Resolución de Problemas de Dynamic Host Configuration Protocol en Catalyst Switch o Enterprise Networks

Contenido

Introducción

Este documento describe cómo resolver varios problemas comunes con el Protocolo de configuración dinámica de host (DHCP) en una red de switches Cisco Catalyst.

Prerequisites

Requirements

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.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

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

> **Nota:** Solo los clientes registrados de Cisco tienen acceso a los informes de errores internos.

Antecedentes

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

DHCP se basa en un paradigma cliente-servidor en el que el cliente DHCP, un PC de escritorio, por ejemplo, se pone en contacto con un servidor de DHCP para obtener parámetros de 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. Dado que los routers no transmiten difusiones de forma predeterminada, se necesitaría un servidor DHCP en cada subred a menos que los routers estén configurados para reenviar la difusión DHCP con la función Agente de retransmisión DHCP.

‘Conceptos clave’

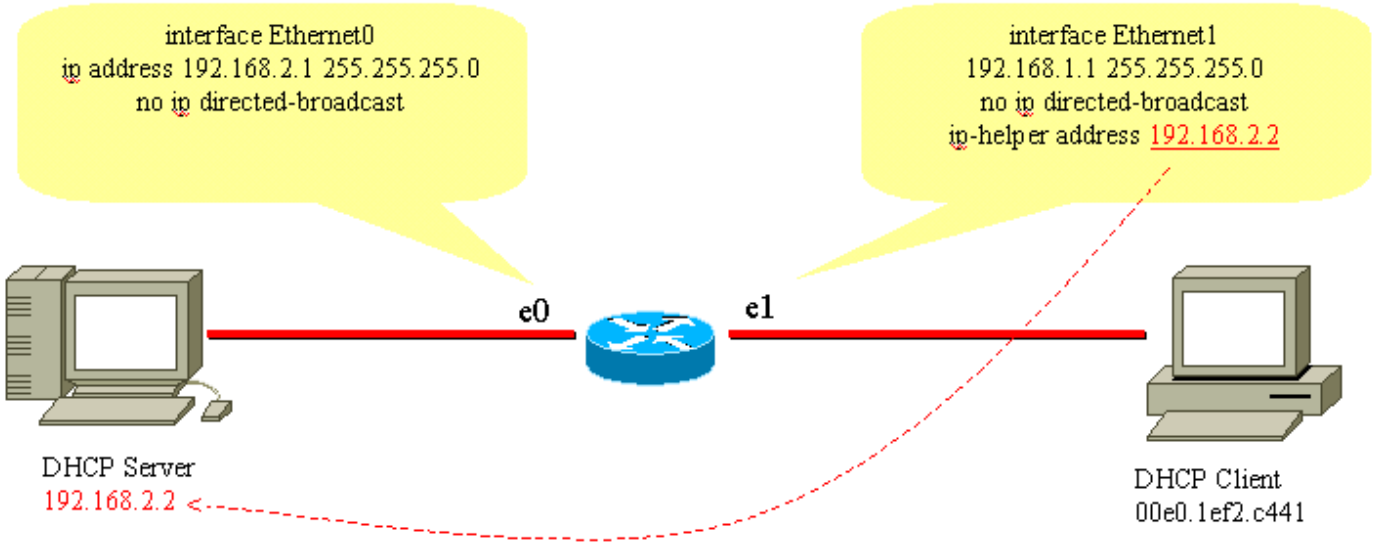
Estos son varios de los conceptos clave del DHCP:

- Los clientes DHCP inicialmente no tienen una dirección IP configurada y, por lo tanto, deben enviar una solicitud de difusión para obtener una dirección IP de un servidor DHCP.
- Como valor predeterminado, los routers no desvían difusiones. 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 Relay de DHCP en el router de Cisco se proporciona mediante los **comandos ip helper de nivel de interfaz.**

“Situaciones de ejemplo”

Escenario 1: Enrutamiento del router de Cisco entre el cliente DHCP y las redes del servidor

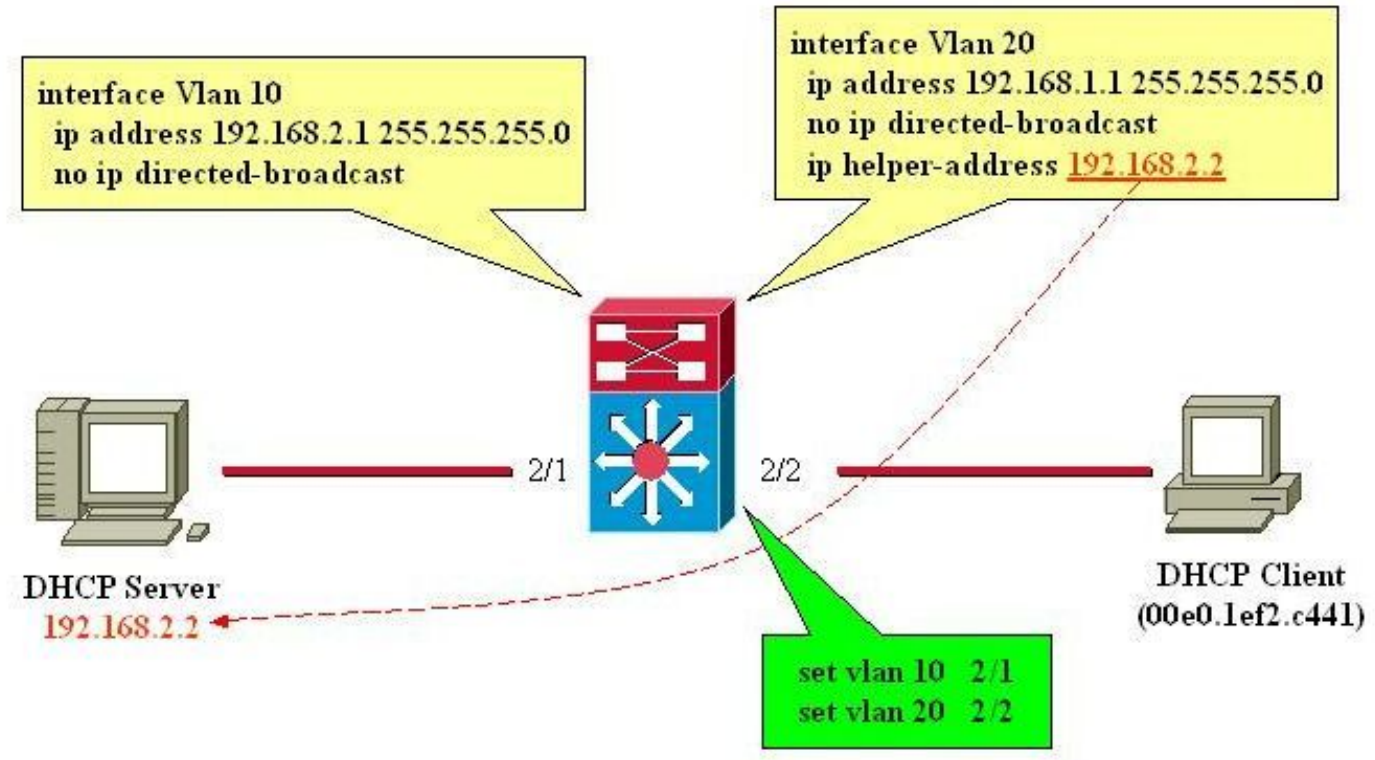
Tal y como se configura en este diagrama, la interfaz Ethernet1 reenvía el cliente transmitido DHCPDISCOVER a 192.168.2.2 a través de la interfaz Ethernet1. El servidor DHCP satisface la solicitud a través de unicast. En este ejemplo, no se necesita más configuración para el router.



Enrutamiento entre el cliente DHCP y las redes de servidor

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

Tal como se configura en el diagrama, la interfaz VLAN20 reenvía el cliente transmitido DHCPDISCOVER a 192.168.2.2 a través de la interfaz VLAN10. El servidor DHCP satisface la solicitud a través de unicast. En este ejemplo, no se necesita más configuración para el router. Los puertos para switches deben configurarse como puertos host, y deben tener habilitado el portfast del Protocolo de árbol transversal (STP), e inhabilitados los enlaces troncales y la canalización.



Ruta del módulo L3 entre el cliente DHCP y las redes del servidor

Comprender DHCP

DHCP se definió originalmente en Solicitudes de comentarios (RFC) 1531 y desde entonces ha quedado obsoleto en RFC 2131. DHCP se basa en el Protocolo de Bootstrap (BootP), que se define en RFC 951.

Las estaciones de trabajo (hosts) usan DHCP para obtener la información de configuración inicial, como dirección IP, máscara de subred y el gateway predeterminado tras el inicio. Con DHCP, no tiene que configurar manualmente cada host con una dirección IP. Además, si un host se mueve a una subred IP diferente, debe utilizar una dirección de IP diferente de la que empleaba antes. DHCP se encarga 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: Interoperabilidad entre DHCP y BootP
- RFC 1542 – Aclaraciones y extensiones para BootP
- RFC 2241 - DHCP Opciones para los servicios de directorio de Novell
- RFC 2242 – Nombre e información de Netware/Dominio IP
- RFC 2489: Procedimiento para definir nuevas opciones de 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 se inicia un host, la pila TCP/IP del host transmite un mensaje de difusión (DHCPDISCOVER) para recibir una dirección IP y una máscara de red, entre otros parámetros de configuración. Este paso inicia un intercambio entre el servidor DHCP y el host. Durante este intercambio, el cliente pasa a través de estos estados bien definidos:

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

Para moverse entre estos estados, el cliente y el servidor pueden intercambiar los tipos de mensajes enumerados en la Tabla de mensajes DHCP.

Tabla de mensajes DHCP

Referencia	Mensaje	Descripción
0x01	DHCPDISCOVER	El cliente busca servidores DHCP disponibles.
0x02	DHCPOFFER	El servidor responde al cliente DHCPDISCOVER.
0x03	DHCPREQUEST	El cliente transmite al servidor, solicita parámetros ofrecidos de un servidor específicamente, como se define en el paquete.
0x04	DHCPDECLINE	La comunicación cliente-servidor indica que la dirección de red ya está en uso.
0x05	DHCPACK	La comunicación de servidor a cliente con los parámetros de configuración, junto

		la dirección de red confirmada.
0x06	DHCPNAK	La comunicación de servidor a cliente rechaza la solicitud del parámetro de configuración.
0x07	DHCPRELEASE	La comunicación de cliente a servidor devuelve la dirección de red y cancela el arrendamiento restante.
0x08	DHCPINFORM	La comunicación cliente-servidor, solicita solamente los parámetros de configura local que el cliente ya ha configurado externamente como una dirección.

DHCPDISCOVER

Cuando un cliente se inicia por primera vez, se dice que está en estado de inicialización y transmite un mensaje DHCPDISCOVER en su subred física local sobre el puerto 67 de Protocolo de datagrama de usuario (UDP) (servidor del BOOTP). Dado que el cliente no tiene forma de conocer la subred a la que pertenece, DHCPDISCOVER es un broadcast de todas las subredes (dirección IP de destino 255.255.255.255), con una dirección IP de origen 0.0.0.0. La dirección IP de origen es 0.0.0.0 ya que el cliente no tiene una dirección IP configurada. Si existe un servidor DHCP en esta subred local y está configurado y funciona correctamente, el servidor DHCP escucha la difusión y responde con 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 de retransmisión puede ser un host dedicado (por ejemplo, Microsoft Windows Server) o un router (por ejemplo, un router de Cisco configurado con instrucciones auxiliares IP de nivel de interfaz).

DHCPOFFER

Un servidor DHCP que recibe un mensaje DHCPDISCOVER puede responder con un mensaje DHCPOFFER en el puerto 68 UDP (cliente BootP). El cliente recibe el DHCPOFFER y pasa al estado Selecting (Seleccionando). Este mensaje DHCPOFFER contiene información de configuración inicial del cliente. Por ejemplo, el servidor DHCP rellena 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 envía el DHCPOFFER a la dirección de difusión pero incluye la dirección de hardware del cliente en el campo chaddr de la oferta, de modo que el cliente sabe que es el destino deseado. En el caso de que el servidor DHCP no esté en la subred local, el servidor DHCP envía el DHCPOFFER, como un paquete de unidifusión, en el puerto UDP 67, de vuelta al Agente de retransmisión DHCP/BootP del que proviene DHCPDISCOVER. A continuación, el Agente de retransmisión DHCP/BootP transmite o unidifusión DHCPOFFER en la subred local del puerto UDP 68, que depende del indicador de difusión establecido por el cliente de inicio.

DHCPREQUEST

Una vez que el cliente recibe un DHCPOFFER, responde con un mensaje DHCPREQUEST, indica su intención de aceptar los parámetros en el DHCPOFFER y pasa al estado de solicitud. El

cliente puede recibir varios mensajes DHCPOFFER, uno de cada servidor DHCP que recibió el mensaje DHCPDISCOVER original. El cliente elige un DHCPOFFER y responde a ese servidor DHCP solamente y, implícitamente, rechaza todos los otros mensajes DHCPOFFER. El cliente identifica el servidor seleccionado después de rellenar el campo de opción Identificador de servidor con la dirección IP del servidor DHCP. DHCPREQUEST también es una transmisión, por lo que todos los servidores DHCP que enviaron una DHCPOFFER ven la DHCPREQUEST y cada uno sabe si su DHCPOFFER fue aceptado o rechazado. Cualquier opción de configuración adicional que requiera el cliente se incluye en el campo de opciones del mensaje DHCPREQUEST. Aunque se ha ofrecido al cliente una dirección IP, envía el mensaje DHCPREQUEST con una dirección IP de origen de 0.0.0.0. En este momento, el cliente aún no ha recibido la verificación de que está claro que debe utilizar la dirección IP.

DHCPACK

Una vez que el servidor DHCP recibe el DHCPREQUEST, reconoce la solicitud con un mensaje DHCPACK y luego 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 la concesión en su base de datos y la identifica de forma única con el identificador o chaddr del cliente y la dirección IP asociada. Tanto el cliente como el servidor utilizan esta combinación de identificadores para hacer referencia a la concesión. El identificador de cliente es la dirección Mac del dispositivo más el tipo de medio.

Antes de que el cliente DHCP comience a utilizar la nueva dirección, el cliente DHCP debe calcular los parámetros de tiempo asociados a una dirección concedida, que son Tiempo de concesión (LT), Tiempo de renovación (T1) y Tiempo de reenlace (T2). 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 responde 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 cuando entra en el estado de Solicitud. El cliente retransmite el DHCPREQUEST al menos cuatro veces en 60 segundos antes de reiniciar el estado de inicialización.

DHCPDECLINE

El cliente recibe el DHCPACK y, opcionalmente, realiza una verificación final de los parámetros. El cliente realiza este procedimiento cuando envía las solicitudes del Protocolo de resolución de direcciones (ARP) para la dirección IP proporcionada en DHCPACK. Si el cliente detecta que la dirección ya está en uso cuando recibe una respuesta a la solicitud ARP, el cliente envía un mensaje DHCPDECLINE al servidor y reinicia el proceso de configuración en el estado Solicitando.

DHCPINFORM

Si un cliente ha obtenido una dirección de red a través de algún otro medio o tiene una dirección

IP configurada manualmente, una estación de trabajo cliente puede utilizar un mensaje de solicitud DHCPINFORM para obtener otros parámetros de configuración local, como el nombre de dominio y los servidores de nombres de dominio (DNS). Cuando los servidores DHCP reciben un mensaje DHCPINFORM, construyan un mensaje DHCPACK con cualquier parámetro de configuración local apropiado para el cliente sin una nueva dirección IP. Este DHCPACK se envía unidifusión al cliente.

DHCPRELEASE

Un cliente DHCP puede optar por renunciar a su concesión en una dirección de red cuando envía un mensaje DHCPRELEASE al servidor DHCP. El cliente identifica la concesión que se liberará mediante el uso delcampo de identificación de cliente y la dirección de red `del` mensaje DHCPRELEASE. Si necesita ampliar el intervalo actual del conjunto DHCP, elimine el conjunto actual de direcciones y especifique el nuevo intervalo de direcciones IP en el conjunto DHCP. Para borrar direcciones IP específicas o un rango de direcciones que desee estar en el conjunto de DHCP, utilice el comando IP DHCP Excluded-Address .

> **Nota:** Si los dispositivos utilizan BOOTP, se muestran arrendamientos de longitud infinita en los enlaces DHCP de los routers.

Renovación del arrendamiento

Debido a que la dirección de IP es arrendada únicamente desde el servidor, la licencia debe renovarse periódicamente. Cuando ha caducado la mitad del tiempo de concesión (T1=0,5 x LT), el cliente intenta renovar la concesión. El cliente ingresa en el estado de renovación y envía un mensaje DHCPREQUEST al servidor, que mantiene la validez actual. El servidor responde a la solicitud de renovación con un mensaje DHCPACK si acepta renovar el arrendamiento. El mensaje DHCPACK contiene el nuevo arrendamiento y los nuevos parámetros de configuración, en caso de que se realicen cambios en el servidor durante el período del arrendamiento anterior. Si el cliente no puede alcanzar el servidor cuando mantiene la concesión por alguna razón, intenta renovar la dirección de cualquier servidor DHCP después de que el servidor DHCP original no haya respondido a las solicitudes de renovación en un tiempo T2. El valor predeterminado de T2 es (7/8 x LT). Esto significa T1 < T2< LT.

Si el cliente tenía previamente una dirección IP asignada por DHCP y se reinicia, el cliente solicita específicamente la dirección IP previamente arrendada en un paquete DHCPREQUEST. Este DHCPREQUEST todavía tiene la dirección IP de origen como 0.0.0.0 y el destino como la dirección de broadcast IP 255.255.255.255.

Cuando un cliente envía una DHCPREQUEST en el curso de un reinicio, no debe rellenar el campo de identificador del servidor y debe rellenar en su lugar el campo de opción de dirección IP solicitada. Sólo los clientes compatibles con RFC rellenan el campo ciaddr con la dirección solicitada en lugar del campo de opción DHCP. El servidor DHCP acepta cualquiera de los métodos. El comportamiento del servidor DHCP depende de varios factores, como en el caso de los servidores DHCP de Windows NT, la versión del sistema que se utiliza y otros factores, como el superámbito. Si el servidor DHCP determina que el cliente todavía puede utilizar la dirección IP solicitada, permanece en silencio o envía un DHCPACK para el DHCPREQUEST. Si el servidor determina que el cliente no puede utilizar la dirección IP solicitada, envía un DHCPNACK al cliente. A continuación, el cliente pasa al estado de inicialización y envía un mensaje DHCPDISCOVER.

Nota: El servidor DHCP asigna la dirección IP inferior de un conjunto de direcciones IP a los clientes DHCP. Cuando expira el arrendamiento de la dirección inferior, se lo asigna a otro cliente si se solicita. No puede realizar cambios en el orden en que se asignan las direcciones DHCP.

Tabla de paquetes DHCP

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

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

Campo	Bytes	Nombre	Descripción
op	1	OpCode	Identifica el paquete como una solicitud o respuesta: 1 = BOOTREQUEST, 2 = BOOTREPLY
htype	1	Tipo de hardware	Especifica el tipo de dirección de red del hardware.
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 DHC intercambiados para una transacción DHCP determinada utilizan el I (xid).
secs	2	Segundos	Especifica el número de segundos desde que el proceso DHCP com
indicadores	2	Indicadores	Indica si el mensaje es de difusión o unidifusión.
ciaddr	4	Dirección IP del cliente	Sólo se utiliza cuando el cliente conoce la dirección de IP, como en e 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 coloca 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 s rellena con la dirección del servidor DHCP. En caso contrario, será utilizado en DHCPOFFER y DHCPACK desde el servidor DHCP.
giaddr	4	Dirección IP del router (GI ADDR)	La dirección IP de la gateway, completada por el agente de 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 inicialización	Nombre del archivo de arranque
opciones	Variable	Parámetros de opciones	Los parámetros optativos que puede proporcionar el servidor DHCP. 2132 proporciona todas las opciones posibles.

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

Descripción de	Dirección MAC de	Direcciones MAC de	Dirección IP de	Direc. IP de

paquete	origen	destino	origen	destino
DHCPDISCOVER	Cliente	Difusión	0.0.0.0	255.255.255
DHCPOFFER	Servidor DHCP	Difusión	Servidor DHCP	255.255.255
DHCPREQUEST	Cliente	Difusión	0.0.0.0	255.255.255
DHCPACK	Servidor DHCP	Difusión	Servidor DHCP	255.255.255

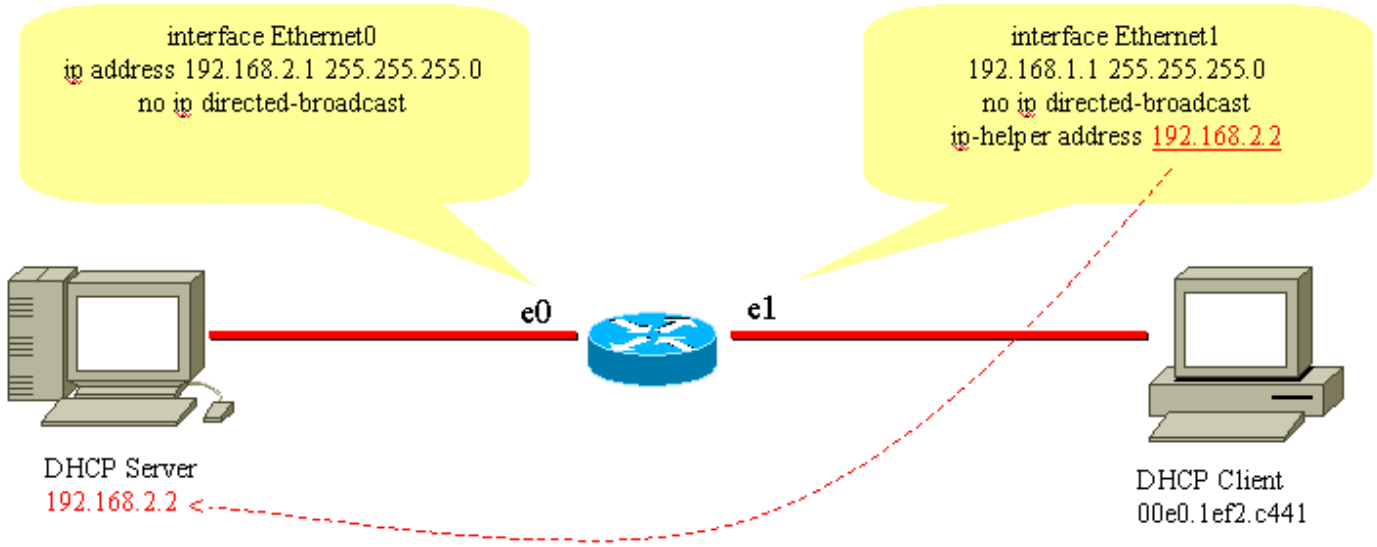
Rol del agente de relé DHCP/BootP

Los routers, de forma predeterminada, no reenvían paquetes de difusión. Dado que los mensajes del cliente DHCP utilizan la dirección IP de destino 255.255.255.255 (todas las transmisiones de red), los clientes DHCP no pueden enviar solicitudes a un servidor DHCP en una subred diferente a menos que el Agente de retransmisión DHCP/BootP esté configurado en el router. El Agente de retransmisión DHCP/BootP reenvía las solicitudes DHCP en nombre de un cliente DHCP al servidor DHCP. El Agente de retransmisión DHCP/BootP agrega su propia dirección IP a la dirección IP de origen de las tramas DHCP que van al servidor DHCP. Esto permite al servidor DHCP responder por unidifusión al agente de retransmisión DHCP/BootP. El Agente de retransmisión DHCP/BootP también rellena el campo Dirección IP de la puerta de enlace con la dirección IP de la interfaz en la que se recibe el mensaje DHCP del cliente. El servidor DHCP usa el campo Dirección IP de gateway para determinar la subred donde se originan los mensajes DHCPDISCOVER, DHCPREQUEST o DHCPINFORM.

Configuración de la Función DHCP/BootP Relay Agent en el Router Cisco IOS®

El proceso para configurar un router Cisco para reenviar solicitudes BootP o DHCP es simple. Sólo tiene que configurar una dirección de ayudante IP que apunte al servidor DHCP/BootP o a la dirección de difusión de subred de la red en la que se encuentra el servidor.

Ejemplo de red:



Agente de retransmisión DHCP/BootP

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. De forma predeterminada, la

dirección de ayudante IP reenvía estas difusiones UDP:

- 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 IP auxiliares pueden dirigir difusiones UDP a una dirección IP de unidifusión o difusión.Sin embargo, no utilice la dirección IP auxiliar para reenviar difusiones UDP de una subred a la dirección de difusión de otra subred, debido a la gran cantidad de inundación de difusión que puede ocurrir. También se soportan múltiples entradas de dirección de ayudante IP en una sola interfaz:

```
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 routers Cisco no son compatibles con el balance de carga de los servidores DHCP que se configuran como agentes de retransmisión DHCP. Los routers Cisco reenvían el mensaje DHCPDISCOVER a todas las direcciones del ayudante que se mencionan para dicha interfaz. El uso de dos o más servidores DHCP para servir a una subred sólo aumenta el tráfico DHCP, ya que los mensajes DHCPDISCOVER, DHCPOFFER y DHCPREQUEST / DHCPDECLINE se intercambian entre cada par de clientes y servidores DHCP.

Establecer enlaces manuales

Existen dos maneras de configurar enlaces manuales; una es para el host de Windows y la otra es para hosts que no son de Windows. Se utilizan dos comandos diferentes para configurar; uno es para clientes DHCP de Microsoft y el otro es para clientes DHCP que no son de Microsoft: **DHCPclient-identifier** (enlace manual - clientes DHCP de Microsoft) **y DHCPhardware-address** (enlace manual - clientes DHCP que no son de Microsoft). La razón de dos comandos diferentes es que una PC que se ejecuta con Windows modifica sus MAC y se agrega un **01** al principio de la dirección. Las siguientes son configuraciones de ejemplo:

- Esta es una configuración para clientes DHCP de Microsoft:

```
configure terminal
ip dhcp pool new_pool
host ip_address subnet_mask
client-identifier 01XXXXXXXXXXX

!--- xxxxxx represents 48 bit MAC address prepended with 01
```

- Esta es una configuración para clientes DHCP que no son de Microsoft:

```
configure terminal
ip dhcp pool new_pool
host ip_address subnet_mask
hardware-address XXXXXXXXXXX

!--- xxxxxx represents 48 bit MAC address
```

Cómo hacer que DHCP funcione en segmentos de IP secundarios

De manera predeterminada, DHCP tiene una limitación en que los paquetes de respuesta se envían solo si la solicitud se recibe de la interfaz configurada con la dirección IP principal. El tráfico de DHCP utiliza la dirección de difusión. Cuando la interfaz de router recibe la solicitud de DHCP, la desvía al servidor DHCP (cuando se configura la dirección IP de ayuda) con una dirección de origen de la IP principal configurada en la interfaz para permitir que el servidor DHCP sepa qué conjunto de IP debe utilizar (para el cliente) en el paquete de respuesta de DHCP.

No hay ninguna manera de que el router sepa si la solicitud de difusión DHCP proviene de un dispositivo que está en la red IP secundaria configurada en la interfaz. Como solución alternativa, la configuración de la subinterfaz (siempre que el dispositivo conectado al router admita el etiquetado dot1q) para separar las dos subredes se puede configurar, de modo que ambas obtengan sus direcciones IP correspondientes en forma correcta.

Si la dirección secundaria es la preferida, existe otra solución alternativa, que es habilitar el comando de configuración global **dhcp smart-relay**. Esto tiene una limitación, ya que solo usa la IP secundaria para retransmitir la solicitud de DHCP si no hay respuesta del servidor DHCP después de tres solicitudes consecutivas para el conjunto de direcciones principales.

Conversación entre cliente y servidor DHCP con la función relé DHCP

La siguiente tabla ilustra el proceso que un cliente DHCP debe seguir para obtener una dirección IP de un servidor DHCP. Esta tabla se basa en el diagrama de red anterior Configuración de la función de agente de relé DHCP/BootP. Cada valor numérico del diagrama representa un paquete que se describe en la siguiente tabla. Utilice esta tabla para comprender el flujo de paquetes de la conversación cliente-servidor DHCP. También le ayuda a determinar dónde se producen los

problemas.

Proceso para que un cliente DHCP obtenga una dirección IP

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.	Dire dest paqu
1. DHCPDISCOVER se envía desde el cliente.	0.0.0.0	0.0.0.0	0.0.0.0	0005.DCC9.C640	0.0.0.0	ffff.ffff.ffff (difusión)	255.
2. El router recibe el DHCPDISCOVER en la interfaz E1. El router reconoce que este paquete es una difusión DHCP UDP. El router ahora actúa como un Agente de retransmisión DHCP/BootP y rellena el campo Dirección IP de la puerta de enlace con la dirección IP de la interfaz entrante, cambia la dirección IP de origen a una dirección IP de la interfaz entrante y reenvía la solicitud directamente al servidor 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.
3. El servidor DHCP ha recibido el DHCPDISCOVER y envía un DHCPOFFER al Agente de retransmisión DHCP.	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.
4. El Agente Relay DHCP recibe un DHCPOFFER y	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.

reenvía el broadcast DHCPOFFER en la LAN local.							
5. DHCPREQUEST enviado desde el cliente.	0.0.0.0	0.0.0.0	0.0.0.0	0005.DCC9.C640	0.0.0.0	ffff.ffff.ffff (difusión)	255.
6. El router recibe el DHCPREQUEST en la interfaz E1. El router reconoce que este paquete es de transmisión DHCP UDP. El router ahora actúa como un Agente de retransmisión DHCP y rellena el campo Dirección IP de la puerta de enlace con la dirección IP de la interfaz enviada, cambia la dirección IP de origen por una dirección IP de la interfaz entrante y reenvía la solicitud directamente al servidor 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.
7. El servidor DHCP ha recibido el DHCPREQUEST y envía un DHCPACK al Agente de retransmisión DHCP/BootP.	192.168.1.2	192.168.2.2	192.168.1.1	Dirección MAC del servidor DHCP	192.168.2.2	Dirección de la interfaz E2 MAC	192.
8. El Agente de retransmisión DHCP/BootP recibe el DHCPACK y reenvía la difusión DHCPACK en la	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.

LAN local. El cliente acepta el ACK y utiliza la dirección IP del cliente.

Consideraciones sobre DHCP de inicio del Entorno de preejecución (PXE)

El entorno de ejecución previa (PXE) permite a una estación de trabajo arrancar desde un servidor de una red antes de arrancar el sistema en el disco duro local. De esta forma, no es necesario que el administrador de red tenga que estar frente a la estación de trabajo para iniciarla manualmente. El sistema operativo y otros programas, como los programas de diagnóstico, se pueden cargar en el dispositivo desde un servidor a través de la red. El entorno PXE utiliza DHCP para configurar su dirección IP.

La configuración del agente de retransmisión DHCP/BootP debe efectuarse en el router si el servidor DHCP está ubicado en otro segmento enrutado de la red. Se debe configurar el comando **ip helper-address** en la interfaz del router local. Consulte la sección Configuración de la Función DHCP/BootP Relay Agent en el Router Cisco IOS de este documento para obtener información de configuración.

Comprensión y Troubleshooting de DHCP con Rastreos de Sniffer

Decodificar el rastro del sabueso del cliente DHCP y el servidor en el mismo segmento LAN

Topología de Red en la que el Cliente DHCP y el Servidor Residen en el Mismo Segmento LAN

El ejemplo de seguimiento del sabueso está compuesto por seis tramas. Estas seis tramas ilustran un escenario en el que el cliente DHCP y el servidor residen en el mismo segmento físico o lógico. Utilice el siguiente ejemplo de código para resolver problemas de DHCP. Es importante hacer coincidir su rastro de sabueso con los rastros de este ejemplo. Puede haber algunas diferencias en comparación con los siguientes seguimientos ilustrados, pero el flujo general de paquetes debe ser exactamente el mismo. 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 Renewal 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 Renewal 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:
```

Decodificar el rastro del sabueso del cliente DHCP y el servidor separados por un router configurado como agente de retransmisión DHCP

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 Renewal 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 Renewal 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:
```

Rastro del analizador de protocolos 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 Renewal 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 Renewal 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:
```

Solucionar problemas de DHCP cuando las estaciones de trabajo cliente no pueden 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 de un servidor DHCP. Pero es poco probable que el router local cause un problema de DHCP. El problema está relacionado con los dispositivos que conectan el servidor DHCP y el cliente DHCP. Sin embargo, el problema puede estar en el servidor DHCP o en el propio cliente. Estos módulos ayudan a resolver problemas y determinar qué dispositivo causa un problema.

> **Nota:** Para configurar el servidor DHCP por VLAN, defina diferentes grupos DHCP para cada VLAN que proporcione direcciones DHCP a sus clientes.

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

Cuando el servidor DHCP y el cliente residen en los diferentes segmentos LAN o VLAN, el router funciona como un agente de retransmisión DHCP/BootP que es responsable de reenviar DHCPREQUEST al servidor DHCP. Se requieren pasos adicionales para resolver problemas del Agente de retransmisión DHCP/BootP, así como del servidor DHCP y el cliente. Si sigue estos módulos, puede determinar qué dispositivo causa los problemas.

El servidor DHCP en el router no puede asignar direcciones con un error de GRUPO AGOTADO

Es posible que algunas direcciones aún sean mantenidas por los clientes, incluso si se liberan del conjunto. Esto se puede verificar mediante la salida de conflicto **show ip dhcp**. Un conflicto de direcciones se produce cuando dos hosts utilizan la misma dirección IP. En la asignación de direcciones, el DHCP verifica los conflictos con el ping y el ARP gratuito.

Si se detecta un conflicto, la dirección se remueve del conjunto. La dirección se asigna hasta que el administrador resuelva.e el conflicto. **Configure un registro de conflictos ip dhcp** para resolver este problema.

Módulos de Troubleshooting de DHCP

Comprender dónde pueden ocurrir problemas de DHCP

El origen de los problemas de DHCP puede deberse a distintos motivos. Los motivos más frecuentes son los problemas de configuración. Sin embargo, muchos problemas de DHCP pueden deberse a defectos de software en los sistemas, controladores de tarjetas de interfaz de red (NIC) o agentes de retransmisión DHCP/BootP que se ejecutan en los routers. Debido al número de áreas potencialmente problemáticas, se requiere un enfoque sistemático para la resolución de problemas.

Lista de las causas posibles preseleccionadas de problemas de DHCP:

- Configuración predeterminada del switch Catalyst
- Configuración del agente de retransmisión DHCP/BootP
- Problema de compatibilidad de NIC o problema de la característica DHCP
- Instalación defectuosa de la NIC o del controlador de la NIC
- Interrupciones intermitentes en la red debido a cálculos frecuentes del árbol de expansión
- Conducta del sistema operativo o defecto del software
- Alcance de la configuración del servidor DHCP o defecto del software.
- Defecto del software del switch Cisco Catalyst o del agente de retransmisión DHCP/BootP de Cisco IOS
- El Desvío de Ruta Inversa de Unidifusión (uRPF) falla en la verificación porque la oferta de DHCP se recibe en una interfaz diferente de la esperada. Cuando la función Reverse Path Forwarding (RPF) está habilitada en una interfaz, un router de Cisco puede descartar los paquetes de protocolo de configuración dinámica de host (DHCP) y protocolo BOOTstrap (BOOTP) que tienen direcciones de origen de 0.0.0.0 y direcciones de destino de 255.255.255.255. El router también puede descartar todos los paquetes IP que tienen un destino IP multidifusión en la interfaz. Este problema se documenta con el ID de bug de Cisco CSCdw31925

Nota Sólo los clientes registrados de Cisco pueden acceder a los informes de errores.

- El agente de base de datos DHCP no se utiliza, pero el registro de conflictos DHCP noestá desactivado

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 está conectado a un switch Catalyst, verifique que tanto el cliente DHCP como el servidor tengan conectividad física. Para los switches basados en Cisco IOS como el Catalyst 2900XL/3500XL/2950/3550, el comando equivalente **toshow port status show interface <interface>**. Si el estado de la interfaz es distinto de **<**`interface`**>** está activo, el protocolo de línea está activo, el puerto no pasa el tráfico, ni siquiera las solicitudes del cliente DHCP. El resultado de los comandos:

```
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 ha verificado la conexión física y no existe realmente un link entre el switch Catalyst y el cliente DHCP, utilice la sección Troubleshooting de Switches Catalyst de Cisco a Problemas de Compatibilidad NIC para resolver problemas con respecto al problema de conectividad de la capa física.

Los errores excesivos de link de datos hacen que los puertos en algunos switches Catalyst entren en estado errdisable. Para obtener más información, consulte Recuperación del Estado del Puerto Errdisable en las Plataformas Cisco IOS, que describen el estado errdisable, explican cómo recuperarse de él y proporcionan ejemplos de recuperación de este estado.

B. Configure la Estación de Trabajo Cliente y la IP Estática para Probar la Conectividad de Red

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

Al resolver cualquier problema de DHCP, es importante configurar una dirección IP estática en una estación de trabajo cliente para verificar la conectividad de red. Si la estación de trabajo no puede alcanzar los recursos de red a pesar de tener una dirección IP configurada estáticamente, la causa raíz del problema no es DHCP. En este momento, debe solucionar los problemas de conectividad de red.

C. Verificar un problema de inicialización

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

Si el cliente DHCP no puede obtener una dirección IP del servidor DHCP al inicio, puede forzar manualmente al cliente a enviar una solicitud DHCP. Siga estos pasos para obtener manualmente una dirección IP de un servidor DHCP para el sistema operativo de la lista.

Microsoft Windows 95/98/ME:

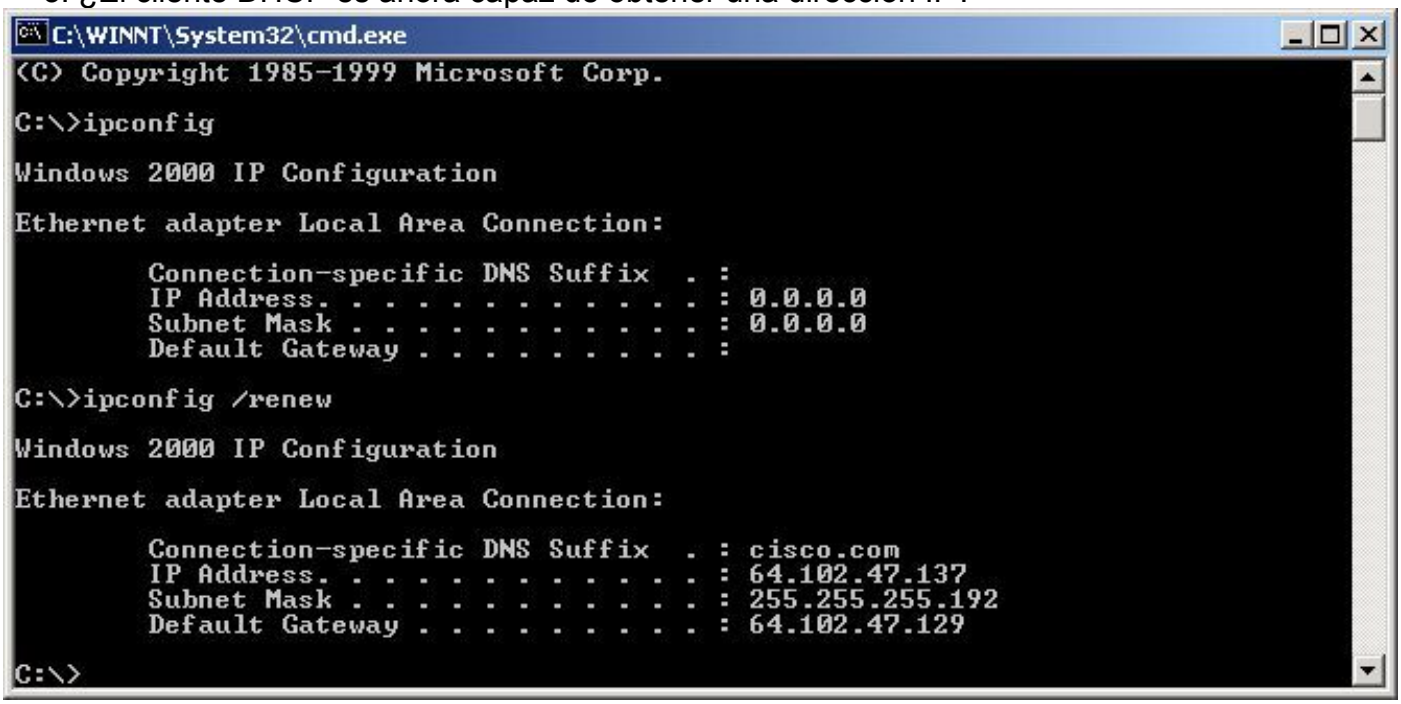
1. Haga clic en el botón Inicio y ejecute el programa WINIPCFG.exe.
2. Haga clic en **el botónLiberar** todo seguido **del botónRenovar** todo.

3. ¿El cliente DHCP es ahora capaz de obtener una dirección IP?

Ventana Configuración de IP

Microsoft Windows NT/2000:

1. Ingrese cmdin theStart/Runfield para abrir una ventana del símbolo del sistema.
2. Ejecute el comando **commandipconfig/**renew en la ventana del símbolo del sistema.
3. ¿El cliente DHCP es ahora capaz de obtener una dirección IP?



Símbolo de línea de comandos

Si el cliente DHCP puede obtener una dirección IP con una renovación manual de la dirección IP después de que el PC haya completado el proceso de inicio, lo más probable es que el problema sea un problema de inicio de DHCP. Si el cliente DHCP está conectado a un switch Catalyst de Cisco, el problema es más probable debido a un problema de configuración que trata con STP portfast y/o canalización y trunking. Otras posibilidades incluyen los problemas con las tarjetas NIC y con el inicio del puerto del switch. Revise los pasos D y E para descartar la configuración del puerto del switch y los problemas de la tarjeta NIC como la causa raíz del problema de DHCP.

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

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

Para obtener más documentación sobre los requisitos de configuración de puertos de switch necesarios para que DHCP funcione correctamente cuando se conecta a switches Catalyst, consulte Uso de Portfast y Otros Comandos para Corregir Demoras de Conectividad de Inicio de Estación de Trabajo.

Una vez revisado el documento, puede continuar solucionando estos problemas.

E. Compruebe si hay problemas conocidos de tarjetas NIC o switches Catalyst

Si la configuración del switch Catalyst es correcta, es posible que exista un problema de compatibilidad de software en el switch Catalyst o en la NIC del cliente DHCP que podría causar los problemas de DHCP. El siguiente paso para resolver problemas es revisar Troubleshooting de Problemas de Compatibilidad entre los Switches Catalyst de Cisco y NIC y descartar cualquier problema de software con el switch Catalyst o NIC que contribuya al problema.

Es necesario conocer el sistema operativo del cliente DHCP, así como información específica de NIC como el fabricante, el modelo y la versión del controlador para descartar correctamente cualquier problema de compatibilidad.

F. Distinga si los clientes DHCP obtienen la dirección IP en la misma subred o VLAN que el servidor DHCP

Es importante distinguir si DHCP funciona correctamente cuando el cliente está en la misma subred o VLAN que el servidor DHCP. Si el DHCP funciona correctamente en la misma subred o VLAN que el servidor DHCP, el problema DHCP es causado principalmente por el Agente de retransmisión DHCP/BootP. Si el problema persiste incluso cuando se prueba DHCP en la misma subred o VLAN que el servidor DHCP, el problema puede ser realmente con el servidor DHCP.

G. Verificar la Configuración de DHCP/BootP Relay del Router

Para verificar la configuración:

1. Cuando configure el relé DHCP en un router, verifique que el comando **ip helper-**addressse encuentre en la interfaz correcta. **El comando ip helper-**addresscommand debe estar presente en la interfaz entrante de las estaciones de trabajo cliente DHCP y debe ser dirigido al servidor DHCP correcto.
2. Verifique que el comando de configuración global **service** dhcp no esté presente. Este parámetro de configuración inhabilita toda la funcionalidad de servidor DHCP y relé en el router. La configuración predeterminada, service dhcp, no aparece en la configuración y es el comando de configuración predeterminado. Si **el servicio dhcp** no está habilitado, los clientes no reciben las direcciones IP del servidor DHCP.**Nota:** En los routers que ejecutan versiones de Cisco IOS más antiguas, el comando de servidor IP BootP administra la función de agente de retransmisión DHCP en lugar del **comando Service DHCP.** Debido a esto, el

comando IP BootP Server debe estar habilitado en estos routers si el comando IP helper-Address está configurado para reenviar difusiones UDP de DHCP y actuar correctamente como agente de retransmisión DHCP en nombre del cliente DHCP.

3. Cuando utilice los comandos **ip helper-**addresspara reenviar broadcasts UDP a una dirección de broadcast de subred, verifique que no ip directed-broadcast no está configurado en ninguna interfaz saliente que los paquetes de broadcast UDP deban atravesar. no ip directed-broadcast bloquea cualquier traducción de una difusión dirigida a difusiones físicas. Esta configuración de interfaz es la configuración predeterminada en las versiones de software 12.0 y posteriores.
4. Cuando las difusiones DHCP se reenvían a la dirección de difusión de subred del servidor DHCP puede surgir un problema de software. Cuando resuelva problemas de DHCP, intente reenviar las difusiones DHCP UDP a la dirección IP del servidor DHCP:

H. Opción de identificación de suscriptor (82) activada

La función información del agente de retransmisión DHCP (opción 82) permite que los agentes de retransmisión DHCP (Catalyst switches) incluyan información sobre sí mismo y el cliente conectado cuando reenvía solicitudes DHCP de un cliente DHCP a un servidor DHCP.

El servidor DHCP puede utilizar esta información para asignar direcciones IP, realizar el control de acceso y establecer políticas de calidad de servicio (QoS) y de seguridad (u otras políticas de asignación de parámetros) para cada suscriptor de una red de proveedor de servicios. Cuando la indagación DHCP está habilitada en un switch, habilita automáticamente la opción 82. Si el servidor DHCP no está configurado para manejar los paquetes con la opción 82, deja de asignar la dirección a esa solicitud. Para resolver este problema, inhabilite la opción de identificación del suscriptor (82) en los switches (agentes de retransmisión) con el comando de configuración global, **no ip dhcp relay information option**.

I. Agente de base de datos DHCP y registro de conflictos DHCP

Un agente de base de datos DHCP es cualquier host (por ejemplo, un servidor FTP, TFTP o RCP) que almacena la base de datos de enlaces DHCP. Puede configurar varios agentes de la base de datos DHCP, y puede configurar el intervalo entre las actualizaciones y las transferencias de la base de datos para cada agente. Utilice el comando **ip dhcp database** para configurar un agente de base de datos y los parámetros del agente de base de datos.

Si decide no configurar un agente de base de datos DHCP, deshabilite la grabación de conflictos de direcciones DHCP en el servidor DHCP. Ejecute el comando **enoip dhcp conflict logging** para inhabilitar el registro de conflictos de direcciones DHCP. Borre los conflictos previamente registrados **conclear ip dhcp conflict**.

Si esto no deshabilita el registro de conflictos, aparece este mensaje de error:

```
%DHCPD-4-DECLINE_CONFLICT: DHCP address conflict: client
```

J. Compruebe CDP para conexiones de teléfono IP

Cuando el switchport que está conectado al teléfono IP de Cisco tiene la Cisco Discovery Protocol (CDP) deshabilitada, el servidor DHCP no puede asignar una dirección IP adecuada al teléfono. El servidor DHCP tiende a asignar la dirección IP que pertenece a la VLAN o subred de los datos

del switchport. Si el CDP está habilitado, el switch es capaz de detectar que el teléfono IP de Cisco solicita el DHCP y puede proporcionar la información de subred correcta. Luego, el servidor DHCP puede asignar una dirección IP del conjunto de subredes o VLAN de voz. No se requieren pasos explícitos para vincular el servicio DHCP a la VLAN de voz.

K. Quitar SVI descendente interrumpe la operación de indagación DHCP

En los switches de la serie Cisco Catalyst 6500, se crea automáticamente un SVI (en estado de apagado) después de que configura el DHCP en el comando snoop para una VLAN en particular. La presencia de este SVI tiene implicaciones directas en el correcto funcionamiento del snooping de DHCP.

El snooping de DHCP en los switches Catalyst de Cisco serie 6500 que ejecutan el IOS de Cisco nativo se implementa principalmente en el procesador de ruta (RP o MSFC), no en el procesador de switch (SP o Supervisor). La serie Cisco Catalyst 6500 intercepta los paquetes en el hardware con VACLs que proporcionan los paquetes a una lógica de destino local (LTL) suscrita por el RP. Una vez que los marcos entran en el RP, primero deben asociarse a una interfaz de capa 3 (SVI) IDB antes de que puedan pasarse a la parte snooping. Sin SVI, este IDB no existe y los paquetes se descartan en el RP.

L. Dirección de difusión limitada

Cuando un cliente DHCP establece el bit de difusión en un paquete DHCP, el servidor DHCP y el agente de retransmisión envían mensajes DHCP a los clientes con la dirección de difusión todo unos (255.255.255.255). Si el comando **ip broadcast-address** se ha configurado para enviar una difusión de red, se invalida la difusión de todos unos enviada por DHCP. Para remediar esta situación, utilice el comando **ip dhcp limited-broadcast-address** para asegurarse de que una transmisión de red configurada no invalide el comportamiento predeterminado de DHCP.

Algunos clientes DHCP solo pueden aceptar una difusión de todos los unos y no pueden adquirir una dirección DHCP, a menos que este comando esté configurado en la interfaz del router conectada al cliente.

M. Debug DHCP con comandos de depuración del router

Verifique que el router reciba la solicitud DHCP con los comandos debug

En los routers que admiten software que procesa paquetes DHCP, puede verificar si un router recibe la solicitud DHCP del cliente. El proceso DHCP falla si el router no recibe solicitudes del cliente. En este paso, configure una lista de acceso para depurar la salida. Esta lista de acceso sólo se utiliza para depurar un comando y no es intrusiva para el router.

En el modo de configuración global, ingrese esta lista de acceso:

access-list 100 permit ip host 0.0.0.0 host 255.255.255.255

En el modo exec, ingrese este comando debug:

depurar paquete ip, detalle 100

Ejemplo de Salida

```
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
```

En este ejemplo de salida, está claro que el router recibe activamente las solicitudes DHCP del cliente. Esta salida sólo muestra un resumen del paquete y no el paquete en sí. Por lo tanto, no es posible determinar si el paquete es correcto. Sin embargo, el router recibió un paquete de transmisión con la fuente y el destino IP y los puertos UDP que son adecuados para DHCP.

Verifique que el router reciba y reenvíe la solicitud DHCP con el comando debug ip udp

El comando **debug ip udp** puede rastrear la trayectoria de una solicitud DHCP a través de un router. Sin embargo, esta depuración es intrusiva en un entorno de producción, ya que todos los paquetes UDP conmutados procesados se muestran en la consola. Este comando debug no se debe utilizar en producción.

> **Advertencia:** El comando **debug ip udp** es intrusivo y puede causar una alta utilización de la Unidad de procesamiento central (CPU).

En el modo exec, ingrese este comando debug: **debug ip udp**

Ejemplo de Salida

```
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 recibe y reenvía la solicitud DHCP con el comando debug ip dhcp server packet

Si el router Cisco IOS es 12.0.x.T o 12.1 y soporta la funcionalidad del servidor DHCP de Cisco IOS, puede utilizar el comando **debug ip dhcp server packet**. Esta depuración estaba pensada para su uso con la función de servidor DHCP del IOS y para resolver problemas de la función de agente de relé DHCP/BootP también. Al igual que con los pasos anteriores, las depuraciones del router no proporcionan una determinación exacta del problema, ya que el paquete real no se puede ver. Sin embargo, los debugs permiten inferencias con respecto al procesamiento DHCP. En el modo exec, ingrese este comando debug:

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.
```

Ejecutar varias depuraciones simultáneamente

Cuando se ejecutan varias depuraciones simultáneamente, se puede descubrir una buena cantidad de información con respecto al funcionamiento del Agente de retransmisión DHCP/BootP y el servidor. Si utiliza los esquemas anteriores para resolver problemas, puede hacer inferencias sobre dónde no funciona correctamente la funcionalidad del Agente de retransmisión DHCP/BootP.

```
IP: s=0.0.0.0 (Ethernet0), d=255.255.255.255, len 604, rcvd 2
UDP src=68, dst=67
UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
DHCPD: setting giaddr to 192.168.1.1.
UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604
IP: s=192.168.1.1 (local), d=192.168.2.2 (Ethernet1), len 604, sending
UDP src=67, dst=67
DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3030.302e.3030.3030.2e30.3030.312d.4574.30 forwarded
to 192.168.2.2.
IP: s=192.168.2.2 (Ethernet1), d=192.168.1.1, len 328, rcvd 4
UDP src=67, dst=67
UDP: rcvd src=192.168.2.2(67), dst=192.168.1.1(67), length=308
DHCPD: forwarding BOOTREPLY to client 0000.0000.0001.
DHCPD: broadcasting BOOTREPLY to client 0000.0000.0001.
UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=328
IP: s=0.0.0.0 (Ethernet0), d=255.255.255.255, len 604, rcvd 2
UDP src=68, dst=67
UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
DHCPD: setting giaddr to 192.168.1.1.
UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604
IP: s=192.168.1.1 (local), d=192.168.2.2 (Ethernet1), len 604, sending
UDP src=67, dst=67
DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3030.302e.3030.3030.2e30.3030.312d.4574.30 forwarded
to 192.168.2.2.
IP: s=192.168.2.2 (Ethernet1), d=192.168.1.1, len 328, rcvd 4
UDP src=67, dst=67
UDP: rcvd src=192.168.2.2(67), dst=192.168.1.1(67), length=308
DHCPD: forwarding BOOTREPLY to client 0000.0000.0001.
DHCPD: broadcasting BOOTREPLY to client 0000.0000.0001.
UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=328.
```

Obtenga la traza del analizador de protocolos para determinar la causa raíz del problema de

DHCP

Revise las secciones Decode Sniffer Trace of DHCP Client and Server on Same LAN Segment y Decode Sniffer Trace of DHCP Client and Server Separated by Router Configured as a DHCP Relay Agent

para descifrar los seguimientos de paquetes DHCP.

Para obtener información sobre cómo obtener seguimientos de sabueso con la función Analizador de puerto conmutado (SPAN) en los switches Catalyst, consulte Ejemplo de Configuración del Analizador de puerto conmutado (SPAN) de Catalyst.

Método alternativo de descodificación de paquetes con depuración en el router

Con el comando **debug ip packet detail dump <acl>** en un router Cisco, es posible obtener un paquete completo en hexadecimal que se muestra en el registro del sistema o en la Interfaz de línea de comandos (CLI). Revise las secciones Verificar que el Router Recibe la Solicitud DHCP con los Comandos de debug y Verificar que el Router Recibe la Solicitud DHCP y Reenvía la Solicitud al Servidor DHCP con los Comandos de debug anteriores, junto con la palabra clave dump agregada a la lista de acceso, para obtener la misma información de debug, pero con los detalles del paquete en hexadecimal. Para determinar el contenido del paquete, éste debe traducirse. En el Apéndice A se presenta un ejemplo.

Apéndice A: Ejemplo de Configuración DHCP de Cisco IOS

La base de datos del servidor DHCP se organiza como un 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, por ejemplo el nombre de dominio, se deben configurar en el nivel más alto (red o subred) del árbol.

Para obtener más información sobre cómo configurar DHCP y los comandos asociados con él, consulte la Lista de Tareas de Configuración DHCP.

```
version 12.1
!
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
enable password cisco
ip subnet-zero
no ip domain-lookup
ip dhcp excluded-address 10.10.1.1 10.10.1.199

!--- Address range excluded from DHCP pools.

ip dhcp pool test_dhcp

!--- DHCP pool (scope) name is test_dhcp.

network 10.10.1.0 255.255.255.0
```

```
!--- DHCP pool (address will be assigned in this range) for associated Gateway IP address.

default-router 10.10.1.1

!--- DHCP option for default gateway.

dns-server 10.30.1.1

!--- DHCP option for DNS server(s).

netbios-name-server 10.40.1.1

!--- DHCP option for NetBIOS name server(s) (WINS).

lease 0 0 1

!--- Lease time.

interface Ethernet0
description DHCP Client Network
ip address 10.10.1.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet1
description Server Network
ip address 10.10.2.1 255.255.255.0
no ip directed-broadcast
!
line con 0
transport input none
line aux 0
transport input all
line vty 0 4
login
!
end
```

Información Relacionada

- Herramientas y Recursos
- Soporte Técnico - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).