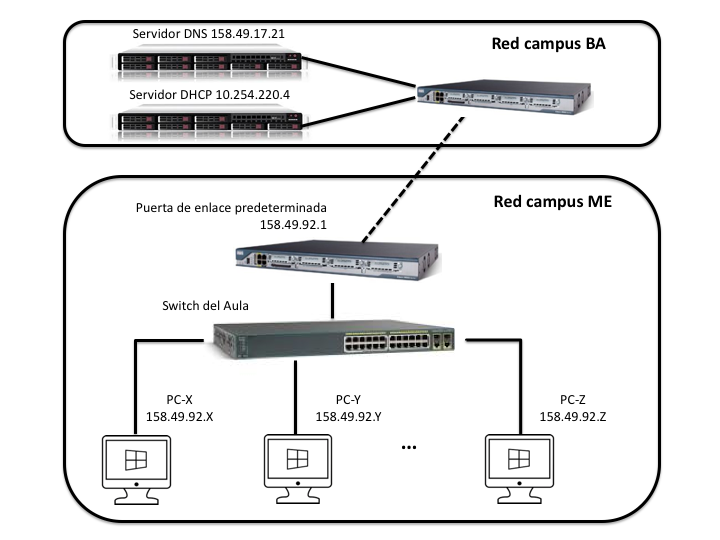
**AL04-3. Investigación de protocolos de capa de Aplicación con Wireshark: DHCP**

*Actividad basada en la traducción del material suplementario del libro Redes de computadores: un enfoque de arriba hacia abajo, 7ª ed, J.F. Kurose y K.W. Ross.*

*“Dime y lo olvido. Muéstrame y recuerdo. Implicarme y entiendo“.* Proverbio chino

**Diagrama de topología**

****

**Objetivos**

**Tarea. Observar el funcionamiento de DHCP**

**Información básica**

En esta actividad de laboratorio, vamos a echar un vistazo rápido a DHCP. Recordemos que DHCP se utiliza ampliamente en la empresa, la universidad y en las redes LAN domésticas cableadas e inalámbricas para asignar dinámicamente direcciones IP a los hosts (así como para configurar otra información de configuración de red). En esta actividad sólo se examinarán los paquetes DHCP capturados por un anfitrión. Si tienes una conexión a Internet en tu casa, lo más probable es que el router esté configurado como un servidor DHCP, por lo que también puedes repetir esta actividad en ese otro contexto.

Recursos necesarios

1 PC con Windows conectado a la red del campus y con la herramienta Wireshark instalada.

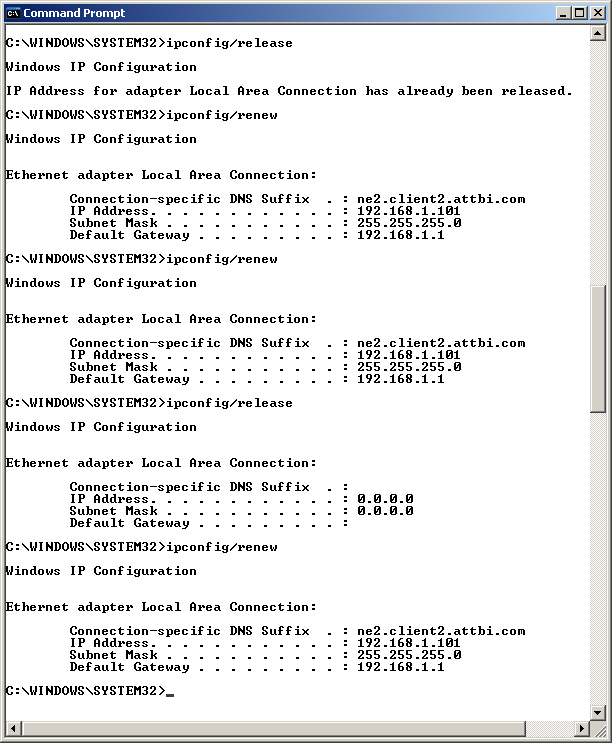
**Tarea. Observar el funcionamiento de DHCP**

Con el fin de observar DHCP en acción, vamos a utilizar varios comandos relacionados con DHCP y capturar con Wireshark los mensajes intercambiados como resultado de la ejecución de los mismos. Haz lo siguiente:

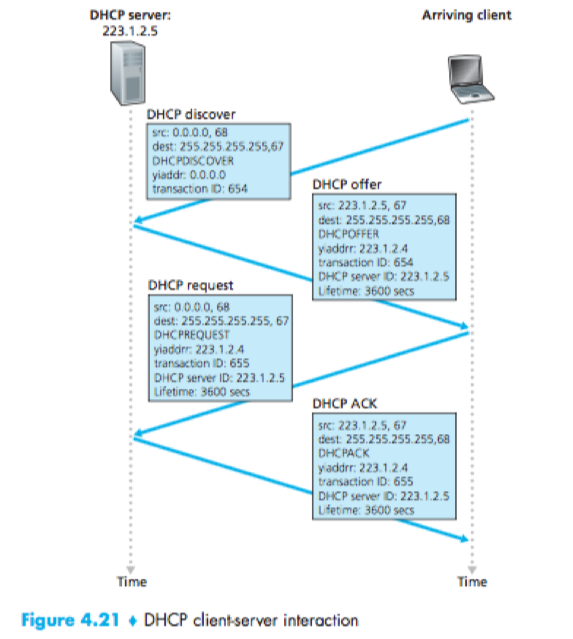
1. Entra en las **Propiedades de Red del adaptador Ethernet (Internet)** y revisa que las siguientes **propiedades del Protocolo de Internet versión 4** estén seleccionadas:
   * **Obtener una dirección IP automáticamente**.
   * **Obtener la dirección del servidor DNS automáticamente.**
2. Después de darle al botón Aceptar, el PC negociará de forma transparente para el usuario la obtención automática de los parámetros de red anteriores con un servidor DHCP. Revisa la configuración obtenida desde el **Símbolo del sistema (CMD)** ejecutando **ipconfig /all.** Completa la siguiente tabla:

|  |  |
| --- | --- |
| **Dirección IP** |  |
| **Dirección MAC** |  |
| **Dirección IP puerta de enlace predeterminada** |  |
| **Direcciones IP servidores DNS locales** |  |
| **Concesión obtenida...** |  |
| **La concesión expira...** |  |

1. A continuación, para poder observar todo el proceso anterior con Wireshark, comenzarás como se muestra en la Figura 1. Escribe **ipconfig /release**. Este comando libera su dirección IP actual, de modo que la dirección IP se convierte en 0.0.0.0 o en blanco.
2. Pon en marcha el analizador de paquetes de Wireshark como ya se ha realizado en actividades anteriores para comenzar la captura de paquetes.
3. Vuelve al **símbolo del sistema** y escribe **ipconfig /renew**. Espera hasta que el comando haya terminado. Esto le indica a tu PC que obtenga una nueva configuración de red. En la Figura 1, el anfitrión obtiene la dirección IP 192.168.1.101.
4. Ahora vuelve de nuevo al **Símbolo del sistema** y escribe otra vez **ipconfig /renew**. Espera hasta que el comando ipconfig /renew haya terminado
5. Para la captura de paquetes.
6. Guarda la captura como **AL04-3.pcapng**.



**Figura 1**. Símbolo del sistema de ventana que muestra la secuencia de comandos ipconfig.

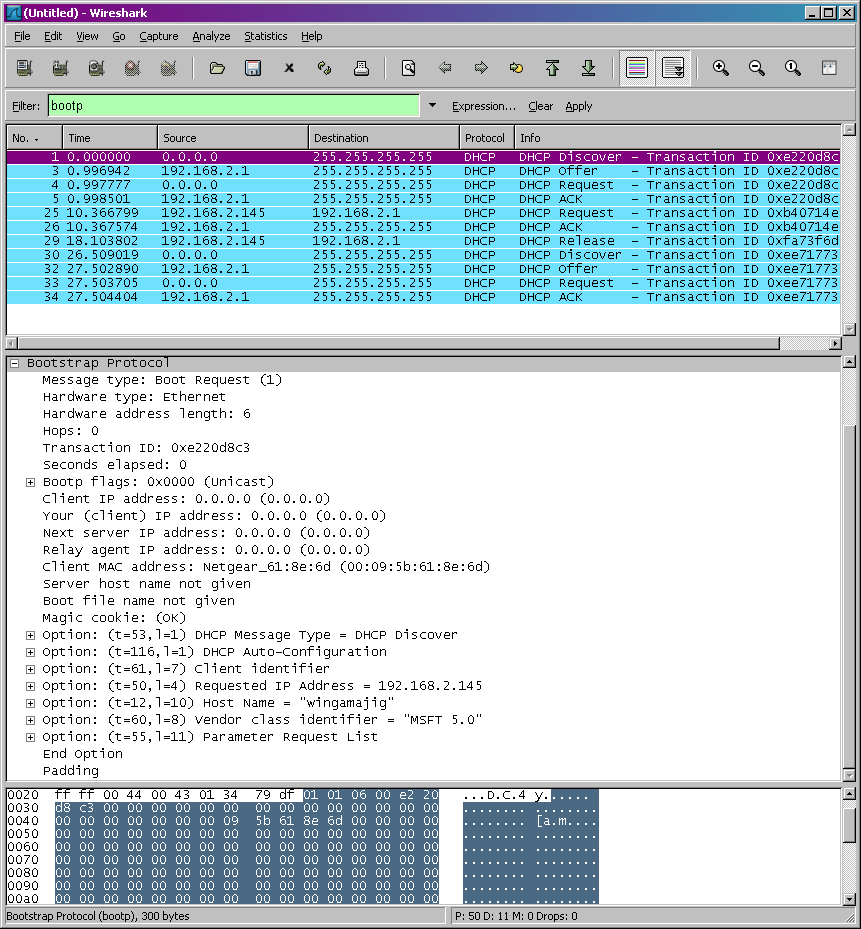


**Figura 2**. Proceso solicitud/respuesta de una petición DHCP.

Ahora vamos a echar un vistazo a la ventana Wireshark resultante. Para ver sólo los paquetes DHCP originados o con destino tu PC, entra en el campo filtro de visualización **bootp&&eth.addr==dirección\_MAC\_PC**. Recuerda que tienes documentada esta dirección en la tabla de más arriba o que puedes obtenerla mediante el comando **ipconfig /all**.

**Nota:** DHCP deriva de un protocolo más antiguo llamado BOOTP. Tanto BOOTP, como DHCP utilizan los mismos números de puerto, 67 y 68. Para ver los paquetes DHCP en la versión actual de Wireshark es necesario introducir “BOOTP” y no “DHCP” en los filtros.

Vemos en la Figura 3, como el comando ipconfig /renew (renovar) generó cuatro paquetes DHCP (primer grupo de mensajes siguiendo el orden de captura): un *paquete de descubrimiento del servidor (DHCP Discover)*, un *paquete de oferta (DHCP Offer)*, un *paquete de solicitud (DHCP Request)* y un *paquete de confirmación (DHCP ACK)*. En la Figura 2 puede verse un diagrama del proceso completo de resolución DHCP.



**Figura 3**. Ventana de Wireshark con el detalle del primer paquete DHCP -DHCP Discover-.

A continuación, responde las siguientes preguntas:

1. Los mensajes DHCP, ¿se envían a través de UDP o TCP?
2. Para cada paquete, indica los números de puerto origen y destino. ¿Serán los mismos números de puerto que en el ejemplo de la Figura 2? Razona tu respuesta.

DHCP Discover puerto origen\_\_\_\_ puerto destino\_\_\_\_

DHCP Offer puerto origen\_\_\_\_ puerto destino\_\_\_\_

DHCP Request puerto origen\_\_\_\_ puerto destino\_\_\_\_

DHCP ACK puerto origen\_\_\_\_ puerto destino\_\_\_\_

1. ¿A quién corresponde la dirección origen de capa de enlace para el paquete DHCP Offer? Razona tu respuesta.
2. ¿Qué encabezado permite diferenciar el mensaje de descubrimiento (Discover) del mensaje de solicitud DHCP (Request)? Indica el número de paquete correspondiente a cada uno de ellos en el primer grupo de mensajes.
3. ¿Cuál es el valor de **Transacción-ID** para el **primer grupo** de mensajes DHCP (Descubrir/Oferta/Solicitud/ACK)? ¿Cuáles son los valores de **Transacción-ID** para el segundo grupo de mensajes DHCP (Solicitud/ACK)? ¿Cuál crees qué es el propósito de este campo identificador?
4. Un host utiliza DHCP para obtener una dirección IP, entre otras cosas. Sin embargo, la dirección IP de un host no se confirma hasta el final del intercambio de los ¡cuatro mensajes! Si la dirección IP no se establece hasta el final del intercambio de cuatro mensajes, entonces, ¿qué direcciones IP se utilizan en los paquetes IP durante el intercambio de esos cuatro mensajes? Para cada uno de los cuatro mensajes DHCP indica las direcciones IP de origen y de destino que se utilizan:

DHCP Discover dir. IP origen\_\_\_\_\_\_\_\_\_\_\_\_ dir. IP destino\_\_\_\_\_\_\_\_\_\_\_\_\_

DHCP Offer dir. IP origen\_\_\_\_\_\_\_\_\_\_\_\_ dir. IP destino\_\_\_\_\_\_\_\_\_\_\_\_\_

DHCP Request dir. IP origen\_\_\_\_\_\_\_\_\_\_\_\_ dir. IP destino\_\_\_\_\_\_\_\_\_\_\_\_\_

DHCP ACK dir. IP origen\_\_\_\_\_\_\_\_\_\_\_\_ dir. IP destino\_\_\_\_\_\_\_\_\_\_\_\_\_

1. ¿Cuál es la dirección IP de su servidor DHCP?
2. ¿Cuál es la dirección IP que el servidor DHCP ofrece a tu PC en el mensaje de oferta? ¿Y cuáles las de los servidores DNS? Indica el nº de paquete que contiene esa información.
3. Explica el propósito del campo **Option: (3) Router** y **Option: (1) Subnet Mask** en el mensaje de oferta DHCP:
4. Explica también el propósito del campo **Tiempo de concesión** (**Option: (51) IP Address Lease Time**). ¿Cuánto tiempo es ese tiempo en tu captura?