# DHCP

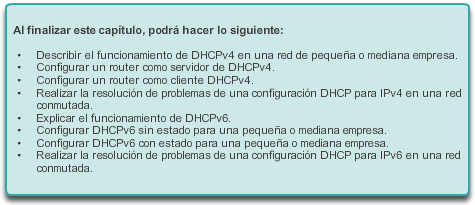
## Introducción

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.

La introducción de un servidor de protocolo de configuración dinámica de host (DHCP) en la red local simplifica la asignación de direcciones IP tanto a los dispositivos de escritorio como a los móviles. El uso de un servidor de DHCP centralizado permite a las organizaciones administrar todas las asignaciones de direcciones IP desde un único servidor. Esta práctica hace que la administración de direcciones IP sea más eficaz y asegura la coherencia en toda la organización, incluso en las sucursales.

DHCP está disponible tanto para IPv4 (DHCPv4) como para IPv6 (DHCPv6). En este capítulo, se explora la funcionalidad, la configuración y la resolución de problemas de DHCPv4 y de DHCPv6.



## Protocolo de configuración dinámica de host v4

### Funcionamiento de DHCPv4

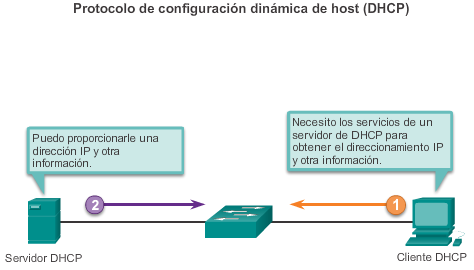
DHCPv4 asigna direcciones IPv4 y otra información de configuración de red en forma dinámica. Dado que los clientes de escritorio suelen componer gran parte de los nodos de red, DHCPv4 es una herramienta extremadamente útil para los administradores de red y ahorra mucho tiempo.

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. Un conjunto de características del IOS de Cisco (denominado “Easy IP”) ofrece un servidor de DHCPv4 optativo con todas las características.

DHCPv4 incluye tres mecanismos diferentes de asignación de direcciones para proporcionar flexibilidad al asignar las direcciones IP:

* **Asignación manual:** el administrador asigna una dirección IPv4 preasignada al cliente, y DHCPv4 comunica solo la dirección IPv4 al dispositivo.
* **Asignación automática:** DHCPv4 asigna automáticamente una dirección IPv4 estática de forma permanente a un dispositivo y la selecciona de un conjunto de direcciones disponibles. No hay arrendamiento, y la dirección se asigna de forma permanente al dispositivo.
* **Asignación dinámica:** 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.

La asignación dinámica es el mecanismo DHCPv4 que se utiliza más comúnmente y es el eje de esta sección. Al utilizar la asignación dinámica, los clientes arriendan la información del servidor durante un período definido administrativamente, como se muestra en la ilustración. 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.



Como se muestra en la figura 1, DHCPv4 funciona en un modo cliente/servidor. 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. Como se muestra en la figura 2, un cliente inicia el proceso con un mensaje de difusión DHCPDISCOVER con su propia dirección MAC para detectar los servidores de DHCPv4 disponibles.

**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. Como se muestra en la figura 3, el servidor de DHCPv4 envía el mensaje DHCPOFFER asignado al cliente que realiza la solicitud. El mensaje DHCPOFFER se envía como una unidifusión, y se utiliza la dirección MAC de capa 2 del servidor como la dirección de origen y la dirección MAC de capa 2 del cliente como el destino.

**Solicitud de DHCP (DHCPREQUEST)**

Cuando el cliente recibe el mensaje DHCPOFFER proveniente del servidor, envía un mensaje DHCPREQUEST, como se muestra en la figura 4. 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.

Muchas redes empresariales utilizan varios servidores de DHCPv4. El mensaje DHCPREQUEST se envía en forma de difusión para informarle a este servidor de DHCPv4 y a cualquier otro servidor de DHCPv4 acerca de la oferta aceptada.

**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 de unidifusión, como se muestra en la figura 5. 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.

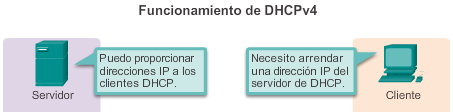
**Renovación del arrendamiento**

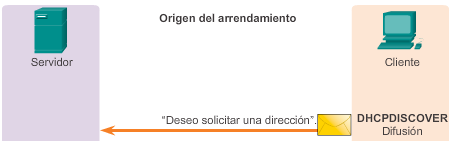
**Solicitud de DHCP (DHCPREQUEST)**

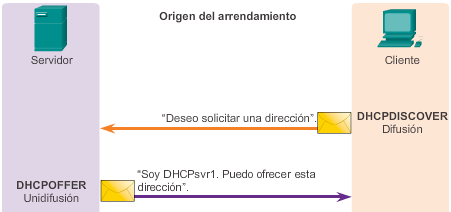
Como se muestra en la figura 6, cuando caduca el arrendamiento, el cliente envía un mensaje DHCPREQUEST directamente al servidor de DHCPv4 que ofreció la dirección IPv4 en primera instancia. Si no se recibe un mensaje DHCPACK dentro de una cantidad de tiempo especificada, el cliente transmite otro mensaje DHCPREQUEST de modo que uno de los otros servidores de DHCPv4 pueda extender el arrendamiento.

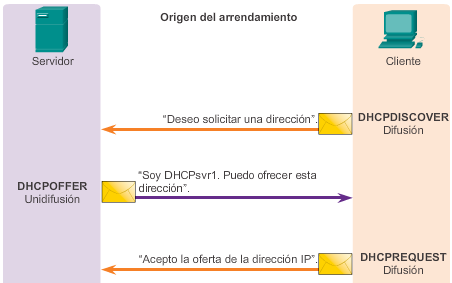
**Acuse de recibo de DHCP (DHCPACK)**

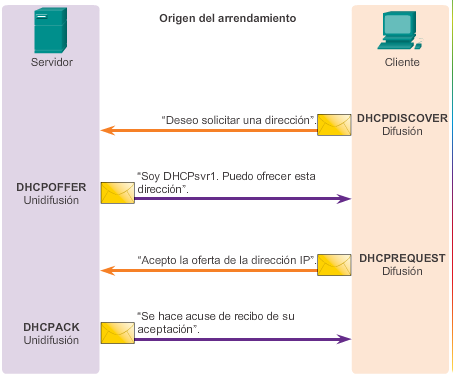
Al recibir el mensaje DHCPREQUEST, el servidor verifica la información del arrendamiento al devolver un DHCPACK, como se muestra en la figura 7.

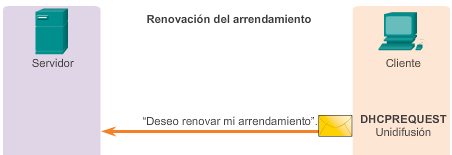


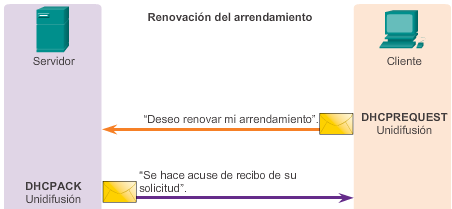








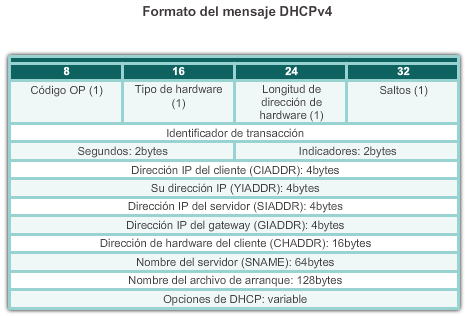




El formato del mensaje DHCPv4 se utiliza para todas las transacciones DHCPv4. Los mensajes DHCPv4 se encapsulan dentro del protocolo de transporte UDP. Los mensajes DHCPv4 que se envían desde el cliente utilizan el puerto de origen UDP 68 y el puerto de destino 67. Los mensajes DHCPv4 que se envían del servidor al cliente utilizan el puerto de origen UDP 67 y el puerto de destino 68.

En la ilustración, se muestra el formato de un mensaje DHCPv4. Los campos son los siguientes:

* **Código de operación (OP):**especifica el tipo de mensaje general. El valor 1 indica un mensaje de solicitud y el valor 2 es un mensaje de respuesta.
* **Tipo de hardware:** identifica el tipo de hardware que se utiliza en la red. Por ejemplo, 1 es Ethernet, 15 es Frame Relay y 20 es una línea serial. Estos son los mismos códigos que se utilizan en mensajes ARP.
* **Longitud de dirección de hardware:**especifica la longitud de la dirección.
* **Saltos:** controla el reenvío de mensajes. Un cliente lo establece en 0 antes de transmitir una solicitud.
* **Identificador de transacción:** lo utiliza el cliente para hacer coincidir la solicitud con respuestas recibidas de los servidores de DHCPv4.
* **Segundos:** identifica la cantidad de segundos transcurridos desde que un cliente comenzó a intentar adquirir o renovar un arrendamiento. Lo utilizan los servidores de DHCPv4 para priorizar respuestas cuando hay varias solicitudes del cliente pendientes.
* **Indicadores:** los utiliza un cliente que no conoce su dirección IPv4 cuando envía una solicitud. Se utiliza solo uno de los 16 bits, que es el indicador de difusión. El valor 1 en este campo le indica al servidor de DHCPv4 o al agente de retransmisión que recibe la solicitud que la respuesta se debe enviar como una difusión.
* **Dirección IP del cliente:** la utiliza un cliente durante la renovación del arrendamiento cuando la dirección del cliente es válida y utilizable, no durante el proceso de adquisición de una dirección. El cliente coloca su propia dirección IPv4 en este campo solamente si tiene una dirección IPv4 válida mientras se encuentra en el estado vinculado. De lo contrario, establece el campo en 0.
* **Su dirección IP:** la utiliza el servidor para asignar una dirección IPv4 al cliente.
* **Dirección IP del servidor:** la utiliza el servidor para identificar la dirección del servidor que debe utilizar el cliente para el próximo paso en el proceso bootstrap, que puede ser, o no, el servidor que envía esta respuesta. El servidor emisor siempre incluye su propia dirección IPv4 en un campo especial llamado opción DHCPv4 Server Identifier (Identificador de servidores DHCPv4).
* **Dirección IP del gateway:** enruta los mensajes DHCPv4 cuando intervienen los agentes de retransmisión DHCPv4. La dirección del gateway facilita las comunicaciones de las solicitudes y respuestas de DHCPv4 entre el cliente y un servidor que se encuentran en distintas subredes o redes.
* **Dirección de hardware del cliente:** especifica la capa física del cliente.
* **Nombre del servidor:** lo utiliza el servidor que envía un mensaje DHCPOFFER o DHCPACK. El servidor puede, de manera optativa, colocar su nombre en este campo. Puede tratarse de un simple apodo de texto o un nombre de dominio DNS, como dhcpserver.netacad.net.
* **Nombre del archivo de arranque:** lo utiliza un cliente de manera optativa para solicitar un determinado tipo de archivo de arranque en un mensaje DHCPDISCOVER. Lo utiliza un servidor en un DHCPOFFER para especificar completamente un directorio de archivos y un nombre de archivo de arranque.
* **Opciones de DHCP:** contiene las opciones de DHCP, incluidos varios parámetros requeridos para el funcionamiento básico de DHCP. Este campo es de longitud variable. Tanto el cliente como el servidor pueden utilizarlo.



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.

Como se muestra en la figura 1, la dirección IPv4 del cliente (CIADDR), la dirección de gateway predeterminado (GIADDR) y la máscara de subred están marcados para indicar que se utiliza la dirección 0.0.0.0.

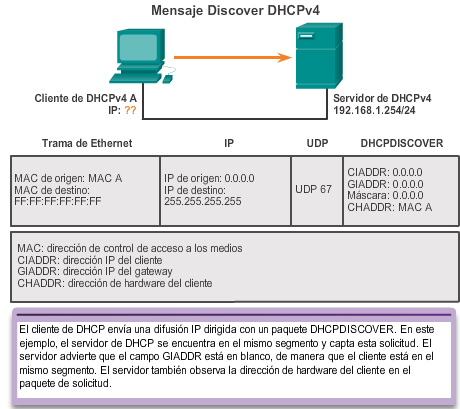
**Nota:** la información desconocida se envía como 0.0.0.0.

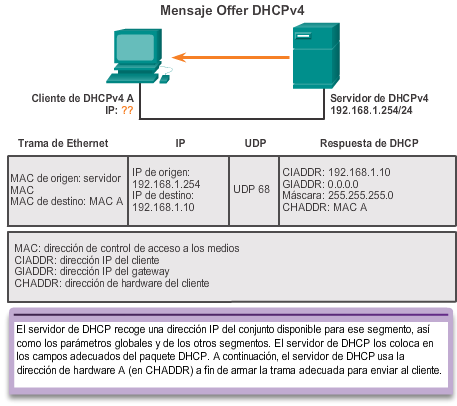
Cuando el servidor de DHCPv4 recibe el mensaje DHCPDISCOVER, responde con un mensaje DHCPOFFER. Este mensaje incluye información de configuración inicial para el cliente, como la dirección IPv4 que el servidor ofrece, la máscara de subred, la duración del arrendamiento y la dirección IPv4 del servidor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

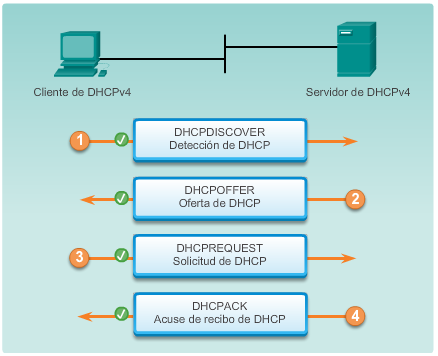
Es posible configurar el mensaje DHCPOFFER para que incluya otra información, como el tiempo de renovación del arrendamiento y la dirección DNS.

Como se muestra en la figura 2, el servidor de DHCP responde al mensaje DHCPDISCOVER asignando valores a la CIADDR y a la máscara de subred. La trama se crea mediante la dirección de hardware del cliente (CHADDR) y se envía al cliente que realiza la solicitud.

El cliente y el servidor envían mensajes de acuse de recibo, y finaliza el proceso.







### 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. La topología que se muestra en la figura 1 se utiliza para ilustrar esta funcionalidad.

**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**, como se muestra en la figura 2.

Se puede excluir una única dirección o un rango de direcciones especificando la dirección más baja y la dirección más alta del rango. Las direcciones excluidas deben incluir las direcciones asignadas a los routers, a los servidores, a las impresoras y a los demás dispositivos que se configuraron manualmente.

**Paso 2. Configurar un pool de DHCPv4**

La configuración de un servidor de DHCPv4 implica definir un conjunto de direcciones que se deben asignar. Como se muestra en la figura 3, el comando **ip dhcp pool***nombre-pool* crea un pool con el nombre especificado e ingresa el router en el modo de configuración DHCPv4, que se identifica por la petición de entrada Router(dhcp-config)#.

**Paso 3. Configurar tareas específicas**

En la figura 4, se indican las tareas para finalizar la configuración del pool de DHCPv4. Algunas de ellas son optativas, mientras que otras deben configurarse.

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.

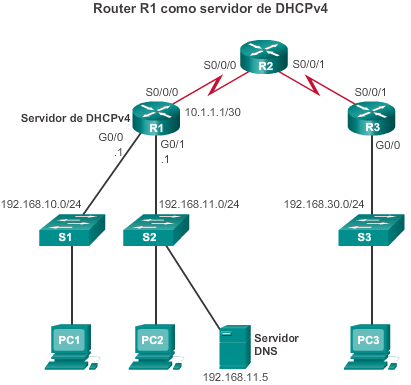
**Ejemplo de DHCPv4**

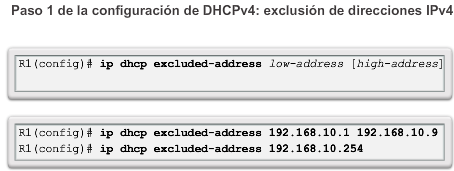
En la figura 5, se utiliza la topología de ejemplo de la figura 1 para mostrar una configuración de ejemplo con parámetros básicos de DHCPv4 configurados en el router R1, un servidor de DHCPv4 para la LAN 192.168.10.0/24.

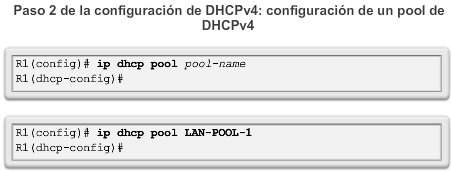
**Deshabilitación de DHCPv4**

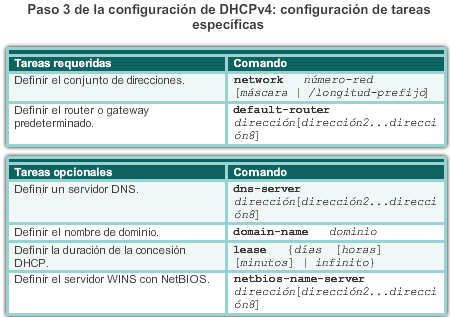
El servicio DHCPv4 está habilitado, de manera predeterminada, en versiones del software IOS de Cisco que lo admiten. Para deshabilitar el servicio, utilice el comando del modo de configuración global **no service dhcp**. Utilice el comando del modo de configuración global **service dhcp** para volver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

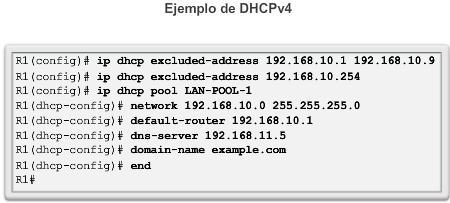
Utilice la actividad del verificador de sintaxis en la figura 6 para configurar parámetros de DHCPv4 similares en el R1 para la LAN 192.168.11.0/24.











En el resultado de ejemplo, se utiliza la topología que se muestra en la figura 1. En este ejemplo, se configuró el R1 para que proporcione servicios DHCPv4. Dado que la PC1 no se encendió, no tiene una dirección IP.

Como se muestra en la figura 2, en el resultado del 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.

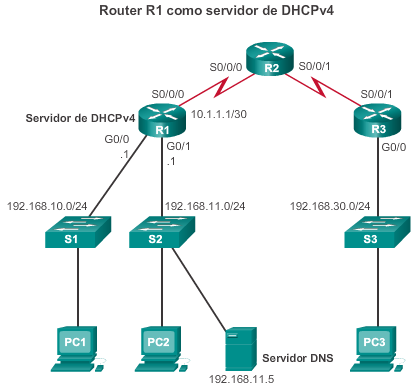
Como se muestra en la figura 3, se puede verificar el funcionamiento de DHCPv4 mediante el comando **show ip dhcp binding**. Este comando muestra una lista de todas las vinculaciones de la dirección IPv4 con la dirección MAC que fueron proporcionadas por el servicio DHCPv4. El segundo comando en la figura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

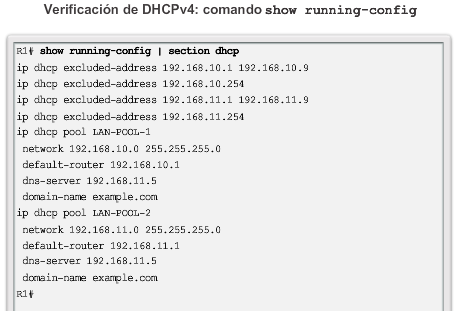
Como se observa en el resultado de estos comandos, actualmente no hay vinculaciones, y las estadísticas indican que no hay mensajes enviados o recibidos. En este momento, ningún dispositivo solicitó servicios DHCPv4 del router R1.

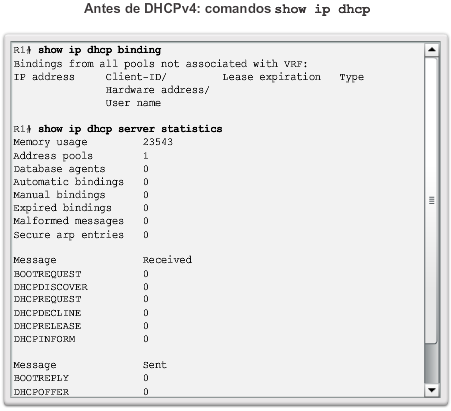
En la figura 4, los comandos se emiten después de que la PC1 y la PC2 se encendieron y finalizaron el proceso de arranque.

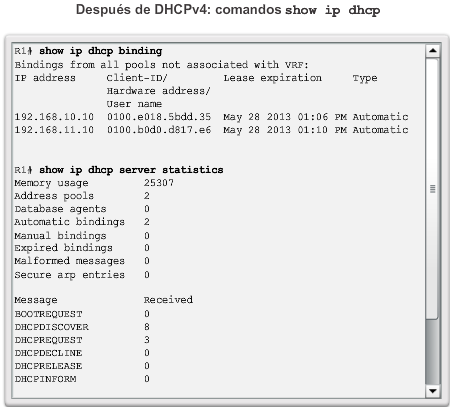
Observe que en la información acerca de las vinculaciones ahora se muestra que las direcciones IPv4 192.168.10.10 a 192.168.11.10 se unieron a las direcciones MAC. Las estadísticas también muestran actividad DHCPDISCOVER, DHCPREQUEST, DHCPOFFER y DHCPACK.

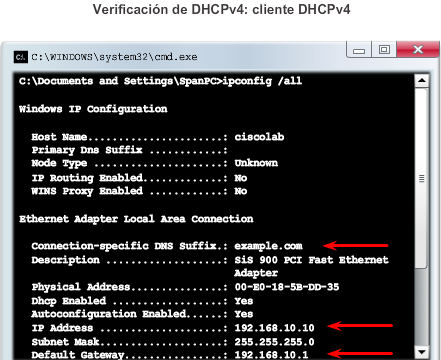
Como se muestra en la figura 5, el comando **ipconfig /all**, cuando se emite en la PC1, muestra los parámetros TCP/IP. Dado que la PC1 se conectó al segmento de red 192.168.10.0/24, recibió automáticamente un sufijo DNS, una dirección IPv4, una máscara de subred, un gateway predeterminado y una dirección del servidor DNS de ese pool. No se requiere configurar la interfaz del router. Si una computadora está conectada a un segmento de red que tiene un pool de DHCPv4 disponible, la computadora puede obtener una dirección IPv4 del pool adecuado de manera automática.











**¿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.

En la figura 1, la PC1 intenta adquirir una dirección IPv4 de un servidor de DHCP mediante un mensaje de difusión. En esta situación, el router R1 no está configurado como servidor de DHCPv4 y no reenvía el mensaje de difusión. Dado que el servidor de DHCPv4 está ubicado en una red diferente, la PC1 no puede recibir una dirección IP mediante DHCP.

En la figura 2, la PC1 intenta renovar su dirección IPv4. Para hacerlo, se emite el comando **ipconfig /release**. Observe que se libera la dirección IPv4, y se muestra que la dirección es 0.0.0.0. A continuación, se emite el comando**ipconfig /renew**. Este comando hace que la PC1 transmita por difusión un mensaje DHCPDISCOVER. En el resultado se muestra que la PC1 no puede ubicar el servidor de DHCPv4. Dado que los routers no reenvían mensajes de difusión, la solicitud no es correcta.

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. En la topología de ejemplo, la PC1 transmitiría por difusión una solicitud para ubicar un servidor de DHCPv4. Si el R1 estuviera configurado como agente de retransmisión DHCPv4, reenviaría la solicitud al servidor de DHCPv4 ubicado en la subred 192.168.11.0.

Como se muestra en la figura 3, la interfaz en el R1 que recibe la difusión se configura con el comando del modo de configuración de interfaz **ip helper-address**. La dirección del servidor de DHCPv4 se configura como el único parámetro.

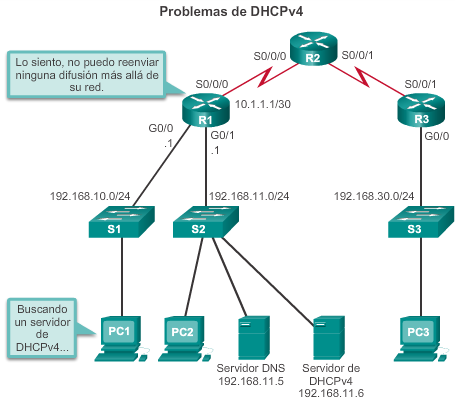
Cuando se configura el R1 como agente de retransmisión DHCPv4, acepta solicitudes de difusión para el servicio DHCPv4 y, a continuación, reenvía dichas solicitudes en forma de unidifusión a la dirección IPv4 192.168.11.6. El comando**show ip interface** se utiliza para verificar la configuración.

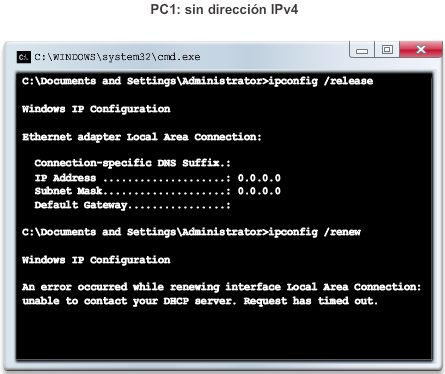
Como se muestra en la figura 4, la PC1 ahora puede adquirir una dirección IPv4 del servidor de DHCPv4.

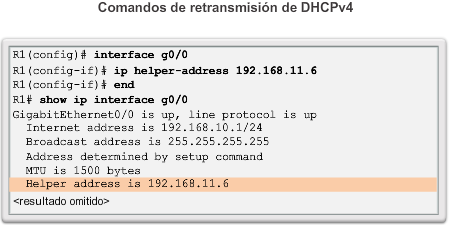
DHCPv4 no es el único servicio que puede configurarse para que retransmita el router. De manera predeterminada, el comando **ip helper-address** reenvía los siguientes ocho siguientes servicios UDP:

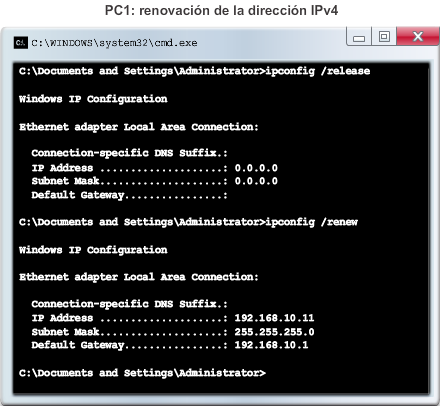
* Puerto 37: Tiempo
* Puerto 49: TACACS
* Puerto 53: DNS
* Puerto 67: cliente DHCP/BOOTP
* Puerto 68: servidor de DHCP/BOOTP
* Puerto 69: TFTP
* Puerto 137: servicio de nombres NetBIOS
* Puerto 138: servicio de datagrama NetBIOS

Mediante el verificador de sintaxis de la figura 5, configure los comandos de retransmisión de DHCPv4 en el router correcto de modo que la PC3 pueda recibir información de direccionamiento IPv4 del servidor de DHCPv4. Consulte nuevamente la figura 1 para ver la topología de la red.







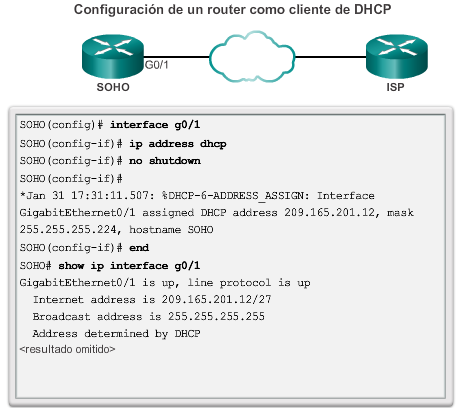


### Configuración de cliente DHCPv4

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**.

En la figura 1, suponga que un ISP se configuró para proporcionar direcciones IP del rango de red 209.165.201.0/27 a clientes selectos. Después de que se configura la interfaz G0/1 con el comando **ip address dhcp**, el comando **show ip interface g0/1** confirma que la interfaz está activada y que la dirección fue asignada por un servidor de DHCPv4.

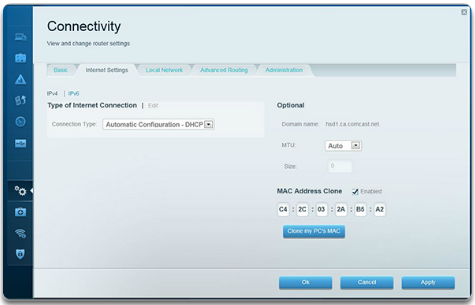
Utilice el verificador de sintaxis de la figura 2 para configurar la interfaz que está conectada al ISP, a fin de adquirir una dirección del servidor de DHCP.



Normalmente, los routers con poca banda ancha para uso doméstico, como los routers Linksys, se pueden configurar para conectarse a un ISP mediante un cable módem o un módem DSL. En la mayoría de los casos, los routers SOHO están establecidos para adquirir una dirección IPv4 automáticamente del ISP.

Por ejemplo, en la ilustración se muestra la página de configuración de WAN predeterminada para un router Linksys EA6500. Observe que el tipo de conexión a Internet está establecido en Automatic Configuration - DHCP (Configuración automática, DHCP). Esto significa que cuando el router se conecta a un cable módem, por ejemplo, es un cliente DHCPv4 y solicita una dirección IPv4 del ISP.

**Nota:** la característica de clonación de la dirección MAC utiliza una dirección especificada como la dirección MAC de origen en el ISP que interactúa con la interfaz del router. Muchos ISP asignan direcciones IPv4 sobre la base de la dirección MAC del dispositivo durante la instalación inicial. Cuando otro dispositivo, como un router SOHO, está conectado al ISP, este puede requerir que se configure la dirección MAC del dispositivo original en la interfaz WAN.



### Resolución de problemas de DHCPv4

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, como se muestra en la ilustración.

**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 conflicto** muestra todos los conflictos de direcciones que registra 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.

R1# **show ip dhcp conflict**

IP address Detection Method Detection time

192.168.10.32 Ping Feb 16 2013 12:28 PM

192.168.10.64 Gratuitous ARP Feb 23 2013 08:12 AM

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

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 conectividad mediante una 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.

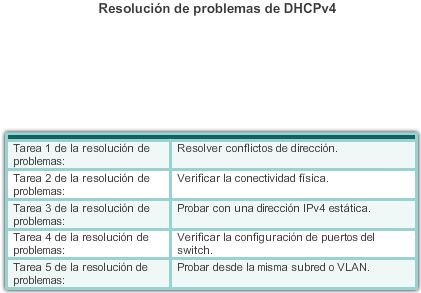
**Tarea 4 de la resolución de problemas: verificar la configuración de puertos del switch**

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. Mediante la configuración de PortFast y las configuraciones de los puertos perimetrales se resuelven los problemas de cliente DHCPv4 más comunes que se presentan con la instalación inicial de un switch Cisco.

**Tarea 5 de la resolución de problemas: probar funcionamiento DHCPv4 en 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.



Cuando el servidor de DHCPv4 está ubicado en una LAN distinta de la del cliente, la interfaz del router que interactúa con el cliente se debe configurar para retransmitir las solicitudes de DHCPv4 mediante la configuración de la dirección IPv4 de ayuda. Si la dirección IPv4 de ayuda no se configura correctamente, las solicitudes de cliente DHCPv4 no se reenvían al servidor de DHCPv4.

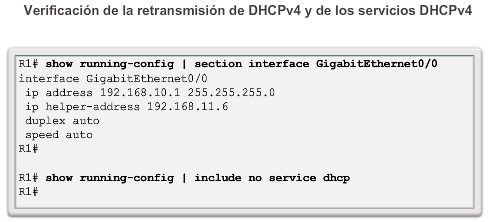
Siga estos pasos para verificar la configuración del router:

**Paso 1.**Verificar que el comando **ip helper-address** esté configurado en la interfaz correcta. Este comando debe estar presente en la interfaz de entrada de la LAN que contiene las estaciones de trabajo cliente DHCPv4 y debe estar dirigido al servidor de DHCPv4 correcto. En la ilustración, el resultado del comando **show running-config** verifica que la dirección IPv4 de retransmisión DHCP4 hace referencia a la dirección del servidor de DHCPv4 en 192.168.11.6.

El comando **show ip interface** también se puede utilizar para verificar la retransmisión DHCPv4 en una interfaz.

**Paso 2.**Verificar que no se haya configurado el comando de configuración global **no service dhcp**. Este comando deshabilita toda la funcionalidad del servidor de DHCP y de retransmisión del router. El comando **service dhcp** no aparece en la configuración en ejecución, debido a que es la configuración predeterminada

En la ilustración, el comando **show running-config | include no service dhcp** verifica que el servicio DHCPv4 esté habilitado, debido a que no hay coincidencia para el comando **show running-config | include no service dhcp**. Si se hubiera deshabilitado el servicio, en el resultado se mostraría el comando **no service dhcp**.

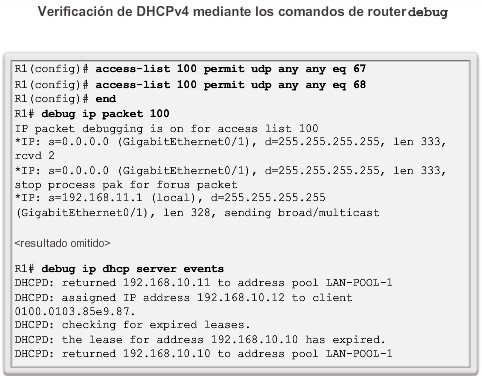


En los routers configurados como servidores de DHCPv4, el proceso DHCPv4 falla si el router no recibe solicitudes del cliente. A modo de tarea de resolución de problemas, verifique que el router reciba la solicitud de DHCPv4 del cliente. Este paso de la resolución de problemas comprende la configuración de una ACL para el resultado de la depuración.

En la ilustración, se muestra una ACL extendida que permite solamente paquetes con puertos de destino UDP de 67 o 68. Estos son los puertos típicos que utilizan los clientes y los servidores de DHCPv4 al enviar mensajes DHCPv4. La ACL extendida se utiliza con el comando **debug ip packet** para mostrar solamente los mensajes DHCPv4.

En el resultado que aparece en la ilustración, se muestra que el router recibe solicitudes de DHCP del cliente. La dirección IP de origen es 0.0.0.0, debido a que el cliente aún no tiene una dirección IP. El destino es 255.255.255.255, debido a que el mensaje de detección de DHCP del cliente se envía como difusión. En este resultado, solo se muestra un resumen del paquete, y no el mensaje DHCPv4 en sí. Sin embargo, el router recibió un paquete de difusión con los puertos UDP e IP de origen y destino adecuados para DHCPv4. En el resultado de depuración completo, se muestran todos los paquetes en las comunicaciones DHCPv4 entre el cliente y 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. También se utiliza para decodificar recepciones y transmisiones DHCPv4.



## Protocolo de configuración dinámica de host v6

### SLAAC y DHCPv6

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:

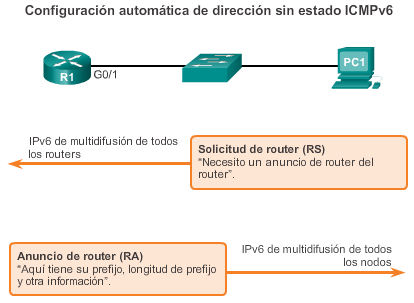
* Configuración automática de dirección sin estado (SLAAC), como se muestra en la ilustración
* Protocolo de configuración dinámica de host para IPv6 (DHCPv6 con estado)

**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.



Para poder enviar mensajes RA, un router se debe habilitar como router IPv6. Para habilitar el routing IPv6, un router se configura con el siguiente comando:

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

1. En la topología de ejemplo que se muestra en la figura 1, la PC1 está configurada para obtener el direccionamiento IPv6 de manera automática. Desde el arranque, la PC1 no recibió un mensaje RA, de modo que envía un mensaje RS a la dirección de multidifusión de todos los routers para informarle al router IPv6 local que necesita un RA.

2. Como se muestra en la figura 2, el R1 recibe el mensaje RS y responde con un mensaje RA. En el mensaje RA, se incluyen el prefijo y la longitud de prefijo de la red. El mensaje RA se envía a la dirección IPv6 de multidifusión de todos los nodos, FF02::1, con la dirección link-local del router como la dirección IPv6 de origen.

3. La PC1 recibe el mensaje RA que contiene el prefijo y la longitud de prefijo para la red local. La PC1 utiliza esta información para crear su propia dirección IPv6 de unidifusión global. La PC1 ahora tiene un prefijo de red de 64 bits, pero necesita una ID de interfaz (IID) de 64 bits para crear una dirección de unidifusión global.

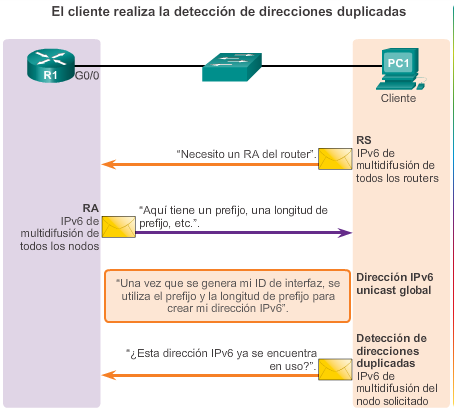
Hay dos maneras en las que la PC1 puede crear su propia IID única:

* **EUI-64:** mediante el proceso EUI-64, la PC1 crea una IID utilizando su MAC de 48 bits.
* **De generación aleatoria:** la IID de 64 bits puede ser un número aleatorio generado por el sistema operativo cliente.

Como se muestra en la figura 3, la PC1 puede crear una dirección IPv6 de unidifusión global de 128 bits combinando el prefijo de 64 bits con la IID de 64 bits. La PC1 utiliza la dirección link-local del router como su dirección IPv6 de gateway predeterminado.

4. Dado que SLAAC es un proceso sin estado, para que la PC1 pueda utilizar esta dirección IPv6 creada recientemente, debe verificar que sea única. Como se muestra en la figura 4, la PC1 envía un mensaje de solicitud de vecino ICMPv6 con su propia dirección como la dirección IPv6 de destino. Si ningún otro dispositivo responde con un mensaje de anuncio de vecino, la dirección es única y puede ser utilizada por la PC1. Si la PC1 recibe un anuncio de vecino, la dirección no es única, y el sistema operativo debe determinar una nueva ID de interfaz para utilizar.

Este proceso forma parte de la detección de vecinos ICMPv6 y se conoce como “detección de direcciones duplicadas (DAD)”.



La decisión de si un cliente se configura para obtener su información de direccionamiento IPv6 de forma automática mediante SLAAC, mediante DHCPv6 o mediante una combinación de ambos depende de la configuración dentro del mensaje RA. Los mensajes RA ICMPv6 contienen dos indicadores para señalar cuál es la opción que debe utilizar el cliente.

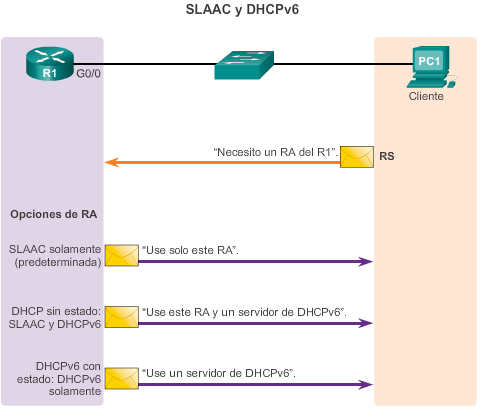
Los dos indicadores son el indicador de configuración de dirección administrada (indicador M) y el indicador de otra configuración (indicador O).

Mediante distintas combinaciones de los indicadores M y O, los mensajes RA tienen una de tres opciones de direccionamiento para el dispositivo IPv6, como se muestra en la ilustración:

* SLAAC (anuncio de router solamente)
* DHCPv6 sin estado (anuncio de router y DHCPv6)
* DHCPv6 con estado (DHCPv6 solamente)

Independientemente de la opción que se utilice, en RFC 4861 se recomienda que todos los dispositivos IPv6 realicen la detección de direcciones duplicadas (DAD) en cualquier dirección de unidifusión, entre las que se incluyen las direcciones configuradas mediante SLAAC o DHCPv6.

**Nota:** aunque el mensaje RA especifique el proceso que debe utilizar el cliente para obtener una dirección IPv6 de forma dinámica, el sistema operativo cliente puede elegir omitir el mensaje RA y utilizar los servicios de un servidor de DHCPv6 exclusivamente.



**Opción de SLAAC (anuncio de router solamente)**

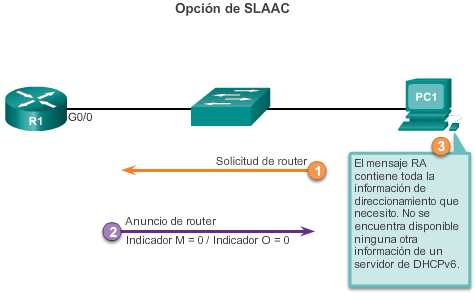
SLAAC es la opción predeterminada en los routers Cisco. Tanto el indicador M como el indicador O están establecidos en 0 en el RA, como se muestra en la ilustración.

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**



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.

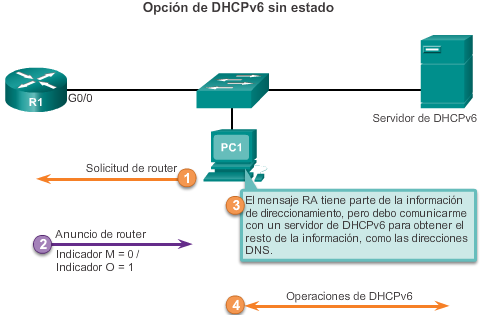
Mediante el prefijo y la longitud de prefijo en el mensaje RA, junto con EUI-64 o una IID generada aleatoriamente, el cliente crea la dirección IPv6 de unidifusión global.

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**

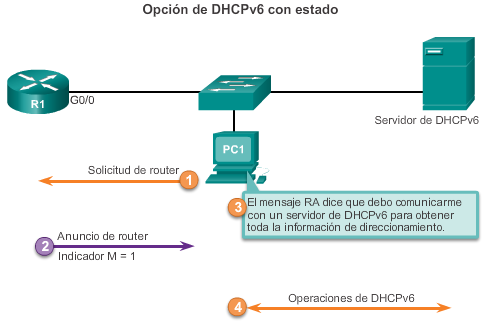


**DHCPv6 con estado (DHCPv6 solamente)**

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**



Como se muestra en la figura 1, 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.

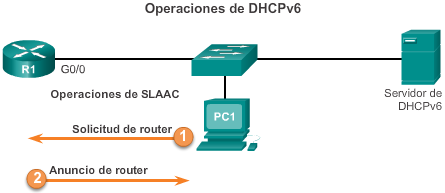
El cliente, ahora un cliente DHCPv6, necesita ubicar el servidor de DHCPv6. En la figura 2, el cliente envía un mensaje DHCPv6 SOLICIT a la dirección IPv6 de multidifusión de todos los servidores de DHCPv6 reservada, FF02::1:2. Esta dirección de multidifusión tiene alcance link-local, lo cual significa que los routers no reenvían los mensajes a otras redes.

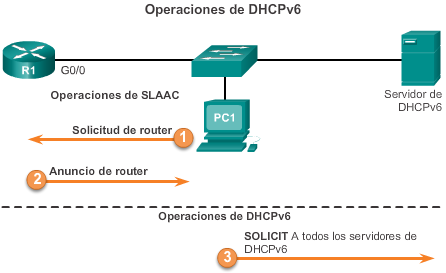
Uno o más servidores de DHCPv6 responden con un mensaje DHCPv6 ADVERTISE, como se muestra en la figura 3. El mensaje ADVERTISE le informa al cliente DHCPv6 que el servidor se encuentra disponible para el servicio DHCPv6.

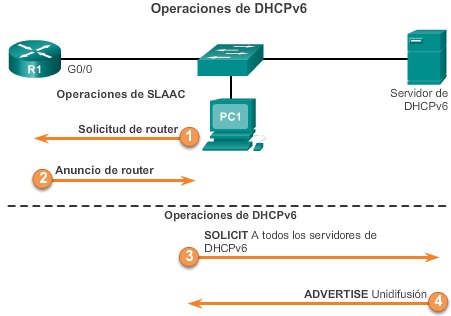
En la figura 4, el cliente responde con un mensaje INFORMATION-REQUEST o DHCPv6 REQUEST al servidor, según si utiliza DHCPv6 con estado o DHCPv6 sin estado.

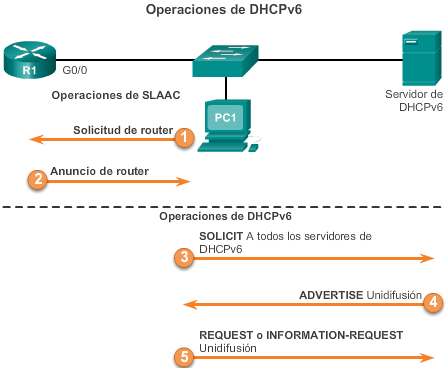
* **Cliente DHCPv6 sin estado:** el cliente envía un mensaje DHCPv6 INFORMATION-REQUEST al servidor de DHCPv6 en el que solicita solamente parámetros de configuración, como la dirección del servidor DNS. El cliente creó su propia dirección IPv6 mediante el uso del prefijo del mensaje RA y una ID de interfaz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

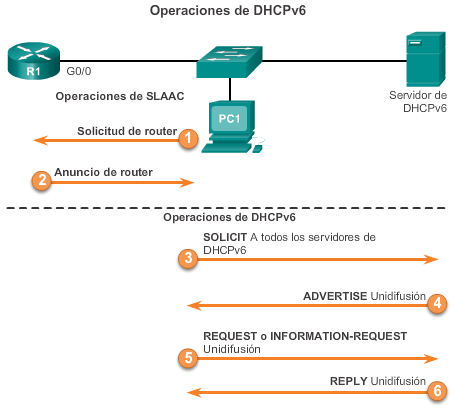
El servidor envía un mensaje DHCPv6 REPLY al cliente que contiene la información solicitada en el mensaje REQUEST o INFORMATION-REQUEST, como se muestra en la figura 5.

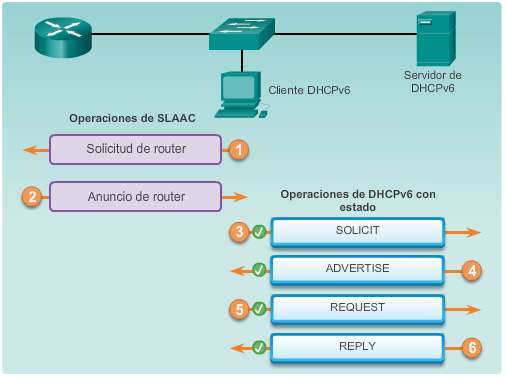












### DHCPv6 sin estado

Como se muestra en la figura 1, hay cuatro pasos para configurar un router como servidor de DHCPv6:

**Paso 1. Habilitar el routing IPv6**

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

**Paso 2. Configurar un pool de DHCPv6**

El comando **ipv6 dhcp pool***nombre-pool* crea un pool e ingresa el router en el modo de configuración DHCPv6, que se identifica por la petición de entradaRouter(config-dhcpv6)#.

**Paso 3. Configurar los parámetros del pool**

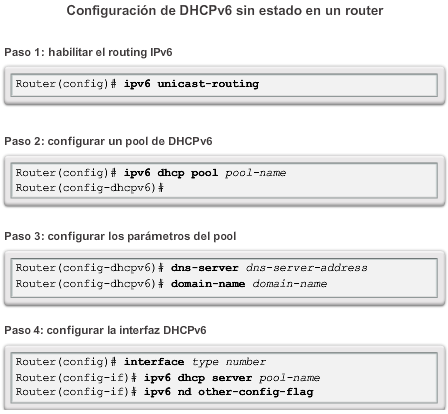
Durante el proceso SLAAC, el cliente recibió la información que necesitaba para crear una dirección IPv6 de unidifusión global. El cliente también recibió la información de gateway predeterminado mediante la dirección IPv6 de origen del mensaje RA, que es la dirección link-local del router. Sin embargo, el servidor de DHCPv6 sin estado puede configurarse para proporcionar otra información que pudo no haberse incluido en el mensaje RA, como la dirección del servidor DNS y el nombre de dominio.

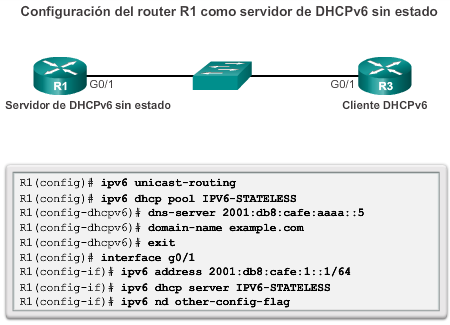
**Paso 4. Configurar la interfaz DHCPv6**

El comando del modo de configuración de interfaz **ipv6 dhcp server***nombre-pool* vincula el pool 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 O debe cambiarse de 0 a 1 mediante el comando de interfaz **ipv6 nd other-config-flag**. Los mensajes RA enviados en esta interfaz indican que hay información adicional disponible de un servidor de DHCPv6 sin estado.

**Ejemplo de servidor de DHCPv6 sin estado**

En la figura 2, se muestra una configuración de ejemplo para que un router se configure como servidor de DHCPv6 sin estado. Observe que el router R3 se muestra como cliente DHCPv6. El R3 está configurado como cliente para ayudar a verificar las operaciones de DHCPv6 sin estado.



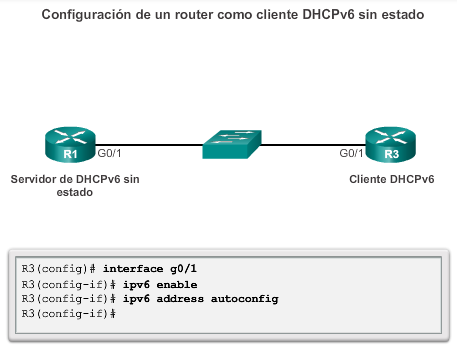


En el ejemplo de esta ilustración, se utiliza un router Cisco como cliente DHCPv6 sin estado. Esta no es una situación típica y se utiliza solo con fines de demostración. Generalmente, un cliente DHCPv6 sin estado es un dispositivo, como una computadora, una tablet PC, un dispositivo móvil o una cámara web.

El router cliente necesita una dirección IPv6 link-local en la interfaz para enviar y recibir mensajes IPv6, como mensajes RS y mensajes DHCPv6. La dirección link-local de un router se crea automáticamente cuando se habilita IPv6 en la interfaz. Esto puede suceder cuando se configura una dirección de unidifusión global en la interfaz o cuando se utiliza el comando **ipv6 enable**. Una vez que el router recibe una dirección link-local, puede enviar mensajes RS y participar en DHCPv6.

En este ejemplo, se utiliza el comando**ipv6 enable**, porque el router aún no tiene una dirección de unidifusión global.

El comando **ipv6 address autoconfig** habilita la configuración automática del direccionamiento IPv6 mediante SLAAC. A continuación, se utiliza un mensaje RA para informarle al router cliente que utilice DHCPv6 sin estado.



**Verificación del servidor de DHCPv6 sin estado**

En la figura 1, 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**

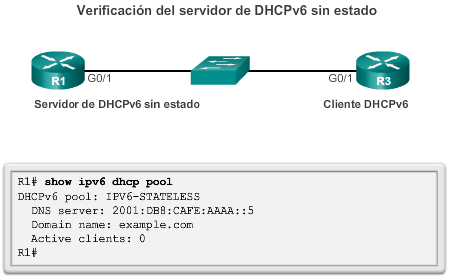
En este ejemplo, se utiliza un router como cliente DHCPv6 sin estado. En la figura 2, el resultado del comando **show ipv6 interface** muestra que el router tiene “Stateless address autoconfig enabled” (Configuración automática de dirección sin estado habilitada) y una dirección IPv6 de unidifusión global. 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.

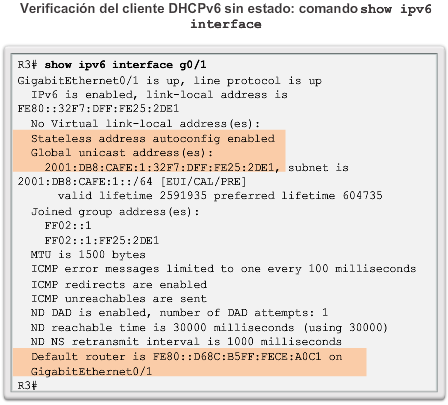
La información de router predeterminado también proviene del mensaje RA. Esta era la dirección IPv6 de origen del paquete que contenía el mensaje RA y la dirección link-local del router.

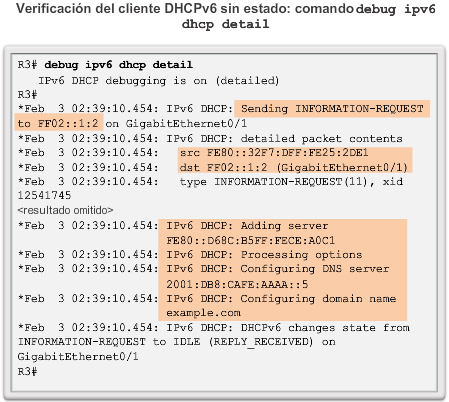
En el resultado del comando **debug ipv6 dhcp detail** de la figura 3, se muestran los mensajes DHCPv6 intercambiados entre el cliente y el servidor. En este ejemplo, se introdujo el comando en el cliente. Se muestra el mensaje INFORMATION-REQUEST, debido a que se envía desde un cliente DHCPv6 sin estado. 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.

Utilice el verificador de sintaxis de la figura 4 para configurar y verificar DHCPv6 sin estado en el router.







### 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**

Como se muestra en la ilustración, se requiere el uso del 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 enviar mensajes RA ICMPv6.

**Paso 2.** **Configurar un pool de DHCPv6**

El comando **ipv6 dhcp pool***nombre-pool* crea un pool e ingresa el router en el modo de configuración DHCPv6, que se identifica por la petición de entrada 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***longitud/prefijo* 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.

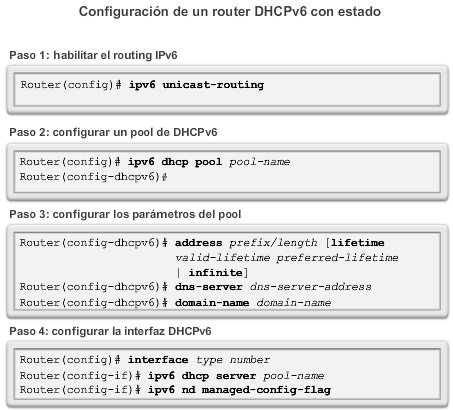
Otra información proporcionada por el servidor de DHCPv6 con estado suele incluir la dirección del servidor DNS y el nombre de dominio.

**Paso 4. Comandos de interfaz**

El comando de interfaz **ipv6 dhcp server***nombre-pool* vincula el pool 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.

**Ejemplo de servidor de DHCPv6 con estado**

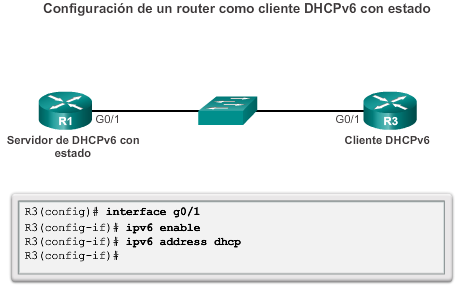
En la figura 2, se muestra un ejemplo de comandos de servidor de DHCPv6 con estado para un router configurado en el R1. Observe que no se especifica el gateway predeterminado, debido a que el router enviará automáticamente su propia dirección link-local como el gateway predeterminado. El router R3 está configurado como cliente para ayudar a verificar las operaciones de DHCPv6 con estado.





Como se muestra en la ilustración, 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 del servidor de DHCPv6 con estado**

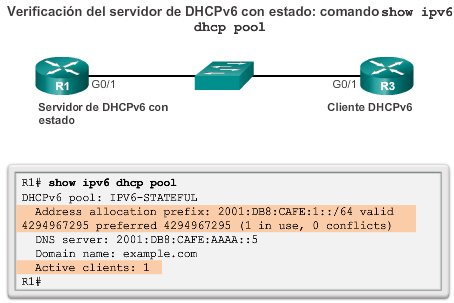
En la figura 1, el comando **show ipv6 dhcp pool** verifica el nombre del pool de DHCPv6 y sus parámetros. La cantidad de clientes activos es 1, lo que refleja que el R3 cliente recibe su dirección IPv6 de unidifusión global de este servidor.

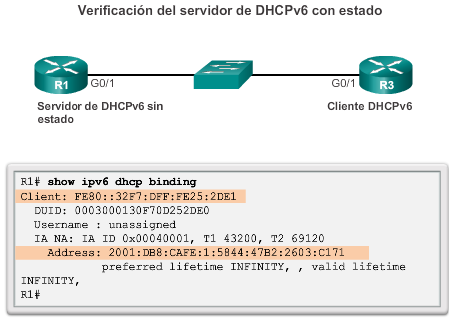
El comando **show ipv6 dhcp binding**, como se muestra en la figura 2, muestra la vinculación automática entre la dirección link-local del cliente y la dirección asignada por el servidor. FE80::32F7:DFF:FE25:2DE1 es la dirección link-local del cliente. En este ejemplo, esta es la interfaz G0/1 del R3. Esta dirección está vinculada a la dirección IPv6 de unidifusión global, 2001:DB8:CAFE:1:5844:47B2:2603:C171, la cual fue asignada por el R1, el servidor de DHCPv6. Esta información la mantiene un servidor de DHCPv6 con estado, y no un servidor de DHCPv6 sin estado.

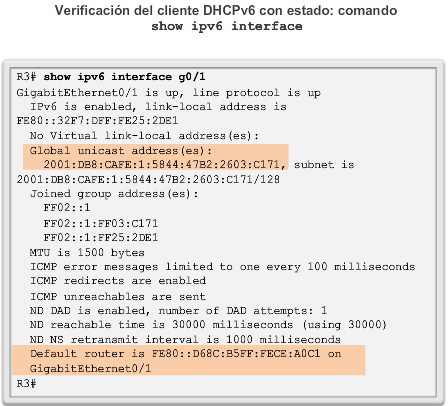
**Verificación del cliente DHCPv6 con estado**

dirección IPv6 de unidifusión global en el R3 cliente DHCPv6 que asignó el servidor de DHCPv6. La información de router predeterminado no proviene del servidor de DHCPv6, sino que se determinó mediante el uso de la dirección IPv6 de origen del mensaje RA. Si bien el cliente no utiliza la información contenida en el mensaje RA, puede utilizar la dirección IPv6 de origen para obtener la información del gateway predeterminado.

Utilice el verificador de sintaxis de la figura 4 para configurar y verificar DHCPv6 sin estado.







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.

**Nota:** si bien la configuración de un agente de retransmisión DHCPv6 es similar a DHCPv4, los routers o los agentes de retransmisión IPv6 reenvían mensajes DHCPv6 de manera levemente distinta que los retransmisores DHCPv4. Los mensajes y el proceso exceden el ámbito de este currículo.

En la figura 1, se muestra una topología de ejemplo en la que un servidor de DHCPv6 se encuentra en la red 2001:DB8:CAFE:1::/64. El administrador de red desea utilizar este servidor de DHCPv6 como un servidor de DHCPv6 central con estado para asignar direcciones IPv6 a todos los clientes. Por lo tanto, los clientes en otras redes, como la PC1 en la red 2001:DB8:CAFE:A::/64, deben comunicarse con el servidor de DHCPv6.

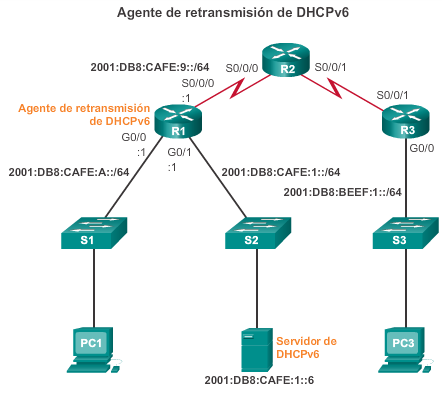
Los mensajes DHCPv6 de los clientes se envían a la dirección IPv6 de multidifusión FF02::1:2. Dirección de todos los agentes de retransmisión y servidores de DHCPv6: esta dirección tiene alcance link-local, lo que significa que los routers no reenvían estos mensajes. El router se debe configurar como agente de retransmisión DHCPv6 para habilitar al cliente y al servidor de DHCPv6 para que se comuniquen.

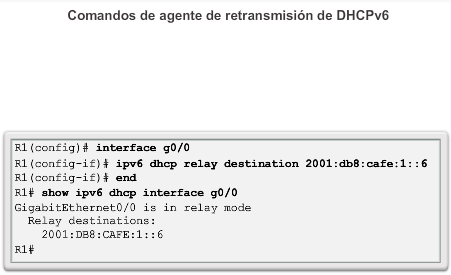
**Configuración del agente de retransmisión DHCPv6**

Como se muestra en la figura 2, 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.

El comando **show ipv6 dhcp interface** verifica que la interfaz G0/0 esté en modo de retransmisión con 2001:DB8:CAFE:1::6 configurado como el servidor de DHCPv6.

Mediante el verificador de sintaxis de la figura 3, configure los comandos de retransmisión de DHCPv6 en el router correcto de modo que la PC3 pueda recibir información de direccionamiento IPv6 del servidor de DHCPv6. Consulte la figura 1 para ver la topología de la red.





### Resolución de problemas de DHCPv6

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 conflicto** 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* puede utilizarse 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, deben resolverse los problemas de conectividad de red.

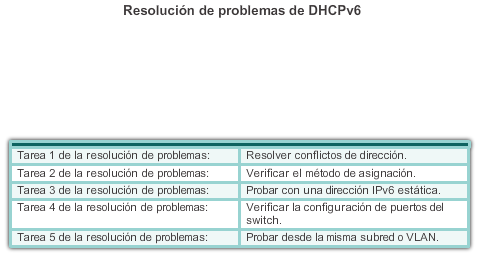
**Tarea 4 de la resolución de problemas: verificar la configuración de puertos del switch**

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 de enlaces troncales y canalización, STP y RSTP. 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: funcionamiento DHCPv6 en la 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**.



Las configuraciones del router para los servicios DHCPv6 con estado y sin estado tienen muchas similitudes, pero también incluyen diferencias significativas. En la figura 1, se muestran los comandos de configuración para los dos tipos de servicios DHCPv6.

**DHCPv6 con estado**

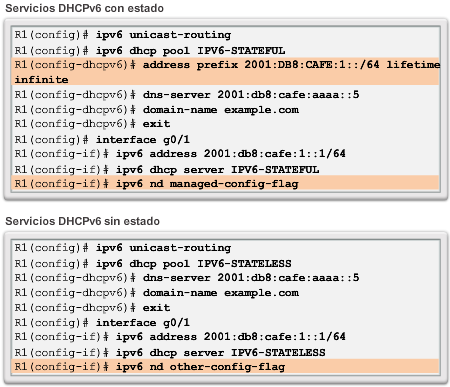
Los routers configurados para servicios DHCPv6 con estado tienen el comando **address prefix** para proporcionar información de direccionamiento.

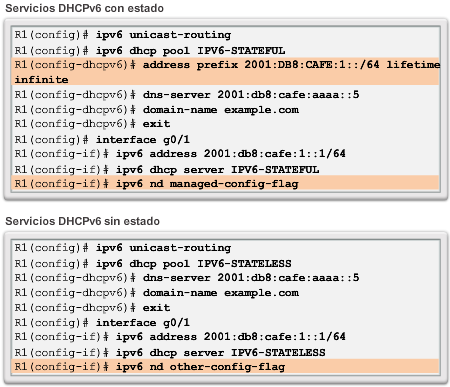
Para servicios DHCPv6 con estado, se utiliza el comando del modo de configuración de interfaz **ipv6 nd managed-config-flag**. En este caso, el cliente omite la información de direccionamiento en el mensaje RA y se comunica con un servidor de DHCPv6 para obtener información de direccionamiento y otra información.

**DHCPv6 sin estado**

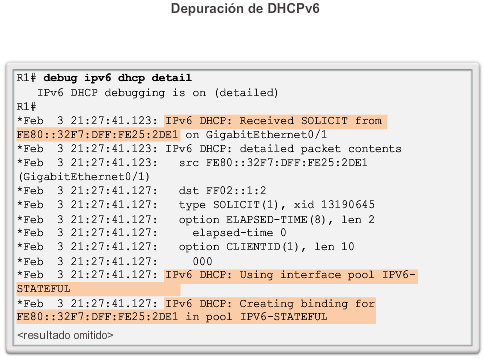
Para servicios DHCPv6 sin estado, se utiliza el comando del modo de configuración de interfaz **ipv6 nd other-config-flag**. Esto le informa al dispositivo que utilice SLAAC para la información de direccionamiento y un servidor de DHCPv6 sin estado para otros parámetros de configuración.

El comando **show ipv6 interface** puede utilizarse para ver la configuración actual para el método de asignación. Como se muestra en la figura 2, la última línea del resultado indica la forma en que los clientes obtienen direcciones y otros parámetros.





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.



## Resumen

Todos los nodos en una red requieren una dirección IP única que se comunique con otros dispositivos. La asignación estática de información de direccionamiento IP en una red grande produce una carga administrativa que puede eliminarse mediante el uso de DHCPv4 o DHCPv6 para asignar de forma dinámica información de direccionamiento IPv4 e IPv6, respectivamente.

DHCPv4 incluye tres mecanismos diferentes de asignación de direcciones para proporcionar flexibilidad al asignar las direcciones IP:

* **Asignación manual:** el administrador asigna una dirección IPv4 preasignada al cliente, y DHCPv4 comunica solo la dirección IPv4 al dispositivo.
* **Asignación automática:** DHCPv4 asigna automáticamente una dirección IPv4 estática de forma permanente a un dispositivo y la selecciona de un conjunto de direcciones disponibles. No hay arrendamiento, y la dirección se asigna de forma permanente al dispositivo.
* **Asignación dinámica:** DHCPv4 asigna dinámicamente, o arrienda, una dirección IPv4 de un conjunto de direcciones durante un período limitado según lo configurado en el servidor o hasta que el cliente ya no necesite la dirección.

La asignación dinámica es el mecanismo DHCPv4 utilizado más comúnmente y comprende el intercambio de diversos paquetes entre el servidor de DHCPv4 y el cliente DHCPv4, lo que deriva en el arrendamiento de información de direccionamiento válida durante un período predefinido.

Los mensajes cuyo origen es el cliente (DHCPDISCOVER, DHCPREQUEST) son mensajes de difusión para permitir que todos los servidores de DHCPv4 en la red escuchen la solicitud de información de direccionamiento y la recepción de dicha información por parte del cliente. Los mensajes cuyo origen es el servidor de DHCPv4 (DHCPOFFER, DHCPACK) se envían como mensajes de unidifusión directamente al cliente que solicita la información.

Existen dos métodos disponibles para la configuración dinámica de las direcciones IPv6 de unidifusión global.

* Configuración automática de dirección sin estado (SLAAC)
* Protocolo de configuración dinámica de host para IPv6 (DHCPv6 con estado)

Con la configuración automática sin estado, el cliente utiliza información proporcionada por el mensaje RA IPv6 para seleccionar y configurar automáticamente una dirección IPv6 única. 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.

DHCPv6 con estado es 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 se obtiene de un servidor de DHCPv6 con estado. El servidor de DHCPv6 mantiene la información de estado IPv6 de manera similar a la que un servidor de DHCPv4 asigna direcciones para IPv4.

Si el servidor de DHCP está ubicado en un segmento de red distinto del segmento del cliente DHCP, se debe configurar un agente de retransmisión. El agente de retransmisión reenvía mensajes de difusión específicos que se originan en un segmento LAN a un servidor especificado ubicado en un segmento LAN distinto (en este caso, un mensaje de difusión DHCP se reenviaría a un servidor de DHCP).

La resolución de problemas con DHCPv4 y DHCPv6 incluye las mismas tareas:

* Resolver conflictos de dirección
* Verificar la conectividad física
* Probar la conectividad con una dirección IP estática
* Verificar la configuración de puertos del switch
* Probar el funcionamiento en la misma subred o VLAN

