Capítulo 8: DHCP

Todo dispositivo que se conecta a una red necesita una dirección IP única. Los administradores de red asignan direcciones IP estáticas a los routers, a los servidores, a las impresoras y a otros dispositivos de red cuyas ubicaciones (físicas y lógicas) probablemente no cambien. Por lo general, se trata de dispositivos que proporcionan servicios a los usuarios y dispositivos en la red. Por lo tanto, las direcciones que se les asignan se deben mantener constantes. Además, las direcciones estáticas habilitan a los administradores para que administren estos dispositivos en forma remota. A los administradores de red les resulta más fácil acceder a un dispositivo cuando pueden determinar fácilmente su dirección IP.

Sin embargo, las computadoras y los usuarios en una organización, a menudo, cambian de ubicación, física y lógicamente. Para los administradores de red, asignar direcciones IP nuevas cada vez que un empleado cambia de ubicación puede ser difícil y llevar mucho tiempo. Además, para los empleados móviles que trabajan desde ubicaciones remotas, puede ser difícil establecer de forma manual los parámetros de red correctos. Incluso para los clientes de escritorio, la asignación manual de direcciones IP y otra información de direccionamiento plantea una carga administrativa, especialmente a medida que crece la red.

Introducción a DHCPv4

DHCPv4 asigna direcciones IPv4 y otra información de configuración de red en forma dinámica. Dado que los clientes de escritorio suelen componer gran parte de los nodos de red, DHCPv4 es una herramienta extremadamente útil para los administradores de red y que ahorra mucho tiempo.

Un servidor de DHCPv4 dedicado es escalable y relativamente fácil de administrar. Sin embargo, en una sucursal pequeña o ubicación SOHO, se puede configurar un router Cisco para proporcionar servicios DHCPv4 sin necesidad de un servidor dedicado. El software Cisco IOS admite un servidor DHCPv4 con funciones completas opcional.

El servidor DHCPv4 asigna dinámicamente, o arrienda, una dirección IPv4 de un conjunto de direcciones durante un período limitado elegido por el servidor o hasta que el cliente ya no necesite la dirección.

Los clientes arriendan la información del servidor durante un período definido administrativamente. Los administradores configuran los servidores de DHCPv4 para establecer los arrendamientos, a fin de que caduquen a distintos intervalos. El arrendamiento típicamente dura de 24 horas a una semana o más. Cuando caduca el arrendamiento, el cliente debe solicitar otra dirección, aunque generalmente se le vuelve a asignar la misma.

Funcionamiento de DHCPv4

Cuando un cliente se comunica con un servidor de DHCPv4, el servidor asigna o arrienda una dirección IPv4 a ese cliente. El cliente se conecta a la red con esa dirección IP arrendada hasta que caduque el

arrendamiento. El cliente debe ponerse en contacto con el servidor de DHCP periódicamente para extender el arrendamiento. Este mecanismo de arrendamiento asegura que los clientes que se trasladan o se desconectan no mantengan las direcciones que ya no necesitan. Cuando caduca un arrendamiento, el servidor de DHCP devuelve la dirección al conjunto, donde se puede volver a asignar según sea necesario.

Origen del arrendamiento

Cuando el cliente arranca (o quiere unirse a una red), comienza un proceso de cuatro pasos para obtener un arrendamiento

Detección de DHCP (DHCPDISCOVER)

El mensaje DHCPDISCOVER encuentra los servidores de DHCPv4 en la red. Dado que el cliente no tiene información de IPv4 válida durante el arranque, utiliza direcciones de difusión de capa 2 y de capa 3 para comunicarse con el servidor.

Oferta de DHCP (DHCPOFFER)

Cuando el servidor de DHCPv4 recibe un mensaje DHCPDISCOVER, reserva una dirección IPv4 disponible para arrendar al cliente. El servidor también crea una entrada ARP que consta de la dirección MAC del cliente que realiza la solicitud y la dirección IPv4 arrendada del cliente.

Solicitud de DHCP (DHCPREQUEST)

Cuando el cliente recibe el mensaje DHCPOFFER proveniente del servidor, envía un mensaje DHCPREQUEST

Este mensaje se utiliza tanto para el origen como para la renovación del arrendamiento. Cuando se utiliza para el origen del arrendamiento, el mensaje DHCPREQUEST sirve como notificación de aceptación vinculante al servidor seleccionado para los parámetros que ofreció y como un rechazo implícito a cualquier otro servidor que pudiera haber proporcionado una oferta vinculante al cliente.

Acuse de recibo de DHCP (DHCPACK)

Al recibir el mensaje DHCPREQUEST, el servidor verifica la información del arrendamiento con un ping ICMP a esa dirección para asegurarse de que no esté en uso, crea una nueva entrada ARP para el arrendamiento del cliente y responde con un mensaje DHCPACK,

El mensaje DHCPACK es un duplicado del mensaje DHCPOFFER, a excepción de un cambio en el campo de tipo de mensaje. Cuando el cliente recibe el mensaje DHCPACK, registra la información de configuración y realiza una búsqueda de ARP para la dirección asignada. Si no hay respuesta al ARP, el cliente sabe que la dirección IPv4 es válida y comienza a utilizarla como propia.

Renovación del arrendamiento

Solicitud de DHCP (DHCPREQUEST)

Antes de que caduque el arrendamiento, el cliente envía un mensaje DHCPREQUEST directamente al servidor de DHCPv4 que ofreció la dirección IPv4 en primera instancia. Si no se recibe un mensaje DHCPACK dentro de una cantidad de tiempo especificada, el cliente transmite otro mensaje DHCPREQUEST de modo que uno de los otros servidores de DHCPv4 pueda extender el arrendamiento.

Acuse de recibo de DHCP (DHCPACK)

Al recibir el mensaje DHCPREQUEST, el servidor verifica la información del arrendamiento al devolver un DHCPACK

Mensajes Discover (Detección) y Offer (Oferta) de DHCPv4

Si un cliente está configurado para recibir su configuración IPv4 dinámicamente y desea unirse a la red, solicita valores de direccionamiento del servidor de DHCPv4. El cliente transmite un mensaje DHCPDISCOVER en su red local cuando arranca o detecta una conexión de red activa. Dado que el cliente no tiene forma de obtener información acerca de la subred a la que pertenece, el mensaje DHCPDISCOVER es una difusión IPv4 (dirección IPv4 de destino 255.255.255.255). El cliente aún no tiene una dirección IPv4 configurada, de modo que se utiliza la dirección IPv4 de origen 0.0.0.0.

Cuando el servidor de DHCPv4 recibe el mensaje DHCPDISCOVER, responde con un mensaje DHCPOFFER. Este mensaje incluye información de configuración inicial para el cliente, como la dirección IPv4 que el servidor ofrece, la máscara de subred, la duración del arrendamiento y la dirección IPv4 del servidor de DHCPv4 que hace la oferta.

Es posible configurar el mensaje DHCPOFFER para que incluya otra información, como el tiempo de renovación del arrendamiento y la dirección DNS.

Configuración de un servidor de DHCPv4 básico

Un router Cisco que ejecuta el software IOS de Cisco puede configurarse para que funcione como servidor de DHCPv4. El servidor de DHCPv4 que utiliza IOS de Cisco asigna y administra direcciones IPv4 de conjuntos de direcciones especificados dentro del router para los clientes DHCPv4

Paso 1: Excluir direcciones IPv4

El router que funciona como servidor de DHCPv4 asigna todas las direcciones IPv4 en un conjunto de direcciones DHCPv4, a menos que esté configurado para excluir direcciones específicas. Generalmente, algunas direcciones IPv4 de un conjunto se asignan a dispositivos de red que requieren asignaciones de direcciones estáticas. Por lo tanto, estas direcciones IPv4 no deben asignarse a otros dispositivos. Para excluir direcciones específicas, utilice el comando **ip dhcp excluded-address**,

Paso 2: Configurar un pool de DHCPv4

La configuración de un servidor de DHCPv4 implica definir un conjunto de direcciones que se deben asignar.

Paso 3: Configurar tareas específicas

El conjunto de direcciones y el router de gateway predeterminado deben estar configurados. Utilice la instrucción **network** para definir el rango de direcciones disponibles.

Utilice el comando **default-router** para definir el router de gateway predeterminado. Normalmente, el gateway es la interfaz LAN del router más cercano a los dispositivos clientes. Se requiere un gateway, pero se pueden indicar hasta ocho direcciones si hay varios gateways.

Otros comandos del pool de DHCPv4 son optativos. Por ejemplo, la dirección IPv4 del servidor DNS que está disponible para un cliente DHCPv4 se configura mediante el comando **dns-server**. El comando **domain-name** *dominio* se utiliza para definir el nombre de dominio. La duración del arrendamiento de

DHCPv4 puede modificarse mediante el comando **lease**. El valor de arrendamiento predeterminado es un día. El comando **netbios-name-server** se utiliza para definir el servidor WINS con NetBIOS.

Deshabilitación de DHCPv4

El servicio DHCPv4 está habilitado de manera predeterminada. Para deshabilitar el servicio, utilice el comando del modo de configuración global **no service dhcp**. Utilice el comando del modo de configuración global **service dhcp** para volver a habilitar el proceso del servidor de DHCPv4. Si los parámetros no se configuran, habilitar el servicio no tiene ningún efecto.

Verificación de DHCPv4

El comando **show running-config | section dhcp**, se muestran los comandos de DHCPv4 configurados en el R1. El parámetro **| section** muestra solamente los comandos asociados a la configuración de DHCPv4.

Como se muestra en la figura 3, se puede verificar el funcionamiento de DHCPv4 mediante el comando **show ip dhcp binding**. Este comando muestra una lista de todas las vinculaciones de la dirección IPv4 con la dirección MAC que fueron proporcionadas por el servicio DHCPv4.

El segundo comando, **show ip dhcp server statistics**, se utiliza para verificar si el router recibe o envía los mensajes. Este comando muestra información de conteo con respecto a la cantidad de mensajes DHCPv4 que se enviaron y recibieron.

Retransmisión de DHCPv4

¿Qué es la retransmisión de DHCP?

En una red jerárquica compleja, los servidores empresariales suelen estar ubicados en una granja de servidores. Estos servidores pueden proporcionar servicios DHCP, DNS, TFTP y FTP para la red. Generalmente, los clientes de red no se encuentran en la misma subred que esos servidores. Para ubicar los servidores y recibir servicios, los clientes con frecuencia utilizan mensajes de difusión.

Por esta razón los routers, no envían mensajes de difusión. Como solución a este problema, un administrador puede agregar servidores de DHCPv4 en todas las subredes. Sin embargo, ejecutar estos servicios en varias computadoras genera un costo adicional y sobrecarga administrativa.

Una mejor solución consiste en configurar una dirección de ayuda de IOS de Cisco. Esta solución permite que el router reenvíe difusiones de DHCPv4 al servidor de DHCPv4. Cuando un router reenvía solicitudes de asignación/parámetros de direcciones, actúa como agente de retransmisión DHCPv4

DHCPv4 no es el único servicio que puede configurarse para que retransmita el router. De manera predeterminada, el comando **ip helper-address** reenvía los siguientes ocho siguientes servicios UDP:

- Puerto 37: Tiempo
- Puerto 49: TACACS
- Puerto 53: DNS
- Puerto 67: cliente DHCP/BOOTP
- Puerto 68: servidor de DHCP/BOOTP

- Puerto 69: TFTP
- Puerto 137: servicio de nombres NetBIOS
- Puerto 138: servicio de datagrama NetBIOS

Configuración de un router como cliente DHCPv4

En ocasiones, los routers Cisco en oficinas pequeñas y oficinas domésticas (SOHO) y en los sitios de sucursales deben configurarse como clientes DHCPv4 de manera similar a los equipos cliente. El método específico utilizado depende del ISP. Sin embargo, en su configuración más simple, se utiliza la interfaz Ethernet para conectarse a un cable módem o a un módem DSL. Para configurar una interfaz Ethernet como cliente DHCP, utilice el comando del modo de configuración de interfaz **ip address dhcp**.

Configuración de un router inalámbrico como cliente DHCPv4

Normalmente, los routers inalámbricos para uso en el hogar o una oficina pequeña se conectan a un ISP mediante un cable módem o DSL. En la mayoría de los casos, los routers inalámbricos se configuran para recibir información de direccionamiento IPv4 automáticamente desde el ISP.

Tareas de resolución de problemas

Los problemas de DHCPv4 pueden surgir debido a diversos motivos, como defectos de software en los sistemas operativos, controladores de NIC o agentes de retransmisión DHCP. Sin embargo, la causa más frecuente son los problemas de configuración. Debido a la cantidad de áreas posiblemente problemáticas, se requiere adoptar un enfoque sistemático a la resolución de problemas.

Tarea 1 de la resolución de problemas: resolver conflictos de direcciones IPv4

El arrendamiento de una dirección IPv4 puede caducar en un cliente que aún está conectado a una red. Si el cliente no renueva el arrendamiento, el servidor de DHCPv4 puede volver a asignar esa dirección IPv4 a otro cliente. Cuando el cliente se reinicia, solicita una dirección IPv4. Si el servidor de DHCPv4 no responde rápidamente, el cliente utiliza la última dirección IPv4. El problema surge cuando dos clientes utilizan la misma dirección IPv4, lo cual crea un conflicto.

El comando **show ip dhcp conflict** muestra todos los conflictos de direcciones que registran el servidor de DHCPv4. El servidor utiliza el comando **ping** para detectar clientes. El cliente utiliza el protocolo de resolución de direcciones (ARP) para detectar conflictos. Si se detecta un conflicto de dirección, esta última se elimina del pool y no se asigna hasta que un administrador resuelva el conflicto.

Este resultado muestra las direcciones IP que tienen conflictos con el servidor de DHCP. Muestra el método de detección y el tiempo de detección para las direcciones IP en conflicto que ofreció el servidor de DHCP.

Tarea 2 de la resolución de problemas: verificar la conectividad física

Primero, utilice el comando **show interfaces** *interfaz* para confirmar que la interfaz del router que funciona como el gateway predeterminado para el cliente esté en funcionamiento. Si la interfaz tiene otro estado que no sea activado, el puerto no pasa tráfico, incluso solicitudes de cliente DHCP.

Tarea 3 de la resolución de problemas: probar la conectividad mediante una dirección IP estática

Al llevar a cabo la resolución de cualquier problema de DHCPv4, verifique la conectividad de red configurando información de la dirección IPv4 estática en una estación de trabajo cliente. Si la estación de trabajo no puede llegar a los recursos de red con una dirección IPv4 configurada estáticamente, la causa raíz del problema no es DHCPv4. En este punto, es necesario resolver los problemas de conectividad de la red.

Tarea 4 de la resolución de problemas: verificar la configuración de puertos del switch

Si el cliente DHCPv4 no puede obtener una dirección IPv4 del servidor de DHCPv4 durante el inicio, intente obtener una dirección IPv4 del servidor de DHCPv4 forzando manualmente al cliente para que envíe una solicitud de DHCPv4.

Nota: si hay un switch entre el cliente y el servidor de DHCPv4 y el cliente no puede obtener la configuración de DHCP, la causa pueden ser problemas con la configuración de puertos del switch. Estas causas pueden incluir problemas de enlaces troncales y canalización, STP y RSTP. Las configuraciones de PortFast y perimetrales resuelven los problemas de clientes DHCPv4 más comunes que se producen con una instalación inicial de un switch Cisco.

Tarea 5 de la resolución de problemas: probar el funcionamiento de DHCPv4 en la misma subred o VLAN

Es importante distinguir si DHCPv4 funciona correctamente cuando el cliente se encuentra en la misma subred o VLAN que el servidor de DHCPv4. Si DHCPv4 funciona correctamente cuando el cliente se encuentra en la misma subred o VLAN, el problema puede ser el agente de retransmisión DHCP. Si el problema persiste incluso con la prueba de DHCPv4 en la misma subred o VLAN que el servidor de DHCPv4, en realidad puede haber un problema con el servidor de DHCPv4.

Otro comando útil para llevar a cabo la resolución de problemas del funcionamiento de DHCPv4 es el comando **debug ip dhcp server events**. Este comando informa eventos del servidor, como asignaciones de direcciones y actualizaciones de bases de datos.

Configuración automática de dirección independiente del estado (SLAAC)

De manera similar a lo que ocurre con IPv4, las direcciones IPv6 de unidifusión global pueden configurarse manualmente o de forma dinámica. Sin embargo, existen dos métodos en los que las direcciones IPv6 de unidifusión global pueden asignarse dinámicamente:

- Configuración automática de dirección sin estado (SLAAC), como se muestra en la ilustración
- Protocolo de configuración dinámica de host para IPv6 (DHCPv6 con estado)

Introducción a SLAAC

SLAAC es un método en el cual un dispositivo puede obtener una dirección IPv6 de unidifusión global sin los servicios de un servidor de DHCPv6. ICMPv6 se encuentra en el centro de SLAAC. ICMPv6 es similar a ICMPv4, pero incluye funcionalidad adicional y es un protocolo mucho más sólido. SLAAC utiliza

mensajes de solicitud y de anuncio de router ICMPv6 para proporcionar direccionamiento y otra información de configuración que normalmente proporcionaría un servidor de DHCP:

- **Mensaje de solicitud de router (RS):** cuando un cliente está configurado para obtener la información de direccionamiento de forma automática mediante SLAAC, el cliente envía un mensaje RS al router. El mensaje RS se envía a la dirección IPv6 de multidifusión de todos los routers, FF02::2.
- **Mensaje de anuncio de router (RA):** los routers envían mensajes RA para proporcionar información de direccionamiento a los clientes configurados para obtener sus direcciones IPv6 de forma automática. El mensaje RA incluye el prefijo y la longitud de prefijo del segmento local. Un cliente utiliza esta información para crear su propia dirección IPv6 de unidifusión global. Los routers envían mensajes RA de forma periódica o en respuesta a un mensaje RS. De manera predeterminada, los routers Cisco envían mensajes de RA cada 200 segundos. Los mensajes RA siempre se envían a la dirección IPv6 de multidifusión de todos los nodos, FF02::1.

Como lo indica el nombre, SLAAC quiere decir "sin estado". Un servicio sin estado significa que no hay ningún servidor que mantenga la información de la dirección de red. A diferencia de DHCP, no hay servidor de SLAAC que tenga información acerca de cuáles son las direcciones IPv6 que están en uso y cuáles son las que se encuentran disponibles.

Funcionamiento de SLAAC

Un router debe tener el routing IPv6 habilitado antes de poder enviar mensajes RA:

Router(config)# **ipv6 unicast-routing**

El proceso que utiliza el cliente para detectar si una IPv6 se encuentra en uso es mediante un ICMPv6 con una dirección de multicast especialmente creada. Este proceso forma parte de la detección de vecinos ICMPv6 y se conoce como "detección de direcciones duplicadas (DAD)".

Opción de SLAAC

Opción de SLAAC (anuncio de router solamente)

SLAAC es la opción predeterminada en los routers Cisco. Tanto el indicador M como el indicador O están establecidos en 0 en el RA, como se muestra en la ilustración.

Esta opción le indica al cliente que utilice la información que se incluye en el mensaje RA de manera exclusiva. Esto incluye información del prefijo, de la longitud de prefijo, del servidor DNS, de la MTU y del gateway predeterminado. No se encuentra disponible ninguna otra información de un servidor de DHCPv6. La dirección IPv6 de unidifusión global se crea combinando el prefijo del mensaje RA y la ID de interfaz mediante EUI-64 o mediante un valor generado aleatoriamente.

Los mensajes RA se configuran en una interfaz individual de un router. Para volver a habilitar una interfaz para SLAAC que pudo haberse establecido en otra opción, se deben restablecer los indicadores M y O a sus valores iniciales de 0. Esto se realiza mediante los siguientes comandos del modo de configuración de interfaz:

Router(config-if)# **No ipv6 nd managed-config-flag**

Router(config-if)# **no ipv6 nd other-config-flag**

Opción de DHCPv6 sin estado

Si bien DHCPv6 es similar a DHCPv4 en cuanto a lo que proporciona, los dos protocolos son independientes respecto sí. DHCPv6 se define en RFC 3315. Se trabajó mucho en esta especificación a través de los años, como lo indica el hecho de que RFC DHCPv6 tiene el número de revisión más alto que cualquier borrador de Internet.

Opción de DHCPv6 sin estado (anuncio de router y DHCPv6)

La opción de DHCPv6 sin estado informa al cliente que utilice la información del mensaje RA para el direccionamiento, pero que hay más parámetros de configuración disponibles de un servidor de DHCPv6. Mediante el prefijo y la longitud de prefijo en el mensaje RA, junto con EUI-64 o una IID generada aleatoriamente, el cliente crea la dirección IPv6 de unidifusión global.

A continuación, el cliente se comunica con un servidor de DHCPv6 sin estado para obtener información adicional que no se proporciona en el mensaje RA. Puede tratarse de una lista de direcciones IPv6 del servidor DNS, por ejemplo. Este proceso se conoce como DHCPv6 sin estado, debido a que el servidor no mantiene información de estado del cliente (es decir, una lista de direcciones IPv6 asignadas y disponibles). El servidor de DHCPv6 sin estado solo proporciona parámetros de configuración para los clientes, no direcciones IPv6.

.

Para DHCPv6 sin estado, el indicador O se configura en 1 y el indicador M se deja en la configuración predeterminada de 0. El valor 1 del indicador O se utiliza para informarle al cliente que hay información de configuración adicional disponible de un servidor de DHCPv6 sin estado.

Para modificar el mensaje RA enviado en la interfaz de un router e indicar DHCPv6 sin estado, utilice el siguiente comando:

Router(config-if)# **ipv6 nd other-config-flag**

Opción de DHCPv6 con estado

DHCPv6 con estado (DHCPv6 solamente)

Esta opción es la más similar a DHCPv4. En este caso, el mensaje RA le informa al cliente que no utilice la información contenida en el mensaje RA. Toda la información de direccionamiento y de configuración debe obtenerse de un servidor de DHCPv6 con estado. Esto se conoce como DHCPv6 con estado, debido a que el servidor de DHCPv6 mantiene información de estado de IPv6. Esto es similar a la asignación de direcciones para IPv4 por parte de un servidor de DHCPv4.

El indicador M señala si se debe utilizar DHCPv6 con estado o no. El indicador O no interviene. El siguiente comando se utiliza para cambiar el indicador M de 0 a 1 para indicar DHCPv6 con estado:

Router(config-if)# **ipv6 nd managed-config-flag**

Operaciones de DHCPv6

DHCPv6 sin estado o con estado, o ambos, comienzan con un mensaje RA ICMPv6 del router. El mensaje RA puede ser un mensaje periódico o un mensaje solicitado por el dispositivo mediante un mensaje RS.
Si en el mensaje RA se indica DHCPv6 con estado o sin estado, el dispositivo inicia las comunicaciones cliente/servidor DHCPv6.

Comunicaciones DHCPv6

Cuando el mensaje RA indica DHCPv6 sin estado o DHCPv6 con estado, se invoca el funcionamiento de DHCPv6. Los mensajes DHCPv6 se envían a través de UDP. Los mensajes DHCPv6 del servidor al cliente utilizan el puerto de destino UDP 546. El cliente envía mensajes DHCPv6 al servidor mediante el puerto de destino UDP 547.
El cliente, ahora un cliente DHCPv6, necesita ubicar el servidor de DHCPv6. El cliente envía un mensaje DHCPv6 SOLICIT a la dirección IPv6 de multidifusión de todos los servidores de DHCPv6 reservada, FF02::1:2. Esta dirección de multidifusión tiene alcance link-local, lo cual significa que los routers no reenvían los mensajes a otras redes.
Uno o más servidores de DHCPv6 responden con un mensaje de unidifusión DHCPv6 ADVERTISE. El mensaje ADVERTISE le informa al cliente DHCPv6 que el servidor se encuentra disponible para el servicio DHCPv6.
El cliente responde con un mensaje de unidifusión INFORMATION-REQUEST o DHCPv6 REQUEST al servidor, según si utiliza DHCPv6 con estado o DHCPv6 sin estado.

- **Cliente DHCPv6 sin estado:** el cliente envía un mensaje DHCPv6 INFORMATION-REQUEST al servidor de DHCPv6 en el que solicita solamente parámetros de configuración, como la dirección del servidor DNS. El cliente creó su propia dirección IPv6 mediante el uso del prefijo del mensaje RA y una ID de interfaz autogenerada aleatoriamente.
- **Cliente DHCPv6 con estado:** el cliente envía un mensaje DHCPv6 REQUEST al servidor para obtener una dirección IPv6 y todos los demás parámetros de configuración del servidor.

El servidor envía un mensaje de unidifusión DHCPv6 REPLY al cliente que contiene la información solicitada en el mensaje REQUEST o INFORMATION-REQUEST.

Verificación de DHCPv6 sin estado

Verificación del servidor de DHCPv6 sin estado

El comando **show ipv6 dhcp pool** verifica el nombre del pool de DHCPv6 y sus parámetros. La cantidad de clientes activos es 0, porque el servidor no mantiene ningún estado.
El comando **show running-config** también se puede utilizar para verificar todos los comandos que se configuraron anteriormente.

Verificación del cliente DHCPv6 sin estado

En este ejemplo, se utiliza un router como cliente DHCPv6 sin estado. El resultado del comando **show ipv6 interface** muestra que el router tiene "Stateless address autoconfig enabled" (Configuración automática de dirección sin estado habilitada) y una dirección IPv6 de unidifusión global. La dirección

IPv6 de unidifusión global se creó mediante SLAAC, que incluye el prefijo contenido en el mensaje RA. La IID se generó mediante EUI-64. No se utilizó DHCPv6 para asignar la dirección IPv6.

La información de router predeterminado también proviene del mensaje RA. Esta era la dirección IPv6 de origen del paquete que contenía el mensaje RA y la dirección link-local del router.

En el resultado del comando **debug ipv6 dhcp detail**, se muestran los mensajes DHCPv6 intercambiados entre el cliente y el servidor. En este ejemplo, se introdujo el comando en el cliente. Se muestra el mensaje INFORMATION-REQUEST, debido a que se envía desde un cliente DHCPv6 sin estado. Observe que el cliente, el router R3, envía los mensajes DHCPv6 desde su dirección link-local hacia la dirección de todos los agentes de retransmisión y servidores de DHCPv6, FF02::1:2.

El resultado de depuración muestra todos los mensajes DHCPv6 enviados entre el cliente y el servidor, entre los que se incluyen las opciones de servidor DNS y de nombre de dominio que se configuraron en el servidor.

Configuración de un router como servidor de DHCPv6 con estado

Configurar un servidor de DHCPv6 con estado es similar a configurar un servidor sin estado. La diferencia más importante es que un servidor con estado también incluye información de direccionamiento IPv6 de manera similar a un servidor DHCPv4.

Paso 1: Habilitar el routing IPv6

Se requiere el comando **ipv6 unicast-routing** para habilitar el routing IPv6. Este comando no es necesario para que el router sea un servidor de DHCPv6 con estado, pero se requiere para que el router origine los mensajes RA ICMPv6.

Paso 2: Configurar un pool de DHCPv6

El comando **ipv6 dhcp pool** *nombre-del-conjunto* crea un conjunto y el router ingresa al comando de configuración DHCPv6, que se identifica por la línea Router(config-dhcpv6)#.

Paso 3: Configurar los parámetros del pool

Con DHCPv6 con estado, todos los parámetros de direccionamiento y otros parámetros de configuración deben ser asignados por el servidor de DHCPv6. El comando **address prefix** se utiliza para indicar el conjunto de direcciones que debe asignar el servidor. La opción **lifetime** indica el tiempo de arrendamiento válido y preferido en segundos. Al igual que con DHCPv6 sin estado, el cliente utiliza la dirección IPv6 de origen del paquete que contenía el mensaje RA.

Otra información proporcionada por el servidor de DHCPv6 con estado suele incluir la dirección del servidor DNS y el nombre de dominio.

Paso 4: Comandos de interfaz

El comando **ipv6 dhcp server** *nombre-del-conjunto* de interfaz vincula el conjunto de DHCPv6 con la interfaz. El router responde a las solicitudes de DHCPv6 sin estado en esta interfaz con la información incluida en el pool. El indicador M debe cambiarse de 0 a 1 mediante el comando de interfaz **ipv6 nd managed-config-flag**. Esto le informa al dispositivo que no utilice SLAAC, sino que obtenga el direccionamiento IPv6 y todos los parámetros de configuración de un servidor de DHCPv6 con estado.

Configuración de un router como cliente DHCPv6 con estado

Utilice el comando del modo de configuración de interfaz **ipv6 enable** para permitir que el router reciba una dirección link-local para enviar mensajes RS y participe en DHCPv6.
El comando del modo de configuración de interfaz **ipv6 address dhcp** habilita al router para que funcione como cliente DHCPv6 en esta interfaz.

Verificación de DHCPv6 con estado

Verificación del servidor de DHCPv6 con estado
El comando **show ipv6 dhcp pool** verifica el nombre del pool de DHCPv6 y sus parámetros
El comando **show ipv6 dhcp binding**, muestra la vinculación automática entre la dirección link-local del cliente y la dirección asignada por el servidor.

Verificación del cliente DHCPv6 con estado
El resultado del comando **show ipv6 interface** verifica la dirección IPv6 de unidifusión global en el cliente DHCPv6 que asignó el servidor de DHCPv6.

Configuración de un router como agente de retransmisión DHCPv6

Si el servidor de DHCPv6 está ubicado en una red distinta de la del cliente, el router IPv6 puede configurarse como agente de retransmisión DHCPv6. La configuración de un agente de retransmisión DHCPv6 es similar a la configuración de un router IPv4 como retransmisor DHCPv4.
Los mensajes DHCPv6 de los clientes se envían a la dirección IPv6 de multidifusión FF02::1:2. Dirección de todos los agentes de retransmisión y servidores de DHCPv6: esta dirección tiene alcance link-local, lo que significa que los routers no reenvían estos mensajes. El router se debe configurar como agente de retransmisión DHCPv6 para habilitar al cliente y al servidor de DHCPv6 para que se comuniquen.

Configuración del agente de retransmisión DHCPv6
Un agente de retransmisión DHCPv6 se configura mediante el comando **ipv6 dhcp relay destination**. Este comando se configura en la interfaz que interactúa con el cliente DHCPv6, y se utiliza la dirección del servidor de DHCPv6 como destino.

Tareas de resolución de problemas

El proceso de resolución de problemas de DHCPv6 es similar al de DHCPv4.
Tarea 1 de la resolución de problemas: resolver conflictos
De manera similar a lo que sucede con las direcciones IPv4, el arrendamiento de una dirección IPv6 puede caducar en un cliente que aún necesita conectarse a la red. El comando **show ipv6 dhcp conflict** muestra todos los conflictos de direcciones que registra el servidor de DHCPv6 con estado. Si se detecta

un conflicto de dirección IPv6, el cliente, por lo general, elimina la dirección y genera una nueva mediante SLAAC o mediante DHCPv6 con estado.

Tarea 2 de la resolución de problemas: verificar el método de asignación

El comando **show ipv6 interface** *interfaz* se puede utilizar para verificar el método de asignación de direcciones que aparece en el mensaje RA, según lo indica la configuración de los indicadores M y O. Esta información se muestra en las últimas líneas del resultado. Si un cliente no recibe la información de la dirección IPv6 de un servidor de DHCPv6 con estado, esto podría deberse a indicadores M y O incorrectos en el mensaje RA.

Tarea 3 de la resolución de problemas: probar con una dirección IPv6 estática

Al llevar a cabo la resolución de cualquier problema de DHCP, ya sea DHCPv4 o DHCPv6, se puede verificar la conectividad de red mediante la configuración de una dirección IP estática en una estación de trabajo cliente. En el caso de IPv6, si la estación de trabajo no puede llegar a los recursos de red con una dirección IPv6 configurada estáticamente, la causa raíz del problema no es SLAAC o DHCPv6. En este punto, es necesario resolver los problemas de conectividad de la red.

Tarea 4 de la resolución de problemas: verificar la configuración de puertos del switch

Si el cliente DHCPv6 no puede obtener información de un servidor de DHCPv6, verifique que el puerto de switch esté habilitado y funcione correctamente.

Nota: si hay un switch entre el cliente y el servidor de DHCPv6, y el cliente no puede obtener la configuración de DHCP, la causa pueden ser problemas con la configuración de puertos del switch. Estas causas pueden incluir problemas relacionados con los enlaces troncales, la canalización o el árbol de expansión. Mediante la configuración de PortFast y las configuraciones de los puertos perimetrales se resuelven los problemas de cliente DHCPv6 más comunes que se presentan con la instalación inicial de un switch Cisco.

Tarea 5 de la resolución de problemas: probar el funcionamiento de DHCPv6 en la misma subred o VLAN

Si el servidor de DHCPv6 con estado o sin estado funciona correctamente, pero se encuentra en una VLAN o red IPv6 distinta de la del cliente, es posible que el problema sea el agente de retransmisión DHCPv6. El cliente que interactúa con la interfaz en el router debe configurarse con el comando **ipv6 dhcp relay destination**.

Depuración de DHCPv6

Cuando el router está configurado como servidor de DHCPv6 con estado o sin estado, el comando **debug ipv6 dhcp detail** es útil para verificar la recepción y la transmisión de mensajes DHCPV6. Como se muestra en la ilustración, un router DHCPv6 con estado recibió un mensaje SOLICIT de un cliente. El router utiliza la información de direccionamiento en su pool IPV6-STATEFUL para la información de asignación.