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

Contenido

Introducción

Este documento contiene información sobre cómo resolver varios problemas comunes de Dynamic Host Configuration Protocol (DHCP) que pueden surgir dentro de una red de switch Cisco Catalyst. Este documento incluye una guía de resolución de problemas relativos al uso de la característica Cisco IOS® DHCP/BootP Relay Agent.

prerrequisitos

Requisitos

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 verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

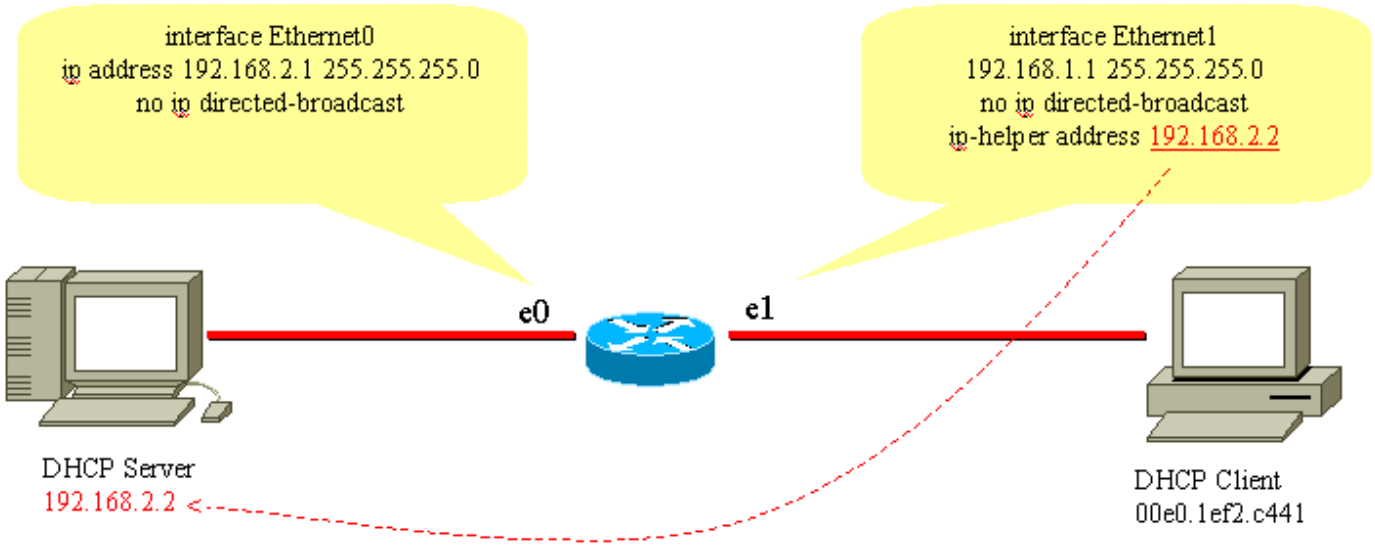
‘Conceptos clave’

Éstos son varios conceptos fundamentales de 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.
- El Routers, por abandono, no remite los broadcasts. Se necesita para acomodar 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 Relay DHCP.
- La implementación del router de Cisco del relé DHCP se proporciona a través de los **comandos ip helper del interfaz-**nivel

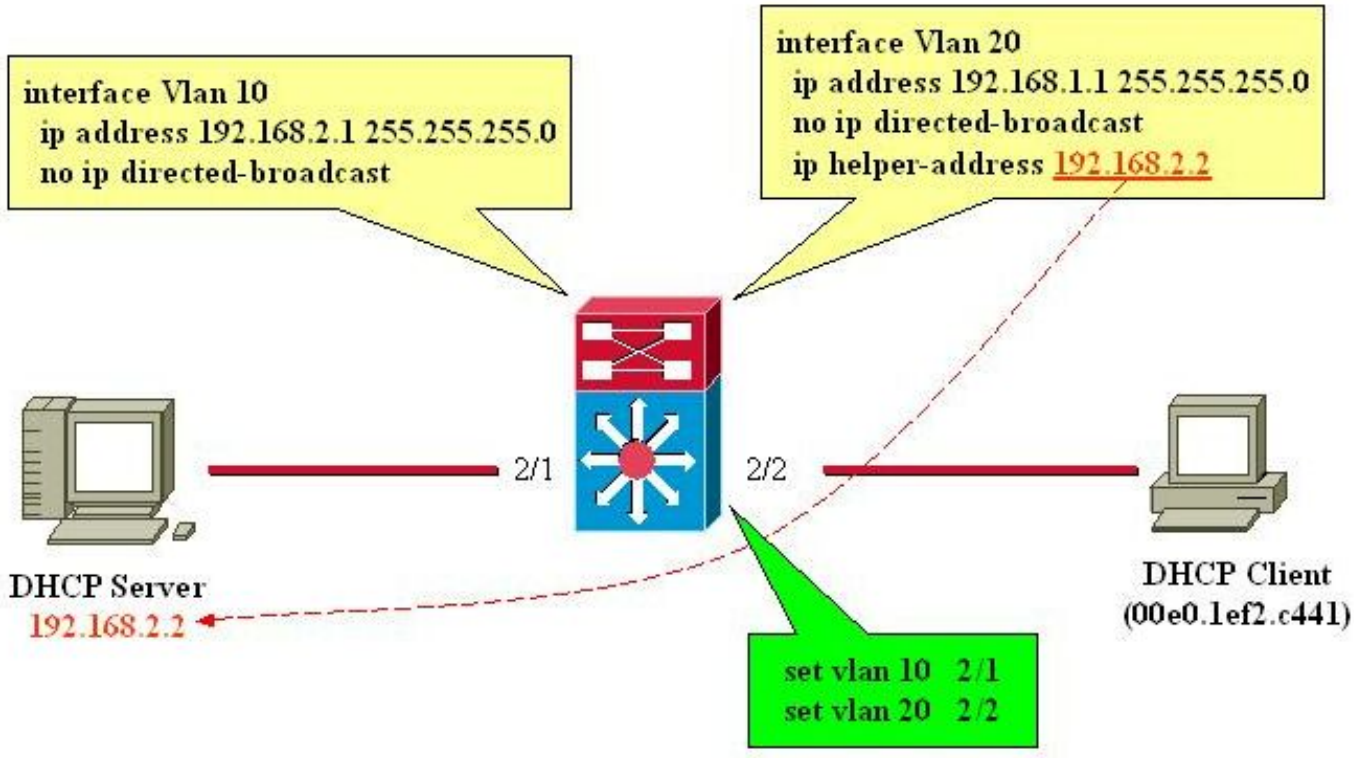
“Situaciones de ejemplo”

Escenario 1: Encaminamiento del router Cisco entre el Cliente de DHCP y las redes del servidor



Como está configurado en este diagrama, Ethernet1 de la interfaz adelante el DHCPDISCOVER transmitido del cliente a 192.168.2.2 con el Ethernet1 de la interfaz. El servidor DHCP satisface la solicitud con el unicast. En este ejemplo, no se necesita más configuración para el router.

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



Como está configurado en el diagrama, interfaz VLAN20 adelante el DHCPDISCOVER transmitido del cliente a 192.168.2.2 a través de la interfaz VLAN10. El servidor DHCP satisface la solicitud con el unicast. En este ejemplo, no se necesita más configuración para el router. Los puertos del switch necesitan ser configurados como puertos de host y tienen portfast del Spanning-Tree Protocol (STP) habilitado, y enlace y canalización inhabilitados.

Antecedentes

El DHCP proporciona un mecanismo a través del cual los ordenadores que utilizan el Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP) puedan obtener los parámetros de la configuración del protocolo automáticamente a través de la red. El DHCP es un estándar abierto que fue desarrollado por el Dynamic Host Configuration-Working Group (DHC-WG) de la Fuerza de tareas de ingeniería en Internet (IETF) (IETF).

El DHCP se basa en un paradigma del servidor del cliente, en el cual el Cliente de DHCP, por ejemplo, una computadora de escritorio, entra en contacto a un servidor DHCP para los parámetros de la configuración. Por lo general, el servidor DHCP está ubicado de manera central y el administrador de red lo opera. Debido a que el servidor es ejecutado por un administrador de red, los clientes DHCP pueden ser configurados de manera confiable y dinámica con parámetros apropiados para la arquitectura de la red actual.

La mayor parte de las redes de empresa están compuestas por varias subredes divididas en múltiples arquitecturas de subredes, denominadas Virtual LANs (VLAN), en las cuales los routers enrutan entre las subredes. Debido a que los routers no pasan difusión por defecto, será necesario un servidor DHCP en cada subred a menos que los routers sean configurados para reenviar la difusión DHCP utilizando la característica de Agente de relé DHCP.

Comprensión de DHCP

El DHCP fue definido originalmente en los pedidos los comentarios (RFC) 1531 , y obsoleted desde entonces por el RFC 2131 . El DHCP se basa en el Bootstrap Protocol (BOOTP), que se define en el RFC 951 .

El DHCP es utilizado por los puestos de trabajo (host) para conseguir la información de configuración inicial, tal como un IP Address, una máscara de subred, y un default gateway sobre el bootup. Como cada host necesita una dirección IP para comunicarse con una red IP, DHCP disminuye la tarea administrativa de tener que configurar manualmente cada host con una dirección IP. Además, si un host se mueve a una diversa subred IP, debe utilizar una diversa dirección IP que la él utilizó previamente. El DHCP toma el cuidado de esto automáticamente. Permite que el host elija 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 - Interoperation entre el DHCP y el 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
- RFC 2489 - Procedimiento para definir las nuevas opciones DHCP

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. Estos parámetros de configuración son arrendados por el servidor al cliente durante un período especificado. Cuando un host arranca, la pila de TCP/IP en el host transmite un mensaje del broadcast (DHCPDISCOVER) para ganar una dirección IP y a una máscara de subred, entre otros parámetros de la configuración. Esto inicia un intercambio entre el servidor DHCP y el host.

Durante este intercambio, el cliente pasa a través de los varios estados bien definidos enumerados abajo:

1. Inicialización
2. Selección
3. Petición
4. Límite
5. Renovación
6. Revinculación

Al moverse entre los estados detallados anteriormente, 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	Utilice
0x01	DHCPDISCOVER	El cliente está buscando servidores DHCP disponibles.
0x02	DHCPOFFER	La respuesta del servidor al cliente DHCPDISCOVER.
0x03	DHCPREQUEST	Los broadcasts del cliente al servidor, pidiendo los parámetros ofrecidos a partir de un servidor específicamente, según lo definido en el paquete.
0x04	DHCPDECLINE	La comunicación entre cliente y servidor, que indica que la dirección de red ya está en uso.
0x05	DHCPACK	La comunicación de servidor a cliente con los parámetros de la configuración, incluyendo la dirección de red confiada.
0x06	DHCPNAK	La comunicación de servidor a cliente, rechazando el pedido el parámetro de la configuración.
0x07	DHCPRELEASE	La comunicación entre cliente y servidor, abandonando a la dirección de red y cancelando el arriendo restante.
0x08	DHCPINFORM	La comunicación entre cliente y servidor, preguntando solamente los parámetros de la configuración local que el cliente externamente ha configurado ya como direccionamiento.

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 de Protocolo

de datagrama de usuario (UDP) (servidor del BOOTP). Debido a que el cliente no tiene forma de conocer la subred a la que pertenece, el DHCPDISCOVER es una difusión de todas las subredes (dirección IP de destino de 255.255.255.255), con una dirección IP de origen de 0.0.0.0. La dirección IP de origen es 0.0.0.0, porque el cliente no posee una dirección IP configurada. Si en esta subred local hay un servidor DHCP configurado correctamente y en funcionamiento, el servidor DHCP podrá oír la transmisión y responder mediante un mensaje DHCPOFFER. Si no existe un servidor DHCP en la subred local, debe existir un agente de relé DHCP/BootP en esta subred local para reenviar el mensaje DHCPDISCOVER a una subred que contenga un servidor DHCP.

Este Agente Relay puede cualquiera ser un host dedicado (por ejemplo, Microsoft Windows server), o router (por ejemplo, un router Cisco configurado con las declaraciones del nivel de la interfaz ayuda IP).

DHCPOFFER

Un servidor DHCP que recibe un mensaje DHCPDISCOVER puede responder con uno DHCPOFFER el puerto 68 de UDP (cliente BootP). El cliente recibe el DHCPOFFER y pasa al estado Selecting (Seleccionando). Este mensaje dhcpoffer contiene la información de configuración inicial para el 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 los campos opciones, máscara de subred y opciones del router, respectivamente. Otras opciones comunes en el mensaje DHCPOFFER incluyen tiempo de arriendo de dirección IP, hora de renovación, servidor de nombres de dominio y el servidor de nombres de NetBIOS (WINS). El servidor DHCP enviará el DHCPOFFER a la dirección de broadcast, pero incluirá a la dirección de hardware de los clientes en el campo del chaddr de la oferta, así que el cliente sabe que es el destino deseado. 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 relé DHCP/BootP de donde vino el DHCPDISCOVER. El DHCP/BootP Relay Agent entonces transmitirá o unicast el DHCPOFFER en la subred local en el puerto 68 UDP, dependiendo del indicador de broadcast fijado por cliente BOOTP.

DHCPREQUEST

Luego de que 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 Solicitud. 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 opciones del Identificador del servidor. DHCPREQUEST también es una difusión; por lo tanto, todos los servidores DHCP que enviaron la DHCPOFFER verán la DHCPREQUEST y cada uno sabrá si su DHCPOFFER fue aceptada o rechazada. Todas las opciones adicionales de configuración que solicite el cliente estarán incluidas en el campo de opciones del mensaje DHCPREQUEST. Si bien se le ha ofrecido al cliente una dirección IP, se le enviará el mensaje DHCPREQUEST con la dirección IP de origen 0.0.0.0. A esta altura, el cliente no ha recibido aún una verificación de que puede utilizar la dirección IP.

DHCPACK

Después de que el servidor DHCP recibe la solicitud DHCPREQUEST, éste reconoce la solicitud

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 transmisión y contiene todos los parámetros que el cliente solicitó en el mensaje DHCPREQUEST. Cuando el cliente recibe el DHCP ACK, ingresa al estado límite y se encuentra libre para usar la dirección IP para comunicarse a la red.. Mientras tanto, el servidor DHCP almacena el arrendamiento en su base de datos y lo identifica excepcionalmente utilizando el identificador de clientes o chaddr y la dirección IP asociada. Tanto el cliente como el servidor utilizarán esta combinación de identificadores para referirse al arrendamiento. El Identificador de cliente es el MAC address del dispositivo más el tipo de media.

Antes de que DHCP cliente comience a utilizar la nueva dirección, éste debe calcular los parámetros de tiempo asociados con la dirección arrendada, que son Lease Time (LT) (Tiempo de arrendamiento), Renewal Time (T1) (Tiempo de renovación) y Rebind Time (T2) (Tiempo de revinculación). El LT típico predeterminado es de 72 horas. Puede utilizar tiempos de validez más cortos para conservar las direcciones, si es necesario.

DHCPNAK

Si el servidor seleccionado no puede satisfacer 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 ingresando al estado de petición. El cliente volverá a transmitir la DHCPREQUEST (Solicitud DHCP) al menos cuatro veces dentro de 60 segundos antes de reiniciar el estado de Inicialización.

DHCPDECLINE

El cliente recibe el DHCPACK y podrá optar por hacer una verificación final de los parámetros. El cliente realiza este procedimiento al enviar peticiones de Protocolo de resolución de dirección (ARP) para la dirección IP que se brinda en el DHCPACK. Si el cliente detecta que el direccionamiento es ya funcionando recibiendo una contestación al pedido ARP, el cliente enviará un mensaje DHCPDECLINE al servidor y recomenzará el proceso de configuración entrando el estado solicitante.

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 solicitud DHCPINFORM para obtener otros parámetros de configuración local, tal como el nombre de dominio y los Servidores de nombre de dominio (DNSs). 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 de IP. Este DHCPACK será enviado unicast al cliente.

DHCPRELEASE

Un Cliente de DHCP puede elegir abandonar su arriendo en una dirección de red enviando un mensaje dhcprelease al servidor DHCP. El cliente identifica el arrendamiento que se debe liberar mediante el campo de identificación de cliente y dirección de red en el mensaje DHCPRELEASE. Si usted necesita prolongar el rango actual del agrupamiento DHCP, quite a la agrupación de direcciones actual y especifique el nuevo rango de los IP Addresses bajo agrupamiento DHCP.

Para quitar los IP Addresses específicos o un rango de direcciones que usted quiere para estar en el agrupamiento DHCP, utilice el comando ip dhcp excluded-address.

Nota: Si los dispositivos utilizan el BOOTP, los arriendos infinitos de la longitud se muestran en los atascamientos del DHCP del Routers.

Renovación de la licencia

Debido a que la dirección de IP es arrendada únicamente desde el servidor, la licencia debe renovarse periódicamente. Cuando ha expirado una mitad del Tiempo de validez (T1=0.5 x LT), el cliente intentará renovar el arriendo. El cliente ingresa en el estado de renovación y envía un mensaje DHCPREQUEST al servidor, que mantiene la validez actual. El servidor responderá a la petición de renovación con un mensaje DHCPACK si está de acuerdo con la renovación del arriendo. El mensaje DHCPACK contendrá el nuevo arriendo y los nuevos parámetros de configuración, en el caso que se hayan realizado cambios en el servidor durante el período de arrendamiento anterior. Si por alguna razón el cliente no puede alcanzar el servidor que contiene la licencia, intentará renovar la dirección de todo servidor DHCP una vez que el servidor DHCP original no haya respondido a las solicitudes de renovación dentro de un período T2. El valor predeterminado del 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 arrendada 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 durante un reinicio no debe completar el campo identificador del servidor, en lugar de eso debe completar el campo de la opción de dirección IP solicitada. Aquellos clientes que cumplen estrictamente con RFC poblarán 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 una cantidad de factores, como en el caso de los servidores DHCP de Windows NT, la versión del sistema operativo, entre otros factores, como superscoping (estudio de alcance amplio). Si el servidor DHCP determina que el cliente aún puede utilizar la dirección de IP solicitada, no hará nada o enviará un DHCPACK para el DHCPREQUEST. Si el servidor determina que el cliente no puede utilizar la dirección IP solicitada, enviará un DHCPNACK al cliente. Luego, el cliente avanzará al estado de inicialización y enviará un mensaje DHCPDISCOVER (Detección de DHCP).

Nota: El servidor DHCP asigna la dirección IP inferior de un pool de los IP Addresses a los clientes DHCP. Cuando expira el arriendo del direccionamiento inferior, se asigna a otro cliente si se pide. Usted no puede realizar ninguna cambios en los DHCP Address de la orden se asigna.

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 original BOOTP.

Campo	Bytes	Nombre	Descripción
op	1	OpCo	Identifica el paquete como una

		de	petición o contestación: 1=BOOTREQUEST, 2=BOOTREPLY
htype	1	Tipo de hardware	Especifica el tipo de dirección del hardware de red.
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 a través de 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 utilizan el ID (xid).
secs	2	Segundos	Especifica el número de segundos desde que el proceso DHCP comenzó.
indicadores	2	Indicadores	Indica si el mensaje será de difusión o de unidifusión.
ciaddr	4	Dirección IP del cliente	Sólo se utiliza cuando el cliente conoce la dirección de IP, como en el caso de los estados Bound, Renew, o Rebinding.
yiaddr	4	Su dirección IP	Si la dirección IP del cliente es 0.0.0.0, el servidor DHCP colocará la dirección IP del cliente ofrecida en este campo.
siaddr	4	Dirección IP del servidor	Si el cliente conoce la dirección IP del servidor DHCP, este campo será poblado con el direccionamiento del servidor DHCP. En caso contrario, será utilizado en DHCPOFFER y DHCPACK desde el servidor DHCP.
giaddr	4	Dirección IP del router (GIADDR)	La dirección IP de la gateway, completada por el agente de relevo 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 de archivo de iniciali zación	Nombre del archivo de 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

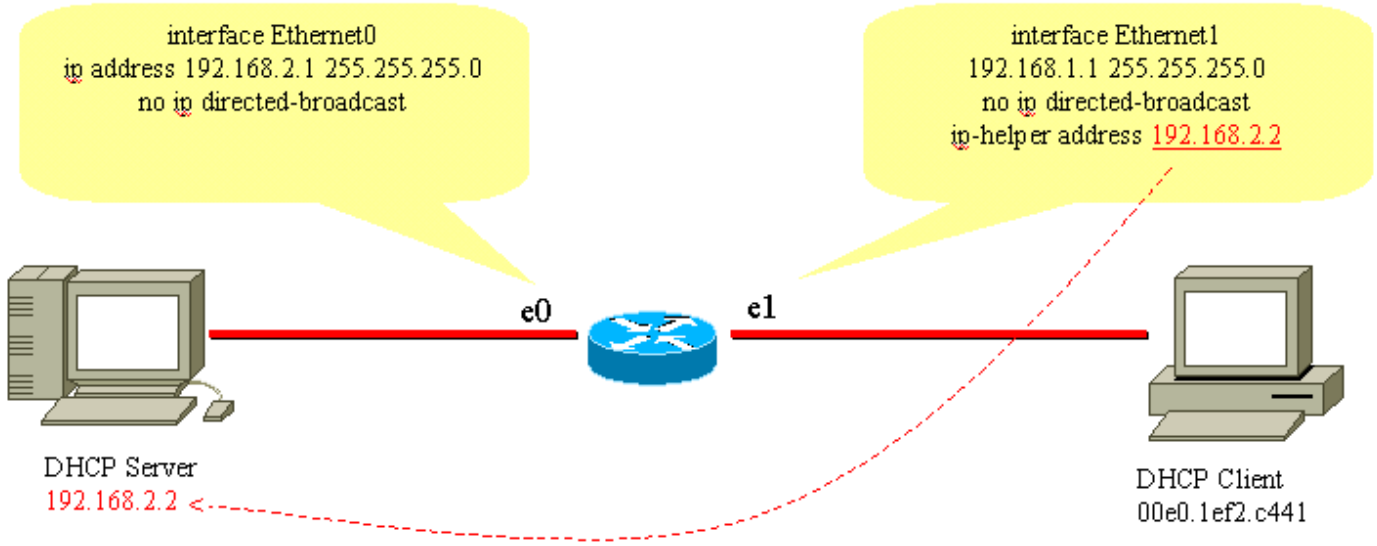
Descripción del paquete	Dirección MAC de origen	Direcciones MAC de destino	Addr IP de la fuente	Direc. IP de destino
DHCPDISCOVER	Cliente	Difusión	0.0.0.0	255.255.255.255
DHCPOFFER	Servidor DHCP	Difusión	Servidor DHCP	255.255.255.255
DHCPREQUEST	Cliente	Difusión	0.0.0.0	255.255.255.255
DHCPACK	Servidor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

Rol del agente de relé DHCP/BootP

El Routers, por abandono, no remitirá los paquetes de broadcast. Debido a que los mensajes del cliente DHCP utilizan la dirección IP de destino 255.255.255.255 (toda la transmisión de redes), los clientes DHCP no podrán enviar solicitudes a un servidor DHCP en otra subred a menos que el agente de relé DHCP/BootP esté configurado en el router. El Agente de relé DHCP/BootP solicita en nombre de un cliente DHCP al servidor DHCP. El agente de relé DHCP/BootP agregará su dirección de IP a la dirección de IP de origen de las tramas DHCP que van al servidor DHCP. Esto permite que el servidor DHCP responda vía el unicast al DHCP/BootP Relay Agent. El DHCP/BootP Relay Agent también poblará el campo de Gateway IP Address con la dirección IP de la interfaz en la cual el mensaje DHCP se recibe del cliente. El servidor DHCP utiliza el campo de Gateway IP Address para determinar la subred de la cual el DHCPDISCOVER, el DHCPREQUEST, o el mensaje DHCPINFORM origina.

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

Resulta fácil configurar un router de Cisco para reenviar solicitudes BootP o DHCP - configure un comando IP helper-address apuntando al servidor DHCP/BootP o apuntando a la dirección de transmisión de subred dentro de la red en la que está encendido el servidor. Por ejemplo, considere el siguiente diagrama de red:



Para reenviar la solicitud BootP/DHCP del cliente al servidor DHCP, se utiliza el comando ip helper-address interface. La dirección del ayudante IP puede ser configurada para reenviar cualquier transmisión UDP basada en el número de puerto UDP. Por abandono, el ip helper-address remitirá los broadcastes UDP siguientes:

- Protocolo trivial de transferencia de archivos (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)

Las direcciones del ayudante IP pueden realizar transmisiones directas de UDP a una dirección de IP de difusión o unidifusión. Sin embargo, no se recomienda utilizar IP helper-address para reenviar transmisiones UDP desde una subred a la dirección de transmisión de otra subred ya que podría ocasionarse un gran nivel inundación de transmisiones. IP múltiple las entradas del ayudante-direccionamiento en una sola interfaz se soportan también, como se muestra abajo:

```
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
```

```
hostname router
!
!
!
interface Ethernet0
ip address 192.168.2.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet1
ip address 192.168.1.1 255.255.255.0
ip helper-address 192.168.2.2
ip helper-address 192.168.2.3
!--- IP helper-address pointing to DHCP server no ip
directed-broadcast ! ! ! line con 0 exec-timeout 0 0
transport input none line aux 0 line vty 0 4 login ! end
```

Los routeres Cisco no soportan el Equilibrio de carga de los servidores DHCP que se configuran como agentes de relé DHCP. Los routeres Cisco transmiten al mensaje DHCPDISCOVER todas las direcciones del ayudante mencionadas para esa interfaz. Teniendo dos o más servidores DHCP servir una subred aumenta solamente el tráfico del DHCP mientras que los DHCPDISCOVER, los DHCPOFFER, y los DHCPREQUEST/los mensajes DHCPDECLINE se intercambian entre cada par de Cliente de DHCP y el servidor.

Determinación de los atascamientos manuales

Hay dos maneras de configurar los atascamientos manuales; uno está para el host de Windows, y el otro está para los host del no Windows. Hay dos diversos comandos usados para configurar; uno está para los clientes DHCP de Microsoft, y el otro está para los clientes DHCP de NON-Microsoft: Cliente-identificador del **DHCP** (atascamiento del manual - Clientes DHCP de Microsoft) y hardware-direccionamiento del **DHCP** (atascamiento del manual - clientes DHCP de NON-Microsoft). La razón de dos diversos comandos es que un PC que se ejecuta con Windows modifica sus MAC, y **01** se agrega al principio del direccionamiento. Las siguientes son configuraciones de ejemplo:

- Lo que sigue es la configuración para los clientes DHCP de Microsoft
  ```
  configuration terminal
  ip dhcp pool new_pool host ip_address subnet_mask client-identifier 01XXXXXXXXXXX !---
  xxxxxx represents 48 bit MAC address prepended with 01
  ```
- Lo que sigue es la configuración para los clientes DHCP de NON-Microsoft
  ```
  configuration terminal
  ip dhcp pool new_pool host ip_address subnet_mask hardware-address XXXXXXXXXXX !--- xxxxxx
  represents 48 bit MAC address
  ```

Cómo hacer el trabajo del DHCP en los segmentos secundarios IP

Por abandono, el DHCP tiene una limitación en que los paquetes de respuesta están enviados solamente si la solicitud se recibe de la interfaz configurada con el IP Address principal. El tráfico del DHCP utiliza a la dirección de broadcast. Cuando el pedido de DHCP es recibido por la interfaz del router, él adelante que al servidor DHCP (cuando se configura el ip helper-address) con una dirección de origen del IP primario configuró en la interfaz para dejar al servidor DHCP saber qué agrupación IP debe utilizar (para el cliente) en el paquete de la respuesta DHCP.

No hay manera para que el router sepa si la solicitud del broadcast DHCP viene de un dispositivo que esté en la red del IP secundaria configurada en la interfaz. Como solución alternativa, la configuración de la sub-interfaz (a condición de que el dispositivo conectado con el dot1q de los

soportes para router que marca con etiqueta) para separar las dos subredes puede ser configurada, así que ambos ellos consiguen sus IP Addresses correspondientes correctamente.

Si la dirección secundaria es la forma más utilizada, hay otra solución alternativa, que es habilitar Esto tiene una limitación en que utiliza solamente el IP secundario para retransmitir el pedido de DHCP si no hay respuesta del servidor DHCP después de que tres pedidos consecutivos el pool de la dirección primaria.

Conversación cliente-servidor DHCP con la función de retransmisión DHCP

La tabla abajo ilustra el proceso para que un Cliente de DHCP obtenga una dirección IP de un servidor DHCP. Esta tabla está basada 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 es también útil para determinar donde los problemas DHCP pueden ocurrir.

Paquete	Dirección 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 del 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 el DHCPDISCOVER en la interfaz del e1. El router reconoce que este paquete es una difusión DHCP	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

UDP. El router actuará ahora como un agente de relé DHCP/ BootP y completará el campo de dirección IP del gateway con la dirección IP de la interfaz entrante, cambiará la dirección IP de la fuente a una dirección IP de la interfaz entrante y reenviará el pedido directamente al servidor DHCP.							
3. El servidor DHCP ha recibido el DHCPDISCOV	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

ER y está enviando un DHCPOFFER al agente de relé DHCP.							
4. El Agente de seguro DHCP recibe un DHCPOFFER y reenviará la emisión 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 enviado del 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 el DHCPREQUEST en la interfaz del e1. El router reconoce que este paquete es de	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

transmisión DHCP UDP. El router ahora actuará como agente de relé DHCP y llenará adentro el campo de Gateway IP Address del IP Address de interfaz entrante, cambia la dirección IP de origen a un IP Address de interfaz entrante, y remite la solicitud directamente al servidor DHCP.							
7. El servidor DHCP ha recibido el DHSCP REQUEST y	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

está enviando un DHCPACK hacia el agente de retransmisión DHCP/BootP.							
8. El Agente de relé DHCP/BootP recibe el DHCPACK y reenviará la difusión de DHCPACK a través de la LAN local. El cliente validará el ACK y utilizará 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

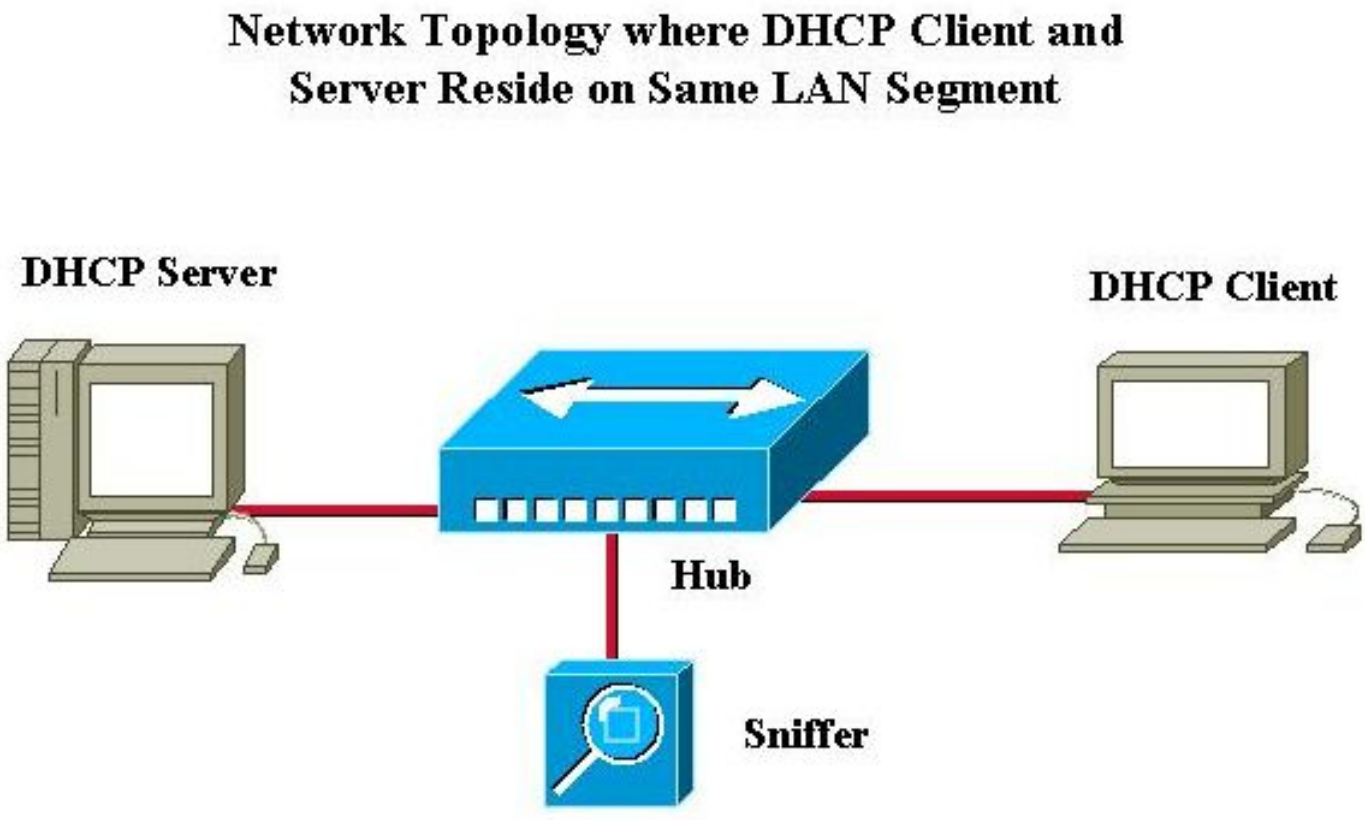
Consideraciones del arranque de DHCP del entorno de la PRE-ejecución (PXE)

El entorno de la PRE-ejecución (PXE) permite que un puesto de trabajo inicie de un servidor en una red antes de iniciar el sistema operativo en la unidad de disco duro local. Un administrador de la red no tiene que físicamente visitar el puesto de trabajo específico y iniciarlo manualmente. Los sistemas operativos y el otro software, tal como programas de diagnóstico, se pueden cargar sobre el dispositivo de un servidor sobre la red. El DHCP de las aplicaciones del entorno PXE para configurarla es dirección IP.

La configuración del DHCP/BootP Relay Agent se debe hacer en el router si el servidor DHCP está situado en otro segmento ruteado de la red. El comando ip helper-address en la interfaz del router local debe ser configurado. Refiera a la característica del DHCP/BootP Relay Agent que configura en la sección del router del Cisco IOS de este documento para la información de la configuración.

Comprensión y resolución de problemas de DHCP usando rastros de sabueso

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



La traza de sniffer abajo se comprende de seis bastidores. 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. Pueden existir algunas diferencias en comparación con los seguimientos a continuación, pero el flujo de paquetes general debe ser exactamente igual. La trama de paquetes es generada por discusiones previas acerca de cómo funciona DHCP.

```
- - - - - - - - - - - - - - - - - - - - - Frame 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:

- **Frame 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 (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 = 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:

- **Frame 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:

- **Frame 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:

- **Frame 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:

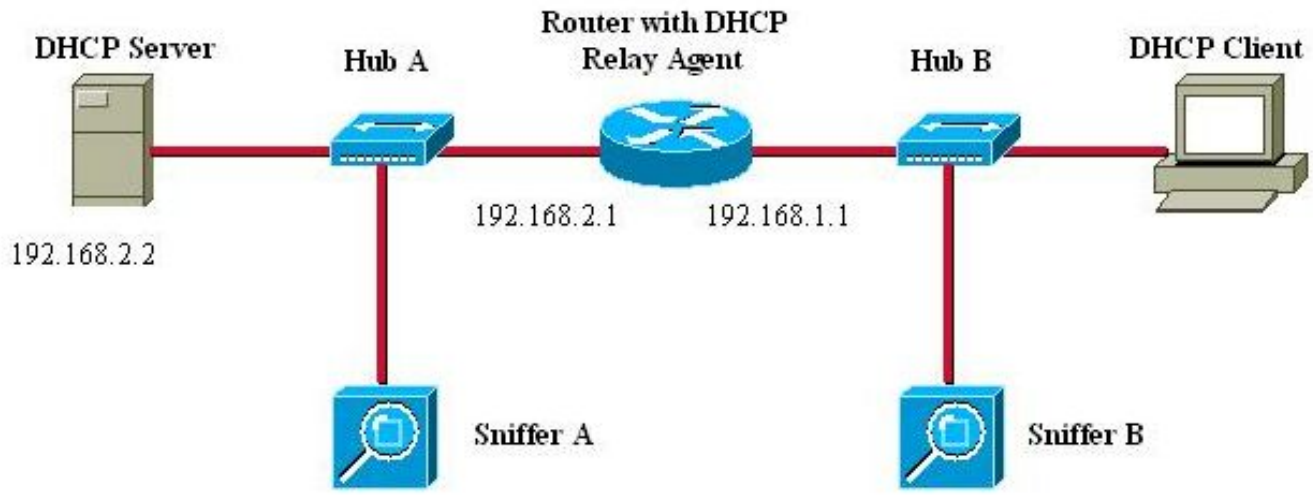
```
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 0005DCC9C640
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:
```

- **Frame 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

DHCP Client and Server separated by router configured as DHCP Relay Agent



Rastro del sabueso-B

```
- - - - - - - - - - - - - - - - - - - - - - Frame 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:

- **Frame 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:

- **Frame 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, Broadcast**
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:

- **Frame 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:

- **Frame 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:

- **Frame 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:
```

Traza del Sniffer-a

```
- - - - - - - - - - - - - - - - - - - - - - - - Frame 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:

- **Frame 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:

- **Frame 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:

- **Frame 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 en las estaciones del cliente no se puede obtener direcciones DHCP

Caso Práctico 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 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. El problema por lo general se relaciona con los dispositivos que conectan el servidor DHCP y el cliente DHCP. Sin embargo, el problema puede estar con el servidor DHCP o el cliente sí mismo. Con los módulos de solución de problemas a continuación, determine qué dispositivo está causando el inconveniente.

Nota: Para configurar al servidor DHCP en a por la base de VLAN, defina a diversos agrupamientos DHCP para los DHCP Address de cada porción del VLA N a sus clientes.

Caso Práctico nº 2: El servidor DHCP y el cliente DHCP están separados por un router configurado para funcionalidad de agente de retransmisión DHCP/BootP

Cuando el servidor DHCP y el cliente residen en los diversos segmentos LAN o VLA N, el router que funciona como un DHCP/BootP Relay Agent es responsable de remitir el DHCPREQUEST al servidor DHCP. Se requieren pasos adicionales de resolución de problemas para resolver el problema del agente de relé BootP/DHCP, así como el servidor y el cliente DHCP. Después de los módulos de Troubleshooting abajo debe determinar qué dispositivo está causando el problema.

El servidor DHCP en el router no puede asignar Adresses con un error AGOTADO POOL

Es posible que algunos direccionamientos todavía son llevados a cabo por los clientes, incluso si se liberan del pool. Esto se puede verificar por la salida del **conflicto DHCP del IP de la demostración**. Un conflicto de dirección ocurre cuando dos host utilizan la misma dirección IP. En la asignación de dirección, el DHCP marca para saber si hay conflictos con el ping y el ARP gratuito.

Si se detecta un conflicto, la dirección se remueve del conjunto. Se asigna el direccionamiento hasta que el administrador resuelva el conflicto. No configure **ningún registro del conflicto DHCP del IP** para resolver este problema.

Módulos de resolución de problemas de DHCP

Dónde pueden ocurrir problemas de DHCP

Los problemas DHCP pueden presentarse debido a una multitud de razones. Los motivos más frecuentes son los problemas de configuración. Sin embargo, los defectos de software de sistemas operativos, controladores de las tarjetas de interfaz de red (NIC) o agentes de relé DHCP/BootP que se ejecutan en routers pueden causar muchos de los problemas de DHCP. Debido al número potencialmente de áreas problemáticas, un enfoque sistemático a resolver problemas se requiere.

Lista de las causas posibles preseleccionadas de problemas de DHCP:

- Configuración predeterminada del switch Catalyst
- Configuración del DHCP/BootP Relay Agent
- Problema de compatibilidad de NIC o problema de la característica DHCP
- NIC defectuoso o instalación incorrecta del driver NIC
- Interrupciones de la red intermitentes debidas frecuentar atravesar - cómputos del árbol
- 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 del IOS de Cisco
- Fall del control del Unicast Reverse Path Forwarding (uRPF) porque la oferta de DHCP se recibe en una diversa interfaz que esperada. Cuando la característica del reenvío de trayecto inverso (RPF) se habilita en una interfaz, un router Cisco puede caer los paquetes del Protocolo de configuración dinámica de host (DHCP) y del Bootstrap Protocol (BOOTP) que tienen las direcciones de origen de 0.0.0.0 y las direcciones destino de 255.255.255.255. El router puede también caer todos los paquetes del IP que tengan un destino del IP de multidifusión en la interfaz. Este problema se documenta en CSCdw31925 (clientes registrados solamente).
- El Database Agent del DHCP no se utiliza, pero el registro del conflicto del DHCP no se inhabilita

Este documento utilizará 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 DHCP cliente como el servidor poseen conectividad física.

Para los switches Catalyst CatOS de las series 2948G, 4000, 5000 y 6000 utilice el comando

show port <mod#>/<port_range> para verificar el estado del puerto. Si el estado del puerto no es conectado, el puerto no pasará tráfico, incluidas las solicitudes 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 connected 1 a-full a-100 10/100BaseTX
```

Para los switches basados en el IOS, tales como Catalyst 2900XL/3500XL/2950/3550, el comando equivalente a show port status es show interface <interface>. Si es el estado de la interfaz cualquier cosa con excepción del <interface> está para arriba, Line Protocol está para arriba, el puerto no pasará el tráfico, incluyendo los pedidos de DHCP cliente. 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 link entre el switch Catalyst y el cliente DHCP, consulte el documento 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.

La causa excesiva de los errores del link de datos vira hacia el lado de babor en algunos switches de Catalyst para entrar un estado `errdisabled`. Refiera a recuperación del estado del puerto errDisable en las Plataformas de CatOS y la recuperación del estado del puerto errDisable en las plataformas de Cisco IOS, que describen al estado de errDisable, explica cómo recuperarse de ella, y proporciona los ejemplos de recuperación de este estado.

B. Pruebe la conectividad de la red configurando la estación de trabajo del cliente con el IP Address estático

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

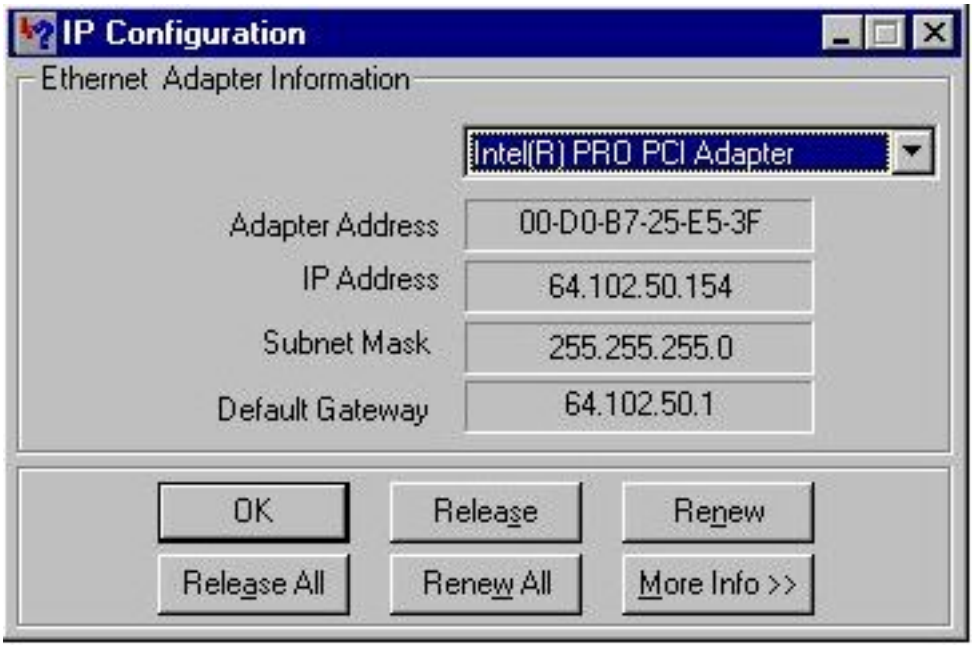
Durante la resolución de cualquier problema de DHCP, es importante verificar la conectividad de la red al configurar una dirección IP estática en una estación de trabajo de cliente. Si la estación de trabajo no puede alcanzar los recursos de red a pesar de tener una dirección IP configurada estáticamente, el origen del problema no es DHCP. En este momento, se necesita resolver los problemas de conectividad de la red.

C. Verifique el problema como problema de inicialización

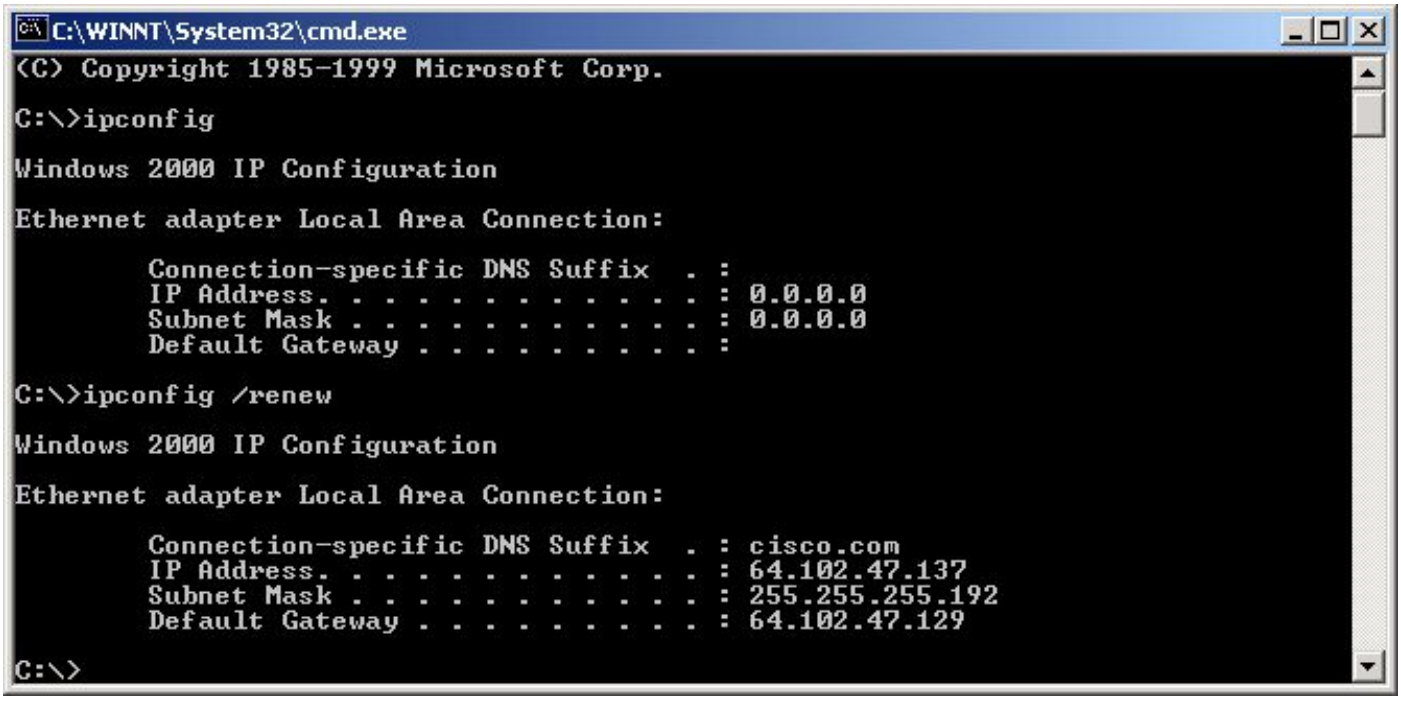
Este procedimiento se puede aplicar a todos los estudios de caso.

Si el DHCP cliente no puede obtener una dirección de IP del servidor DHCP durante el inicio, intente obtener una dirección de IP del servidor DHCP forzando manualmente al cliente a enviar una petición DHCP. Publique los pasos siguientes para obtener manualmente una dirección IP de un servidor DHCP para los sistemas operativos enumerados abajo.

Microsoft Windows 95/98/ME: Haga clic el **botón Start Button**, y funcione con el programa WINIPCFG.exe. Haga clic el **botón de** ReleaseAll, seguido por el **botón de** RenewAll. ¿El cliente DHCP es ahora capaz de obtener una dirección IP?



Microsoft Windows NT/2000: Abra una ventana de prompt de comando tecleando el **cmd** en el **comienzo/el** campo **funcionado con**. Ejecute el comando ipconfig/renew en la ventana símbolo de sistema, como se ilustra a continuación: ¿El cliente DHCP es ahora capaz de obtener una dirección IP?



Si el cliente DHCP puede obtener una dirección IP al renovar manualmente la dirección IP luego de que la PC haya finalizado el proceso de inicio del sistema, es probable que el problema sea del inicio de DHCP. Si asocian al Cliente de DHCP a un Switch del Cisco Catalyst, el problema es muy probablemente debido a un problema de configuración que trata del STP portfast y/o canalización y enlace. Otras posibilidades incluyen los problemas con las tarjetas NIC y con el inicio del puerto del switch.

D. Verifique la configuración de puerto de 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 el enlace troncal/con canalización inhabilitado. La configuración predeterminada es

STP portfast inhabilitado y enlace troncal/canalización automática, si corresponde. Para el Switches 2900XL/3500XL/2950/3550, el 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 de puerto de conmutación para que DHCP funcione correctamente cuando está conectado a los switches Catalyst, consulte el siguiente documento:

Usando Portfast y otros comandos de reparar los retardos de la conectividad de inicialización de la estación de trabajo

Después de revisar las pautas de configuración en el documento arriba, vuelva a este documento para el Troubleshooting adicional.

E. Marque para saber si hay indicador luminoso LED amarillo de la placa muestra gravedad menor o problemas del switch Catalyst del NIC conocido

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

Troubleshooting de Problemas de Compatibilidad entre Cisco Catalyst Switches y NIC

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

F. Distinción si los clientes DHCP obtienen la dirección IP en la misma subred o el VLA N 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 está trabajando correctamente en la misma subred o VLAN como el servidor de DHCP, el problema DHCP puede ser con el Agente Relay 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. Verifique la configuración del router Relay DHCP/BootP

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

1. Cuando configure el relé DHCP en un router, verifique que el comando ip helper-address se ubique en la interfaz correcta. El comando ip helper-address debe estar presente en la interfaz interna de las estaciones de trabajo DHCP cliente y debe direccionarse al servidor DHCP correcto.
2. Compruebe que el comando de configuración global no service dhcp no está presente. Este parámetro desactivará todos los servidores DHCP y la funcionalidad de relé en el router. La configuración predeterminada, `DHCP del servicio`, no aparecerá en la configuración, y es el

comando default configuration. Si el DHCP del servicio no se habilita, los clientes no reciben los IP Addresses del servidor DHCP.**Nota:** En el Routers que funciona con un Cisco IOS más viejo libera, el comando ip bootp server maneja la función del agente de relé DHCP en vez del **comando service dhcp**. Debido a esto, el **comando ip bootp server** necesita ser habilitado en este Routers si configuran al **comando ip helper-address** para remitir los broadcastes DHCP UDP y de actuar correctamente como agente de relé DHCP en nombre del Cliente de DHCP.

3. Al aplicar los comandos ip helper-address para reenviar difusiones UDP a una dirección de difusión de subred, verifique que no haya ningún ip directed-broadcast configurado en ninguna interfaz de salida que los paquetes de difusión UDP deban atravesar. La difusión directa sin ip bloqueará cualquier traducción de una difusión directa a difusiones físicas. Esta configuración de la interfaz es configuración predeterminada en los 12.0 y superiores de las versiones de software.
4. El reenvío de difusiones DHCP a la dirección de difusión de subred del servidor DHCP es un problema de software aislado. Al resolver problemas el DHCP, intente siempre remitir los broadcastes DHCP UDP a la dirección IP del servidor DHCP, como se muestra abajo:

H. Opción de la identificación de suscriptor (82) girada

La característica de la información del agente de relé DHCP (opción 82) permite a los agentes de relé DHCP (switches de Catalyst) para incluir la información sobre sí mismo y el cliente asociado cuando él adelante los pedidos de DHCP de un Cliente de DHCP a un servidor DHCP.

El servidor DHCP puede utilizar esta información para asignar los IP Addresses, para realizar el control de acceso, y para fijar el Calidad de Servicio (QoS) y las políticas de seguridad (u otras directivas de la parámetro-asignación) para cada suscriptor de una red del proveedor de servicios.

Cuando el snooping del DHCP se habilita en un Switch, habilita automáticamente la opción 82.

Si no configuran al servidor DHCP para manejar los paquetes con la opción 82, deja de afectar un aparato el direccionamiento a esa solicitud.

Para resolver este problema, inhabilite la opción de la identificación de suscriptor (82) en el Switches (Agentes Relay) con el comando global configuration, **ninguna opción de información de la retransmisión DHCP del IP**.

I. Database Agent del DHCP y registro del conflicto del DHCP

Un Database Agent del DHCP es cualquier host — por ejemplo, un FTP, un TFTP, o un servidor RCP — ese salva la base de datos de los atascamientos del DHCP. Usted puede configurar los agentes múltiples de la base de datos del DHCP, y usted puede configurar el intervalo entre las actualizaciones de base de datos y las transferencias para cada agente. Utilice el comando ip dhcp database de configurar un Database Agent y los parámetros del Database Agent.

Si usted elige no configurar un Database Agent del DHCP, inhabilite la grabación de los conflictos del DHCP Address en el servidor DHCP. No ejecute el **ningún** comando ip dhcp conflict logging de inhabilitar el registro del conflicto del DHCP Address. Borre los conflictos previamente registrados con el conflicto claro DHCP del IP.

Si esto no puede inhabilitar el registro del conflicto, este mensaje de error aparece:

```
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)
```

J. Control CDP para las conexiones del teléfono del IP

Cuando el switchport que está conectado con el Cisco IP Phone tiene Cisco Discovery Protocol (CDP) inhabilitado, el servidor DHCP no puede asignar una dirección IP apropiada al teléfono. El servidor DHCP tiende a asignar la dirección IP que pertenece al VLAN de dato/a la subred del switchport. Si se habilita el CDP, el Switch puede detectar que el Cisco IP Phone pide el DHCP y puede proporcionar la información de subred correcta. El servidor DHCP entonces puede asignar una dirección IP del VLA N de la Voz/del pool de la subred. No hay pasos explícitos requeridos para atar el servicio DHCP a la Voz vlan.

K. La eliminación abajo del SVI interrumpe la operación del snooping del DHCP

En los Cisco Catalyst 6500 Series Switch, un SVI (en el estado de cierre normal) se crea automáticamente después de que configure el DHCP para snoop para un VLAN determinado. La presencia de este SVI tiene implicaciones directas en la operación correcta del snooping del DHCP.

El snooping del DHCP en los Cisco Catalyst 6500 Series Switch que ejecutan el Native IOS se implementa sobre todo en el Route Processor (RP o MSFC), no en el Procesador del switch (SP o supervisor). Las Cisco Catalyst 6500 Series interceptan los paquetes en hardware con los VACL que suministran los paquetes a una lógica de destino local (LTL) inscrita por al RP. Una vez que las tramas ingresan el RP, primero necesitan ser asociadas a un IDB de la interfaz L3 (SVI) antes de que puedan ser pasadas apagado a la partición del snooping. Sin un SVI, este IDB no existe, y los paquetes consiguen caídos en el RP.

L. Dirección de broadcast limitada

Cuando un Cliente de DHCP fija el broadcast mordido en un paquete DHCP, el servidor DHCP y el Agente Relay envían los mensajes DHCP a los clientes con la dirección de broadcast del todo uno (255.255.255.255). Si han configurado al comando ip broadcast-address de enviar un broadcast de red, el broadcast del todo uno enviado por el DHCP se reemplaza. Para remediar esta situación, utilice el comando del limitado-transmitir-direccionamiento DHCP del IP de asegurarse de que un broadcast de la red configurada no reemplaza el comportamiento predeterminado del DHCP.

Algunos clientes DHCP pueden validar solamente el todo uno transmitido y no pueden adquirir un DHCP Address a menos que este comando se configure en la interfaz del router conectada con el cliente.

M. Hacer el debug del DHCP usando los comandos debug del router

Verifique al router está recibiendo el pedido de DHCP usando los comandos debug

En el Routers que el proceso del software de soporte de los paquetes DHCP, usted puede verificar si un router está recibiendo el pedido de DHCP del cliente. El proceso DHCP fallará si el router no está recibiendo las solicitudes del cliente. Este paso de resolución de problemas implica configurar una lista de acceso para la salida de depuración. Esta lista de acceso sólo se utiliza

para la depuración y no es intrusiva para el 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, es claro que el router está recibiendo pedidos 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 está correcto. Sin embargo, el router recibió un paquete de transmisión con la fuente y el destino IP y los puertos UDP que son adecuados para DHCP.

Verifique al router está recibiendo el pedido de DHCP y los pedidos de reenvío al servidor DHCP que usa los comandos debug

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

eq 67 del host del host UDP del permiso de la lista de acceso 100 <dhcp_relay_agent> <dhcp_server>

eq 67 del host del host UDP del permiso de la lista de acceso 100 <dhcp_server> <dhcp_relay_agent>

Por ejemplo:

access-list 100 permit ip host 0.0.0.0 host 255.255.255.0

eq 67 de 192.168.2.2 del host de 192.168.1.1 del host UDP del permiso de la lista de acceso 100

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

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

eq 68 de 192.168.1.1 del host de 192.168.2.2 del host UDP del permiso de la lista de acceso 100

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
```

De la salida arriba, está claro que el router está recibiendo los pedidos de DHCP del cliente y está remitiendo la solicitud, por la configuración del DHCP/BootP Relay Agent, al servidor DHCP. El servidor DHCP también contestó directamente al DHCP/BootP Relay Agent. 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 DHCPNAK. Sin embargo, el router recibió un paquete de transmisión con la fuente y el destino IP y los puertos UDP que son adecuados para DHCP, y hay comunicación bidireccional con el servidor DHCP.

Verifique que el router esté recibiendo y reenviando la petición DHCP con el comando debug ip udp

El comando debug ip udp puede ser usado para rastrear la ruta de una solicitud DHCP a través del router. Sin embargo, esta depuración es intrusiva en un entorno de producción, ya que todos los paquetes UDP conmutados procesados serán mostrados en la consola. Esta depuración no debe utilizarse en producción.

Advertencia: El comando debug ip udp es intruso, y puede causar la alto nivel de uso de la Unidad de procesamiento central (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
!--- Router receiving DHCPDISCOVER from DHCP client. 00:18:48: UDP: sent src=192.168.1.1(67),
dst=192.168.2.2(67), length=604 !--- Router forwarding DHCPDISCOVER unicast to DHCP server using
DHCP/BootP Relay Agent source IP address. 00:18:48: UDP: rcvd src=192.168.2.2(67),
dst=192.168.1.1(67), length=313 !--- Router receiving DHCPOFFER from DHCP server directed to
DHCP/BootP Relay Agent IP address. 00:18:48: UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68),
length=333 !--- Router forwarding DHCPOFFER from DHCP server to DHCP client via DHCP/BootP Relay
Agent. 00:18:48: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584 !--- Router
receiving DHCPREQUEST from DHCP client. 00:18:48: UDP: sent src=192.168.1.1(67),
dst=192.168.2.2(67), length=604 !--- Router forwarding DHCPDISCOVER unicast to DHCP server using
DHCP/BootP Relay Agent source IP address. 00:18:48: UDP: rcvd src=192.168.2.2(67),
dst=192.168.1.1(67), length=313 !--- Router receiving DHCPACK (or DHCPNAK) from DHCP directed to
DHCP/BootP Relay Agent IP address. 00:18:48: UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68),
length=333 !--- Router forwarding DHCPACK (or DHCPNAK) to DHCP client via DHCP/BootP Relay
```

```
Agent. 00:18:48: UDP: rcvd src=192.168.1.2(520), dst=255.255.255.255(520), length=32 !--- DHCP
client verifying IP address not in use by sending ARP request for its own IP address. 00:18:50:
UDP: rcvd src=192.168.1.2(520), dst=255.255.255.255(520), length=32 !--- DHCP client verifying
IP address not in use by sending ARP request for its own IP address.
```

Verifique que el router esté recibiendo y reenviando la solicitud DHCP utilizando el comando debug ip dhcp server packet.

Si el IOS del router es 12.0.x.T o 12.1 y soporta la funcionalidad del servidor DHCP IOS, el debugging adicional se puede hacer usando el **comando debug ip dhcp server packet**. Este debug fue pensado para el uso con la característica del servidor DHCP de IOS, pero se puede utilizar para resolver problemas la característica del DHCP/BootP Relay Agent también. Como con los pasos de Troubleshooting anteriores, los debugs del router no proporcionan una determinación exacta del problema puesto que el paquete real no puede ser visto. Sin embargo, las depuraciones permiten realizar las interfaces 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.
!--- Router received DHCPDISCOVER/REQUEST/INRORM and setting Gateway IP address to 192.168.1.1
for forwarding. 00:20:54: DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3065.302e.3165.6632.2e63..
!--- BOOTREQUEST includes DHCPDISCOVER, DHCPREQUEST, and DHCPINFORM. !---
0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indicates client identifier. 00:20:54: DHCPD:
forwarding BOOTREPLY to client 00e0.1ef2.c441. !--- BOOTREPLY includes DHCPOFFER and DHCPNAK. !-
-- Client's MAC address is 00e0.1ef2.c441. 00:20:54: DHCPD: broadcasting BOOTREPLY to client
00e0.1ef2.c441. !--- Router is forwarding DHCPOFFER or DHCPNAK broadcast on local LAN interface.
00:20:54: DHCPD: setting giaddr to 192.168.1.1. !--- Router received DHCPDISCOVER/REQUEST/INFORM
and set Gateway IP address to 192.168.1.1 for forwarding. 00:20:54: DHCPD: BOOTREQUEST from
0063.6973.636f.2d30.3065.302e.3165.6632.2e63.. !--- BOOTREQUEST includes DHCPDISCOVER,
DHCPREQUEST, and DHCPINFORM. !--- 0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indicates client
identifier. 00:20:54: DHCPD: forwarding BOOTREPLY to client 00e0.1ef2.c441. !--- BOOTREPLY
includes DHCPOFFER and DHCPNAK. !--- Client's MAC address is 00e0.1ef2.c441. 00:20:54: DHCPD:
broadcasting BOOTREPLY to client 00e0.1ef2.c441. !--- Router is forwarding DHCPOFFER or DHCPNAK
broadcast on local LAN interface.
```

Ejecución simultánea de depuraciones múltiples

Al ejecutar múltiples depuraciones en forma simultánea, es posible descubrir una buena cantidad de información sobre la operación del servidor y el agente de retransmisión DHCP/BootP. Con la utilización de las anteriores pautas de solución de problemas, puede hacer inferencias sobre dónde es posible que la funcionalidad de agente de relé DHCP/BootP no esté funcionando correctamente.

```
Router#debug ip dhcp server packet
00:20:54: DHCPD: setting giaddr to 192.168.1.1.
!--- Router received DHCPDISCOVER/REQUEST/INRORM and setting Gateway IP address to 192.168.1.1
for forwarding. 00:20:54: DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3065.302e.3165.6632.2e63..
!--- BOOTREQUEST includes DHCPDISCOVER, DHCPREQUEST, and DHCPINFORM. !---
0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indicates client identifier. 00:20:54: DHCPD:
forwarding BOOTREPLY to client 00e0.1ef2.c441. !--- BOOTREPLY includes DHCPOFFER and DHCPNAK. !-
-- Client's MAC address is 00e0.1ef2.c441. 00:20:54: DHCPD: broadcasting BOOTREPLY to client
00e0.1ef2.c441. !--- Router is forwarding DHCPOFFER or DHCPNAK broadcast on local LAN interface.
00:20:54: DHCPD: setting giaddr to 192.168.1.1. !--- Router received DHCPDISCOVER/REQUEST/INFORM
and set Gateway IP address to 192.168.1.1 for forwarding. 00:20:54: DHCPD: BOOTREQUEST from
0063.6973.636f.2d30.3065.302e.3165.6632.2e63.. !--- BOOTREQUEST includes DHCPDISCOVER,
```

```
DHCPREQUEST, and DHCPINFORM. !--- 0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indicates client
identifier. 00:20:54: DHCPD: forwarding BOOTREPLY to client 00e0.1ef2.c441. !--- BOOTREPLY
includes DHCPOFFER and DHCPNAK. !--- Client's MAC address is 00e0.1ef2.c441. 00:20:54: DHCPD:
broadcasting BOOTREPLY to client 00e0.1ef2.c441. !--- Router is forwarding DHCPOFFER or DHCPNAK
broadcast on local LAN interface.
```

Obtenga la traza de sniffer y determine la causa raíz del problema de DHCP

El uso de técnicas de depuración del router no siempre determinará la causa raíz exacta de un problema DHCP. El último paso de la solución de un problema de DHCP es obtener un rastro del sabueso y detectar en qué parte el proceso no funciona correctamente. Los rastros de los paquetes DHCP pueden ser desencripcións remitiéndose a las secciones de este documento Decodificación de rastros del sabueso de un cliente DHCP y un servidor en el mismo segmento de LAN y Decodificación de rastros del sabueso de un cliente DHCP y un servidor separados por un router configurado como un agente de relé DHCP.

Para la información sobre la obtención de las trazas de sniffer usando la característica del Switched Port Analyzer (SPAN) en los switches de Catalyst, refiera al documento siguiente:

- Configurar el (SPAN) del Catalyst Switched Port Analyzer.

Método alternativo de decodificación de paquetes mediante depuración en el router

Usando

comando debug ip packet detail dump <acl> en un router Cisco, es posible conseguir un paquete entero en el maleficio visualizado en la interfaz de línea del comando system log or (CLI). Si utiliza las secciones Verifique que el router esté recibiendo peticiones DHCP, Utilización de comandos debug y Verifique que el router esté recibiendo peticiones DHCP y reenviando peticiones al servidor DHCP, Utilización de los comandos debug anteriores, junto con la palabra clave dump agregada a la lista de acceso, obtendrá la misma información de depuración, pero con packet detail in hex. Para determinar el contenido del paquete, el paquete necesitará tradujo. En el Apéndice A se presenta un ejemplo.

Las palabras claves ingresadas después de la opción del comando ip dhcp pool {option_number} ASCII están en las comillas dobles

Un router Cisco con una opción DHCP con el número de opción configurado puede encontrar un incidente si intenta analizar el URL porque algunas palabras claves ingresadas después de que el *número de opción* ASCII de la **opción del comando ip dhcp pool** esté en las comillas dobles después de que recarguen al router. Este comportamiento se considera en los dispositivos que ejecutan el IOS 12.4(17a), que es un bug conocido y se documenta en CSCsk96976 (clientes registrados solamente).

Este problema se resuelve en las versiones de IOS 12.4(17b), 12.4(18a) y posterior, y 12.4(19)T1.

Apéndice A: Configuración de IOS DHCP de muestra

La base de datos de servidor DHCP se ordena como árbol. El root del árbol es el conjunto de direcciones para las redes naturales, las ramas son conjuntos 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, deben configurarse en el nivel más elevado (red o subred) del árbol.

Para obtener más información sobre cómo configurar DHCP y sus comandos asociados consulte el siguiente link.

- Lista de tareas de configuración de DHCP

```
Router#debug ip dhcp server packet
00:20:54: DHCPD: setting giaddr to 192.168.1.1.
!--- Router received DHCPDISCOVER/REQUEST/INRORM and
setting Gateway IP address to 192.168.1.1 for
forwarding. 00:20:54: DHCPD: BOOTREQUEST from
0063.6973.636f.2d30.3065.302e.3165.6632.2e63.. !---
BOOTREQUEST includes DHCPDISCOVER, DHCPREQUEST, and
DHCPINFORM. !---
0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indicates
client identifier. 00:20:54: DHCPD: forwarding BOOTREPLY
to client 00e0.1ef2.c441. !--- BOOTREPLY includes
DHCPOFFER and DHCPNAK. !--- Client's MAC address is
00e0.1ef2.c441. 00:20:54: DHCPD: broadcasting BOOTREPLY
to client 00e0.1ef2.c441. !--- Router is forwarding
DHCPOFFER or DHCPNAK broadcast on local LAN interface.
00:20:54: DHCPD: setting giaddr to 192.168.1.1. !---
Router received DHCPDISCOVER/REQUEST/INFORM and set
Gateway IP address to 192.168.1.1 for forwarding.
00:20:54: DHCPD: BOOTREQUEST from
0063.6973.636f.2d30.3065.302e.3165.6632.2e63.. !---
BOOTREQUEST includes DHCPDISCOVER, DHCPREQUEST, and
DHCPINFORM. !---
0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indicates
client identifier. 00:20:54: DHCPD: forwarding BOOTREPLY
to client 00e0.1ef2.c441. !--- BOOTREPLY includes
DHCPOFFER and DHCPNAK. !--- Client's MAC address is
00e0.1ef2.c441. 00:20:54: DHCPD: broadcasting BOOTREPLY
to client 00e0.1ef2.c441. !--- Router is forwarding
DHCPOFFER or DHCPNAK broadcast on local LAN interface.
```

Información Relacionada

- Función de Relay DHCP en el ejemplo de configuración concentrador VPN 3000
- PIX/ASA 7.x como ejemplo de configuración del relé DHCP
- Herramientas y Recursos
- Soporte Técnico - Cisco Systems