Práctica 3: DHCP, funcionamiento y análisis de trazas.

1. Sesión L3

Lectura previa: Kurose 4.4.2, subapartado "Cómo obtener una dirección de host: Protocolo de configuración dinámica de host" (pags. 336-339).

Trabajo previo a realizar antes de la sesión de laboratorio:

- Lectura del apartado: **Introducción.**
- Estudio del apartado: **Funcionamiento del protocolo DHCP.**

La práctica se realizará en ***WINDOWS*** porque, a diferencia de lo que ocurre en Linux, permite ejecutar el cliente DHCP sin necesidad de ser administrador del sistema.

2. Objetivos

Al acabar esta práctica deberías conocer lo suficiente sobre el protocolo DHCP para ser capaz de:

- Explicar la utilidad del protocolo DHCP.
- Describir sus mensajes básicos y cómo se llaman.
- Interpretar los principales campos de un mensaje DHCP capturado mediante el programa Wireshark.
- Explicar el papel que desempeña un agente retransmisor DHCP.
- Interpretar en una captura Wireshark si se utiliza o no un agente retransmisor y, en el caso de que se utilice, cuál es su dirección IP.

3. Introducción.

En esta práctica vamos a estudiar la forma más habitual que tiene un nodo para obtener una dirección IP: mediante la utilización del **Protocolo de Configuración Dinámica de Host (**Dynamic Host Configuration Protocol**).**

Hemos estudiado en clase, cómo una organización puede obtener un bloque de direcciones IP para ser distribuido entre todos los nodos que pertenecen a su subred. También hemos visto que un nodo necesita tener una dirección IP para quedar perfectamente identificado en Internet y esta dirección se la tiene que asignar su organización (habitualmente su ISP).

Esta asignación se puede hacer de forma manual, es decir, es el administrador el que configura el equipo asignando una dirección IP fija. Esta forma de configuración es habitual en los routers.

Pero otras veces es interesante que la asignación se realice de forma automática, en el proceso de arranque del sistema. Esto resulta especialmente útil cuando las computadoras tienen la opción de conectarse a redes diferentes, como es el caso hoy en día de los equipos portátiles.

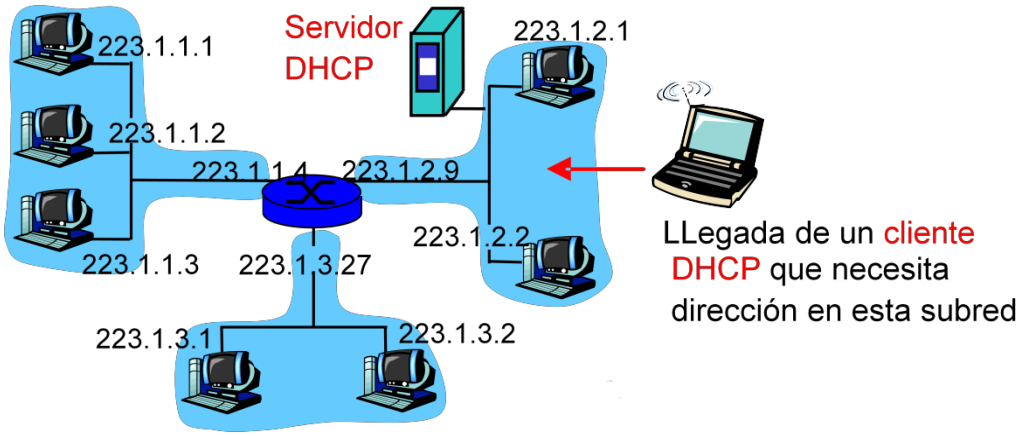
El protocolo DHCP permite realizar esta asignación automática de direcciones IP. Además de la asignación de direcciones IP a los nodos, DHCP también permite que un nodo obtenga información adicional necesaria para el funcionamiento en Internet:

máscara de subred, dirección del router asignado (gateway) y dirección de su servidor DNS local.

A pesar de que abordamos el estudio del protocolo DHCP junto con el nivel de red de la pila de protocolos TCP/IP, es necesario aclarar que el protocolo DHCP es un protocolo del **nivel de aplicación** que se apoya en el protocolo UDP. DHCP permite que dos partes se comuniquen:

- **Cliente DHCP:** nodo que se conecta a una subred y solicita dirección IP.
- **Servidor DHCP:** nodo que se encarga de gestionar el bloque de direcciones IP de una organización. El servidor DHCP se identifica mediante el puerto 67.

En el caso más simple cada subred tendrá un servidor DHCP. Si en la subred no hay ningún servidor, será necesario un agente de retransmisión DHCP (normalmente un router) que conozca la dirección de un servidor DHCP para dicha red. La figura que mostramos a continuación nos presenta los dos casos



4. Funcionamiento del protocolo DHCP

Cuando un nodo arranca y no tiene todavía configuración IP, tendrá que pasar por cuatro etapas para conseguirla:

1. **Etapa de Descubrimiento:** cuando un nodo con configuración IP dinámica arranca ni siquiera tiene la información de la dirección de la red a la que se está conectando, ni mucho menos la dirección de un servidor DHCP de esa red. La primera tarea, por tanto, será encontrar un servidor DHCP con el que interactuar.

   Para ello, el nodo enviará un mensaje DHCP de descubrimiento (DHCPDiscover) al puerto 67 y dirigido a toda la red. Como no conoce su propia IP ni la del servidor, el datagrama IP que contenga el mensaje de descubrimiento utilizará las siguientes direcciones:

   - Dirección IP origen: 0.0.0.0. Ya que el nodo todavía no tiene dirección IP asignada.
   - Dirección IP destino: 255.255.255.255. Dirección IP de difusión para que llegue a toda la red.

   Por último, comentar que el mensaje DHCPDISCOVER contendrá un **Identificador de Transacción** que permite asociar las respuestas con la petición.
2. **Etapa de ofrecimientos:** El mensaje DHCPDISCOVER lo van a recibir todos los elementos de la red local, incluidos todos los servidores DHCP de la red. Pero sólo los

servidores que hayan sido programados para responder a un cliente en particular enviarán un mensaje DHCP de ofrecimiento (DHCPOFFER).

Por tanto, un cliente podrá recibir cero o más respuestas. Cada mensaje DHCPOFFER contendrá: el Identificador de Transacción que llevaba el mensaje DHCPDISCOVER, la dirección IP que el servidor ofrece al cliente, la máscara de red correspondiente y el tiempo de concesión de la dirección IP ofrecida: tiempo de validez de dicha dirección.

Los mensajes DHCPOFFER son unicast, salvo que el cliente solicite que le devuelvan la respuesta por difusión:

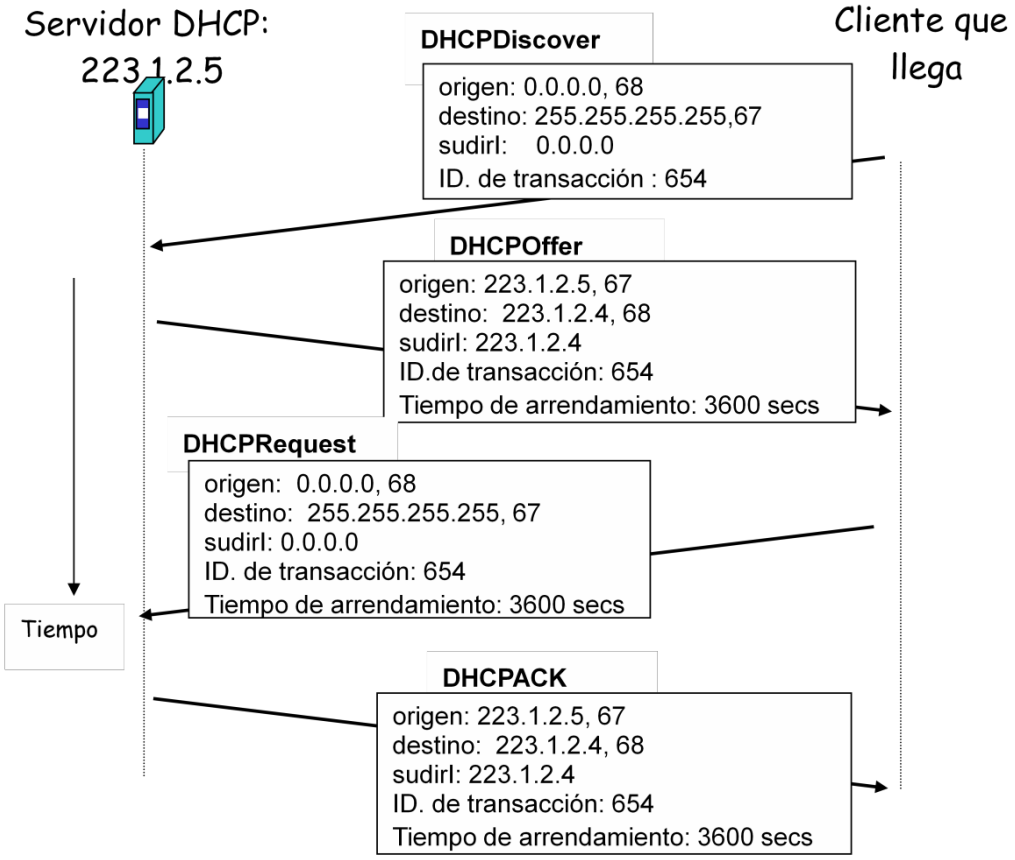
- Dirección origen: dirección IP del servidor DHCP.
- Dirección destino: dirección IP que el servidor ofrece al cliente o 255.255.255.255 si el cliente lo ha solicitado.

3. **Etapa de Petición DHCP**: El nodo cliente deberá seleccionar una de las respuestas según algún criterio: primero en llegar, mayor tiempo asignado,… Después de elegir, el cliente mandará un mensaje de petición DHCP al servidor elegido: DHCPREQUEST. Este mensaje repetirá los parámetros de configuración que le han propuesto al cliente.

4. **Etapa de Confirmación:** Enviado el mensaje de petición, el cliente espera la confirmación del servidor, que le llegará mediante un mensaje DHCP de reconocimiento (DHCPACK).

5. A partir de este momento el nodo cliente pasará a un estado estable en el que ya podrá utilizar la dirección IP asignada durante el tiempo de arrendamiento.

La siguiente figura muestra estos cuatro pasos:



Una vez el cliente ha conseguido su dirección IP, puede dejar de necesitarla en cualquier momento. Para finalizar el arrendamiento de la dirección IP antes del tiempo asignado, el cliente deberá mandar un mensaje **DHCPRELEASE** al servidor. A partir de ese momento el cliente ya no podrá usar esa dirección IP y el servidor DHCP podrá asignarla a cualquier otro nodo que lo solicite.

Por el contrario, si un nodo agota el tiempo de arrendamiento que se le ha concedido en la asignación de la dirección IP y desea seguir utilizándola puede renovar su tiempo de arrendamiento mediante un mensaje DHCPREQUEST.

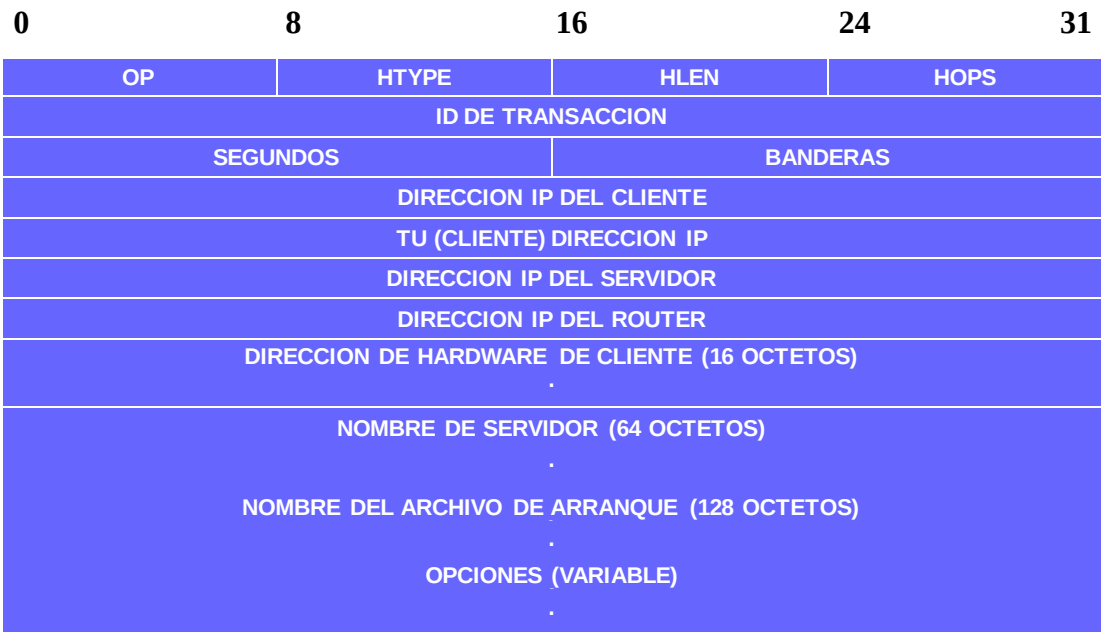
El servidor podrá contestar afirmativamente mediante un DHCPACK, o bien, denegar la prórroga de tiempo mediante un mensaje DHCPNACK (mensaje DHCP de reconocimiento negativo). En este último caso, el cliente abandonará la dirección IP inmediatamente.

Agente retransmisor DHCP

Como hemos visto, varios de los mensajes DHCP se envían por difusión, mediante la dirección destino 255.255.255.255. Las difusiones realizadas de esta forma son filtradas por los routers, y por tanto, no pueden alcanzar a destinos externos a la red local donde se haya originado la difusión. Esto supone que, en principio, se requeriría un servidor DHCP en cada red que deseara utilizar el servicio. Para evitar este requerimiento pueden emplearse agentes retransmisores DHCP (*DHCP relay agent*). Son dispositivos que reciben las solicitudes de los clientes enviadas como difusiones y las reenvían en modo unicast a la dirección del servidor DHCP. Se puede configurar como agente retransmisor el router de salida de la red, o bien un host que esté en la misma red que el cliente DHCP.

Formato del mensaje DHCP

Tanto los mensajes DHCP de petición como los de respuesta tienen el mismo formato que se muestra a continuación:



Veamos el significado de cada uno de los campos:

- **OP**: (1) Solicitud (2) Réplica.
- **HTYPE**: Tipo de Hardware de Red. Ej: (1) Ethernet.
- **HLEN**: Longitud de la dirección Hardware. Ej: Ethernet (6).
- **HOPS**: Número de saltos. El cliente lo pone a cero. Si el servidor recibe la solicitud y decide pasarla a otra máquina lo incrementa.
- **ID. DE TRANSACCIÓN**: entero que la máquina utiliza para emparejar las respuestas con las solicitudes.
- **SEGUNDOS**: el cliente apunta el número de segundos desde que comenzó el arranque.
- **BANDERAS**: sólo el bit de orden superior tiene asignado significado. El resto se pone a cero. Un 1 en el bit de orden superior indica que el servidor debe responder con la difusión IP, lo que implicará también una difusión hardware. Con un 0 se solicita una respuesta unicast.
- **DIR. IP DEL CLIENTE:** Si el cliente ya tiene asignada una dirección IP utilizará este campo para ponerla. En caso contrario, pondrá a cero este campo.
- **TU (CLIENTE) DIRECCIÓN IP:** cuando el cliente todavía no tiene dirección asignada, se utiliza este campo para indicar la dirección IP que se le ofrece.
- **DIR. IP DEL SIGUIENTE SERVIDOR**: lo utiliza el servidor en sus respuestas al cliente (DHCPOFFER y DHCPACK) para indicarle la dirección del siguiente servidor DHCP que debe usar en el proceso de arranque.
- **DIR. IP DEL AGENTE RETRANSMISOR:** si se quiere especificar.
- **NOMBRE DEL SERVIDOR:** funciona igual que la dirección IP del servidor.
- **NOMBRE DEL FICHERO DE ARRANQUE:** un administrador puede querer tener varios tipos de arranque (Ej. UNIX, WINDOWS, etc.). En ese caso, puede especificarlo en este campo.
- **OPCIONES:** con este campo DHCP puede codificar una gran variedad de cosas diferentes: duración del arrendamiento, tipo de mensaje, máscara de red, … Cada opción está a su vez formada por tres campos:
    1. **Código:** indica el tipo de opción. Ocupa un byte.
    2. **Longitud:** indica el número de bytes del campo datos. Ocupa un byte
    3. **Datos:** la información concreta que atañe a esa opción. Tiene longitud variable.

    Ejemplo de opción: Una opción que aparece en todos los mensajes DHCP es la número 53, que indica el tipo de mensaje DHCP. Se trata de una opción de 3 octetos que tienen el siguiente significado y valor:

CODIGO (53)	LONGITUD (1)	TIPO (1-7)

    Donde el tipo de mensaje puede ser:

TIPO	MENSAJE
1	DHCPDISCOVER
2	DHCPOFFER
3	DHCPREQUEST
4	DHCPDECLINE
5	DHCPACK
6	DHCPNACK
7	DHCPRELEASE

El mensaje DHCPDECLINE lo utiliza el cliente para comunicar al servidor que la dirección IP ofrecida ya está en uso.

4. Análisis de tráfico

En esta práctica vamos a utilizar el analizador de protocolos que ya conocemos, *Wireshark*, para analizar el tráfico que generan un cliente y un servidor DHCP, tanto cuando el cliente solicita dirección IP al servidor como cuando la libera.

Pero antes de ponernos a trabajar con el analizador de protocolos, es interesante recordar de la práctica 1 cómo averiguan los ordenadores del Laboratorio de Redes el tipo de configuración IP, es decir, cómo obtienen la dirección IP. Veíamos en la práctica 1 que nuestros equipos de trabajo obtienen la configuración IP de forma automática, es decir, mediante el diálogo con un servidor DHCP. Recordad que ese servidor DHCP estaba fuera de la red del Laboratorio de Redes. Por lo tanto, en ese diálogo entre nuestra máquina (cliente DHCP) y el servidor DHCP que le proporciona la información IP intervendrán agentes retransmisores.

Ejercicio 1. Abre una ventana de DOS y ejecuta la orden ***ipconfig /all.*** De toda la información que se te muestra, ¿qué parámetros están relacionados con el diálogo DHCP inicial que se ha producido en el arranque del sistema? ¿Cuándo se ha obtenido la concesión de la dirección IP? ¿Cuándo caduca?

La particularidad que tiene el protocolo DHCP es que el tráfico DHCP se genera fundamentalmente en el arranque del equipo. Una vez el nodo está listo para poder tomar capturas con el Wireshark, el diálogo DHCP ya ha finalizado. Puede aparecer un nuevo diálogo DHCP cuando se cumpla el tiempo de concesión de la dirección IP y se quiera renovar, pero no es cuestión de esperar hasta entonces.

Podríamos utilizar una orden que ya estudiasteis en la práctica 1. Esta nos permite liberar la dirección IP que le han asignado a la máquina en el arranque, y volver a pedir después una nueva asignación mediante un diálogo DHCP.

Esta orden es el **ipconfig,** de la que destacamos 3 opciones solamente:

ipconfig /all	Muestra toda la información de configuración
ipconfig /release	Libera la dirección IPv4
ipconfig /renew	Renueva la dirección IPv4

Ejercicio 2. Ponemos en marcha el analizador de protocolos Wireshark e iniciamos una captura filtrando el tráfico UDP que utilice el puerto 67. A continuación, utilizamos el comando ***ipconfig /release*** para liberar la información IP que tiene nuestro ordenador y después el comando ***ipconfig /renew*** para volver a obtener dirección IP, mientras está en marcha la captura con el Wireshark. Una vez finalizado este proceso paramos la captura.

Con este proceso hemos obtenido todo el diálogo DHCP que realizan un cliente y servidor DHCP para conseguir una dirección IP. Este diálogo, en nuestro caso, estará precedido por el diálogo mediante el cual el cliente ha renunciado a la configuración IP que había obtenido en el arranque del sistema.

Vamos a analizar los resultados obtenidos en la captura.

Por si acaso el proceso de obtención de mensajes DHCP nos da problemas, y con el objetivo de que trabajemos todos con las mismas capturas hemos dejado en Poliformat dos capturas: **Captura1Practica3.pcap** que recoge el proceso de obtención de configuración IP y **Captura2Practica3.pcap** que recoge el proceso de liberación de la configuración IP. Ämbas están listas para su análisis y podemos trabajar con ellas a partir ahora.

Ejercicio 3. Descárgate del Poliformat la captura **Captura1Practica3.pcap** y ábrela con el programa Wireshark.

a) Nos centramos en primer lugar en el primer mensaje DHCP que interviene en el proceso de obtención de dirección IP: DHCPDISCOVER. Basándote en la información obtenida, ¿qué servicio utiliza DHCP, TCP o UDP? Mirando las direcciones IP origen y destino del datagrama de este primer mensaje DHCP que te aparece, ¿podrías justificar la elección de DHCP por un servicio sin conexión?

b) Selecciona el **mensaje DHCPDiscover** y busca la información para rellenar los siguientes campos (se trata de información que corresponde a distintos niveles de la arquitectura y está en diferentes cabeceras):

Tipo de Mensaje (en el campo de opciones DHCP)	
Dir. IP origen del datagrama (en cab. IP)	
Dir. IP destino del datagrama (en cab. IP)	
Puertos origen y destino (en cab. UDP)	
Id. Transacción (en cabecera DHCP)	
Campo dir. IP Cliente (en cabecera DHCP)	
Campo Tu dirección IP (en cabecera DHCP)	
Campo Dir. IP del Agente Retransmisor (cab. DHCP)	

c) En este mensaje el nodo no solicita una dirección IP cualquiera, sino que pide una dirección concreta que está asociada a su dirección física. ¿En qué campo del mensaje se hace esta solicitud?

d) Entre las distintas opciones aparece la lista de parámetros que el cliente solicita al servidor. Cita las cuatro primeras.

Ejercicio 4. A continuación podemos ver los mensajes de ofrecimiento de los servidores: DHCPOFFER.

a) ¿Cuántos mensajes de este tipo hay? ¿Qué conclusiones podemos sacar acerca del número de servidores DHCP disponibles en la red de la UPV?

b) Busca en el primer mensaje DHCPOffer la información para rellenar los siguientes campos:

Tipo de Mensaje (en el campo de opciones DHCP)	
Dir. IP origen del datagrama (en cab. IP)	
Dir. IP destino del datagrama (en cab. IP)	
Puertos origen y destino (en cab. UDP)	
Id. Transacción (en cabecera DHCP)	
Campo dir. IP Cliente (en cabecera DHCP)	
Campo Tu dirección IP (en cabecera DHCP)	
Campo Dir. IP del Agente Retransmisor (cab. DHCP)	

c) ¿En qué campo de los mensajes DHCPOffer aparece la mayor parte de la información de configuración IP que el Servidor ofrece al Cliente? Comprueba todo lo que ofrecen los servidores DHCP. En particular, fíjate en el valor del campo "***DHCP Server Identifier***". ¿Coincide con alguno de los que has anotado en la tabla?

d) Con la ayuda del comando *ipconfig /all* averigua a quién pertenece la dirección IP origen de estos datagramas (DHCPOFFER). ¿Qué conclusiones puedes sacar acerca de la localización de los servidores DHCP de la UPV con respecto a la subred en la que está tu equipo?

e) Compara los valores del campo "DHCP Server Identifier" de los mensajes DHCPOffer restantes que aparecen en la captura. ¿Cuántos servidores DHCP distintos están contestando?

Ejercicio 5. Analizamos ahora el mensaje DHCPREQUEST con el que contesta el cliente a uno de los servidores que le ha realizado una oferta.

a) Completa la siguiente tabla con la información sobre este mensaje:

Tipo de Mensaje (en el campo de opciones DHCP)	
Dir. IP origen del datagrama (en cab. IP)	
Dir. IP destino del datagrama (en cab. IP)	
Puertos origen y destino (en cab. UDP)	
Id. Transacción (en cabecera DHCP)	
Campo dir. IP Cliente (en cabecera DHCP)	
Campo Tu dirección IP (en cabecera DHCP)	
Campo Dir. IP del Agente Retransmisor (cab. DHCP)	

b) Busca entre las distintas opciones del mensaje la dirección IP del servidor DHCP al que el cliente está contestando.

Ejercicio 6. Por último, tenemos los mensajes DHCPACK de los servidores de la UPV que confirman la obtención de la dirección IP por parte del cliente. Busca en estos mensajes las direcciones IP de los diferentes servidores DHCP de la UPV.

Ejercicio 7. Y para terminar, vamos a analizar una nueva captura con el Wireshark con el fin de estudiar el tráfico DHCP que se genera cuando un nodo libera su dirección IP. Para ello abrimos la captura **Captura2Practica3.pcap** (la hemos obtenido ejecutando el comando: ***ipconfig /release***).

¿Qué tipo de mensaje DHCP interviene en este proceso? ¿Quién es el origen y el destino de este mensaje? ¿Hay contestación a este mensaje?