local reservadas. Estas direcciones se utilizarán con grupos multicast en una red local. Un router conectado a la red local reconoce que estos paquetes están dirigidos a un grupo multicast de enlace local y nunca los reenvía nuevamente. Un uso común de las direcciones de link-local reservadas se da en los protocolos de enrutamiento usando transmisión multicast para intercambiar información de enrutamiento.

Las direcciones agrupadas globalmente son de 224.0.1.0 a 238.255.255.255. Se les puede usar para transmitir datos en Internet mediante multicast. Por ejemplo, se reservó 224.0.1.1 para que el protocolo de hora de red (NTP) sincronice los relojes con la hora del día de los dispositivos de red.

Los hosts que reciben datos multicast específicos se denominan “clientes multicast”. Los clientes multicast utilizan servicios solicitados por un programa cliente para subscribirse al grupo multicast.

Cada grupo multicast está representado por una sola dirección IPv4 de destino multicast. Cuando un host IPv4 se suscribe a un grupo multicast, el host procesa paquetes dirigidos a esta dirección multicast y paquetes dirigidos a su dirección unicast asignada exclusivamente.

Direcciones públicas y privadas

Aunque la mayoría de las direcciones IPv4 de host son direcciones públicas designadas para uso en redes a las que se accede desde Internet, existen bloques de direcciones que se utilizan en redes que requieren o no acceso limitado a Internet. Estas direcciones se denominan direcciones privadas.

10.0.0.0 a 10.255.255.255 (10.0.0.0/8)

172.16.0.0 a 172.31.255.255 (172.16.0.0/12)

192.168.0.0 a 192.168.255.255 (192.168.0.0/16)

Las direcciones privadas se definen en RFC 1918, Asignación de direcciones para redes de Internet privadas, y en ocasiones se hace referencia a ellas como direcciones RFC 1918. Los bloques de direcciones de espacio privado se utilizan en redes privadas. Los hosts que no requieren acceso a Internet pueden utilizar direcciones privadas. Sin embargo, dentro de la red privada, los hosts aún requieren direcciones IP únicas dentro del espacio privado.

Hosts en distintas redes pueden utilizar las mismas direcciones de espacio privado. Los paquetes que utilizan estas direcciones como la dirección de origen o de destino no deberían aparecer en la Internet pública. El router o el dispositivo de firewall del perímetro de estas redes privadas deben bloquear o convertir estas direcciones. Incluso si estos paquetes fueran a llegar hasta Internet, los routers no tendrían rutas para reenviarlos a la red privada correcta.

En RFC 6598, IANA reservó otro grupo de direcciones conocidas como “espacio de dirección compartido”. No son enrutables globalmente y el propósito de estas direcciones es ser utilizadas en redes de proveedores de servicios. El bloque de direcciones compartido es 100.64.0.0/10.

La amplia mayoría de las direcciones en el rango de host unicast IPv4 son direcciones públicas. Estas direcciones están diseñadas para ser utilizadas en los hosts de acceso público desde Internet. Aun dentro de estos bloques de direcciones IPv4, existen muchas direcciones designadas para otros fines específicos.

Direcciones especiales

Existen determinadas direcciones que no pueden asignarse a los hosts. También hay direcciones especiales que pueden asignarse a los hosts, pero con restricciones respecto de la forma en que dichos hosts pueden interactuar dentro de la red.

Como se explicó anteriormente, no es posible asignar la primera ni la última dirección a hosts dentro de cada red. Éstas son, respectivamente, la dirección de red y la dirección de broadcast.

Una de estas direcciones reservadas es la dirección de loopback IPv4 127.0.0.1. La dirección de loopback es una dirección especial que los hosts utilizan para dirigir el tráfico hacia ellos mismos. La dirección de loopback crea un método de acceso directo para las aplicaciones y servicios TCP/IP que se ejecutan en el mismo dispositivo para comunicarse entre sí. Al utilizar la dirección de loopback en lugar de la dirección host IPv4 asignada, dos servicios en el mismo host pueden desviar las capas inferiores del stack de TCP/IP. También es posible hacer ping a la dirección de loopback para probar la configuración de TCP/IP en el host local.

A pesar de que sólo se usa la dirección única 127.0.0.1, se reservan las direcciones 127.0.0.0 a 127.255.255.255. Cualquier dirección dentro de este bloque producirá un loop back al host local. Las direcciones dentro de este bloque no deben figurar en ninguna red.

Las direcciones IPv4 del bloque de direcciones que va de **169.254.0.0 a 169.254.255.255** (169.254.0.0/16) se designan como **direcciones link-local o APIPA**. El sistema operativo puede asignar automáticamente estas direcciones al host local en entornos donde no se dispone de una configuración IP. Se pueden utilizar en una red punto a punto pequeña o para un host que no pudo obtener una dirección de un servidor de DHCP automáticamente.

La comunicación mediante direcciones link-local IPv4 sólo es adecuada para comunicarse con otros dispositivos conectados a la misma red, como se muestra en la figura. Un host no debe enviar un paquete con una dirección de destino link-local IPv4 a ningún router para ser reenviado, y debería establecer el tiempo de vida (TLL) de IPv4 para estos paquetes en 1.

Las direcciones link-local no proporcionan servicios fuera de la red local. Sin embargo, muchas aplicaciones de cliente/servidor y punto a punto funcionarán correctamente con direcciones de enlace local IPv4.

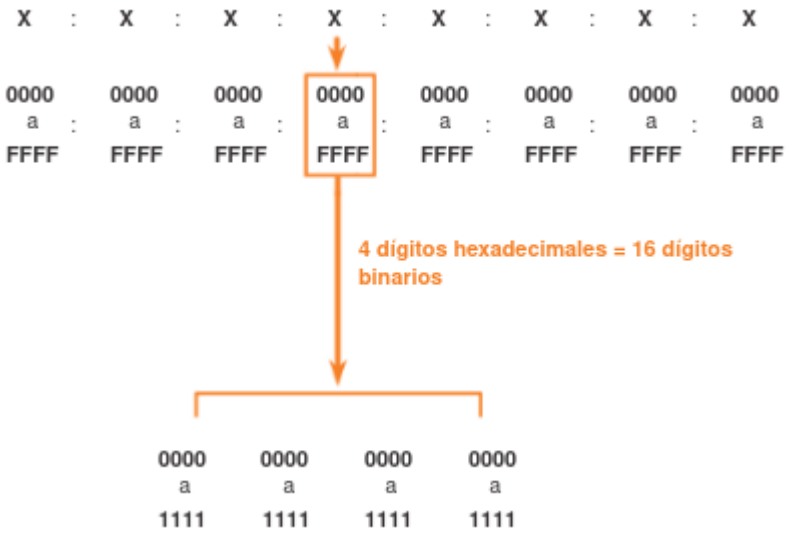
El bloque de direcciones que va de 192.0.2.0 a 192.0.2.255 (**192.0.2.0/24**) se reserva para fines de enseñanza y aprendizaje. Estas direcciones pueden usarse en ejemplos de documentación y redes. A diferencia de las direcciones experimentales, los dispositivos de red aceptarán estas direcciones en su configuración. A menudo puede encontrar que estas direcciones se usan con los nombres de dominio example.com o example.net en la documentación de las RFC, del fabricante y del protocolo. Las direcciones dentro de este bloque no deben aparecer en Internet.

Las direcciones del bloque que va de **240.0.0.0 a 255.255.255.254** se indican como reservadas para uso futuro (RFC 3330). En la actualidad, estas direcciones solo se pueden utilizar para fines de investigación o experimentación, y no se pueden utilizar en una red IPv4. Sin embargo, según RFC 3330, podrían, técnicamente, convertirse en direcciones utilizables en el futuro.

Estructura de la dirección Ipv6

Las direcciones IPv6 tienen una longitud de 128 bits y se escriben como una cadena de valores hexadecimales. Cuatro bits se representan mediante un único dígito hexadecimal, con un total de 32 valores hexadecimales. Las direcciones IPv6 no distinguen mayúsculas de minúsculas y pueden escribirse en minúscula o en mayúscula.

El formato preferido para escribir una dirección IPv6 es x:x:x:x:x:x:x:x, donde cada “x” consta de cuatro valores hexadecimales. Al hacer referencia a 8 bits de una dirección IPv4, utilizamos el término “octeto”. En IPv6, un “hexteto” es el término no oficial que se utiliza para referirse a un segmento de 16 bits o cuatro valores hexadecimales. Cada “x” es un único hexteto, 16 bits o cuatro dígitos hexadecimales.



“Formato preferido” significa que la dirección IPv6 se escribe utilizando 32 dígitos hexadecimales. No significa necesariamente que es el método ideal para representar la dirección IPv6. Veremos dos reglas que permiten reducir el número de dígitos necesarios para representar una dirección IPv6.

La primera regla que permite reducir la notación de direcciones IPv6 es que se puede omitir cualquier 0 (cero) inicial en cualquier sección de 16 bits o hexteto. Por ejemplo:

01AB puede representarse como 1AB.

Esta regla solo es válida para los ceros iniciales, y NO para los ceros finales.

La segunda regla que permite reducir la notación de direcciones IPv6 es que los dos puntos dobles (::) pueden reemplazar cualquier cadena única y contigua de uno o más segmentos de 16 bits (hextetos) compuestos solo por ceros.

Los dos puntos dobles (::) se pueden utilizar solamente una vez dentro de una dirección; de lo contrario, habría más de una dirección resultante posible. Cuando se utiliza junto con la técnica de omisión de ceros iniciales, la notación de direcciones IPv6 generalmente se puede reducir de manera considerable. Esto se suele conocer como “formato comprimido”.

Recuerde que es posible identificar el prefijo, o la porción de red, de una dirección IPv4 mediante una **máscara de subred** en formato decimal punteado o una duración de prefijo (notación con barras). Por ejemplo, la dirección IP 192.168.1.10 con la máscara de subred decimal punteada 255.255.255.0 equivale a 192.168.1.10/24.

IPv6 utiliza el prefijo para representar la porción de prefijo de la dirección. IPv6 no utiliza la notación decimal punteada de máscara de subred. La duración de prefijo se utiliza para indicar la porción de red de una dirección IPv6 mediante el formato de dirección IPv6/prefijo.

El prefijo puede ir de 0 a 128. Un prefijo IPv6 típico para LAN es /64. Esto significa que la porción de red tiene una longitud de 64 bits, lo cual deja otros 64 bits para la ID de interfaz (porción de host)

Direcciones IPV6 unicast

Las direcciones IPv6 unicast identifican de forma exclusiva una interfaz en un dispositivo con IPv6 habilitado. Un paquete que se envía a una dirección unicast es recibido por la interfaz que tiene asignada esa dirección. Como sucede con IPv4, las direcciones IPv6 de origen deben ser direcciones unicast. Las direcciones IPv6 de destino pueden ser direcciones unicast o multicast.

Unicast global

Las direcciones unicast globales son similares a las direcciones IPv4 públicas. Estas son direcciones enrutables de Internet globalmente exclusivas. Las direcciones unicast globales pueden configurarse estáticamente o asignarse de forma dinámica. Existen algunas diferencias importantes con respecto a la forma en que un dispositivo recibe su dirección IPv6 dinámicamente en comparación con DHCP para IPv4.

Link-local

Las direcciones link-local se utilizan para comunicarse con otros dispositivos en el mismo enlace local. Con IPv6, el término “enlace” hace referencia a una subred. Las direcciones link-local se limitan a un único enlace. Su exclusividad se debe confirmar solo para ese enlace, ya que no se pueden enrutar más allá del enlace. En otras palabras, los routers no reenvían paquetes con una dirección de origen o de destino link-local.

Loopback

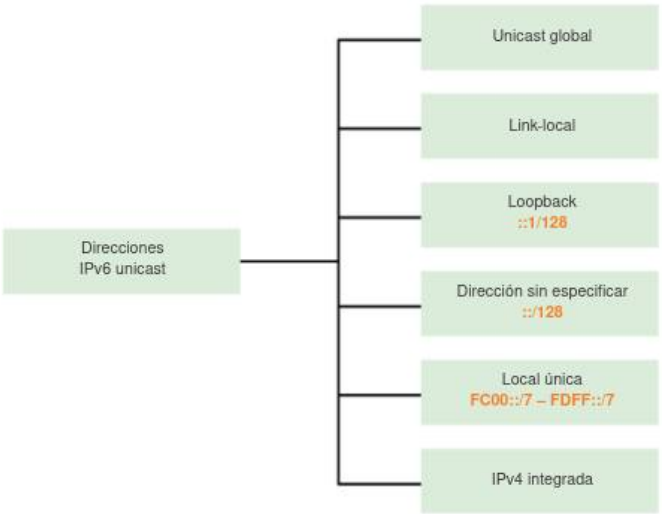
Los hosts utilizan la dirección de loopback para enviarse paquetes a sí mismos, y esta dirección no se puede asignar a una interfaz física. Al igual que en el caso de una dirección IPv4 de loopback, se puede hacer ping a una dirección IPv6 de loopback para probar la configuración de TCP/IP en el host local. La dirección IPv6 de loopback está formada por todos ceros, excepto el último bit, representado como ::1/128 o, simplemente, ::1 en el formato comprimido.

Dirección sin especificar

Una dirección sin especificar es una dirección compuesta solo por ceros representada como ::/128 o, simplemente, :: en formato comprimido. No puede asignarse a una interfaz y solo se utiliza como dirección de origen en un paquete IPv6. Las direcciones sin especificar se utilizan como direcciones de origen cuando el dispositivo aún no tiene una dirección IPv6 permanente o cuando el origen del paquete es irrelevante para el destino.

Local única

Las direcciones IPv6 locales únicas tienen cierta similitud con las direcciones privadas para IPv4 definidas en RFC 1918, pero también existen diferencias importantes. Las direcciones locales únicas se utilizan para el direccionamiento local dentro de un sitio o entre una cantidad limitada de sitios. Estas direcciones no deben ser enrutables en la IPv6 global. Las direcciones locales únicas están en el rango de FC00::/7 a FDFF::/7.



IPv4 integrada

El último tipo de dirección unicast es la dirección IPv4 integrada. Estas direcciones se utilizan para facilitar la transición de IPv4 a IPv6.

Direccion link-local

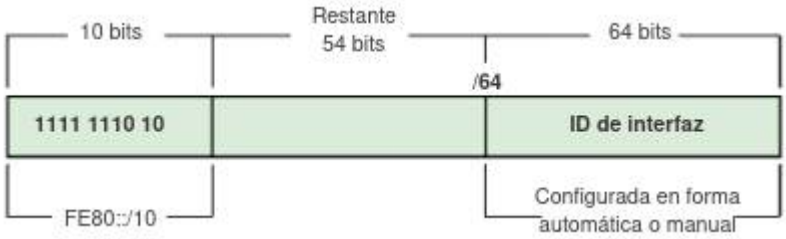
Una dirección IPv6 link-local permite que un dispositivo se comunique con otros dispositivos con IPv6 habilitado en el mismo enlace y solo en ese enlace (subred). Los paquetes con una dirección link-local de origen o de destino no se pueden enrutar más allá del enlace en el cual se originó el paquete.

A diferencia de las direcciones IPv4 link-local, las direcciones IPv6 link-local cumplen una función importante en diversos aspectos de la red. La dirección unicast global no constituye un requisito, pero toda interfaz de red con IPv6 habilitado debe tener una dirección link-local.

Si en una interfaz no se configura una dirección link-local de forma manual, el dispositivo crea automáticamente su propia dirección sin comunicarse con un servidor de DHCP. Los hosts con IPv6 habilitado crean una dirección IPv6 link-local incluso si no se asignó una dirección IPv6 unicast global al dispositivo. Esto permite que los dispositivos con IPv6 habilitado se comuniquen con otros dispositivos con IPv6 habilitado en la misma subred. Esto incluye la comunicación con el gateway predeterminado (router).

Las direcciones IPv6 link-local están en el rango de FE80::/10. /10 indica que los primeros 10 bits son 1111 1110 10xx xxxx. El primer hexteto tiene un rango de 1111 1110 1000 0000 (FE80) a 1111 1110 1011 1111 (FEBF).

Los protocolos de enrutamiento IPv6 también utilizan direcciones IPv6 link-local para intercambiar mensajes y como la dirección del siguiente salto en la tabla de enrutamiento IPv6.



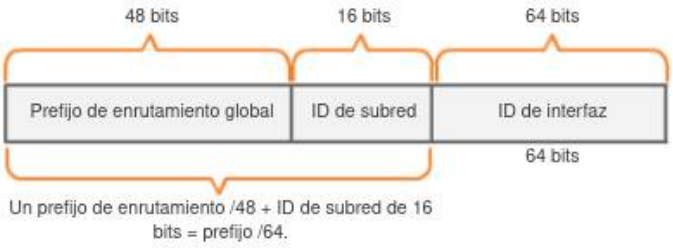
Por lo general, la dirección que se utiliza como gateway predeterminado para los otros dispositivos en el enlace es la dirección link-local del router, y no la dirección unicast global.

Dirección unicast global

Las direcciones IPv6 unicast globales son globalmente únicas y enrutables en Internet IPv6. Estas direcciones son equivalentes a las direcciones IPv4 públicas. La Internet Corporation for Assigned Names and Numbers (ICANN), el operador de la Internet Assigned Numbers Authority (IANA), asigna bloques de direcciones IPv6 a los cinco RIR. Actualmente, solo se asignan direcciones unicast globales con los tres primeros bits de 001 o 2000::/3. Esto solo constituye un octavo del espacio total disponible de direcciones IPv6, sin incluir solamente una parte muy pequeña para otros tipos de direcciones unicast y multicast.

Una dirección unicast global consta de tres partes:

- Prefijo de enrutamiento global
- ID de subred
- ID de interfaz



Prefijo de enrutamiento global

El prefijo de enrutamiento global es la porción de prefijo, o de red, de la dirección que asigna el proveedor (por ejemplo, un ISP) a un cliente o a un sitio. En la actualidad, los RIR asignan a los clientes el prefijo de enrutamiento global /48. Esto incluye desde redes comerciales de empresas hasta unidades domésticas Para la mayoría de los clientes, este espacio de dirección es más que suficiente.

Por ejemplo, la dirección IPv6 2001:0DB8:ACAD::/48 tiene un prefijo que indica que los primeros 48 bits (3 hextetos) (2001:0DB8:ACAD) son la porción de prefijo o de red de la dirección. Los dos puntos dobles (::) antes de la duración de prefijo /48 significan que el resto de la dirección se compone solo de ceros.

ID de subred

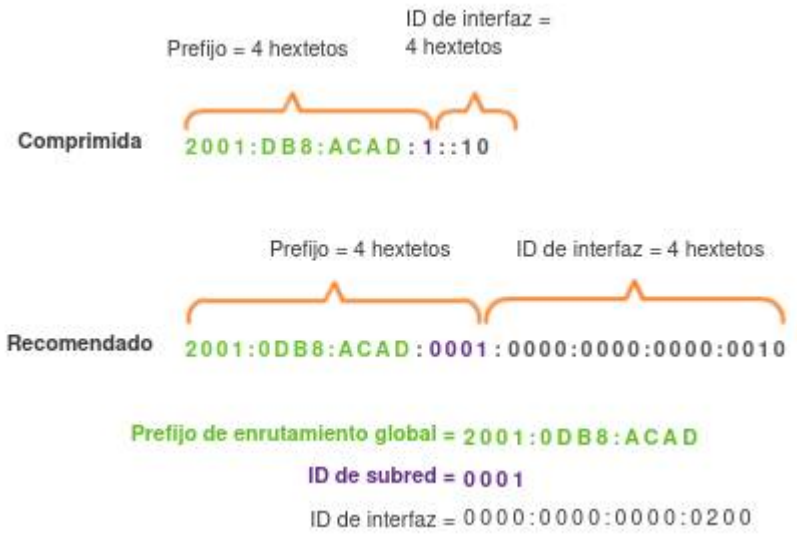
Las organizaciones utilizan la ID de subred para identificar una subred dentro de su ubicación.

ID de interfaz

La ID de interfaz IPv6 equivale a la porción de host de una dirección IPv4. Se utiliza el término “ID de interfaz” debido a que un único host puede tener varias interfaces, cada una con una o más direcciones IPv6.

A diferencia de IPv4, en IPv6 se pueden asignar las direcciones de host compuestas solo por ceros y unos a un dispositivo. Se puede usar la dirección compuesta solo por unos debido al hecho de que en IPv6 no se usan las direcciones de broadcast. También se puede utilizar la dirección compuesta solo por ceros, pero se reserva como una dirección anycast de subred y router, y se debe asignar solo a routers.

Una forma fácil de leer la mayoría de las direcciones IPv6 es contar la cantidad de hextetos. En una dirección unicast global /64 los primeros cuatro hextetos son para la porción de red de la dirección, y el cuarto hexteto indica la ID de subred. Los cuatro hextetos restantes son para la ID de interfaz.



Direcciones multicast

Las direcciones IPv6 multicast son similares a las direcciones IPv4 multicast. Recuerde que las direcciones multicast se utilizan para enviar un único paquete a uno o más destinos (grupo multicast). Las direcciones IPv6 multicast tienen el prefijo FF00::/8. Sólo pueden ser direcciones de destino, no de origen.

Existen dos tipos de direcciones IPv6 multicast:

- Dirección multicast asignada
- Dirección multicast de nodo solicitado

Dirección multicast asignada

Las direcciones multicast asignadas son direcciones multicast reservadas para grupos predefinidos de dispositivos. Una dirección multicast asignada es una única dirección que se utiliza para llegar a un grupo de dispositivos que ejecutan un protocolo o servicio común. Las direcciones multicast asignadas se utilizan en contexto con protocolos específicos, como DHCPv6.

Dos grupos comunes de direcciones multicast IPv6 asignadas incluyen los siguientes:

Grupo multicast de todos los nodos FF02::1: grupo multicast al que se unen todos los dispositivos con IPv6 habilitado. Los paquetes que se envían a este grupo son recibidos y procesados por todas las interfaces IPv6 en el enlace o en la red. Esto tiene el mismo efecto que una dirección de broadcast en IPv4. Un router IPv6 envía mensajes de RA de protocolo de mensajes de control de Internet versión 6 (ICMPv6) al grupo multicast de todos los nodos. El mensaje de RA proporciona a todos los dispositivos en la red con IPv6 habilitado la información de direccionamiento, como el prefijo, la duración de prefijo y el gateway predeterminado.

Grupo multicast de todos los routers FF02::2: grupo multicast al que se unen todos los routers con IPv6 habilitado. Un router se convierte en un miembro de este grupo cuando se habilita como router IPv6 mediante el comando de configuración global **ipv6 unicast-routing**. Los paquetes que se envían a este grupo son recibidos y procesados por todos los routers IPv6 en el enlace o en la red.

Los dispositivos con IPv6 habilitado envían mensajes de solicitud de router (RS) de ICMPv6 a la dirección multicast de todos los routers. El mensaje de RS solicita un mensaje de RA del router IPv6 para contribuir a la configuración de direcciones del dispositivo.

Dirección multicast de nodo solicitado

Las direcciones multicast de nodo solicitado son similares a las direcciones multicast de todos los nodos. Recuerde que la dirección multicast de todos los nodos es esencialmente lo mismo que una dirección IPv4 de broadcast. Todos los dispositivos en la red deben procesar el tráfico enviado a la dirección de todos los nodos. Para reducir el número de dispositivos que deben procesar tráfico, utilice una dirección multicast de nodo solicitado.

Una dirección multicast de nodo solicitado es una dirección que coincide solo con los últimos 24 bits de la dirección IPv6 unicast global de un dispositivo. Los únicos dispositivos que deben procesar estos paquetes son aquellos que tienen estos mismos 24 bits en la porción menos significativa que se encuentra más hacia la derecha de la ID de interfaz.

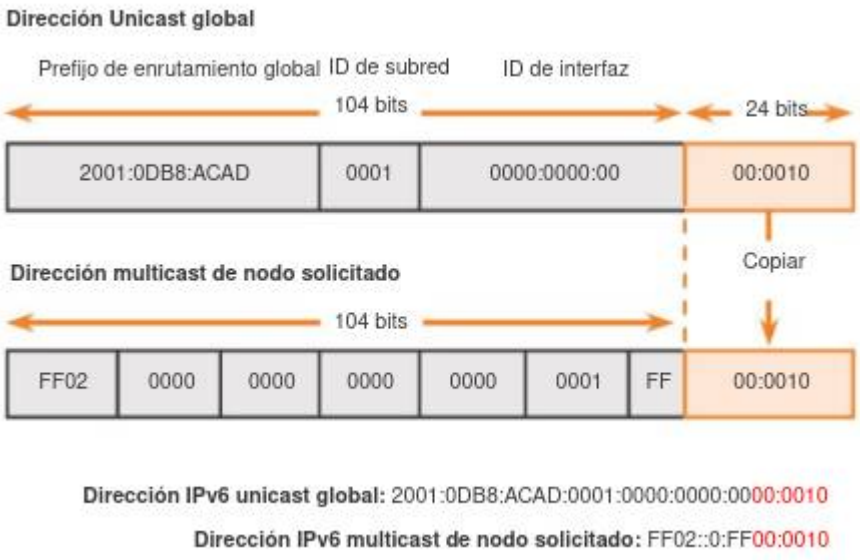
Una dirección IPv6 multicast de nodo solicitado se crea de forma automática cuando se asigna la dirección unicast global o la dirección unicast link-local. La dirección IPv6 multicast de nodo solicitado se crea combinando un prefijo especial FF02:0:0:0:0:1:FF00::/104 con los 24 bits de su dirección unicast que se encuentran en el extremo derecho.

La dirección multicast de nodo solicitado consta de dos partes:

Prefijo multicast FF02:0:0:0:0:1:FF00::/104: los primeros 104 bits de la dirección multicast de todos los nodos solicitados.

24 bits menos significativos.

Los 24 bits finales o que se encuentran más hacia la derecha de la dirección multicast de nodo solicitado. Estos bits se copian de los 24 bits del extremo derecho de la dirección unicast global o unicast link-local del dispositivo.



Es posible que varios dispositivos tengan la misma dirección multicast de nodo solicitado. Si bien es poco común, esto puede suceder cuando los dispositivos tienen los mismos 24 bits que se encuentran más hacia la derecha en sus ID de interfaz. Esto no genera ningún problema, ya que el dispositivo aún procesa el mensaje encapsulado, el cual incluye la dirección IPv6 completa del dispositivo en cuestión.

Asignación dinámica de direcciones. DHCP

IPv4

Cada dispositivo de una red basada en TCP/IP debe tener una dirección IP de unidifusión única para acceder a la red y sus recursos. Sin DHCP, las direcciones IP de los equipos nuevos o de los equipos que se mueven de una subred a otra deben configurarse manualmente, mientras que las direcciones IP de los equipos que se quitan de la red deben recuperarse manualmente.

Con DHCP, todo este proceso está automatizado y se administra de forma centralizada. El servidor DHCP mantiene un grupo de direcciones IP y concede una dirección a cualquier cliente habilitado para DHCP cuando se inicia en la red. Dado que las direcciones IP son dinámicas (concedidas) en lugar de estáticas (asignadas permanentemente), las direcciones que ya no están en uso se devuelven automáticamente al grupo para la reasignación.

El administrador de red establece servidores DHCP que mantienen la información de configuración de TCP/IP y proporcionan la configuración de direcciones a los clientes habilitados para DHCP en forma de oferta de concesión. El servidor DHCP almacena la información de configuración en una base de datos que incluye lo siguiente:

Parámetros de configuración de TCP/IP válidos para todos los clientes de la red.

Direcciones IP válidas, mantenidas en un grupo para la asignación a clientes, así como direcciones excluidas.

Direcciones IP reservadas asociadas a determinados clientes DHCP. Esto permite una asignación coherente de una única dirección IP a un único cliente DHCP.

La duración de la concesión, o el período de tiempo durante el que se puede usar la dirección IP antes de que se requiera una renovación de la concesión.

Cuando un cliente habilitado para DHCP acepta una oferta de concesión, recibe lo siguiente:

Una dirección IP válida para la subred a la que se conecta.

Las opciones DHCP solicitadas, que son parámetros adicionales que un servidor DHCP está configurado para asignar a los clientes. Algunos ejemplos de opciones DHCP son Enrutador (puerta de enlace predeterminada), Servidores DNS y Nombre de dominio DNS.

IPv6

Configuración automática de dirección sin estado (SLAAC)

La configuración automática de dirección sin estado (SLAAC) es un método que permite que un dispositivo obtenga su prefijo, duración de prefijo e información de la dirección de gateway predeterminado de un router IPv6 sin utilizar un servidor de DHCPv6. Mediante SLAAC, los dispositivos dependen de los mensajes de anuncio de router (RA) de ICMPv6 del router local para obtener la información necesaria.

Los routers IPv6 envían mensajes de anuncio de router (RA) de ICMPv6 a todos los dispositivos en la red con IPv6 habilitado de forma periódica. De manera predeterminada, los routers Cisco envían mensajes de RA cada 200 segundos a la dirección IPv6 de grupo multicast de todos los nodos. Los dispositivos IPv6 en la red no tienen que esperar estos mensajes periódicos de RA. Un dispositivo puede enviar un mensaje de solicitud de router (RS) utilizando la dirección IPv6 de grupo multicast de todos los routers. Cuando un router IPv6 recibe un mensaje de RS, responde inmediatamente con un anuncio de router.

Si bien es posible configurar una interfaz en un router Cisco con una dirección IPv6, esto no lo convierte en un “router IPv6”. Un router IPv6 es un router que presenta las siguientes características:

Reenvía paquetes IPv6 entre redes.

Puede configurarse con rutas estáticas IPv6 o con un protocolo de enrutamiento dinámico IPv6.

Envía mensajes RA ICMPv6.

El enrutamiento IPv6 no está habilitado de manera predeterminada ya que los routers CISCO están habilitados como routers IPv4 por defecto. Para habilitar un router como router IPv6, se debe utilizar el comando de configuración global **ipv6 unicast-routing**.

El mensaje de RA de ICMPv6 contiene el prefijo, la duración de prefijo y otra información para el dispositivo IPv6. El mensaje de RA también informa al dispositivo IPv6 cómo obtener la información de direccionamiento. El mensaje de RA puede contener una de las siguientes tres opciones, como se muestra en la ilustración:

Opción 1, SLAAC solamente: el dispositivo debe utilizar el prefijo, la duración de prefijo y la información de la dirección de gateway predeterminado incluida en el mensaje de RA. No se encuentra disponible ninguna otra información de un servidor de DHCPv6.

Opción 2, SLAAC y DHCPv6: el dispositivo debe utilizar el prefijo, la duración de prefijo y la información de la dirección de gateway predeterminado incluida en el mensaje de RA. Existe otra información disponible de un servidor de DHCPv6, como la dirección del servidor DNS. El dispositivo obtiene esta información adicional mediante el proceso normal de descubrimiento y consulta a un servidor de DHCPv6. Esto se conoce como DHCPv6 sin estado, debido a que el servidor de DHCPv6 no necesita asignar ni realizar un seguimiento de ninguna asignación de direcciones IPv6, sino que solo proporciona información adicional, tal como la dirección del servidor DNS.

Opción 3, DHCPv6 solamente: el dispositivo no debe utilizar la información incluida en el mensaje de RA para obtener la información de direccionamiento. En cambio, el dispositivo utiliza el proceso normal de descubrimiento y consulta a un servidor de DHCPv6 para obtener toda la información de direccionamiento. Esto incluye una dirección IPv6 unicast global, la duración de prefijo, la dirección de gateway predeterminado y las direcciones de los servidores DNS. En este caso, el servidor de DHCPv6 actúa como un servidor de DHCP sin estado, de manera similar a DHCP para IPv4. El servidor de DHCPv6 asigna direcciones IPv6 y realiza un seguimiento de ellas, a fin de no asignar la misma dirección IPv6 a varios dispositivos.

Los routers envían mensajes de RA de ICMPv6 utilizando la dirección link-local como la dirección IPv6 de origen. Los dispositivos que utilizan SLAAC usan la dirección link-local del router como su dirección de gateway predeterminado.

DHCPv6

El protocolo de configuración dinámica de host para IPv6 (DHCPv6) es similar a DHCP para IPv4. Los dispositivos pueden recibir de manera automática la información de direccionamiento, incluso una dirección unicast global, la duración de prefijo, la dirección de gateway predeterminado y las direcciones de servidores DNS, mediante los servicios de un servidor de DHCPv6.

Los dispositivos pueden recibir la información de direccionamiento IPv6 en forma total o parcial de un servidor de DHCPv6 en función de si en el mensaje de RA de ICMPv6 se especificó la opción 2 (SLAAC y DHCPv6) o la opción 3 (DHCPv6 solamente). Además, el S.O del host puede optar por omitir el contenido del mensaje de RA del router y obtener su dirección IPv6 y otra información directamente de un servidor de DHCPv6.

Antes de implementar dispositivos IPv6 en una red, se recomienda primero verificar si el host observa las opciones dentro del mensaje ICMPv6 de RA del router.

Un dispositivo puede obtener la dirección IPv6 unicast global dinámicamente y también estar configurado con varias direcciones IPv6 estáticas en la misma interfaz. IPv6 permite que varias direcciones IPv6 (que pertenecen a la misma red IPv6) se configuren en la misma interfaz.

Si el cliente no utiliza la información incluida en el mensaje de RA y depende exclusivamente de DHCPv6, el servidor de DHCPv6 proporciona la dirección IPv6 unicast global completa, incluidos el prefijo y la ID de interfaz.

Sin embargo, si se utiliza la opción 1 (SLAAC solamente) o la opción 2 (SLAAC con DHCPv6), el cliente no obtiene la porción de ID de interfaz real de la dirección mediante este estos procesos. El dispositivo cliente debe determinar su propia ID de interfaz de 64 bits, ya sea mediante el proceso EUI-64 o generando un número aleatorio de 64 bits.

Al utilizar SLAAC (SLAAC solamente o SLAAC con DHCPV6), los dispositivos reciben el prefijo y la duración de prefijo del mensaje de RA de ICMPv6. Debido a que el mensaje de RA designa el prefijo de la dirección, el dispositivo debe proporcionar únicamente la porción de ID de interfaz de su dirección. Como se indicó anteriormente, la ID de interfaz se puede generar de forma automática mediante el proceso EUI-64, o, según el OS, se puede generar de forma aleatoria. Con la información del mensaje de RA y la ID de interfaz, el dispositivo puede establecer su dirección unicast global.

Proceso EUI-64

El IEEE definió el identificador único extendido (EUI) o proceso EUI-64 modificado. Este proceso utiliza la dirección MAC de Ethernet de 48 bits de un cliente e introduce otros 16 bits en medio de la dirección MAC de 48 bits para crear una ID de interfaz de 64 bits.

Las direcciones MAC de Ethernet, por lo general, se representan en formato hexadecimal y constan de dos partes:

Identificador único de organización (OUI): el OUI es un código de proveedor de 24 bits (seis dígitos hexadecimales) que asigna el IEEE.

Identificador de dispositivo: el identificador de dispositivo es un valor único de 24 bits (seis dígitos hexadecimales) dentro de un OUI común.

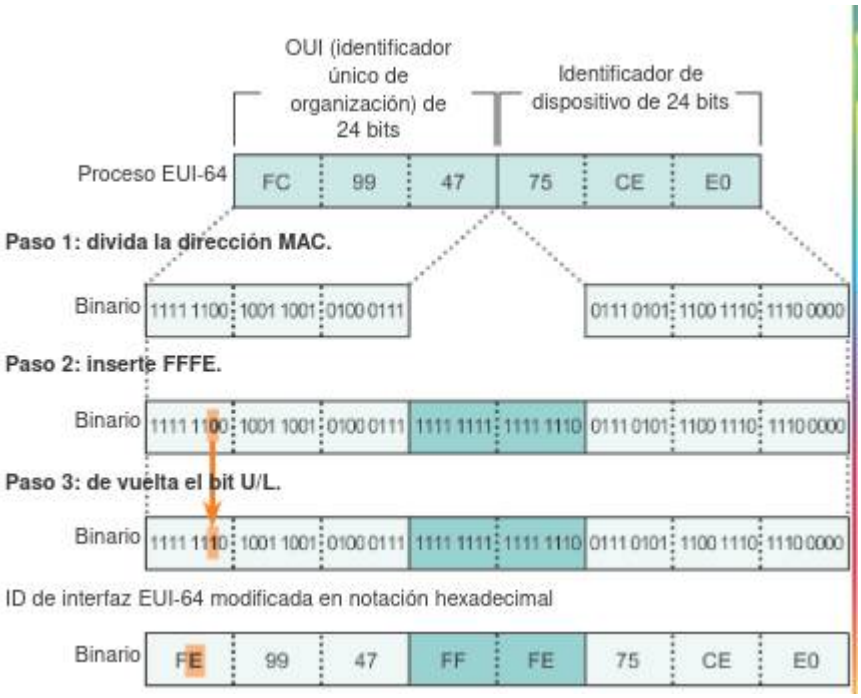
Las ID de interfaz EUI-64 se representan en sistema binario y constan de tres partes:

OUI de 24 bits de la dirección MAC del cliente, pero el séptimo bit (bit universal/local, U/L) se invierte. Esto significa que si el séptimo bit es un 0, se convierte en 1, y viceversa.

Valor de 16 bits FFFE introducido (en formato hexadecimal)

Identificador de dispositivo de 24 bits de la dirección MAC del cliente

Por ejemplo podemos ver el proceso EUI-64, con la siguiente dirección MAC FC99:4775:CEE0.



La ventaja de EUI-64 es que se puede utilizar la dirección MAC de Ethernet para determinar la ID de interfaz. También permite que los administradores de red rastreen fácilmente una dirección IPv6 a un dispositivo final mediante la dirección MAC única. Sin embargo, esto generó inquietudes con respecto a la privacidad a muchos usuarios. Les preocupa que los paquetes puedan ser rastreados a la PC física real. Debido a estas inquietudes, se puede utilizar en cambio una ID de interfaz generada aleatoriamente.

ID de interfaz generadas aleatoriamente

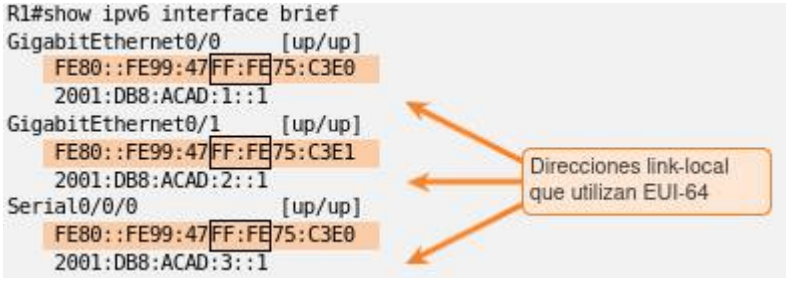
Según el sistema operativo, un dispositivo puede utilizar una ID de interfaz generada aleatoriamente en lugar de utilizar la dirección MAC y el proceso EUI-64. Por ejemplo, comenzando con Windows Vista, Windows utiliza una ID de interfaz generada aleatoriamente en lugar de una ID de interfaz creada mediante EUI-64. Windows XP y sistemas operativos Windows anteriores utilizaban EUI-64.

Una manera sencilla de identificar que una dirección muy probablemente se creó mediante EUI-64 es el valor FFFE ubicado en medio de la ID de interfaz.

Después de que se establece una ID de interfaz, ya sea mediante el proceso EUI-64 o mediante la generación aleatoria, se puede combinar con un prefijo IPv6 para crear una dirección unicast global o una dirección link-local.

Dirección unicast global: al utilizar SLAAC, el dispositivo recibe su prefijo del mensaje de RA de ICMPv6 y lo combina con la ID de interfaz.

Dirección link-local: los prefijos link-local comienzan con FE80::/10. Los dispositivos suelen utilizar FE80::/64 como prefijo o duración de prefijo, seguido de la ID de interfaz.



Después de que se asigna una dirección unicast global a una interfaz, el dispositivo con IPv6 habilitado genera la dirección link-local automáticamente. Los dispositivos con IPv6 habilitado deben tener, como mínimo, la dirección link-local. Recuerde que una dirección IPv6 link-local permite que un dispositivo se comunique con otros dispositivos con IPv6 habilitado en la misma subred.

Las direcciones IPv6 link-local se utilizan para diversos fines, incluidos los siguientes:

Los hosts utilizan la dirección link-local del router local para obtener la dirección IPv6 de gateway predeterminado.

Los routers intercambian mensajes de protocolo de enrutamiento dinámico mediante direcciones link-local.

Las tablas de enrutamiento de los routers utilizan la dirección link-local para identificar el router del siguiente salto al reenviar paquetes IPv6.

Las direcciones link-local se pueden establecer dinámicamente o se pueden configurar de forma manual como direcciones link-local estáticas.

Dirección link-local asignada dinámicamente

La dirección link-local se crea dinámicamente mediante el prefijo **FE80::/10** y la ID de interfaz.

De manera predeterminada, los routers en los que se utiliza Cisco IOS utilizan EUI-64 para generar la ID de interfaz para todas las direcciones link-local en las interfaces IPv6. Para las interfaces seriales, el router utiliza la dirección MAC de una interfaz Ethernet. Recuerde que una dirección link-local debe ser única solo en ese enlace o red. Sin embargo, una desventaja de utilizar direcciones link-local asignadas dinámicamente es su longitud, que dificulta identificar y recordar las direcciones asignadas.