Resolución de problemas de DHCP en el switch Catalyst o en las redes corporativas e introducción.

Contenidos

Introducción

Este documento contiene información sobre la resolución de diferentes problemas relacionados con el Protocolo de configuración de host dinámico (DHCP) que pueden surgir dentro de una red de conmutación de Cisco Catalyst. Este documento incluye una guía de resolución de problemas relativos al uso de la función Agente de retransmisión DHCP/BootP de Cisco IOS®.

Antes de comenzar

Convenciones

Si desea obtener más información sobre las convenciones del documento, consulte las Convenciones sobre consejos técnicos de Cisco.

Requisitos previos

No hay requisitos previos específicos para este documento.

Componentes utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración despejada (predeterminada). Si la red está en uso, asegúrese de haber comprendido el efecto que puede tener cualquier comando antes de ejecutarlo.

'Conceptos clave'

A continuación hay varios conceptos claves del DHCP:

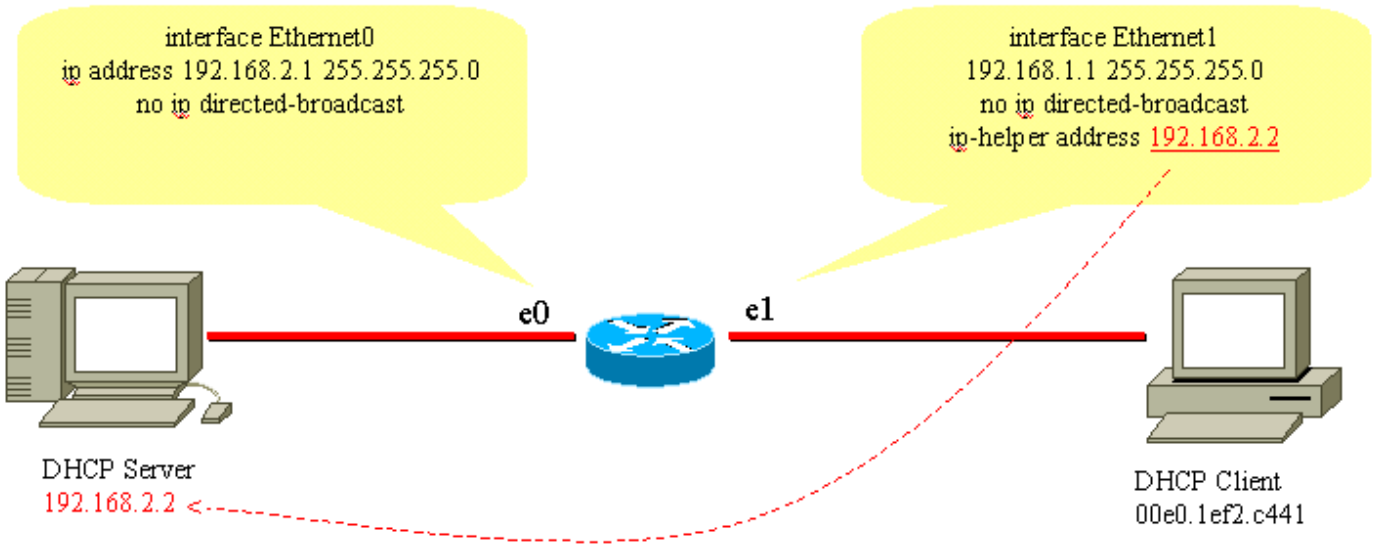
Los clientes DHCP no poseen una dirección IP configurada desde el inicio y por consiguiente deben enviar una solicitud de transmisión para obtener una dirección IP de un servidor DHCP.

Como valor predeterminado, los routers no reenvían difusiones. Esto es necesario para poder resolver las peticiones de difusión DHCP de los clientes si el servidor DHCP se encuentra en otro dominio de difusión (red de Capa 3 (L3)). Para esto, se utiliza el Agente de retransmisión DHCP.

La implementación del Relay de DHCP en el router Cisco se proporciona mediante los comandos **ip helper** de nivel de interfaz

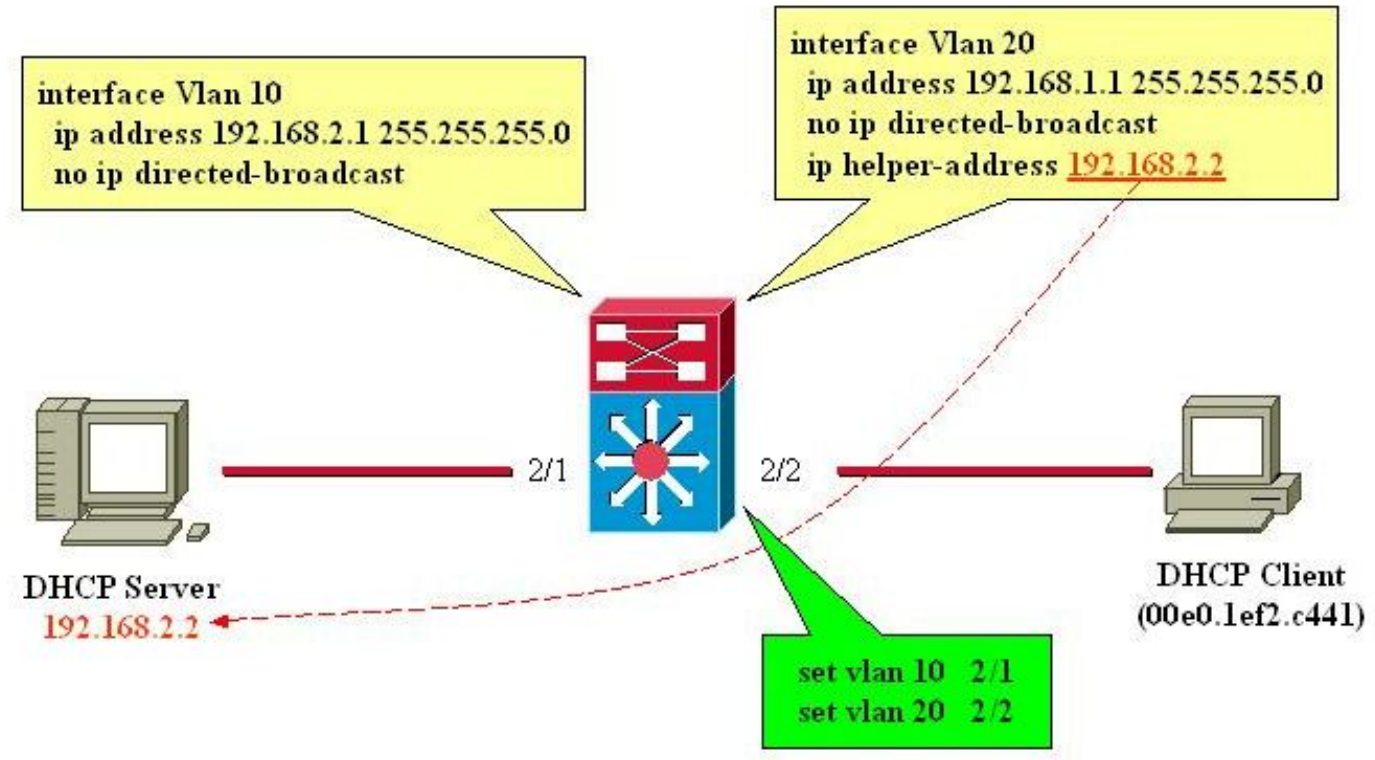
"Situaciones de ejemplo"

Situación 1: ruteo del router Cisco entre el cliente DHCP y las redes de servidor



Como aparece configurado en el diagrama anterior, la interfaz Ethernet1 reenviará el DHCPDISCOVER difundido del cliente a 192.168.2.2 vía la interfaz Ethernet1. El servidor de DHCP cumplirá la petición por unidifusión. En este ejemplo, no se necesita más configuración para el router.

Escenario 2: Switch Catalyst de Cisco con ruteo del módulo L3 entre el cliente DHCP y las redes de servidor



Como aparece configurado en el diagrama anterior, la interfaz VLAN20 reenviará el DHCPDISCOVER difundido del cliente a 192.168.2.2 vía la interfaz VLAN10. El servidor de DHCP cumplirá la petición por unidifusión. En este ejemplo, no se necesita más configuración para el router. Los puertos de los switches deben configurarse como puertos host, y deben tener habilitado el portfast del Protocolo de árbol transversal, e inhabilitadas la conexión troncal y la canalización.

Antecedentes

DHCP proporciona un mecanismo a través del cual los equipos que usan el Protocolo de transmisión de Control/Protocolo de Internet (TCP/IP) pueden obtener parámetros de configuración de protocolo de automáticamente a través de la red. DHCP es un estándar abierto desarrollado por Dynamic Host Configuration-Working Group (DHC-WG) de la Internet Engineering Task Force (IETF).

DHCP se basa en un paradigma cliente-servidor en el que el cliente DHCP, un PC, por ejemplo, se pone en contacto con un servidor de DHCP para obtener parámetros de configuración. Por lo general, el servidor DHCP se ubica de forma centralizada y lo gestiona un administrador de red. Dado que un administrador de red ejecuta el servidor, los clientes DHCP se pueden configurar de manera fiable y dinámica con parámetros apropiados para la arquitectura de la red actual.

La mayor parte de las redes empresariales están compuestas por varias subredes divididas en múltiples arquitecturas de subredes, denominadas redes LAN virtuales (VLAN), en las cuales los routers enrutan entre las subredes. Dado que los routers no transmiten difusiones de forma predeterminada, se necesita un servidor DHCP en cada subred a menos que los routers se configuren para reenviar la difusión DHCP con la función Agente de retransmisión DHCP.

Comprensión de DHCP

En un principio, DHCP se definió en la Solicitud de comentarios (RFC) 1531, que se ha actualizado con la RFC 2131. El DHCP se basa en el Protocolo de la rutina de arranque (BootP), que se define en la RFC 951.

Las estaciones de trabajo (hosts) usan DHCP para obtener la información de configuración inicial, como dirección IP, máscara de subred y la gateway predeterminada tras el inicio. Como cada host necesita una dirección IP para comunicarse con una red IP, DHCP permite disminuir la carga administrativa asociada a la configuración manual de cada host con una dirección IP. Además, si un host se mueve a una subred IP diferente, debe utilizar una dirección de IP diferente de la que empleaba antes. DHCP se hace cargo de esto automáticamente, lo que permite al host elegir una dirección IP en la subred IP correcta.

Referencias DHCP RFC actuales

RFC 2131 - DHCP

RFC 2132: opciones DHCP y extensiones de proveedor BOOTP

RFC 1534 - Interoperabilidad entre DHCP y BootP

RFC 1542 – Aclaraciones y extensiones para BootP

RFC 2241 - DHCP Opciones para los servicios de directorio de Novell

RFC 2242 – Nombre e información de Netware/Dominio IP

DHCP utiliza un modelo cliente-servidor donde uno o más servidores (servidores DHCP) asignan direcciones IP y otros parámetros de configuración opcional a los clientes (hosts) cuando se inicia el cliente. El servidor concede al cliente estos parámetros de configuración durante un período determinado. Cuando se inicia un host, la pila TCP/IP del host transmite un mensaje de difusión (DHCPDISCOVER) para recibir una dirección IP y una máscara de red, entre otros parámetros de configuración. Este paso inicia un intercambio entre el servidor DHCP y el host. Durante este intercambio, el cliente pasa por varios estados bien definidos que se muestran a continuación:

Inicialización

Selección

Petición

Límite

Renovación

Revinculación

Al moverse entre los estados detallados antes, el cliente y el servidor pueden intercambiar los tipos de mensajes incluidos en la Tabla de mensajes DHCP que aparece a continuación.

Tabla de mensajes DHCP

Referencia	Mensaje	Use
0x01	DHCPDISCOVER	El cliente está buscando servidores DHCP disponibles.
0x02	DHCPOFFER	El servidor responde al cliente DHCPDISCOVER.
0x03	DHCPREQUEST	El cliente transmite al servidor y solicita los parámetros ofrecidos desde un servidor en concreto, como se define en el paquete.
0x04	DHCPDECLINE	La comunicación cliente a servidor, indica que la dirección de red ya está en uso.
0x05	DHCPACK	La comunicación servidor a cliente con los parámetros de configuración, incluida la dirección de red comprometida.
0x06	DHCPNAK	La comunicación servidor a cliente, en la que se rechaza la petición del parámetro de configuración.
0x07	DHCPREL	La comunicación cliente a servidor,

	EASE	en la que se renuncia a la dirección de red y se cancela la concesión restante.
0x08	DHCPINFORM	La comunicación cliente a servidor, donde se solicitan parámetros de configuración local que el cliente ya ha configurado externamente como una dirección.

DHCPDISCOVER

Cuando un cliente se inicia por primera vez, se dice que está en estado de inicialización y transmite un mensaje DHCPDISCOVER en su subred física local sobre el puerto 67 (servidor de Boota) de Protocolo de datagrama de usuario (UDP). Dado que el cliente no tiene forma de conocer la subred a la que pertenece, el DHCPDISCOVER es una difusión a todas las subredes (dirección IP de destino 255.255.255.255), con una dirección IP de origen 0.0.0.0. La dirección IP de origen es 0.0.0.0, porque el cliente no tiene una dirección IP configurada. Si en esta subred local hay un servidor DHCP configurado correctamente y en funcionamiento, el servidor DHCP escuchará la difusión y responderá mediante un mensaje DHCPOFFER. Si no hay un servidor DHCP en la subred local, debe haber un agente de retransmisión DHCP/BootP en esta subred local para reenviar el mensaje DHCPDISCOVER a una subred que contenga un servidor DHCP.

Este agente de retransmisión puede ser un host dedicado (por ejemplo, Microsoft Windows Server) o un router (por ejemplo, un router Cisco configurado con sentencias de ayudante IP de nivel de interfaz).

DHCPOFFER

Un servidor DHCP que recibe un mensaje DHCPDISCOVER puede responder con un mensaje DHCPOFFER por el puerto 68 de UDP (cliente BootP). El cliente recibe el DHCPOFFER y pasa al estado Selección. Este mensaje DHCPOFFER contiene información de configuración inicial del cliente. Por ejemplo, el servidor DHCP completará el campo yiaddr del mensaje DHCPOFFER con la dirección IP solicitada. La máscara de subred y la gateway predeterminada se especifican en el campo opciones, máscara de subred y opciones del router, respectivamente. Otras opciones comunes en el mensaje DHCPOFFER son tiempo de concesión de dirección IP, hora de renovación, servidor de nombres de dominio y servidor de nombres de NetBIOS (WINS). El servidor DHCP envía DHCPOFFER a la dirección de difusión, pero incluye la dirección de hardware del cliente en el campo chaddr de la oferta, por lo que el cliente sabe que es el destino pretendido. Si el servidor DHCP no llegase a estar en la subred local, el servidor DHCP enviará el DHCPOFFER, como un paquete de unidifusión, al puerto 67 UDP, de regreso al agente de retransmisión DHCP/BootP de donde procede DHCPDISCOVER. El agente de retransmisión DHCP/BootP envía por difusión o por unidifusión el DHCPOFFER en la subred local por el puerto 68 UDP, en función del indicador de difusión definido por el cliente Bootp.

DHCPREQUEST

Cuando el cliente recibe un DHCPOFFER, responde con un mensaje DHCPREQUEST, lo que indica su intención de aceptar los parámetros en el DHCPOFFER y luego pasa al estado de Petición. El cliente puede recibir diversos mensajes DHCPOFFER, uno por cada servidor DHCP que haya recibido el mensaje original DHCPDISCOVER. El cliente elige un mensaje DHCPOFFER y responde sólo a ese servidor DHCP, rechazando implícitamente todos los demás mensajes DHCPOFFER. Para identificar al servidor seleccionado, el cliente introduce la dirección

IP del servidor DHCP en el campo de opción Identificador del servidor. DHCPREQUEST también es una difusión; por lo tanto, todos los servidores DHCP que enviaron DHCPOFFER verán la DHCPREQUEST y cada uno sabrá si su DHCPOFFER se aceptó o rechazó. Todas las opciones adicionales de configuración que solicite el cliente estarán incluidas en el campo de opciones del mensaje DHCPREQUEST. Aunque se le ha ofrecido al cliente una dirección IP, este enviará el mensaje DHCPREQUEST con la dirección IP de origen 0.0.0.0. En este punto, el cliente todavía no ha recibido la verificación de que puede usar la dirección IP.

DHCPACK

Cuando el servidor DHCP recibe la petición DHCPREQUEST, éste soporta la petición con un mensaje DHCPACK y así se completa el proceso de inicialización. El mensaje DHCPACK tiene una dirección IP de origen del servidor DHCP, y la dirección de destino es una vez más una difusión y contiene todos los parámetros que el cliente solicitó en el mensaje DHCPREQUEST. Cuando el cliente recibe el DHCPACK, adquiere el estado Vinculado (Bound) y es libre para usar la dirección IP para comunicarse en la red. Mientras tanto, el servidor DHCP almacena la concesión en su base de datos y la identifica de forma única con el identificador de cliente o chaddr y la dirección IP asociada. Tanto el cliente como el servidor usarán esta combinación de identificadores para referirse a la concesión.

Antes de que el cliente DHCP comience a usar la nueva dirección, éste debe calcular los parámetros de tiempo asociados a la dirección que se ha concedido, que son Lease Time (LT) (Tiempo de concesión), Renewal Time (T1) (Tiempo de renovación) y Rebind Time (T2) (Tiempo de revinculación). El LT típico predeterminado es de 72 horas. Si es necesario, puede usar tiempos de concesión más cortos para conservar las direcciones.

DHCPNAK

Si el servidor seleccionado no puede cumplir con el mensaje DHCPREQUEST, el servidor DHCP responderá con un mensaje DHCPNAK. Cuando el cliente recibe un mensaje DHCPNAK o no recibe una respuesta a un mensaje DHCPREQUEST, el cliente reinicia el proceso de configuración pasando al estado Petición. El cliente volverá a transmitir la DHCPREQUEST al menos cuatro veces en 60 segundos antes de reiniciar el estado Inicialización.

DHCPDECLINE

El cliente recibe el DHCPACK y podrá optar por hacer una verificación final de los parámetros. El cliente efectúa este procedimiento mediante el envío de peticiones de Protocolo de resolución de dirección (ARP) para la dirección IP que se proporciona en el DHCPACK. Si el cliente detecta que la dirección ya la está usando una petición ARP, el cliente envía un mensaje DHCPDECLINE al servidor y reinicia el proceso de configuración al pasar al estado Petición.

DHCPINFORM

Si un cliente ha obtenido una dirección de red a través de otros medios o tiene una dirección IP configurada, una estación de trabajo de cliente puede usar un mensaje de petición DHCPINFORM para obtener otros parámetros de configuración local, tal como el nombre de dominio y los Servidores de nombre de dominio (DNS). Los servidores DHCP que reciben un mensaje DHCPINFORM crean un mensaje DHCPACK con un parámetro de configuración local apropiado para el cliente sin asignar una nueva dirección IP. Este DHCPACK se envía por unidifusión al cliente.

DHCPRELEASE

Un cliente DHCP puede optar por renunciar a su concesión en una dirección de red si envía un mensaje DHCPRELEASE al servidor DHCP. El cliente identifica la concesión a liberar por el uso del campo `client identifier (Identificador de cliente)` y la dirección de red en el mensaje DHCPRELEASE.

Renovación de la licencia

Dado que la dirección IP se concede únicamente desde el servidor, la concesión debe renovarse periódicamente. Cuando haya transcurrido una mitad del tiempo de concesión (T1=0.5 x LT), el cliente intentará renovarla. El cliente tiene ahora el estado de renovación y envía un mensaje DHCPREQUEST al servidor, que mantiene la concesión actual. El servidor responderá a la petición de renovación con un mensaje DHCPACK si está de acuerdo con la renovación de la concesión. El mensaje DHCPACK contendrá la nueva concesión y los nuevos parámetros de configuración, en el caso de que se hayan realizado cambios en el servidor durante el período de concesión anterior. Si por alguna razón el cliente no puede tener acceso al servidor que contiene la concesión, intentará renovar la dirección de cualquier servidor DHCP una vez que el servidor DHCP original no haya respondido a las peticiones de renovación dentro de un período T2. El valor predeterminado de T2 es (7/8 x LT). Esto significa T1 < T2< LT.

Si el cliente tenía anteriormente una dirección IP asignada por DHCP y se reinicia, el cliente solicitará específicamente la dirección IP previamente concedida en un paquete DHCPREQUEST. Este DHCPREQUEST todavía tendrá la dirección IP de origen establecida como 0.0.0.0 y la de destino como dirección de transmisión IP 255.255.255.255.

Un cliente que envía un DHCPREQUEST cuando se reinicia un equipo, no debe completar el campo identificador del servidor, en lugar de eso debe completar el campo opción de dirección IP solicitada. Aquellos clientes que cumplen estrictamente con RFC rellenarán el campo ciaddr con la dirección solicitada en lugar del campo de opción DHCP. El servidor DHCP aceptará cualquier método. El comportamiento del servidor DHCP depende de muchos factores, como en el caso de los servidores DHCP de Windows NT, de la versión del sistema operativo y de otros factores, como superscoping (súper alcance). Si el servidor DHCP determina que el cliente aún puede usar la dirección de IP solicitada, no hará nada o enviará un DHCPACK para el DHCPREQUEST. Si el servidor determina que el cliente no puede usar la dirección IP solicitada, volverá a enviar un DHCPNACK al cliente. El cliente pasará entonces al estado Inicialización y enviará un mensaje DHCPDISCOVER.

Paquete DHCP

El mensaje de DHCP tiene una longitud variable y contiene los campos enumerados en la siguiente tabla.

Nota: Este paquete es una versión modificada del paquete BootP original.

Campo	Bytes	Nombre	Descripción
op	1	OpCode	Identifica el paquete como una petición o una respuesta: 1=BOOTREQUEST, 2=BOOTREPLY
htype	1	Tipo de hardwar	Especifica el tipo de dirección de red del hardware.

		e	
hlen	1	Longitud del hardware	Especifica la longitud de la extensión de la dirección de hardware.
saltos	1	Saltos	El cliente configura el valor en cero y se incrementa si la petición se reenvía por un router.
xid	4	ID de la transacción	Un número aleatorio elegido por el cliente. Todos los mensajes DHCP intercambiados para una transacción DHCP determinada usan el ID (xid).
secs	2	Segundos	Especifica el número de segundos desde que se inició el proceso DHCP.
indicadores	2	Indicadores	Indica si el mensaje será de difusión o de unidifusión.
ciaddr	4	Dirección IP del cliente	Sólo se usa cuando el cliente conoce la dirección IP, como en el caso de los estados Vinculado, Renovación, o Revinculación.
yiaddr	4	Su dirección IP	Si la dirección IP del cliente es 0.0.0.0, el servidor DHCP pondrá la dirección IP ofrecida al cliente en este campo.
siaddr	4	Dirección IP del servidor	Si el cliente tiene conocimiento de la dirección IP del servidor DHCP, este campo se cumplimenta con la dirección del servidor DHCP. En caso contrario, se usa en DHCPOFFER y DHCPACK desde el servidor DHCP.
giaddr	4	Dirección IP del router (GI ADDR)	La dirección IP de la gateway, completada por el agente de retransmisión DHCP/BootP.
chaddr	16	Dirección MAC del cliente	La dirección MAC del cliente DHCP.
sname	64	Nombre del servidor	El nombre del host servidor opcional.
archivo	128	Nombre	Nombre del archivo de

		de archivo de inicialización	arranque
opciones	Variable	Parámetros de opciones	Los parámetros optativos que puede proporcionar el servidor DHCP. RFC 2132 proporciona todas las opciones posibles.

Conversación de cliente-servidor para el cliente que obtiene la dirección DHCP donde el cliente y el servidor DHCP residen en la misma subred

Descripción de paquete	Dirección MAC de origen	Direcciones MAC de destino	Dirección IP de origen	Direc. IP de destino
DHCPDISCOVER	Cliente	Difusión	0.0.0.0	255.255.255.255
DHCPOFFER	Servidor DHCP	Difusión	Servidor DHCP	255.255.255.255
DHCPREQUEST	Cliente	Difusión	0.0.0.0	255.255.255.255
DHCPACK	Servidor DHCP	Difusión	Servidor DHCP	255.255.255.255

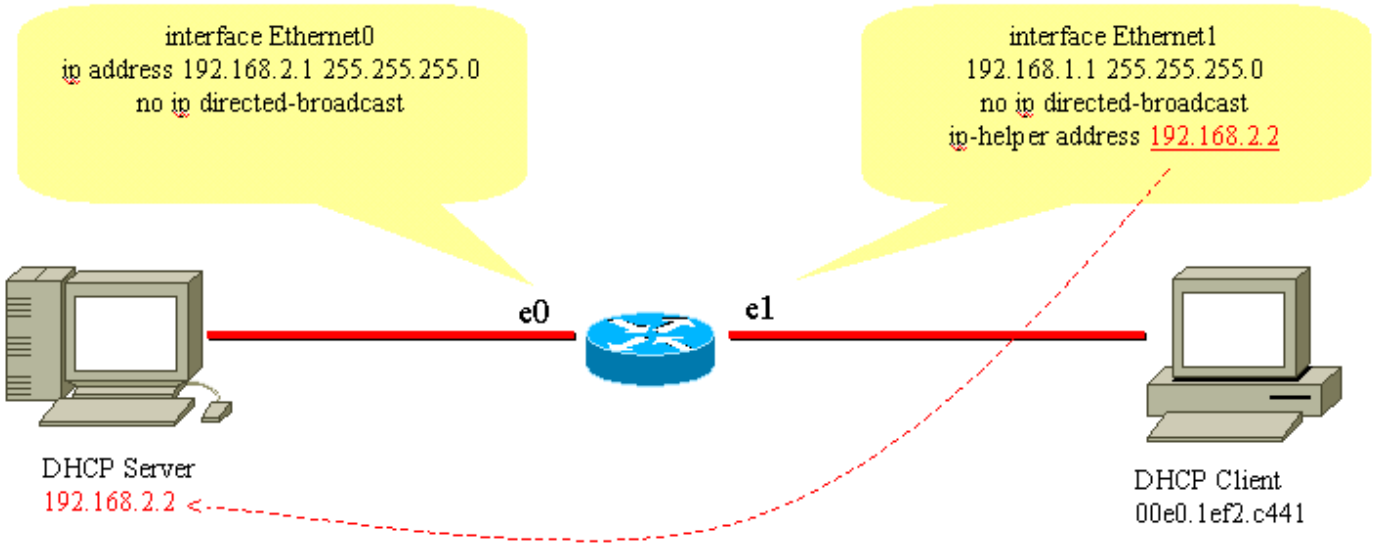
Rol del agente de retransmisión DHCP/BootP

Como valor predeterminado, los routers no reenvían paquetes de difusión. Dado que los mensajes del cliente DHCP usan la dirección IP de destino 255.255.255.255 (difusión a todas las redes), los clientes DHCP no podrán enviar peticiones a un servidor DHCP en otra subred a menos que el agente de retransmisión DHCP/BootP esté configurado en el router. El agente de retransmisión DHCP/BootP reenviará las peticiones DHCP en nombre de un cliente DHCP al servidor DHCP. El agente de retransmisión DHCP/BootP agregará su dirección IP a la dirección IP de origen de las tramas DHCP que van al servidor DHCP. Esto permite al servidor DHCP responder por unidifusión al agente de retransmisión DHCP/BootP. El agente de retransmisión DHCP/BootP también cumplimentará el campo Gateway IP address (Dirección IP de la gateway) de la interfaz en la que se recibe el mensaje DHCP del cliente. El servidor DHCP usa el campo Dirección IP de gateway para determinar el punto donde se originan los mensajes DHCPDISCOVER, DHCPREQUEST o DHCPINFORM.

Configuración de la función Agente de retransmisión DHCP/BootP en el router de Cisco IOS

Resulta fácil configurar un router de Cisco para reenviar peticiones BootP o DHCP: configure un IP helper-address (dirección de ayudante IP) que apunte al servidor DHCP/BootP o a la dirección

de difusión de subred dentro de la red en la que se ejecuta el servidor. Considere, por ejemplo, el siguiente diagrama de red:



Para reenviar la petición BootP/DHCP del cliente al servidor DHCP, se usa el comando **ip helper-address interface**. La dirección del ayudante IP se puede configurar para reenviar cualquier transmisión UDP basada en el número de puerto UDP. Como valor predeterminado, el IP helper-address reenvía las siguientes difusiones UDP:

Protocolo de transferencia de archivos trivial (TFTP) (puerto 69)

DNS (puerto 53), servicio de tiempo (puerto 37)

Nombre del servidor NetBIOS (puerto 137)

Servidor de datagramas NetBIOS (puerto 138)

Datagramas de clientes y servidores del protocolo de inicio (DHCP/BootP) (puertos 67 y 68)

Servicio de Sistema de control de acceso del controlador de acceso a terminales (TACACS) (puerto 49)

IEN-116 nombre de servicio (puerto 42)

Los IP helper-address pueden dirigir difusiones UDP a una dirección IP de difusión o unidifusión. **Sin embargo, no se recomienda usar el IP helper-address para reenviar difusiones UDP desde una subred a la dirección de difusión de otra subred, por la cantidad de inundaciones de difusión que podrían producirse**. También se soportan múltiples entradas de IP helper-address en un único interfaz, como se muestra a continuación:

Los routers Cisco no son compatibles con el balance de carga de los servidores DHCP que se

configuran como agentes de retransmisión DHCP. Los routers Cisco reenvían el mensaje DHCPDISCOVER a todas las direcciones del ayudante que se mencionan para dicha interfaz. Disponer de uno o más servidores DHCP para ofrecer servicio a una subred sólo aumenta el tráfico de DHCP cuando se intercambian los mensajes DHCPDISCOVER, DHCPOFFER, y DHCPREQUEST / DHCPDECLINE entre cada par de cliente y servidor DHCP.

Conversación entre cliente y servidor DHCP con la función de retransmisión DHCP

La tabla siguiente ilustra el proceso que debe seguir un cliente DHCP para recibir una dirección IP de un servidor DHCP. Esta tabla se basa en el diagrama de red anterior. Cada valor numérico en el diagrama representa un paquete que se describe a continuación. Esta tabla es un punto de referencia para comprender el flujo de paquetes de una conversación DHCP entre cliente y servidor. Esta tabla también es útil para determinar dónde puede haber problemas DHCP.

Paquete	Dirección de IP del cliente	Dirección de servidor IP	Dirección GI	Dirección MAC de la fuente de los paquetes	Dirección IP de origen del paquete.	Dirección MAC de destino de paquetes.	Dirección IP de destino del paquete.
1. DHCPDISCOVER se envía desde el cliente.	0.0.0.0	0.0.0.0	0.0.0.0	0005.DCC9.C640	0.0.0.0	ffff.ffff.ffff (difusión)	255.255.255.255
2. El router recibe DHCPDISCOVER en la interfaz E1. El router reconoce que este paquete es una difusión DHCP UDP. El router actúa	0.0.0.0	0.0.0.0	192.168.1.1	Dirección de la interfaz E2 MAC	192.168.1.1	Dirección MAC del servidor DHCP	192.168.2.2

como un agente de retransmisión DHCP/BootP y completa el campo Gateway IP address (Dirección IP de gateway) con la dirección IP de la interfaz de entrada, cambia la dirección IP de origen a una dirección IP de la interfaz de entrada y reenvía la petición directamente al servidor DHCP.							
3. El servidor DHCP ha recibido	192.168.1.2	192.168.2.2	192.168.1.1	Dirección MAC del servido	192.168.2.2	Dirección de la interfaz	192.168.1.1

DHSCPREQUEST y está enviando un DHCPACK al agente de retransmisión DHCP/BootP.				r DHCP		E2 MAC	
4. El agente de retransmisión DHCP recibe un DHCPOFFER y reenvía la difusión de DHCPOFFER a través de la LAN local.	192.168.1.2	192.168.2.2	192.168.1.1	Dirección de interfaz E1 MAC	192.168.1.1	ffff.ffff.ffff (transmisión)	255.255.255.255
5. DHCPREQUEST se envía desde el cliente.	0.0.0.0	0.0.0.0	0.0.0.0	0005.DCC9.C640	0.0.0.0	ffff.ffff.ffff (difusión)	255.255.255.255
6. El router recibe DHCPREQUEST en la interfaz E1. El router reconoc	0.0.0.0	0.0.0.0	192.168.1.1	Dirección de la interfaz E2 MAC	192.168.1.1	Dirección MAC del servidor DHCP	192.168.2.2

e que este paquete es una difusión DHCP UDP. El router actúa como un agente de retransmisión DHCP/BootP y completa el campo Gateway IP address (Dirección IP de gateway) con la dirección IP de la interfaz de entrada, cambia la dirección IP de origen a una dirección IP de la interfaz de entrada y reenvía la petición directa							

mente al servidor DHCP.							
7. El servidor DHCP ha recibido el DHSCP REQUEST y está enviando un DHCPACK al agente de retransmisión DHCP/ BootP.	192.168.1.2	192.168.2.2	192.168.1.1	Dirección MAC del servidor DHCP	192.168.2.2	Dirección de la interfaz E2 MAC	192.168.1.1
8. El agente de retransmisión DHCP/ BootP recibe el DHCPACK y reenvía la difusión de DHCPACK a través de la LAN local. El cliente acepta el ACK y usa la dirección IP del cliente.	192.168.1.2	192.168.2.2	192.168.1.1	Dirección de interfaz E1 MAC	192.168.1.1	ffff.ffff.ffff (transmisión)	255.255.255.255

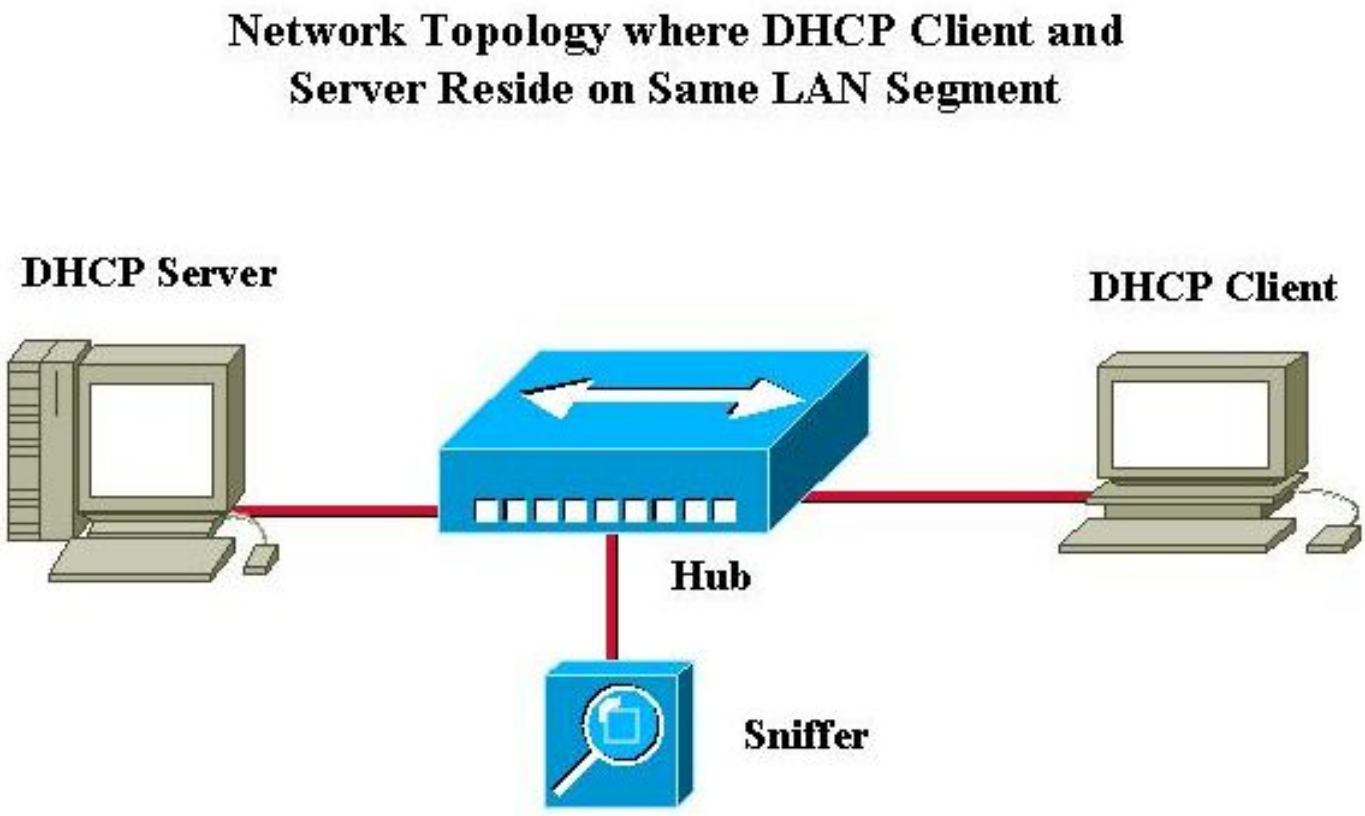
Consideraciones de inicio de DHCP, Pre-Execution Environment (Entorno de ejecución de inicio) (PXE)

Pre-Execution Environment (PXE) (Entorno de ejecución de inicio) permite a una estación de trabajo iniciarse desde un servidor de red antes de iniciar el sistema operativo en el disco duro local. De esta forma, no es necesario que el administrador de red tenga que estar frente a la estación de trabajo para iniciarla manualmente. Los sistemas operativos y otras aplicaciones, como los programas de diagnóstico se pueden cargar en el dispositivo desde un servidor de la red. El entorno PXE usa DHCP para configurar su dirección IP.

La configuración del agente de retransmisión DHCP/BootP debe efectuarse en el router si el servidor DHCP está ubicado en otro segmento enrutado de la red. Debe configurarse el comando **ip helper address** en la interfaz del router local. Consulte la sección Configuración de la función Agente de retransmisión DHCP/BootP en el router Cisco IOS de este documento para obtener información de configuración.

Comprensión y resolución de problemas de DHCP usando rastros de sabueso (sniffer)

Decodificación de rastros de sabueso (sniffer) de un cliente DHCP y un servidor en el mismo segmento de LAN



El rastro de sabueso (sniffer) siguiente se compone de seis tramas. Estas seis tramas ilustran un escenario de trabajo para DHCP, donde el cliente y el servidor DHCP residen en el mismo segmento físico o lógico. Cuando tenga que resolver problemas de DHCP, es importante que su rastro de sabueso coincida con los siguientes rastros. Puede haber algunas diferencias en comparación con los siguientes rastros, pero el flujo de paquetes general debe ser exactamente

igual. El rastro de paquetes se genera a partir de análisis previos acerca de cómo funciona DHCP.

```
- - - - - - - - - - - - - - - - - - - - - Trama 1 - DHCPDISCOVER - - - - - - - - - - - -
- - - - - - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
1[0.0.0.0] [255.255.255.255] 618 0:01:26.810 0.575.244 05/07/2001 11:52:03 AM DHCP:
Request,
 Message type: DHCP Discover
DLC: ----- DLC Header -----
DLC:
DLC: Frame 1arrived at 11:52:03.8106; frame size is 618 (026A hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station 0005DCC9C640
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 9
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = B988 (correct)
IP: Source address = [0.0.0.0]
IP: Destination address = [255.255.255.255]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 68 (BootPc/DHCP)
UDP: Destination port = 67 (BootPs/DHCP)
UDP: Length = 584
UDP: No checksum
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
```

DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00000882**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCC9C640**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: **Message Type = 1 (DHCP Discover)**
DHCP: Maximum message size = 1152
DHCP: **Client identifier = 00636973636F2D303030352E646363392E633634302D564C31**
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 66 = TFTP Option
DHCP: 6 = Domain name server
DHCP: 3 = Routers on the client's subnet
DHCP: 67 = Boot File Option
DHCP: 12 = Host name server
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- **Trama 2 - DHCPOFFER** -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
2[192.168.1.1] [255.255.255.255] 331 0:01:26.825 0.015.172 05/07/2001 11:52:03 AM
DHCP: Reply,
Message type: **DHCP Offer**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 2 arrived at 11:52:03.8258; frame size is 331 (014B hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF**, Broadcast
DLC: **Source = Station 0005DCC42484**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability

```
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 317 bytes
IP: Identification = 5
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = F901 (correct)
IP: Source address = [192.168.1.1]
IP: Destination address = [255.255.255.255]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 67 (BootPs/DHCP)
UDP: Destination port = 68 (BootPs/DHCP)
UDP: Length = 297
UDP: No checksum
UDP: [289 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 00000882
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [192.168.1.2]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: Client hardware address = 0005DCC9C640
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 2 (DHCP Offer)
DHCP: Server IP address = [192.168.1.1]
DHCP: Request IP address lease time = 85535 (seconds)
DHCP: Address Renewel interval = 42767 (seconds)
DHCP: Address Rebinding interval = 74843 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: Domain Name Server address = [192.168.1.3]
DHCP: Domain Name Server address = [192.168.1.4]
DHCP: Gateway address = [192.168.1.1]
```

DHCP:

- **Trama 3 - DHCPREQUEST** -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
3[0.0.0.0] [255.255.255.255] 618 0:01:26.829 0.003.586 05/07/2001 11:52:03 AM DHCP: Request,
Message type: **DHCP Request**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 56 arrived at 11:52:03.8294; frame size is 618 (026A hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF**, Broadcast
DLC: **Source = Station 0005DCC9C640**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 10
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = B987 (correct)
IP: **Source address = [0.0.0.0]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 68 (BootPc/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 584
UDP: No checksum
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:

DHCP: Hops = 0
DHCP: **Transaction id = 00000882**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCC9C640**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 3 (DHCP Request)
DHCP: Maximum message size = 1152
DHCP: **Client identifier = 00636973636F2D303030352E646363392E633634302D564C31**
DHCP: **Server IP address = [192.168.1.1]**
DHCP: **Request specific IP address = [192.168.1.2]**
DHCP: Request IP address lease time = 85535 (seconds)
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 66 = TFTP Option
DHCP: 6 = Domain name server
DHCP: 3 = Routers on the client's subnet
DHCP: 67 = Boot File Option
DHCP: 12 = Host name server
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- **Trama 4 - DHCPACK** -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
4[192.168.1.1] [255.255.255.255] 331 0:01:26.844 0.014.658 05/07/2001 11:52:03 AM
DHCP: Reply,
Message type: **DHCP Ack**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 57 arrived at 11:52:03.8440; frame size is 331 (014B hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF**, Broadcast
DLC: **Source = Station 0005DCC42484**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay

IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 317 bytes
IP: Identification = 6
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = F900 (correct)
IP: **Source address = [192.168.1.1]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 68 (BootPc/DHCP)**
UDP: Length = 297
UDP: No checksum
UDP: [289 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00000882**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: **Client IP address = [192.168.1.2]**
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCC9C640**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 5 (DHCP Ack)
DHCP: Server IP address = [192.168.1.1]
DHCP: Request IP address lease time = 86400 (seconds)
DHCP: Address Renewel interval = 43200 (seconds)
DHCP: Address Rebinding interval = 75600 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: **Domain Name Server address = [192.168.1.3]**

DHCP: **Domain Name Server address = [192.168.1.4]**
DHCP: **Gateway address = [192.168.1.1]**
DHCP:

- **Trama 5 - ARP** -

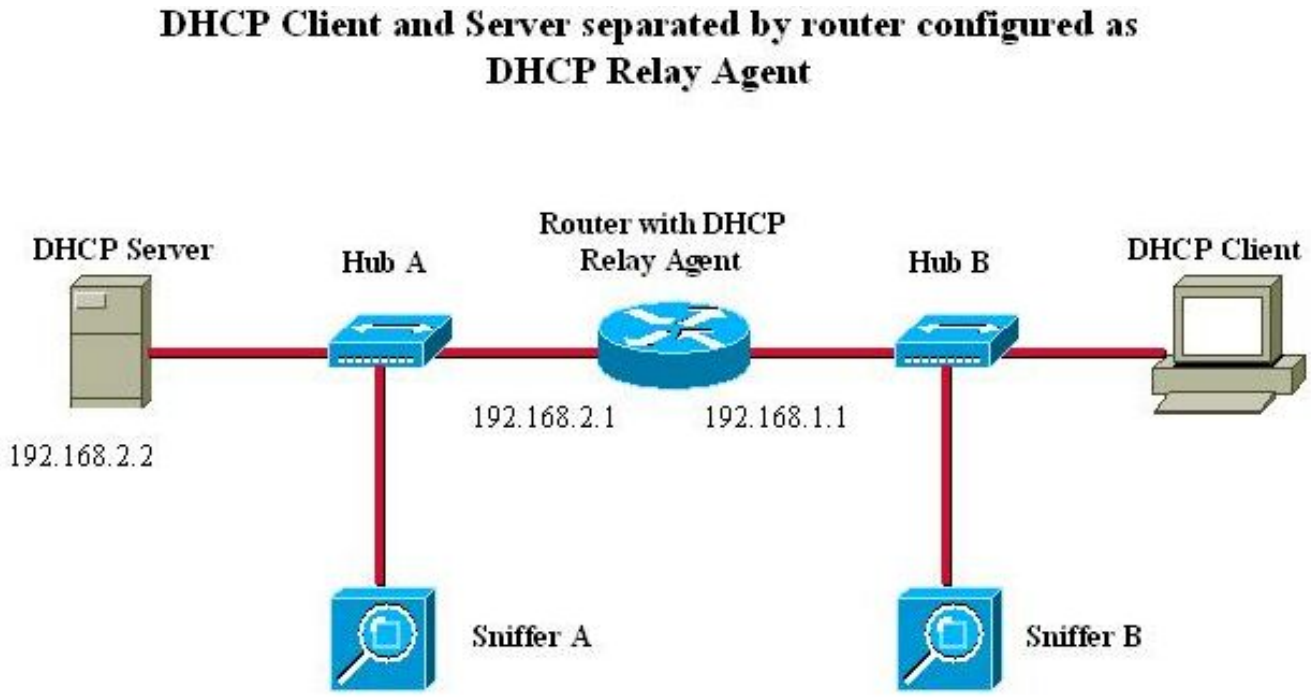
Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
5 0005DCC9C640 Broadcast 60 0:01:26.846 0.002.954 05/07/2001 11:52:03 AM ARP: R
PA=[192.168.1.2]
 HA=0005DCC9C640 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 58 arrived at 11:52:03.8470; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station 0005DCC9C640
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 0005DCC9C640
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:

- **Trama 6 - ARP** -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
6 0005DCC9C640 Broadcast 60 0:01:27.355 0.508.778 05/07/2001 11:52:04 AM ARP: R
PA=[192.168.1.2]
 HA=0005DCC9C640 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 59 arrived at 11:52:04.3557; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station 0005DCC9C640
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes

```
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 0005DCC9C640
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:
```

Decodificación de rastros del sabueso de un cliente DHCP y un servidor separados por un router configurado como agente de retransmisión



Rastro del sabueso-B

```
- - - - - - - - - - - - - - - - - - - - Trama 1 - DHCPDISCOVER - - - - - - - - - - - -
- - - - - - - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
1 [0.0.0.0] [255.255.255.255] 618 0:02:05.759 0.025.369 05/31/2001 06:53:04 AM DHCP:
Request,
 Message type: DHCP Discover
DLC: ----- DLC Header -----
DLC:
DLC: Frame 124 arrived at 06:53:04.2043; frame size is 618 (026A hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station 0005DCF2C441
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
```

```
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 183
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = B8DA (correct)
IP: Source address = [0.0.0.0]
IP: Destination address = [255.255.255.255]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 68 (BootPc/DHCP)
UDP: Destination port = 67 (BootPs/DHCP)
UDP: Length = 584
UDP: No checksum
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 00001425
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: Client hardware address = 0005DCF2C441
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 1 (DHCP Discover)
DHCP: Maximum message size = 1152
DHCP: Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
```

DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- **Trama 2 - DHCPOFFER** -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summaryr
125 [192.168.1.1] [255.255.255.255] 347 0:02:05.772 0.012.764 05/31/2001 06:53:04 AM
DHCP: Reply,
Message type: **DHCP Offer**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 125 arrived at 06:53:04.2171; frame size is 347 (015B hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF, Broadcast**
DLC: **Source = Station 003094248F71**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 333 bytes
IP: Identification = 45
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = F8C9 (correct)
IP: **Source address = [192.168.1.1]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 68 (BootPc/DHCP)**
UDP: Length = 313
UDP: Checksum = 8517 (correct)

UDP: [305 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00001425**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: **Client IP address = [192.168.1.2]**
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: **Relay Agent = [192.168.1.1]**
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 2 (DHCP Offer)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 99471 (seconds)
DHCP: Address Renewel interval = 49735 (seconds)
DHCP: Address Rebinding interval = 87037 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: **Domain Name Server address = [192.168.10.1]**
DHCP: **Domain Name Server address = [192.168.10.2]**
DHCP: **NetBIOS Server address = [192.168.10.1]**
DHCP: **NetBIOS Server address = [192.168.10.3]**
DHCP: **Domain name = "cisco.com"**
DHCP:

- **Trama 3 - DHCPREQUEST** -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
3 [0.0.0.0] [255.255.255.255] 618 0:02:05.774 0.002.185 05/31/2001 06:53:04 AM DHCP: Request,
Message type: **DHCP Request**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 126 arrived at 06:53:04.2193; frame size is 618 (026A hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF**
DLC: **Source = Station Cisc14F2C441**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes

IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 184
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = B8D9 (correct)
IP: **Source address = [0.0.0.0]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 68 (BootPc/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 584
UDP: No checksum
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00001425**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 3 (DHCP Request)
DHCP: Maximum message size = 1152
DHCP: **Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30**
DHCP: **Server IP address = [192.168.2.2]**

DHCP: **Request specific IP address = [192.168.1.2]**
DHCP: Request IP address lease time = 99471 (seconds)
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- **Trama 4 - DHCPACK** -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
4 [192.168.1.1] [255.255.255.255] 347 0:02:05.787 0.012.875 05/31/2001 06:53:04 AM
DHCP: Reply,
Message type: **DHCP Ack**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 127 arrived at 06:53:04.2321; frame size is 347 (015B hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF, Broadcast**
DLC: **Source = Station 003094248F71**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 333 bytes
IP: Identification = 47
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = F8C7 (correct)
IP: **Source address = [192.168.1.1]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:

UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 68 (BootPc/DHCP)**
UDP: Length = 313
UDP: Checksum = 326F (correct)
UDP: [305 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00001425**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [192.168.1.2]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: **Relay Agent = [192.168.1.1]**
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 5 (DHCP Ack)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 172800 (seconds)
DHCP: Address Renewel interval = 86400 (seconds)
DHCP: Address Rebinding interval = 151200 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: **Domain Name Server address = [192.168.10.1]**
DHCP: **Domain Name Server address = [192.168.10.2]**
DHCP: **NetBIOS Server address = [192.168.10.1]**
DHCP: **NetBIOS Server address = [192.168.10.3]**
DHCP: **Domain name = "cisco.com"**
DHCP:

- **Trama 5 - ARP** -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
5 Cisc14F2C441 Broadcast 60 0:02:05.798 0.011.763 05/31/2001 06:53:04 AM ARP: R
PA=[192.168.1.2]
 HA=Cisc14F2C441 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 128 arrived at 06:53:04.2439; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station Cisc14F2C441
DLC: Ethertype = 0806 (ARP)

```
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 00E01EF2C441
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:
```

- **Trama 6 - ARP** -

```
Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
5 Cisc14F2C441 Broadcast 60 0:02:05.798 0.011.763 05/31/2001 06:53:04 AM ARP: R
PA=[192.168.1.2]
 HA=Cisc14F2C441 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 128 arrived at 06:53:04.2439; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station Cisc14F2C441
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 00E01EF2C441
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:
```

Rastro del sabueso

- **Trama 1 - DHCPDISCOVER** -

```
Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
118 [192.168.1.1] [192.168.2.2] 618 0:00:51.212 0.489.912 05/31/2001 07:02:54 AM
DHCP: Request,
```

```
 Message type: DHCP Discover
DLC: ----- DLC Header -----
DLC:
DLC: Frame 118 arrived at 07:02:54.7463; frame size is 618 (026A hex) bytes.
DLC: Destination = Station 0005DC0BF2F4
DLC: Source = Station 003094248F72
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 52
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 3509 (correct)
IP: Source address = [192.168.1.1]
IP: Destination address = [192.168.2.2]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 67 (BootPs/DHCP)
UDP: Destination port = 67 (BootPs/DHCP)
UDP: Length = 584
UDP: Checksum = 0A19 (correct)
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 1
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
```

DHCP: **Relay Agent = [192.168.1.1]**
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 1 (DHCP Discover)
DHCP: Maximum message size = 1152
DHCP: Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- **Trama 2 - DHCPOFFER** -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
2 [192.168.2.2] [192.168.1.1] 347 0:00:51.214 0.002.133 05/31/2001 07:02:54 AM DHCP: Request,
Message type: **DHCP Offer**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 119 arrived at 07:02:54.7485; frame size is 347 (015B hex) bytes.
DLC: **Destination = Station 003094248F72**
DLC: **Source = Station 0005DC0BF2F4**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 333 bytes
IP: Identification = 41
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops

IP: Protocol = 17 (UDP)
IP: Header checksum = 3623 (correct)
IP: **Source address = [192.168.2.2]**
IP: **Destination address = [192.168.1.1]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 313
UDP: Checksum = A1F8 (correct)
UDP: [305 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [192.168.1.2]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [192.168.1.1]
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 2 (DHCP Offer)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 172571 (seconds)
DHCP: Address Renewel interval = 86285 (seconds)
DHCP: Address Rebinding interval = 150999 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: **Domain Name Server address = [192.168.10.1]**
DHCP: **Domain Name Server address = [192.168.10.2]**
DHCP: **NetBIOS Server address = [192.168.10.1]**
DHCP: **NetBIOS Server address = [192.168.10.3]**
DHCP: **Domain name = "cisco.com"**
DHCP:

- **Trama 3 - DHCPREQUEST** -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
3 [192.168.1.1] [192.168.2.2] 618 0:00:51.240 0.025.974 05/31/2001 07:02:54 AM DHCP:

```
Request,
 Message type: DHCP Request
DLC: ----- DLC Header -----
DLC:
DLC: Frame 120 arrived at 07:02:54.7745; frame size is 618 (026A hex) bytes.
DLC: Destination = Station 0005DC0BF2F4
DLC: Source = Station 003094248F72
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 54
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 3507 (correct)
IP: Source address = [192.168.1.1]
IP: Destination address = [192.168.2.2]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 67 (BootPs/DHCP)
UDP: Destination port = 67 (BootPs/DHCP)
UDP: Length = 584
UDP: Checksum = 4699 (correct)
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 1
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
```

DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: **Relay Agent = [192.168.1.1]**
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 3 (DHCP Request)
DHCP: Maximum message size = 1152
DHCP: **Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30**
DHCP: Server IP address = [192.168.2.2]
DHCP: Request specific IP address = [192.168.1.2]
DHCP: Request IP address lease time = 172571 (seconds)
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- **Trama 4 - DHCPACK** -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
4 [192.168.2.2] [192.168.1.1] 347 0:00:51.240 0.000.153 05/31/2001 07:02:54 AM DHCP: Request,
Message type: **DHCP Ack**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 121 arrived at 07:02:54.7746; frame size is 347 (015B hex) bytes.
DLC: **Destination = Station 003094248F72**
DLC: **Source = Station 0005DC0BF2F4**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 333 bytes
IP: Identification = 42
IP: Flags = 0X

```
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 3622 (correct)
IP: Source address = [192.168.2.2]
IP: Destination address = [192.168.1.1]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 67 (BootPs/DHCP)
UDP: Destination port = 67 (BootPs/DHCP)
UDP: Length = 313
UDP: Checksum = 7DF6 (correct)
UDP: [305 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [192.168.1.2]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [192.168.1.1]
DHCP: Client hardware address = 0005DCF2C441
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 5 (DHCP Ack)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 172800 (seconds)
DHCP: Address Renewel interval = 86400 (seconds)
DHCP: Address Rebinding interval = 151200 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: Domain Name Server address = [192.168.10.1]
DHCP: Domain Name Server address = [192.168.10.2]
DHCP: NetBIOS Server address = [192.168.10.1]
DHCP: NetBIOS Server address = [192.168.10.3]
DHCP: Domain name = "cisco.com"
DHCP:
```

Resolución de problemas de DHCP cuando las estaciones de trabajo cliente no pueden obtener direcciones DHCP

Estudio de caso No. 1: Servidor DHCP en el mismo segmento LAN o VLAN como cliente DHCP

Cuando el servidor DHCP y el cliente residen en el mismo segmento de la LAN o VLAN y el cliente no puede obtener una dirección IP del servidor DHCP, es poco probable que el router local sea la causa del problema DHCP. Es más probable que el problema esté relacionado con los dispositivos que conectan el servidor DHCP y el cliente DHCP. El problema, sin embargo, puede hallarse en el mismo servidor o cliente DHCP. Con los siguientes módulos de solución de problemas, puede determinar qué dispositivo está causando el problema.

Estudio de caso No. 2: El servidor DHCP y DHCP cliente están separados por un router configurado para funcionalidad de agente de retransmisión DHCP/BootP

Cuando el servidor y el cliente DHCP se hallan en diferentes segmentos de la LAN o VLAN, el router que funciona como agente de retransmisión DHCP/BootP es el responsable de reenviar DHCPREQUEST al servidor DHCP. Se requieren pasos adicionales de resolución de problemas para resolver el problema del agente de retransmisión BootP/DHCP, así como el servidor y el cliente DHCP. Con los siguientes módulos de solución de problemas, puede determinar qué dispositivo está causando el problema.

Módulos de resolución de problemas de DHCP

Dónde pueden ocurrir problemas de DHCP

El origen de los problemas de DHCP puede deberse a distintos motivos. Los motivos más frecuentes son los problemas de configuración. Sin embargo, muchos de los problemas de DHCP pueden estar provocados por defectos de software de los sistemas operativos, controladores de las tarjetas de interfaz de red (NIC) o agentes de retransmisión DHCP/BootP que se ejecutan en los routers. Por el gran número de áreas problemáticas, se requiere un planteamiento sistemático para solucionar los problemas.

Lista de las causas posibles preseleccionadas de problemas de DHCP:

- Configuración predeterminada del switch Catalyst
- Configuración del agente de retransmisión DHCP/BootP
- Problema de compatibilidad de NIC o problema de la característica DHCP
- Conducta del sistema operativo o defecto del software
- Alcance de la configuración del servidor DHCP o defecto del software.

Defecto del software del switch Catalyst o del agente de retransmisión DHCP/BootP de Cisco IOS

Este documento usa los siguientes módulos de resolución de problemas para determinar la causa raíz de dichos problemas, cómo se indica en la lista anterior.

A. Verifique la conectividad física

Este procedimiento se puede aplicar a todos los estudios de caso.

En primer lugar, verifique la conectividad física de un cliente y servidor DHCP. Si están conectados a un switch Catalyst, verifique que tanto el cliente DHCP como el servidor tengan conectividad física.

Para los switches Catalyst CatOS de las series 2948G, 4000, 5000 y 6000 use el comando **show port <mod#>/<port_range>** para verificar el estado del puerto. Si el estado del puerto no es `conectado`, el puerto no transmite tráfico, incluidas las peticiones de cliente de DHCP. El resultado de los comandos es el siguiente:

```
Switch (enable) show port 5/1
Port Name Status Vlan Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
5/1 conectado 1 a-full a-100 10/100BaseTX
```

Para los switches basados en IOS, como Catalyst 2900XL/3500XL/2950/3550, el comando equivalente a **show port status** es **show interface <interface>**. Si el estado de la interfaz es diferente a <`interfaz`> activa, el protocolo de línea está activo, el puerto no va a transferir el tráfico, incluidas las peticiones de cliente de DHCP. El resultado de los comandos es el siguiente:

```
Switch#show interface fastEthernet 0/1
FastEthernet0/1 is up, line protocol is up
Hardware is Fast Ethernet, address is 0030.94dc.acc1 (bia 0030.94dc.acc1)
```

Si se verificó la conexión física y no hay enlace entre el switch Catalyst y el cliente DHCP, consulte el documento Troubleshooting Cisco Catalyst Switches to NIC Compatibility Issues (Resolución de problemas de los switches Catalyst de Cisco para problemas de compatibilidad de NIC) para la resolución de problemas adicionales relacionados con la conectividad de la capa física.

B. Pruebe la conectividad de la red configurando la estación de trabajo del cliente con dirección IP estática

Este procedimiento se puede aplicar a todos los estudios de caso.

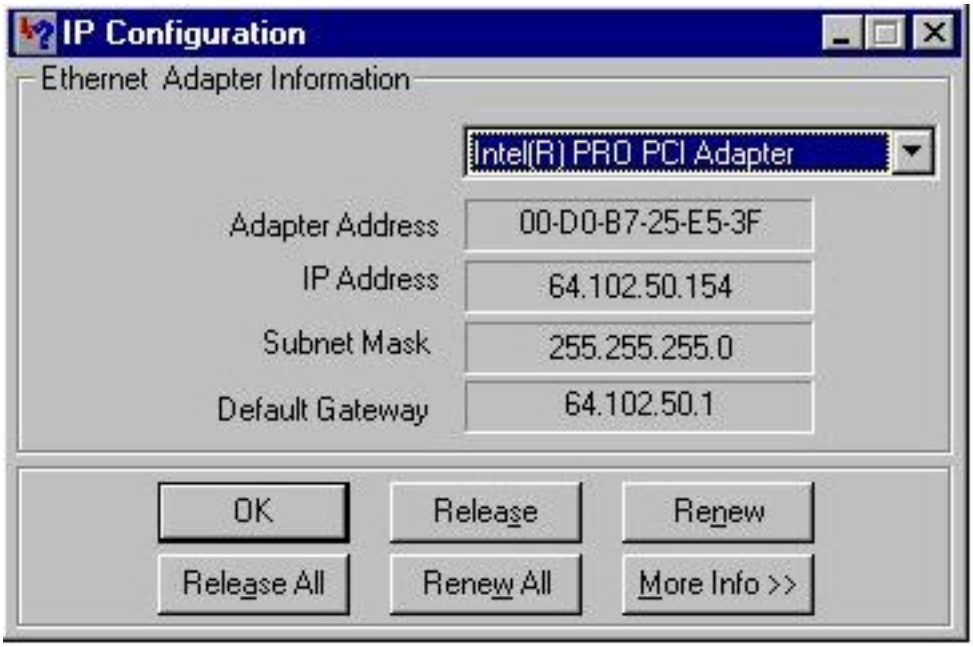
Durante la resolución de cualquier problema de DHCP, es importante verificar la conectividad de la red mediante la configuración de una dirección IP estática en una estación de trabajo cliente. Si la estación de trabajo no puede tener acceso a los recursos de red a pesar de tener una dirección IP configurada estáticamente, el origen del problema no es DHCP. A partir de aquí, es necesario resolver los problemas de conectividad de la red.

C. Verificar un problema de inicialización

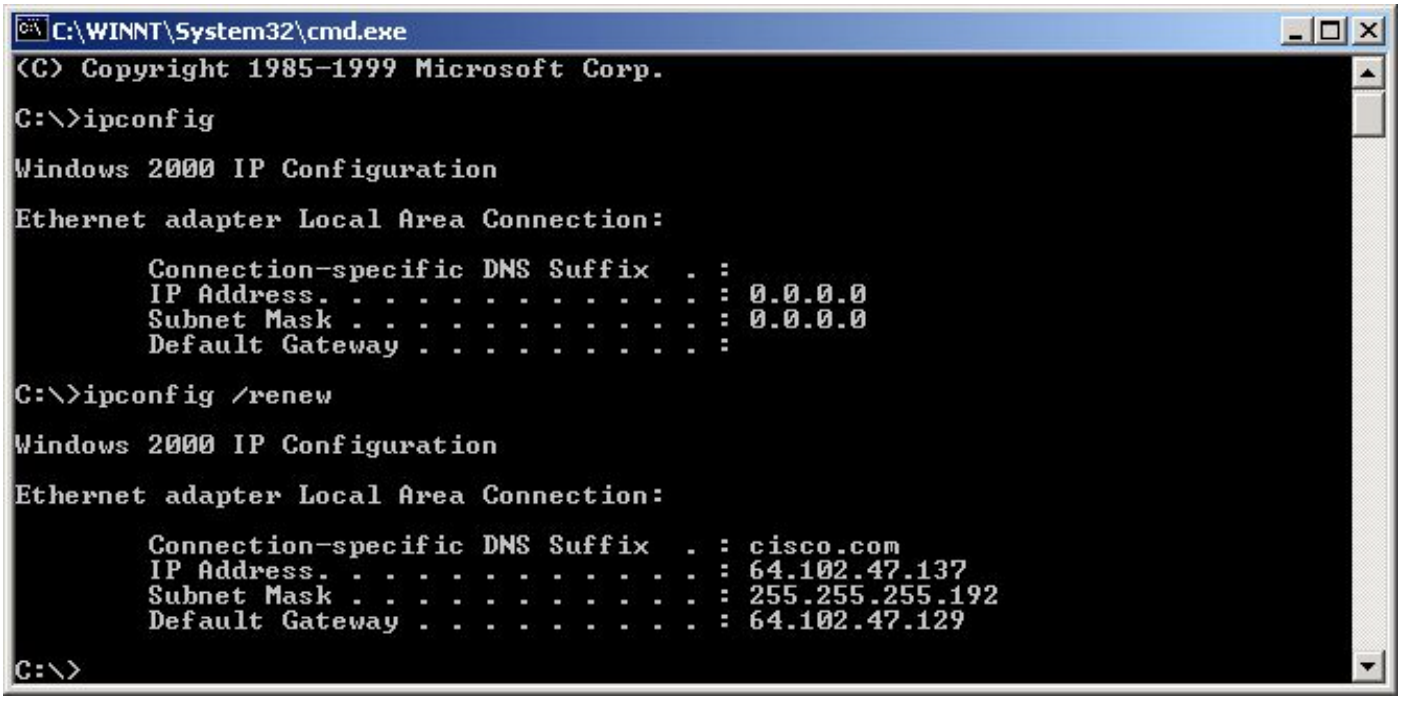
Este procedimiento se puede aplicar a todos los estudios de caso.

Si el cliente DHCP no puede obtener una dirección de IP del servidor DHCP durante el inicio, intente obtener una dirección IP del servidor DHCP forzando manualmente al cliente a enviar una petición DHCP. Ejecute los siguientes pasos para obtener manualmente una dirección IP de un servidor DHCP para los sistemas operativos que se listan a continuación.

Microsoft Windows 95/98/ME: Haga clic en el botón **Inicio**, y ejecute el programa WINIPCFG.exe. Haga clic en el botón **Release All (Liberar todo)**, seguido por el botón **Renew All (Renovar todo**. ¿El cliente DHCP es ahora capaz de obtener una dirección IP?



Microsoft Windows NT/2000: Abra una ventana de indicador de comandos especificando **cmd** en el campo **Inicio/Ejecutar**. Ejecute el comando **ipconfig/renew** en la ventana de indicador de comandos, como se ilustra a continuación: ¿Puede ahora el cliente DHCP obtener una dirección IP?



Si el cliente DHCP puede obtener una dirección IP al renovar manualmente la dirección IP después de que el equipo haya finalizado el proceso de inicio del sistema, es probable que el problema sea del inicio de DHCP. Si el cliente DHCP se conecta a un switch Catalyst de Cisco, es

probable que el problema se deba a un problema de configuración relacionado con STP portfast y/o canalización y conexión troncal. Otras posibilidades son los problemas con las tarjetas NIC y con el inicio del puerto del switch. Los pasos D y E de la resolución de problemas deberían revisarse para regularizar la configuración del puerto del switch y los problemas de la tarjeta NIC, ya que es la causa principal del problema DHCP.

D. Verifique la configuración del puerto del switch (STP Portfast y otros comandos)

Si el switch es un Catalyst 2900/4000/5000/6000, verifique que el puerto tenga STP portfast habilitado y la conexión troncal/canalización inhabilitada. La configuración predeterminada es STP portfast inhabilitado y conexión troncal/canalización automática, si corresponde. Para los switches 2900XL/3500XL/2950/3550, STP portfast es la única configuración necesaria. Estos cambios de configuración resuelven los problemas del cliente DHCP más comunes que se producen en la instalación inicial de un switch Catalyst.

Para más documentación relativa a los requisitos necesarios de configuración del puerto del switch para que DHCP funcione correctamente cuando está conectado a los switches Catalyst, consulte el siguiente documento:

Using Portfast and Other Commands to Fix Workstation Startup Connectivity Delays (Utilización de PortFast y otros comandos para solucionar retrasos al iniciar la conectividad de la estación de trabajo)

Una vez que haya revisado las directrices de configuración del documento anterior, vuelva a este documento para resolver problemas adicionales.

E. Compruebe los problemas conocidos de la tarjeta NIC o de los switches de Catalyst

Si la configuración del switch Catalyst es correcta, es posible que haya un problema de compatibilidad de software en el switch de Catalyst o en el NIC del cliente DHCP que podría estar causando problemas de DHCP. El próximo paso en la resolución de problemas es revisar el siguiente documento y dictaminar cualquier problema de software con el switch Catalyst o NIC que pueda contribuir al problema:

Troubleshooting Cisco Catalyst Switches to NIC Compatibility Issues (Resolución de problemas de compatibilidad entre los switches Catalyst de Cisco y las NIC)

Para descartar adecuadamente cualquier problema de compatibilidad, es necesario tener conocimiento del sistema operativo del cliente DHCP así como también de la información específica de la NIC; como por ejemplo, fabricante, modelo y versión de controlador.

F. Distinción entre si los clientes DHCP obtienen su dirección IP en la misma subred o en la VLAN como servidor DHCP

Es importante distinguir si DHCP funciona correctamente cuando el cliente se encuentra en la misma subred o VLAN que el servidor DHCP. Si el DHCP funciona correctamente en la misma subred o VLAN como el servidor de DHCP, el problema DHCP puede ser con el agente de retransmisión DHCP/BootP. Si el problema persiste, aun probando con DHCP en la misma subred o VLAN como el servidor DHCP, es posible que el problema sea el servidor DHCP.

G. Compruebe la configuración del router de retransmisión DHCP/BootP

Siga los pasos que figuran a continuación para comprobar la configuración:

Cuando configure la retransmisión DHCP en un router, verifique que el comando **ip helper-address** está en la interfaz correcta. El comando **ip helper-address** debe estar presente en la interfaz de entrada de las estaciones de trabajo cliente DHCP y debe direccionarse al servidor DHCP correcto.

Compruebe que el comando de configuración global **no service dhcp**no esté presente. Este parámetro de configuración inhabilitará todos los servidores DHCP y la función de retransmisión en el router. La configuración predeterminada, `service dhcp`, no aparece en la configuración, y es el comando de configuración predeterminado.

Cuando aplique los comandos **ip helper-address** para reenviar difusiones UDP a una dirección de difusión de subred, verifique que `no ip directed-broadcast` no se haya configurado en ninguna interfaz de salida que los paquetes UDP tengan que atravesar. El comando no ip directed-broadcast bloqueará cualquier traducción de una difusión directa a difusiones físicas. Esta configuración de interfaz es la configuración predeterminada en las versiones 12.0 y posteriores.

El reenvío de difusiones DHCP a la dirección de difusión de subred del servidor DHCP es un problema de software aislado. Cuando se solucionen problemas en DHCP, intente reenviar siempre difusiones DHCP UDP a la dirección IP del servidor DHCP, como se muestra a continuación:

```
Switch#show interface fastEthernet 0/1
FastEthernet0/1 is up, line protocol is up
Hardware is Fast Ethernet, address is 0030.94dc.acc1
(bia 0030.94dc.acc1)
```

H. Depuración de DHCP mediante los comandos de depuración del router

Verifique que el router recibe la petición DHCP con los comandos de depuración

En routers que soportan el procesamiento por software de paquetes DHCP, puede verificar si un router recibe la petición DHCP del cliente. El proceso de DHCP no tendrá éxito si el router no recibe peticiones del cliente. Este paso en la resolución de problemas implica configurar una lista de acceso para la salida de información de depuración. Esta lista de acceso sólo se usa para la depuración y no obstaculiza el funcionamiento del router.

En el modo de configuración global, ingrese la siguiente lista de acceso:

access-list 100 permit ip host 0.0.0.0 host 255.255.255.255

En el modo EXEC, ingrese el siguiente comando de depuración:

debug ip packet detail 100

Ejemplo de resultado

```
Router#debug ip packet detail 100
IP packet debugging is on (detailed) for access list 100
Router#
00:16:46: IP: s=0.0.0.0 (Ethernet4/0), d=255.255.255.255, len 604, rcvd 2
00:16:46: UDP src=68, dst=67
00:16:46: IP: s=0.0.0.0 (Ethernet4/0), d=255.255.255.255, len 604, rcvd 2
```

```
00:16:46: UDP src=68, dst=67
```

Del resultado expuesto anteriormente, se deduce que el router está recibiendo peticiones DHCP del cliente. Esta salida sólo muestra un resumen del paquete y no el paquete en sí. Por lo tanto, no es posible determinar si el paquete es correcto. Sin embargo, el router recibió un paquete de difusión con las IP de origen y de destino y los puertos UDP que son adecuados para DHCP.

Verifique que el router esté recibiendo la petición DHCP y reenviando peticiones al servidor DHCP con comandos de depuración.

Se pueden agregar más entradas en la lista de acceso para determinar si el router se está comunicando correctamente con el servidor DHCP. Nuevamente, estas depuraciones no analizan el paquete, pero pueden confirmar si el agente de retransmisión DHCP reenvía o no las peticiones al servidor DHCP.

En el modo de configuración global, cree la siguiente lista de acceso:

access-list 100 permit ip host 0.0.0.0 host 255.255.255.255

access-list 100 permit udp host <dhcp_relay_agent> host <dhcp_server> eq 67

access-list 100 permit udp host <dhcp_server> host <dhcp_relay_agent> eq 67

Por ejemplo:

access-list 100 permit ip host 0.0.0.0 host 255.255.255.0

access-list 100 permit udp host 192.168.1.1 host 192.168.2.2 eq 67

access-list 100 permit udp host 192.168.1.1 host 192.168.2.2 eq 68

access-list 100 permit udp host 192.168.2.2 host 192.168.1.1 eq 67

access-list 100 permit udp host 192.168.2.2 host 192.168.1.1 eq 68

En el modo EXEC, ingrese el siguiente comando de depuración:

```
Router#debug ip packet detail 100
IP packet debugging is on (detailed) for access list 100
Router#
00:16:46: IP: s=0.0.0.0 (Ethernet4/0), d=255.255.255.255, len 604, rcvd 2
00:16:46: UDP src=68, dst=67
00:16:46: IP: s=0.0.0.0 (Ethernet4/0), d=255.255.255.255, len 604, rcvd 2
00:16:46: UDP src=68, dst=67
```

Del resultado anterior se deduce que el router recibe las peticiones DHCP del cliente, y que reenvía la petición, por configuración de agente de retransmisión DHCP/BootP, al servidor DHCP. El servidor DHCP también respondió directamente al agente de retransmisión DHCP/BootP. Esta salida sólo muestra un resumen del paquete y no el paquete en sí. Por lo tanto, no es posible determinar si el paquete es correcto o si el servidor responde con un DHCPNAK. Sin embargo, el router recibió un paquete de difusión con las IP de origen y destino y los puertos UDP que son adecuados para DHCP, y hay comunicación bidireccional con el servidor DHCP.

Verifique que el router recibe y reenvía la petición DHCP con el comando debug ip udp

El comando **debug ip udp** se puede usar para rastrear la trayectoria de una petición DHCP a

través de un router. Sin embargo, esta depuración obstaculiza el funcionamiento normal en un entorno de producción, ya que todos los paquetes UDP conmutados procesados se muestran en la consola. Esta depuración no debe utilizarse en producción.

Advertencias: El comando **debug ip udp** obstaculiza el funcionamiento normal y puede tener como consecuencia un uso elevado de la Unidad central de procesamiento (CPU).

En el modo EXEC, ingrese el siguiente comando de depuración:

debug ip udp

Ejemplo de resultado

```
Router#debug ip udp
UDP packet debugging is on
Router#

00:18:48: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
!--- El router que recibe DHCPDISCOVER del cliente DHCP. 00:18:48: UDP: sent
src=192.168.1.1(67), dst=192.168.2.2(67), length=604 !--- El router que reenvía
DHCPDISCOVER por unidifusión al servidor DHCP !--- con la dirección IP de origen del
agente de retransmisión DHCP/BootP. 00:18:48: UDP: rcvd src=192.168.2.2(67),
dst=192.168.1.1(67), length=313 !--- El router que recibe DHCPOFFER del servidor DHCP
!--- dirigido a la dirección IP del agente de retransmisión DHCP/BootP. 00:18:48:
UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=333 !--- El router que
reenvía DHCPOFFER del servidor DHCP !--- al cliente DHCP por el agente de
retransmisión DHCP/BootP. 00:18:48: UDP: rcvd src=0.0.0.0(68),
dst=255.255.255.255(67), length=584 !--- El router que recibe DHCPREQUEST del cliente
DHCP. 00:18:48: UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604 !---
El router que reenvía DHCPDISCOVER por unidifusión al servidor DHCP !--- con la
dirección IP de origen del agente de retransmisión DHCP/BootP. 00:18:48: UDP: rcvd
src=192.168.2.2(67), dst=192.168.1.1(67), length=313 !--- El router que recibe
DHCPACK (o DHCPNAK) del DHCP !--- dirigido a la dirección IP del agente de
retransmisión DHCP/BootP. 00:18:48: UDP: sent src=0.0.0.0(67),
dst=255.255.255.255(68), length=333 !--- El router que reenvía DHCPACK (o DHCPNAK) al
cliente DHCP !--- mediante el agente de retransmisión DHCP/BootP. 00:18:48: UDP: rcvd
src=192.168.1.2(520), dst=255.255.255.255(520), length=32 !--- El cliente DHCP que
verifica la dirección IP !--- que no se usa mediante el envío de una petición ARP
para su propia dirección IP. 00:18:50: UDP: rcvd src=192.168.1.2(520),
dst=255.255.255.255(520), length=32 !--- El cliente DHCP que verifica la dirección IP
!--- que no se usa mediante el envío de una petición ARP para su propia dirección IP.
```

Verifique que el router recibe y reenvía la petición DHCP con el comando debug ip dhcp server packet.

Si el router IOS es 12.0.x.T o 12.1 y soporta la función de servidor IOS DHCP, la depuración adicional se puede efectuar con el comando **debug ip dhcp server packet**. Esta depuración se había diseñado para usarla con la función del servidor IOS DHCP, pero se puede usar también para solucionar problemas de la función Agente de retransmisión DHCP/BootP. Al igual que ocurre con los anteriores pasos de resolución, los comandos de depuración no determinan exactamente el problema, porque el paquete real no se puede ver. Sin embargo, las depuraciones permiten efectuar inferencias relacionadas con el procesamiento DHCP.

En el modo EXEC, ingrese el siguiente comando de depuración:

debug ip dhcp server packet

```
Router#debug ip dhcp server packet
00:20:54: DHCPD: setting giaddr to 192.168.1.1.
!--- El router recibió DHCPDISCOVER/REQUEST/INRORM y se definió la dirección IP de la
gateway !--- en 192.168.1.1 para su reenvío. 00:20:54: DHCPD: BOOTREQUEST from
0063.6973.636f.2d30.3065.302e.3165.6632.2e63.. !--- BOOTREQUEST incluye DHCPDISCOVER,
DHCPREQUEST y DHCPINFORM. !--- 0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indica el
identificador del cliente. 00:20:54: DHCPD: forwarding BOOTREPLY to client
00e0.1ef2.c441. !--- BOOTREPLY incluye DHCPOFFER y DHCPNAK. !--- La dirección MAC del
cliente es 00e0.1ef2.c441. 00:20:54: DHCPD: broadcasting BOOTREPLY to client
00e0.1ef2.c441. !--- El router está reenviando difusión DHCPOFFER o DHCPNAK en la
interfaz LAN local. 00:20:54: DHCPD: setting giaddr to 192.168.1.1. !--- El router
recibió DHCPDISCOVER/REQUEST/INFORM y se definió la dirección IP de la gateway !---
en 192.168.1.1 para su reenvío. 00:20:54: DHCPD: BOOTREQUEST from
0063.6973.636f.2d30.3065.302e.3165.6632.2e63.. !--- BOOTREQUEST incluye DHCPDISCOVER,
DHCPREQUEST y DHCPINFORM. !--- 0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indica el
identificador del cliente. 00:20:54: DHCPD: forwarding BOOTREPLY to client
00e0.1ef2.c441. !--- BOOTREPLY incluye DHCPOFFER y DHCPNAK. !--- La dirección MAC del
cliente es 00e0.1ef2.c441. 00:20:54: DHCPD: broadcasting BOOTREPLY to client
00e0.1ef2.c441. !--- El router reenvía la difusión DHCPOFFER o DHCPNAK en la interfaz
LAN local.
```

Ejecución simultánea de depuraciones múltiples

Al ejecutar varias depuraciones de forma simultánea, es posible descubrir una buena cantidad de información sobre el funcionamiento del servidor y del agente de retransmisión DHCP/BootP. El uso de las anteriores pautas de solución de problemas permite hacer inferencias sobre dónde es posible que la función del agente de retransmisión DHCP/BootP no esté funcionando correctamente.

```
Router#debug ip dhcp server packet
00:20:54: DHCPD: setting giaddr to 192.168.1.1.
!--- El router recibió DHCPDISCOVER/REQUEST/INRORM y se definió la dirección IP de la
gateway !--- en 192.168.1.1 para su reenvío. 00:20:54: DHCPD: BOOTREQUEST from
0063.6973.636f.2d30.3065.302e.3165.6632.2e63.. !--- BOOTREQUEST incluye DHCPDISCOVER,
DHCPREQUEST y DHCPINFORM. !--- 0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indica el
identificador del cliente. 00:20:54: DHCPD: forwarding BOOTREPLY to client
00e0.1ef2.c441. !--- BOOTREPLY incluye DHCPOFFER y DHCPNAK. !--- La dirección MAC del
cliente es 00e0.1ef2.c441. 00:20:54: DHCPD: broadcasting BOOTREPLY to client
00e0.1ef2.c441. !--- El router está reenviando difusión DHCPOFFER o DHCPNAK en la
interfaz LAN local. 00:20:54: DHCPD: setting giaddr to 192.168.1.1. !--- El router
recibió DHCPDISCOVER/REQUEST/INFORM y se definió la dirección IP de la gateway !---
en 192.168.1.1 para su reenvío. 00:20:54: DHCPD: BOOTREQUEST from
0063.6973.636f.2d30.3065.302e.3165.6632.2e63.. !--- BOOTREQUEST incluye DHCPDISCOVER,
DHCPREQUEST y DHCPINFORM. !--- 0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indica el
identificador del cliente. 00:20:54: DHCPD: forwarding BOOTREPLY to client
00e0.1ef2.c441. !--- BOOTREPLY incluye DHCPOFFER y DHCPNAK. !--- La dirección MAC del
cliente es 00e0.1ef2.c441. 00:20:54: DHCPD: broadcasting BOOTREPLY to client
00e0.1ef2.c441. !--- El router reenvía la difusión DHCPOFFER o DHCPNAK en la interfaz
LAN local.
```

Utilice trazas de rastreador (sniffer) para determinar la causa raíz del problema de DHCP

El uso de técnicas de depuración del router no siempre determina la causa raíz exacta de un problema DHCP. El último paso para solucionar un problema de DHCP es obtener una traza de rastreador y detectar en qué parte el proceso no funciona correctamente. Las trazas de los paquetes DHCP se pueden descifrar remitiéndose a las secciones de este documento Decodificación de trazas de rastreador de cliente y servidor DHCP en un mismo segmento de LAN y Decodificación de trazas de rastreador de cliente y servidor DHCP separados por un router configurado como un agente de retransmisión DHCP.

Si desea más información sobre cómo obtener trazas de rastreador con la función Analizador de Puertos del Switch (SPAN), en los switches de Cisco, consulte el siguiente documento:

> Configuring the Catalyst Switched Port Analyzer (SPAN) (Configuración del Analizador de puerto conmutado de Catalyst).

Método alternativo de decodificación de paquetes mediante depuración en el router

Al usar el comando **debug ip packet detail dump <acl>** en el router de Cisco, es posible obtener un paquete completo en hexadecimal que aparece en el registro del sistema o la interfaz de línea de comando (CLI). Si usa las secciones Verifique que el router está recibiendo la petición DHCP con los comandos de depuración y Verifique que el router está recibiendo la petición DHCP y reenviando peticiones al servidor DHCP con comandos de depuración, junto con la palabra clave dump agregada a la lista de acceso, obtendrá la misma información de depuración, pero con el detalle de paquete en hexadecimal. Para determinar el contenido del paquete, éste debe traducirse. En el Apéndice A se presenta un ejemplo.

Apéndice A: Configuración de IOS DHCP de muestra

La base de datos del servidor DHCP se organiza como un árbol. La raíz del árbol es la agrupación de direcciones para las redes naturales, las ramas son agrupaciones de direcciones de subred y las hojas, vinculaciones manuales a clientes. Las subredes heredan los parámetros de la red y los clientes heredan los parámetros de las subredes. Por lo tanto, los parámetros comunes, como el nombre de dominio, deberían configurarse en el nivel más elevado (red o subred) del árbol.

Si desea más información sobre cómo configurar DHCP y sus comandos asociados, consulte el siguiente enlace:

> Lista de tareas de configuración de DHCP

```
Router#debug ip dhcp server packet
00:20:54: DHCPD: setting giaddr to 192.168.1.1.
!--- El router recibió DHCPDISCOVER/REQUEST/INRORM y se
definió la dirección IP de la gateway !--- en
192.168.1.1 para su reenvío. 00:20:54: DHCPD:
BOOTREQUEST from
0063.6973.636f.2d30.3065.302e.3165.6632.2e63.. !---
BOOTREQUEST incluye DHCPDISCOVER, DHCPREQUEST y
DHCPINFORM. !---
0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indica el
identificador del cliente. 00:20:54: DHCPD: forwarding
```

```
BOOTREPLY to client 00e0.1ef2.c441. !--- BOOTREPLY
incluye DHCPOFFER y DHCPNAK. !--- La dirección MAC del
cliente es 00e0.1ef2.c441. 00:20:54: DHCPD: broadcasting
BOOTREPLY to client 00e0.1ef2.c441. !--- El router está
reenviando difusión DHCPOFFER o DHCPNAK en la interfaz
LAN local. 00:20:54: DHCPD: setting giaddr to
192.168.1.1. !--- El router recibió
DHCPDISCOVER/REQUEST/INFORM y se definió la dirección IP
de la gateway !--- en 192.168.1.1 para su reenvío.
00:20:54: DHCPD: BOOTREQUEST from
0063.6973.636f.2d30.3065.302e.3165.6632.2e63.. !---
BOOTREQUEST incluye DHCPDISCOVER, DHCPREQUEST y
DHCPINFORM. !---
0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indica el
identificador del cliente. 00:20:54: DHCPD: forwarding
BOOTREPLY to client 00e0.1ef2.c441. !--- BOOTREPLY
incluye DHCPOFFER y DHCPNAK. !--- La dirección MAC del
cliente es 00e0.1ef2.c441. 00:20:54: DHCPD: broadcasting
BOOTREPLY to client 00e0.1ef2.c441. !--- El router
reenvía la difusión DHCPOFFER o DHCPNAK en la interfaz
LAN local.
```