Problemas con IPv4.

Necesidad de utilizar IPv6.

IPv6 está diseñado para ser el sucesor de IPv4. IPv6 tiene un mayor espacio de direcciones de 128 bits, lo que proporciona 340 sextillones de direcciones. (Es decir, el número 340 seguido por 36 ceros). Sin embargo, IPv6 es más que solo direcciones más extensas. Cuando el IETF comenzó el desarrollo de un sucesor de IPv4, utilizó esta oportunidad para corregir las limitaciones de IPv4 e incluir mejoras adicionales. Un ejemplo es el protocolo de mensajes de control de Internet versión 6 (ICMPv6), que incluye la resolución de direcciones y la configuración automática de direcciones, las cuales no se encuentran en ICMP para IPv4 (ICMPv4). ICMPv4 e ICMPv6 se analizan más adelante en este capítulo.

Necesidad de utilizar IPv6

El agotamiento del espacio de direcciones IPv4 fue el factor que motivó la migración a IPv6. Debido al aumento de la conexión a Internet en África, Asia y otras áreas del mundo, las direcciones IPv4 ya no son suficientes como para admitir este crecimiento. Como se muestra en la ilustración, a cuatro de cinco RIR se les agotaron las direcciones IPv4.

IPv4 tiene un máximo teórico de 4300 millones de direcciones. Las direcciones privadas en combinación con la traducción de direcciones de red (NAT) fueron esenciales para demorar la reducción del espacio de direcciones IPv4. Sin embargo, la NAT rompe muchas aplicaciones y tiene limitaciones que obstaculizan considerablemente las comunicaciones entre pares.

Internet de todo

En la actualidad, Internet es significativamente distinta de como era en las últimas décadas. Actualmente, Internet es mucho más que el correo electrónico, las páginas web y la transferencia de archivos entre computadoras. Internet evoluciona y se está convirtiendo en una Internet de los objetos. Ya no serán solo las computadoras, las tabletas PC y los teléfono inteligentes los únicos dispositivos que accedan a Internet. Los dispositivos del futuro preparados para acceder a Internet y equipados con sensores incluirán desde automóviles y dispositivos biomédicos hasta electrodomésticos y ecosistemas naturales.

Con una población que accede a Internet cada vez mayor, un espacio de direcciones IPv4 limitado, los problemas de NAT y la Internet de todo, llegó el momento de comenzar la transición hacia IPv6.

Coexistencia de IPv4 e IPv6.

No hay una única fecha para realizar la transición a IPv6. En un futuro cercano, IPv4 e IPv6 coexistirán. Se espera que la transición demore años. El IETF creó diversos protocolos y herramientas para ayudar a los administradores de redes a migrar las redes a IPv6. Las técnicas de migración pueden dividirse en tres categorías:

- **Dual-stack:** como se muestra en la figura 1, la técnica dual-stack permite que IPv4 e IPv6 coexistan en el mismo segmento de red. Los dispositivos dual-stack ejecutan pilas de protocolos IPv4 e IPv6 de manera simultánea.
- **Tunelización:** como se muestra en la figura 2, el protocolo de túnel es un método para transportar un paquete IPv6 en una red IPv4. El paquete IPv6 se encapsula dentro de un paquete IPV4, de manera similar a lo que sucede con otros tipos de datos.
- **Traducción:** como se muestra en la figura 3, la traducción de direcciones de red 64 (NAT64) permite que los dispositivos habilitados para IPv6 se comuniquen con los dispositivos habilitados para IPv4 mediante una técnica de traducción similar a NAT para IPv4. Un paquete IPv6 se traduce a un paquete IPv4 y viceversa.

Nota: la tunelización y la traducción solo se usan cuando es necesario. El objetivo debe ser las comunicaciones IPv6 nativas de origen a destino.

Direccionamiento IPv6.

Representación de dirección IPv6.

Las direcciones IPv6 tienen una longitud de 128 bits y se escriben como una cadena de valores hexadecimales. Cada 4 bits se representan con un único dígito hexadecimal para llegar a un total de 32 valores hexadecimales, como se muestra en la figura 1. Las direcciones IPv6 no distinguen entre mayúsculas y minúsculas, y pueden escribirse en minúsculas o en mayúsculas.

Formato preferido

Como se muestra en la figura 1, 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 los 32 dígitos hexadecimales. No significa necesariamente que sea el método ideal para representar la dirección IPv6. En las siguientes páginas, veremos dos reglas que permiten reducir el número de dígitos necesarios para representar una dirección IPv6.

En la figura 2, se presenta un resumen de la relación entre decimal, binario y hexadecimal. En la figura 3, se muestran ejemplos de direcciones IPv6 en el formato preferido.

Regla 1: omitir los 0 iniciales.

La primera regla para ayudar a reducir la notación de las direcciones IPv6 consiste en omitir los 0 (ceros) iniciales en cualquier sección de 16 bits o hexteto. Por ejemplo:

- 01AB puede representarse como 1AB.
- 09F0 puede representarse como 9F0.
- 0A00 puede representarse como A00.
- 00AB puede representarse como AB.

Esta regla solo es válida para los ceros iniciales, y NO para los ceros finales; de lo contrario, la dirección sería ambigua. Por ejemplo, el hexteto "ABC" podría ser "0ABC" o "ABC0", pero estos no representan el mismo valor.

En las figuras 1 a 8, se muestran varios ejemplos de cómo se puede utilizar la omisión de ceros iniciales para reducir el tamaño de una dirección IPv6. Para cada ejemplo, se muestra el formato preferido. Advierta cómo la omisión de ceros iniciales en la mayoría de los ejemplos da como resultado una representación más pequeña de la dirección.

Regla 2: omitir los segmentos de 0.

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”.

Dirección incorrecta:

- 2001:0DB8::ABCD::1234

Expansiones posibles de direcciones comprimidas ambiguas:

- 2001:0DB8::ABCD:0000:0000:1234
- 2001:0DB8::ABCD:0000:0000:0000:1234
- 2001:0DB8:0000:ABCD::1234
- 2001:0DB8:0000:0000:ABCD::1234

En las figuras 1 a 7, se muestran varios ejemplos de cómo el uso de los dos puntos dobles (::) y la omisión de los 0 iniciales pueden reducir el tamaño de una dirección IPv6.

Tipos de direcciones IPv6.

Existen tres tipos de direcciones IPv6:

- **Unidifusión:** una dirección IPv6 de unidifusión identifica de manera única una interfaz de un dispositivo habilitado para IPv6. Como se muestra en la ilustración, las direcciones IPv6 de origen deben ser direcciones de unidifusión.
- **Multidifusión:** las direcciones IPv6 de multidifusión se usan para enviar un único paquete IPv6 a varios destinos.
- **Difusión por proximidad:** una dirección IPv6 de difusión por proximidad es cualquier dirección IPv6 de unidifusión que puede asignarse a varios dispositivos. Los paquetes enviados a una dirección de difusión por proximidad se enrutan al dispositivo más cercano que tenga esa dirección. Las direcciones de difusión por proximidad exceden el ámbito de este curso.

A diferencia de IPv4, IPv6 no tiene una dirección de difusión. Sin embargo, existe una dirección IPv6 de multidifusión de todos los nodos que brinda básicamente el mismo resultado.

Longitud de prefijo IPv6.

Recuerde que el prefijo, o la porción de red, de una dirección IPv4 se puede identificar con una máscara de subred decimal punteada o con la longitud de prefijo (notación con barra diagonal). Por ejemplo, la dirección IPv4 192.168.1.10 con la máscara de subred decimal punteada 255.255.255.0 equivale a 192.168.1.10/24.

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

La longitud de prefijo puede ir de 0 a 128. Una longitud de prefijo IPv6 típica para LAN y la mayoría de los demás tipos de redes es /64. Esto significa que la porción de prefijo o de red de la dirección tiene una longitud de 64 bits, lo cual deja otros 64 bits para la ID de interfaz (porción de host) de la dirección.

Direcciones IPv6 de unidifusión.

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

Los tipos de direcciones IPv6 de unidifusión más comunes son las direcciones de unidifusión globales (GUA) y las direcciones de unidifusión link-local.

Unidifusión global

Las direcciones de unidifusión globales son similares a las direcciones IPv4 públicas. Estas son direcciones enrutables de Internet globalmente exclusivas. Las direcciones de unidifusión globales pueden configurarse estáticamente o asignarse de forma dinámica.

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.

Local única

Otro tipo de dirección de unidifusión es la dirección de unidifusión local única. Las direcciones IPv6 locales únicas tienen ciertas similitudes con las direcciones privadas RFC 1918 para IPv4, pero existen grandes diferencias. Las direcciones locales únicas se utilizan para el direccionamiento local dentro de un sitio o entre una cantidad limitada de sitios. Estas direcciones no deberían poder enrutarse en la IPv6 global, y no deberían traducirse hacia direcciones IPv6 globales. Las direcciones locales únicas están en el rango de FC00::/7 a FDFF::/7.

Con IPv4, las direcciones privadas se combinan con NAT/PAT para proporcionar una traducción de varios a uno de direcciones privadas a públicas. Esto se hace debido a la disponibilidad limitada del espacio de direcciones IPv4. Muchos sitios también utilizan la naturaleza privada de las direcciones definidas en RFC 1918 para ayudar a proteger u ocultar su red de posibles riesgos de seguridad. Sin embargo, este nunca fue el uso previsto de esas tecnologías, y el IETF siempre recomendó que los sitios tomaran las precauciones de seguridad adecuadas en el router del lado de Internet. Las direcciones locales únicas pueden usarse en dispositivos que nunca necesitan o nunca pueden acceder a otra red.

Direcciones IPv6 de unidifusión 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 direcciones link-local de origen o destino no pueden enrutarse más allá del enlace en el que se originó el paquete.

La dirección de unidifusión global no es un requisito. Sin embargo, cada 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 DHCP. Los hosts con IPv6 habilitado crean una dirección IPv6 link-local incluso si no se asignó una dirección IPv6 de unidifusión 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).

En la figura 1, se muestra un ejemplo de comunicación mediante direcciones IPv6 link-local.

En la figura 2, se muestran algunos usos de las direcciones IPv6 link-local.

Nota: Generalmente, es la dirección de enlace local del router, y no la dirección de unidifusión global, que se usa como gateway predeterminado para otros dispositivos del enlace.

Direcciones IPv6 de unidifusión.

Estructura de una dirección IPv6 de unidifusión global.

Las direcciones IPv6 de unidifusión globales (GUA) son globalmente únicas y enrutables en Internet IPv6. Estas direcciones son equivalentes a las direcciones IPv4 públicas. La Corporación de Internet para la Asignación de Nombres y Números (ICANN), operador de la IANA, asigna bloques de direcciones IPv6 a los cinco RIR. Actualmente, solo se asignan direcciones de unidifusión globales con los tres primeros bits 001 o 2000::/3. Es decir que el primer dígito hexadecimal de una dirección de GUA comienza con 2 o 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 de unidifusión y multidifusión.

Nota: se reservó la dirección 2001:0DB8::/32 con fines de documentación, incluido el uso en ejemplos.

En la figura 1, se muestra la estructura y el intervalo de una dirección de unidifusión global.

Una dirección de unidifusión global consta de tres partes:

- Prefijo de routing global
- ID de subred
- ID de interfaz

Prefijo de routing global

El prefijo de routing global es la porción de prefijo, o de red, de la dirección asigna el proveedor (por ejemplo, un ISP) a un cliente o a un sitio. En general, los RIR asignan un prefijo de routing global /48 a los clientes. Estos incluyen a todos, desde redes comerciales de empresas a hogares individuales.

En la figura 2, se muestra la estructura de una dirección de unidifusión global con el prefijo de routing global /48. Los prefijos /48 son los prefijos de routing global más comunes y se utilizan en la mayoría de los ejemplos a lo largo de este curso.

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 longitud de prefijo /48 significan que el resto de la dirección se compone solo de ceros.

El tamaño del prefijo de routing global determina el tamaño de la ID de subred.

ID de subred

Las organizaciones utilizan la ID de subred para identificar subredes dentro de su ubicación. Cuanto mayor es la ID de subred, más subredes habrá disponibles.

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. Se recomienda especialmente usar subredes /64 en la mayoría de los casos. En otras palabras, una ID de interfaz de 64 bits como la que se muestra en la figura 2.

Nota: a diferencia de IPv4, en IPv6, pueden asignarse a un dispositivo las direcciones de host compuestas solo por ceros y solo por unos. Se puede usar la dirección compuesta solo por unos debido al hecho de que en IPv6 no se usan las direcciones de difusión. Las direcciones compuestas solo por ceros también pueden usarse, pero se reservan como dirección de difusión por proximidad subred-router, y solo deben asignarse a los routers.

Una forma fácil de leer la mayoría de las direcciones IPv6 es contar la cantidad de hextetos. Como se muestra en la figura 3, en una dirección de unidifusión 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.

Configuración estática de una dirección de unidifusión global.

Configuración del router

La mayoría de los comandos de configuración y verificación IPv6 de Cisco IOS son similares a sus equivalentes de IPv4. En la mayoría de los casos, la única diferencia es el uso de ipv6 en lugar de ip dentro de los comandos.

El comando para configurar una dirección IPv6 de unidifusión global en una interfaz es ipv6 address ipv6-address/prefix-length.

Observe que no hay un espacio entre *ipv6-address y prefix-length*.

La configuración del ejemplo usa la topología que se muestra en la figura 1 y estas subredes IPv6:

- 2001:0DB8:ACAD:0001:/64 (o 2001:DB8:ACAD:1::/64)
- 2001:0DB8:ACAD:0002:/64 (o 2001:DB8:ACAD:2::/64)
- 2001:0DB8:ACAD:0003:/64 (o 2001:DB8:ACAD:3::/64)

En la figura 1, también se muestran los comandos necesarios para configurar la dirección IPv6 de unidifusión global en la interfaz GigabitEthernet 0/0, GigabitEthernet 0/1 y Serial 0/0/0 del R1.

Configuración de host

Configurar la dirección IPv6 en un host de forma manual es similar a configurar una dirección IPv4.

Como se muestra en la figura 2, la dirección de gateway predeterminado configurada para la PC1 es 2001:DB8:ACAD:1::1. Esta es la dirección de unidifusión global de la interfaz GigabitEthernet del R1 de la misma red. De manera alternativa, la dirección de gateway predeterminado puede configurarse para que coincida con la dirección link-local de la interfaz GigabitEthernet. Cualquiera de las dos configuraciones funciona.

Al igual que con IPv4, la configuración de direcciones estáticas en clientes no se extiende a entornos más grandes. Por este motivo, la mayoría de los administradores de redes en una red IPv6 habilitan la asignación dinámica de direcciones IPv6.

Los dispositivos pueden obtener automáticamente una dirección IPv6 de unidifusión global de dos maneras:

- Configuración automática de dirección independiente del estado (SLAAC)
- Mediante DHCPv6 con estado

Nota: cuando se usa DHCPv6 o SLAAC, se especifica automáticamente la dirección link-local del router local como dirección de gateway predeterminado.

Configuración dinámica: SLAAC.

La configuración automática de dirección independiente del estado (SLAAC) es un método que permite que un dispositivo obtenga su prefijo, la longitud de prefijo, la dirección de gateway predeterminado y otra información de un router IPv6, sin usar un servidor 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 RA de ICMPv6 periódicamente, cada 200 segundos, a todos los dispositivos con IPv6 habilitado en la red. También se envía un mensaje RA en respuesta a un host que envía un mensaje ICMPv6 de solicitud de router (RS).

El routing IPv6 no está habilitado de manera predeterminada. Para habilitar un router como router IPv6, se debe usar el comando de configuración global **ipv6 unicast-routing**.

Nota: se pueden configurar direcciones IPv6 en un router sin que sea un router IPv6.

El mensaje RA de ICMPv6 es una sugerencia a un dispositivo sobre cómo obtener una dirección IPv6 de unidifusión global. La decisión final la tiene el sistema operativo del dispositivo. El mensaje RA de ICMPv6 incluye lo siguiente:

- **Prefijo de red y longitud de prefijo:** indica al dispositivo a qué red pertenece.
- **Dirección de gateway predeterminado:** es una dirección IPv6 link-local, la dirección IPv6 de origen del mensaje RA.
- **Direcciones DNS y nombre de dominio:** direcciones de los servidores DNS y un nombre de dominio.

Como se muestra en la figura 1, existen tres opciones para los mensajes RA:

- Opción 1: SLAAC
- Opción 2: SLAAC con un servidor DHCPv6 sin información de estado
- Opción 3: DHCPv6 con información de estado (no SLAAC)

Opción 1 de RA: SLAAC

De manera predeterminada, el mensaje RA sugiere que el dispositivo receptor use la información de dicho mensaje para crear su propia dirección IPv6 de unidifusión global y para toda la demás información. No se requieren los servicios de un servidor DHCPv6.

SLAAC es independiente del estado, o sea que no existe un servidor central (por ejemplo, un servidor DHCPv6 con información de estado) que asigne direcciones de unidifusión globales y mantenga una lista de los dispositivos y sus direcciones. Con SLAAC, el dispositivo cliente usa la información del mensaje RA para crear su propia dirección de unidifusión global. Como se muestra en la figura 2, las dos partes de la dirección se crean del siguiente modo:

- **Prefijo:** se recibe en el mensaje RA.
- **ID de interfaz:** usa el proceso EUI-64 o genera un número aleatorio de 64 bits.

Configuración dinámica: DHCPv6.

De manera predeterminada, el mensaje RA es la opción 1, solo SLAAC. La interfaz del router puede configurarse para enviar un anuncio de router mediante SLAAC y un DHCPv6 sin información de estado, o solo DHCPv6 con información de estado.

Opción 2 de RA: SLAAC y DHCPv6 sin información de estado

Con esta opción, el mensaje RA sugiere que el dispositivo use lo siguiente:

- SLAAC para crear su propia dirección IPv6 de unidifusión global.

- La dirección link-local del router, la dirección IPv6 de origen del RA para la dirección de gateway predeterminado
- Un servidor DHCPv6 sin información de estado que obtendrá otra información como la dirección del servidor DNS y el nombre de dominio

Un servidor DHCPv6 sin información de estado distribuye las direcciones del servidor DNS y los nombres de dominio. No asigna direcciones de unidifusión globales.

Opción 3 de RA: DHCPv6 con información de estado

DHCPv6 con información de estado es similar a DHCP para IPv4. Un dispositivo puede recibir automáticamente la información de direccionamiento, que incluye una dirección de unidifusión global, la longitud de prefijo y las direcciones de los servidores DNS que usan los servicios de un servidor DHCPv6 con información de estado.

Con esta opción, el mensaje RA sugiere que el dispositivo use lo siguiente:

- La dirección link-local del router, la dirección IPv6 de origen del RA para la dirección de gateway predeterminado
- Un servidor DHCPv6 con información de estado para obtener una dirección de unidifusión global, una dirección del servidor DNS, un nombre de dominio y toda la información restante.

Un servidor DHCPv6 con información de estado asigna y mantiene una lista de qué dispositivo recibe cuál dirección IPv6. DHCP para IPv4 tiene información de estado.

Nota: la dirección de gateway predeterminado solo puede obtenerse de manera dinámica del mensaje RA. El servidor DHCPv6 con información de estado o sin ella no brinda la dirección de gateway predeterminado.

Proceso EUI-64 y generación aleatoria.

Cuando el mensaje RA es SLAAC o SLAAC con DHCPv6 sin información de estado, el cliente debe generar su propia ID de interfaz. El cliente conoce la porción de prefijo de la dirección del mensaje RA, pero debe crear su propia ID de interfaz. La ID de interfaz puede crearse mediante el proceso EUI-64 o mediante un número de 64 bits de generación aleatoria, como se muestra en la figura 1.

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 (6 dígitos hexadecimales) asignado por el IEEE.
- Identificador de dispositivo: el identificador de dispositivo es un valor único de 24 bits (6 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 quiere decir que si el séptimo bit es un 0, se transforma en un 1, y viceversa.
- Valor de 16 bits FFFE introducido (en formato hexadecimal)
- Identificador de dispositivo de 24 bits de la dirección MAC del cliente

En la figura 2, se ilustra el proceso EUI-64, con la siguiente dirección MAC de GigabitEthernet de R1: FC99:4775:CEE0.

Paso 1: Dividir la dirección MAC entre el OUI y el identificador de dispositivo.

Paso 2: Insertar el valor hexadecimal FFFE, que en sistema binario es 1111 1111 1111 1110.

Paso 3: Convertir los primeros 2 valores hexadecimales del OUI a sistema binario y cambie el bit U/L (bit 7). En este ejemplo, el 0 en el bit 7 se cambia a 1.

El resultado es una ID de interfaz FE99:47FF:FE75:CEE0 generada mediante EUI-64.

Nota: en RFC 5342, se analiza el uso del bit U/L y las razones para invertir su valor.

En la figura 3, se muestra la dirección IPv6 de unidifusión global de la PCA creada de manera dinámica mediante SLAAC y el proceso 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, como se muestra en la figura 3.

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 redes rastreen fácilmente una dirección IPv6 a un terminal mediante la dirección MAC única. Sin embargo, esto generó inquietudes a muchos usuarios con respecto a la privacidad. 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, a partir de Windows Vista, Windows utiliza una ID de interfaz

generada aleatoriamente en lugar de una ID de interfaz creada mediante EUI-64. Windows XP y los sistemas operativos Windows anteriores utilizaban EUI-64.

Después de establecer la ID de interfaz, ya sea mediante el proceso EUI-64 o mediante la generación aleatoria, se la puede combinar con un prefijo IPv6 en el mensaje RA para crear una dirección de unidifusión global, como se muestra en la figura 4.

Nota: para garantizar la exclusividad de cualquier dirección IPv6 de unidifusión, el cliente puede usar un proceso denominado "detección de direcciones duplicadas" (DAD). Es similar a una solicitud de ARP para su propia dirección. Si no se obtiene una respuesta, la dirección es única.

Direcciones link-local dinámicas.

Todos los dispositivos IPv6 deben tener direcciones IPv6 link-local. Las direcciones link-local se pueden establecer dinámicamente o se pueden configurar de forma manual como direcciones link-local estáticas.

En la figura 1, se muestra que la dirección link-local fue creada de manera dinámica con el prefijo FE80::/10 y la ID de interfaz mediante el proceso EUI-64 o un número de 64 bits de generación aleatoria. En general, los sistemas operativos usan el mismo método, tanto para una dirección de unidifusión global creada por SLAAC como para una dirección link-local asignada de manera dinámica, como se muestra en la figura 2.

Los routers Cisco crean automáticamente una dirección IPv6 link-local cada vez que se asigna una dirección de unidifusión global a la interfaz. De manera predeterminada, los routers con 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 de enlace local asignadas dinámicamente es su ID de interfaz larga, que dificulta identificar y recordar las direcciones asignadas. En la figura 3, se muestra la dirección MAC en la interfaz GigabitEthernet 0/0 del router R1. Esta dirección se usa para crear de manera dinámica las direcciones link-local en la misma interfaz.

Para que sea más fácil reconocer y recordar estas direcciones en los routers, es habitual configurar las direcciones IPv6 link-local de manera estática en ellos.

Direcciones link-local estáticas.

Configurar la dirección link-local manualmente permite crear una dirección reconocible y más fácil de recordar. Por lo general, solo es necesario crear direcciones de enlace local reconocibles en los routers. Esto es útil, ya que utilizan direcciones de enlace local del router como direcciones de gateway predeterminado y en los mensajes routing de anuncios.

Las direcciones link-local pueden configurarse manualmente mediante el mismo comando de interfaz utilizado para crear las direcciones IPv6 de unidifusión globales, pero con un parámetro link-local adicional. Cuando una dirección comienza con este hexteto dentro del rango de FE80 a FEBF, el parámetro de link-local debe seguir a la dirección.

En la ilustración, se muestra la configuración de una dirección link-local con el comando de interfaz ipv6 address. La dirección link-local FE80::1 se utiliza para que sea posible reconocer fácilmente que pertenece al router R1. Se configura la misma dirección IPv6 link-local en todas las interfaces del R1. Se puede configurar FE80::1 en cada enlace, debido a que solamente tiene que ser única en ese enlace.

De manera similar al R1, el router R2 se configura con FE80::2 como la dirección IPv6 link-local en todas las interfaces.

Verificación de la configuración de la dirección IPv6.

Como se muestra en la figura 1, el comando para verificar la configuración de la interfaz IPv6 es similar al comando que se utiliza para IPv4.

El comando **show interface** muestra la dirección MAC de las interfaces Ethernet. EUI-64 utiliza esta dirección MAC para generar la ID de interfaz para la dirección link-local. Además, el comando **show ipv6 interface brief** muestra el resultado abreviado para cada una de las interfaces. El resultado **[up/up]** en la misma línea que la interfaz indica el estado de interfaz de la capa 1 y la capa 2. Esto es lo mismo que las columnas **Status** Estado y **Protocol** (Protocolo) en el comando IPv4 equivalente.

Observe que cada interfaz tiene dos direcciones IPv6. La segunda dirección para cada interfaz es la dirección de unidifusión global que se configuró. La primera dirección, la que comienza con FE80, es la dirección de unidifusión link-local para la interfaz. Recuerde que la dirección link-local se agrega automáticamente a la interfaz cuando se asigna una dirección de unidifusión global.

Además, observe que la dirección link-local Serial 0/0/0 de R1 es igual a la interfaz GigabitEthernet 0/0. Las interfaces seriales no tienen direcciones MAC de Ethernet, por lo que Cisco IOS usa la dirección MAC de la primera interfaz Ethernet disponible. Esto es posible porque las interfaces link-local solo deben ser únicas en ese enlace.

La dirección link-local de la interfaz de router suele ser la dirección de gateway predeterminado para los dispositivos en ese enlace o red.

Como se muestra en la figura 2, se puede usar el comando **show ipv6 route** para verificar que las redes IPv6 y las direcciones de interfaz IPv6 específicas se hayan instalado en la tabla de routing IPv6. El comando **show ipv6 route** muestra solamente las redes IPv6, no las redes IPv4.

Dentro de la tabla de rutas, una **C** junto a la ruta indica que es una red conectada directamente. Cuando la interfaz de router se configura con una dirección de unidifusión global y su estado es “up/up”, se agrega el prefijo y la longitud de prefijo IPv6 a la tabla de routing IPv6 como una ruta conectada.

Note: La **L** indica una ruta local, la dirección IPv6 específica asignada a la interfaz. Esta no es una dirección de enlace local. Las direcciones de enlace local no están incluidas en la tabla de routing del router, ya que no son direcciones enrutables.

La dirección IPv6 de unidifusión global configurada en la interfaz también se instala en la tabla de routing como una ruta local. La ruta local tiene un prefijo /128. La tabla de routing utiliza las rutas locales para procesar eficazmente paquetes cuya dirección de destino es la dirección de interfaz del router.

El comando **ping** de IPv6 es idéntico al comando que se usa en IPv4, excepto que se usa una dirección IPv6. Como se muestra en la figura 3, el comando se utiliza para verificar la conectividad de capa 3 entre el R1 y la PC1. Al hacer ping de un router a una dirección link-local, Cisco IOS solicita al usuario la interfaz de salida. Como la dirección link-local de destino puede ser uno o más de sus enlaces o redes, el router debe saber a qué interfaz enviar el comando ping.

Direcciones IPv6 de multidifusión.

Direcciones IPv6 de multidifusión asignadas.

Las direcciones IPv6 de multidifusión son similares a las direcciones IPv4 de multidifusión. Recuerde que las direcciones de multidifusión se utilizan para enviar un único paquete a uno o más destinos (grupo de multidifusión). Las direcciones IPv6 de multidifusión tienen el prefijo FF00::/8.

Nota: las direcciones de multidifusión solo pueden ser direcciones de destino y no direcciones de origen.

Existen dos tipos de direcciones IPv6 de multidifusión:

- Dirección de multidifusión asignada
- Dirección de multidifusión de nodo solicitado

Dirección de multidifusión asignada

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

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

- **Grupo de multidifusión FF02::1 para todos los nodos:** este es un grupo de multidifusión 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 difusión en IPv4. En la ilustración, se muestra un ejemplo de comunicación mediante la dirección de multidifusión de todos los nodos. Un router IPv6 envía mensajes de RA de protocolo de mensajes de control de Internet versión 6 (ICMPv6) al grupo de multidifusión de todos los nodos. El mensaje RA proporciona a todos los dispositivos en la red con IPv6 habilitado la información de direccionamiento, como el prefijo, la longitud de prefijo y el gateway predeterminado.
- **Grupo de multidifusión FF02::2 para todos los nodos:** este es un grupo de multidifusión al que se unen todos los routers IPv6. Un router comienza a formar parte de este grupo cuando se lo habilita como router IPv6 con 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 de multidifusión de todos los routers. El mensaje RS solicita un mensaje RA del router IPv6 para contribuir a la configuración de direcciones del dispositivo.

Direcciones IPv6 de multidifusión de nodo solicitado.

Una dirección de multidifusión de nodo solicitado es similar a una dirección de multidifusión de todos los nodos. La ventaja de una dirección de multidifusión de nodo solicitado es que se asigna a una dirección especial de multidifusión de Ethernet. Esto permite que la NIC Ethernet filtre el marco al examinar la dirección MAC de destino sin enviarla al proceso de IPv6 para ver si el dispositivo es el objetivo previsto del paquete IPv6.

ICMP.

ICMPv4 e ICMPv6.

Si bien IP es solo un protocolo de máximo esfuerzo, el paquete TCP/IP permite que los mensajes se envíen en caso de que se produzcan determinados errores. Estos mensajes se envían mediante los servicios de ICMP. El objetivo de estos mensajes es proporcionar respuestas acerca de temas relacionados con el procesamiento de paquetes IP en determinadas condiciones, no es hacer que IP sea confiable. Los mensajes de ICMP no son obligatorios y, a menudo, no se permiten dentro de una red por razones de seguridad.

El protocolo ICMP está disponible tanto para IPv4 como para IPv6. El protocolo de mensajes para IPv4 es ICMPv4. ICMPv6 proporciona estos mismos servicios para IPv6, pero incluye funcionalidad adicional. En este curso, el término ICMP se utilizará para referirse tanto a ICMPv4 como a ICMPv6.

Existe una gran variedad de tipos de mensajes de ICMP y de razones para enviarlos. Analizaremos algunos de los mensajes más comunes.

Los mensajes ICMP comunes a ICMPv4 y a ICMPv6 incluyen lo siguiente:

- Confirmación de host
- Destino o servicio inaccesible
- Tiempo superado
- Redireccionamiento de ruta

Confirmación de host

Se puede utilizar un mensaje de eco ICMP para determinar si un host funciona. El host local envía una solicitud de eco ICMP a un host. Si el host se encuentra disponible, el host de destino responde con una respuesta de eco. En la ilustración, haga clic en el botón Reproducir para ver una animación de la solicitud de eco/respuesta de eco ICMP. Este uso de los mensajes de eco ICMP es la base de la utilidad ping.

Destino o servicio inaccesible

Cuando un host o gateway recibe un paquete que no puede entregar, puede utilizar un mensaje ICMP de destino inalcanzable para notificar al origen que el destino o el servicio son inalcanzables. El mensaje incluye un código que indica el motivo por el cual no se pudo entregar el paquete.

Algunos de los códigos de destino inalcanzable para ICMPv4 son los siguientes:

- 0: red inalcanzable
- 1: host inalcanzable
- 2: protocolo inalcanzable
- 3: puerto inalcanzable

Nota: ICMPv6 tiene códigos similares, pero levemente diferentes para los mensajes de destino inalcanzable.

Tiempo superado

Los routers utilizan los mensajes de tiempo superado de ICMPv4 para indicar que un paquete no puede reenviarse debido a que el campo de tiempo de duración (TTL) del paquete se disminuyó a 0. Si un router recibe un paquete y disminuye el campo TTL en el paquete IPV4 a cero, descarta el paquete y envía un mensaje de tiempo superado al host de origen.

ICMPv6 también envía un mensaje de tiempo superado si el router no puede reenviar un paquete IPv6 debido a que el paquete caducó. IPv6 no tiene un campo TTL, por lo que utiliza el campo de límite de saltos para determinar si el paquete caducó.

Mensajes de solicitud y de anuncio de router de ICMPv6.

Los mensajes informativos y de error que se encuentran en ICMPv6 son muy similares a los mensajes de control y de error que implementa ICMPv4. Sin embargo, ICMPv6 tiene nuevas características y funcionalidad mejorada que no se encuentran en ICMPv4. Los mensajes ICMPv6 están encapsulados en IPv6.

ICMPv6 incluye cuatro protocolos nuevos como parte del protocolo de detección de vecino (ND o NDP).

Mensajería entre un router IPv6 y un dispositivos IPv6:

- Mensaje de solicitud de router (RS)
- Mensaje de anuncio de router (RA)

Mensajería entre dispositivos IPv6:

- Mensaje de solicitud de vecino (NS)
- Mensaje de anuncio de vecino (NA)

Nota: El ND de ICMPv6 también incluye el mensaje de redireccionamiento, que tiene una función similar al mensaje de redireccionamiento utilizado en ICMPv4.

En la figura 1, se muestra un ejemplo de una PC y un router que intercambian mensajes de anuncio de router y de solicitud. Haga clic en cada mensaje para obtener más información.

Los mensajes de solicitud y anuncio de vecino se usan para la resolución de direcciones y para la detección de direcciones duplicadas (DAD).

Resolución de direcciones

La resolución de direcciones se utiliza cuando un dispositivo en la LAN conoce la dirección IPv6 de unidifusión de un destino, pero no conoce la dirección MAC de Ethernet. Para determinar la dirección MAC del destino, el dispositivo envía un mensaje de NS a la dirección de nodo solicitado. El mensaje incluye la dirección IPv6 conocida (objetivo). El dispositivo que se destinó a la dirección IPv6 responde con un mensaje NA que contiene la dirección MAC de Ethernet. En la figura 2, se muestran dos PC que intercambian mensajes de NS y NA. Haga clic en cada mensaje para obtener más información.

Detección de direcciones duplicadas

Cuando se asigna una dirección de unidifusión global o link-local a un dispositivo, se recomienda realizar una operación DAD en la dirección para garantizar que sea única. Para verificar la singularidad de una dirección, el dispositivo envía un mensaje de NS con su propia dirección IPv6 como dirección IPv6 de destino, como

se muestra en la figura 3. Si otro dispositivo de la red tiene esta dirección, responde con un mensaje NA. Este mensaje NA notifica al dispositivo emisor que la dirección está en uso. Si no se devuelve un mensaje NA correspondiente dentro de determinado período, la dirección de unidifusión es única y su uso es aceptable.

Nota: no es necesaria la operación DAD, pero la RFC 4861 recomienda que se realice una DAD en las direcciones de unidifusión.

Prueba y verificación.

Ping: Prueba de la pila local.

Ping es una utilidad de prueba que utiliza mensajes de solicitud y de respuesta de eco ICMP para probar la conectividad entre hosts. Ping funciona con hosts IPv4 e IPv6.

Para probar la conectividad con otro host de una red, se envía una solicitud de eco a la dirección de host mediante el comando ping. Si el host en la dirección especificada recibe la solicitud de eco, responde con una respuesta de eco. A medida que se recibe cada respuesta de eco, el comando ping proporciona comentarios acerca del tiempo transcurrido entre el envío de la solicitud y la recepción de la respuesta. Esto puede ser una medida del rendimiento de la red.

El comando ping tiene un valor de tiempo de espera para la respuesta. Si no se recibe una respuesta dentro del tiempo de espera, el comando ping proporciona un mensaje que indica que no se recibió una respuesta. Generalmente, esto indica que existe un problema, pero también podría indicar que se habilitaron características de seguridad que bloquean los mensajes ping en la red.

Una vez que se envían todas las solicitudes, la utilidad ping proporciona un resumen que incluye la tasa de éxito y el tiempo promedio del viaje de ida y vuelta al destino.

Ping del bucle invertido local

Existen casos especiales de prueba y verificación para los cuales se puede usar el comando ping. Un caso es la prueba de la configuración interna de IPv4 o de IPv6 en el host local. Para realizar esta prueba, se debe hacer ping a la dirección de bucle invertido local 127.0.0.1 para IPv4 (::1 para IPv6). En la ilustración, se muestra la prueba de la dirección IPv4 de bucle invertido.

Una respuesta de 127.0.0.1 para IPv4 (o ::1 para IPv6) indica que IP está instalado correctamente en el host. Esta respuesta proviene de la capa de red. Sin embargo, esta respuesta no indica que las direcciones, las máscaras o los gateways estén configurados adecuadamente. Tampoco indica nada acerca del estado de la capa inferior de la pila de red. Simplemente, prueba el protocolo IP en la capa de red de dicho protocolo. Un mensaje de error indica que TCP/IP no funciona en el host.

Una posibilidad es que se haya configurado la dirección de gateway incorrecta en el host. Otra posibilidad es que la interfaz del router puede estar en funcionamiento, pero se le ha aplicado seguridad, de manera que no procesa o responde solicitudes de ping.

Ping: Prueba de la conectividad a la LAN local.

También es posible utilizar el comando ping para probar la capacidad de comunicación de un host en la red local. Por lo general, esto se realiza haciendo ping a la dirección IP del gateway del host. Un ping al gateway indica que la interfaz del host y la interfaz del router que cumplen la función de gateway funcionan en la red local.

Para esta prueba, se suele usar la dirección de gateway porque el router generalmente está en funcionamiento. Si la dirección de gateway no responde, se puede enviar un ping a la dirección IP de otro host en la red local que se sepa que funciona.

Si el gateway u otro host responden, los hosts locales pueden comunicarse correctamente en la red local. Si el gateway no responde pero otro host sí lo hace, esto podría indicar un problema con la interfaz de router que sirve como gateway.

Una posibilidad es que se haya configurado la dirección de gateway incorrecta en el host. Otra posibilidad es que la interfaz del router puede estar en funcionamiento, pero se le ha aplicado seguridad, de manera que no procesa o responde solicitudes de ping.

Ping: Prueba de la conectividad a una red remota.

También se puede utilizar el comando ping para probar la capacidad de un host local para comunicarse en una interconexión de redes. El host local puede hacer ping a un host IPv4 operativo de una red remota, como se muestra en la ilustración.

Si este ping se realiza correctamente, se puede verificar el funcionamiento de una amplia porción de la interconexión de redes. Un ping correcto en una interconexión de redes confirma la comunicación en la red local, el funcionamiento del router que sirve como gateway y el funcionamiento de todos los routers que podrían estar en la ruta entre la red local y la red del módulo remoto de E/S.

De manera adicional, se puede verificar la funcionalidad del módulo remoto de E/S. Si el módulo remoto de E/S no podía comunicarse fuera de la red local, no hubiera respondido.

Nota: muchos administradores de redes limitan o prohíben la entrada de mensajes ICMP a la red de la empresa; por lo tanto, la falta de una respuesta de ping puede ser por razones de seguridad.

Traceroute: Prueba de la ruta.

El comando ping se usa para probar la conectividad entre dos hosts, pero no proporciona información sobre los detalles de los dispositivos entre los hosts. Traceroute (tracert) es una utilidad que genera una lista de saltos que se alcanzaron correctamente a lo largo de la ruta. Esta lista puede proporcionar información importante sobre la verificación y la solución de problemas. Si los datos llegan al destino, el rastreo indica la interfaz de cada router que aparece en

la ruta entre los hosts. Si los datos fallan en algún salto a lo largo del camino, la dirección del último router que respondió al rastreo puede indicar dónde se encuentra el problema o las restricciones de seguridad.

Tiempo de ida y vuelta (RTT)

El uso de traceroute proporciona el tiempo de ida y vuelta para cada salto a lo largo de la ruta e indica si un salto no responde. El tiempo de ida y vuelta es el tiempo que le lleva a un paquete llegar al módulo remoto de E/S y el tiempo que la respuesta del host demora en regresar. Se utiliza un asterisco (*) para indicar un paquete perdido o sin respuesta.

Esta información se puede utilizar para ubicar un router problemático en la ruta. Si en la pantalla se muestran tiempos de respuesta elevados o pérdidas de datos de un salto en particular, esto constituye un indicio de que los recursos del router o sus conexiones pueden estar sobrecargados.

TTL de IPv4 y límite de saltos de IPv6

Traceroute utiliza una función del campo TTL en IPv4 y del campo límite de saltos de IPv6 en los encabezados de capa 3, junto con el mensaje de tiempo superado de ICMP.

La primera secuencia de mensajes enviados desde traceroute tiene un valor de 1 en el campo TTL. Esto hace que el TTL agote el tiempo de espera del paquete IPv4 en el primer router. Este router luego responde con un mensaje de ICMPv4. Traceroute ahora tiene la dirección del primer salto.

A continuación, Traceroute incrementa progresivamente el campo TTL (2, 3, 4...) para cada secuencia de mensajes. De esta manera se proporciona al rastreo la dirección de cada salto a medida que los paquetes agotan el límite de tiempo a lo largo del camino. El campo TTL sigue aumentando hasta que se alcanza el destino, o se incrementa a un máximo predefinido.

Después de alcanzar el destino final, el host responde con un mensaje ICMP de puerto inalcanzable o con un mensaje ICMP de respuesta de eco en lugar del mensaje ICMP de tiempo superado.